Practical Fully Secure Inner Product Functional Encryption modulo p

Guilhem Castagnos[1] Fabien Laguillaumie[2] Ida Tucker[2]

[1]Université de Bordeaux, INRIA, CNRS, IMB UMR 5251,
F-33405 Talence, France.

[2]Univ Lyon, CNRS, Université Claude Bernard Lyon 1, ENS de Lyon,
INRIA, LIP UMR 5668, F-69007, LYON Cedex 07, France.

Table of contents

Functional Encryption (FE)

Functional Encryption [BSW11]

Alice

m

Auth.

Setup

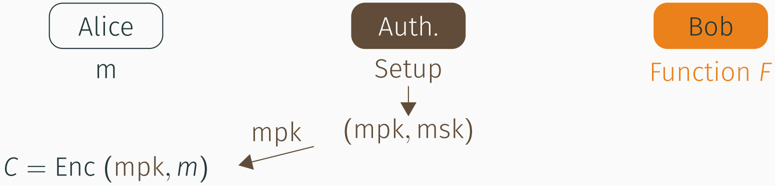
↓

(mpk, msk)

Bob

Function F

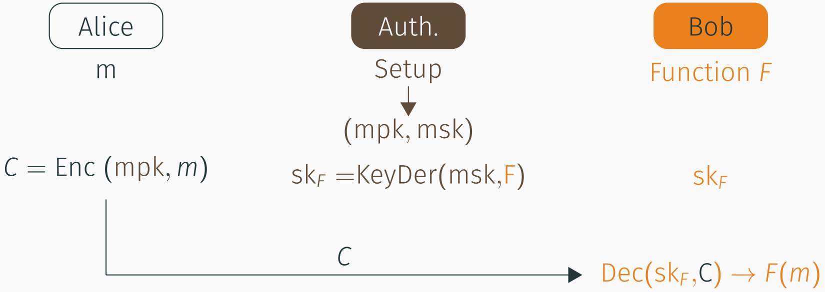
Functional Encryption [BSW11]



Functional Encryption [BSW11]

Alice	Auth.	Bob
m	Setup	Function F
	$\downarrow$ (mpk, msk)
$C = \text{Enc}(\text{mpk}, m)$	$\text{sk}_F = \text{KeyDer}(\text{msk}, F)$ $\xleftarrow{F}$ $\xrightarrow{\text{sk}_F}$	sk_F

Functional Encryption [BSW11]

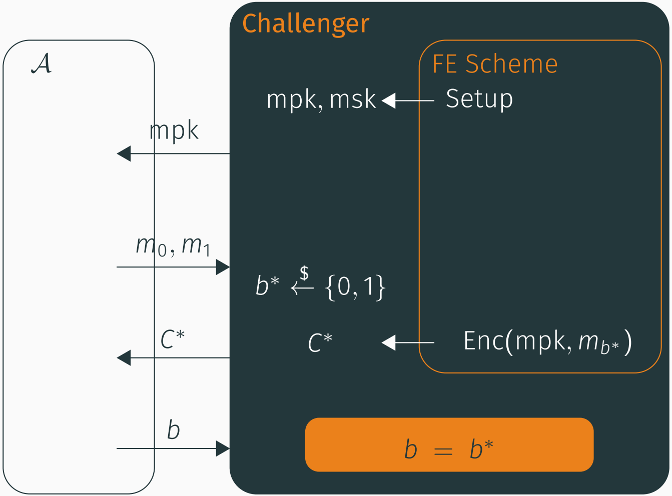


Functional Encryption [BSW11]

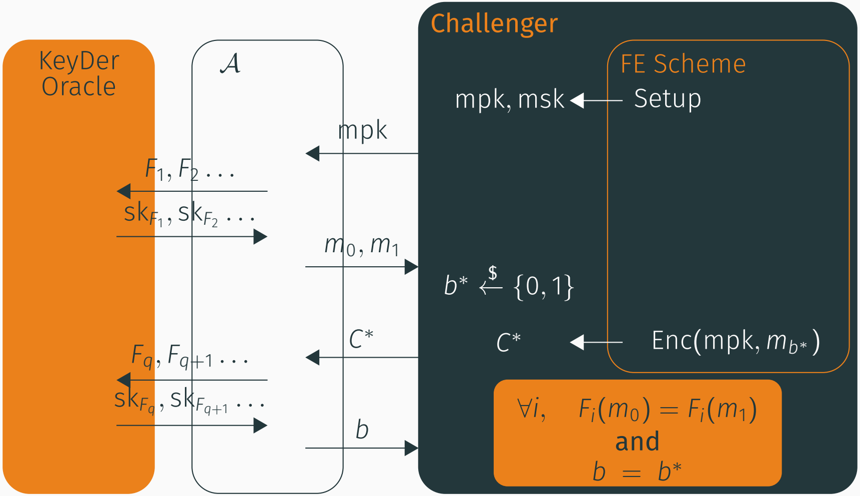
Alice	Auth.	Bob
m	Setup	Function F
	↓	
	(mpk, msk)	
$C = \text{Enc}(\text{mpk}, m)$	$\text{sk}_F = \text{KeyDer}(\text{msk}, F)$	sk_F
		$\text{Dec}(\text{sk}_F, C) \rightarrow F(m)$

Bob **only learns** $F(m)$.

FE Security – Indistinguishability



FE Security – Indistinguishability



Limits of General Functional Encryption

Constructions of FE for **general functions** exist, but are **not practical**

[SS10, GVW12, GKP+13a, GKP+13b, ABSV15, Wat15, BGJS16, GGHZ16]

Limits of General Functional Encryption

Constructions of FE for **general functions** exists, but are **not practical** [SS10, GVW12, GKP+13a, GKP+13b, ABSV15, Wat15, BGJS16, GGHZ16]

$\Rightarrow$ **Linear Functions:** simple with many applications

Limits of General Functional Encryption

Constructions of FE for **general functions** exists, but are **not practical**
[SS10, GVW12, GKP+13a, GKP+13b, ABSV15, Wat15, BGJS16, GGHZ16]

$\Rightarrow$ **Linear Functions:** simple with many applications

- Understand general FE
- Statistical analysis on encrypted data
- Evaluation of polynomials over encrypted data [KSW08]
- Constructing trace-and-revoke systems [ABP+17]
- etc.

The Inner Product Functionality

The inner product functionality

Auth.

Setup

$(\mathsf{mpk}, \mathsf{msk})$

Alice

$\vec{y}$

$C = \mathsf{Enc}\,(\mathsf{mpk}, \vec{y})$

C →

Bob

$\vec{x}, \mathsf{sk}_{\vec{x}}$

$\langle \vec{x}, \vec{y} \rangle = \mathsf{Dec}(\mathsf{sk}_{\vec{x}}, C)$

$$\begin{aligned} F_x : \mathcal{R}^{\ell} &\mapsto \mathcal{R} \\ y &\mapsto \langle \vec{x}, \vec{y} \rangle \end{aligned}$$

Previous work

Schemes mod p do not recover large inner products or are inefficient.

PKC 2015	Crypto 2016	2016	PKC 2017
[ABDP15]	[ALS16]	[ABCP16]	[BBL17]
First IPFE schemes, from LWE and DDH, only selectively secure.	Full security, from LWE, DDH and DCR.	Full security, less efficient than [ALS16].	Generic constructions from HPS.

Previous work

Schemes mod p do not recover large inner products or are inefficient.

PKC 2015	Crypto 2016	2016	PKC 2017	Asiacrypt 2018
[ABDP15]	[ALS16]	[ABCP16]	[BBL17]	**This work:**
First IPFE schemes, from LWE and DDH, only selectively secure.	Full security, from LWE, DDH and DCR.	Full security, less efficient than [ALS16].	Generic constructions from HPS.	IPFE mod p adaptive security no restriction on size and efficient!

Framework

Framework (sketch) [CL15]

Group with an easy discrete logarithm (DL) subgroup

- $G = \langle g \rangle$ cyclic group of order $p \cdot s$ such that $\gcd(p, s) = 1$.
- p large prime
- s unknown
- $F = \langle f \rangle$ subgroup of G of order p.
- $G^p = \langle g_p \rangle = \{x^p, x \in G\}$ subgroup of G of order s,

$$G = F \times G^p.$$

- DL is **easy** in F (DL: given f and $h = f^x$, find $x \in \mathbf{Z}/p\mathbf{Z}$)

New Assumption

Hard Subgroup Membership problem HSM:

Hard to distinguish p-th powers in G

$$\{x \xleftarrow{\$} G\} \approx_c \{x \xleftarrow{\$} G^p\}.$$

Analogy to Paillier's cryptosystem

Paillier's framework

- Message space $\mathbf{Z}/N\mathbf{Z}$ with N RSA modulus
- Relies on Paillier's DCR assumption
  - e.g. distinguishing N^{th} powers in $\mathbf{Z}/N^2\mathbf{Z}$

Our framework

- Messages encoded in $\mathbf{Z}/p\mathbf{Z}$ with p prime
  - Size of p **independent** of security parameter
- Relies on HSM assumption
  - e.g. distinguishing p^{th} powers in G of order $p \cdot s$
- **Instantiation:** class groups of an imaginary quadratic field [CL15]

Sampling exponents

Problem

s unknown, so orders of G^p and G unknown

$\Rightarrow$ Cannot sample uniformly from G or G^p!

Sampling exponents

Problem

s unknown, so orders of G^p and G unknown

$\Rightarrow$ Cannot sample uniformly from G or G^p!

Solution

Use upper bound $\tilde{s}$ of s to instantiate distributions $\mathcal{D}$ and $\mathcal{D}_p$ s.t.

$$\{g^x, x \hookleftarrow \mathcal{D}\} \approx \mathcal{U}(G) \text{ and } \{g_p^x, x \hookleftarrow \mathcal{D}_p\} \approx \mathcal{U}(G^p)$$

In practice: Folded gaussian distributions with large standard deviation

$\Rightarrow$ better efficiency (shorter exponents) than folded uniforms

Inner Product Functional Encryption mod p from HSM

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$$\mathsf{msk} = \vec{t} \text{ and } \mathsf{mpk} = (h_1, \ldots, h_\ell)$$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$$\mathsf{msk} = \vec{t} \text{ and } \mathsf{mpk} = (h_1, \ldots, h_\ell)$$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \dots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \dots, h_\ell)$

Enc **Plaintext:** $\vec{y} = (y_1, \dots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \dots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \dots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \dots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \dots, h_\ell)$

Enc Plaintext: $\vec{y} = (y_1, \dots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \dots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer Input: $\vec{x} = (x_1, \dots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec From $\vec{C}, \vec{x}$ and $\mathsf{sk}_{\vec{x}}$:

$$\langle \vec{x}, \vec{y} \rangle \bmod p$$

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$$\mathsf{msk} = \vec{t} \text{ and } \mathsf{mpk} = (h_1, \ldots, h_\ell)$$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \ldots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec **From** $\vec{C}, \vec{x}$ **and** $\mathsf{sk}_{\vec{x}}$ **:** $\prod_{i=1}^{\ell} C_i^{x_i} = \prod (f^{y_i} \cdot h_i^r)^{x_i}$

$$\langle \vec{x}, \vec{y} \rangle \bmod p$$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \ldots, h_\ell)$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \ldots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec **From** $\vec{C}, \vec{x}$ **and** $\mathsf{sk}_{\vec{x}}$ **:** $\prod_{i=1}^{\ell} C_i^{x_i} = f^{\sum y_i x_i} \cdot g_p^{r \cdot \sum t_i x_i}$

$\langle \vec{x}, \vec{y} \rangle \bmod p$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \ldots, h_\ell)$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \ldots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec From $\vec{C}, \vec{x}$ **and** $\mathsf{sk}_{\vec{x}}$ **:** $\prod_{i=1}^{\ell} C_i^{x_i} = f^{\langle \vec{y}, \vec{x} \rangle} \cdot g_p^{r \cdot \langle \vec{t}, \vec{x} \rangle}$

$\langle \vec{x}, \vec{y} \rangle \bmod p$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \ldots, h_\ell)$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \ldots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec **From** $\vec{C}, \vec{x}$ **and** $\mathsf{sk}_{\vec{x}}$ **:** $\prod_{i=1}^{\ell} C_i^{x_i} = f^{\langle \vec{y}, \vec{x} \rangle} \cdot g_p^{r \cdot \langle \vec{t}, \vec{x} \rangle}$ **and** $C_0^{\mathsf{sk}_{\vec{x}}} = g_p^{r \cdot \langle \vec{t}, \vec{x} \rangle}$

$\langle \vec{x}, \vec{y} \rangle \bmod p$

IPFE scheme mod p from HSM (simplified)

Setup For $i = 1, \ldots, \ell$ do $t_i \hookleftarrow \mathcal{D}$ and $h_i = g_p^{t_i}$

$\mathsf{msk} = \vec{t}$ and $\mathsf{mpk} = (h_1, \ldots, h_\ell)$

Enc **Plaintext:** $\vec{y} = (y_1, \ldots, y_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Sample $r \hookleftarrow \mathcal{D}_p$

Ciphertext:

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_1} \cdot h_1^r, \ldots, C_\ell = f^{y_\ell} \cdot h_\ell^r)$$

KeyDer **Input:** $\vec{x} = (x_1, \ldots, x_\ell) \in (\mathbf{Z}/p\mathbf{Z})^\ell$

Output key: $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Dec **From** $\vec{C}, \vec{x}$ **and** $\mathsf{sk}_{\vec{x}}$ **:** $\prod_{i=1}^{\ell} C_i^{x_i} = f^{\langle \vec{y}, \vec{x} \rangle} \cdot g_p^{r \cdot \langle \vec{t}, \vec{x} \rangle}$ **and** $C_0^{\mathsf{sk}_{\vec{x}}} = g_p^{r \cdot \langle \vec{t}, \vec{x} \rangle}$

Such that:

$$\prod_{i=1}^{\ell} C_i^{x_i} / C_0^{\mathsf{sk}_{\vec{x}}} = f^{\langle \vec{x}, \vec{y} \rangle} \xrightarrow{\text{DL}} \langle \vec{x}, \vec{y} \rangle \bmod p$$

Security

This scheme is secure under the HSM assumption.

Proof overview – inspired by [ALS16]

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_{b*,1}} \cdot h_1^r, \ldots, C_\ell = f^{y_{b*,\ell}} \cdot h_\ell^r)$$

- Game 0 original security game

Proof overview – inspired by [ALS16]

$$\vec{C} = (C_0 = g_p^r, C_1 = f^{y_{b^*,1}} \cdot C_0^{t_1}, \ldots, C_\ell = f^{y_{b^*,\ell}} \cdot C_0^{t_\ell})$$

- Game 0 original security game
- Game 1 use **secret key** to compute challenge ciphertext [CS02]

Proof overview – inspired by [ALS16]

$$\vec{C} = (C_0 = g_p^r f^u, C_1 = f^{y_{b^*,1}} \cdot C_0^{t_1}, \ldots, C_\ell = f^{y_{b^*,\ell}} \cdot C_0^{t_\ell})$$

- Game 0 original security game
- Game 1 use **secret key** to compute challenge ciphertext [CS02]
- Game 2 indistinguishable from Game 1 under the HSM assumption.

Proof overview – inspired by [ALS16]

$$\vec{C} = (C_0 = g_p^r f^u, C_1 = f^{y_{b^*,1}} \cdot C_0^{t_1}, \ldots, C_\ell = f^{y_{b^*,\ell}} \cdot C_0^{t_\ell})$$

- Game 0 original security game
- Game 1 use **secret key** to compute challenge ciphertext [CS02]
- Game 2 indistinguishable from Game 1 under the HSM assumption.

In Game 2, from $\mathcal{A}$'s view b^* is **statistically hidden**, given

- the public key
- the challenge ciphertext
- key derivation queries

Information fixed by public key

$$\mathsf{mpk} = \{h_i = g_p^{t_i \bmod s}\}_{i \in [\ell]}$$

$$\Big\downarrow \text{ Fixes}$$

$$(t_1, \ldots, t_\ell) \bmod s$$

$(t_1, \ldots, t_\ell) \bmod p$ is still **uniformly** distributed to $\mathcal{A}$.

Information fixed by challenge ciphertext

$$\vec{C}^* = (C_0 = g_p^r \cdot f^u, \{C_i = f^{y_{b^*,i}} \cdot {C_0}^{t_i}\}_{i \in [\ell]})$$

Information fixed by challenge ciphertext

$$\vec{C}^* = (C_0 = g_p^r \cdot f^u, \{C_i = f^{y_{b^*,i}} \cdot {C_0}^{t_i}\}_{i \in [\ell]})$$

For $i = 1 \ldots, \ell$

$$C_i = g_p^{r \cdot t_i \mod s} \cdot f^{y_{b^*,i} + u \cdot t_i \mod p}$$

Information fixed by challenge ciphertext

$$\vec{C}^* = (C_0 = g_p^r \cdot f^u, \{C_i = f^{y_{b*,i}} \cdot {C_0}^{t_i}\}_{i \in [\ell]})$$

For $i = 1 \ldots, \ell$

$$\downarrow$$

$$C_i = g_p^{r \cdot t_i \mod s} \cdot f^{y_{b*,i} + u \cdot t_i \mod p}$$

Fixes

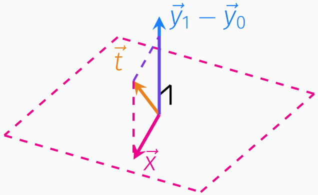
$$\downarrow$$

$$\vec{y}_{b*,i} + u \cdot t_i \mod p$$

Information fixed by key derivation oracle

Because of restriction on secret key queries,
all queries $\vec{x}$ satisfy $\langle \vec{x}, \vec{y}_0 \rangle = \langle \vec{x}, \vec{y}_1 \rangle \mod p$

$\downarrow$

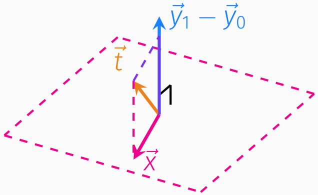


$\forall\, \vec{x}$ s.t. $\langle \vec{x}, \vec{y}_0 - \vec{y}_1 \rangle = 0 \mod p$,
$\mathcal{A}$ can learn $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

Information fixed by key derivation oracle

Because of restriction on secret key queries,
all queries $\vec{x}$ satisfy $\langle \vec{x}, \vec{y}_0 \rangle = \langle \vec{x}, \vec{y}_1 \rangle \mod p$

↓



$\forall \vec{x}$ s.t. $\langle \vec{x}, \vec{y}_0 - \vec{y}_1 \rangle = 0 \mod p$,
$\mathcal{A}$ can learn $\mathsf{sk}_{\vec{x}} = \langle \vec{t}, \vec{x} \rangle$

↓

Remaining entropy on $\vec{t}$ contained in $\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$

Information fixed by key derivation oracle

Given info from mpk and C^*, the distribution

$\mathcal{D}_0$ of $\vec{t}$ is over 1-dim lattice Λ_0 proportional to $\vec{y}_0 - \vec{y}_1$

Information fixed by key derivation oracle

Given info from mpk and C^*, the distribution

$\mathcal{D}_0$ of $\vec{t}$ is over 1-dim lattice Λ_0 proportional to $\vec{y}_0 - \vec{y}_1$

Reduce $\mathcal{D}_0$ mod sub-lattice $p\Lambda_0$ s.t. $\Lambda_0 / p\Lambda_0 \simeq (\vec{y}_0 - \vec{y}_1)\mathbf{Z}/p\mathbf{Z}$

↓

Choosing large enough standard deviation ensures

$\vec{t} \mod p$ follows a distribution $\approx \mathcal{U}(\Lambda_0 / p\Lambda_0)$ [GPV08]

Information fixed by key derivation oracle

Given info from mpk and C^*, the distribution

$\mathcal{D}_0$ of $\vec{t}$ is over 1-dim lattice Λ_0 proportional to $\vec{y}_0 - \vec{y}_1$

↓

Reduce $\mathcal{D}_0$ mod sub-lattice $p\Lambda_0$ s.t. $\Lambda_0/p\Lambda_0 \simeq (\vec{y}_0 - \vec{y}_1)\mathbf{Z}/p\mathbf{Z}$

↓

Choosing large enough standard deviation ensures

$\vec{t} \mod p$ follows a distribution $\approx \mathcal{U}(\Lambda_0/p\Lambda_0)$ [GPV08]

↓

$\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$ follows a distribution $\approx \mathcal{U}(\mathbf{Z}/p\mathbf{Z})$

$\mathcal{A}$'s success probability

From $\mathcal{A}$'s view, $\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$ follows a distribution $\approx \mathcal{U}(\mathbf{Z}/p\mathbf{Z})$.

$\mathcal{A}$'s success probability

From $\mathcal{A}$'s view, $\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$ follows a distribution $\approx \mathcal{U}(\mathbf{Z}/p\mathbf{Z})$.

The ciphertext reveals:

$$\vec{y}_{b*} + u\vec{t} \bmod p$$

$\mathcal{A}$'s success probability

From $\mathcal{A}$'s view, $\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$ follows a distribution $\approx \mathcal{U}(\mathbf{Z}/p\mathbf{Z})$.

The ciphertext reveals:

$$\vec{y}_{b^*} + u\vec{t} \bmod p$$

The information on b^* is contained in:

$$\langle \vec{y}_{b^*}, \vec{y}_0 - \vec{y}_1 \rangle + u\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \bmod p$$

$\mathcal{A}$'s success probability

From $\mathcal{A}$'s view, $\langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \mod p$ follows a distribution $\approx \mathcal{U}(\mathbf{Z}/p\mathbf{Z})$.

The ciphertext reveals:

$$\vec{y}_{b^*} + u\vec{t} \bmod p$$

The information on b^* is contained in:

$$\langle \vec{y}_{b^*}, \vec{y}_0 - \vec{y}_1 \rangle + u \langle \vec{t}, \vec{y}_0 - \vec{y}_1 \rangle \bmod p$$

$\mathcal{A}$ cannot guess b^* with proba $> 1/2 + \text{negl}$

Conclusion

- Many **details** hidden in this talk (stateful KeyDer)
- IPFE from weaker assumption DDH-f
- Instantiation using **class groups** of an imaginary quadratic field
  - Best known algorithms for underlying problems in $L(1/2)$
  - Shorter keys!
- **Efficiency** comparison for 128-bit security, $\ell = 100$
  - Enc $\approx$ 0.7s; Dec $\approx$ 1.9s **vs.** 0.8s and 9.6s in [ALS16]
  - $sk_{\vec{x}}$ of 13852 bits **vs.** 313344 bits in [ALS16]
  - Dependency in ℓ is linear
- **Ongoing work**
  - CCA secure schemes
  - Applying framework to other cryptographic primitives

Questions?

M. Abdalla, F. Bourse, A. D. Caro, and D. Pointcheval.
Better security for functional encryption for inner product evaluations.
Cryptology ePrint Archive, Report 2016/011, 2016.
`http://eprint.iacr.org/2016/011`.

M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval.
Simple functional encryption schemes for inner products.
In *PKC 2015*, *LNCS* 9020, pages 733–751. Springer, Heidelberg, March / April 2015.

S. Agrawal, S. Bhattacherjee, D. H. Phan, D. Stehlé, and S. Yamada.
Efficient public trace and revoke from standard assumptions: Extended abstract.
In *ACM CCS 17*, pages 2277–2293. ACM Press, October / November 2017.

References ii

P. Ananth, Z. Brakerski, G. Segev, and V. Vaikuntanathan.
From selective to adaptive security in functional encryption.
In *CRYPTO 2015, Part II*, *LNCS* 9216, pages 657–677. Springer, Heidelberg, August 2015.

S. Agrawal, B. Libert, and D. Stehlé.
Fully secure functional encryption for inner products, from standard assumptions.
In *CRYPTO 2016, Part III*, *LNCS* 9816, pages 333–362. Springer, Heidelberg, August 2016.

F. Benhamouda, F. Bourse, and H. Lipmaa.
CCA-secure inner-product functional encryption from projective hash functions.
In *PKC 2017, Part II*, *LNCS* 10175, pages 36–66. Springer, Heidelberg, March 2017.

S. Badrinarayanan, V. Goyal, A. Jain, and A. Sahai.
Verifiable functional encryption.
In *ASIACRYPT 2016, Part II*, *LNCS* 10032, pages 557–587. Springer, Heidelberg, December 2016.

D. Boneh, A. Sahai, and B. Waters.
Functional encryption: Definitions and challenges.
In *TCC 2011*, *LNCS* 6597, pages 253–273. Springer, Heidelberg, March 2011.

G. Castagnos and F. Laguillaumie.
Linearly homomorphic encryption from DDH**.**
In *CT-RSA 2015*, *LNCS* 9048, pages 487–505. Springer, Heidelberg, April 2015.

R. Cramer and V. Shoup.
Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption.
In *EUROCRYPT 2002*, *LNCS* 2332, pages 45–64. Springer, Heidelberg, April / May 2002.

S. Garg, C. Gentry, S. Halevi, and M. Zhandry.
Functional encryption without obfuscation.
In *TCC 2016-A, Part II*, *LNCS* 9563, pages 480–511. Springer, Heidelberg, January 2016.

S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich.
How to run turing machines on encrypted data.
In *CRYPTO 2013, Part II*, *LNCS* 8043, pages 536–553. Springer, Heidelberg, August 2013.

S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich.
Reusable garbled circuits and succinct functional encryption.
In *45th ACM STOC*, pages 555–564. ACM Press, June 2013.

C. Gentry, C. Peikert, and V. Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

S. Gorbunov, V. Vaikuntanathan, and H. Wee.
Functional encryption with bounded collusions via multi-party computation.
In *CRYPTO 2012*, *LNCS* 7417, pages 162–179. Springer, Heidelberg, August 2012.

- J. Katz, A. Sahai, and B. Waters.
  Predicate encryption supporting disjunctions, polynomial equations, and inner products.
  In *EUROCRYPT 2008*, *LNCS* 4965, pages 146–162. Springer, Heidelberg, April 2008.
- A. Sahai and H. Seyalioglu.
  Worry-free encryption: functional encryption with public keys.
  In *ACM CCS 10*, pages 463–472. ACM Press, October 2010.
- B. Waters.
  A punctured programming approach to adaptively secure functional encryption.
  In *CRYPTO 2015, Part II*, *LNCS* 9216, pages 678–697. Springer, Heidelberg, August 2015.