New Privacy-Preserving Architectures for Identity-/Attribute-based Encryption

by

Sze-Ming Chow

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Computer Science
Courant Institute of Mathematical Sciences
New York University
September 2010

Yevgeniy Dodis

Victor Shoup

Acknowledgments

I am privileged to be a student of Yevgeniy Dodis and Victor Shoup, my co-advisors at New York University. I am grateful for this opportunity. Discussions with Yevgeniy are always fruitful, in particular, have given me inspiration of the first part of the result in this thesis. Apart from his technical guidance, I am thankful for his advice and help in my professional development. Sincere thanks go also to Victor Shoup, for all his support and advice, the belief he puts in me, and his insightful comments and suggestions of future directions regarding the results of this thesis.

I thank Kristin Lauter for hosting me in Microsoft Redmond. My internship experience with the Cryptography group managed by Kristin is excellent. Part of my current research is influenced by her vision. I was lucky to work with Melissa Chase and Seny Kamara when I was with Microsoft. I would not be so productive in that summer without them. I also thank them for sharing their research problems with me. Special thanks go to Melissa. I met her when she has just graduated but she is already a good mentor. I am thankful to have worked with her, and all her work from our co-authored paper which I reported here.

I would like to thank Kenneth Paterson for his invaluable assistance and suggestions given when part of the result in this thesis was published in a conference, thank Brent Waters for letting me to work on his idea which is integral to the second part of this thesis, and thank for the feedback from all anonymous reviewers.

During my PhD study I am fortunate to have several institutions and research groups hosting me as a visitor or as an intern. I am grateful for all the arrangements and kind hospitality of all these places. Thanks to Tatsuaki Okamoto and Masayuki Abe for mentoring me in the trainee

program of Nippon Telegraph and Telephone Corporation. Thanks also go to other members of the NTT Information Sharing Platform Laboratories (a group that is too large to list each of you here). Living in Japan is awesome especially when my fellow interns Claudio Orlandi and Sanjam Garg are around. Thanks to Brent Waters for hosting me in The University of Texas, Austin. Thanks also go to Allison Lewko, and I am in debt to Yannis Rouselakis for generously sharing his project with me after we found out that we independently reached a similar result. Thanks to Alfred Menezes and his arrangement in connecting me to other members in Centre for Applied Cryptographic Research, the University of Waterloo. Thanks to Ronald Rivest for sharing one of his electronic voting project ideas with me when I was visiting Massachusetts Institute of Technology. Thanks to Volker Roth, Eleanor Rieffel and Wolfgang Polak for mentoring me when I was a research intern of Fuji Xerox Palo Alto Laboratory. Thank also go to other members and interns of FXPAL. That is the first time I work and live outside New York after I moved to United States, which will be a dear memory to me. The summer I spent in the Microsoft headquarter with Ariel Feldman, Vipul Goyal, David Gruenwald, Dan Shumow and other interns is also full of fun. Thanks also go to Josh Benaloh, Peter Montgomery, Ramarathnam Venkatesan and other members of MSR. Last but not the least; I am thankful to Colin Boyd and Juan Manuel González Nieto for the opportunity of visiting the Information Security Institute of Queensland University of Technology for five months. That is the first time I live outside Hong Kong, I thank Riza Aditya, Raymond Choo, Praveen Guaravaram, Kun Peng, Kenneth Wong, Charles Woo, and other members of QUT for their help, friendship, and discussions.

I wish to take this opportunity to say thank you to my fellow groupmates in NYU: Joël Alwen, Adriana Lopez-Alt, Nelly Fazio, Antonio Nicolosi, Prashant Puniya, Aristeidis Tentes, Shabsi Walfish, Daniel Wichs, and visitors Dario Fiore and Luan Ibraimi. I am in debt to the help of Carl Bosley otherwise I would not have a chance to visit MIT. Special thanks go to Kristiyan Haralambiev. We went to NYU on the same year, we have the same advisor, and it is good to have his accompany during my study here.

I would also like to thank Lakshminarayanan Subramanian, who is like my third advisor in NYU. I thank him for pushing me to be a better researcher and all his advices. I am also grateful to have worked with Jinyang Li, Nguyen Tran and Matt Tierney. I would like to thank to all the faculty members, staff, and my fellow graduate students in Courant Institute of Mathematical

Sciences, especially those in the 715 Broadway building or has shared the office space with me in Room 715, for providing me a nice study environment.

I am fortunate to have met many research buddies, Man Ho Au, Cheng-Kang Chu, Kai-Min Chung, Apu Kapadia, Pierre Lai, Jin Li, Hsiao-Ying Lin, Feng-Hao Liu, Joseph Liu, Raphael Phan, Willy Susilo, Patrick Tsang, Cong Wang, Jian Weng, Guomin Yang, Wun-She Yap, Ching-Hua Yu, Tsz Hon Yuen, Miaomiao Zhang, and Hong-Sheng Zhou. They are always available when I want to talk with someone about research ideas or research life. I am also thankful to the contributions of Robert Deng, Xiaotie Deng, Bok-Min Goi, Swee-Huay Heng, Wenjing Lou, Changshe Ma, Kui Ren, Sean Smith, Qian Wang, Yanjiang Yang, Jianying Zhou and all my other collaborators who contributed to the success of our joint papers.

I am grateful to K.P. Chow, Lucas Hui, Victor Wei, Duncan Wong and Siu Ming Yiu. Without their encouragement and support I would not have the opportunity or courage to finish my PhD study overseas.

I am privileged to hold my thesis defense with Rosario Gennaro, Craig Gentry and Moti Yung on the thesis committee. Thank you for their help and sparing their invaluable time despite their busy schedules.

My heartfelt thank to my friends who shared with me all the ups and downs, the fun time as a tourist and the hard time as an international student or a foreigner.

My love and gratitude to my parents and my grandmother who let their only child or only grandchild to spend so many years living outside Hong Kong.

I am grateful to a lot of people for the completion of this thesis and I am sure (and sorry) that I have not listed them all here. Thank you!

Abstract

The notion of identity-based encryption (IBE) was proposed as an economical alternative to public-key infrastructures. IBE is also a useful building block in various cryptographic primitives such as searchable encryption. A generalization of IBE is attribute-based encryption (ABE). A major application of ABE is fine-grained cryptographic access control of data. Research on these topics is still actively continuing.

However, security and privacy of IBE and ABE are hinged on the assumption that the authority which setups the system is honest. Our study aims to reduce this trust assumption.

The inherent key escrow of IBE has sparkled numerous debates in the cryptography/security community. A curious key generation center (KGC) can simply generate the user's private key to decrypt a ciphertext. However, can a KGC still decrypt if it *does not* know the intended recipient of the ciphertext? This question is answered by formalizing KGC anonymous ciphertext indistinguishability ($\mathcal{ACI} - \mathcal{KGC}$). All existing practical pairing-based IBE schemes without random oracles do not achieve this notion. In this thesis, we propose an IBE scheme with $\mathcal{ACI} - \mathcal{KGC}$, and a new system architecture with an anonymous secret key generation protocol such that the KGC can issue keys to authenticated users without knowing the list of users' identities. This also matches the practice that authentication should be done with the local registration authorities. Our proposal can be viewed as mitigating the key escrow problem in a new dimension.

For ABE, it is not realistic to trust a single authority to monitor all attributes and hence distributing control over many attribute-authorities is desirable. A multi-authority ABE scheme

can be realized with a trusted central authority (CA) which issues part of the decryption key according to a user's global identifier (GID). However, this CA may have the power to decrypt every ciphertext, and the use of a consistent GID allowed the attribute-authorities to collectively build a full profile with all of a user's attributes. This thesis proposes a solution without the trusted CA and without compromising users' privacy, thus making ABE more usable in practice.

Underlying both contributions are our new privacy-preserving architectures enabled by borrowing techniques from anonymous credential.

Table of Contents

List of Figures

List of Tables

Part I

Background

Chapter 1

Introduction

Secrecy of communication has been a concern of people since ancient times. Encryption "encodes" or "scrambles" data into an "unreadable" form to ensure secrecy. The study carried out in this thesis is to improve the modern encryption systems, which include identity-based encryption and a more general notion of attribute-based encryption. In this chapter, we first take a look of the major steps in the evolution of the idea of encryption – from Caesar cipher before Christ, to identity-based encryption (IBE) and attribute-based encryption (ABE) nowadays. After a discussion on the benefits brought by IBE and ABE over their predecessors, we point out their shortcomings regarding user privacy, and survey existing attempts to address them. Finally, we describe our new architectures for IBE and ABE which constitute the main contribution of this thesis.

1.1 Evolution of Encryption

1.1.1 From Secret-Key Encryption to Public-Key Encryption

Secret writing is what people have been doing over several thousand years. In Greek, it is called "kryptos" (secret) "grapho" (writing), which leads to the English word "cryptography". If you know nothing about Greek, probably "kryptos grapho" is already a kind of secret writing to you. It is an example of encryption by substitution. The Arabs were the first to protect texts by using digits to substitute for letters. The earliest well-known cryptosystem (a system for encoding and

decoding messages using cryptography) dates back to the first century BC, which is known as Caesar cipher now. This is also a type of substitution cipher. The encryption process substitutes each letter in the plaintext (the original message before encryption) by a letter some fixed number of positions down the alphabet.

In the history of cryptology up to 1975, encryption (encoding the plaintext into ciphertext) and decryption (the reverse of encryption) algorithm of all the cryptosystems employ the same key. This means the encryption key ek, held by the principal who encrypts a message, and the decryption key dk, held by the one who will receive the ciphertext and decrypt it, are the same. Taking Caesar cipher as an example, we can consider the fixed number of positions shifted in the plaintext as both the encryption key and the decryption key. Such kind of cryptosystems is known as symmetric-key cryptosystem.

The symmetric nature of the encryption and the decryption keys requires a key to be agreed upon by the two communicating parties by some possibly non-cryptographic means; for example, a face-to-face meeting, such that no one else knows any part of the key. In other words, a prior shared secret should be established by an authenticated and private communications channel before a cryptosystem can be used.

In practice, various difficulties may arise to distribute keys. After all, the task of establishing a secret is closely related to the original goal of an encryption system. In 1975 (when the preprint version of the paper was first distributed), Diffie and Hellman [DH76b] proposed a protocol for establishing a shared secret-key over a public (but still authenticated) communication channel, without using any prior shared secret. Eavesdroppers can still read the transcripts of communication generated during the execution of the protocol, but cannot derivate the session key that the protocol participants compute locally and secretly. The protocol is now known as Diffie-Hellman key exchange, or Diffie-Hellman-Merkle key exchange as suggested by Hellman in 2002, in recognition of the influence by Merkle's work [Mer78] (now known as Merkle's puzzle). This discovery was considered as a brand new concept in the field which was named as *public-key cryptography*, where ek and dk are different and ek can be made public. Public-key cryptosystems are also referred to as asymmetric cryptosystems.

Diffie and Hellman [DH76a] introduced the concept of one-way trapdoor functions and pointed out that their asymmetric nature is very useful in constructing public-key encryption systems.

Informally, it is easy to evaluate the one-way trapdoor function but it is difficult to invert it unless certain trapdoor information is known. The modulo exponentiation used in the Diffie-Hellman protocol is a possible candidate for realizing a one-way function. (Roughly speaking, inverting the modulo exponentiation is known as the discrete logarithm problem.) The knowledge of the exponent may act as a trapdoor for computing function which is otherwise difficult. In 1977, based on the factoring problem, Rivest, Shamir and Adleman proposed a public key encryption scheme (and a digital signature scheme) in Gardner's column on Mathematical Games in Scientific American [Gar77]. Nowadays this cryptosystem is known as RSA named after its inventors [RSA78].

Since then, many encryption, digital signature, key agreement, and other public-key schemes have been developed, such as the ElGamal cryptosystem [Gam84] and the DSA signature [NIS94]. Similar to Diffie-Hellman protocol, their security is related to the intractability of the discrete logarithm problem. In 1985, Koblitz [Kob87] and Miller [Mil85] independently suggest the use elliptic curves in cryptography. Public key systems enabled by elliptic curves often provide smaller key sizes and faster operations for an equivalent level of expected security. The security of elliptic curve based systems relies on the assumption that finding the discrete logarithm (of a random elliptic curve element with respect to a publicly-known base point) is difficult.

1.1.2 From Public Key Encryption to Identity-Based Encryption

The goal of using encryption is to ensure that only the intended recipient can decrypt the message. In public key encryption, the sender specifies the intended recipient by encrypting with respect to the public key ek, such that only the owner of the decryption key dk corresponding to ek is able to decrypt. However, the public key is usually a "random" string that is unrelated to the identity of its owner. When the message recipient is online and authenticated communication channels are available, we can resort to key-exchange protocol like Diffie-Hellman protocol to have confidential communication. But for an unsecured public network such as the Internet, it is not clear how to ensure who is the owner of a key.

While it is difficult for an individual to authenticate all other parties over the network, one can rely on a trusted third party to perform the authentication on behalf. One way to getting this

trust is to rely on the help of an infrastructure which is known as public key infrastructure (PKI). In PKI, a trusted-by-all party called certificate authority (CA) provides a digital certificate to each entity, may it be an individual or an organization. Via the certificate, the CA certifies the relationship between an identity and a public key. In this way, the public key represents an entity in the electronic world, while the corresponding private key can be used to decrypt the encrypted document that is directed to this entity (or can be used to digitally sign an electronic document). A critical component of a certificate is an unforgeable signature issued by the CA which is signing on a user's public key.

Unfortunately, PKI has not been adopted as widely or as quickly as hoped, despite many years of effort. There are many well documented reasons [Gut02] about the difficulty of deploying the technology by the service providers (such as maintaining a gigantic online certificate directory) and the difficulty of using the technology by users (such as the strict online requirement and difficulty of locating the certificate). There is also privacy issue associated: the certificate must be accessible to the user of the PKI system and hence a vast amount of information about the certificate entities is made available to the world. Another major problem is that users must first subscribe to the PKI in order to receive an encrypted message since the message sender must obtain an authorized certificate that contains the public key of the recipient. As potential users are unable to assess the potential value of PKI before subscribing, this creates a "chicken-and-egg" situation.

In 1984, Shamir [Sha84] introduced the notion of identity-based (ID-based) cryptography to solve the certificate management problem (or the public key distribution problem). The feature that differentiates identity-based encryption (IBE) schemes from other public key encryption schemes lies in the way a public and private key pair is set up – every arbitrary string is a valid public key. There is a trusted authority, called the key generation center (KGC), responsible for the generation of private keys after user authentications. Private key generation applies the KGC's master secret key to the users' identities. The major benefit of this approach is to largely reduce the need for processing and storage of public key certificates under traditional PKI. Nevertheless, the advantages come with a major drawback which is known as the *escrow problem*. The KGC could decrypt any message addressed to a user by generating that user's private key. In other words, the KGC is trusted to be not "curious". The associated risks have

been heavily discussed in the literature (e.g., [AAB+97]).

1.1.3 From Identity-Based Encryption to Attribute-Based Encryption

In IBE, the identity associated with a user secret key must match exactly with the identity associated with the ciphertext to make decryption possible. This strict requirement may be considered as a shortcoming in certain scenarios. For example, when someone mistyped a single character when inputting the identity string in the encryption interface, the ciphertext can never be decrypted by the intended recipient. While it may not be a perfect example to illustrate that some error tolerance is desirable (e.g., should we allow "Sherman" to decrypt the ciphertext for "Sheryl"?), there do exist applications where such an error is natural and should be tolerated, such as using noisy biometric measurements as identities. In view of this, Sahai and Waters [SW05] proposed a fuzzy IBE scheme, which some error around the chosen identity can be tolerated.

Further generalizing this concept, fuzzy IBE can be used to support "attribute-based encryption" (ABE) [SW05], in which encryption can be done with respect to a set of entities who share a certain set of attributes. For example, in an enterprise scenario, some classified documents related to the recruitment of new research staff might be encrypted in a way such that either the long-term staff from the research department or the employee at the management level from the human-resource department can decrypt.

One may consider that the functionality of ABE can be realized by composing multiple IBE systems. Taking the above example, an authority of the system may assign keys for the attributes "long-term", "research", "management" and "human-resource" as identity strings. That is roughly the underlying idea of the older IBE-based access control systems [Sma03, BHS04]. However, in these systems, malicious users may collude together by sharing their secret keys, such as creating a composite key for "management" level of "research" department when a human-resource manager and a short-term research staff collude. For both biometric applications and access control applications, it is essential for an ABE scheme to have collusion resistance, which guarantees that two colluding users cannot pool their keys to decrypt a message that they are not entitled to.

The Need for Multiple Authorities. The deployment implications of earlier ABE systems such as [SW05, GPSW06] may not be entirely realistic, in that it assumes the existence of a single trusted party who monitors all attributes and issues all decryption keys. Instead, we often have different entities responsible for monitoring different attributes of a person, e.g. the Department of Motor Vehicles tests whether you can drive, a university can certify that you are a student, etc. Thus, Chase [Cha07] gave a multi-authority ABE scheme which supports many different authorities operating simultaneously, each handing out secret keys for a different set of attributes. However, as we will see in the next section, there are still some trust issues regarding the well behaviour of the authority which setups the whole system.

1.2 Problem Statement and Previous Work

The problem we would like to solve in this thesis is

"Can we reduce trust the users need to place in identity-/attribute-based encryption?"

1.2.1 Security and Privacy Problems of IBE

Assuming that each user has a unique identity in an IBE system, a natural security requirement is that no attacker can read the plaintext encrypted to a user without knowing that user's private key. However, when the KGC is the attacker, the user has no security at all. This is due to the basic functionality requirement of IBE ensuring that any party who owns the master secret key can perform user private key generation, and all it takes for decryption is a user private key.

Indeed, that is a problem also related to the privacy issue of IBE – the KGC knows the identity of all users of the system since it is responsible for user authentication. The KGC could decrypt any message addressed to a user by generating that user's private key.

1.2.2 Security and Privacy Problems of Multi-Authority ABE

Existing solution for multi-authority ABE is not ideal. There are two main problems: one concern of security of the encryption, the other the privacy of the users.

Security Problem. The solution presented in [Cha07] assumed the presence of a single trusted "central authority" (CA) in addition to the attribute authorities. This CA did not manage any attributes, but was responsible for issuing each user a unique key. It also needs to store the master secrets of each of the attribute authorities, so it has the power to decrypt any ciphertext. This decryption power seems somehow contradictory to the original motivation of distributing control of the attributes over many potentially untrusted authorities. Indeed, the secret owned by this CA is very similar in nature to the master secret key held by the KGC in IBE.

Privacy Problem. The privacy problem of (multi-authority) ABE is more subtle and deserves more explanations. Recall that in a multi-authority ABE system, each authority is responsible for different set of attributes. For efficiency concern of a practical deployment, we want to allow them to issue decryption keys independently, without having to communicate with one another. In order to prevent collusion in such a setting, we need some consistent notion of user identity, as argued in [Cha07]. Otherwise, a user could easily obtain keys from one authority and then give them all to a friend. Hence, each user should have a unique global identifier (GID), which they must present to each authority, and to require that the user prove in some way that he is the owner of the GID he presents. (Further discussion on these properties of GID can be found in [Cha07].)

Unfortunately, the *mere existence of GID* makes it very hard for the users to guarantee *any* kind of privacy. Because a user must present the same GID to each authority, it is very easy for colluding authorities to pool their data and build a "complete profile" of all of the attributes corresponding to each GID. However, this might be undesirable, particularly if the user uses the ABE system in many different settings, and wishes to keep information about some of those settings private.

This situation seems to be unavoidable if all one's attributes are determined by some kind of public identity like a name or a social security number – in that case users will need to identify themselves in order to get the decryption key for each attribute, so privacy is unavoidably compromised. However, there are many attributes which do not belong to this category. The ability to drive is a good example. One should be able to prove the ability to do something in an examination and then get the corresponding credential, without presenting any identifying

information. Alternatively, one might interact with a service via a pseudonym (e.g. a login name) and wish to obtain attributes relating to this interaction without revealing one's full identity.

Regardless, as the attribute-authorities (AAs) are responsible for managing each user's attributes, it seems inevitable that they will learn which subsets of its attributes are held by different users. However, we could imagine applications where some of the authorities are different online service providers giving attributes related to online activities like blog or wiki contributions, access to online news sites, participation in social networking sites, or purchases at an online store. In this case, it would make sense for the user to be able to maintain different, unlinkable attribute sets with each authority. At the same time, it also makes sense for each AA to gather the statistics of their system usage (e.g. the number of users subscribed a particular service as indicated by the number of users who requested a decryption key for a certain attribute) without compromising individual's privacy.

1.3 Existing Works

1.3.1 Attempts in Reducing Trust in the KGC

Inherent key-escrow of IBE is a well-known problem and there are various different attempts to address this problem.

Accountable IBE. In accountable IBE [Goy07] (AIBE), the trust in the KGC is reduced in another dimension, such that the KGC is discouraged from leaking or selling any user secret key. Consider an IBE scheme with an exponential number of user secret keys for any given identity, such that deriving any other secret key from any one of them (without the knowledge of the master secret key) is intractable; if the key issuing protocol ensures that the user can obtain a user private key without letting the KGC know which one it is, we can conclude that the KGC must be the one who leaks the user private key if a user can show the existence of two private keys for the same identity. Goyal [Goy07] showed that Gentry-IBE [Gen06] satisfies the aforementioned properties, and proposed the corresponding key issuing protocol. This protocol also works with our modified Gentry-IBE to be presented in Section 4.4, which is a scheme achieves our new security notion advocated in this thesis.

Another AIBE scheme that is based on Waters-IBE [Wat05] and Sahai-Waters fuzzy IBE [SW05] was also proposed in [Goy07]. Goyal *et al.* [GLSW08] later proposed a black-box accountable IBE (BBAIBE). However, these schemes are not secure under our new security definition ($\mathcal{OW} - \mathcal{KGC}$-security, to be defined in Section 4.2.4) which indicates that accountability and our notion is independent.

KGC-Anonymous ID-based KEM. Independent of our work, anonymity against an honest but curious KGC attack was considered by Izabachène and Pointcheval [IP08]. Their notion of key anonymity with respective to authority (KwrtA), given in the context of identity-based key-encapsulation mechanism (IB-KEM), requires the adversary to guess between the two possibilities of recipient identity, with the master secret key and the challenge ciphertext, but *without* the ephemeral session key. In the context of IBE, the ciphertext always contain a component which encrypts the message by this session key. Taking it away means that the challenge is "incomplete" since partial knowledge of it can be seen in the ciphertext produced by IBE. Hence, the real-world impact on IBE given by their security notion may be unclear. Nevertheless, they showed that an IB-KEM with this KwrtA-anonymity and ID-based non-malleability (another new notion in [IP08]) is a useful tool for constructing password-authenticated key exchange protocols. Relationships between our notion and theirs will become apparent in Section 4.4.3.

Distributed KGCs. A standard method to avoid the inherent key escrow is to split the master secret key to multiple KGCs. The user private key generation is then done in a threshold manner, where each KGC uses a share of the master secret key to generate a private key component for a user. In our approach, the master secret key is not distributed. It is always possible to have this key distribution on top of our idea if an extra layer of protection is desirable.

1.3.2 Shortcomings of Existing Multi-Authority ABE Systems

Similar to the distributed KGC approach in IBE, it seems natural that one might want to divide control of the various attributes in an ABE system over many different authorities. Prior to our work, the only multi-authority (key-policy) ABE schemes we are aware of are Chase's original proposal [Cha07] and the recent Lin *et al.* extension [LCLS08]. Both schemes operate in a setting

where multiple authorities are responsible for disjoint sets of attributes. The disadvantages of Chase's scheme have already been discussed in Section 1.2.2.

The scheme of Lin *et al.* [LCLS08], like the scheme we will present in this thesis, has the advantage that it does not rely on a central authority. However, their scheme only achieves *m-resilience*, in that security is only guaranteed against a maximum of m colluding users. (In contrast, the results of [Cha07] and our new results consider a much stronger model, which remains secure against any number of colluding users.) And this is not merely an issue of formal security: Lin *et al.* demonstrated a collusion attack of $m+1$ users [LCLS08]. In their scheme m is the number of secret keys that each authority obtains from a distributed key generation protocol. (This also means m must be determined when the system is initialized.) Clearly, for a large-scale system, m should set reasonably high in order to guarantee security (a very loose desirable lower bound should be N^2, where N is the number of authorities). This imposes burdens on the interactive distributed key generation protocol among all the authorities, and on their secure storage. Finally, $O(m)$ online modular operations are required by each authority to issue secret keys to a user. We further note that this weaker notion of security seems undesirable. It may be of commercial interest to have as many users as possible, yet it simultaneously increases the risk of being compromised. (Even if users themselves are not malicious, one might worry about malware on a user's machine, or information leaked unintentionally through side channels.) Thus, we argue that it is still a very important open problem to design an *efficient* and *secure* multi-authority ABE scheme without a trusted CA, and this is one of the problems we will attempt to solve here.

An attempt to devise a multi-authority (ciphertext-policy) ABE scheme has been made in [MKE09], under the naming of S distributed ABE. However, there exists a special authority for creating key for each user, and the master secret for doing so is also a trapdoor which allows decryption of every ciphertext.

1.4 Our Contributions

We formally study how the "inherent" escrow can be removed from identity-based encryption. Our approach addresses this problem in a new dimension that has not been considered before.

The solution is more than a formalization of the new security requirement and a construction of an IBE scheme that satisfy the new requirement. We also propose a new architecture that is not only privacy-friendly to the users but also makes the authentication process more convenient.

The second part of the thesis presents a multi-authority ABE with user privacy and without the trusted authority. These requirements are non-trivial to satisfy, due in both cases to the collusion resistance requirement of ABE.

1.4.1 Removing Escrow from Identity-Based Encryption

To escape from the eye of the KGC, two users may execute an interactive key agreement protocol (e.g. [CC07]) to establish a session key known only to themselves, or the recipient can setup another key pair and employ certificateless encryption [ARP03, Cho08, CRR08, DLP08], which is a two-factor encryption method involving both IBE and public key encryption. However, one of the main benefits of IBE is lost – it is no longer true that a ciphertext can be prepared without any action by the recipient.

Can anonymity help confidentiality?

We try to use anonymity against a malicious KGC to fight against the escrow problem. If the KGC *does not* know the intended recipient of the ciphertext, is it still possible for it to decrypt on behalf of the user? We answer this question by introducing the notions of KGC one-wayness ($\mathcal{OW} - \mathcal{KGC}$) and KGC anonymous ciphertext indistinguishability ($\mathcal{ACI} - \mathcal{KGC}$). Current study of IBE only considers anonymity against malicious users' attack, except a recent and independent work [IP08] which considers the application of KGC-anonymous IBE in password-authenticated key exchange but without any application in the context of IBE itself.

We find that (to the best of our knowledge) no existing practical (pairing-based) IBE schemes without random oracles can achieve the weakest notion of confidentiality $\mathcal{OW} - \mathcal{KGC}$, no matter whether it is user-anonymous. In view of this, we show to equip Gentry's IBE scheme [Gen06] with $\mathcal{ACI} - \mathcal{KGC}$ in the standard model.

1.4.2 New Key Management Architecture and Techniques

How can KGC *not* know the users' identities?

Our notion of $\mathcal{ACI} - \mathcal{KGC}$ minimizes the damage of master secret key exposure, providing protection against adversaries who hold the master secret key but not the list of user identities. However, it is natural for the KGC to have this list. By generating all possible user private keys, the KGC can decrypt all ciphertexts. In view of this, we propose a new system architecture to prevent the KGC from knowing it.

We acknowledge that the KGC can always try to derive all possible user private keys according to a certain "dictionary". It seems that there is not much we can do to protect ourselves against a strong adversary like the KGC in this situation. Nevertheless our notion is useful when there is some min-entropy from the identities (e.g. biometric identity [SW05]). On the other hand, nothing can be gained if one always stores the identity with the ciphertext.[1]

We separate the tasks of authentication and key issuing, hence our system architecture employs two parties, namely, an identity-certifying authority (or ICA in short) and a KGC. This setting is different from a typical ID-based cryptosystem, but actually better matches the practice that authentication should be done with the local registration authorities, especially when the KGC is not globally available to authenticate users.

The master secret is still solely owned by the KGC. In particular, it is not spilt across two authorities, in contrast with the distributed KGCs approach. The ICA is responsible for issuing some kind of certificates, but it does not need to store any of them, and only the KGC is required to verify the certificate. After obtaining the private key, users do not require any further interaction with these authorities for decryption. Last but not least, the certificate is not used anywhere else in the system, i.e. the encryption itself is still purely ID-based.

Under this model, we show that one can put anonymous ciphertext indistinguishability in practice. We give a design of the anonymous private key issuing protocol, and present a concrete protocol construction for Gentry-IBE.

[1] Don't write your address on a tag with your key to guide the thief who picked it up.

1.4.3 Removing the Trusted Authority from Multi-Authority ABE

Before our discussion, we first briefly describe how collusion resistance can be obtained for single authority ABE. The key trick is that the components of private key for a given user is associated with a randomly chosen polynomial. When multiple users collude, it is hard for them to combine their private key components in any useful way since the associated polynomials do not match. This technique cannot be easily generalized in multi-authority case, since it relies on the fact that the single authority can generate all components of a user's keys at once, to ensure that they can only be used together, and cannot be combined with any other user's keys.

Now we are ready to discuss the difficulty in removing the trusted CA from a multi-authority ABE. To see why the CA is crucial in Chase's system [Cha07], the intuition was that, for each user, each attribute authority (AA) would use his own secret (not known by other AAs) to generate a share of a system-wide master secret key. The authorities needed to be able to generate these shares *independently* (i.e., without communicating with any other authority during user key issuing). At the same time, in order to prevent collusion it is necessary to use a *different* sharing for each user. This made it difficult to guarantee that all shares always add up to the same master secret. The solution was to have the CA issue each user a special value to cancel out all these shares from the AAs and enable the user to "recover" a function of the system-wide master secret key. Obviously, this computation requires the CA to know the master secret of the system, and the secret information of each AA. This implies that it must also have the power to decrypt any ciphertext.

Thus, in this work, we ask whether it would be possible to instead distribute the functionality of the CA over all of the AAs, so that as long as some of them are honest, the scheme will still be secure. Under an appropriate model, our proposed scheme can be provably secure as long as at least one of the AAs is honest. The new solution uses techniques for distributed pseudorandom functions (PRF) introduced in [NPR99].

1.4.4 Privacy-Preserving Attribute-Based Key Issuing

We also present an anonymous key issuing protocol which allows multi-authority ABE with the following two enhanced privacy properties.

1. We allow the users to communicate with AAs via pseudonyms instead of having to provide their GIDs in the clear, and

2. We prevent the AAs from pooling their data and linking multiple attribute sets belonging to the same user.

This idea is closely related to the notion of anonymous credential, but in fact it is not straightforward to satisfy our security and privacy requirements simultaneously. First, the existing constructions for multi-authority ABE schemes (by Chase [Cha07] and Lin *et al.* [LCLS08]) require that the user presents the GID in the clear to each authority. The authority then uses this GID to generate the user's decryption keys, in order to ensure collusion-resistance. This obviously does not provide any user privacy. On the other hand, if the user was allowed to present a different anonymized value to each authority, then we would no longer be able to guarantee the security of the multi-authority ABE against colluding users. To the best of our knowledge, there is no prior study in privacy-preserving issuing of credential that can be used as a decryption key. Actually, it is arguably easier to design an anonymous credential than an anonymous attribute-based key issuing protocol since the credential is just for verification. In our case, the "credential" should have enough structure that is useful for decryption of the ciphertext according to the embedded policy.

Our protocol is "generic" in the sense that it can be applied to Chase's system (with a little modification) in a rather straightforward manner and our proposed scheme which removes the CA. In the latter case the keys are a bit more complex, so we need somewhat more involved techniques. Moreover, our protocol can been seen as a generalization of the oblivious PRF techniques of Jarecki and Liu [JL09].

1.5 Synopsis

This thesis is structured in three parts.

Part I presents and explains relevant background material. In this chapter, we give an overall idea on evolution of encryption technology, the problem we want to solve in this thesis, how previous work address this problem and our contributions. Next chapter continues our exposition

of encryption technology, in particular identity-based encryption and attribute-based encryption. Their applications will also be described. Chapter 3 contains the technical preliminaries that help the understanding the rest of the thesis.

Part II and Part III present the results of this thesis on identity-based encryption and attribute-based encryption respectively. The organizations of these two parts can be found in the respective chapters. We then conclude the thesis with some possible research directions.

□ End of chapter.

Chapter 2

Related Work

History of the development of identity-based encryption and attribute-based encryption will be presented in this chapter. To motivate this study further, we will discuss various applications of these two notions. Readers who are more interested in the result of this thesis may skip this chapter.

2.1 Development of Identity-Based Encryption

The concept of IBE was formulated by Shamir in 1984 [Sha84]. Satisfactory proposals for IBE did not exist until nearly two decades afterward, when Boneh and Franklin [BF01] and Sakai *et al.* [SOK01] presented two IBE solutions based on pairing and full-domain hash to elliptic curve points (referred to as FDH-IBE).

Reduction Improvement. Since Boneh-Franklin's work (BF-IBE), there has been a flurry of variants. For improving the security reduction in the random oracle model, Attrapadung *et al.* [AFG+06] worked out an FDH-IBE having two public keys for an identity, an idea which was used to improve the security reduction of FDH signature and has been outlined in [GJKW07]. Galindo [Gal05] gave a variant of BF-IBE using another transformation technique (different from the one in [BF01]) to get adaptive chosen-ciphertext security (CCA2) due to Fujisaki and Okamoto [FO00]. Modifying BF-IBE, Libert and Quisquater [LQ05] gave an IBE without redundancy [PP03]. An adoption of the tag-KEM framework [AGKS05] with the implicit KEM (key

encapsulation mechanism) in BF-IBE was proposed in [ZI05] All these schemes share a similar $\mathcal{ACI} - \mathcal{KGC}$ analysis.

Multi-Recipient and Hierarchical ID-Based Encryption (HIBE). In HIBE, the workload of private key generation of a single root KGC is delegated to many lower-level KGCs. Gentry and Silverberg proposed the first full-blown (compared with [HL02]) HIBE (GS-HIBE) [GS02]. For encrypting to multiple recipients more efficiently than in the straightforward approach, multi-recipient IBE was proposed by Baek *et al.* (BSS-MIBE) [BSNS05]. An extension of [BSNS05] with shorter ciphertext was proposed in [LQ05]. These schemes bear similarities to GS-HIBE.

Exponent-Inversion IBE. Sakai and Kasahara [SK03] proposed another IBE (SK-IBE) with a private key derivation algorithm based on exponent-inversion, which is different from FDH-IBE. Instead of using a full-domain hash mapping to points on an elliptic curve, identity strings are hashed to a finite prime-order cyclic group and exponent-inversion is used to derive the user secret key. The CCA2-security of SK-IBE is proven in another work [CC05], albeit in the random oracle model.

The first exponent-inversion IBE in the standard model was proposed by Boneh and Boyen [BB04a] (hereinafter referred to as BB-EIIBE), which offers selective-ID security. (More details about selective-ID security and adaptive-ID security will be given in the next chapter.) Using the chameleon hashing technique due to Waters [Wat05], an extension of [BB04a] with adaptive-ID security was proposed in [Kil07]. Since only the way of hashing the identity is changed, they share the same $\mathcal{ACI} - \mathcal{KGC}$ analysis.

Standard Model (Commutative-Blinding). Boneh and Boyen proposed selective-ID IBE and HIBE schemes in [BB04a] (hereinafter referred to as BB-(H)IBE). Shortly afterward, they gave an adaptive-ID version [BB04b]. Waters simplified [BB04b] in [Wat05], and gave a fuzzy version with Sahai in [SW05]. Extending from [Wat05], Kiltz and Galindo [GK06] gave a CCA2 ID-based key encapsulation without using any explicit transformation, and Kiltz and Vahlis [KV08] gave an efficient CCA2 ID-based key encapsulation scheme using authenticated symmetric encryption. Extending from [SW05], Boldyreva *et al.* [BGK08] gave an IBE with efficient revocation.

Regarding HIBE, [BB04b] and [Wat05] suggested HIBE extensions similar to the approach in [BB04a]. An HIBE with constant-size ciphertext was proposed in [BBG05], which was later made adaptive-ID secure in [CS06d]. Generalizations of the selective-ID model for HIBE, with two HIBE constructions, were proposed in [CS06a]. HIBE with short public parameters was proposed in [CS06b]. A multi-recipient IBE and a parallel key-insulated IBE in standard model were proposed in [CS06c] and [WLCM06] respectively. An ID-based broadcast encryption with adaptive security (GW-IBBE) was recently proposed in [GW09].

Despite their apparent versatility (e.g. different ways of generating public keys from identities), all these schemes use a similar implicit key encapsulation method. As a result, they share a similar $\mathcal{ACI} - \mathcal{KGC}$ analysis (all of them are not $\mathcal{OW} - \mathcal{KGC}$ secure). Finally, [CS05, Nac07] studied the tradeoff between key size and security reduction for [Wat05].

Standard Model (with User Anonymity). Boyen and Waters [BW06] proposed an anonymous IBE scheme (BW-IBE) and the first anonymous HIBE (AHIBE). It has been suggested in [BW06] that AHIBE can obtain adaptive security by the hashing technique of Waters [Wat05]. Similar to the extension of [BB04a] in [Kil07], whether the hashing technique is used or not does not affect the $\mathcal{ACI} - \mathcal{KGC}$ analysis. Recently, [BBG05] has been made anonymous in [SKOS09]. Although these schemes are anonymous, they can be shown to be not $\mathcal{OW} - \mathcal{KGC}$-secure in a similar way to BB-(H)IBE.

Gentry's scheme also provides anonymity in the standard model [Gen06]. It has been extended by Kiltz and Vahlis using authenticated symmetric encryption for better efficiency (KV-IBE) [KV08], and by Libert and Vergnaud for more efficient weak black-box accountable IBE (LV-IBE) [LV09]. We will show that Gentry-IBE can be made $\mathcal{ACI} - \mathcal{KGC}$ secure, but interestingly, its extensions [KV08, LV09] are not. Actually, LV-IBE mixes commutative-blinding and exponent-inversion – its $\mathcal{OW} - \mathcal{KGC}$-security can be broken similar to breaking BB-EIIBE or BB-(H)IBE.

Generalizations of IBE. Recently, there have been many generalizations of IBE, such as hidden-vector encryption [BW07], predicate encryption [KSW10] and spatial encryption [BH08]. However, these specific constructions can be shown to be not $\mathcal{OW} - \mathcal{KGC}$-secure.

Some Other IBE Schemes. The discussion above covers most of the IBE schemes which are constructed from pairings. IBE schemes without pairings exist but they are still relatively inefficient. Some other IBE schemes which were proposed in a weaker security model are also not investigated in this work.

Cocks [Coc01] proposed an IBE scheme based on the quadratic residuosity, encryption is done at bit-level and thus inefficient. Au and Wei [AW04] later proposed an IBE based on the composite degree residuosity, which also encrypts a single bit at a time. It has been shown in [BCOP04] that [Coc01] is not user-anonymous. A space-efficient IBE without pairing which also relies on the quadratic residuosity problem is proposed [BGH07]. An anonymous extension is also presented.

The early IBE systems in standard model are only shown to be secure against a weaker adversary, which is required to commit to an identity it intended to attack before it learns the system parameter. Canetti *et al.* [CHK07] proposed this "selective-ID" model and an IBE scheme in this weaker model without random oracles. However, their construction is inefficient since a pairing operation is required for every bit in the identity.

The HIBE scheme by Horwitz and Lynn [HL02] is not a full-blown one since it supports only two levels of identities and only resistant against limited collusion at the second level. Heng and Kurosawa proposed a k-resilient IBE [HK04] in the standard model, where the adversary can corrupt up to a maximum of k users. The parameter k is pre-determined at the Setup stage and grows linearly with the parameter size. Their scheme coincide with Dodis *et al.*'s key-insulated encryption scheme [DKXY02]. Their scheme's user-anonymity has been utilized to derive a public key encryption with keyword searches [Kha06] (More details in Section 2.3).

2.2 Attribute-Based Encryption for Different Policies

We often identify people by their attributes. ABE is actually a generalization of IBE (identity-based encryption [Sha84]): in an IBE system, ciphertexts are associated with only one attribute (the identity). In 2005, Sahai and Waters [SW05] proposed a system (described in more recent terminology as a key-policy attribute-based encryption (KP-ABE) system for threshold policies) in which a sender can encrypt a message specifying an attribute set and a number d, such

that only a recipient with at least d of the given attributes can decrypt the message. Goyal *et al.* [GPSW06] proposed a KP-ABE scheme which supports any monotonic access formula consisting of AND, OR, or threshold gates. A construction for KP-ABE with non-monotonic access structures (which also include NOT gates, i.e. negative constraints in a key's access formula) was proposed by Ostrovsky, Sahai and Waters [OSW07]. All of these schemes are characterized as key-policy ABE since the access structure is specified in the private key, while the attributes are used to describe the ciphertexts.

The roles of the ciphertexts and keys are reversed in the ciphertext-policy ABE (CP-ABE) introduced by Bethencourt, Sahai and Waters [BSW07], in that the ciphertext is encrypted with an access policy chosen by an encryptor but a key is simply created with respect to an attributes set. Their scheme supports tree-based access structure, but its security is argued in the generic group model (GGM). Subsequently, Cheung and Newport [CN07] proposed a CP-ABE scheme in the standard model. Their scheme supports AND of attributes or negation of attributes, by using different parameters for all three possible cases (positive, negative and wildcard or "don't care") of every single attribute. Finally, Waters [Wat08] proposed CP-ABE constructions based on a few different pairing assumptions in the standard model which work for any access policy that can be expressed in terms of a linear secret-sharing scheme (LSSS) matrix.

Apart from increasing the expressibility of the access control policy, Nishide, Yoneyama and Ohta [NYO08] considered partially-hidden encryptors-specified access structures. Their scheme extended [CN07] to multiple values (more than just yes and no) for each attribute by extending the size of the system parameters. One of their schemes has proof given in the standard model. Li *et al.* [LRZW09] proposed anonymous CP-ABE schemes supporting multi-values with short system parameters, in the random oracle model. Anonymity in this work means that everyone except those who are eligible to decrypt the ciphertext cannot tell who can decrypt the ciphertext, i.e., the ciphertext policy specified in the ciphertext.

For design approaches of ABE schemes, Goyal *et al.* [GJPS08] proposed a transformation from KP-ABE to what they called bounded CP-ABE, by a re-interpretation of KP-ABE and the use of dummy attributes technique. A subsequent work following this direction is done in [LCLX09]. Most of these proposals can be seen as based on an identity-based encryption (IBE) in commutative blinding framework [Boy07]. Boyen [Boy07] built KP-ABE from any IBE in

exponent inversion framework with a certain set of properties.

Attrapadung *et al.* [AI09c] proposed a dual-policy scheme supporting both key-policy and ciphertext-policy, which can be seen as a generalization of CP-ABE of Waters [Wat08] and KP-ABE of Goyal *et al.* [GPSW06]. The notion of attribute set based encryption is proposed in [BKP09] with an instantiation in GGM. Boneh and Waters [BW07] proposed the notion of hidden vector encryption, and Katz, Sahai, and Waters [KSW10] proposed an inner-product predicates encryption scheme. These two schemes are very general and in particular can be used to realize an anonymous CP-ABE, albeit at the price of high computational complexities relative to schemes like [NYO08, LRZW09].

There are a few work studying broadcast and revocation issues. The scheme in [EMN+09] achieves constant ciphertext length for policy without wildcards. Since AND-gates are considered, the lack of wildcards mean one cannot "skip" any of the attributes, which makes the choice of policy rather limited. The scheme of Lubicz and Sirvent [LS08] achieves ciphertext size which is independent of the number of positive attributes, yet linear in the number of negative attributes. Their scheme is non-anonymous by design and its proof is given in the GGM. Attrapadung and Imai [AI09b] proposed an ABE scheme where the broadcast is made with respect to identities, but not according to attributes. The same authors [AI09a] also proposed a KP-ABE scheme supporting two different modes of revocation. They claim that their underlying methodology can be applied on CP-ABE. Mediated CP-ABE based on [CN07] has been described in [IPN+09], which supports instant revocation by decryption mechanism similar to that of [HJSNS08].

In this thesis, we will look only at the KP-ABE setting. We will look at both the simple threshold, and the more complicated monotonic access structure case, and will build a construction based on the same assumptions as Sahai and Waters [SW05] and Goyal *et al.*[GPSW06]. Both non-monotonic access structures and the ciphertext policy schemes require much stronger assumptions, and very different techniques, so we will not consider these cases in our work.

2.3 Applications of IBE and ABE

Applications of IBE. IBE found applications in many scenarios. To name a few:

1. Light-weight Secure Email (e.g. [AHR05, SD03]): For PKI-based solution, one must retrieve the other party's certificate before sending encrypted message. The public key is some non human-memorizable string, so certificate look-up is essential. Another major problem is users must first subscribe to PKI in order to receive an encrypted message. Thus has created a "chicken and egg" situation, as potential users are unable to assess the potential value of PKI before subscribing.

   With IBE, public key can just be derived from an user's identity, which is a meaningful string instead of random-looking bytes. Moreover, one can encrypt message to virtually anyone in the world as long as the recipient's identity is known. The recipient can obtain the corresponding private key after feeling the need to decrypt the messages. It also provides seamless client mobility as the recipient can use any device to obtain the private keys from anywhere.

2. Role-Based Access Control (RBAC) (e.g. [MBH03]): We can control the access of information by using the policy as the public key for encryption, where the corresponding private key will only be generated for those who satisfy the policy requirement. In this way IBE realizes a RBAC system without trusted data storage.

3. Workflow (e.g. [ARMLS06]): Workflow refers to a system in which actions must be performed in a particular order. Cryptographic workflow means a certain cryptographic operation (e.g. decryption) is a privileged action that can only be executed by users having completed other tasks, and thus granted a certain credential. With a similar idea as RBAC, cryptographic workflow can be realized easily with IBE.

4. Network Security (e.g. [AAK+02, SD03]): IBE also finds its application in network security. For examples, the use of addressed based keys as the public key in securing IPv6 neighbor and router discovery [AAK+02], and removing the trouble of dealing with certificates in IP security and transport layer security [SD03].

Relations with Other Primitives. IBE is also powerful as a cryptographic building block. One of the distinctive features is that there is an exponential number of identities "embedded" in the relatively short system parameters, which opens many possibilities in application.

1. Public Key Encryption Secure against Chosen-Ciphertext Attack (CCA2): Boneh, Canetti, Halevi, and Katz [BCHK07] showed that a CCA2-secure public-key encryption scheme can be constructed from any identity-based encryption (IBE) which is only secure against selective-identity and chosen-plaintext attack. This is a new approach of constructing CCA2-secure scheme without relying on the standard approach of non-interactive proofs of "well-formedness".

2. Public Key Encryption with Keyword Search (PEKS): Anonymous IBE has been utilized to build PEKS [BCOP04, ABC+08]. Informally, an IBE scheme is anonymous when the ciphertext does not reveal the intended recipient to any one other than the intended recipient himself or herself. Part of the results in this thesis is closely related to the notion of anonymous IBE and it will be discussed in more details later, such as in Section 4.2.1 and Section 5.6.

3. Password Authenticated Key Exchange (PAKE): The PEKS application requires anonymity against user attack. Anonymity against KGC has been leveraged to build PAKE [IP08]. This gives yet another cryptographic application of IBE. Their security model and significance in the context of IBE will be discussed shortly.

4. Verifiable Random Function (VRF): Informally speaking, VRF is a pseudorandom function (will be reviewed in Section 3.4.1) that the owner of the function's secret seed can generate a non-interactive proof such that anyone with the proof can verify the function was correctly evaluated for a particular input value. Instead of relying on anonymity in the cases for PEKS or PAKE, another "special" properties of IBE are extracted which are shown to be useful in constructing VRF by Abdalla, Catalano and Fiore [ACF09].

5. Oblivious Transfer (OT): In the basic notion of oblivious transfer, one party has many pieces of data, one and only one piece of them should be transferred to a requester, and the requester does not want to leak the choice of the interested piece of data. Similar to IBE, OT protocols turn out to be a very useful primitive for realizing many cryptographic goals. Green and Hohenberger built an blind key extraction protocol on top of an IBE scheme which is useful for implementing simulatable OT [GH07]. This notion is similar to

the notion of anonymous secret key issuing protocol introduced in this thesis and we will contrast their differences in Section 5.5.

6. Public Key Encryption with Non-Interactive Opening (PKENO): In PKENO, the receiver of a ciphertext can verifiably reveal the decryption result of the ciphertext, without compromising the confidentiality of other ciphertexts. The idea of building PKENO from IBE has been informally discussed by Damgård and Thorbek [DT07] which was later formalized by Damgård *et al.* [DHKT08], with a generic construction from IBE and a direct pairing-based construction. The result has latter been improved [Gal09, GLF+10].

Applications of Attribute-Based Systems. For applications of ABE, Pirretti *et al.* [PTMW06] demonstrated an information management architecture based on ABE which utilized an optimized implementation of the original Sahai-Waters scheme. Their result showed that complex policies can be supported efficiently if one buys the random oracle heuristics. Traynor *et al.* [TBEM08] pointed out that the investigations of Pirretti *et al.* [PTMW06] just considered a maximum of 32 attributes, and showed that it is undesirably slow for ABE systems with a much larger set of attributes, when used as a massive-scale broadcast encryption mechanism. They thus proposed a tiered construction using the concept of group attributes and individual attributes, for efficient join and leave operation in ABE-based conditional access systems, such as IPtv and satellite radio.

ABE also helps in solving the group key management problem where a group controller maintains a shared data encryption key to encrypt multicast traffic to a subset of current group members. Cheung *et al.* [CCKN07] realized the membership revocation without the re-distribution of key to all remaining group members by defining attributes in a way that any subset of users can be distinguished from the rest using a combination of attributes. Recently, Boldyreva, Goyal and Kumar [BGK08] used ABE to solve the revocation problem of identity-based encryption as well. Roughly speaking, each encryption is done under an identity and a time, which correspond to two attributes. Attribute key for current time period will be issued to unrevoked user.

Other than encryption, different attribute-based cryptographic schemes have been examined in some recent works, such as attribute-based authentication [MPR08, SY08, LK10].

□ **End of chapter.**

Chapter 3

Preliminaries

Explanation of the notations to be used in the rest of this thesis, the cryptographic groups to be used in our proposed constructions, and the complexity assumptions our work rely on will be given in this chapter. A few useful building blocks used in our construction will also be reviewed briefly. The end of this chapter presents the existing formal definitions of the framework and the security requirements of identity-based encryption and attribute-based encryption. Readers can skip the latter parts of this chapter if they are familiar with the literature.

3.1 Notations

Most cryptographic primitives require randomness, such as in the generation of secret keys. We use $x \in_R S$ to denote the operation of picking an element x at random and uniformly from a finite set S. For a probabilistic algorithm $\mathcal{A}$, $x \xleftarrow{\$} \mathcal{A}$ assigns the output of $\mathcal{A}$ to the variable x. We write PPT for probabilistic polynomial time. Sometimes, we may want the random coin used by an algorithm to come from a public common reference string, which we denote by CRS. For some algorithms considered in this thesis, a special symbol "$\perp$" can be a possible output, which generally denotes the input is "invalid". We use the notation $\varnothing$ to denote an empty set.

This thesis mostly deals with the computational security settings, where the security level of a system depends on the number of bits to be used. For $\lambda \in \mathbb{N}$ where $\mathbb{N}$ denotes the set of natural numbers, 1^λ denotes a string of λ ones. If x is a string, $|x|$ denotes its length, e.g., $|1^\lambda| = \lambda$.

We define the security of a system in terms of the maximum probability that an adversary can "break" the system. We quantify this probability with the standard notion of negligible function as defined below.

Definition 3.1 (Negligible Function)**.** A function $\epsilon : \mathbb{N} \to \mathbb{R}$ which maps a natural number to a real number is called *negligible* ($\mathsf{negl}(\lambda)$) if for every constant $c \geq 0$ there exists an integer λ_c λ_c such that $\epsilon(\lambda) < \lambda^{-c}$ for all $\lambda > \lambda_c$.

The cryptosystems studied in this thesis are based on algebraic groups. All groups in this thesis are represented in a multiplicative form. The order of a group depends upon λ, which is chosen according to the desired level of security. In most cases, the order is a prime number p. So the exponent is an element in $\mathbb{Z}_p$, a set of integers modulo p. For composite order group, the factors of order are usually expected to be dependent on λ. We use $\mathbb{G}$, $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ to represent the groups.

3.2 Bilinear Groups

The study in this thesis is largely related to cryptosystems based on algebraic groups called *bilinear groups*, which are groups with a bilinear map. A common cryptographic practice to generate these groups is to employ elliptic curve groups defined over finite fields

Definition 3.2 (Bilinear Map)**.** Suppose $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are three multiplicative cyclic groups of prime order p. A *bilinear map* $e(\cdot, \cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a deterministic function that takes as input one element from $\mathbb{G}_1$, one element from $\mathbb{G}_2$, and outputs an element in target group $\mathbb{G}_T$ which satisfies:

1. *Bilinearity*: For all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ $a, b \in \mathbb{Z}_p$, $e(u^a, v^b) = e(u, v)^{ab}$.

2. *Non-degeneracy*: $e(g_1, g_2) \neq 1$ where g_1, g_2 are a generator of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.

Bilinear maps are also referred to as pairings, named after the Weil pairing [GHS02, BLS04] and the Tate pairing [GHS02] which give typical implementations of bilinear maps.

Definition 3.3 (Bilinear Group)**.** Let $\mathsf{BDH\_Gen}(1^\lambda; \mathfrak{S})$ be a PPT algorithm which takes the

input of a security parameter 1^λ and possibly a CRS $\mathfrak{S} \in \{0,1\}^{\mathrm{poly}(\lambda)}$, outputs the context parameters for bilinear groups $(p, \mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle, \mathbb{G}_T, e(\cdot,\cdot))$ where:

1. $\mathbb{G}_1$ and $\mathbb{G}_T$ are (multiplicative) cyclic groups of prime order $p = \Theta(2^\lambda)$;
2. each element of $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ has a unique binary representation;
3. the description of the groups in the parameters include the respective generators such as $\mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle$;
4. the group action in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are all efficient (which takes polynomial time in λ);
5. $e(\cdot,\cdot)$ is a bilinear map and it is efficient to compute $e(u,v)$ for all $u_{\in}\mathbb{G}_1$ and $v \in \mathbb{G}_2$.

We call any three algebraic groups which satisfy the above abstract definitions *bilinear groups*.

We can classify bilinear groups into two categories by the existence of efficiently-computable isomorphisms between the groups $\mathbb{G}_1$ and $\mathbb{G}_2$.

1. Double Isomorphisms: There exists a pair of distortion maps (ψ, ψ') where ψ is an efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$. Similarly, ψ' is an efficiently computable isomorphism from $\mathbb{G}_1$ to $\mathbb{G}_2$, with $\psi'(g_1) = g_2$, and $\psi' = \psi^{-1}$. It is well known that efficient isomorphisms exist for supersingular curves [Ver01, BF03].

   In this case, the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ can be treated abstractly as a single group. We can then use simplified notations of $\mathbb{G} = \mathbb{G}_1 = \mathbb{G}_2$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

2. Single-or-None Isomorphisms: There does not exist an efficiently computable isomorphism ψ' from $\mathbb{G}_1$ to $\mathbb{G}_2$. (An efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ may or may not exist.) It is conjectured that bilinear groups with single-or-none isomorphism can be realized using ordinary elliptic curves such as [Cha06].

3.3 Complexity Assumptions

We start by the well-known discrete logarithm problem and the decisional Diffie-Hellman (DDH) problem.

Definition 3.4. Discrete Logarithm Problem (DLP): Given two group elements g and h, find an integer $a \in \mathbb{Z}_p$ such that $h = g^a$ whenever such an integer exists.

Definition 3.5. Decisional Diffie-Hellman (DDH) problem in prime order group $\mathbb{G} = \langle g \rangle$: On input $g, g^a, g^b, g^c \in \mathbb{G}$, decide if $c = ab$ or c is a random element of $\mathbb{Z}_p$.

DDH problem is easy in bilinear groups with double isomorphism, but one may hope that it is difficult in $\mathbb{G}_T$. The following problem is somewhat along this line of thinking.

Definition 3.6. Let algorithm $\mathsf{BDH\_Gen}(1^\lambda)$ output the parameters $(p, \mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle, \mathbb{G}_t, e(\cdot,\cdot))$ where there is an efficiently computable isomorphism ψ from $\mathbb{G}_2$ to $\mathbb{G}_1$. The Decisional Bilinear Diffie-Hellman (DBDH) problem is defined as follows: given $g_1 \in \mathbb{G}_1$, $g_2, g_2^a, g_2^b, g_2^c \in \mathbb{G}_2$ and $Z \in \mathbb{G}_T$ as input, decide if $Z = e(g_1, g_2)^{abc}$ or $e(g_1, g_2)^R$ for $R \in_R \mathbb{Z}_p$.

The security of the ABE schemes by Sahai-Waters [SW05], Goyal *et al.* [GPSW06], Chase [Cha07], and our ABE construction relies on the intractability of the DBDH problem.

For our IBE, we introduce two problems whose names are inspired by the decisional linear problem [BBS04].

Definition 3.7. Decisional Bilinear Problem (DBP): Given two $\mathbb{G}$ elements g and g^a, two $\mathbb{G}_T$ elements $e(g,g)^b$ and $\hat{t}$, output 'yes' if $\hat{t} = e(g,g)^{ab}$ and 'no' otherwise. We name $(g, g^a, e(g,g)^b, e(g,g)^{ab})$ as a decisional bilinear tuple.

Definition 3.8. Modified Decisional Bilinear Problem (MDBP): Given $g, g^a, g^{b^{-1}} \in \mathbb{G}$, and $e(g,g)^b, \hat{t} \in \mathbb{G}_T$, output '$\mathsf{yes}$' if $\hat{t} = e(g,g)^{ab}$ and 'no' otherwise.

An oracle for solving the first one makes solving the DBDH problem easy.

Lemma 3.1. *DBDH assumption implies Decisional Bilinear assumption.*

Proof. Given $(g, g^a, g^b, g^c, \hat{t})$, computes $e(g,g)^{b'} = e(g^b, g^c)$ where $b' = bc$, feeds $(g, g^a, e(g,g)^{b'}, \hat{t})$ to the DBP oracle and outputs its answer. □

Now we review a number-theoretic problem related to an existing IBE system.

Definition 3.9. (Decisional) q-Bilinear Diffie-Hellman Exponent Problem (q-BDHEP): Given $(q+2)$ $\mathbb{G}$ elements $(g', g, g^\alpha, \cdots, g^{\alpha^q})$, and one $\mathbb{G}_T$ element $\hat{t}$, output 'yes' if $\hat{t} = e(g^{\alpha^{q+1}}, g')$ and 'no' otherwise.

A stronger version of q-BDHEP is assumed difficult for the security of Gentry-IBE [Gen06]. We remark that the hard problem considered in [Gen06] is augmented with ${g'}^{\alpha^{q+2}}$ and q equals to the number of users compromised by the adversary.

Lemma 3.2. *Decisional 2-Bilinear Diffie-Hellman Exponent assumption implies Modified Decisional Bilinear assumption.*

Proof. Given $(g', g, g^{\alpha}, g^{\alpha^2}, \hat{t})$, set $\theta_1 = g^{\alpha}$, $\theta_2 = g'$, $\theta_3 = g$, $\hat{\theta} = e(g^{\alpha}, g^{\alpha^2})$ and feed $(\theta_1, \theta_2, \theta_3, \hat{\theta}, \hat{t})$ to the MDBP oracle. The input is valid since $\theta_3 = (\theta_1)^{\alpha^{-1}}$ and $\hat{\theta} = e(\theta_1, \theta_1)^{\alpha}$. Let $\theta_2 = \theta_1^{\gamma}$ where $\gamma \in \mathbb{Z}_p$, the MDBP oracle outputs 'yes' if and only if $\hat{t} = e(\theta_1, \theta_1)^{\gamma\alpha}$, since $e(\theta_1, \theta_1)^{\gamma\alpha} = e(g^{\alpha}, g^{\alpha})^{\gamma\alpha} = e(g^{\alpha^3}, g')$. □

Definition 3.10. q-Decisional Diffie-Hellman Inversion (q-DDHI) problem in prime order group $\mathbb{G} = \langle g \rangle$: On input a $(q+2)$-tuple $(g, g^s, g^{s^2}, \ldots, g^{s^q}, g^u) \in \mathbb{G}^{q+2}$, decide if $u = 1/s$ or u is a random element of $\mathbb{Z}_p$.

For our ABE key issuing protocol, we will use a modified version of the Dodis-Yampolskiy pseudorandom function [DY05], suggested in [JL09], which relies on the intractability of the q-DDHI problem in group $\mathbb{G}_1$ of bilinear groups. Note that q-DDHI is solvable when given a DDH oracle, thus we must also make the following assumption:

Definition 3.11. Let $\mathsf{BDH\_Gen}(1^{\lambda})$ output the parameters for a bilinear mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. The eXternal Diffie-Hellman (XDH) assumption states that, for all probabilistic polynomial time adversaries $\mathcal{A}$, the DDH problem is hard in $\mathbb{G}_1$. This implies that there does not exist an efficiently computable isomorphism $\psi' : \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

3.4 Building Blocks

3.4.1 Pseudorandom Function

Pseudorandom function (PRF) is a notion defined by Goldreich, Goldwasser, and Micali [GGM86]. Informally, the output of a PRF cannot be distinguishable by a PPT adversary from a value selected uniformly at random from the range of the function, even the adversary has seen the output of the function for many other inputs.

Definition 3.12 (Pseudo Random Function Family)**.** A family $\mathcal{F} = \langle f_s | s \in \{0,1\}^\lambda \rangle_{\lambda \in \mathbb{N}}$ is called a family of $(\ell(\lambda), L(\lambda))$ *pseudo random function* if

1. $\forall \lambda \in \mathbb{N}, \forall s \in \{0,1\}^\lambda$, $f_s : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{L(\lambda)}$;
2. $\forall \lambda \in \mathbb{N}, \forall s \in \{0,1\}^\lambda$, f_s is polynomial time computable;
3. $\mathcal{F}$ is pseudorandom: for all PPT algorithm $\mathcal{A}$, $|\Pr[\mathcal{A}^{f_s}(1^\lambda) = 1 | s \xleftarrow{\$} \{0,1\}^\lambda] - \Pr[\mathcal{A}^F(1^\lambda) = 1 | F \xleftarrow{\$} \mathcal{R}(\ell(\lambda), L(\lambda))]| \leq \mathsf{negl}(\lambda)$, where $\mathcal{R}(\ell(\lambda), L(\lambda))$ is the space all possible functions $F : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{L(\lambda)}$

3.4.2 Proof-of-Knowledge Protocol

The goal of a proof is to convinces a verifier that a certain statement is true. It is zero-knowledge when the verifier learns nothing except the validity of the assertion, a concept formally defined by Goldwasser, Micali and Rackoff [GMR89]. A proof-of-knowledge (PoK) is a protocol where a verifier can be convinced by a prover about the claimed possession of a certain value w called the witness, which satisfies some publicly known relation R with respect to a commonly known string x.

3.4.3 Secure Multi-Party Computation

In two-party computation, two parties want to jointly compute a public function $f(x_1, x_2)$ from their own secret inputs x_1 and x_2. Informally, a two-party protocol for computing a function f is secure if participants do not learn anything from the protocol execution beyond what is revealed by the output of the function. General feasibility results have been developed in the 1980s [Yao82], which the security (confidentiality of the secret input) of the honest party holds even if the other part deviates arbitrarily from the prescribed protocol (the malicious setting).

3.4.4 Threshold Secret Sharing

Many threshold schemes are based on Shamir's secret sharing [Sha79], which is derived from the concept of Lagrange polynomial interpolation.

For a (t, n) instantiation, a trusted dealer first selects t random coefficients $a_0, a_1, \cdots, a_{t-1}$ from $\mathbb{Z}_p$ where a_0 is the master secret to be shared. Then n different public points $x_{i_j} \in \mathbb{Z}_p^*$ are chosen (where $1 \leq j \leq n$), one for each participant. Let f be a polynomial of degree $(t-1)$ and $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$, the share to be distributed to the participant with public point x_{i_j} assigned is $f(x_{i_j})$.

When t participants decided to reconstruct the secret, they can do so by recovering the polynomial. With the knowledge of t points $(x_{i_j}, f(x_{i_j}) = s_{i_j})$ on the curve, the coefficients $(a_0, \cdots, a_t)$ of f can be computed by solving the following system of equations.

$$\begin{aligned} s_{i_1} &= a_0 + a_1 x_{i_1} + \cdots + a_{t-1} x_{i_1}^{t-1}, \\ s_{i_2} &= a_0 + a_1 x_{i_2} + \cdots + a_{t-1} x_{i_2}^{t-1}, \\ &\vdots \\ s_{i_t} &= a_0 + a_1 x_{i_t} + \cdots + a_{t-1} x_{i_t}^{t-1}, \end{aligned}$$

The above system has a unique solution for $(a_0, \cdots, a_t)$ since

$$\mathbf{\Delta} = \begin{pmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & \dots & x_{i_2}^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_t} & \dots & x_{i_t}^{t-1} \end{pmatrix}$$

is a non-zero Vandermonde determinant (all of its elements are non-zero and pair-wise unique). The unique solution and hence the polynomial can be found by the Lagrange interpolation of these t points by using the below formula.

$$f(x) = \sum_{j=1}^{t} s_{i_j} \prod_{1 \leq l \leq t, l \neq j} \frac{x - x_{i_l}}{x_{i_j} - x_{i_l}}.$$

Thus the secret $a_0 = f(0)$ can be obtained by $\sum_{j=1}^{t} b_j s_{i_j}$ where $b_j = \prod_{1 \leq l \leq t, l \neq j} \frac{x_{i_l}}{x_{i_l} - x_{i_j}}$.

3.5 Formal Definitions

Under the standard definition, an IBE scheme consists of four algorithms:

1. Via $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ the randomized key generation algorithm outputs the system parameters mpk and the master secret key msk; mpk also defines an identity space $\mathcal{ID}$ and a message space $\mathcal{M}$ and we assume all other algorithms below implicitly include mpk as an input;

2. Via $usk[\mathsf{ID}] \xleftarrow{\$} \mathsf{KeyDer}(msk, \mathsf{ID})$ the KGC outputs (either deterministically or probabilistically) a secret key for user ID;

3. Via $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\mathsf{ID}, m)$ anyone can encrypt a message m to user ID in $\mathfrak{C}$;

4. Via $m \leftarrow \mathsf{Dec}(usk[\mathsf{ID}], \mathfrak{C})$ user ID uses secret key $usk[\mathsf{ID}]$ to recover a message m from ciphertext $\mathfrak{C}$, or an invalid symbol if $\mathfrak{C}$ is an invalid ciphertext for ID.

Consistency requires that for all $\lambda \in \mathbb{N}$, all identities ID in $\mathcal{ID}$, all messages $m \in \mathcal{M}$, all $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ and all $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\mathsf{ID}, m)$, $\Pr[\mathsf{Dec}(\mathsf{KeyDer}(msk, \mathsf{ID}), \mathfrak{C}) = m] = 1$, where the probability is taken over the coins of all the above algorithms.

The de-facto security definition of an IBE scheme is semantic security against adaptive chosen ciphertext attack defined as below.

Definition 3.13 (Adaptive Chosen Ciphertext Security (CCA2))**.**

Experiment $\mathbf{Exp}^{\mathrm{cca2}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$

$(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$
$(m_0, m_1, \mathsf{ID}^*, st) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}_{\mathsf{find}}(mpk)$
$b \xleftarrow{\$} \{0,1\}$, $\mathfrak{C}^* \xleftarrow{\$} \mathsf{Enc}(\mathsf{ID}^*, m_b)$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}_{\mathsf{guess}}(\mathfrak{C}^*, st)$
If $(|m_0| \neq |m_1|) \vee (b \neq b')$ then return 0 else return 1

where st is some state information maintained by $\mathcal{A}$ and $\mathcal{O}$ is a set of two oracles $\{\mathsf{ExtractO}, \mathsf{DecO}\}$ defined as:

1. An $\mathsf{ExtractO}$ oracle that takes an identity $\mathsf{ID} \in \mathcal{ID}$ as input and returns a user secret key $usk[\mathsf{ID}]$.

2. A DecO oracle that takes a ciphertext $\mathfrak{C}$ and an identity $\mathsf{ID} \in \mathcal{ID}$, outputs $\mathsf{Dec}(usk[\mathsf{ID}], \mathfrak{C})$ where $usk[\mathsf{ID}]$ is output by $\mathsf{KeyDer}(msk, \mathsf{ID})$, provided that $(\mathfrak{C}, \mathsf{ID}) \neq (\mathfrak{C}^*, \mathsf{ID}^*)$.

Chosen Plaintext Security. If we modify the above security game so that the adversary is not allowed to query the decryption oracle DecO, we get the "semantic security against chosen plaintext attack" (CPA) game.

Selective Security. If we modify the above security game so that the adversary is required to give the challenge identity ID^* to the challenger before seeing the output of the Setup algorithm, we get the "selective-ID" game.

Before we define the syntax of attribute-based encryption, we first give the definition of access structure we will be using.

Definition 3.14 (Access Structure [Bei96])**.** Let $\{A_1, A_2, \cdots, A_n\}$ be a set of attributes. A collection $\mathbb{A} \subseteq 2^{\{A_1, A_2, \cdots, A_n\}}$ is monotone if $\forall P_1, P_2$: if $P_1 \in \mathbb{A}$ and $P_1 \subseteq P_2$ then $P_2 \in \mathbb{A}$. A (monotone) *access structure* is a (monotone) collection $\mathbb{A}$ of non-empty subsets of $\{A_1, A_2, \cdots, A_n\}$, i.e. $\mathbb{A} \subseteq 2^{\{A_1, A_2, \cdots, A_n\}} \backslash \{\varnothing\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

A key-policy attribute-based encryption scheme consists of four algorithms:

1. Via $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ the randomized key generation algorithm outputs the system parameters mpk and the master secret key msk; mpk also defines a message space $\mathcal{M}$, the set of attributes and the supported access structure. We assume all other algorithms below implicitly include mpk as an input.

2. Via $usk[\mathbb{A}] \xleftarrow{\$} \mathsf{AKeyGen}(msk, \mathbb{A})$ the authority probabilistically outputs a decryption key for the access structure defined by $\mathbb{A}$;

3. Via $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\mathbb{A}, m)$ anyone can encrypt a message m under a set of attributes $\mathbb{A}$;

4. Via $m \leftarrow \mathsf{Dec}(usk[\mathbb{A}], \mathfrak{C})$ a user uses decryption key $usk[\mathbb{A}]$ to recover a message m from ciphertext $\mathfrak{C}$ if the set of attributes of the ciphertext matches with the access structure defined by $\mathbb{A}$.

Consistency requires that for all $\lambda \in \mathbb{N}$, all $\mathbb{A}^u, \mathbb{A}^C$ such that $\mathbb{A}^C \in \mathbb{A}^u$, all messages $m \in \mathcal{M}$, all $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ and all $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\mathbb{A}^C, m)$, $\Pr[\mathsf{Dec}(\mathsf{AKeyGen}(msk, \mathbb{A}^u), \mathfrak{C}) = m] = 1$, where the probability is taken over the coins of all the above algorithms.

Now we review the selective-attribute model for proving the semantic security of the ABE under chosen plaintext attack, which can be seen as analogous to the selective-ID model in IBE.

Definition 3.15. Experiment $\mathbf{Exp}^{\mathrm{saa}}_{\mathcal{ABE},\mathcal{A}}(\lambda)$

$\mathbb{A}^C \leftarrow \mathcal{A}()$;
$(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$;
$(m_0^*, m_1^*, st) \xleftarrow{\$} \mathcal{A}^{\mathsf{AKeyGenO}(\cdot)}(\text{'find'}, mpk)$;
$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C}^* \xleftarrow{\$} \mathsf{Enc}(\mathbb{A}^C, m_b^*)$;
$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{AKeyGenO}(\cdot,\cdot,\cdot)}(\text{'guess'}, \mathfrak{C}^*, st)$;
If $(|m_0| \neq |m_1|) \vee (b \neq b')$ then return 0 else return 1;

where st is state information, and the attribute-key generation oracle $\mathsf{AKeyGenO}(\mathbb{A}^u)$ is defined as:

if $(\mathbb{A}^C \in \mathbb{A}^u)$ then return $\perp$;
return $\mathsf{AKeyGen}(msk, \mathbb{A}^u)$.

Apart from two very recent works on single-authority ABE [LOS+10, OT10], all existing ABE schemes in the standard model have not been proven to be adaptively secure.

□ End of chapter.

Part II

Identity-Based Encryption

Chapter 4

Removing Escrow from Identity-Based Encryption

Removing the trust from the authority is the main goal of this research. As the first step we remove key escrow from identity-based encryption in this chapter.

This chapter starts by a description of our framework for identity-based encryption, follows by the formalization of anonymous ciphertext indistinguishability against the KGC, which captures the guarantees our proposed scheme can provide when the KGC is an adversary. We then analyze representative schemes selected from Chapter 2 and present our scheme which achieves anonymous ciphertext indistinguishability against the KGC.

4.1 Our Framework for Identity-Based Encryption

In our definition, we separate the master key generation from the Setup algorithm.

Definition 4.1. An IBE scheme consists of the following five PPT algorithms:

1. via $param \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ the setup algorithm outputs the system parameters $param$ for security parameter $\lambda \in \mathbb{N}$, with message space $\mathcal{M}(\lambda)$ included.

2. via $(mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param)$ the key generation algorithm outputs the master public/secret key (mpk, msk) conforming to $param$.

3. KeyDer, Enc and Dec are defined as in the standard definition.

We can view Setup as a trusted initializer for choosing the system parameters (for example, the choice of elliptic cure) which are implicitly included in the input of KeyDer, Enc and Dec. The KGC generates a master public/secret key pair only via MKeyGen. We assume it is efficient to check if a message m is in $\mathcal{M}(\lambda)$ or if mpk comes from a group that matches with what is specified in $param$. We denote the latter check by (an abused notation) $mpk \in param$.

4.2 Anonymity and Indistinguishability against the KGC

4.2.1 Anonymity against User Attack

User-anonymity is defined by the game below [ABC+08]. The adversarial goal is to distinguish the intended recipient of a ciphertext between two chosen identities

Experiment $\mathbf{Exp}^{\text{ano}-\text{cpa}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$

$\mathsf{IDset} \leftarrow \varnothing$; $(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; $(mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param)$;

$(\mathsf{ID}_0, \mathsf{ID}_1, m^*, st) \xleftarrow{\$} \mathcal{A}^{\text{KeyDerO}(\cdot)}(\text{`find'}, param, mpk)$;

If $m^* \notin \mathcal{M}(\lambda)$ then return 0;

$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}_b, m^*)$; $b' \xleftarrow{\$} \mathcal{A}^{\text{KeyDerO}(\cdot)}(\text{`guess'}, \mathfrak{C}, st)$;

If $b \neq b'$ or $(\{\mathsf{ID}_0, \mathsf{ID}_1\} \cap \mathsf{IDset} \neq \varnothing)$ then return 0 else return 1;

where the private key derivation oracle KeyDerO(ID) is defined as:

$$\mathsf{IDset} \leftarrow \mathsf{IDset} \cup \{\mathsf{ID}\}; usk[\mathsf{ID}] \leftarrow \mathsf{KeyDer}(msk, \mathsf{ID});\ \text{return}\ usk[\mathsf{ID}]$$

and st denotes the state information maintained by the adversary $\mathcal{A}$.

We remark that IBE's ciphertext does not mean to reveal the recipient's identity, so our model does not consider anonymity revocation oracle which is present in some cryptographic schemes (e.g. [BBS04]).

4.2.2 Anonymous Ciphertext Indistinguishability

We use the term "anonymous ciphertext" to refer a ciphertext that the KGC holds without the knowledge of who is the intended recipient. We do not model the case where the KGC

maliciously generates the system parameters (e.g. the choice of elliptic curve), but we provide a new "embedded-identity encryption" oracle, which lets the adversary adaptively get many ciphertexts designated to the same person, without knowing the real identity. The absence of such an oracle gives the adversary no way to see more than one ciphertext for the unknown recipient. For the ease of discussion, we suppose an identity is of n-bit length.

Definition 4.2. An IBE scheme is (t, q_E, ϵ) $\mathcal{ACI} - \mathcal{KGC}$ secure if all t-time adversaries making at most q_E embedded-identity encryption oracle queries have advantage at most ϵ in winning the game below (i.e. the experiment returns 1).

Experiment $\mathbf{Exp}^{\text{aci}-\text{kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$

$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; $\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$;
$(mpk, st) \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{gen}\text{'}, param)$;
If $mpk \notin param$ then return 0;
$(m_0^*, m_1^*, st) \xleftarrow{\$} \mathcal{A}^{\text{ENCO}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{`}\mathsf{find}\text{'}, mpk, st)$;
If $\{m_0^*, m_1^*\} \nsubseteq \mathcal{M}(\lambda)$ or $|m_0^*| \neq |m_1^*|$ then return 0;
$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}^*, m_b^*)$;
$b' \xleftarrow{\$} \mathcal{A}^{\text{ENCO}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}, st)$;
If $b \neq b'$ then return 0 else return 1;

where the embedded-identity oracle $\text{ENCO}_{(mpk,\mathsf{ID}^*)}(m)$ returns $\mathsf{Enc}(mpk, \mathsf{ID}^*, m)$ and the advantage of $\mathcal{A}$ is defined as $|\Pr[\mathbf{Exp}^{\text{aci}-\text{kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = 1] - \frac{1}{2}|$.

Anonymous Ciphertext Indistinguishability in HIBE.

Below gives a possible extension to $\ell-$HIBE (i.e. an HIBE scheme supporting at most ℓ levels) case, in which only the first-level identity is chosen from a uniform distribution with high entropy as oppose to a weaker definition which requires the whole identity string (i.e., the identities at all levels) to be from a uniform distribution with high entropy. We consider this stronger definition since it appears that GS-HIBE [GS02] can achieve this level of security.

Experiment $\mathbf{Exp}^{\text{aci}-\text{kgc}}_{\ell-\dashv\int\rangle\dashv\rfloor\nabla\dagger\sqrt{\ }\sqcup/\mathcal{G}\rceil\setminus\sqcup\nabla\dagger\mathcal{S}\prime\in,\mathcal{A}}(\lambda)$

$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; $\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$;

$(mpk, st) \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{gen}\text{'}, param)$;

If $mpk \notin param$ then return 0;

$(m_0^*, m_1^*, \mathsf{ID}_2, \cdots, \mathsf{ID}_j, st) \xleftarrow{\$} \mathcal{A}^{\textsc{Enco}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{`}\mathsf{find}\text{'}, mpk, st)$;

If $\{m_0^*, m_1^*\} \nsubseteq \mathcal{M}(\lambda)$ or $|m_0^*| \neq |m_1^*|$ then return 0;

$b \xleftarrow{\$} \{0,1\}$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \{\mathsf{ID}^*, \mathsf{ID}_2, \cdots, \mathsf{ID}_j\}, m_b^*)$;

$b' \xleftarrow{\$} \mathcal{A}^{\textsc{Enco}_{(mpk,\mathsf{ID}^*)}(\cdot)}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}, st)$;

If $(b \neq b') \wedge (1 \leq j \leq \ell)$ then return 0 else return 1;

Embedded-Identity Decryption.

The above game just considers chosen-plaintext attack (CPA). One may consider giving the adversary adaptive access to a decryption oracle, or even an "embedded-identity decryption oracle". We consider this stronger notion from both the theory and practice perspectives.

Our security notion is actually quite strong in the sense that the adversary is not required to reveal the master secret key to the challenger. We start our discussion with a weakened definition such that the adversary is instead required to do so. While it is possible that the decryption oracle could help the adversary to deduce information about the challenge ciphertext, this happens when a maliciously formed ciphertext is presented to the decryption oracle. If we are able to put some validity tag in the ciphertext such that the challenger, with the master secret key, can do a sanity check before the actual decryption; only "invalid" will be returned for any malformed ciphertext or those not encrypted for the challenge identity, i.e. CCA2-security against user also helps in here.

If the challenger does not know the master secret, it may sound impossible to simulate the decryption oracle. Nevertheless, our definition assumes trusted parameter generation, which possibly allows us to solve the problem with approaches similar to simulating the strong decryption oracle in certificateless encryption [ARP03, Cho08, CRR08, DLP08], such as a knowledge-extractor with the help of the random oracle, or a non-interactive zero-knowledge proof system setup according to the trusted parameters. We leave it as a future work.

In practice, while it makes sense to trick a user into encrypting some pre-defined messages (as modeled by the embedded-identity encryption oracle); it may not make much sense to consider the

case that the KGC gained accesses to an embedded-identity decryption oracle – which possibly means the KGC has identified this user already. Due to these complications, we keep our focus on the CPA notion. Nevertheless, this does not preclude the possibility of achieving $\mathcal{ACI} - \mathcal{KGC}$-security and CCA2-security against user attack simultaneously.

4.2.3 Anonymity against the KGC

One may define semantic security of the hidden identity in a similar way. However, when the KGC is being considered as the adversary, we cannot afford to have the indistinguishability in modelling user anonymity – the KGC can simply generate the two corresponding private keys and try decrypting the challenge ciphertext. Hence, we consider one-wayness here, in which the adversarial goal is to recover the identity of the intended recipient in full. Private key derivation oracle and decryption oracle are provided by the master secret key.

Experiment $\mathbf{Exp}^{\text{ano}-\text{kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$

$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$;

$(mpk, m^*, st) \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{find}\text{'}, param)$;

If $mpk \notin param$ or $m^* \notin \mathcal{M}(\lambda)$ then return 0;

$\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}^*, m^*)$;

$\mathsf{ID}' \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}, st)$;

If $\mathsf{ID}^* \neq \mathsf{ID}'$ then return 0 else return 1;

We note that it is easy to make an IBE scheme $\mathcal{ANO} - \mathcal{KGC}$. One can simply requiring all identities involved in IBE to be fed into a one-way hash function. The simulation goes by using a random bit string in the domain of the hash as the identity to be used in the encryption. Breaking $\mathcal{ANO} - \mathcal{KGC}$ means the one-wayness of the hash is broken.

We note the relationship that $\mathcal{ACI} - \mathcal{KGC} \Rightarrow \mathcal{ANO} - \mathcal{KGC}$.

Theorem 4.3. *If an IBE scheme is secure in the sense of $\mathcal{ACI} - \mathcal{KGC}$, it is $\mathcal{ANO} - \mathcal{KGC}$ secure.*

Proof. We prove by contrapositivity. Assume there is an adversary $\mathcal{A}_{\text{ano}}$ that wins the game $\mathcal{ANO} - \mathcal{KGC}$ with advantage ϵ in time t, we shall construct an adversary $\mathcal{A}_{\text{aci}}$ that win the game $\mathcal{ACI} - \mathcal{KGC}$ with advantage $\epsilon/2$ in time t.

$\mathcal{A}_{\text{aci}}$ simply passes all parameters it received to $\mathcal{A}_{\text{ano}}$, and forwards all oracle queries of $\mathcal{A}_{\text{ano}}$ to its corresponding oracles. After the find stage, $\mathcal{A}_{\text{ano}}$ gives a message m^* to $\mathcal{A}_{\text{aci}}$. $\mathcal{A}_{\text{aci}}$ picks another random message m_1 of the same length as m^* from the message space $\mathcal{M}(\lambda)$, gives (m^*, m_1) to its challenger, and receives $\mathfrak{C}$ in return. $\mathcal{A}_{\text{aci}}$ forwards $\mathfrak{C}$ to $\mathcal{A}_{\text{ano}}$. At the end of the guess stage, $\mathcal{A}_{\text{ano}}$ outputs ID' with probability ϵ, fail otherwise.

$\mathcal{A}_{\text{aci}}$ answers 0 for the first case and 1 for the latter. Let b be the bit chosen by $\mathcal{A}_{\text{aci}}$'s challenger. We have $\Pr[\mathcal{A}_{\text{aci}} \text{ wins}] = \Pr[b = 0] \cdot \Pr[\mathcal{A}_{\text{ano}} \text{ succeeds} | b = 0] + \Pr[b = 1] \cdot \Pr[\mathcal{A}_{\text{ano}} \text{ fails} | b = 1] = \frac{\epsilon}{2} + \frac{1}{2}$. □

4.2.4 Comparison of User Anonymity and KGC One-wayness

A KGC is a powerful adversary. We consider KGC one-wayness ($\mathcal{OW} - \mathcal{KGC}$), a notion strictly weaker than $\mathcal{ACI} - \mathcal{KGC}$, to better reflect the security of IBE against KGC attacks. We also present two separation results.

Definition 4.4. An IBE is $\mathcal{OW} - \mathcal{KGC}$ secure if $\Pr[\mathbf{Exp}^{\text{ow-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = 1] < \mathsf{negl}(\lambda)$.

Experiment $\mathbf{Exp}^{\text{ow-kgc}}_{\mathcal{IBE},\mathcal{A}}(\lambda)$

$(param) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$, $\mathsf{ID}^* \xleftarrow{\$} \{0,1\}^n$;

$(mpk, st) \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{gen}\text{'}, param)$; If $mpk \notin param$ then return 0;

$m^* \xleftarrow{\$} \mathcal{M}(\lambda)$; $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(mpk, \mathsf{ID}^*, m^*)$; $m' \xleftarrow{\$} \mathcal{A}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}, st)$;

If $m^* \neq m'$ then return 0 else return 1;

Theorem 4.5. *User anonymity does not imply $\mathcal{OW} - \mathcal{KGC}$.*

Proof. Given any user-anonymous IBE scheme with encryption algorithm Enc, define a new IBE with encryption algorithm $\mathsf{Enc}'(mpk, \mathsf{ID}, m) = (\mathsf{Enc}(mpk, \mathsf{ID}, m), \mathsf{Enc}(mpk, \text{“0”}, \mathsf{ID}))$, where “0” is a dummy identity and the corresponding user secret key is never released by the KGC. If the IBE scheme is semantically secure, the ciphertext produced by Enc' is still user-anonymous. But it is not $\mathcal{OW} - \mathcal{KGC}$ since the KGC can just generate the user secret key for “0”, decrypt the second component of the ciphertext and then decrypt the first component. □

Theorem 4.6. *$\mathcal{ACI} - \mathcal{KGC}$ does not imply user anonymity.*

Proof. Given any $\mathcal{ACI} - \mathcal{KGC}$ with encryption algorithm Enc, define a new IBE with encryption algorithm which appends the first bit of identity to the ciphertext. Any adversary can just choose two identities which differ at the first bit to break the user-anonymity. On the other hand, the notion of $\mathcal{ACI} - \mathcal{KGC}$ depends on the number of random bits in the identity; essentially only one bit of security is lost and $\mathcal{ACI} - \mathcal{KGC}$ is still preserved. □

Shortly afterward, we will see they are also orthogonal to each other in practice.

4.3 Analysis of Existing Schemes

Seven (H)IBE schemes representing a large class of IBE schemes in the literature are selected. Capital letters are used to denote elements in $\mathbb{G}$, small letters are for elements in $\mathbb{Z}_p$ and small letters with hat (e.g. $\hat{g}$) are used to denote elements in $\mathbb{G}_T$. To unify the naming of variables across different schemes, r denotes the ephemeral random parameter employed in encryption (if two random parameters are needed, they are denoted by r, r'); the master secret msk is denoted by $s \in \mathbb{Z}_p$ or $S \in \mathbb{G}$ (if more than 1 element are present in msk, they are denoted by s_1, s_2, s_3). For elements which may appear in the system parameter mpk, P denotes the generator of $\mathbb{G}$ and $\hat{g} = e(P, P)$ denotes a generator of $\mathbb{G}_T$. For the schemes stemmed from FDH-IBE, let $H_0(\cdot) : \{0,1\}^n \to \mathbb{G}$ be a cryptographic hash; denote $Q_{\mathsf{ID}} = H_0(\mathsf{ID})$ as the public key of user ID, and $\{Q_1, Q_2, \cdots, Q_j\}$ as the public key of user $(\mathsf{ID}_1, \mathsf{ID}_2, \cdots \mathsf{ID}_j)$ for a j-level HIBE.

Note that we made many simplifications and omitted many elegant components of the IBE schemes being analyzed. We do not intend to give a complete review of the constructions of all these schemes (it seems we are reducing these IBE schemes to ID-based key encapsulations or even just public key encryption schemes), but we want to keep our focus on how a KGC can decrypt the message using the master secret key. Thus, we only show the essential components in the master public key mpk, the master secret key msk, the ciphertext, and the variable that can be computed (without using any secret key) from the ciphertext (t in KV-IBE), which are sufficient for the KGC to do the decryption. We use $\mathcal{K}$ to denote the random session key created by the implicit KEM, which is a crucial piece of data to decrypt the ciphertext.

Schemes	mpk	msk	Ciphertext	$\mathcal{K}$
FDH-IBE [BF01, SOK01]	P^s	s	P^r	$e(Q_{\mathsf{ID}}{}^r, P^s)$
GS-HIBE [GS02]	P^s	s	$P^r, Q_{\mathsf{ID}_2}^r, \cdots$	$e(Q_{\mathsf{ID}_1}{}^r, P^s)$
BSS-MIBE [BSNS05]	P^s, Q	s	P^r	$e(Q, P^s)^r$
BB-EIIBE [BB04a]	$\hat{g}, V = P^s$	s	V^r	$\hat{g}^r$
BB-(H)IBE [BB04a]	$e(P, S)$	S	P^r	$e(P, S)^r$
BW-IBE [BW06]	$\hat{v} = \hat{g}^{s_1 s_2 s_3}, V_1 = P^{s_1}, V_2 = P^{s_2}$	s_1, s_2, s_3	$V_1^{r-r'}, V_2^{r'}$	$\hat{v}^r$
KV-IBE [KV08]	$\hat{g}, \hat{v}_1 = \hat{g}^{s_1}, \hat{v}_2 = \hat{g}^{s_2}$	s_1, s_2	$\hat{g}^r, t$	$(\hat{v}_1^t \hat{v}_2)^r$

Table 4.1: *Concise Review of IBE Schemes for $\mathcal{ACI} - \mathcal{KGC}$ Analysis*

4.3.1 Schemes that are not $\mathcal{OW} - \mathcal{KGC}$-Secure

The session key $\mathcal{K}$ in BSS-MIBE can be computed by $e(Q, P^r)^s$. For BB-EIIBE, $\mathcal{K}$ can be computed by $e(P, V^r)^{1/s}$. For BB-(H)IBE, $e(P^r, S) = \mathcal{K}$. For BW-IBE, it can be computed by $e((V_2^{r'})^{1/s_2}(V_1^{r-r'})^{1/s_1}, P)^{s_1 s_2 s_3} = e(P^{r'} P^{r-r'}, P^{s_1 s_2 s_3}) = \hat{v}^r$. For KV-IBE, $(\hat{g}^r)^{s_1 t + s_2} = \mathcal{K}$. Hence, they are not $\mathcal{OW} - \mathcal{KGC}$-secure. BBAIBE [GLSW08] is not exactly covered by the above analysis, however, it can be easily shown that it is not $\mathcal{OW} - \mathcal{KGC}$-secure. Note that all of the above computations use the master secret key as-is, instead of exploiting the knowledge of any discrete logarithm between some group elements in the system parameters.

4.3.2 Schemes that are $\mathcal{ACI} - \mathcal{KGC}$-Secure

We consider FDH-IBE [BF01, SOK01] – when $\mathcal{K} = e(Q_{\mathsf{ID}}{}^r, P^s)$ is used to encrypt the message $m \in \mathbb{G}_T$ by $m\mathcal{K}$, this gives a CPA-secure IBE scheme in the ROM. To prove its $\mathcal{ACI} - \mathcal{KGC}$-security, we assume the parameters for the hash functions are setup by an honest party, which means the random oracles are not controlled by the adversary in the security proof.

Theorem 4.7. *If DBP is hard, FDH-IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure.*

We first give an informal argument to get some intuition on why is it so. Given any pair of messages (m_0^*, m_1^*) and an encryption of one of them, there is always a pair of identities $(\mathsf{ID}_0, \mathsf{ID}_1)$ such that the decryption of the ciphertext using session key $e(Q_{\mathsf{ID}_0}{}^r, P^s)$ gives m_0^*

and decryption using $e({Q_{\mathsf{ID}_1}}^r, P^s)$ gives m_1^*. If the challenge identity is chosen from a uniform distribution with high entropy, any adversary simply has no clue to distinguish, and hence the scheme is $\mathcal{ACI} - \mathcal{KGC}$-secure. Note that the above argument remains valid even if the adversary can compute r from P^r.

Proof. Let $\mathcal{A}$ be an adversary that breaks $\mathcal{ACI} - \mathcal{KGC}$ of BasicIdent with advantage ϵ. We construct an algorithm, $\mathcal{S}$, that solves the decisional bilinear problem as follows.

$\mathcal{S}$ executes the Setup algorithm of BasicIdent, and returns the parameter *param* to $\mathcal{A}$. In particular, a description of $H_0(\cdot)$ is returned, which is a hash function mapping an identity string to an element in $\mathbb{G}$. $\mathcal{A}$ then returns $g^\alpha \in \mathbb{G}$ as the master public key, $\alpha \in \mathbb{Z}_p$ is not given to $\mathcal{S}$ and $\mathcal{S}$ never uses α in the simulation. $\mathcal{S}$ takes as input a random decisional bilinear challenge $(g, g^r, e(g,g)^s, \hat{t})$.

To simulate the embedded-identity encryption oracle with message m_i as input, $\mathcal{S}$ randomly chooses $y_i \in \mathbb{Z}_p$. The ciphertext can be computed by $(g^{y_i}, (e(g,g)^s)^{y_i} \cdot m_i)$. The ephemeral random parameter implicitly used is y_i. Suppose the intended recipient ID' of these ciphertexts is defined by v' where $H_0(\mathsf{ID}') = Q_{\mathsf{ID}'} = g^{v'}$. A consistent ciphertext requires $s = v'\alpha$. Since s is a random element in $\mathbb{Z}_p$, there must exists such an element v'. The intended recipients of all the ciphertexts returned by the embedded-identity encryption oracle will be the same. Note that $\mathcal{S}$ does not need to return anything about v' for requests to any oracle other than the embedded-identity encryption oracle, so the simulation goes through even v' is unknown to $\mathcal{S}$.

When $\mathcal{A}$ outputs two equal length messages (m_0^*, m_1^*) at the end of the find stage, $\mathcal{S}$ randomly generates a bit b and returns the ciphertext $(g^r, \hat{t} \cdot m_b^*)$, which means the ephemeral random parameter implicitly used is r. Let the intended recipient of this ciphertext be ID^* and $H_0(ID^*) = Q_{\mathsf{ID}^*} = g^v$. If we write $\hat{t} = e(g,g)^\beta$, for a valid ciphertext we have $\beta = vr\alpha$. Note that the value of v is unknown to $\mathcal{S}$ but it is never used elsewhere in the simulation.

At the guess stage, the embedded-identity encryption oracle is simulated as in the find stage.

If $\beta = rs$, i.e. $\mathcal{S}$ receives a DBP tuple. The equation defined by the challenge ciphertext gives $rs = vr\alpha \Rightarrow s = v\alpha$, i.e. $v = v'$, which makes the simulation perfect.

If $\beta \neq rs$, $\mathcal{S}$ made an invalid ciphertext for m_b^* (as $(\hat{t} \cdot m_b^*)/e(g,g)^{v'r\alpha} \neq m_b^*$). The probability that the challenge ciphertext is a valid one of another message m_{1-b}^* for the same recipient (i.e.

$(\hat{t} \cdot m_b^*)/e(g,g)^{v'r\alpha} = m_{1-b}^*$) is also negligible (and we ignore this case in our probability analysis below). However, even the challenge ciphertext does not match with the ciphertexts returned by the embedded-identity encryption oracle, $\hat{t}$ is a random element in $\mathbb{G}_T$ and the challenge ciphertext leaks no information about the bit b. Assuming $\mathcal{A}$ would not abort in this case (or it will only increase $\mathcal{S}$'s probability to decide that $\hat{t} \neq e(g,g)^{rs}$), the probability it can guess b correctly is $1/2$.

The strategy of $\mathcal{S}$ is if $b = b'$, it outputs 'yes' (meaning $\hat{t} = e(g,g)^{rs}$); 'no' otherwise. We have

$$\begin{aligned} & \Pr[\mathcal{S} \text{ solves } DBP] \\ = \; & \Pr[\hat{t} = e(g,g)^{rs}] \cdot \Pr[\mathcal{A}_{\text{ano}} \text{ succeeds}|\text{valid ciphertexts}] + \Pr[\hat{t} \neq e(g,g)^{rs}] \cdot \Pr[b \neq b'] \\ = \; & (\frac{1}{2})(\frac{1}{2} + \epsilon) + (\frac{1}{2})(\frac{1}{2}) = \frac{1}{2} + \frac{\epsilon}{2} \end{aligned}$$

□

For the CCA2-secure BF-IBE [BF01], we can prove it is $\mathcal{ACI} - \mathcal{KGC}$ secure by considering the computational bilinear problem (CBP), the computational variant of DBP (i.e., to compute $e(g,g)^{ab}$ instead of distinguishing it from random). The simulation is similar to that in Theorem 4.7, but $e(g,g)^{ab}$ will be "trapped" by the random oracle if the adversary has non-negligible in winning the game.

Lemma 4.1. *If CBP is hard, BF-IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure.*

Thus, we can still enjoy the usual CCA2-security against the user (outsider adversary) with the extra $\mathcal{ACI} - \mathcal{KGC}$ protection. A similar argument applies to Gentry-Silverberg HIBE and Yao *et al.*'s HIBE [YFDL04]. Extra elements in the challenge ciphertext only contain more information about r and the identities at the lower level, which cannot help the adversary to determine the first-level identity or distinguish the ciphertext. They can also be easily simulated by manipulating the random oracle. This gives an interesting result that even when the ciphertext is not "strictly" user-anonymous, it is still possible to get $\mathcal{ACI} - \mathcal{KGC}$-security.

4.4 "Escrow-Free" IBE in the Standard Model

BF-IBE is $\mathcal{ACI} - \mathcal{KGC}$-secure but its CCA2-security is only proven in the random oracle model. Below we review Gentry-IBE [Gen06], an IBE with CCA2-security proven in the standard model, under the original four-algorithm IBE framework.

Setup: The KGC selects g, h_1, h_2, h_3 randomly from $\mathbb{G}$, randomly chooses an exponent $\alpha \in_R \mathbb{Z}_p$, sets $g_1 = g^\alpha \in \mathbb{G}$, and chooses a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of universal one-way hash functions. The public parameters and the master secret key are given by $mpk = (g, g_1, h_1, h_2, h_3, H(\cdot))$, $msk = \alpha$.

KeyDer: To generate a private key for identity $\mathsf{ID} \in \mathbb{Z}_p$, the KGC picks $\tau_{\mathsf{ID},i} \in_R \mathbb{Z}_p$ and computes $h_{\mathsf{ID},i} = \left(h_i g^{-\tau_{\mathsf{ID},i}}\right)^{\frac{1}{\alpha - \mathsf{ID}}}$ for $i \in \{1,2,3\}$, outputs $\{\tau_{\mathsf{ID},i}, h_{\mathsf{ID},i}\}_{i\in\{1,2,3\}}$. The KGC must always use the same random value $\tau_{\mathsf{ID},i}$ for ID. This can be accomplished by using a pseudorandom function (PRF) or an internal log [Gen06].

Enc: To encrypt $m \in \mathbb{G}_T$ for identity $\mathsf{ID} \in \mathbb{Z}_p$, the sender picks $r \in_R \mathbb{Z}_p$, computes $\mathfrak{C} = (u, v, w, y) = \Big(\ (g_1 g^{-\mathsf{ID}})^r \ , \ e(g,g)^r \ , \ m/e(g,h_1)^r \ , \ e(g,h_2)^r e(g,h_3)^{r\cdot H(u,v,w)} \ \Big)$.

Dec: To decrypt the ciphertext $\mathfrak{C}$ with a private key $\{\tau_{\mathsf{ID},i}, h_{\mathsf{ID},i}\}_{i\in\{1,2,3\}}$, first check $\mathfrak{C}$'s validity by testing if $y = e(u, h_{\mathsf{ID},2} {h_{\mathsf{ID},3}}^\beta) v^{\tau_{\mathsf{ID},2} + \tau_{\mathsf{ID},3}\beta}$ where $\beta = H(u,v,w)$. In case of inequality, $\perp$ is outputted. Otherwise, return $m = w \cdot e(u, h_{\mathsf{ID},1}) v^{\tau_{\mathsf{ID},1}}$.

4.4.1 Proposed Construction

To get $\mathcal{ACI} - \mathcal{KGC}$-security, instead of letting the KGC to select g, h_1, h_2, h_3 randomly from $\mathbb{G}$, we require that the discrete logarithm of one with respect to another be unknown to the KGC, or $\mathcal{OW} - \mathcal{KGC}$-security can be easily broken. This requirement was not stated in [Gen06]. In practice, this can be achieved by using a common public seed to generate these parameters with a cryptographic hash function. Specifically, we separate the master key generation from the Setup as follows.

Setup: The trusted initializer chooses the group $\mathbb{G}$ according to the security parameter, and selects g, h_1, h_2, h_3 randomly from $\mathbb{G}$. It also chooses a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of

universal one-way hash functions. The public parameter *param* is given by $(g, h_1, h_2, h_3, H(\cdot))$.

MKeyGen: The KGC chooses an exponent $\alpha \in_R \mathbb{Z}_p$. It sets $g_1 = g^\alpha \in \mathbb{G}$. The master public/secret key pair is given by $(mpk = g_1, msk = \alpha)$.

Note that the above change does not affect the original security guarantees of Gentry-IBE against users attack, i.e. CCA2-security and user anonymity.

4.4.2 $\mathcal{ACI} - \mathcal{KGC}$-Security

With Lemma 3.2, the below theorem shows that the above IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure without extra number-theoretic assumptions other than what has been assumed in the original proof for indistinguishability against users' attack [Gen06].

Theorem 4.8. *If MDBP is hard, the above IBE is $\mathcal{ACI} - \mathcal{KGC}$ secure.*

Proof. Let $\mathcal{A}$ be an adversary that breaks $\mathcal{ACI} - \mathcal{KGC}$ of the IBE system described above. We construct an algorithm, $\mathcal{S}$, that solves an MDBP instance $(g, g^r, g^{s^{-1}}, e(g,g)^s, \hat{t})$ as follows.

$\mathcal{S}$ randomly chooses two exponents $\gamma_2, \gamma_3 \in_R \mathbb{Z}_p$ and a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of universal one-way hash functions. The system parameter *param* is set as $(g, h_1, h_2, h_3, H(\cdot))$ where $h_1 = g^r$, $h_2 = g^{\gamma_2}$ and $h_3 = g^{\gamma_3}$. $\mathcal{A}$ then returns $g_1 = g^\alpha \in \mathbb{G}$ as the master public key, $\alpha \in \mathbb{Z}_p$ is not given to $\mathcal{S}$ and $\mathcal{S}$ never uses α in the simulation. $\mathcal{S}$ also picks a random element $c \in_R \mathbb{Z}_p$.

To simulate the embedded-identity encryption oracle with message m_i as input (for $i \in \{1, \cdots, q_E\}$), $\mathcal{S}$ selects a random element $d_i \in_R \mathbb{Z}_p$ and returns

$$(u_i, v_i, w_i, y_i) = \left((g^{s^{-1}})^{cd_i}, e(g,g)^{d_i}, m_i / e(g,h_1)^{d_i}, e(g,g)^{d_i(\gamma_2 + \gamma_3 \cdot H(u_i, v_i, w_i))}\right).$$

Let $\hat{s} = e(g,g)^s$. When $\mathcal{A}$ outputs two equal length messages (m_0^*, m_1^*), $\mathcal{S}$ randomly generates a bit b, the challenge ciphertext is given by $\mathfrak{C} = (u, v, w, y) = \left(g^c, \hat{s}, m_b^* / \hat{t}, \hat{s}^{\gamma_2 + \gamma_3 \cdot \beta}\right)$, where $\beta = H(u, v, w)$. From the structure of the ciphertext, the intended recipient's identity ID^* is implicitly defined by $c = s(\alpha - \mathsf{ID}^*)$.

Since $s^{-1}c = s^{-1}s(\alpha - \mathsf{ID}^*) = \alpha - \mathsf{ID}^*$, the ciphertexts returned by the embedded-identity encryption oracle are valid ciphertexts encrypted for ID^*.

After $\mathcal{A}$ receives $\mathfrak{C}$, it outputs b' with probability ϵ at the end of the guess stage. If $b = b'$, $\mathcal{S}$ outputs 0 (meaning $\hat{t} = e(g,g)^{rs}$); otherwise, it outputs 1.

If $\hat{t} = e(g,g)^{rs}$, (u,v,w,y) is a valid, appropriately-distributed challenge to $\mathcal{A}$. If $\hat{t} \neq e(g,g)^{rs}$, since $\hat{t}$ is uniformly random and independent from $\mathcal{A}$'s view (other than the challenge ciphertext), (u,v,w,y) imparts no information regarding the bit b, so we have the success probability equal to

$$\begin{aligned} & \Pr[\hat{t} = e(g,g)^{rs}] \cdot \Pr[\mathcal{A} \text{ succeeds}] + \Pr[\hat{t} \neq e(g,g)^{rs}] \cdot \Pr[b \neq b'] \\ = \quad & (\frac{1}{2})(\frac{1}{2} + \epsilon) + (\frac{1}{2})(\frac{1}{2}) = \frac{1}{2} + \frac{\epsilon}{2} \end{aligned}$$

□

Using a similar argument, SK-IBE [SK03] can be proven $\mathcal{ACI} - \mathcal{KGC}$-secure.

The following theorem shows that without using the trick of hashing the identity string as suggested in Section 4.2.3. The above scheme can achieve $\mathcal{ANO} - \mathcal{KGC}$-security under a weaker assumption which is the discrete logarithm assumption.

Theorem 4.9. *If DLP is hard, our IBE system is $\mathcal{ANO} - \mathcal{KGC}$ secure.*

Proof. Let $\mathcal{A}$ be an adversary that breaks $\mathcal{ANO} - \mathcal{KGC}$-security of the IBE system described above with advantage ϵ. We construct an algorithm, $\mathcal{S}$, that solves the discrete logarithm problem as follows.

$\mathcal{S}$ takes as input a random discrete logarithm challenge (g,h). It randomly chooses generators $h_1, h_2, h_3 \in_R \mathbb{G}$, an exponent $\alpha \in_R \mathbb{Z}_p$ and a hash function $H : \{0,1\}^n \to \mathbb{Z}_p$ from a family of universal one-way hash functions. The system parameter *param* is $(g, h_1, h_2, h_3, H(\cdot))$. $\mathcal{A}$ then returns $g_1 = g^a lpha \in \mathbb{G}$ as the master public key, where $\alpha \in \mathbb{Z}_p$ is not given to $\mathcal{S}$.

When $\mathcal{A}$ outputs message m^*, $\mathcal{S}$ randomly chooses $r \in_R \mathbb{Z}_p$ and computes

$$\mathfrak{C} = (u,v,w,y) = \left(h \cdot g_1^r, e(g,g^r), m/e(g^r,h_1), e(g^r,h_2)e(g^r,h_3)^{\beta}\right)$$

where $\beta = H(u,v,w)$.

After $\mathcal{A}$ received $\mathfrak{C}$, it outputs ID' with probability ϵ at the end of the guess stage. $\mathcal{S}$ gets the solution of DLP by computing $-r \cdot \mathsf{ID}'$. □

4.4.3 Relation between $\mathcal{ACI} - \mathcal{KGC}$-Security and Other Notions

Now we modify the scheme presented in Section 4.4.1 to give a contrived construction in the standard model. The modification just introduces the term g^{ID} to the ciphertext. An immediate consequence is that the modified scheme no longer provides user-anonymity, To revise the $\mathcal{ACI} - \mathcal{KGC}$ proof, the extra term in the challenge ciphertext (and this term appears in all ciphertexts returned by the embedded-identity encryption oracle as well) can be simulated by $g^{\alpha}/(g^{s^{-1}})^{c}$. That is, the resulting scheme is still $\mathcal{ACI} - \mathcal{KGC}$-secure.

Our proposed scheme can be made to be accountable [Goy07], but other accountable IBE schemes [GLSW08, LV09] are not $\mathcal{ACI} - \mathcal{KGC}$-secure, which shows that accountability is orthogonal to $\mathcal{ACI} - \mathcal{KGC}$-security. For KwrtA-anonymous IBE, [IP08] showed that BF-IBE [BF01] is KwrtA but not ID-based non-malleable, a variant of SK-IBE [SK03] is both KwrtA and ID-based non-malleable, while BB-IBE [BB04a], AHIBE [BW06] and Gentry-IBE [Gen06] are *not* KwrtA but are ID-based non-malleable. Together with our analysis in Section 4.3, it is clear that the notions of KGC-anonymity, ID-based non-malleability and $\mathcal{ACI} - \mathcal{KGC}$-security are independent of each other.

□ End of chapter.

Chapter 5

Anonymous Key Issuing for Identity-Based Encryption

Master secret key is a powerful weapon to compromise the security of any IBE system. In this chapter, we describe how to take away some of its power by hiding the identity list of the system from the owner of the master secret key, via the use of anonymous key issuing protocol and a new system architecture for key issuing.

We start by presenting the framework for our new architecture and protocol, and the security requirements of our protocol. We then present our proposed key issuing protocol for our scheme in Chapter 4 and analyze its security. We conclude this chapter by contrasting our protocol with related constructions, and a new application of our protocol outside the context of identity-based encryption.

5.1 General Framework

In anonymous key issuing (AKI), we need to achieve two somewhat contradictory requirements simultaneously. On one hand, the identity of a user should not be leaked, but a user must be authenticated to obtain the corresponding private key. We propose a new system architecture to realize such an AKI protocol, by employing non-colluding identity-certifying authority (ICA) and KGC.

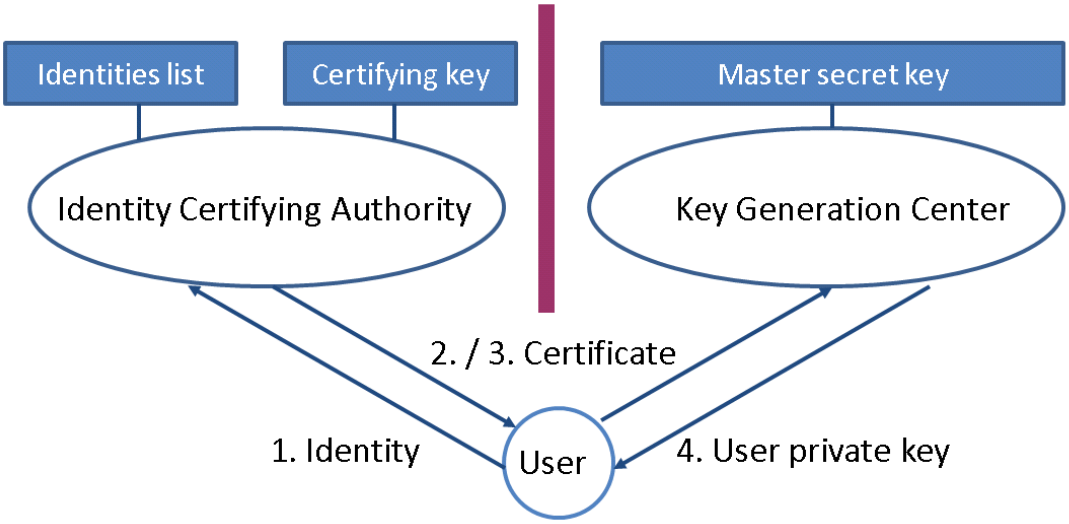

Figure 5.1: *Our New System Architecture for IBE*

From a high level, the ICA is responsible for issuing each user a certificate on the purported identity after authentication. This certificate is generated using the master certifying key sk_{cert}. The certificate alone would not enable the user to decrypt. The user should contact the KGC who issues a private key based on the certificate presented, but the KGC never gets to know the identity involved in the certificate. The user private key is still generated with the help of the master secret key, that is owned by the KGC and kept secret from the ICA. Figure 5.1 depicts the certification and the key issuing process. Since the ICA keeps the identities list of the system's users, we make the trust assumption that the ICA does not collude with the KGC (or the KGC can get the identities list easily). As in PKI, we also assume that the ICA would not impersonate any user. Our solution requires a user to contact two parties before getting a key. Nevertheless, it may be cost-prohibitive to have a globally available KGC to authenticate users and issue keys to users via secure channels in a typical ID-based cryptosystem.

5.1.1 Formal Definition

An anonymous key issuing protocol for an IBE scheme consists of four polynomial-time algorithms in additional to the Setup and MKeyGen algorithms from the IBE. For brevity, the public

parameter $param$ output by Setup is omitted below.

1. via $(pk_{cert}, sk_{cert}) \xleftarrow{\$} \mathsf{IKeyGen}()$ the ICA probabilistically outputs the public/secret key pair for certification pk_{cert}, sk_{cert};

2. via $(cert, aux) \xleftarrow{\$} \mathsf{SigCert}(sk_{cert}, \mathsf{ID})$ the ICA probabilistically outputs a certificate for identity ID and some auxiliary information aux;

3. $\mathsf{ObtainKey}(mpk, \mathsf{ID}, cert, aux) \leftrightarrow \mathsf{IssueKey}(sk, cert)$ are two interactive algorithms which execute a user secret key issuing protocol between a user and the KGC. Recall that the key generation algorithm $\mathsf{MKeyGen}(param)$ outputs (mpk, msk). The user takes as input the master public key mpk, an identity ID, and the corresponding certificate $cert$ with auxiliary information aux, and gets a user secret key $usk[\mathsf{ID}]$ as output. The KGC takes the master secret key msk and the certificate $cert$ as input and gets nothing as output.

5.1.2 Design Framework

Here we give a general design framework of such a protocol. We do not claim that any design based on the primitives mentioned here must be secure, but we will analyze the security of our concrete protocol to be proposed shortly afterward, which is based on the standard argument in anonymous credential literature [BCKL08, Cha08].

The first step of our AKI protocol is to get a certificate on an identity from the ICA, which just utilizes a signature scheme. However, the user needs to show this signature to the KGC without leaking the identity (being signed). So the ICA signs on a hiding commitment of the identity instead. This also requires the ability to prove that the contents of a commitment have been signed.

For the KGC side, considering that a user secret key in IBE is essentially a signature on an identity given by the master secret key, obtaining a user secret key without leaking the identity to the KGC boils down to obtaining something similar to a blind signature from the KGC (not to be confused with the signature by the ICA). The blinding step can make a commitment to the identity, the key issuing protocol then becomes one for obtaining a signature on a committed value. A crucial difference between our protocol and a blind signature or anonymous credential is

manifest at the final stage of our protocol. We require that the user can transform the response from the KGC to a normal signature which directly signs on the value being committed, such that it can be used as the private decryption key of the IBE scheme. In particular, if the final signature just includes a non-interactive proof for proving that the contents of a commitment have been signed, it does not seem to work with any of the existing IBE schemes.

5.2 Security Requirements

One can view $(cert, aux)$ as a signature and $\mathsf{SigCert}$ as the signing algorithm of a signature scheme. For security we require existential unforgeability against adaptive chosen message attack. We omit this standard definition. Our framework assumes $\mathsf{SigCert}$ is used to sign on the (perfectly binding and strongly computationally hiding) commitment of an identity, which is included in $cert$.

Regarding $\mathsf{ObtainKey}$ and $\mathsf{IssueKey}$, we require that malicious users can only get the user private key for the identity "embedded" in the ICA's certificate from the interaction with the KGC, but nothing else. For security protection of the users, we require that the KGC cannot learn anything from the certificate about the real identity of the user. Below is a formalization of the above intuition, which is adopted from some of the security properties of the P-signature [BCKL08], a suite of protocols for obtaining signature in a privacy-preserving way.

Definition 5.1. An AKI protocol satisfies *issuer privacy* if there exists a simulator $\mathsf{SimIssue}$ such that for all PPT adversaries $(\mathcal{A}_1, \mathcal{A}_2)$,

$$
\begin{aligned}
|\Pr\ [\ & param \xleftarrow{\$} \mathsf{Setup}(1^\lambda); (mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param); \\
& (\mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param, mpk, msk); com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux); \\
& b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{IssueKey}(param, msk, com) : b = 1] \\
-\Pr\ [\ & param \xleftarrow{\$} \mathsf{Setup}(1^\lambda); (mpk, msk) \xleftarrow{\$} \mathsf{MKeyGen}(param); \\
& (\mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param, mpk, msk); com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux); \\
& b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{SimIssue}(param, \mathsf{KeyDer}(msk, \mathsf{ID}), com) : b = 1]| < \mathsf{negl}(\lambda).
\end{aligned}
$$

Intuitively, this captures the requirement that the protocol itself reveals no information to

the adversary (in particular, msk) other than a user secret key.

In our definition, both $\mathsf{SimIssue}$ and $\mathsf{IssueKey}$ get an honestly generated commitment, for adversarially chosen identity ID and opening aux. Since we assume the commitment is perfectly binding, this automatically guarantees that the identity associated with the commitment is well defined, and only a user secret key corresponding to that particular identity is obtained by the adversary.

For a cleaner definition, $\mathsf{SigCert}$ is not involved. Whether $\mathsf{SimIssue}$ and $\mathsf{IssueKey}$ receives a signature on a commitment of ID or ID itself is just about how their interfaces take ID as the input. We allow $\mathsf{SimIssue}$ to rewind the adversary and it can extract the hidden ID from the commitment.

The above definition assumes the adversary knows msk even its purpose is for the protection of the secrecy of msk. This is adopted from the security definition of secure two-party computation protocols, which models the situation that even the adversary is given some partial information of msk (e.g. through our IBE scheme), it is still unable to distinguish whether it is interacting with a simulator or the real key issuing protocol. Together with the security of the underlying IBE scheme (e.g. CCA2 with access to a user secret key oracle), our definition guarantees that the AKI protocol can be used with the IBE scheme.

Definition 5.2. An AKI protocol satisfies *user privacy* if there exists a simulator $\mathsf{SimObtain}$ such that for all PPT adversaries $(\mathcal{A}_1, \mathcal{A}_2)$,

$$
\begin{aligned}
|\Pr\ [\ & param \xleftarrow{\$} \mathsf{Setup}(1^\lambda), (mpk, \mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param); \\
& com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux); \\
& b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{ObtainKey}(param, mpk, \mathsf{ID}, com, aux) : b = 1] \\
-\Pr\ [\ & param \xleftarrow{\$} \mathsf{Setup}(1^\lambda), (mpk, \mathsf{ID}, aux, st) \xleftarrow{\$} \mathcal{A}_1(param); \\
& com \leftarrow \mathsf{Commit}(param, \mathsf{ID}, aux); \\
& b \xleftarrow{\$} \mathcal{A}_2(st) \leftrightarrow \mathsf{SimObtain}(param, mpk, com) : b = 1]| < \mathsf{negl}(\lambda).
\end{aligned}
$$

This models that the protocol reveals no information about the identity ID to the malicious KGC which interacts with the user. Both privacy notions are defined based on a single interaction, but a simple hybrid argument can be used to show that these definitions imply privacy over many

sequential instances.

5.3 AKI Protocol for Modified Gentry-IBE

Our protocol extends the interactive protocol for obtaining a signature on a committed value of the first P-signature scheme in [BCKL08]. We change the signature structure of their scheme so that it fits with the user secret key produced in the modified Gentry-IBE. There are three components sharing the same structure in the key. For brevity, we just show how to build the first component.

Setup: This algorithm executes Setup of modified Gentry-IBE, setups the perfectly binding, strongly computationally hiding commitment scheme and the signature scheme.

IKeyGen: The ICA generates a key pair (pk_{cert}, sk_{cert}) from the key generation algorithm of the signature scheme.

SigCert: For $\mathsf{ID} \in \{0,1\}^n$, the ICA creates the certificate $cert = (sig, com, aux)$ by randomly picking aux from the decommitment-string space of the commitment scheme for each ID; and generating a signature sig on $com = \mathsf{Commit}(\mathsf{ID}, aux)$ by running the signing algorithm of the signature scheme using sk_{cert}.

We require that the ICA always use the same aux for a given ID. We can just take aux as the output of a PRF with input ID, for a seed only known to the ICA.

$\mathsf{ObtainKey}(mpk, \mathsf{ID}, cert, aux) \leftrightarrow \mathsf{IssueKey}(msk, cert)$:

1. The user and the KGC engage in a secure two-party computation protocol where the user's private input is (ρ, ID, aux) where $\rho \in_R \mathbb{Z}_p$, and the KGC's private input is α. The KGC then gets a private output which is either $x = (\alpha - \mathsf{ID})\rho$ if $com = \mathsf{Commit}(\mathsf{ID}, aux)$, or $x = \perp$ otherwise.

2. If $x \neq \perp$, the KGC randomly picks $\tau_{\mathsf{ID},1} \in \mathbb{Z}_p$ for each certificate presented. Then it computes $usk'_{cert} = (usk'_1 = (h_1 g^{-\tau_{\mathsf{ID},1}})^{1/x}, usk'_2 = \tau_{\mathsf{ID},1})$.

3. The user outputs $(usk_1, usk_2) = ((usk'_1)^{\rho} = (h_1 g^{-\tau_{\mathsf{ID},1}})^{1/(\alpha - \mathsf{ID})}, usk'_2)$.

Similar to the treatment of aux in SigCert, if a certificate signing the same commitment is presented later, same $\tau_{\mathsf{ID},1}$ is used.

Instead of relying on a generic secure two-party computation protocol for the first step, an efficient protocol for securely computing $g'^{1/(sk+m)}$ based on any homomorphic encryption in the standard model [Cha08, §4.3.3] can be used. In our case, the base g' is $h_1 g^{-\tau_{\mathsf{ID},1}}$, sk is α and m is $-\mathsf{ID}$.

While the signature of the second construction in [BCKL08] shares similarity with the user secret key of BB-IBE [BB04a], the second component r of the user secret key in BB-IBE (which is needed in the decryption) cannot be recovered since the simulation in the security proof can only give a one-way function value of r. More importantly, BB-IBE is not $\mathcal{ACI} - \mathcal{KGC}$ secure.

5.4 Security Analysis

Signer privacy and user privacy follow exactly as in the protocol in [BCKL08]. SimIssue invokes the simulator for the two-party computation (2PC) protocol to extract the adversary's input (ρ, ID, aux), check if $com = \mathsf{Commit}(\mathsf{ID}, aux)$ and send (usk_1^{ρ}, usk_2) to the user. SimObtain also invokes the same simulator to extract the secret key. Then the simulator is given the target output of the computation x, and proceeds to interact with the adversary such that if the adversary completes the protocol, its output is x. In both cases, if the adversary can determine that it is talking with a simulator, it must be the case that the adversary's input to the protocol was incorrect which breaks the security of 2PC.

5.5 Related Constructions

"Anonymous" secret key issuing in ID-based cryptosystems was firstly considered by Sui *et al.* [SCH+05], in a system where the duties of authentication and key issuing are separated to local registration authorities (LRAs) and the KGC. Instead of having an LRA to issue a signature, a user supplies a password to the LRA. To use their protocol, an LRA is required to send a list of identities and passwords to the KGC, while our protocol does not require any communication between them and this requirement is not suitable for our purpose. Secondly, their anonymity

requirement just consider outsider adversaries.

The blind extraction protocols for IBE by Green and Hohenberger [GH07] is defined based on the notion of leak freeness and selective-failure blindness. The motivating application in [GH07] is oblivious transfer, hence the notion of selective-failure blindness considers maliciously generated parameter. Our notion of issuer privacy is very similar to leak freeness as both are defined in a secure 2PC fashion. A minor difference is that their definition is not coupled with any specific way (e.g. commitment) to bind the identity, although their concrete protocols utilize commitment scheme as well. Also, for the application of oblivious transfer, it is not one of the essential goals to make sure that the hidden identity is certified by some third party. Our user privacy is weaker, but it should be fine for our purpose, especially when the KGC is not motivated to induce a selective failure and the user can verify the validity of the key obtained.

As noted in [GH07], it is non-trivial to come up with an efficient AKI protocol for BF-IBE, another IBE that we showed is $\mathcal{ACI} - \mathcal{KGC}$-secure. However, if one is willing to weaken the security guarantee from 2PC to something like one-more unforgeability of blind signature [Bol03], we conjecture that an efficient AKI protocol for BF-IBE can be constructed similar to the blind signature scheme in [Bol03].

5.6 Privacy-Preserving Searches on Encrypted Data

Anonymous IBE has attracted attention for the privacy benefits, and as a leverage to construct public key encryption with keyword search [ABC+08, BCOP04] as follows. Identity strings are used to represent the keywords. The private key for a particular identity is the trapdoor for testing whether a ciphertext is tagged with a particular keyword. The role of the KGC is now known as the trapdoor generator. To create an encrypted tag, one encrypts a random message using the keyword as the identity in IBE, and appends the message with the tag. To locate the ciphertexts tagged with a keyword, one tries to use a trapdoor to decrypt the tag, and see if the result matches the accompanying message.

Back to our notion, $\mathcal{ACI} - \mathcal{KGC}$ implies that the compromise of the private key does not leak the keyword from an encrypted tag. Our AKI protocol also finds application in privacy-preserving delegated forensic search with authorization, which the government issues a warrant

on a keyword to a law enforcing agent (e.g. the police). This warrant is then presented to the encrypted-data owner to indicate that the agent is authorized to ask for a trapdoor for the certified keyword, without revealing what is of forensic interests or (the extreme way of) asking the data owner to surrender the private key. While the idea of privacy-preserving delegated keyword search has been considered, only blind protocols for non-user-anonymous IBE schemes like BB-IBE and Waters-IBE are proposed [GH07], and without addressing a realistic concern that the hidden keyword should be certified by some authority. We remark that the government can be responsible for the system parameter generation to ensure keyword privacy.

□ End of chapter.

Part III

Attribute-Based Encryption

Chapter 6

Anonymous Key Issuing for Attribute-Based Encryption

After presenting anonymous key issuing for identity-based encryption, now we study anonymous key issuing for attribute-based encryption. However, note that the natures of the two protocols are quite different. In the former, the identity is what determines the decryption privilege of the user secret key but still we want it to be hidden from the KGC. For the protocol in this chapter, the identity does not determine the decryption privilege but it just binds different attributes together and is crucial for the collusion resistance of the encryption system.

We firstly give a high level description of our idea, which is followed by a formalization of the required algorithms and security requirements. We then present our proposed protocol, and how to incorporate the protocol with an existing attribute-based encryption system. We end this chapter by a discussion on how to prevent abuse in anonymous systems in general.

6.1 Anonymous Credential for Attribute-Based Encryption

In our anonymous key issuing protocol, we will make use of some basic techniques in anonymous credential systems to protect the privacy of ABE users. Up until now, there has been little relationship between anonymous credentials and ABE (except the result in the previous chapter

which is about the key-escrow problem of IBE).

In an anonymous credential system (see [Bra99, CL01]), users wish to obtain and prove possession of credentials while remaining anonymous. In such work it is assumed that each user has a unique secret key (and there are different proposals for how to prove that a given key is valid and to prevent users from loaning out their keys, which we will discuss in Section 6.5). Then the user can interact with each authority under a different pseudonym in such a way that it is impossible to link multiple pseudonyms belonging to the same user. At the same time, all of a user's pseudonyms, and the resulting credentials, are tied to the same secret key so that the user can prove that he has *both* attribute set $\mathbb{A}$ from one authority and set $\mathbb{B}$ from another.

We will use techniques from anonymous credentials to allow the users to obtain decryption keys from the authorities without revealing their global identifiers GID's.

The basic idea is to let the GID play the role of the anonymous credential secret key. We will now assume that each user has a unique and *secret* GID value. A user interacts with authorities using pseudonyms based on this value, and thus obtains decryption keys.[2] Thus, we will replace the GID with the assumption that each user has unique secret key as in an anonymous credential system. Guaranteeing that this secret key is unique involves a number of subtle issues. See Section 6.5 for a discussion of relevant techniques from the anonymous credential literature. Note, however, that anonymous credentials do not immediately solve the privacy issue in an ABE setting, as argued in Section 1.4.4. We design a protocol by which a user can obtain a set of decryption keys for his secret GID without revealing any information about that GID to the authority. At the same time, the authority is guaranteed that the agreed upon decryption keys are the only thing that the user learns from the transaction.

Finally, we stress that, although we use several elements of anonymous credential systems, our solution does not encrypt with respect to a user's secret key. This is still strictly an attribute-based encryption system, in which decryption ability is determined only by a user's attributes. The secret key/GID is only used in communicating with the various authorities, and in determining the appropriate decryption keys.

[2] Another option would be to allow the user to reveal the GID to select authorities, but to require that there be some additional secret information that was known only to the user, to prevent impersonation.

6.2 Framework and Security Requirements

Our definition of an authority-unlinkable ABE scheme extends the existing multi-authority ABE definition [Cha07] by adding an interactive protocol to allow the user to obtain a decryption key from the authority without revealing his GID.

Definition 6.1. An N-authority-unlinkable ABE scheme is an N-authority ABE scheme with three extra algorithms ($param$ and $\{apk_k\}_{k\in\{1,\dots N\}}$ are omitted from the input):

1. $(nym, aux) \xleftarrow{\$} \mathsf{FormNym}(\mathsf{GID})$ probabilistically outputs a pseudonym for identity GID, and some auxiliary information aux.

2. $\mathsf{ObtainKey}(apk_k, \mathsf{GID}, \mathbb{A}_k, nym, aux) \leftrightarrow \mathsf{IssueKey}(ask_k, \mathbb{A}_k, nym)$ are two interactive algorithms which execute a user secret key issuing protocol between a user and the attribute authority k. The user takes as input the public key apk_k of the attribute authority k, an attribute set $\mathbb{A}_k$, an identity GID, and the corresponding pseudonym nym with auxiliary information aux, and gets what $\mathsf{AKeyGen}(ask_k, \mathsf{GID}, \mathbb{A}_k)$ outputs, i.e. a decryption key for identity GID corresponding to the attribute set $\mathbb{A}_k$. The attribute authority gets the secret key ask_k, the set of attributes $\mathbb{A}_k$ and the pseudonym nym as input, and gets nothing as output.

with the following properties

1. $(nym, aux) \xleftarrow{\$} \mathsf{FormNym}(\mathsf{GID})$ produces a commitment nym to the user's GID with randomness aux,

2. $\mathsf{ObtainKey} \leftrightarrow \mathsf{IssueKey}$ form a secure two party computation (2PC) protocol for the following functionality F, where $(\{(apk_k, ask_k)\}_{k\in\{1,\dots N\}})$ is as output by $\mathsf{Setup}(1^\lambda, N)$:

   F takes as public input the authority's public key apk_k, the user's pseudonym nym, and the attribute set $\mathbb{A}_k$. It also receives as secret input the user's identity GID and the corresponding aux, and the authority's secret key ask_k. It outputs the result of $\mathsf{AKeyGen}(ask_k, \mathsf{GID}, \mathbb{A}_k)$ to the user.

6.3 Generic Anonymous Key Issuing Protocol

Now we present an anonymous key issuing protocol which allows multi-authority ABE with enhanced user privacy. The users can communicate with AAs via pseudonyms instead of having to provide their GIDs in the clear. At the same time, the AAs are prevented from linking multiple attribute sets belonging to the same user by pooling their data.

As a building block we construct a protocol for an oblivious computation of a key of the form $(SK \cdot PRF_\beta(u))^\gamma$, where u is a user's GID, SK represents some secret information related to the private key of an authority, β is the secret seed for the PRF owned by an authority and γ corresponds to some secret related to an attribute controlled by an authority. The key is produced obliviously, i.e. without either the authority or the user revealing any of their secret information ((SK, β, γ) or u respectively). We chose to present the protocol in this "generic" way (without coupling with any particular ABE scheme) to illustrate its applicability. We show how this protocol can be applied to Chase system (with a little modification) in a rather straightforward manner (see Section 6.4). We also show how to efficiently apply this protocol to our scheme which removes the CA. (In this case the keys are a bit more complex, so we need somewhat more involved techniques - see Chapter 7.)

Finally, our results may be of additional interest because they show new applications of the oblivious computation protocol for a distributed PRF, and a generalization of the oblivious PRF techniques of Jarecki and Liu [JL09].

As mentioned before, a multi-authority ABE system which requires a user to present his unique identifier to every authority would have severe privacy shortcomings. In particular, it will be trivial for the various authorities to combine their data and assemble a complete picture of all of a user's attributes in all domains. To avoid this we look to related work on anonymous credentials [Bra99, CL01]. We will treat the GID as the user's secret key. Then the user can form different pseudonyms based on this GID to use when interacting with different authorities. (See Section 6.5 for a discussion of how we can do this while ensuring that users honestly use their true GIDs.) When the user wishes to obtain decryption keys for certain attributes associated with this authority, he performs an interactive protocol with the authority. As a result of this protocol, he gets decryption keys tied to the GID that corresponds to his pseudonym. These can

then be combined with decryption keys obtained from other authorities using other pseudonyms for the same GID. However, from the authorities' point of view the GID is completely hidden. In fact it is even infeasible for two authorities to tell that they are talking to the same user.

Here we present a "generic" protocol such that a user with a private value $u \in \mathbb{Z}_p$ and an authority with private keys $\alpha, \beta, \gamma \in \mathbb{Z}_p$ can jointly compute the value $(h^\alpha g^{1/(\beta+u)})^\gamma$ for commonly known $g, h \in \mathbb{G}$ where the discrete logarithm between g and h be unknown to any corrupt user. Only the user gets this output, and all other information is hidden.

The roles of each private value will be apparent when this protocol is used as the anonymous key issuing protocol for the ABE systems to be presented in Section 6.4 and 7.4. The basic intuition is that the structure of the final value $(h^\alpha g^{1/(\beta+u)})^\gamma$ resembles a product of h^α, which corresponds to something related to the private key of an authority, and a randomizer computed as $PRF_\beta(u)$, where β is the secret seed for Dodis-Yampolskiy PRF [DY05], and u is the GID of the user. [3] Finally, γ corresponds to some secret related to an attribute controlled by an authority.

User u		Attribute Authority
$\rho_1 \in_R \mathbb{Z}_p$,	$\xleftarrow{\quad 2PC \quad}$	$x := (\beta + u)\rho_1, \tau \in_R \mathbb{Z}_p$
$\rho_2 \in_R \mathbb{Z}_p$	$\xleftarrow{X_1, X_2, \mathsf{PoK}(\alpha, \tau, x)}$	$X_1 := g^{\tau/x}, X_2 = h^{\alpha\tau}$
$Y := (X_1^{\rho_1} X_2)^{\rho_2}$	$\xrightarrow{Y, \mathsf{PoK}(\rho_2)}$	
$D := Z^{1/\rho_2}$	$\xleftarrow{Z, \mathsf{PoK}(\tau, \gamma)}$	$Z := Y^{\gamma/\tau}$

Figure 6.1: *Our Anonymous ABE Key Issuing Protocol*

Figure 6.1 shows our protocol for anonymous key issuing. In each step, PoK represents a proof of knowledge of the secret values used in the computation. For simplicity we have omitted the statement being proved. Here the first step denotes a 2PC protocol which takes (u, ρ_1) from the user and β from the authority and returns $x := (\beta + u)\rho_1 \bmod q$ to the authority. This can

[3] In order for this to be a valid PRF, we need u to be chosen from some predefined polynomial-sized domain. Alternatively, we can choose $u = H(\mathsf{GID})$ for hash function H, but the result will be secure in the random oracle model instead.

be implemented via a general 2PC protocol for a simple arithmetic computation. Alternatively, we can do this more efficiently using the construction in [BCC+09]. The necessary proofs of knowledge (PoK) for the above statements can be efficiently realized, e.g. via a Schnorr protocol.

Theorem 6.2. *The above protocol is a secure 2PC protocol for computing* $(h^\alpha g^{1/(\beta+u)})^\gamma$*, assuming that the underlying arithmetic 2PC and zero knowledge proofs are secure, and (for security against corrupt user) that DDH is hard.*

Proof. For correctness, $Z^{1/\rho_2} = Y^{\gamma/(\tau\rho_2)} = (X_1^{\rho_1\gamma/\tau} \cdot X_2^{\gamma/\tau}) = (g^{\rho_1\gamma/x} \cdot h^{\alpha\gamma}) = (h^\alpha g^{1/(\beta+u)})^\gamma$. To show security we consider the cases of corrupt issuer and corrupt user below.

Corrupt issuer. In the case of a corrupt issuer, our simulator proceeds as follows:

Sim_U First, it will run the arithmetic 2PC simulator for computation of $(\beta+u)\rho_1$. This 2PC will extract β from the issuer and expect to be provided with $x = \rho_1(\beta + u) \mod p$. We will choose a random value $x \in_R \mathbb{Z}_p$, and give it to the arithmetic 2PC simulator. Note that this is correctly distributed, since for any x, β, u, there is some ρ_1 such that $x = \rho_1(\beta + u) \mod p$. Next, our simulator will receive X_1, X_2 from the adversary, and two corresponding zero knowledge proofs. We will use the extractor for the proof system to extract α. We will choose a random $Y \in_R \mathbb{G}$ and return it. (Again, this will be distributed exactly as in a real execution.) Finally, we will receive Z from the adversary, and use the extractor to extract γ from the corresponding proof. We will give α, β, γ to the trusted party, and receive $(h^\alpha g^{1/(\beta+u)})^\gamma$, which will be the user's private output.

Consider a hybrid simulator Hyb_U that takes as input the user's identifier u. It first runs the arithmetic 2PC simulator for the computation of x (with the correct output value according to u), and then completes the protocol as the honest user would. This is clearly indistinguishable from the real user's protocol by the security of the arithmetic 2PC.

Now, assuming that the proof of knowledge scheme is secure, Hyb_U should be indistinguishable from the above simulator Sim_U. This is because the values x, Y used by Sim_U will be distributed identically to those in Hyb_U. (Since ρ_1, ρ_2 are chosen at random in the real protocol, x will be distributed uniformly over $\mathbb{Z}_p$, and Y will be distributed uniformly over $\mathbb{G}$ in the real protocol

as in the simulated protocol.) Thus, interaction with our simulator is indistinguishable from interaction with an honest user.

Corrupt user. In the case of a corrupt user, our simulator proceeds as follows:

Sim_I First, it will run the arithmetic 2PC simulator for computation for $(\beta+u)\rho_1$ (in the process it will extract u). Next the simulator will choose random values $X_1, X_2 \in_R \mathbb{G}$, and send them to the user. It will receive Y from the user, and extract ρ_2 from the corresponding proof. Then it will send u to the trusted party and receive $D = (h^\alpha g^{1/(\beta+u)})^\gamma$. Finally, it will compute $Z = D^{\rho_2}$ and send it to the user.

Consider a hybrid simulator Hyb_I that takes as input the issuer secrets α, β, γ. It will compute $x = (\beta + u)\rho_1$ using the arithmetic 2PC simulator. When the 2PC simulator provides u, ρ_1 and asks for output, it will correctly compute $x = \rho_1(\beta + u)$. Then it will complete the execution as in the real protocol. This protocol is clearly indistinguishable from the real protocol by the security of the arithmetic 2PC.

Next, we consider a second hybrid Hyb'_I which proceeds as in Hyb_I, but which uses the zero-knowledge simulator for all proofs of knowledge. This must be indistinguishable by the zero-knowledge property of the proof system. Now we need only show that this second hybrid is indistinguishable from the interaction with the above simulator.

Consider the following reduction from DDH: Given $g, A = g^a, B = g^b, C = g^c$, where $a, b \in_R \mathbb{Z}_p$, and we must decide whether $c = ab$ or $c \in_R \mathbb{Z}_p$. We set $h = A^\theta$, for $\theta \in_R \mathbb{Z}_p$. As described in Sim_I, we run the arithmetic 2PC simulator to compute $x = \rho_1(\beta+u)$, and to extract u. Then we compute $X_1 = B^{(1/x)}, X_2 = C^{\theta\alpha}$, and send them to the adversary, along with a simulated proof of knowledge. We receive Y and extract ρ_2 from the corresponding proof. Finally, we compute $Z = (g^{1/(\beta+u)} A^{\alpha\theta})^{\gamma\rho_2}$, and return it to the user.

Note that, assuming that the proofs of knowledge are secure, if $c = ab$, X_1, X_2, Z will be distributed correctly, and this will be indistinguishable from Hyb'_I. On the other hand, if c is random, then X_1, X_2 are just values chosen at random from $\mathbb{G}$, as in Sim_I. Thus, any adversary that can distinguish Hyb'_I from Sim_I will allow us to solve DDH. We conclude that under the DDH assumption, interaction with Sim_I is indistinguishable from interaction with a real authority.

Thus our construction is a secure 2PC protocol. □

6.4 Adding the Anonymous Key Issuing Protocol

Before we can apply our oblivious key issuing protocol, we need to make suitable modifications to the scheme used in [Cha07]. In particular, Chase assumes a PRF with range $\mathbb{Z}_p$ and generates decryption keys blinded by $g_1^{PRF_k(\mathsf{GID})}$. Here instead, we wish to use the modified Dodis-Yampolskiy PRF (DY-PRF), which has range $\mathbb{G}_1$. We observe that the PRF in the exponent used in [Cha07] can be replaced by DY-PRF with group elements as its range, so that the values are instead blinded by $PRF_k(\mathsf{GID})$. With this modification and a little twist in the key structure, we can directly apply our key issuing protocol.

The scheme below is modified from the Chase scheme [Cha07] with the following changes.

1. We have rephrased it in the asymmetric bilinear map setting ($e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ instead of $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$) and we assume there does not exist an efficiently computable isomorphism from $\mathbb{G}_1$ to $\mathbb{G}_2$, i.e. the XDH assumption is made.

2. The PRF is assumed to produce output in $\mathbb{G}_1$, not in $\mathbb{Z}_p$, so $PRF_k(u)$ is used in place of $g_1^{PRF_k(u)}$, this change allows us to use the DY-PRF [DY05], which works with our anonymous key issuing protocol.

3. The attribute key for user is changed, and a little step is added in the decryption algorithm accordingly.

In the following description, we begin by the setup for the whole system, then we proceed to the key generation of the central authority and each attribute authority. After that, we will describe the encryption and the decryption algorithm.

System

Setup: Fix prime order groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, and generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$. Choose seeds $s_1, \ldots, s_K$ for all authorities. Also choose $y_0 \in_R \mathbb{Z}_p$.

System Public Key: $Y_0 = e(g_1, g_2)^{y_0}$.

Central Authority

Central Authority Secret Key:

- y_0 that is kept secret
- s_k which is sent to authority k for $k = 1, \cdots, K$

Secret Key for User u:

- $D_{\text{CA}} = g_1^{y_0} / \prod_{k=1}^{K} PRF_k(u)$

Attribute Authority k

Authority Secret Key: $t_{k,1} \dots t_{k,n} \in_R \mathbb{Z}_p$, and s_k.

Authority Public Key: $T_{k,1} \dots T_{k,n}$ where $T_{k,i} = g_2^{t_{k,i}}$.

Secret Key for User u: Choose a random $d-1$ degree polynomial p with $p(0) = 0$. Secret key: $\{D_{k,i} = g_1^{p(i)/t_{k,i}} \cdot PRF_k(u)^{1/t_{k,i}}\}_{i \in \mathbb{A}^u}$.

Encryption for attribute set $\mathbb{A}^C$:

Choose random $s \in_R \mathbb{Z}_p$. $E = Y_0^s m$, $E_{\text{CA}} = g_2^s$, $\{E_{k,i} = T_{k,i}^s\}_{i \in \mathbb{A}_k^C, \forall k}$.

Decryption :

1. For each authority k, for d attributes $i \in \mathbb{A}_k^C \cap \mathbb{A}^u$, compute $e(D_{k,i}, E_{k,i}) = e(g_1, g_2)^{p(i)s} \cdot e(PRF_k(u), g_2)^s$.
2. Interpolate to find $e(g,g)^{p(0)s} \cdot (e(PRF_k(u), g_2)^s)^X = e(PRF_k(u), g_2)^{sX}$, where X is a sum of different Lagrange interpolation coefficients known to the decryptor. It is thus easy to obtain $Y_k^s = e(PRF_k(u), g_2)^s$.
3. Compute $Y_{\text{CA}}^s = e(D_{\text{CA}}, E_{\text{CA}})$ which is also equal to $e(g_1^{y_0}, g_2^s) / e(\prod_{k=0}^{K} PRF_k(u), g_2^s)$.
4. Combine these values to obtain $Y_{\text{CA}}^s \cdot \prod_{k=1}^{K} Y_k^s = Y_0^s$. Then $m = E / Y_0^s$.

Security Analysis. Although we change the structure of the attribute-key obtained by the user, it is just syntactical change and we claim that (somewhat surprisingly) the original security proof still follows, with an extra XDH assumption. The original proof are omitted here since it is just a simpler version of our proof in Section 7.5 in the next chapter.

The crucial details are as follow. In our scheme, $D_{k,i} = g_1^{p(i)/t_{k,i}} \cdot PRF_k(u)^{1/t_{k,i}}$. In the simulation, $D_{k,i} = g_1^{\phi(i)/t_{k,i}} \cdot g_1^{R_k/t_{k,i}}$ where $\phi(x) = p'(x) - p'(0)$ for all x, $R_k = z_{k,u} b$ for $k \neq \hat{k}$ and $R_k = ab + z_{k,u} b$ for $k = \hat{k}$. Since $\phi(0) = 0$ and the polynomial p is randomly selected under

the constraint that $p(0) = 0$, the first component of $D_{k,i}$ is simulated perfectly. For the second component, it is computationally indistinguishable as long as DY-PRF is pseudorandom.

6.5 Preventing Abuse in Anonymous Systems

A number of approaches exist in the anonymous credential literature for preventing abuse. Here we describe a few techniques that could be used in our setting.

One important issue is how we will ensure that users are using the correct GID when this information is hidden from the authorities. How can we ensure that users do not share their GID's with their friends, or generate fake GID's?

The way this is generally addressed in the anonymous credential literature [Bra99, Lys02] is to have separate certification authority who does get to see the user's GID, but knows nothing about his other activities in the system. This authority will verify the user's identity (how this is done depends on exactly what is used as the GID), and then issue a credential stating that the GID is valid. This credential is such that the user can later present a pseudonym based on his GID and prove that he has a credential for that GID, without revealing the GID itself. (This functionality can also be distributed across many independent certification authorities.)

This does not in itself prevent the user from sharing his GID. He could easily give away both his GID and the associated credential. Thus, several anonymous credential systems propose additional measures [GPR98, Bra99, LRSW99], where some additional secret and important information is tied into the credential. (This could be for example a credit card number, electronic check, or a secret key for an existing, important signature scheme.) This will be done in such a way that the user cannot share the credential without also sharing this secret information. One approach is to design the system in such a way that using the credential will require the user to prove knowledge of this information.

Finally, in our system we have the additional requirement that we must ensure that each user only gets one set of keys from each authority. We will do this using techniques developed for credential revocation [BCC04, BL07]. The certification authority will include in the credential some additional random value *rtag*, generated jointly by the authority and user and unknown to the authority. Then when he requests attribute keys from a given authority, the user will

compute $h_k(rtag)$ using the authority's function h_k (e.g. under the XDH assumption we might use $h_k(rtag) = X_k^{rtag}$ for some value $X_k \in \mathbb{G}_1$ whose discrete logarithm is unknown) and send the resulting value along with his pseudonym and credential proof. Then the authority can verify that this value is new before issuing decryption keys to the user.

□ End of chapter.

Chapter 7

Decentralizing Key-Policy Attribute-Based Encryption

New technique for decentralizing key-policy attribute-based encryption will be presented in this chapter, at the same time user privacy can still be preserved without introducing too much computational overhead.

This chapter starts by the definitions of multi-authority ABE. We then give the intuition behind existing attempts and our approach in removing the trusted central authority (CA) from multi-authority ABE. For a complete privacy-preserving solution, we need to incorporate our anonymous key issuing protocol presented in Chapter 6 to our CA-free system. However, a trivial adaptation will result in a rather inefficient scheme and we explain our way to circumvent this problem, which leads to our final construction. We analyze our proposed construction in terms of security and efficiency. Finally, various extensions of our proposed system are presented.

7.1 Definitions of Multi-Authority ABE

We begin by defining a multi-authority ABE scheme with a trusted setup (but without an online trusted CA), and without any privacy guarantees. For now, we consider a key-policy threshold scheme, where the user's decryption key corresponds to a set of attributes and a threshold value. (See Section 7.6 for an extension to more general policies.)

In a multi-authority ABE system, we have many attribute authorities, and many users. There are also a set of system-wide public parameters available to everyone (either created by a trusted party, or by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the ciphertext. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

In what follows, we use GID to denote the global identity of a user and $\mathbb{A}$ to denote a set of attributes. We use $\mathbb{A}^u$ and $\mathbb{A}^C$ to denote the attribute set of a user and that specified by a ciphertext respectively. We assume all the attribute sets can be partitioned into N disjoint sets, handled by the N attribute authorities, and we use a subscript k to denote the attributes handled by the authority k.

Definition 7.1. An N-authority ABE scheme consists of four algorithms:

1. Via $(param,\ \{(apk_k, ask_k)\}_{k\in\{1,\dots N\}}) \xleftarrow{\$} \mathsf{Setup}(1^\lambda, N)$ the randomized key generation algorithm takes a security parameter $\lambda \in \mathbb{N}$ and the number of authorities $N \in \mathbb{N}$, and outputs the system parameters $param$ and N public/secret key pairs (apk_k, ask_k), one for each attribute authority $k \in \{1, \dots N\}$. The threshold values $\{d_k\}_{k\in\{1,\dots N\}}$ for each authority are also included in $param$. For simplicity, we assume $param$ and $\{apk_k\}_{k\in\{1,\dots N\}}$ are the implicit inputs of the rest of the algorithms.

2. Via $usk_k[\mathsf{GID}, \mathbb{A}_k] \xleftarrow{\$} \mathsf{AKeyGen}(ask_k, \mathsf{GID}, \mathbb{A}_k)$ the attribute authority k uses its secret key ask_k to output a decryption key corresponding to the attribute set $\mathbb{A}_k$ for the user with identity GID.

3. Via $\mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\{\mathbb{A}_k\}_{k\in\{1,\dots N\}}, m)$ a sender encrypts a message m for the set of attributes $\{\mathbb{A}_k\}$, resulting in a ciphertext $\mathfrak{C}$, where $\mathbb{A}_k$ denotes a subset of the attribute domain of the authority k.

4. Via $m \leftarrow \mathsf{Dec}(\{usk_k[\mathsf{GID}, \mathbb{A}_k]\}_{k\in\{1,\dots N\}}, \mathfrak{C})$ a user GID who possesses a sufficient set of

decryption keys $\{usk_k[\mathsf{GID}, \mathbb{A}_k]\}$ from each authority k decrypts $\mathfrak{C}$ to recover m.

7.1.1 Consistency

Definition 7.2. An N-authority ABE scheme satisfies the consistency property if for all $\lambda, N \in \mathbb{N}$, all identities GID and all messages m, for all $\{\mathbb{A}_k^u\}$ and $\{\mathbb{A}_k^C\}$ such that $|\mathbb{A}_k^C \cap \mathbb{A}_k^u| > d_k$ for all authorities $k \in \{1, \ldots, N\}$,

$$\Pr[(param,\ \{(apk_k, ask_k)\}_{k\in\{1,\ldots N\}}) \leftarrow \mathsf{Setup}(1^\lambda, N); \mathfrak{C} \xleftarrow{\$} \mathsf{Enc}(\{\mathbb{A}_k^C\}_{k\in\{1,\ldots N\}}, m);$$
$$\mathsf{Dec}(\{\mathsf{AKeyGen}(ask_k, \mathsf{GID}, \mathbb{A}_k^u)\}_{k\in\{1,\ldots N\}}, \mathfrak{C}) = m] = 1,$$

where the probability is taken over the random coins of all the algorithms in the expressions above.

7.1.2 Security

Definition 7.3. An N-authority ABE scheme is (t, n, ϵ)-secure against selective-attribute attack if all t-time adversaries $\mathcal{A}$ compromising at most n authorities have advantage at most ϵ in making the game below return 1.

Experiment $\mathbf{Exp}^{\mathrm{saa}}_{N-\mathcal{ABE},\mathcal{A}}(\lambda)$

$(\mathbb{A}^C = \{\mathbb{A}_1^C, \ldots, \mathbb{A}_N^C\}, \mathbb{K}_{corr} \subset [1, N]\}) \leftarrow \mathcal{A}$;
if $|\mathbb{K}_{corr}| > n$ then return 0;
$\{\mathbb{U}_k\}_{k\notin\mathbb{K}_{corr}} \leftarrow \varnothing$;
$(param, \{(apk_k, ask_k)\}_{k\in\{1,\ldots N\}}) \xleftarrow{\$} \mathsf{Setup}(1^\lambda, N)$;
$(m_0^*, m_1^*, st) \xleftarrow{\$} \mathcal{A}^{\mathsf{AKeyGenO}(\cdot,\cdot,\cdot)}(\text{`}\mathsf{find}\text{'}, param, \{apk_k\}_{k\in\{1,\ldots N\}}, \{ask_k\}_{k\in\mathbb{K}_{corr}})$;
$b \xleftarrow{\$} \{0, 1\}$; $\mathfrak{C}^* \xleftarrow{\$} \mathsf{Enc}(\mathbb{A}^C, m_b^*)$;
$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{AKeyGenO}(\cdot,\cdot,\cdot)}(\text{`}\mathsf{guess}\text{'}, \mathfrak{C}^*, st)$;
if $b \neq b'$ then return 0 else return 1;

where st is state information maintained by $\mathcal{A}$, and the attribute-key generation oracle $\mathsf{AKeyGenO}(\mathsf{GID}, \mathbb{A}_k^u, k)$ is defined as:

if $(k \in \mathbb{K}_{corr})$ return $\perp$;
if $(\exists \mathbb{A}_k^{u\prime}$ s.t. $(\mathsf{GID}, \mathbb{A}_k^{u\prime}) \in \mathbb{U}_k)$ return $\perp$;

if $(|\mathbb{A}_k^u \cap \mathbb{A}_k^C| \geq d_k)$

$\wedge \{\forall j \neq k, [(j \in \mathbb{K}_{corr})$

$\vee (\exists \mathbb{A}_j^u \text{ s.t. } ((\mathsf{GID}, \mathbb{A}_j^u) \in \mathbb{U}_j \wedge |\mathbb{A}_j^u \cap \mathbb{A}_j^C| \geq d_j))]\}$

return $\perp$;

$\mathbb{U}_k \leftarrow \mathbb{U}_k \cup (\mathsf{GID}, \mathbb{A}_k^u)$; return $\mathsf{AKeyGen}(ask_k, \mathsf{GID}, \mathbb{A}_k^u)$.

As in all ABE schemes to date, users are not allowed to simply add attributes to their decryption key set. Instead, a user who wants to update his attribute set must receive an entirely new set of keys. In the multi-authority case (see e.g. [Cha07]), this means that a user cannot simply return to an authority with the same GID – he must obtain new keys from all authorities.

7.2 Removing the Trusted Authority

We review the motivation behind the use of the CA, and show how to avoid it. To have a concrete discussion, we assume the following details of an ABE system. The master public key is $e(g_1, g_2)^{msk}$ and the message m is encrypted in the form of $(e(g_1, g_2)^{s \cdot msk} \cdot m)$ where s is the randomness of the ciphertext.

Simple Secret Sharing Allows Collusion. To allow for multiple attribute authorities, the first step is to distribute the master secret key msk across the different attribute authorities. However, care must be taken to prevent collusion attacks so that users A and B who each have the appropriate attributes from one of two different authorities cannot combine their knowledge to decrypt something neither of them is entitled to.

Now let's look at what happens when we want to divide this msk among the authorities. Consider the two-authority case. Suppose we use a trivial additive sharing of the master secret key $y_1 + y_2 = msk$ where one authority uses y_1 and the other uses y_2, and a scheme where an honest user gets a decryption key based on g^{y_1} and g^{y_2} from the respective authorities. Then a user A with enough attributes from the first authority can recover $e(g_1, g_2)^{y_1 s}$, and similarly, user B with enough attributes from the second authority can recover $e(g_1, g_2)^{y_2 s}$. Even if neither alone has sufficient attributes from both authorities, i.e., user A has not enough attribute from

the second authority, together they will be able recover $e(g_1, g_2)^{s \cdot msk}$ and hence the message m. Thus we cannot use a straightforward sharing of the master secret key between the authorities.

The basic idea is to use a different sharing for each user. But, since we do not want these authorities to communicate among themselves for *every* secret key request, how can they ensure that the values used for each user always sum to msk?

Using PRFs to make the Key "User-Specific". The answer in [Cha07] was to require that authorities compute shares deterministically, each using their own PRF, and then to have a separate CA, whose job was to ensure that the sharing would add up: it would know each authority's PRF seed as well as the msk, it would use this information to generate the shares used for each user, and it would generate the appropriate final share. Specifically, for user GID, each authority k uses share $g^{PRF_k(\mathsf{GID})}$, and the CA gives to user GID the value $g^{msk - \sum_{k=1}^{N}(PRF_k(\mathsf{GID}))}$, where $PRF_k(\cdot)$ denotes a pseudorandom function using authority k's secret seed. A user GID with enough attributes from authority k can recover $e(g_1, g_2)^{s \cdot PRF_k(\mathsf{GID})}$ from the ciphertext. Then this can be combined with the "matching" value obtained from the CA and some component in the ciphertext to recover the session key $e(g_1, g_2)^{s \cdot msk}$.

Ideas behind Lin *et al.*'s Proposal. Instead of using PRFs, Lin *et al.* [LCLS08] uses a degree m polynomial – $F_k(\mathsf{GID}) = a_{k0} + a_{k1}(\mathsf{GID}) + \cdots + a_{km}(\mathsf{GID})^m$ to replace the function $msk - \sum_{k=1}^{N}(PRF_k(u))$. The coefficients of the polynomials $\{F_k\}_{k \in [1,\ldots N]}$ are chosen distributively by all the authorities at the initial setup (i.e. no further communication is necessary for user secret key issuing). The polynomials are constructed in a way such that when they are interpolated, the constant terms $\{a_{k0}\}_{k \in [1,\ldots N]}$ give the master secret key and all other terms become 0. For malicious users A and B to "glue" their keys, terms like $a_{kj}(\mathsf{GID}_A) + a_{k\ell}(\mathsf{GID}_B)$ appear which make the cancellation of the coefficients difficult, but not impossible. Obviously, a degree-m polynomial cannot be random when one sees more than m evaluations of it at different points. As suggested in [LCLS08], a collusion of $(m+1)$ users could interpolate their keys to compute keys corresponding to $F_k(\mathsf{GID}')$ for any GID'.

Ideas behind Our Proposal. The beauty of a PRF family is that no polynomial-time adversary can distinguish (with significant advantage) between a randomly chosen function and a

truly random function (in contrast with a degree m polynomial used in [LCLS08]). The idea here (suggested by Waters and formalized here) is to eliminate the need for the CA by using a set of PRFs whose output values on any particular input always sum to zero.

In more details, each pair of authorities (j, k) shares a secret PRF seed $seed_{jk}$ (again, this sharing is done once and for all at the initial setup stage). This means there are $O(N^2)$ PRFs to be used in total. The final "random-looking" $F_k(\mathsf{GID})$ used by each authority is a linear combination of $N-1$ basic PRFs. More specifically, it is the summation of all of these PRFs, each weighted by either 1 or -1. An appropriate choice of summation and subtraction makes all these PRF values cancel each other when $F_k(\mathsf{GID})$ for different k are added together. Informally, such a "sum-of-PRF" construction still looks pseudorandom to any adversary who knows less than $N-2$ of a particular authority k's secret seeds $seed_{kj}$ (i.e. to any adversary controlling less than $N-2$ other authorities). The final composite PRF is computed as $F_k(\mathsf{GID}) = \sum_{j<k} PRF_{jk}(\mathsf{GID}) - \sum_{j>k} PRF_{jk}(\mathsf{GID})$. This PRF construction is similar to the simplest construction in [NPR99], where it is used to build a distributed key distribution center.

7.3 Adding the Anonymous Key Issuing Protocol

While our anonymous key issuing protocol is general enough to allow issuing keys of the form $(SK \cdot PRF(u))^{1/t_i}$ where (SK, t) is some secret held by the key-issuing authority and u is a private value of the key-requesting user (e.g. GID), a straightforward adoption in the CA-less multi-authority ABE may result in a fairly inefficient system. To see this, recall from Section 6.4 that the keys are of the form $g_1^{p(i)/t_i} PRF_k(u)^{1/t_i}$ for polynomial p (this gives us "user-specific secret keys" which provides collusion-resistance) for each attribute $i \in \mathbb{A}^u$. This means that our key issuing protocol will be invoked $O(|\mathbb{A}^u|)$ times. On top of that, we require $O(N^2)$ copies of the underlying PRF in order to remove the trusted authority, which makes a total of $O(N^2|\mathbb{A}^u|)$ invocations of our key issuing protocol, an undesirably high price for preserving user privacy.

Instead, we will make the number of invocations independent of $|\mathbb{A}^u|$, by introducing extra randomness in the attribute key issuing process. We add $N-1$ blinding factors R_{kj} to the secret value ask used to generate the attribute keys from authority k. The objective is to make the attribute part of the decryption key independent of user GID (but still different for each user) so

that it can be generated without interaction with the user. We then use these R's to play the role of master secret key in the key issuing protocol, i.e. $g_1^{R_{kj}} \cdot PRF_{kj}(u)$ will be issued to user u for each value j. In the decryption process, the user will recover a function of $p(0)$, and can then use these values to remove the blinding.

To see how the new key structure ensures collusion resistance, when a user has enough attributes from a particular authority, he can recover a term with these R terms embedded (because of the way we define $p(0)$). The user secret key contains the term $g_1^{R_{kj}} \cdot PRF_{kj}(u)$, which is the only other information about these R terms. Intuitively, to get rid of these R terms will introduce the user-specific PRF value, which can only be cancelled out by the other PRF values for the *same* user, as hinted in the previous subsection.

7.4 Construction

Our final CA-less multi-authority anonymous ABE works as follows:

Setup The setup stage starts by the following initializations.

- (System Parameter) Given a security parameter λ and a public random string $\mathfrak{S} \in \{0,1\}^{\mathrm{poly}(\lambda)}$, the authorities generate an admissible bilinear group parameters $\langle e(\cdot,\cdot), \psi(\cdot), q, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T \rangle$ from $\mathsf{BDH\_Gen}(1^\lambda; \mathfrak{S})$.

- (Collision-Resistant Hash Function (CRHF)) The authorities also generate from $\mathfrak{S}$ a CRHF $H : \{0,1\}^* \to \mathbb{Z}_p$, which takes the user's global identifier GID as an input. We denote the corresponding output by u.

Since the groups have prime order q and no hidden structure, this can safely be generated from public coins, so each authority can do this independently. The next stage is an interactive protocol. We assume the authorities have authenticated channels with one another.

- (Master Public/Secret Key) Each authority k picks $v_k \in_R \mathbb{Z}_p$ and sends $Y_k = e(g_1, g_2)^{v_k}$ to the other authorities. They all individually compute $Y = \prod Y_k = e(g_1, g_2)^{\sum_k v_k}$.

- (PRF Seed) Each pair of authorities engages in a 2-party key exchange such that each

authority k shares with another authority j a seed $s_{kj} \in \mathbb{Z}_p$ which is only known to them and not to any other authority $i \notin \{j, k\}$. We define $s_{kj} = s_{jk}$.

- (PRF Base) Each authority k randomly picks $x_k \in \mathbb{Z}_p$ and computes $y_k = g_1^{x_k}$, which defines a pseudorandom function $PRF_{kj}(\cdot)$ that can only be computed by authority k and j. Define $PRF_{kj}(u) = g_1^{x_k x_j/(s_{kj}+u)}$ where $u \in \mathbb{Z}_p$, which can be computed by $y_k^{x_j/(s_{kj}+u)}$ or $y_j^{x_k/(s_{kj}+u)}$.

Each authority k also gives non-interactive proofs of knowledge of v_k and x_k. The proofs can be computed and verified efficiently using Groth-Sahai non-interactive proof systems for bilinear groups [GS08], which is based on a variety of assumptions, in particular, the XDH assumption.

The rest of the setup can be carried out by each authority autonomously:

- (Attribute Public/Secret Key) Authority k proceeds as follows: for each attribute $i \in \{1, \ldots, n_k\}$ it picks $t_{k,i} \in \mathbb{Z}_p$ and computes $T_{k,i} = g_2^{t_{k,i}}$.

Each authority k stores

$$\langle x_k, \{s_{kj}\}_{j \in \{1,\ldots,N\}\backslash\{k\}}, \{t_{k,i}\}_{i \in [1,\ldots,n_k]} \rangle$$

securely as its private key. Finally the system parameters *param* are published as follows:

$$\langle Y = e(g_1, g_2)^{\sum_k v_k}, \{y_k, \{T_{k,i} = g_2^{t_{k,i}}\}_{i \in [1,\ldots,n_k]}\}_{k \in [1,\ldots,N]} \rangle.$$

We remark that $\{y_k\}_{k \in [1,\ldots,N]}$ is only used by the authority but not the users.

Key Issuing To get the key, user u executes the following with each authority k.

1. For $j \in \{1, \ldots, N\}\backslash\{k\}$, user u starts $N-1$ independent invocations of our anonymous key issuing protocol for $g = y_j^{x_k}$, $h = g_1$, $\alpha_k = \delta_{kj} R_{kj}$, $\beta_k = s_{kj}$ and $\gamma_k = \delta_{kj}$ where $R_{kj} \in \mathbb{Z}_p$ is randomly picked by authority k and $\delta_{kj} = 1$ if $k > j$ and -1 otherwise. As a result, user u obtains $D_{kj} = g_1^{R_{kj}} PRF_{kj}(u)$ for $k > j$ or $D_{kj} = g_1^{R_{kj}} / PRF_{kj}(u)$ for $k < j$.
2. Authority k randomly picks a degree d_k polynomial $p_k(\cdot)$ with $p_k(0) = v_k - \sum_{j \in \{1,\ldots,N\}\backslash\{k\}} R_{kj}$.
3. Authority k issues $S_{k,i} = g_1^{p(i)/t_{k,i}}$ for each eligible attribute i for the user.

4. User u computes $D_u = \prod_{(k,j)\in\{1,\ldots,N\}\times(\{1,\ldots,N\}\setminus\{k\})} D_{kj}$. Note that all PRF terms in the above project cancel each other out by the choice of δ_{kj}, we have $D_u = g_1^{R_u}$, where $R_u = \sum_{(k,j)\in\{1,\ldots,N\}\times(\{1,\ldots,N\}\setminus\{k\})} R_{kj}$.

Encryption To encrypt m for attribute set $\mathbb{A}^C = \{\mathbb{A}_1^C, \ldots, \mathbb{A}_N^C\}$, pick $s \in_R \mathbb{Z}_p$, return $\langle E_0 = mY^s, E_1 = g_2^s, \{C_{k,i} = T_{k,i}^s\}_{i\in\mathbb{A}_k^C, \forall k\in[1\ldots N]}\rangle$. (Note that this is identical to the encryption algorithm in [Cha07].

Decryption

1. For each authority $k \in [1, \ldots N]$:
   (a) For any d_k attributes $i \in \mathbb{A}_k^C \cap \mathbb{A}_k^u$, pair up $S_{k,i}$ and $C_{k,i}$, i.e. compute $e(S_{k,i}, C_{k,i}) = e(g_1^{p_k(i)/t_{k,i}}, g_2^{st_{k,i}}) = e(g_1, g_2)^{sp_k(i)}$.
   (b) Interpolate all the values $e(g_1, g_2)^{sp_k(i)}$ to get $P_k = e(g_1, g_2)^{sp_k(0)} = e(g_1, g_2)^{s(v_k - \sum_{j\neq k} R_{kj})}$.
2. Multiply P_k's together to get $Q = e(g_1, g_2)^{s(\sum\{v_k\} - R_u)} = Y^s / e(g_1^{R_u}, g_2^s)$.
3. Compute $e(D_u, E_1) \cdot Q = e(g_1^{R_u}, g_2^s) \cdot Q = Y^s$.
4. Recover m by E_0/Y^s.

7.5 Analysis

7.5.1 Confidentiality

Theorem 7.4. *The construction of N-authority ABE described in Section 7.4 is a $(poly(t), N-1, \epsilon)$-secure multi-authority ABE under the assumption that no t-time algorithm can solve DBDH or q-DDHI with probability ϵ better than $1/2$, where q is polynomial in t.*

The intuition behind our reduction to DBDH problem is as follows: We are given a DBDH problem instance (g_2^a, g_2^b, g_2^c, Z). We choose the secret key share of one honest attribute authority to be something that $\mathcal{S}$ cannot compute (ab). Then decrypting the challenge ciphertext would require computing a function of this value $(e(g_1^{ab}, g_2^c))$. The original Sahai-Waters single authority

scheme [SW05] had techniques for setting up a challenge ciphertext, and for issuing decryption keys for attribute sets that were insufficient to decrypt the challenge. What makes things challenging in the multi-authority case is that the adversary can request decryption keys for sufficient attribute sets from all but one of the authorities. And we do not know a priori which authority that one will be. Thus, we have to set up our parameters so that we can set any of our authorities as the one that corresponds to the uncomputable portion of the master key.

The way we do this in the proof is first to choose at random an authority k^* and form its parameters based on this uncomputable value. If it turns out that this is the authority from which the adversary requests insufficient attributes for user u, then we are all set, and we can simply reuse the Sahai-Waters techniques. If not, we use the fact that, in our scheme, the authority does not give out keys only based on its share of the secret – it also incorporates some pseudorandom values based on the seeds that it shares with other authorities. Thus, we can pretend the challenge values are incorporated in this pseudorandomness. (If only honest parties know the seed of a PRF, then in our reduction we can replace it with any other "random-looking" function.) This of course means that at least one other authority must adjust its pseudorandomness to compensate, and we choose this authority to be one of the other honest authorities from which the adversary does not request sufficient attributes. (The security game guarantees that there must be at least one other such authority.)

The above argument follows when there are at most $N-2$ corrupted authorities. Our selective model makes it easier to analyze the case when $N-1$ authorities are corrupted since the adversary is required to announce which $N-1$ authorities to be corrupted at the very beginning of the game, even before the setup stage. In this case, we just need to set the index k^* to be the honest authority.

Proof. Suppose there exists an adversary that wins the security game as described previously with non-negligible probability ϵ. Then we show how to construct a simulator $\mathcal{S}$ which uses it to solve the DBDH problem – given $g_1 \in \mathbb{G}_1$, $g_2, A_2 = g_2^a, B_2 = g_2^b, C_2 = g_2^c \in \mathbb{G}_2$, it decides whether $Z = e(g_1, g_2)^{abc}$ or $e(g_1, g_2)^R$ for random $R \in \mathbb{Z}_p$. At the beginning, $\mathcal{S}$ receives a list of attribute sets $\{\mathbb{A}_k^C\}$ and a list of corrupted authorities $\mathbb{K}_{corr}$. $\mathcal{S}$ initializes as follows:

- If $|\mathbb{K}_{corr}| \neq N-2$, randomly pick $k^* \in [1, \ldots, N]$.

- Otherwise, set k^* to be the single element in the set $1, \cdots, N \backslash \mathbb{K}_{corr}$.

- **Public key and private key of honest authority** k: Choose random $\beta_{k,i} \in \mathbb{Z}_p$, set $T_{k,i} = g_2^{\beta_{k,i}}$ for $i \in \mathbb{A}_k^u \cap \mathbb{A}_k^C$ and $T_{k,i} = B_2^{\beta_{k,i}}$ for $i \notin \mathbb{A}_k^u \cap \mathbb{A}_k^C$.

  - For $k \neq k^*$, choose random $w_k \in \mathbb{Z}_p$ and implicitly sets $v_k = w_k b$.
  - For authority k^*, choose random w_{k^*} and implicitly sets $v_{k^*} = ab + w_{k^*} b$.

  For each pair of authorities j, k, choose a random PRF seed and a random PRF base to define the pseudorandom function PRF_{kj}.

- **Private key of corrupted authority** k: Choose random $t_{k,i} \in \mathbb{Z}_p$ for all attribute i, and a random master secret key share v_k, the public key is set as $T_{k,i} = g_2^{t_{k,i}}$ for all i accordingly. The corrupt authority must also receive pseudorandom seeds for each other authority j, defining functions PRF_{kj}.

- **Public key of the system**:

$$Y = e(A_1, B_2) e(g_1, g_2^b)^{\sum_{k \notin \mathbb{K}_{corr}} \{w_k\}} e(g_1, g_2)^{\sum_{k \in \mathbb{K}_{corr}} \{v_k\}}$$

Attributes key queries to any corrupted authority can be simulated by the adversary since it has the secret key already. Attributes key queries to an honest authority k for $\mathbb{A}_k^u$ are answered differently depending on whether $k = \hat{k}(u)$, which denotes the first authority the user u (controlled by the adversary $\mathcal{A}$) queried such that $|\mathbb{A}_k^u \cap \mathbb{A}_k^C| < d_k$. In the below description, z_k are different for different users (i.e. z_k should better be denoted by z_k^U and they are user specific).

- $k \neq \hat{k}(u)$: $\mathcal{S}$ sets $p(0) = w_k b + z_k b$ for a random $z_{kj} \in \mathbb{Z}_p$ by choosing a random polynomial ρ such that $\rho(0) = w_k + z_k$ and implicitly setting $p(i) = b\rho(i)$.

  For $i \in \mathbb{A}_k^C$, (i.e. $i \in \mathbb{A}_k^u \cap \mathbb{A}_k^C$), $T_{k,i} = g_2^{\beta_{k,i}}$, so $S_{k,i} = g_1^{b\rho(i)/\beta_{k,i}} = B_1^{\rho(i)/\beta_{k,i}}$.

  For $i \notin \mathbb{A}_k^C$, (i.e. $i \in \mathbb{A}_k^u \backslash \mathbb{A}_k^C$), $T_{k,i} = g_2^{b\beta_{k,i}}$, $S_{k,i} = g_1^{b\rho(i)/b\beta_{k,i}} = g_1^{\rho(i)/\beta_{k,i}}$.

  Since $p(0) = v_k - \sum_{j \in \{1,\ldots,N\} \backslash \{k\}} R_{kj}$, if we let $R = \sum_{j \in \{1,\ldots,N\} \backslash \{k\}} R_{kj}$, this settings mean $\mathcal{S}$ sets $R = -z_k b$ for $k \neq k^*$ or $R = ab - z_{k^*} b$ for $k = k^*$.

To compute the D_{kj} terms, we consider two cases.

If $k \neq k^*$, $\mathcal{S}$ can compute $g_1^{v_k} = B_1^{w_k}$. Likewise, $g_1^R = g_1^{p(0)}/g_1^{v_k} = B_1^{-z_k}$ can be computed. Note that this value is the D_u component that the user u will eventually compute from the D_{kj} terms obtained from the authority k.

In the protocol, authority k issues these D_{kj} terms to the user u instead of a single D_u value. This can be simulated easily. $\mathcal{S}$ randomly picks R'_{kj} for $j \in \{1, \ldots, N\}\backslash\{k\}$ which satisfy $\sum_{j\in\{1,\ldots,N\}\backslash\{k\}} R'_{kj} = -z_k$, implicitly sets each $R_{kj} = bR'_{kj}$ and sets $D_{kj} = B_1^{R'_{kj}} \cdot PRF_{kj}(u)$ for $k > j$ or $B_1^{R'_{kj}}/PRF_{kj}(u)$ otherwise. This is distributed exactly like the output of the honest key generation algorithm.

If $k = k^*$, $\mathcal{S}$ cannot compute $g_1^{v_{k^*}} = g_1^{ab+w_k^*b}$. However, we can still proceed as above. $\mathcal{S}$ will choose random values R'_{kj} such that $\prod_{j\in\{1,\ldots,N\}\backslash\{k\}} R'_{kj} = -z_k$ and set $D_{kj} = B_1^{R'_{kj}} \cdot PRF_{kj}(u)$ or $B_1^{R'_{kj}}/PRF_{kj}(u)$. Now, this is slightly different from the real world, an honest algorithm would compute $\sum R_{kj} = v_k - p(0) = ab - z_{k^*}b$. Here $\sum R_{kj} = -z_{k^*}b$ instead.

However, note that user u eventually computes D_u which is the multiplication of D_{kj} for $(k, j) \in \{1, \ldots, N\} \times(\{1, \ldots, N\}\backslash\{k\})$. It turns out that for authority $\hat{k}(u)$, $\mathcal{S}$ will also compute things slightly incorrectly so that $\sum R_{\hat{k}(u)j}$ is off by ab. Thus, we can interpret $D_{k\hat{k}(u)} = B_1^{R'_{k\hat{k}(u)}} \cdot PRF_{k\hat{k}(u)}$ as $g_1^{R_{k\hat{k}(u)}} \cdot (PRF_{k\hat{k}(u)} \cdot B_1^a)$ to resolve both problems, i.e. implicitly setting $R_{k\hat{k}(u)}$ (the variable) as $-ab + R_{k\hat{k}(u)}b'$ (the value). In this case, we get the correct value for $\sum R_{kj}$. The only inconsistency is that we are using $PRF_{k\hat{k}(u)} \cdot B_1^a$ in place of $PRF_{k\hat{k}(u)}$. However, we will use the same value when computing keys from $\hat{k}(u)$, and thus by pseudorandomness of the PRF, this should be indistinguishable from correctly generated output. Finally, we are still computing all D_{kj} values in the same way in both cases (only changing our interpretation), thus we don't at this point need to know which authority will be $\hat{k}(u)$.

- $k = \hat{k}(u)$: As previously promised, $\mathcal{S}$ should set $p(0) = ab+w_kb+z_kb$ implicitly for a random $z_k \in \mathbb{Z}_p$. To do so, $\mathcal{S}$ first chooses $(d_k - 1)$ random points $r_i \in \mathbb{Z}_p$ and set $p(i) = r_ib$ for $i \in \mathbb{A}_k^C$ (recall that $|\mathbb{A}_k^u \cap \mathbb{A}_k^C| < d_k$). Since $T_{k,i} = g_2^{\beta_{k,i}}$, $S_{k,i} = g_1^{p(i)/\beta_{k,i}} = B_1^{r_i/\beta_{k,i}}$. Under these d_k constraints, p is fully determined.

For other attributes $i \notin \mathbb{A}_k^C$, we can compute $S_{k,i}$ by interpolation. Specifically, since $T_{k,i} = g_2^{b\beta_{k,i}}$,

$$\begin{aligned} & S_{k,i} = g_1^{p(i)/b\beta_{k,i}} \\ = \; & g_1^{(\Delta_0(i)(ab+z_kb+w_kb)+\sum \Delta_j(i)r_jb)/b\beta_{k,i}} \\ = \; & g_1^{(\Delta_0(i)(a+z_k+w_k)+\sum \Delta_j(i)r_j)/\beta_{k,i}} \\ = \; & A_1^{\Delta_0(i)/\beta_{k,i}} g_1^{z_k+w_k \sum \Delta_j(i)r_j/\beta_{k,i}} \end{aligned}$$

where $\Delta_j(i)$ is the Lagrange interpolation coefficient.

For the D_{kj} terms, again we consider two cases.

If $k = k^*$, to compute D_{kj}, R'_{kj} are chosen such that $\sum R'_{kj} = -z_k$. $\mathcal{S}$ implicitly sets $R_{kj} = R'_{kj}b$, then computes $D_{kj} = B_1^{R'_{kj}} PRF_{kj}(u)$ or $D_{kj} = B_1^{R'_{kj}}/PRF_{kj}(u)$. The result is distributed as in the original algorithm.

If $k(= \hat{k}(u)) \neq k^*$, i.e. $\exists k' \neq \hat{k}(u)$ such that $k' = k^*$, it means that when computing $D_{k'\hat{k}(u)}$, we replaced $PRF_{k'k(u)}$ with $PRF_{k'k(u)} * B_1^a$. Thus, we must use the same value here: We choose random $R_{kj'}$ such that $\sum R'_{kj} = z_k$. Then we compute $D_{kj} = B_1^{R'_{kj}} PRF_{kj}(u)$ for all $j \neq k$. Now if we interpret $R_{kk'}$ (the variable) as $ab + R_{kk'}$ (the value), then $D_{kk'} = B_1^{R'_{kk'}}/PRF_{kj}(u) = g_1^{R_{kk'}}/(PRF_{kj}(u)B_1^a)$, which means that it is consistent with the value used by authority k'.

Challenge ciphertext is

$$(m \cdot Z \cdot e(g_1^c, g_2^b)^{\sum \{w_k\}} e(g_1^c, g_2)^{\sum_{k \in \mathbb{K}_{corr}} \{v_k\}}, g_2^c, \{(g_2^c)^{\beta_{k,i}}\}_{i \in \mathbb{A}^C}).$$

If $\mathcal{A}$ **guesses** correctly, $\mathcal{S}$ guesses $Z = e(g_1, g_2)^{abc}$, $Z \in_R \mathbb{G}_T$ otherwise. □

Theorem 7.5. *The construction of N-authority ABE described in Chapter 7.4 is an authority unlinkable ABE when at most $N - 2$ of authorities are corrupted, under the XDH assumption, and the assumption that the underlying 2PC and zero knowledge proofs of knowledge are secure.*

Proof. In Chapter 6.3, we have proven that our anonymous key issuing protocol is a 2PC protocol. Recall that our anonymous key issuing protocol requires that the discrete logarithm between $g_1 = g^{x_j x_k}$ and $h = g_1$ be unknown. This condition is satisfied since a collusion of $N - 2$ AAs

cannot learn the discrete logarithm x_j if the authority j is outside the collusion group. (In this case the colluding parties will only see $y_j = g_1^{x_j}$ and a corresponding zero-knowledge proof of knowledge of x_j.) □

7.5.2 Efficiency

The above construction requires that each authority store $N-1$ seeds and run $N-1$ invocations of our anonymous key issuing protocol for each user. The user in turn has to store $|\mathbb{A}_k^u| + 1$ values for each authority k. The main overhead is on the side of the authority, and even so, it seems a fairly small cost to pay in exchange for guaranteeing security when any $N-1$ out of N authorities are corrupted.

For initial setup, we do not require any explicit distributed key generation (DKG). Thanks to the non-interactive zero-knowledge proof, the number of communication rounds is quite minimal (2 rounds). When compared with the trusted CA approach, the load on the authorities is still somewhat higher in that they must participate in an initial setup phase and communicate with all other authorities. However, it seems unavoidable given that we have no party who is guaranteed to be trusted. Finding an approach that would avoid this limitation, while still providing the strong security guarantees that we consider, is a very interesting problem.

Lin *et al.*'s construction [LCLS08] requires designers to fix a constant m for the system, which directly determines efficiency. The resulting construction is such that any group of $m+1$ colluding users will be able to break security of the encryption.

A detailed comparison among different multi-authority ABE proposals is given in Table 7.1. "Tolerated compromise" refers to the maximum colluding set against which a system remains secure. "DKG instance" refers to the number of invocations of the distributed key generation protocol required among the AAs in the setup stage. "Ciphertext overhead" is defined to be the ciphertext size minus the plaintext size. For a fair comparison with Lin *et al.*'s scheme [LCLS08], since our scheme is secure against polynomially-many users, we suggest m should be much larger than N, since it seems reasonable to assume there are more malicious users than malicious authorities. Our system performs better when $m > N-1$. The efficiency of our scheme compares favorably with that of previous multi-authority ABE schemes, even though we provide

Properties	Chase [Cha07]	Lin *et al.* [LCLS08]	Ours
Tolerated Compromise	0 CA	m users	$(N-1)$ AAs
DKG Instance	0	$m+2$	0
Authority Key Size	$\|\mathbb{A}_k\|+1$	$\|\mathbb{A}_k\|+m+1$	$\|\mathbb{A}_k\|+N$
User Key Size	$\|\mathbb{A}^u\|+1$	$\|\mathbb{A}^u\|$	$\|\mathbb{A}^u\|+1$
Ciphertext Overhead	$\|\mathbb{A}^C\|+1$	$\|\mathbb{A}^C\|$	$\|\mathbb{A}^C\|+1$

Table 7.1: *Comparisons of Different Multi-Authority ABE Proposals*

a stronger security guarantee.

7.6 Extensions

7.6.1 Supporting Large Universe

In our basic construction, the universe of attributes is constrained by the size of the public parameters (specifically $\{T_{k,i}\}$). This contrasts with the large universe model (first introduced in [SW05]), in which the universe of attributes is exponentially large, but public parameter size depends on a fixed maximum on the number of attributes allowed in a ciphertext. That approach also has the advantage that any arbitrary string can be used as an attribute via the use of a collision resistant hash function. A large universe construction was presented in [SW05] and a similar concept has been used in [GPSW06].

Our anonymous key issuing protocol and the removal of the central authority technique can also be applied to the multi-authority version of the large universe and complex access structure construction in [GPSW06]. We highlight five major distinctions of the large universe construction:

1. Functions $\{T_k(i)\} : \mathbb{Z}_p \to \mathbb{G}_1$ are used to replace the group elements $T_{k,i}$ for attribute i of each authority k. $T_k(i)$ is publicly computable.

2. Accordingly, $C_{k,i}$ in the ciphertext is changed from $T_{k,i}^s$ to $T_k(i)^s$.

3. $g_1^{p(i)/t_{k,i}}$ in the user secret key is replaced with $g_1^{p(i)} T_k(i)^r$.

4. Since the randomness r is introduced in the user secret key, g_2^r is also given to "cancel out" r in the decryption.

5. To decrypt a ciphertext, merely computing $e(g_1^{p(0)} \cdot T_k(i)^r, g_2^s)$ results in $e(g_1, g_2)^{sp(0)} \cdot e(T_k(i)^r, g_2^s)$, so the later term should be cancelled out by $e(T_k(i)^s, g_2^r)$.

While the proof of confidentiality in [GPSW06] relies critically on the construction of $T_k(i)$ in the simulation, the key idea of the multi-authority scheme in [Cha07] is that $p(0)$ will be set as the PRF computed on the user's GID, and thus this technique is independent of how $T_k(i)$ is constructed. As hinted at in the intuition provided in the proof of our basic scheme, the crux in our proof for multi-authority ABE is about how to embed an unknown master secret key (which is related to the solution of the hard problem) by taking advantage of the pseudorandom values blinding the user secret key. We can show security by applying the same techniques as in our basic scheme.

Here we present an extension of our basic scheme to support a large universe of attributes. Changes are underlined.

Setup.

- (Attribute Public Key) Let $\mathcal{N} = \{1, \ldots, n+1\}$. Each authority picks $T_{k,i} \in \mathbb{G}_1$ for $i \in \mathcal{N}$. Define $T_k(X) = g_1^{X^n} \prod_{i=1}^{n+1} T_{k,i}^{\Delta_i(X)}$, where $\Delta_i(X)$ is the Lagrange interpolation coefficient with respect to the set of points $\mathcal{N}$.

Key Issuing. For each authority k, user u executes the following

1. For $j \in \{1, \ldots, N\} \backslash \{k\}$, user u starts in $N-1$ independent invocations of our anonymous key issuing protocol to obtain $D_{kj} = g_1^{R_{kj}} PRF_{kj}(u)^{\pm 1}$.

2. Authority k randomly picks a degree d_k polynomial $p_k(\cdot)$ with $p_k(0) = v_k - \sum_{j \in \{1,\ldots,N\} \backslash \{k\}} R_{kj}$.

3. For each attribute x, authority k picks $r_x \in_R \mathbb{Z}_p$ and issues $S_{kx} = g_1^{p(x)} \cdot T_k(x)^{r_x}, S'_{kx} = g_2^{r_x}$.

4. User u computes $D_u = \prod_{(k,j) \in \{1\ldots N\} \times (\{1\ldots N\} \backslash \{k\})} D_{kj}$. It can be easily shown that $D_i == g_1^{R_u}$ where $R_u = \sum_{(k,j) \in \{1\ldots N\} \times (\{1\ldots N\} \backslash \{k\})} R_{kj}$.

Encryption. For attributes $\{\mathbb{A}_1^C, \ldots, \mathbb{A}_N^C\}$, encryption first chooses random $s \in \mathbb{Z}_p$, and return

$$\langle E_0 = mY^s, E_1 = g_2^s, \{C_{kx} = \underline{T_k(x)^s}\}_{x \in \mathbb{A}_k^C, \forall k \in [1 \ldots N]} \rangle, s \in \mathbb{Z}_p.$$

Decryption.

1. For each authority $k \in [1, \ldots N]$:

   (a) For any d_k attributes $x \in \mathbb{A}_k^C \cap \mathbb{A}_k^u$, compute

   $$\begin{aligned} & \underline{e(S_{kx}, E_1)/e(C_{kx}, S'_{kx})} \\ = \; & e(g_1^{p(x)} \cdot T_k(x)^{r_x}, g_2^s)/e(T_k(x)^s, g_2^{r_x}) \\ = \; & e(g_1^{p(x)}, g_2^s)e(T_k(x)^{r_x}, g_2^s)/e(T_k(x)^s, g_2^{r_x}) \\ = \; & e(g_1, g_2)^{sp(x)}. \end{aligned}$$

   (b) Interpolate all these $e(g_1, g_2)^{sp_k(i)}$ to get
   $P_k = e(g_1, g_2)^{sp_k(0)} = e(g_1, g_2)^{s(v_k - \sum_{j \neq k} R_{kj})}$.

2. Multiply P_k's together to get $Q = e(g_1, g_2)^{s(\sum \{v_k\} - R_u)} = Y^s / e(g_1^{R_u}, g_2^s)$.

3. Multiply $e(D_u, E_1) = e(g_1^{R_u}, g_2^s)$ with Q to get Y^s.

4. Recover m by E_0 / Y^s.

7.6.2 Complex Access Structure

Another limitation of our basic construction is that it only supports simple d_k-out-of-n threshold policies, while Goyal *et al.*'s construction [GPSW06] supports a tree access structure. When we consider the tree as a circuit, the interior nodes consist of t-out-of-n gates for arbitrary values of t and n, and each leaf node is associated with an attribute and has value 1 if that attribute is present in a given ciphertext.

This tree is the key idea behind the complex access structure construction. A polynomial p_x is chosen for each node x in the tree. These polynomials are chosen in a top-down manner, starting from the root node r, such that the degree of the polynomial p_x is one less than the threshold value t_x of that node. The value $p_r(0)$ at the root node depends on the AKeyGen algorithm. (In

our case $p_r(0) = v_k - \sum_{j \in \{1,\ldots,N\} \setminus \{k\}} R_{kj}$.) For the other nodes x of the tree, $p_x(0)$ is defined to be $p_{\mathsf{parent}[x]}(\mathsf{index}[x])$ where $\mathsf{parent}[x]$ denotes the parent node of x and $\mathsf{index}[x]$ is merely a distinct number for each node at the same level. Using the same approach as in [Cha07], it is not difficult to see that the same tree-based key-structure can be used in our schemes, simply by changing how the root key $p(0)$ is generated.

7.6.3 Variable Thresholds across Authorities

Our basic construction requires the user to have enough attributes from *every* authority, but we can easily let the encryptor leave out a certain subset of authorities by asking each authority to issue to every user a decryption key corresponding to d_k dummy attributes. In contrast to a normal threshold cryptosystem, here the threshold will only be reduced if the encryptor chooses to do so (by including dummy attributes in the ciphertext attribute set). Thus, each ciphertext may have a different threshold.

Generalizing the above idea, each encryptor can reduce the threshold for a chosen set of authorities to a non-zero value by adjusting the number of dummy variables included for those authorities accordingly. Suppose $dmax$ is the maximum threshold. If the encryptor wanted to require $d' < dmax$ of the attributes, he could encrypt with respect to $(dmax - d')$ dummy attributes in additional to the usual attributes. This does not incur heavy penalty in the efficiency of the system, especially when we have a large universe construction to host the dummy attributes.

The use of dummy variables for flexible threshold policy in the *ciphertext* was suggested in [Cha07]. We note that our scheme also allows flexibility in setting the threshold policy in the *key*, simply due to the fact that our scheme supports different threshold values d_k for different users.

□ End of chapter.

Conclusion

The notion of identity-based encryption (IBE) was proposed as an economical alternative to public-key infrastructures, and it turns out to be very useful in constructing various seemingly unrelated cryptographic primitives. However, IBE is subject to the inherent key escrow problem. Our proposal can be viewed as mitigating the key escrow problem in a new dimension. We propose a new notion of anonymous ciphertext indistinguishability against KGC attacks ($\mathcal{ACI} - \mathcal{KGC}$), which is orthogonal to existing notions like user anonymity. We modified Gentry's IBE to get an $\mathcal{ACI} - \mathcal{KGC}$-secure IBE in the standard model. We propose a new system architecture with an anonymous key issuing (AKI) protocol to protect the confidentiality of the users identities. We hope that future IBE proposals will consider $\mathcal{ACI} - \mathcal{KGC}$ as one of the key properties, and IBE with $\mathcal{ACI} - \mathcal{KGC}$ or AKI protocol will find more applications.

This work opens a new area of research. An immediate problem is to see if a stronger level of security is possible where the adversary is given an access of an embedded-identity decryption oracle. Minimizing the trusted setup assumption and reducing the computational assumption are also two important problems to address. Specifically, our proposal requires that two group generators are generated honestly and requires a non-static assumption for security against malicious users. Other possible research directions include proposing a new security model, perhaps borrowing some elements from the paradigm of password-based key exchange in the sense the "gain" obtained by the adversary from one query can be "limited". Also, our scheme was obtained by modifying existing IBE scheme, it may be interesting to design a new IBE scheme "directly" for anonymous ciphertext indistinguishability.

It is unrealistic to assume there is a single authority which can monitor every single attribute of all users. Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different authorities are responsible for issuing different sets of attributes. The original solution by Chase employs a trusted central authority and the use of a global identifier for each user, which means the confidentiality depends critically on the security of the central authority and the user-privacy depends on the honest behavior of the attribute-authorities. We propose an attribute-based encryption scheme without the trusted authority, and an anonymous key issuing protocol which works for both existing schemes and for our new construction. We hope that our work gives a more practice-oriented attribute based encryption system.

After the research in this thesis has been done, there are two new functional encryption systems which achieve adaptive security in the standard model [LOS+10, OT10]. A natural goal is to make any of these schemes support multi-authority, still with provable security guarantee in the standard model.

Bibliography

[AAB+97] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. *World Wide Web Journal*, 2:241–257, June 1997. (Cited on page 5.)

[AAK+02] Jari Arkko, Tuomas Aura, James Kempf, Vesa-Matti Mäntylä, Pekka Nikander, and Michael Roe. Securing IPv6 Neighbor and Router Discovery. In W. Douglas Maughan and Nitin H. Vaidya, editors, *Workshop on Wireless Security*, pages 77–86. ACM, 2002. (Cited on page 22.)

[ABC+08] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. *J. Cryptology*, 21(3):350–391, 2008. (Cited on page 23, 37, 57.)

[ACF09] Michel Abdalla, Dario Catalano, and Dario Fiore. Verifiable Random Functions from Identity-Based Key Encapsulation. In Joux [Jou09], pages 554–571. (Cited on page 23.)

[AFG+06] Nuttapong Attrapadung, Jun Furukawa, Takeshi Gomi, Goichiro Hanaoka, Hideki Imai, and Rui Zhang. Efficient Identity-Based Encryption with Tight Security Reduction. In David Pointcheval, Yi Mu, and Kefei Chen, editors, *CANS*, volume

4301 of *Lecture Notes in Computer Science*, pages 19–36. Springer, 2006. (Cited on page 16.)

[AGKS05] Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM. In Cramer [Cra05], pages 128–146. (Cited on page 16.)

[AHR05] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Lightweight Encryption for Email. In *USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI 05)*, pages 93–99, Berkeley, CA, USA, 2005. USENIX Association. (Cited on page 21.)

[AI09a] Nuttapong Attrapadung and Hideki Imai. Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes. In *IMA Int. Conf.*, volume 5921 of *LNCS*, pages 278–300, 2009. (Cited on page 21.)

[AI09b] Nuttapong Attrapadung and Hideki Imai. Conjunctive Broadcast and Attribute-Based Encryption. In *Pairing*, volume 5671 of *LNCS*, pages 248–265, 2009. (Cited on page 21.)

[AI09c] Nuttapong Attrapadung and Hideki Imai. Dual-Policy Attribute Based Encryption. In *ACNS*, volume 5536 of *LNCS*, pages 168–185, 2009. (Cited on page 20.)

[APM04] Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*. ACM, 2004. (Cited on page 95, 110.)

[ARMLS06] Sattam S. Al-Riyami, John Malone-Lee, and Nigel P. Smart. Escrow-free Encryption Supporting Cryptographic Workflow. *Int. J. Inf. Sec.*, 5(4):217–229, 2006. (Cited on page 22.)

[ARP03] Sattam S. Al-Riyami and Kenneth G. Paterson. Certificateless Public Key Cryptography. In Laih [Lai03], pages 452–473. (Cited on page 12, 39.)

[AW04] Man Ho Au and Victor K. Wei. ID-based Cryptography from Composite Degree Residuosity. Cryptology ePrint Archive, 04/164, 2004. (Cited on page 19.)

[BB04a] Dan Boneh and Xavier Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In Cachin and Camenisch [CC04], pages 223–238. (Cited on page 17, 18, 43, 49, 56.)

[BB04b] Dan Boneh and Xavier Boyen. Secure Identity Based Encryption Without Random Oracles. In Franklin [Fra04], pages 443–459. (Cited on page 17.)

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In Cramer [Cra05], pages 440–456. (Cited on page 17, 18.)

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short Group Signatures. In Franklin [Fra04], pages 41–55. (Cited on page 28, 37.)

[BCC04] Ernest F. Brickell, Jan Camenisch, and Liqun Chen. Direct Anonymous Attestation. In *ACM Conference on Computer and Communications Security*, pages 132–145, 2004. (Cited on page 69.)

[BCC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable Proofs and Delegatable Anonymous Credentials. In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 108–125. Springer, 2009. (Cited on page 65.)

[BCHK07] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007. (Cited on page 22.)

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and Noninteractive Anonymous Credentials. In Ran Canetti, editor, *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374. Springer, 2008. (Cited on page 52, 53, 55, 56.)

[BCOP04] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption with Keyword Search. In Cachin and Camenisch [CC04], pages 506–522. (Cited on page 19, 23, 57.)

[Bei96] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996. (Cited on page 33.)

[BF01] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001. (Cited on page 16, 43, 45, 49.)

[BF03] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.*, 32(3):586–615, 2003. (Cited on page 27.)

[BGH07] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-Efficient Identity Based Encryption Without Pairings. In *FOCS*, pages 647–657. IEEE Computer Society, 2007. (Cited on page 19.)

[BGK08] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-Based Encryption with Efficient Revocation. In Ning et al. [NSJ08], pages 417–426. (Cited on page 17, 24.)

[BH08] Dan Boneh and Michael Hamburg. Generalized Identity Based and Broadcast Encryption Schemes. In Josef Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 455–470. Springer, 2008. (Cited on page 18.)

[BHS04] Robert W. Bradshaw, Jason E. Holt, and Kent E. Seamons. Concealing Complex Policies with Hidden Credentials. In Atluri et al. [APM04], pages 146–157. (Cited on page 6.)

[BKP09] Rakeshbabu Bobba, Himanshu Khurana, and Manoj Prabhakaran. Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption. In *ESORICS*, volume 5789 of *LNCS*, pages 587–604, 2009. (Cited on page 20.)

[BL06] Rana Barua and Tanja Lange, editors. *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*, volume 4329 of *Lecture Notes in Computer Science*. Springer, 2006. (Cited on page 99, 110.)

[BL07] Ernie Brickell and Jiangtao Li. Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. In *WPES*, pages 21–30, 2007. (Cited on page 69.)

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. *J. Cryptology*, 17(4):297–319, 2004. (Cited on page 26.)

[Bol03] Alexandra Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In Yvo Desmedt, editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2003. (Cited on page 57.)

[Boy07] Xavier Boyen. General *Ad Hoc* Encryption from Exponent Inversion IBE. In Naor [Nao07], pages 394–411. (Cited on page 20.)

[Bra99] Stefan Brands. *Rethinking Public Key Infrastructure and Digital Certificates – Building in Privacy*. PhD thesis, Eindhoven Inst. of Tech. 1999. (Cited on page 61, 63, 69.)

[BSNS05] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. In Vaudenay [Vau05], pages 380–397. (Cited on page 17, 43.)

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society, 2007. (Cited on page 20.)

[BW06] Xavier Boyen and Brent Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In Cynthia Dwork, editor, *CRYPTO*, volume 4117

of *Lecture Notes in Computer Science*, pages 290–307. Springer, 2006. (Cited on page 18, 43, 49.)

[BW07] Dan Boneh and Brent Waters. Conjunctive, Subset, and Range Queries on Encrypted Data. In Vadhan [Vad07], pages 535–554. (Cited on page 18, 20.)

[CC04] Christian Cachin and Jan Camenisch, editors. *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*. Springer, 2004. (Cited on page 94, 95.)

[CC05] Liqun Chen and Zhaohui Cheng. Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. In Nigel P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 442–459. Springer, 2005. (Cited on page 17.)

[CC07] Sherman S.M. Chow and Kim-Kwang Raymond Choo. Strongly-Secure Identity-Based Key Agreement and Anonymous Extension. In Juan A. Garay, Arjen K. Lenstra, Masahiro Mambo, and René Peralta, editors, *ISC*, volume 4779 of *Lecture Notes in Computer Science*, pages 203–220. Springer, 2007. (Cited on page 12.)

[CCKN07] Ling Cheung, Joseph A. Cooley, Roger Khazanand, and Calvin Newport. Collusion-Resistant Group Key Management using Attribute-Based Encryption. In *1st International Workshop on Group-Oriented Cryptographic Protocols*, 2007. (Cited on page 24.)

[Cha06] Denis Charles. On the Existence of Distortion Maps on Ordinary Elliptic Curves. Cryptology ePrint Archive, Report 2006/128, 2006. (Cited on page 27.)

[Cha07] Melissa Chase. Multi-authority Attribute Based Encryption. In Vadhan [Vad07], pages 515–534. (Cited on page 7, 8, 10, 11, 14, 28, 62, 67, 74, 75, 79, 85, 86, 87, 88.)

[Cha08] Melissa Chase. *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications*. PhD thesis, Brown University, 2008. (Cited on page 52, 56.)

[CHK07] Ran Canetti, Shai Halevi, and Jonathan Katz. A Forward-Secure Public-Key Encryption Scheme. *J. Cryptology*, 20(3):265–294, 2007. (Cited on page 19.)

[Cho08] Sherman S. M. Chow. Certificateless Encryption. In Marc Joye and Gregory Neven, editors, *Identity-Based Cryptography*. IOS Press, 2008. (Cited on page 12, 39.)

[CL01] Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In Pfitzmann [Pfi01], pages 93–118. (Cited on page 61, 63.)

[CN07] Ling Cheung and Calvin C. Newport. Provably Secure Ciphertext Policy ABE. In Ning et al. [NdVS07], pages 456–465. (Cited on page 20, 21.)

[Coc01] Clifford Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In Bahram Honary, editor, *IMA Int. Conf.*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, 2001. (Cited on page 19.)

[Cra05] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005. (Cited on page 93, 94, 109, 110.)

[CRR08] Sherman S.M. Chow, Volker Roth, and Eleanor G. Rieffel. General Certificateless Encryption and Timed-Release Encryption. In Ostrovsky et al. [OPV08], pages 126–143. (Cited on page 12, 39.)

[CS05] Sanjit Chatterjee and Palash Sarkar. Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model. In Dongho Won and Seungjoo Kim, editors, *ICISC*, volume 3935 of *Lecture Notes in Computer Science*, pages 424–440. Springer, 2005. (Cited on page 18.)

[CS06a] Sanjit Chatterjee and Palash Sarkar. Generalization of the Selective-ID Security Model for HIBE Protocols. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 241–256. Springer, 2006. (Cited on page 18.)

[CS06b] Sanjit Chatterjee and Palash Sarkar. HIBE With Short Public Parameters Without Random Oracle. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284

of *Lecture Notes in Computer Science*, pages 145–160. Springer, 2006. (Cited on page 18.)

[CS06c] Sanjit Chatterjee and Palash Sarkar. Multi-receiver Identity-Based Key Encapsulation with Shortened Ciphertext. In Barua and Lange [BL06], pages 394–408. (Cited on page 18.)

[CS06d] Sanjit Chatterjee and Palash Sarkar. New Constructions of Constant Size Ciphertext HIBE Without Random Oracle. In Min Surp Rhee and Byoungcheon Lee, editors, *ICISC*, volume 4296 of *Lecture Notes in Computer Science*, pages 310–327. Springer, 2006. (Cited on page 18.)

[DH76a] Whitfield Diffie and Martin E. Hellman. Multiuser Cryptographic Techniques. In *AFIPS '76: Proceedings of the June 7-10, 1976, National Computer Conference and Exposition*, pages 109–112, New York, NY, USA, 1976. ACM. (Cited on page 3.)

[DH76b] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976. (Cited on page 3.)

[DHKT08] Ivan Damgård, Dennis Hofheinz, Eike Kiltz, and Rune Thorbek. Public-Key Encryption with Non-interactive Opening. In Malkin [Mal08], pages 239–255. (Cited on page 23.)

[DKXY02] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. Key-Insulated Public Key Cryptosystems. In Knudsen [Knu02], pages 65–82. (Cited on page 19.)

[DLP08] Alexander W. Dent, Benoît Libert, and Kenneth G. Paterson. Certificateless Encryption Schemes Strongly Secure in the Standard Model. In Ronald Cramer, editor, *Public Key Cryptography*, volume 4939 of *Lecture Notes in Computer Science*, pages 344–359. Springer, 2008. (Cited on page 12, 39.)

[DT07] Ivan Damgård and Rune Thorbek. Non-interactive Proofs for Integer Multiplication. In Naor [Nao07], pages 412–429. (Cited on page 23.)

[DY05] Yevgeniy Dodis and Aleksandr Yampolskiy. A Verifiable Random Function with Short Proofs and Keys. In Vaudenay [Vau05], pages 416–431. (Cited on page 29, 64, 67.)

[EMN+09] Keita Emura, Atsuko Miyaji, Akito Nomura, Kazumasa Omote, and Masakazu Soshi. A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. In *ISPEC*, volume 5451 of *LNCS*, pages 13–23, 2009. (Cited on page 21.)

[FO00] Eiichiro Fujisaki and Tatsuaki Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. *IEICE Trans. Fund.*, E83-9(1):24–32, 2000. (Cited on page 16.)

[Fra04] Matthew K. Franklin, editor. *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*. Springer, 2004. (Cited on page 94.)

[Gal05] David Galindo. Boneh-Franklin Identity Based Encryption Revisited. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP*, volume 3580 of *Lecture Notes in Computer Science*, pages 791–802. Springer, 2005. (Cited on page 16.)

[Gal09] David Galindo. Breaking and Repairing Damgård et al. Public Key Encryption Scheme with Non-interactive Opening. In Marc Fischlin, editor, *CT-RSA*, volume 5473 of *Lecture Notes in Computer Science*, pages 389–398. Springer, 2009. (Cited on page 24.)

[Gam84] Taher El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In *CRYPTO*, pages 10–18, 1984. (Cited on page 4.)

[Gar77] Martin Gardner. Mathematical Games: A New Kind of Cipher that would take Millions of Years to Break. *Scientific American*, 237(2):120–124, August 1977. (Cited on page 4.)

[Gen06] Craig Gentry. Practical Identity-Based Encryption Without Random Oracles. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2006. (Cited on page 9, 12, 18, 29, 46, 47, 49.)

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to Construct Random Functions. *J. ACM*, 33(4):792–807, 1986. (Cited on page 29.)

[GH07] Matthew Green and Susan Hohenberger. Blind Identity-Based Encryption and Simulatable Oblivious Transfer. In Kaoru Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 265–282. Springer, 2007. (Cited on page 23, 56, 57, 58.)

[GHS02] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate Pairing. In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 2002. (Cited on page 26.)

[GJKW07] Eu-Jin Goh, Stanislaw Jarecki, Jonathan Katz, and Nan Wang. Efficient Signature Schemes with Tight Reductions to the Diffie-Hellman Problems. *J. Cryptology*, 20(4):493–514, 2007. (Cited on page 16.)

[GJPS08] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded Ciphertext Policy Attribute Based Encryption. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP (2)*, volume 5126 of *LNCS*, pages 579–591. Springer, 2008. (Cited on page 20.)

[GK06] David Galindo and Eike Kiltz. Chosen-Ciphertext Secure Threshold Identity-Based Key Encapsulation Without Random Oracles. In Roberto De Prisco and Moti Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 173–185. Springer, 2006. (Cited on page 17.)

[GLF+10] David Galindo, Benoît Libert, Marc Fischlin, Georg Fuchsbauer, Anja Lehmann, Mark Manulis, and Dominique Schröder. Public-Key Encryption with Non-Interactive Opening: New Constructions and Stronger Definitions. In Daniel J.

Bernstein and Tanja Lange, editors, *AFRICACRYPT*, volume 6055 of *Lecture Notes in Computer Science*, pages 333–350. Springer, 2010. (Cited on page 24.)

[GLSW08] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-Box Accountable Authority Identity-Based Encryption. In Ning et al. [NSJ08], pages 427–436. (Cited on page 9, 43, 49.)

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1):186–208, 1989. (Cited on page 30.)

[Goy07] Vipul Goyal. Reducing Trust in the PKG in Identity Based Cryptosystems. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 430–447. Springer, 2007. (Cited on page 9, 49.)

[GPR98] Oded Goldreich, Birgit Pfitzmann, and Ronald L. Rivest. Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop. In *CRYPTO*, pages 153–168, 1998. (Cited on page 69.)

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Juels et al. [JWdV06], pages 89–98. (Cited on page 6, 19, 20, 21, 28, 85, 86, 87.)

[GS02] Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002. (Cited on page 17, 38, 43.)

[GS08] Jens Groth and Amit Sahai. Efficient Non-interactive Proof Systems for Bilinear Groups. In Nigel P. Smar, editor, *EUROCRYPT*, volume 4965 of *LNCS*, pages 415–432. Springer, 2008. (Cited on page 78.)

[Gut02] Peter Gutmann. PKI: It's Not Dead, Just Resting. *IEEE Computer*, 35(8):41 – 49, 2002. (Cited on page 5.)

[GW09] Craig Gentry and Brent Waters. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In Joux [Jou09], pages 171–188. (Cited on page 18.)

[HJSNS08] M. Jason Hinek, Shaoquan Jiang, Reihaneh Safavi-Naini, and Siamak Fayyaz Shahandashti. Attribute-Based Encryption with Key Cloning Protection. Cryptology ePrint 2008/478, 2008. (Cited on page 21.)

[HK04] Swee-Huay Heng and Kaoru Kurosawa. k-Resilient Identity-Based Encryption in the Standard Model. In Tatsuaki Okamoto, editor, *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 67–80. Springer, 2004. (Cited on page 19.)

[HL02] Jeremy Horwitz and Ben Lynn. Toward Hierarchical Identity-Based Encryption. In Knudsen [Knu02], pages 466–481. (Cited on page 17, 19.)

[IP08] Malika Izabachène and David Pointcheval. New Anonymity Notions for Identity-Based Encryption. In Ostrovsky et al. [OPV08], pages 375–391. (Cited on page 10, 12, 23, 49.)

[IPN+09] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter H. Hartel, and Willem Jonker. Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application. In *WISA*, volume 5932 of *LNCS*, pages 309–323, 2009. (Cited on page 21.)

[JL09] Stanislaw Jarecki and Xiaomin Liu. Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection. In Omer Reingold, editor, *TCC*, volume 5444 of *LNCS*, pages 577–594. Springer, 2009. (Cited on page 15, 29, 63.)

[Jou09] Antoine Joux, editor. *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*. Springer, 2009. (Cited on page 92, 102.)

[JT09] Stanislaw Jarecki and Gene Tsudik, editors. *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, volume 5443 of *Lecture Notes in Computer Science*. Springer, 2009. (Cited on page 106, 109.)

[JWdV06] Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors. *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*. ACM, 2006. (Cited on page 102, 108.)

[Kha06] Dalia Khader. Public Key Encryption with Keyword Search Based on K-Resilient IBE. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Laganà, Youngsong Mun, and Hyunseung Choo, editors, *ICCSA (3) - ACIS*, volume 3982 of *Lecture Notes in Computer Science*, pages 298–308. Springer, 2006. (Cited on page 19.)

[Kil07] Eike Kiltz. From Selective-ID to Full Security: The Case of the Inversion-Based Boneh-Boyen IBE Scheme. Cryptology ePrint Archive, 07/033, 2007. (Cited on page 17, 18.)

[Knu02] Lars R. Knudsen, editor. *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*. Springer, 2002. (Cited on page 99, 103.)

[Kob87] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987. (Cited on page 4.)

[KSW10] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. *J. Cryptology*, 2010. To appear. (Cited on page 18, 21.)

[KV08] Eike Kiltz and Yevgeniy Vahlis. CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption. In Malkin [Mal08], pages 221–238. (Cited on page 17, 18, 43.)

[Lai03] Chi-Sung Laih, editor. *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings*, volume

2894 of *Lecture Notes in Computer Science*. Springer, 2003. (Cited on page 93, 108.)

[LCLS08] Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao. Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT*, volume 5365 of *LNCS*, pages 426–436. Springer, 2008. (Cited on page 10, 11, 14, 75, 84, 85.)

[LCLX09] Xiaohui Liang, Zhenfu Cao, Huang Lin, and Dongsheng Xing. Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption. In *ASIACCS*, pages 343–352, 2009. (Cited on page 20.)

[LK10] Jin Li and Kwangjo Kim. Hidden Attribute-Based Signatures without Anonymity Revocation. *Information Sciences*, 180(9):1681–1689, 2010. (Cited on page 24.)

[LOS+10] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010. (Cited on page 34, 91.)

[LQ05] Benoît Libert and Jean-Jacques Quisquater. Identity Based Encryption Without Redundancy. In John Ioannidis, Angelos D. Keromytis, and Moti Yung, editors, *ACNS*, volume 3531 of *Lecture Notes in Computer Science*, pages 285–300, 2005. (Cited on page 16, 17.)

[LRSW99] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In *Selected Areas in Cryptography*, pages 184–199, 1999. (Cited on page 69.)

[LRZW09] Jin Li, Kui Ren, Bo Zhu, and Zhiguo Wan. Privacy-Aware Attribute-Based Encryption with User Accountability. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *ISC*, volume 5735 of *Lecture Notes in Computer Science*, pages 347–362. Springer, 2009. (Cited on page 20, 21.)

[LS08] David Lubicz and Thomas Sirvent. Attribute-Based Broadcast Encryption Scheme Made Efficient. In *AFRICACRYPT*, volume 5023 of *LNCS*, pages 325–342, 2008. (Cited on page 21.)

[LV09] Benoît Libert and Damien Vergnaud. Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In Jarecki and Tsudik [JT09], pages 235–255. (Cited on page 18, 49.)

[Lys02] Anna Lysyanskaya. *Signature Schemes and Applications to Cryptographic Protocol Design*. PhD thesis, MIT, 2002. (Cited on page 69.)

[Mal08] Tal Malkin, editor. *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008. Proceedings*, volume 4964 of *Lecture Notes in Computer Science*. Springer, 2008. (Cited on page 99, 104.)

[MBH03] Marco Casassa Mont, Pete Bramhall, and Keith Harrison. A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care. In *DEXA Workshops*, pages 432–437. IEEE Computer Society, 2003. (Cited on page 22.)

[Mer78] Ralph C. Merkle. Secure Communications over Insecure Channels. *Commun. ACM*, 21(4):294–299, 1978. (Cited on page 3.)

[Mil85] Victor S. Miller. Use of Elliptic Curves in Cryptography. In Hugh C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985. (Cited on page 4.)

[MKE09] Sascha Müller, Stefan Katzenbeisser, and Claudia Eckert. On Multi-Authority Ciphertext-Policy Attribute-Based Encryption. *Bulletin of the Korean Mathematical Society*, 46(4), 2009. Journal version of "Distributed Attribute-Based Encryption" appeared in ICISC 2008. (Cited on page 11.)

[MPR08] Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. Cryptology ePrint Archive, Report 2008/328, 2008. (Cited on page 24.)

[Nac07] David Naccache. Secure and Practical Identity-based Encryption. *IET Inf. Sec.*, 1(2):59–64, 2007. (Cited on page 18.)

[Nao07] Moni Naor, editor. *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*, volume 4515 of *Lecture Notes in Computer Science*. Springer, 2007. (Cited on page 96, 99.)

[NdVS07] Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors. *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*. ACM, 2007. (Cited on page 98, 108.)

[NIS94] Digital Signature Standard, May 1994. (Cited on page 4.)

[NPR99] Moni Naor, Benny Pinkas, and Omer Reingold. Distributed Pseudo-random Functions and KDCs. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *LNCS*, pages 327–346. Springer, 1999. (Cited on page 14, 76.)

[NSJ08] Peng Ning, Paul F. Syverson, and Somesh Jha, editors. *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008. (Cited on page 95, 102.)

[NYO08] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *ACNS*, volume 5037 of *LNCS*, pages 111–129, 2008. (Cited on page 20, 21.)

[OPV08] Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, editors. *Security and Cryptography for Networks, 6th International Conference, SCN 2008, Amalfi, Italy,*

September 10-12, 2008. Proceedings, volume 5229 of *Lecture Notes in Computer Science*. Springer, 2008. (Cited on page 98, 103.)

[OSW07] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-Based Encryption with Non-Monotonic Access Structures. In Ning et al. [NdVS07], pages 195–203. (Cited on page 19.)

[OT10] Tatsuaki Okamoto and Katsuyuki Takashima. Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption. In Tal Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010. (Cited on page 34, 91.)

[Pfi01] Birgit Pfitzmann, editor. *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*. Springer, 2001. (Cited on page 98, 110.)

[PP03] Duong Hieu Phan and David Pointcheval. Chosen-Ciphertext Security without Redundancy. In Laih [Lai03], pages 1–18. (Cited on page 16.)

[PTMW06] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In Juels et al. [JWdV06], pages 99–112. (Cited on page 24.)

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. (Cited on page 4.)

[SCH+05] Ai Fen Sui, Sherman S.M. Chow, Lucas Chi Kwong Hui, Siu-Ming Yiu, K. P. Chow, Wai Wan Tsang, C. F. Chong, Kevin K. H. Pun, and H. W. Chan. Separable and Anonymous Identity-Based Key Issuing. In *ICPADS*, pages 275–279. IEEE Computer Society, 2005. (Cited on page 56.)

[SD03] D. K. Smetters and Glenn Durfee. Domain-Based Authentication of Identity-Based Cryptosystems for Secure Email and IPsec. In *USENIX Security Symposium*. USENIX, 2003. (Cited on page 21, 22.)

[Sha79] Adi Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, 1979. (Cited on page 30.)

[Sha84] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO*, pages 47–53. Springer, 1984. (Cited on page 5, 16, 19.)

[SK03] Ryuichi Sakai and Masao Kasahara. ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, 03/054, 2003. (Cited on page 17, 48, 49.)

[SKOS09] Jae Hong Seo, Tetsutaro Kobayashi, Miyako Ohkubo, and Koutarou Suzuki. Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts. In Jarecki and Tsudik [JT09], pages 215–234. (Cited on page 18.)

[Sma03] Nigel P. Smart. Access Control using Pairing Based Cryptography. In Marc Joye, editor, *CT-RSA*, volume 2612 of *LNCS*, pages 111–121. Springer, 2003. (Cited on page 6.)

[SOK01] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on Pairing over Elliptic Curve (in Japanese). In *SCIS 01*, 2001. (Cited on page 16, 43.)

[SW05] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In Cramer [Cra05], pages 457–473. (Cited on page 6, 9, 13, 17, 19, 21, 28, 79, 85.)

[SY08] Guo Shanqing and Zeng Yingpei. Attribute-based Signature Scheme. In *2008 International Conference on Information Security and Assurance*, Los Alamitos, CA, USA, 2008. IEEE Computer Society. (Cited on page 24.)

[TBEM08] Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *NDSS*. The Internet Society, 2008. (Cited on page 24.)

[Vad07] Salil P. Vadhan, editor. *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings*, volume 4392 of *Lecture Notes in Computer Science*. Springer, 2007. (Cited on page 97.)

[Vau05] Serge Vaudenay, editor. *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, volume 3386 of *Lecture Notes in Computer Science*. Springer, 2005. (Cited on page 96, 100.)

[Ver01] Eric R. Verheul. Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems. In Pfitzmann [Pfi01], pages 195–210. (Cited on page 27.)

[Wat05] Brent Waters. Efficient Identity-Based Encryption Without Random Oracles. In Cramer [Cra05], pages 114–127. (Cited on page 9, 17, 18.)

[Wat08] Brent Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Cryptology ePrint Archive, Report 2008/290, 2008. (Cited on page 20.)

[WLCM06] Jian Weng, Shengli Liu, Kefei Chen, and Changshe Ma. Identity-Based Parallel Key-Insulated Encryption Without Random Oracles: Security Notions and Construction. In Barua and Lange [BL06], pages 409–423. (Cited on page 18.)

[Yao82] Andrew Chi-Chih Yao. Protocols for Secure Computations (Extended Abstract). In *FOCS*, pages 160–164. IEEE, 1982. (Cited on page 30.)

[YFDL04] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. ID-based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In Atluri et al. [APM04], pages 354–363. (Cited on page 45.)

[ZI05] Rui Zhang and Hideki Imai. Improvements on Security Proofs of Some Identity Based Encryption Schemes. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *CISC*, volume 3822 of *Lecture Notes in Computer Science*, pages 28–41. Springer, 2005. (Cited on page 17.)

Vita

Sherman was born in Hong Kong when Hong Kong was a British Colony. He grew up there and witnessed the handover of Hong Kong to China. He obtained both of his Bachelor of Engineering degree (First Class Honors in Computer Engineering) and Master of Philosophy degree from the University of Hong Kong. He also obtained his Master of Science degree from New York University.

He has been research interns of Information Sharing Platform Laboratories of NTT Research and Development, Cryptography Group of Microsoft Research (Redmond) and Fuji Xerox Palo Alto Laboratory. He visited the Information Security Institute at Queensland University of Technology as a visiting scholar, funded by the Australia government. He also visited CSAIL at MIT and Department of CS at the University of Texas, Austin in 2009.

Enchanted by its power and variety, cryptography is the area in which Sherman did his PhD training. The beauty of number-theoretic constructs and the resulting resiliencies against digital threat just fascinate him. His research over the past few years has been primarily focused on devising practical yet provably secure cryptographic schemes for the emerging computing paradigms, and for the increasingly complex applications, which involve conflicting requirements, or the collaboration of entities that are mutually untrustful. After all, cryptography is for security and hence security is also his research space.

He has published over 40 papers (some of them with researchers from Australia, China, England, Hong Kong, Malaysia, Singapore, Taiwan, and USA) on the topics of identity-based, attribute-based and certificateless cryptography, pairing-based crpyography, anonymous creden-

tial, two-factor encryption, key agreement, group-oriented signature, privacy-oriented signature, and distributed system security (e.g., e-voting, e-cash, P2P, privacy-preserving queries), which are accepted by major conferences such as CCS, CT-RSA, NDSS, PKC, SAC, SCN, etc.

He is on the program committee of CANS 10, Indocrypt 10, ProvSec 07, its predecessor ACIS 06 (as a program co-chairman), and as reviewers for AsiaCCS 11, CT-RSA 11 (10, 09), Eurocrypt 11 (06), Africacrypt 10, Asiacrypt 10 (09, 05), CCS 10, ICDCS 10, Latincrypt 10, PETS 10, SCN 10, TCC 10 (08), FC 09, ISC 09 (08), FOCS 08, ACISP 08 (07), Crypto 07, ACM E-Commerce 07, Pairing 07, Journal of Cryptology, IEEE Transaction on Information Theory, Designs, Codes and Cryptography, etc.

Published Materials

Most of the results in this thesis have been published in the two following papers:

1. Melissa Chase and **S. Chow**. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption. ***ACM Conference on Computer and Communications Security (CCS) 2009***, p.121-130.

2. **S. Chow**. Removing Escrow from Identity-Based Encryption. ***Public Key Cryptography (PKC) 2009***, volume 5443 of *Lecture Notes in Computer Science*, p.256-276.

Patent Information

The following contribution of this thesis has patents pending:

Description: Anonymous Key Issuing for Attribute-Based Encryption

Inventors: Melissa E. Chase and Sze Ming Chow

Held by: Microsoft Corporation

Filed: January 19, 2009

Current U.S. Class: 713/171

Class at Publication: 713/171

International Class: H04L 9/00 20060101 H04L009/00