RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CRYP-F01

Traceable Inner Product Functional Encryption

Xuan Thanh Do [1,2], Duong Hieu Phan [2], David Pointcheval [3]

[1] Vietnam National University, Vietnam

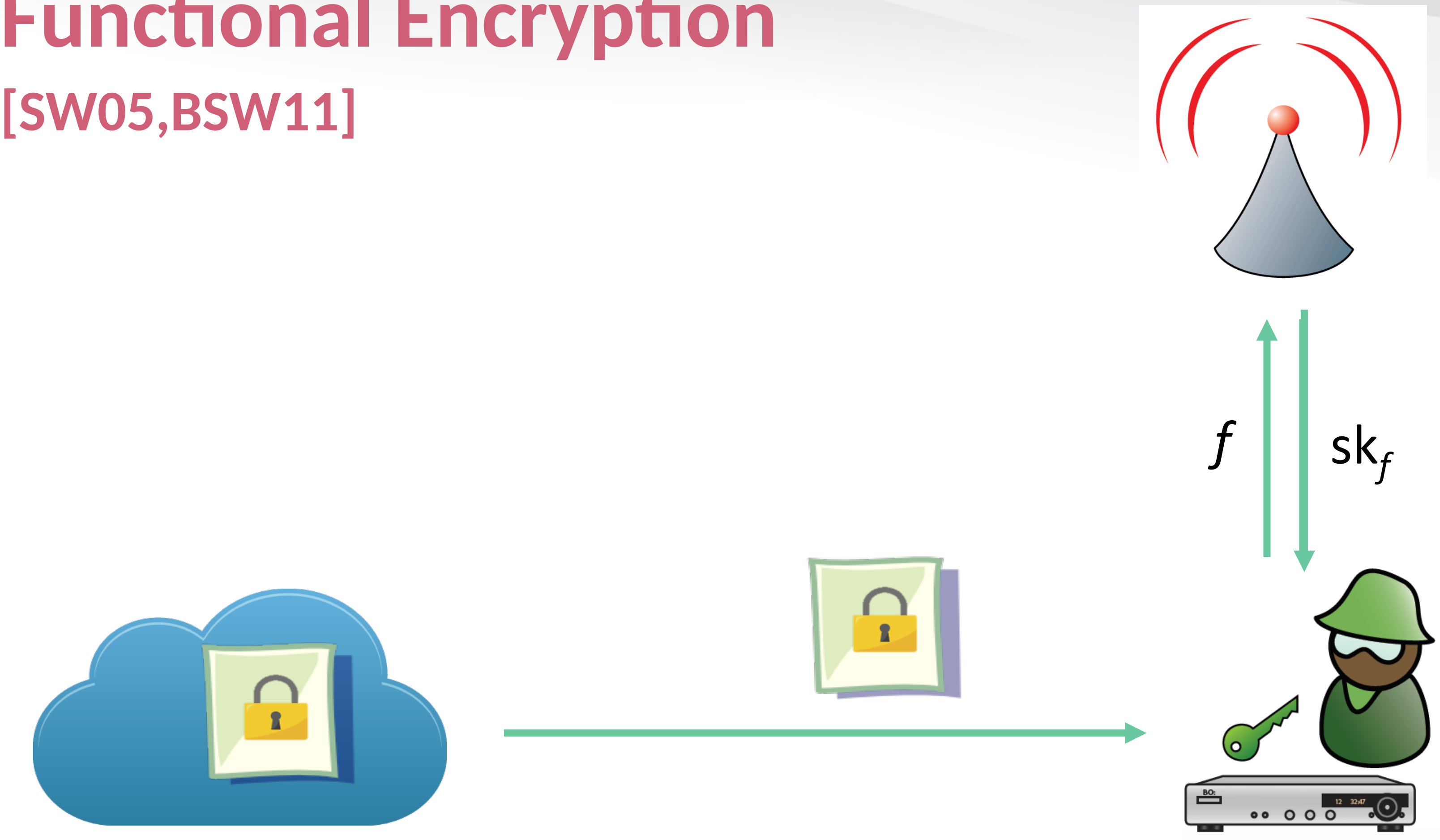
[2] XLIM, University of Limoges, France

[3] Ecole normale supérieure / PSL, Paris, France

#RSAC

Functional Encryption

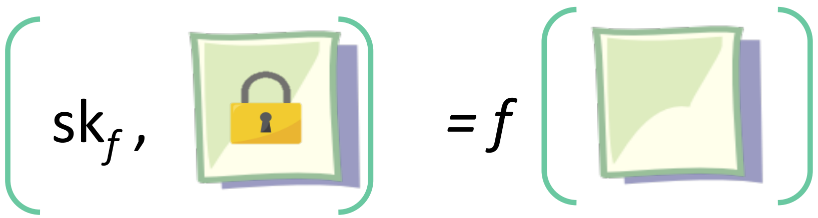
[SW05,BSW11]



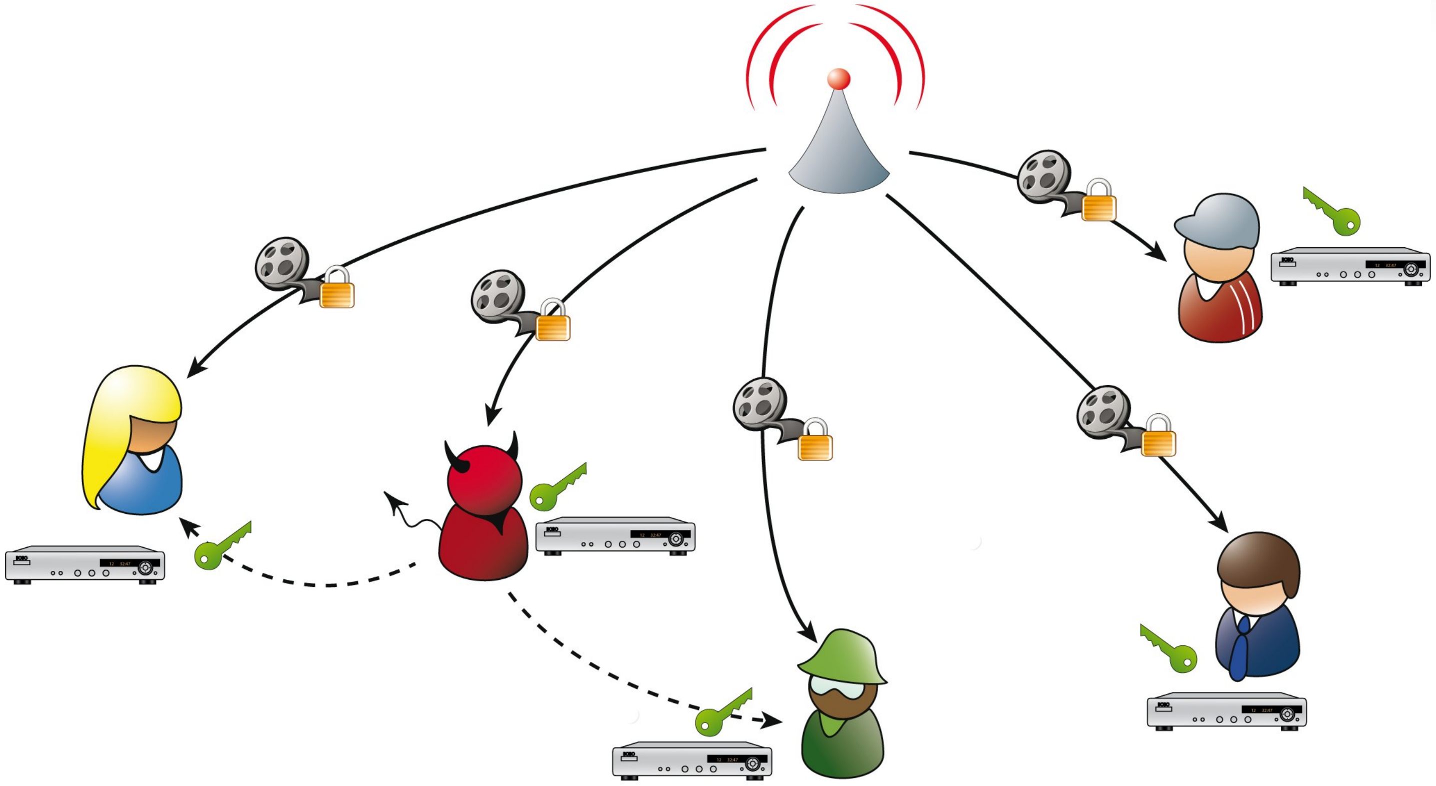
Exemples of function f

- Average value
- Statistical value

Decrypt



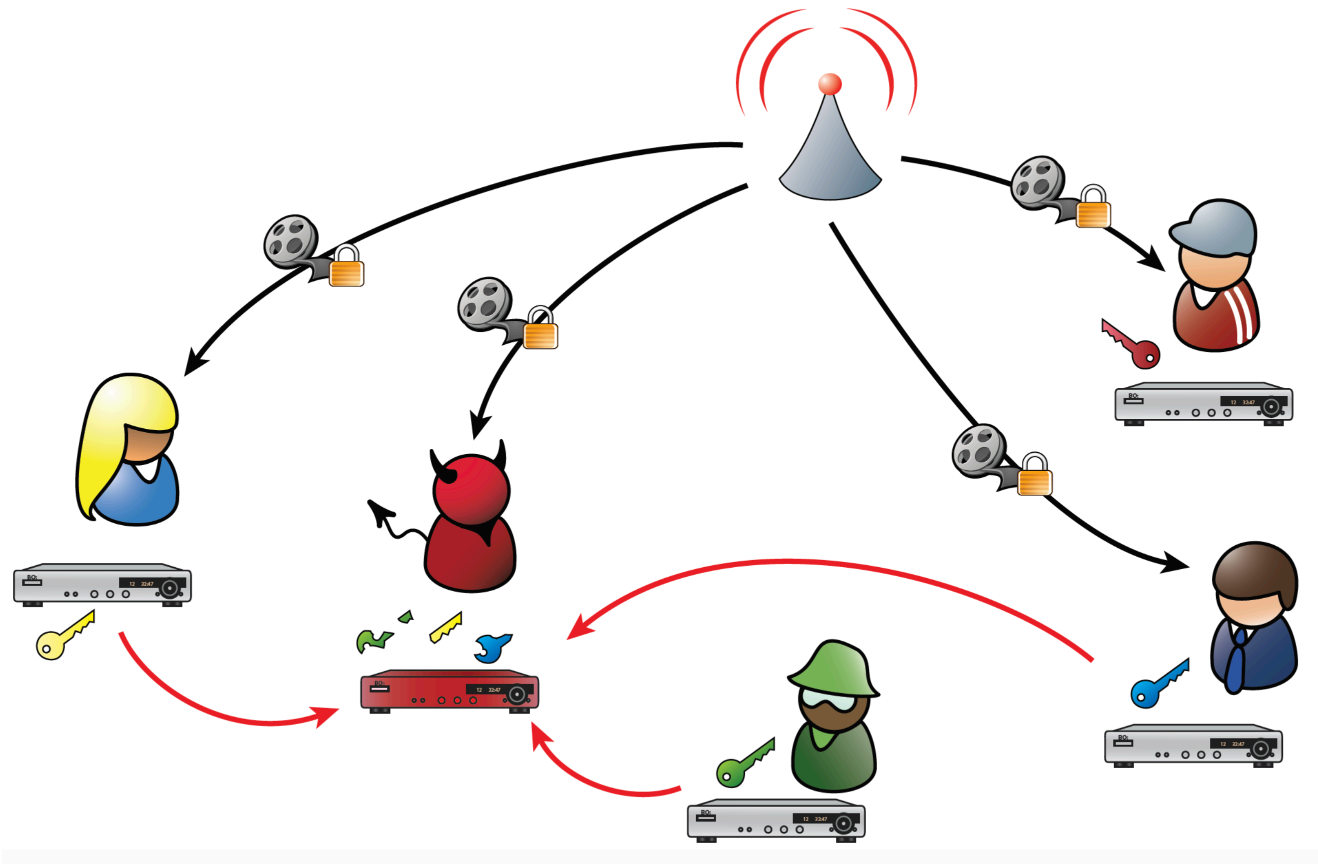
Functional Encryption in Multi-user setting



Problem with the same key:
Untraceable Pirate Decoder
➡ Personal functional key

Remark:
When $f(x) = x$
➡ Classical Traitor Tracing

Traceable Functional Encryption



Traceability: From a pirate decoder for a function f, find out a traitor.

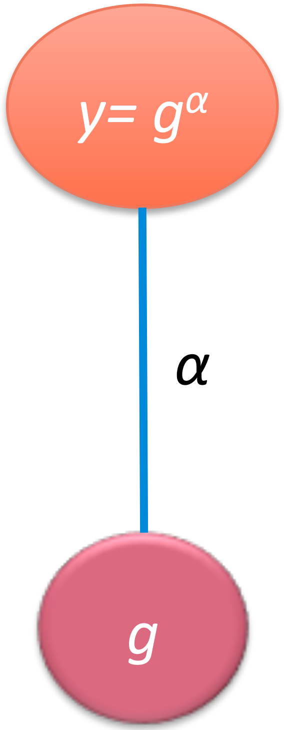
Traceable IPFE

- Functional encryption for general circuit: based on iO
- Efficient Construction for inner product functions (IPFE) [ABCP15]
  - For a vector $\overrightarrow{x} = (x_1, \ldots, x_k)$, user is given a key sk_x
  - For a vector $\overrightarrow{y} = (y_1, \ldots, y_k)$:

$$Decrypt(sk_x, Encrypt(\overrightarrow{y})) = < \overrightarrow{x}, \overrightarrow{y} > = \Sigma_{i=1}^{k} x_i y_i$$

- **This work: Efficient construction for Traceable IPFE**
- **Tools: Combining ElGamal-based IPFE and Traitor Tracing**

ElGamal Encryption



Setup: $G = < g >$ of order q

Secret key:

$$\alpha \leftarrow \mathbb{Z}_q$$

Public key:

$$g, y = g^{\alpha}$$

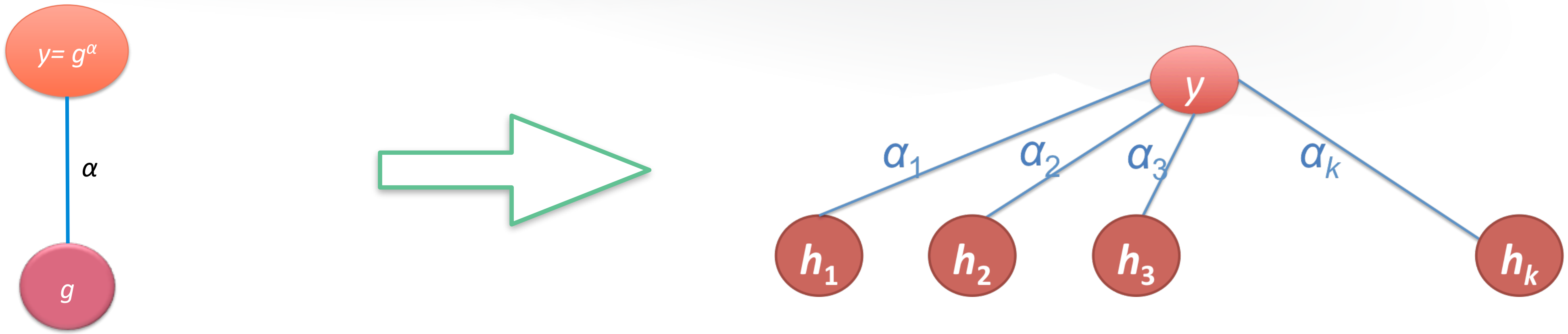
Ciphertext:

$$(g^r, y^r m), \text{ where } r \leftarrow \mathbb{Z}_q$$

Decryption:

Compute $(g^r)^{\alpha} = y^r$ and recover m

Elgamal Encryption -> Multi-user (Boneh-Franklin '01)



Public key: $(y, h_1, \ldots, h_k) \in G^{k+1}$

User key: a representation $(\alpha_1, \ldots, \alpha_k)$ of y in the basis $(h_1, \ldots, h_k)$:

$$y = h_1^{\alpha_1} \ldots h_k^{\alpha_k}$$

Ciphertext:

$$(y^r m, h_1^r, \ldots, h_k^r), \text{ where } r \leftarrow \mathbb{Z}_q$$

Decryption: Each user can compute y^r from $(h_1^r, \ldots, h_k^r)$ and recover m

Elgamal Encryption -> IPFE [ABCP '15]

Master secret key $MSK = \vec{s} = (s_1, \ldots, s_k)$

Public key: $pk = (h_1 = g^{s_1}, \ldots, h_k = g^{s_k}) \in G^k$

User key for vector $\overrightarrow{x} = (x_1, \ldots, x_k)$: $sk_x = < \vec{s}, \overrightarrow{x} > = \Sigma_{i=1}^k s_i x_i$

$$Enc(pk, \overrightarrow{y} = (y_1, \ldots, y_k)) = (g^r, h_1^r g_1^y, \ldots, h_k^r g_k^y), \text{ where } r \leftarrow \mathbb{Z}_q$$

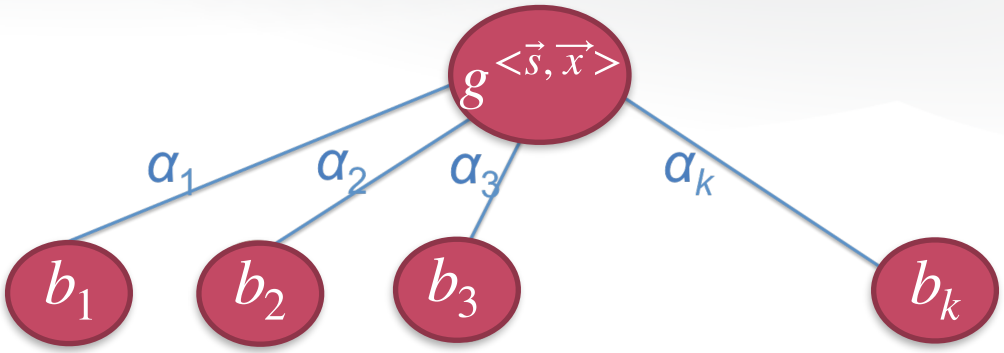
Decryption: remove « ElGamal 's mask » $(g^r)^{<\vec{s}, \overrightarrow{x}>} = \Pi_{i=1}^k ((g_i^r)^{s_i})^{x_i} = \Pi_{i=1}^k (h_i^r)^{x_i}$, thus:

$$\frac{(h_1^r g^{y_1})^{x_1} \times \ldots \times (h_k^r g_k^y)^{x_k}}{(g^r)^{sk_x}} = \frac{(h_1^r)^{x_1} \times \ldots \times (h_k^r)^{x_k}}{(g^r)^{(s_1 x_1 + \ldots + s_k x_k)}} \times g^{<\overrightarrow{x}, \overrightarrow{y}>} = g^{<\overrightarrow{x}, \overrightarrow{y}>}$$

Problem: one key for each function!

Idea: randomized keys for computing $(g^r)^{<\vec{s}, \overrightarrow{x}>}$

Our technique: Adding BF tracing to IPFE



Public key: $pk = (b_1 = g^{t_1}, \ldots, b_k = g^{t_k}, h_1 = g^{s_1}, \ldots, h_k = g^{s_k}) \in G^{2k}$

User ID is associated to a public codeword $\vec{\theta}_{\mathrm{ID}} = (\theta_1, \ldots, \theta_k)$:

for vector $\vec{x} = (x_1, \ldots, x_k)$, user's secret key $tk_{\vec{x},\mathrm{ID}} = \langle \vec{s}, \vec{x} \rangle / \langle \vec{t}, \vec{\theta}_{\mathrm{ID}} \rangle$.

$(tk_{\vec{x},\mathrm{ID}}\theta_i)_{i=1}^{k}$ **is a representation of** $g^{<\vec{s},\vec{x}>}$ **in the basis** $(b_1, \ldots, b_k)$

$Enc(pk, \vec{y} = (y_1, \ldots, y_k)) = (b_1^r, \ldots, b_k^r, h_1^r g_1^y, \ldots, h_k^r g_k^y)$, where $r \leftarrow \mathbb{Z}_q$

Decryption: **remove** $g^{r<\vec{s},\vec{x}>}$ **from** $b_1^r, \ldots, b_k^r$ **with** $(tk_{\vec{x},\mathrm{ID}}\theta_i)_{i=1}^{k}$

The use of pairings

- When the secret keys are scalars:

from $tk_{\vec{x}_1,\mathsf{ID}_1} = \frac{\langle \vec{s}, \vec{x}_1 \rangle}{\langle \vec{t}, \vec{\theta}_{\mathsf{ID}_1} \rangle}$ and $tk_{\vec{x}_2,\mathsf{ID}_1} = \frac{\langle \vec{s}, \vec{x}_2 \rangle}{\langle \vec{t}, \vec{\theta}_{\mathsf{ID}_1} \rangle}$ and $tk_{\vec{x}_1,\mathsf{ID}_2} = \frac{\langle \vec{s}, \vec{x}_1 \rangle}{\langle \vec{t}, \vec{\theta}_{\mathsf{ID}_2} \rangle}$.

one can compute $tk_{\vec{x}_2,\mathsf{ID}_2} = \frac{tk_{\vec{x}_2,\mathsf{ID}_1} \cdot tk_{\vec{x}_1,\mathsf{ID}_2}}{tk_{\vec{x}_1,\mathsf{ID}_1}}$

- Corrupting $2k$ keys then break the master secret key
- **Solution:**
  - put $t_{\vec{x},\mathsf{ID}}$ in the exponent $sk_{\vec{x},\mathsf{ID}} = g^{tk_{\vec{x},\mathsf{ID}}}$
  - decryption will then be performed in the target group of the pairing.

Security

- Confidentiality: selective security under the BDDH assumption
- Tracing: Black-box confirmation from the linear tracing technique
  $\mathscr{K}_{\text{suspect}} = \{tk_1, \ldots, tk_t\}, t \leq k,$ for a fixed vector $\overrightarrow{x} = (x_1, \ldots, x_k)$:

$$\mathsf{Tr}_i = \left\{ \left(H_1^a G^{y_1}, \ldots, H_k^a G^{y_k}, g_1^{z_1}, \ldots, g_1^{z_k} \right) \;\middle|\; a \leftarrow \mathbb{Z}_q, \vec{z} \leftarrow \mathbb{Z}_q^k, \langle \vec{z}, tk_j \overrightarrow{\theta}_j \rangle = a \langle \vec{s}, \overrightarrow{x} \rangle, \forall j \in [i] \right\}$$

i) Without the key tk_i: Tr_i and Tr_{i-1} are indistinguishable

ii) Tr_0 is indistinguishable from **Random**

iii) Tr_t is indistinguishable from **Normal ciphertexts** that the Pirate can decrypt

There exists i: gap in probability of decrypting Tr_i and Tr_{i-1} $\rightarrow$ i is a traitor.

Conclusion

- Open technical problems:
  - Stronger security (with more general security, adaptive security, unbounded collusion)
  - More general functions (*e.g.*, quadratic function).
- Perspectives:
  - Decentralized setting: Multi-client setting for traceable IPFE
  - Integrating revocation.