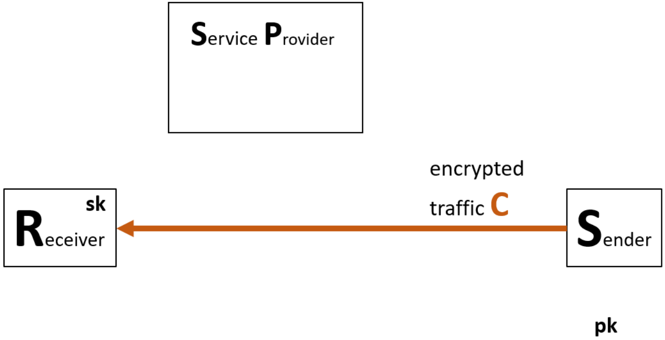
Pattern matching on encrypted streams

Élie Bouscatié Guilhem Castagnos Olivier Sanders

November 29, 2022

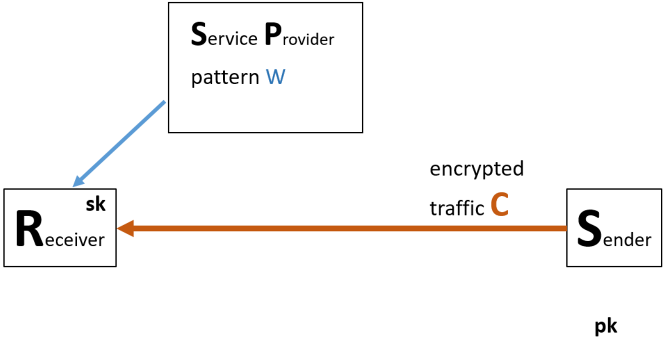
Context

Public key encryption

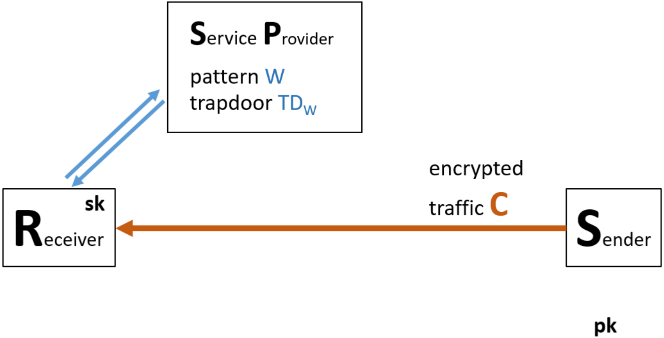


- In 2021, $\sim$ 80-90% of the worldwide internet traffic was encrypted.
- Classical encryption incompatible with functionalities such as Intrusion Detection Systems (IDS).

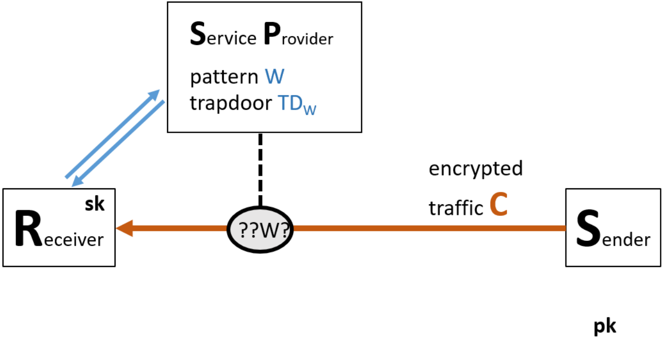
Functional encryption for pattern matching



Functional encryption for pattern matching



Functional encryption for pattern matching



Why pairings

Allow Service Provider to detect virus signatures inside internet traffic with

- minimal leakage
- minimal interactivity
- updating virus signatures
- variable length of virus signatures

Handle arbitrary long messages

Ideal functionality

arbitrary long Encrypted Data:

Banana

From Wikipedia, the free encyclopedia

This article is about bananas generally. For the genus to which banana plants belong, see Musa (genus). For starchier bananas used in cooking, see Cooking banana. For the most common commercial type, see Cavendish banana. For other uses, see Banana (disambiguation).

A banana is an elongated, edible fruit – botanically a berry[1][2] – produced by several kinds of large herbaceous flowering plants in the genus *Musa*.[3] In some countries, bananas used for cooking may be called "plantains", distinguishing them from **dessert bananas**. The fruit is variable in size, color, and firmness, but is usually elongated and curved, with soft flesh rich in starch covered with a rind, which may be green, yellow, red, purple, or brown when ripe. The fruits grow upward in clusters near the top of the plant. Almost all modern edible seedless (parthenocarp) bananas come from two wild species – *Musa acuminata* and *Musa balbisiana*. The scientific names of most cultivated bananas are *Musa acuminata*, *Musa balbisiana*, and *Musa × paradisiaca* for the hybrid *Musa acuminata × M. balbisiana*, depending on their genomic constitution. The old scientific name for this hybrid, *Musa sapientum*, is no longer used.

Musa species are native to tropical Indomalaya and Australia, and are likely to have been first domesticated in Papua New Guinea.[4][5] They are grown in 135 countries,[6] primarily for their fruit, and to a lesser extent to make fiber, banana wine, and banana beer and as ornamental plants. The world's largest producers of bananas in 2017 were India and China, which together accounted for approximately 38% of total production.[7]

Worldwide, there is no sharp distinction between "bananas" and "plantains". Especially in the Americas and Europe, "banana" usually refers to soft, sweet, dessert bananas, particularly those of the Cavendish group, which are the main exports from banana-growing countries. By contrast, *Musa* cultivars with firmer, starchier fruit are called "plantains". In other regions, such as Southeast Asia, many more kinds of banana are grown and eaten, so the binary distinction is not as useful and is not made in local languages.

Banana

Peeled, whole, and longitudinal section

Scientific classification	
Kingdom:	Plantae
(unranked):	Angiosperms
(unranked):	Monocots
(unranked):	Commelinids
Order:	Zingiberales
Family:	Musaceae
Genus:	Musa

Service Provider's view with trapdoor for **banana**:

positions of all occurrences 1, 12, 33, 57,...

Ideal functionality

arbitrary long Encrypted Data:

Banana

From Wikipedia, the free encyclopedia

This article is about bananas generally. For the genus to which banana plants belong, see Musa (genus). For starchier bananas used in cooking, see Cooking banana. For the most common commercial type, see Cavendish banana. For other uses, see Banana (disambiguation).

A **banana** is an elongated, edible fruit – botanically a berry[1][2] – produced by several kinds of large herbaceous flowering plants in the genus *Musa*.[3] In some countries, bananas used for cooking may be called "plantains", distinguishing them from **dessert bananas**. The fruit is variable in size, color, and firmness, but is usually elongated and curved, with soft flesh rich in starch covered with a rind, which may be green, yellow, red, purple, or brown when ripe. The fruits grow upward in clusters near the top of the plant. Almost all modern edible seedless (parthenocarp) bananas come from two wild species – *Musa acuminata* and *Musa balbisiana*. The scientific names of most cultivated bananas are *Musa acuminata*, *Musa balbisiana*, and *Musa* × *paradisiaca* for the hybrid *Musa acuminata* × *M. balbisiana*, depending on their genomic constitution. The old scientific name for this hybrid, *Musa sapientum*, is no longer used.

Musa species are native to tropical Indomalaya and Australia, and are likely to have been first domesticated in Papua New Guinea.[4][5] They are grown in 135 countries,[6] primarily for their fruit, and to a lesser extent to make fiber, banana wine, and banana beer and as ornamental plants. The world's largest producers of bananas in 2017 were India and China, which together accounted for approximately 38% of total production.[7]

Worldwide, there is no sharp distinction between "bananas" and "plantains". Especially in the Americas and Europe, "banana" usually refers to soft, sweet, dessert bananas, particularly those of the Cavendish group, which are the main exports from banana-growing countries. By contrast, *Musa* cultivars with firmer, starchier fruit are called "plantains". In other regions, such as Southeast Asia, many more kinds of banana are grown and eaten, so the binary distinction is not as useful and is not made in local languages.

Banana

Peeled, whole, and longitudinal section

Scientific classification	
Kingdom:	Plantae
(unranked):	Angiosperms
(unranked):	Monocots
(unranked):	Commelinids
Order:	Zingiberales
Family:	Musaceae
Genus:	Musa

Service Provider's view with trapdoor for **cholesterol**:

positions of all occurrences none

Existing functionality: HVE

bounded length Encrypted Data:

A steamboat is a bo at that is propelled primarily by...

Test **unique position** with $\mathbf{td}_{\mathit{boat},3}$: no

Search **all occurrences** in **bounded length** encryption

bounded length Encrypted Data:

A steamboat is a bo at that is propelled primarily by...

Give $\mathbf{td}_{boat,1}, \mathbf{td}_{boat,2}, \mathbf{td}_{boat,3}, \mathbf{td}_{boat,4}, \ldots, \mathbf{td}_{boat,15}$.

Search all occurrences in arbitrary long encryption

Difficulties

- length of public key **bounds** encryption length
- one trapdoor element **by position**

Search all occurrences in arbitrary long encryption

Difficulties

- length of public key **bounds** encryption length
- one trapdoor element **by position**

Results

- Okamoto, Takashima 2011
  $\rightarrow$ unbounded HVE

Search all occurrences in arbitrary long encryption

Difficulties

- length of public key **bounds** encryption length
- one trapdoor element **by position**

Results

- Okamoto, Takashima 2011
  $\rightarrow$ unbounded HVE
- Desmoulins, Fouque, Onete, Sanders 2018
  $\rightarrow$ shiftable trapdoors in bounded HVE.

Search all occurrences in arbitrary long encryption

Difficulties

- length of public key **bounds** encryption length
- one trapdoor element **by position**

Results

- Okamoto, Takashima 2011
  $\rightarrow$ unbounded HVE
- Desmoulins, Fouque, Onete, Sanders 2018
  $\rightarrow$ shiftable trapdoors in bounded HVE.

$>$INCOMPATIBLE

Fragmentation [AC20, Bkakria et al.]

bounded HVE:

A steamboat is a bo at that is propelled primarily by steam

Give $\mathbf{td}_{boat,1}, \mathbf{td}_{boat,2}, \mathbf{td}_{boat,3}, \mathbf{td}_{boat,4}, ..., \mathbf{td}_{boat,15}$.

= "Stream Encryption supporting Pattern Matching" (SEPM)

Fragmentation [AC20, Bkakria et al.]

Naive fragmentation:

A steamboat is a bo	at that is propell	ed primarily by steam

Give $\mathbf{td}_{boat,1}, \mathbf{td}_{boat,2}, \mathbf{td}_{boat,3}, \mathbf{td}_{boat,4}, \ldots, \mathbf{td}_{boat,15}$.

= "Stream Encryption supporting Pattern Matching" (SEPM)

Fragmentation [AC20, Bkakria et al.]

Tiled fragmentation:

A steamboat is a bo	at that is propell	ed primarily by steam
	at is a boat that is	proppelled primar

Give $\mathbf{td}_{boat,1}, \mathbf{td}_{boat,2}, \mathbf{td}_{boat,3}, \mathbf{td}_{boat,4}, \ldots, \mathbf{td}_{boat,15}$.

= "Stream Encryption supporting Pattern Matching" (SEPM)

Fragmentation [AC20, Bkakria et al.]

Tiled fragmentation:

A steamboat is a bo	at that is propell	ed primarily by steam

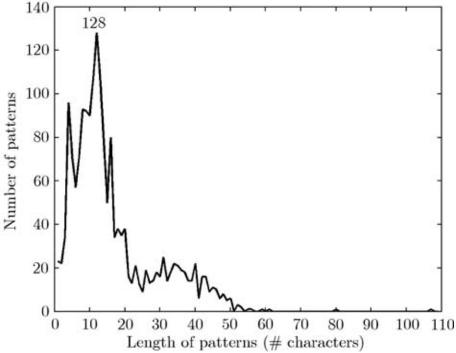
at is a boat that is	proppelled primar

Give $\mathbf{td}_{boat,1}, \mathbf{td}_{boat,2}, \mathbf{td}_{boat,3}, \mathbf{td}_{boat,4}, \ldots, \mathbf{td}_{boat,15}$.

Search all occurrences of bounded substrings in arbitrary long encryption = "Stream Encryption supporting Pattern Matching" (SEPM)

Example of pattern distribution

- Snort pattern length distribution (based on version 2.3.3)[1]
  Total number of patterns = 1785, Maximum length = 107 bytestrings



- Search many patterns of varying short sizes in arbitrary long streams.

[1] Song et al., A parameterized multilevel pattern matching architecture on FPGAs for network intrusion detection and prevention. Sci. China Ser. F-Inf. Sci. 52, 949–963 (2009).

Build an HVE

Type 3 bilinear groups

- $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ of prime order p with a map, called pairing,

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

Type 3 bilinear groups

- $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ of prime order p with a map, called pairing,

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

- Bilinear: for any $g \in \mathbb{G}_1, \widetilde{g} \in \mathbb{G}_2$, and $a, b \in \mathbb{F}_p$,

$$e(g^a, \widetilde{g}^b) = e(g, \widetilde{g})^{ab}$$

Trapdoors for DDH

Let $g \xleftarrow{\$} \mathbb{G}_1$ and $\widetilde{g} \xleftarrow{\$} \mathbb{G}_2$ be public.

- (**DDH**) Knowing $g^{a}, g^{x} \xleftarrow{\$} \mathbb{G}_1$,
  it is **hard** to distinguish $\zeta_0 = g^{ax}$ from $\zeta_1 \xleftarrow{\$} \mathbb{G}_1$.

Trapdoors for DDH

Let $g \xleftarrow{\$} \mathbb{G}_1$ and $\widetilde{g} \xleftarrow{\$} \mathbb{G}_2$ be public.

- (**DDH**) Knowing $g^a, g^x \xleftarrow{\$} \mathbb{G}_1$,
  it is **hard** to distinguish $\zeta_0 = g^{ax}$ from $\zeta_1 \xleftarrow{\$} \mathbb{G}_1$.
- (Trapdoor) With $\widetilde{g}^x$, it becomes **easy**:

$$e(g^a, \widetilde{g}^x) = e(g, \widetilde{g})^{ax} = e(g^{ax}, \widetilde{g}) \quad \textbf{but} \quad e(\zeta_1, \widetilde{g}) \text{ is random.}$$

Trapdoors for DDH

Let $g \xleftarrow{\$} \mathbb{G}_1$ and $\widetilde{g} \xleftarrow{\$} \mathbb{G}_2$ be public.

- (**DDH**) Knowing $g^{a}, g^{x} \xleftarrow{\$} \mathbb{G}_1$,
  it is **hard** to distinguish $\zeta_0 = g^{ax}$ from $\zeta_1 \xleftarrow{\$} \mathbb{G}_1$.
- (Trapdoor) With $\widetilde{g}^{x}$, it becomes **easy**:

$$e(g^{a}, \widetilde{g}^{x}) = e(g, \widetilde{g})^{ax} = e(g^{ax}, \widetilde{g}) \quad \textbf{but} \quad e(\zeta_1, \widetilde{g}) \text{ is random.}$$

- (Mirror elements) In **type 3** bilinear groups, it is hard to compute $\widetilde{g}^{x}$ from g^{x}.

Trapdoors for DDH

Let $g \xleftarrow{\$} \mathbb{G}_1$ and $\widetilde{g} \xleftarrow{\$} \mathbb{G}_2$ be public.

- (**DDH**) Knowing $g^{a}, g^{x} \xleftarrow{\$} \mathbb{G}_1$, it is **hard** to distinguish $\zeta_0 = g^{ax}$ from $\zeta_1 \xleftarrow{\$} \mathbb{G}_1$.
- (Trapdoor) With $\widetilde{g}^{x}$, it becomes **easy**:

$$e(g^{a}, \widetilde{g}^{x}) = e(g, \widetilde{g})^{ax} = e(g^{ax}, \widetilde{g}) \quad \textbf{but} \quad e(\zeta_1, \widetilde{g}) \text{ is random.}$$

- (Mirror elements) In **type 3** bilinear groups, it is hard to compute $\widetilde{g}^{x}$ from g^{x}.
- (Randomness on trapdoors) With some $\widetilde{g}^{s}$ and $\widetilde{g}^{sx}$:

$$e(g^{ax}, \widetilde{g}^{s}) = e(g, \widetilde{g})^{sax} = e(g^{a}, \widetilde{g}^{sx})$$

$\rightarrow$ *This will allow the Receiver to issue non-malleable trapdoors.*

Simple HVE

- **sk** is a random map

$$\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$$
$$(\ \sigma\ \ ,\ \ i\ ) \mapsto \alpha(\sigma, i)$$

Simple HVE

- **sk** is a random map
  $\alpha \colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$

- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$

Simple HVE

- **sk** is a random map
  $\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\ \sigma\ \ ,\ \ i\ ) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

s t e a m

Simple HVE

- **sk** is a random map
  $\alpha \colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\ \sigma \quad , \quad i\ ) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s t e a m

Simple HVE

- **sk** is a random map
  $\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\ \sigma\ ,\ i\ ) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s t e a m

C_0
$=$
g^a

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s t e a m

$C_0 = g^a$

$C_1 = (g^{\alpha(s,1)})^a$

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- $\textbf{pk} = \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s t e a m

$C_0 = g^a$ $C_1 = (g^{\alpha(s,1)})^a$ $C_2 = (g^{\alpha(t,2)})^a$

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\ \sigma \quad , \quad i\ ) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$
g^a	$(g^{\alpha(s,1)})^a$	$(g^{\alpha(t,2)})^a$	$(g^{\alpha(e,3)})^a$	$(g^{\alpha(a,4)})^a$	$(g^{\alpha(m,5)})^a$

Simple HVE

- **sk** is a random map
  $\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$
g^a	$(g^{\alpha(s,1)})^a$	$(g^{\alpha(t,2)})^a$	$(g^{\alpha(e,3)})^a$	$(g^{\alpha(a,4)})^a$	$(g^{\alpha(m,5)})^a$

- Trapdoor with **sk**

$$\mathbf{td}_{tea,2} = \{\alpha(t, 2), \alpha(e, 3), \alpha(a, 4)\}$$

Simple HVE

- **sk** is a random map
  $\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\ \sigma \ \ ,\ \ i\ ) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\Vert$	$\Vert$	$\Vert$	$\Vert$	$\Vert$	$\Vert$
g^a	$(g^{\alpha(\mathsf{s},1)})^a$	$(g^{\alpha(\mathsf{t},2)})^a$	$(g^{\alpha(\mathsf{e},3)})^a$	$(g^{\alpha(\mathsf{a},4)})^a$	$(g^{\alpha(\mathsf{m},5)})^a$

- Trapdoor with **sk**

$$\mathbf{td}_{\mathsf{tea},2} = \alpha(\mathsf{t}, 2) + \alpha(\mathsf{e}, 3) + \alpha(\mathsf{a}, 4)$$

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$
g^a	$(g^{\alpha(\mathsf{s},1)})^a$	$(g^{\alpha(\mathsf{t},2)})^a$	$(g^{\alpha(\mathsf{e},3)})^a$	$(g^{\alpha(\mathsf{a},4)})^a$	$(g^{\alpha(\mathsf{m},5)})^a$

- Trapdoor with **sk**

$$s \xleftarrow{\$} \mathbb{F}_p \qquad \mathbf{td}_{\mathsf{tea},2} = s[\alpha(\mathsf{t}, 2) + \alpha(\mathsf{e}, 3) + \alpha(\mathsf{a}, 4)]$$

Simple HVE

- **sk** is a random map
  $\alpha\colon \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \overset{\$}{\leftarrow} \mathbb{F}_p$ s t e a m

$$C_0 = g^a \quad C_1 = (g^{\alpha(s,1)})^a \quad C_2 = (g^{\alpha(t,2)})^a \quad C_3 = (g^{\alpha(e,3)})^a \quad C_4 = (g^{\alpha(a,4)})^a \quad C_5 = (g^{\alpha(m,5)})^a$$

- Trapdoor with **sk**

$s \overset{\$}{\leftarrow} \mathbb{F}_p$

$$\mathbf{td}_{tea,2} = \{ T = \widetilde{g}^s, T' = (\widetilde{g}^{\alpha(t,2)+\alpha(e,3)+\alpha(a,4)})^s \}$$

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma, i) \mapsto \alpha(\sigma, i)$
- $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$$a \xleftarrow{\$} \mathbb{F}_p \quad \mathsf{s} \quad \mathsf{t} \quad \mathsf{e} \quad \mathsf{a} \quad \mathsf{m}$$

$$C_0 = g^a, \quad C_1 = (g^{\alpha(\mathsf{s},1)})^a, \quad C_2 = (g^{\alpha(\mathsf{t},2)})^a, \quad C_3 = (g^{\alpha(\mathsf{e},3)})^a, \quad C_4 = (g^{\alpha(\mathsf{a},4)})^a, \quad C_5 = (g^{\alpha(\mathsf{m},5)})^a$$

- Trapdoor with **sk**

$$s \xleftarrow{\$} \mathbb{F}_p \qquad \mathbf{td}_{\mathsf{tea},2} = \{T = \tilde{g}^s, T' = (\tilde{g}^{\alpha(\mathsf{t},2)+\alpha(\mathsf{e},3)+\alpha(\mathsf{a},4)})^s\}$$

- Test

$$\prod_{i=2}^{4} C_i \qquad T'$$

Simple HVE

- **sk** is a random map
  $\alpha : \Sigma \times [\![1, n]\!] \to \mathbb{F}_p$
  $(\sigma , i) \mapsto \alpha(\sigma, i)$
- **pk** $= \{g^{\alpha(\sigma,i)}\}_{\sigma,i}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$

	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$
g^a	$(g^{\alpha(\mathsf{s},1)})^a$	$(g^{\alpha(\mathsf{t},2)})^a$	$(g^{\alpha(\mathsf{e},3)})^a$	$(g^{\alpha(\mathsf{a},4)})^a$	$(g^{\alpha(\mathsf{m},5)})^a$

- Trapdoor with **sk**

$s \xleftarrow{\$} \mathbb{F}_p \qquad \mathbf{td}_{\mathsf{tea},2} = \{T = \tilde{g}^s, T' = (\tilde{g}^{\alpha(\mathsf{t},2)+\alpha(\mathsf{e},3)+\alpha(\mathsf{a},4)})^s\}$

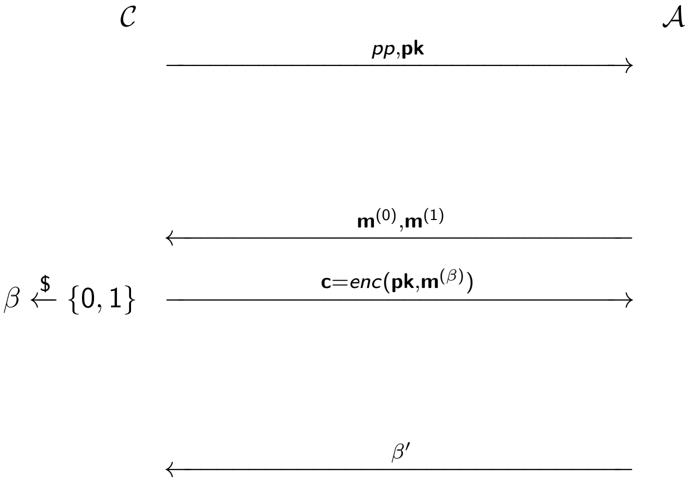
- Test

$$e\Big(\prod_{i=2}^{4} C_i, T\Big) = e(C_0, T')$$

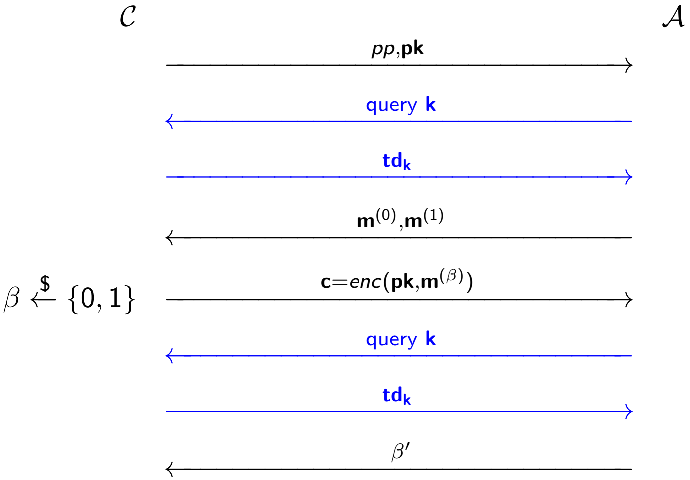
Match!

Prove security

IND-CPA for public key encryption

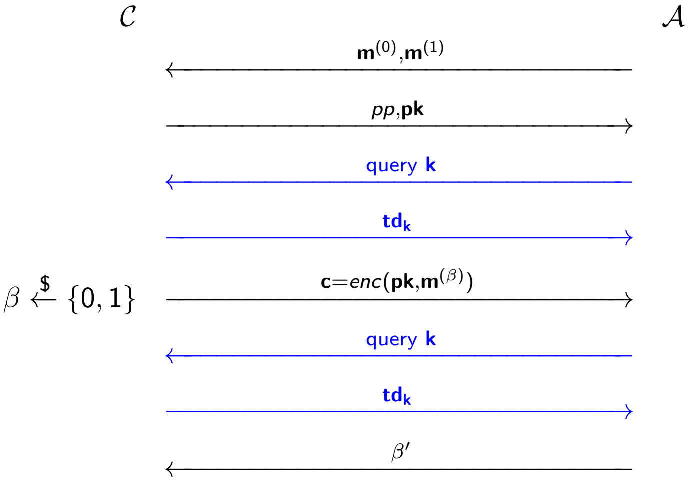


IND-CPA for functional encryption



each **k** must match **neither** or **both** $\mathbf{m}^{(0)}$ and $\mathbf{m}^{(1)}$.

selective IND-CPA for functional encryption

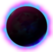


each **k** must match **neither** or **both** $\mathbf{m}^{(0)}$ and $\mathbf{m}^{(1)}$.

Simulation

- challenge messages
  $\mathbf{m}^{(0)} = \text{paysages}$
  $\mathbf{m}^{(1)} = \text{passages}$
- public key
  $\alpha(\sigma, i) \xleftarrow{\$} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$
- challenge ciphertext
  $a \xleftarrow{\$} \mathbb{F}_p, g^a \ (g^{\alpha(\text{p},1)})^a, (g^{\alpha(\text{a},2)})^a, (g^{\alpha(\text{s},3)})^a, (g^{\alpha(\text{s},4)})^a, \ldots$

Simulation

- DDH challenge $g^a, g^x,$  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \xleftarrow{\$} \mathbb{F}_p,\ \mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$
- challenge ciphertext
  $a \xleftarrow{\$} \mathbb{F}_p, g^a\ (g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a, (g^{\alpha(\mathsf{s},3)})^a, (g^{\alpha(\mathsf{s},4)})^a, \ldots$

Simulation

- DDH challenge $g^a, g^x,$  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \xleftarrow{\$} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$ except $g^{\alpha(\mathsf{s},3)} = g^x$
- challenge ciphertext
  $a \xleftarrow{\$} \mathbb{F}_p, g^a \; (g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a, (g^{\alpha(\mathsf{s},3)})^a, (g^{\alpha(\mathsf{s},4)})^a, \ldots$

Simulation

- DDH challenge $g^a, g^x,$  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \overset{\$}{\leftarrow} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$ except $g^{\alpha(\mathsf{s},3)} = g^x$
- challenge ciphertext
  $g^a \ (g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a, (g^{\alpha(\mathsf{s},3)})^a, (g^{\alpha(\mathsf{s},4)})^a, \ldots$

Simulation

- DDH challenge g^a, g^x,  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \stackrel{\$}{\leftarrow} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$ except $g^{\alpha(\mathsf{s},3)} = g^x$
- challenge ciphertext

  g^a $(g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a,$  $, (g^{\alpha(\mathsf{s},4)})^a, \dots$

Simulation

- DDH challenge $g^a, g^x,$  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \xleftarrow{\$} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$ except $g^{\alpha(\mathsf{s},3)} = g^x$
- challenge ciphertext
  $g^a \; (g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a,$  $, (g^{\alpha(\mathsf{s},4)})^a, \ldots$
- answer trapdoor queries
  invalid (pass, 1)
  valid (sage, 4), (soup, 2), (pasta, 1)

Simulation

- DDH challenge g^a, g^x,  $= g^{ax}$ or random
- challenge messages
  $\mathbf{m}^{(0)} =$ paysages
  $\mathbf{m}^{(1)} =$ passages
- public key
  $\alpha(\sigma, i) \xleftarrow{\$} \mathbb{F}_p$, $\mathbf{pk} = \{g^{\alpha(\sigma,i)}\}$ except $g^{\alpha(\mathsf{s},3)} = g^x$
- challenge ciphertext
  $g^a \ (g^{\alpha(\mathsf{p},1)})^a, (g^{\alpha(\mathsf{a},2)})^a$,  $, (g^{\alpha(\mathsf{s},4)})^a, \ldots$
- answer trapdoor queries
  invalid (pass, 1)
  valid (sage, 4), (soup, 2), (pasta, 1) but $\widetilde{g}^x$ breaks DDH.

We succed with **EXDH: Given**: g^a, g^b, g^{ab}, g^c and $\widetilde{g}^a, \widetilde{g}^b$

Distinguish: g^{abc} from $h \xleftarrow{\$} \mathbb{G}_1$

Lighter public key

$$\text{secret: } \{x_i, y_i \xleftarrow{\$} \mathbb{F}_p\}_i$$
$$\text{public: } \Sigma \subset \mathbb{F}_p$$

$$\begin{aligned} \alpha\colon \Sigma \times [\![1, n]\!] &\to \mathbb{F}_p \\ (\ \sigma \quad , \quad i\ ) &\mapsto x_i + y_i.\sigma \end{aligned}$$

$\downarrow$

$|\mathbf{pk}|$ = constant in the size of the alphabet

Lighter public key

- **sk** $= \{x_i, y_i \xleftarrow{\$} \mathbb{F}_p\}_{1 \le i \le n}$
- **pk** $= \{g^{x_i}, g^{y_i}\}_{1 \le i \le n}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s   t   e   a   m

C_0	C_1	C_2	C_3	C_4	C_5
$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$
g^{a}	$(g^{x_1}(g^{y_1})^{\mathsf{s}})^{a}$	$(g^{x_2}(g^{y_2})^{\mathsf{t}})^{a}$	$(g^{x_3}(g^{y_3})^{\mathsf{e}})^{a}$	$(g^{x_4}(g^{y_4})^{\mathsf{a}})^{a}$	$(g^{x_5}(g^{y_5})^{\mathsf{m}})^{a}$

Lighter public key

- $\textbf{sk} = \{x_i, y_i \xleftarrow{\$} \mathbb{F}_p\}_{1 \leq i \leq n}$
- $\textbf{pk} = \{g^{x_i}, g^{y_i}\}_{1 \leq i \leq n}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$
g^a	$(g^{x_1 + y_1 \mathsf{s}})^a$	$(g^{x_2 + y_2 \mathsf{t}})^a$	$(g^{x_3 + y_3 \mathsf{e}})^a$	$(g^{x_4 + y_4 \mathsf{a}})^a$	$(g^{x_5 + y_5 \mathsf{m}})^a$

Lighter HVE

- $\mathbf{sk} = \{x_i, y_i, z_i \xleftarrow{\$} \mathbb{F}_p\}_{1 \leq i \leq n}$
- $\mathbf{pk} = \{g^{x_i}, g^{y_i}, g^{z_i}\}_{1 \leq i \leq n}$
- Encryption with **pk**

$a \xleftarrow{\$} \mathbb{F}_p$ s t e a m

	s	t	e	a	m
C_0	C_1	C_2	C_3	C_4	C_5
$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$
g^a	$(g^{x_1 + y_1 \mathrm{s}})^a$	$(g^{x_2 + y_2 \mathrm{t}})^a$	$(g^{x_3 + y_3 \mathrm{e}})^a$	$(g^{x_4 + y_4 \mathrm{a}})^a$	$(g^{x_5 + y_5 \mathrm{m}})^a$
	$(g^{z_1})^a$	$(g^{z_2})^a$	$(g^{z_3})^a$	$(g^{z_4})^a$	$(g^{z^5})^a$
	$\|\|$	$\|\|$	$\|\|$	$\|\|$	$\|\|$
	C'_1	C'_2	C'_3	C'_4	C'_5

- Trapdoor with **sk**

$$s_1, s_2 \xleftarrow{\$} \mathbb{F}_p \quad \mathbf{td_m} = \{ T_1 = \tilde{g}^{s_1}, \{ T_2 = \tilde{g}^{s_2}, T' = \tilde{g}^{s_1 \sum (x_i + y_i m_i) + s_2 \sum z_i} \}$$

- Test

$$e\left(\prod_{i=2}^{4} C_i, T_1\right) e\left(\prod_{i=2}^{4} C'_i, T_2\right) = e(C_0, T')$$

Inner Product Encryption

Test if $<$ message vector, trapdoor vector $>= 0$.

- stronger security notion (adaptivity)
- weaker assumptions (DLIN)
- can be used as HVE scheme

Converting IPE schemes

	Existing SEPM schemes			New SEPM schemes built by conversions			
	[BCC20, 3]	[BCS21, 4.3]	[BCS21, 4.4]	[DIP13]	[OT12a, 4.2]	[OT12a, 4.2]	[CGW18, 3.4]
IPE→HVE					Fig. 2	Fig. 4	Fig. 2
HVE→SEPM				Fig. 1	Fig. 1	Fig. 1	Fig. 1
PK	$2d \cdot \lvert\Sigma\rvert$	$4d$	$6d$	$2d \cdot \lvert\Sigma\rvert$	$64d^2$	$16d^2$	$40d$
CT	4	2	4	2	16	8	20
$SK_{\mathbf{k}}$	2	2	3	$len(\mathbf{k})$	$16d$	$8d$	8
TEST	2	2	3	$len(\mathbf{k})$	$16d$	$8d$	8
Group Order	Prime	Prime	Prime	Composite	Prime	Prime	Prime
Security	Selective	Selective	Selective	**Adaptive**	**Adaptive**	**Adaptive**	**Adaptive**
Assumption	i-GDH	i-GDH	EXDH	CSD, CDDH	**DLIN**	**DLIN**	**DLIN**