Verifiable Inner Product Encryption Scheme

Najmeh Soroush, Vincenzo Iovino, Alfredo Rial,
Peter Roenne, Peter Y.A. Ryan

PKC 2020 – Virtual version
June 2020

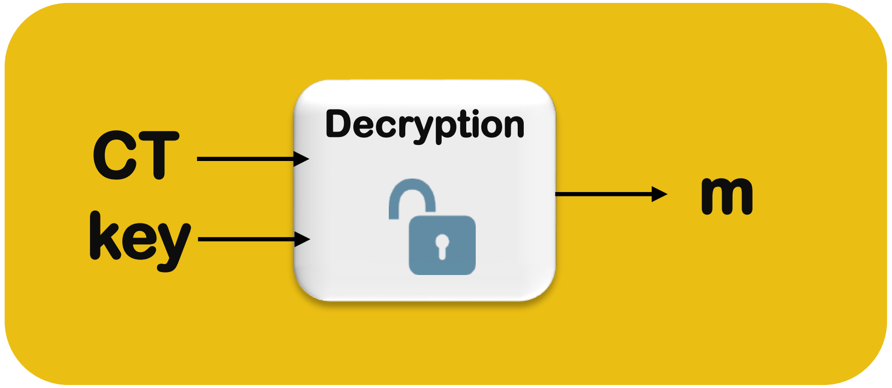
securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

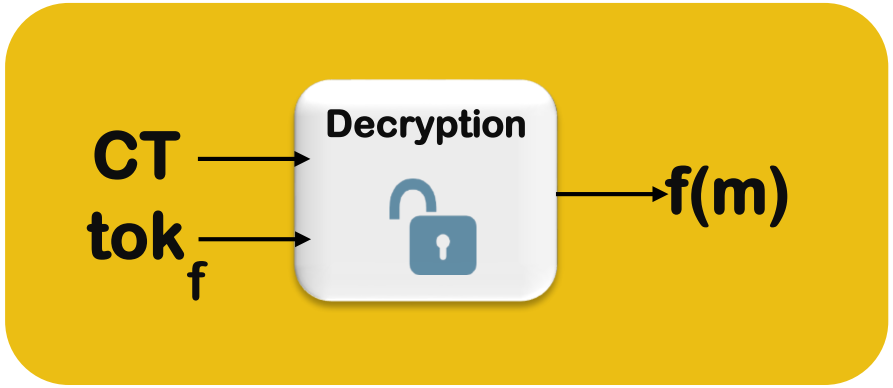
Outline

- Functional Encryption “FE”
- Verifiability concept for FE
- Inner Product Encryption as FE
- Perfectly correct IPE
- Verifiable Inner Product Encryption
- Some applications of IPE/VIPE

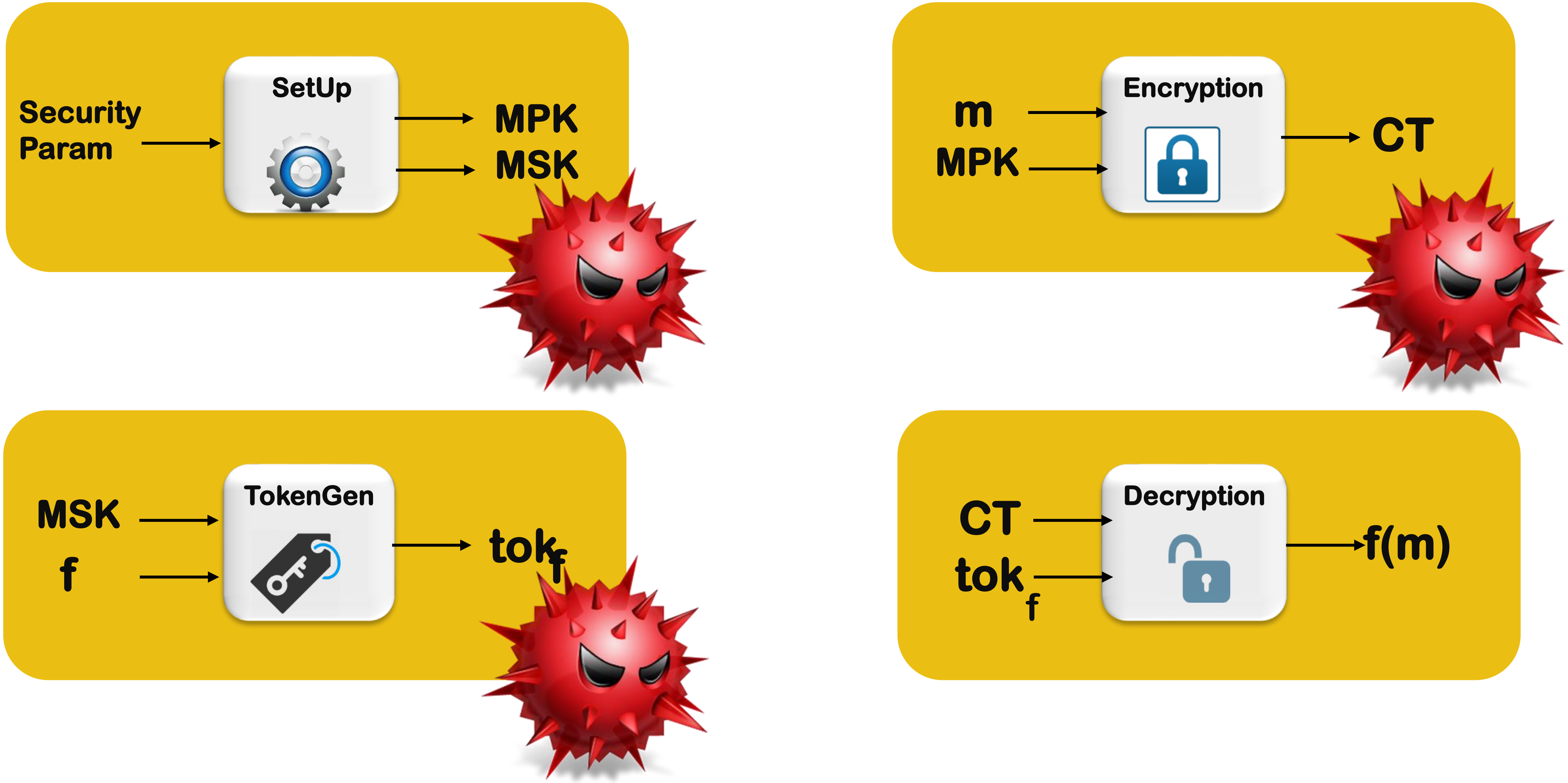
Encryption Scheme



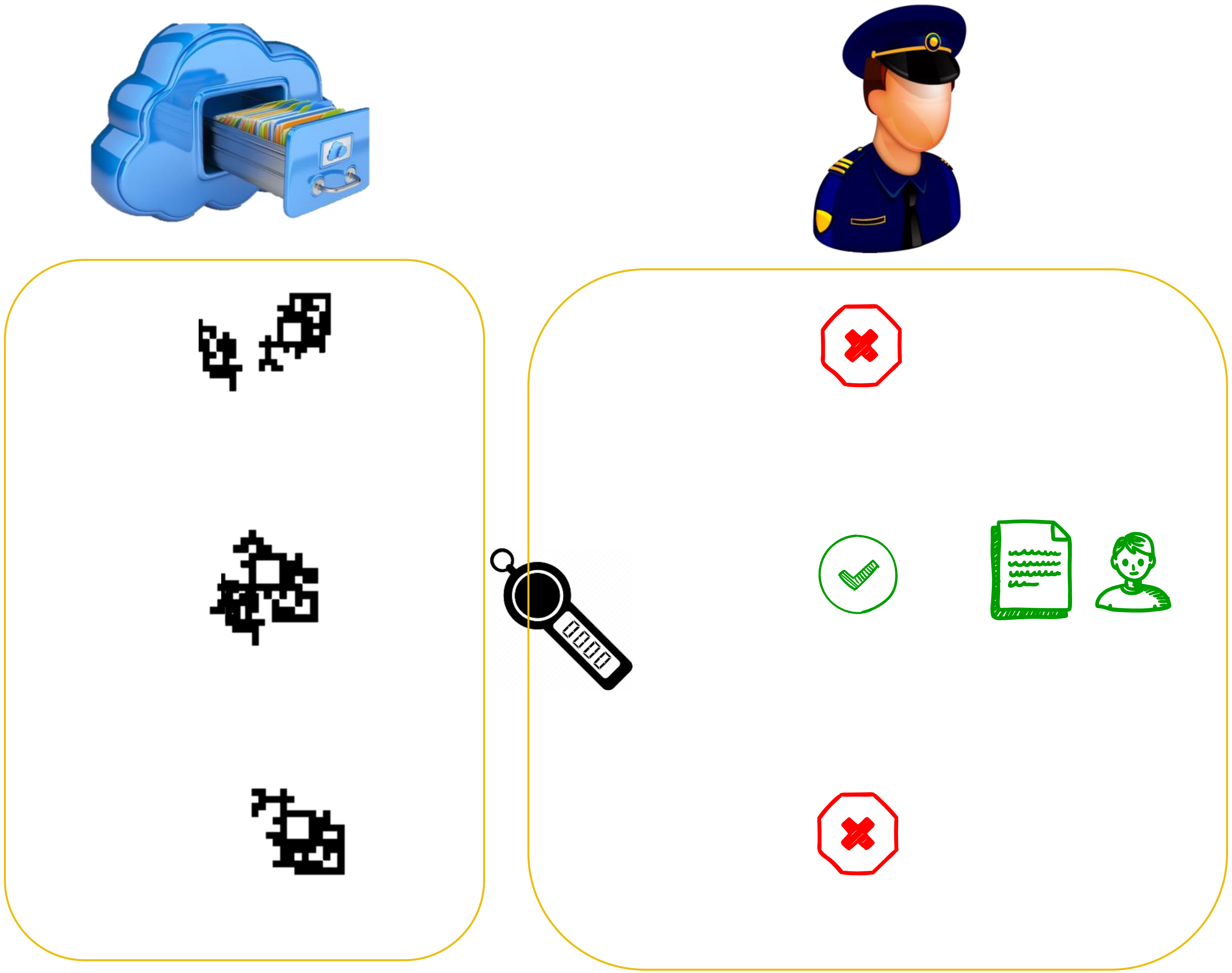
Functional Encryption Scheme



Functional Encryption for functionality $\mathcal{F}$ ={ f }:



Encryted data



[BGJS16]: Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai. Veriable functional encryption. ASIACRYPT 2016

Verifiability for FE [BGJS16] :

CT

MPK

for all f: Tok_f

Public Verification algorithm

- Decryption(CT , Tok_f)=y

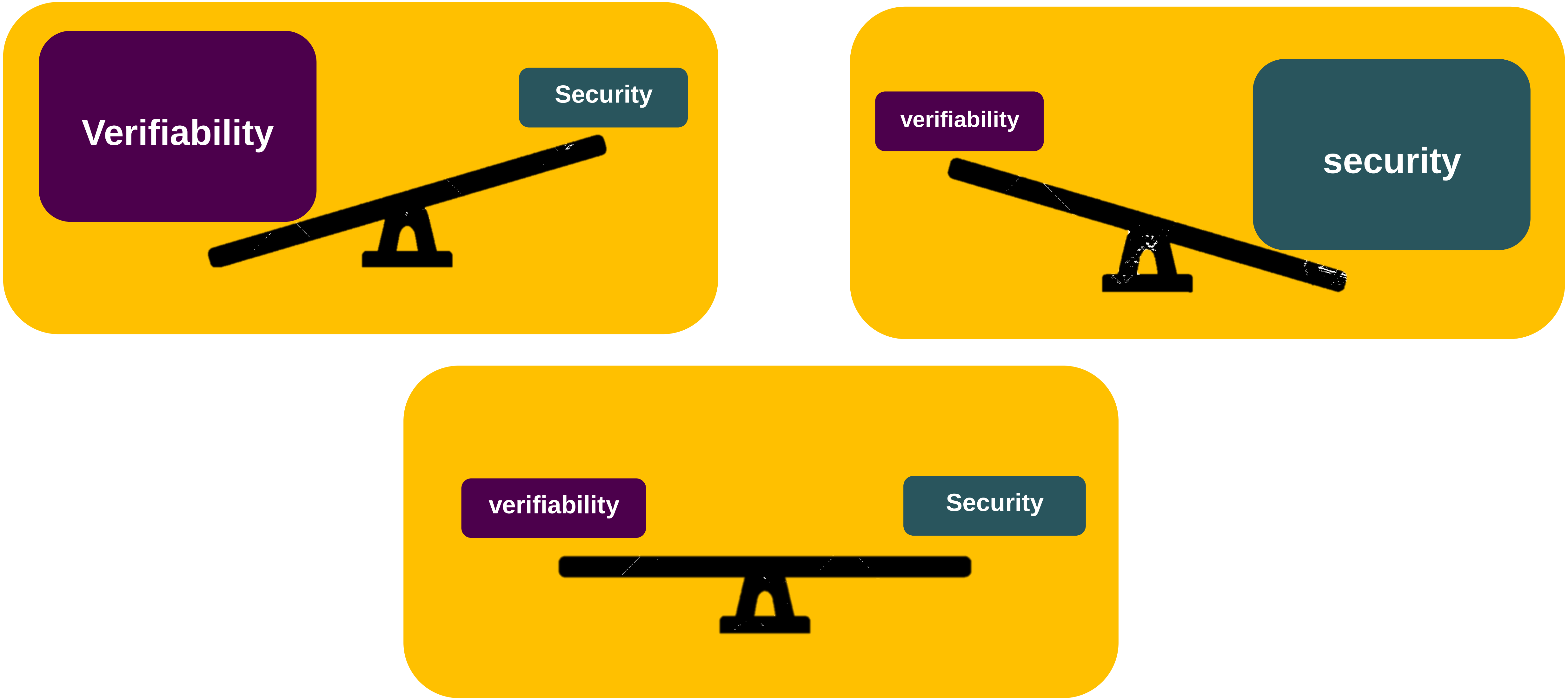
There exist some m :
f(m)=y

- Decryption(CT , Tok_f)=y
- Decryption(CT , Tok_g)=z

There exist some m :
f(m)=y, g(m)=z

[BGJS16]: Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai. Veriable functional encryption. ASIACRYPT 2016

Verifiability vs Security



Inner Product Encryption as FE:

$$\mathcal{F} = \{\mathcal{F}_n\}_{n \in \mathbb{Z}^+}, \mathcal{F}_n = \{f_{\vec{v}}\}_{\vec{v} \in \Sigma_n}$$

$$f_{\vec{v}} : \Sigma_n \times \mathcal{M} \to \mathcal{M} \cup \{\perp\}$$

$$f_{\vec{v}}(\vec{x}, m) = \begin{cases} m \text{ If } \langle \vec{x}, \vec{v} \rangle = 0 \\ \perp \text{ If } \langle \vec{x}, \vec{v} \rangle \neq 0 \end{cases}$$

$\vec{v} \in \Sigma_n$:

- n: A positive integer, (vector length)
- Σ_n: A set of vectors of length n defined over some field ($\mathbb{Z}_p$)
- $\mathcal{M}$: A message space

Inner Product Encryption:

$\mathsf{IP} = \langle \mathsf{SetUp}, \mathsf{TokGen}, \mathsf{Enc}, \mathsf{Dec},$

- $\mathsf{SetUp}(1^\lambda, n) \longrightarrow (\mathsf{MPK}, \mathsf{MSK})$
- $\mathsf{TokGen}(\mathsf{MPK}, \mathsf{MSK}, \vec{v}) \longrightarrow \mathsf{Tok}_{\vec{v}}$
- $\mathsf{Enc}(\mathsf{MPK}, \overrightarrow{x}, m) \longrightarrow \mathsf{CT}$
- $\mathsf{Dec}(\mathsf{MPK}, \mathsf{Tok}_{\vec{v}}, \mathsf{CT}) \longrightarrow m \in \mathcal{M} \cup \{\perp\}$

Correctness

$$\Pr\left[\mathsf{Dec}(\mathsf{Tok}_{\vec{v}}, \mathsf{CT}) = f_{\vec{v}}(\vec{x}, m) \;\middle|\; \begin{array}{l} (\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{SetUp}(1^\lambda, n), \\ \mathsf{Tok}_{\vec{v}} \leftarrow \mathsf{TokGen}(\mathsf{MSK}, \vec{v}), \\ \mathsf{CT} \leftarrow \mathsf{Enc}(\mathsf{MPK}, \vec{x}, m) \end{array} \right] \approx 1$$

Verifiable Inner Product Encryption:

$\mathsf{IP} = \langle \mathsf{SetUp}, \mathsf{TokGen}, \mathsf{Enc}, \mathsf{Dec},$

- $\mathsf{SetUp}(1^\lambda, n) \longrightarrow (\mathsf{MPK}, \mathsf{MSK})$
- $\mathsf{TokGen}(\mathsf{MPK}, \mathsf{MSK}, \vec{v}) \longrightarrow \mathsf{Tok}_{\vec{v}}$
- $\mathsf{Enc}(\mathsf{MPK}, \vec{x}, m) \longrightarrow \mathsf{CT}$
- $\mathsf{Dec}(\mathsf{MPK}, \mathsf{Tok}_{\vec{v}}, \mathsf{CT}) \longrightarrow m \in \mathcal{M} \cup \{\perp\}$

Correctness

$$\Pr\left[\mathsf{Dec}(\mathsf{Tok}_{\vec{v}}, \mathsf{CT}) = f_{\vec{v}}(\vec{x}, m) \;\middle|\; \begin{array}{l} (\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{SetUp}(1^\lambda, n), \\ \mathsf{Tok}_{\vec{v}} \leftarrow \mathsf{TokGen}(\mathsf{MSK}, \vec{v}), \\ \mathsf{CT} \leftarrow \mathsf{Enc}(\mathsf{MPK}, \vec{x}, m) \end{array}\right] = 1$$

Verifiability

$\forall \mathsf{MPK} \in \{0,1\}^*, \forall \mathsf{CT} \in \{0,1\}^*,$
$\exists n > 0, (\vec{x}, m) \in \Sigma_n \times \mathcal{M}:$
$\forall \vec{v} \in \Sigma_n, \mathsf{Tok}_{\vec{v}} \in \{0,1\}^*:$

1. $\mathsf{VrfyMPK}(\mathsf{MPK}) = 1$
2. $\mathsf{VrfyCT}(\mathsf{MPK}, \mathsf{CT}) = 1$
3. $\mathsf{VrfyTok}(\mathsf{MPK}, \vec{v}, \mathsf{Tok}_{\vec{v}}) = 1$

$\Downarrow$

$\Pr[\mathsf{Dec}(\mathsf{MPK}, \vec{v}, \mathsf{Tok}_{\vec{v}}, \mathsf{CT}) = f_{\vec{v}}(m)] = 1$

Perfect correctness

First challenge : Perfectly correct IPE

Randomness from Encryption algorithm

$$\mathsf{Enc}(\mathsf{MPK}, \vec{x}, m) \to \mathsf{CT}$$

$$\mathsf{Dec}(\mathsf{Tok}_{\vec{v}}, \mathsf{CT}) \to m^* = m \cdot \mathbf{e}(g,h)^{(\lambda_1 s_3 + \lambda_2 s_4)\langle \vec{x}, \vec{v} \rangle}$$

Randomness from TokGen algorithm

[Par11]:

[Par11]: Jong Hwan Park. Inner-product encryption under standard assumptions.Des. Codes Cryptography, 58(3):235-257, 2011.

First challenge : Perfectly correct IPE

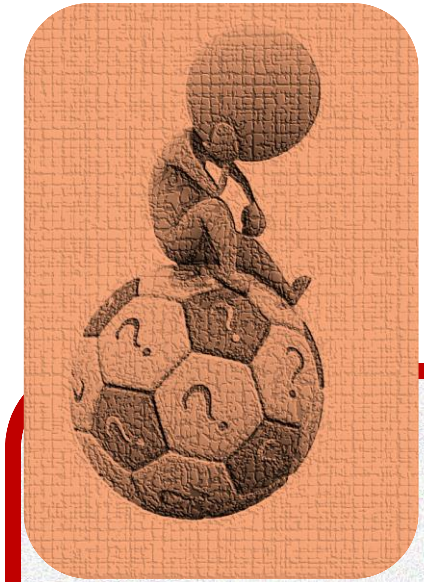
Randomness from Encryption algorithm

$$\mathsf{Enc}(\mathsf{MPK}, \vec{x}, m) \to \mathsf{CT}$$

$$\mathsf{Dec}(\mathsf{Tok}_{\vec{v}}, \mathsf{CT}) \to m^* = m \cdot \boxed{\mathbf{e}(g,h)^{(\lambda_1 s_3 + \lambda_2 s_4)\langle \vec{x}, \vec{v} \rangle}}$$

[Par11]:

Random value



$$\langle \vec{x}, \vec{v} \rangle = 0 \Rightarrow m^* = m \checkmark$$

$$\lambda_1 s_3 + \lambda_2 s_4 = 0 \Rightarrow m^* = m \times$$

Decryption algorithm : m* OR ‘ERROR’

[Par11]: Jong Hwan Park. Inner-product encryption under standard assumptions.Des. Codes Cryptography, 58(3):235-257, 2011.

First attemp:

$$\mathsf{CT} = (\mathsf{ct}, \mathsf{ct}') : \begin{array}{l} \mathsf{ct} = \mathsf{Enc}(m, \mathsf{MPK}; \{s_i\}) \\ \mathsf{ct}' = \mathsf{Enc}(m, \mathsf{MPK}; \{s'_i\}) \end{array},$$

$$\begin{aligned} m_1 &= \mathsf{Dec}(\mathsf{ct}) = m \cdot e(h, g)^{(\lambda_1 s_3 + s_4 \lambda_2)\langle \vec{x}, \vec{v} \rangle} \\ m_2 &= \mathsf{Dec}(\mathsf{ct}') = m \cdot e(h, g)^{(\lambda_1 s'_3 + s'_4 \lambda_2)\langle \vec{x}, \vec{v} \rangle} \end{aligned}$$

Decryption algorithm

$$\begin{array}{ll} m_1 = m_2 : & \texttt{Output} \quad m_1 \\ m_1 \neq m_2 : & \texttt{Output} \quad \perp \end{array}$$

$$(\lambda_1 s_3 + \lambda_2 s_4) = (\lambda_1 s'_3 + \lambda_2 s'_4)$$
$$\Downarrow$$
$$m_1 = m_2$$

Our Solution:

$$\mathsf{CT} = (\mathsf{ct}, \mathsf{ct}') : \quad \begin{aligned} \mathsf{ct} &= \mathsf{Enc}(m, \mathsf{MPK}; \{s_i\}) \\ \mathsf{ct}' &= \mathsf{Enc}(m, \mathsf{MPK}; \{s_i'\}) \end{aligned}$$

$$\boxed{s_4 = s_4', s_3 \neq s_3'}$$

$$m_1 = \mathsf{Dec}(\mathsf{ct}) = m \cdot e(h, g)^{(\lambda_1 s_3 + s_4 \lambda_2)\langle \vec{x}, \vec{v} \rangle}$$

$$m_2 = \mathsf{Dec}(\mathsf{ct}') = m \cdot e(h, g)^{(\lambda_1 s_3' + s_4 \lambda_2)\langle \vec{x}, \vec{v} \rangle}$$

Decryption algorithm

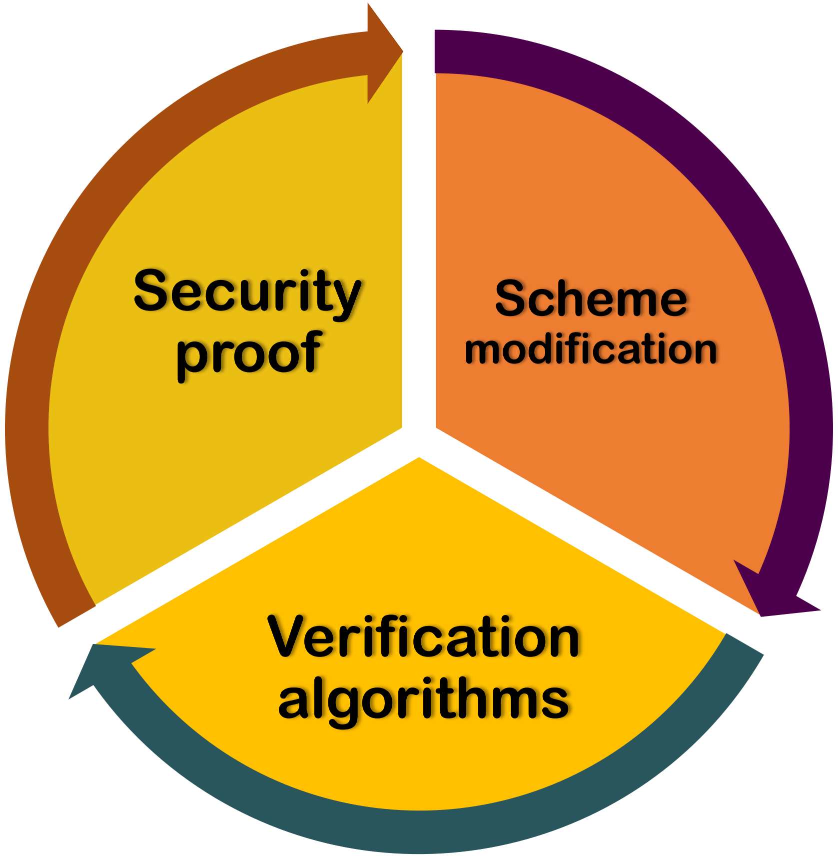
$$m_1 = m_2 : \quad \texttt{Output} \quad m_1$$

$$m_1 \neq m_2 : \quad \texttt{Output} \quad \perp$$

$$(\lambda_1 s_3 + \lambda_2 s_4) \neq (\lambda_1 s_3' + \lambda_2 s_4)$$

$$\Downarrow$$

$$m_1 = m_2 \Leftrightarrow \langle \vec{x}, \vec{v} \rangle = 0$$



Perfectly correct Inner Product Encryption

Efficiency:
- No need to solve the discret log
- Efficient for long message space

Security:
- Indistinguishable-secure
- Security based on DLin & BDDH
- Attribute-Hiding

Verifiable Inner Product Encryption

- No trusted party!

Verifiable Inner Product Encryption

Perfectly binding commitment scheme

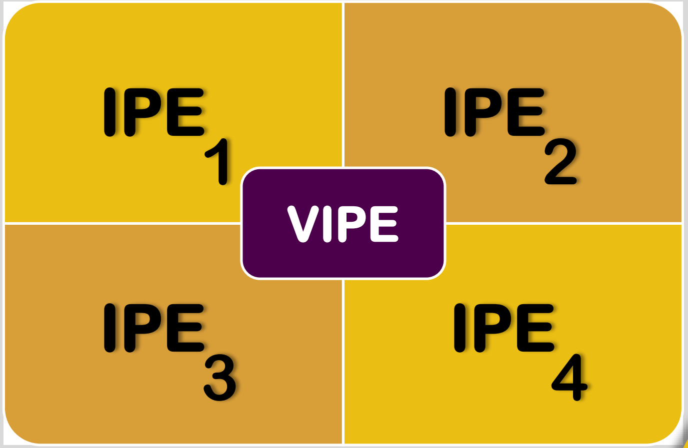
NIWI proofs: π

[BGJS16]

[BGJS16]: Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai. Veriable functional encryption. ASIACRYPT 2016

Verifiable Inner Product Encryption

Perfectly binding commitment scheme



NIWI proofs: π

$\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4$:

$\exists m : \forall i \in [4] : \mathsf{CT}_i = \mathsf{Enc}(\mathsf{MPK}_i, m; \mathsf{random}_i)$

OR :

$\exists i, j \in [4], \exists m :$

$\mathsf{CT}_i = \mathsf{Enc}(\mathsf{MPK}_i, m; \mathsf{random}_i), \mathsf{CT}_j = \mathsf{Enc}(\mathsf{MPK}_j, m; \mathsf{random}_j)$

AND :

$z_0 = \mathsf{Com}(\{c_i\}_{i\in[4]}; \mathsf{r}_0^{\mathsf{com}}) \wedge \; z_1 = \mathsf{Com}(0; \mathsf{r}_1^{\mathsf{com}})$

$\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4$:

$\exists m : \forall i \in [4] : \mathsf{CT}_i = \mathsf{Enc}(\mathsf{MPK}_i, m; \mathsf{random}_i)$

OR :

$\exists i, j \in [4], \exists m$:

$\mathsf{CT}_i = \mathsf{Enc}(\mathsf{MPK}_i, m; \mathsf{random}_i), \mathsf{CT}_j = \mathsf{Enc}(\mathsf{MPK}_j, m; \mathsf{random}_j)$

AND :

$z_0 = \mathsf{Com}(\{c_i\}_{i\in[4]}; \mathsf{r}_0^{\mathsf{com}}) \wedge z_1 = \mathsf{Com}(0; \mathsf{r}_1^{\mathsf{com}})$

1- Relations:

- $\mathsf{R}_{\mathsf{IP}}^{k,\mathsf{ct}}\left(\overbrace{((\mathsf{ct}_1, \mathsf{mpk}_1), \ldots, (\mathsf{ct}_k, \mathsf{mpk}_k))}^{x}, \overbrace{(\vec{x}, m, \mathsf{r}_1^{\mathsf{enc}}, \ldots, \mathsf{r}_k^{\mathsf{enc}})}^{w}\right) =$ $\mathsf{TRUE}, k \in [4] \iff \forall i \in [k]\ \mathsf{ct}_i = \mathsf{IP.Enc}(\mathsf{mpk}_i, \vec{x}, m; \mathsf{r}_i^{\mathsf{enc}})$
- $\mathsf{R}^{\mathsf{enc}}(x, w) = \mathsf{TRUE} \iff \mathsf{P}_1^{\mathsf{enc}}(x, w) \vee \mathsf{P}_2^{\mathsf{enc}}(x, w)$, with

$\mathsf{P}_1^{\mathsf{enc}}\left((\{c_i\}_{i\in[4]}, \{a_i\}_{i\in[4]}, z_0, z_1), (m, \vec{x}, \{\mathsf{r}_i^{\mathsf{enc}}\}_{i\in[4]}, i_1, i_2, \mathsf{r}_0^{\mathsf{com}}, \mathsf{r}_1^{\mathsf{com}})\right) =$

$\mathsf{TRUE} \iff \left(((c_1, a_1), \ldots, (c_4, a_4)), (\vec{x}, m, \{\mathsf{r}_i^{\mathsf{enc}}\})\right) \in \mathsf{R}_{\mathsf{IP}}^{4,\mathsf{ct}}$

$\mathsf{P}_2^{\mathsf{enc}}\left((\{c_i\}_{i\in[4]}, \{a_i\}_{i\in[4]}, z_0, z_1), (m, \vec{x}, \{\mathsf{r}_i^{\mathsf{enc}}\}_{i\in[4]}, i_1, i_2, \mathsf{r}_0^{\mathsf{com}}, \mathsf{r}_1^{\mathsf{com}})\right) =$

$\mathsf{TRUE} \iff$

$$\left(\begin{array}{c} i_1, i_2 \in [4] \wedge (i_1 \neq i_2) \wedge \left(\left((c_{i_1}, a_{i_1}), (c_{i_2}, a_{i_2})\right), (\vec{x}, m, \mathsf{r}_i^{\mathsf{enc}})\right) \in \mathsf{R}_{\mathsf{IP}}^{2,\mathsf{ct}} \\ \wedge\ z_0 = \mathsf{Com}(\{c_i\}_{i\in[4]}; \mathsf{r}_0^{\mathsf{com}}) \wedge z_1 = \mathsf{Com}(0; \mathsf{r}_1^{\mathsf{com}}) \end{array}\right)$$

Encryption Algorithm:

$\mathsf{IP.Enc}(\mathsf{MPK}, \vec{x}, m) \longrightarrow \mathsf{CT} = (\mathsf{ct}, \mathsf{ct}')$:

- $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and a message $m \in \mathbb{G}_T$
- Random elements: $s_1, \ldots s_4, s'_1, \ldots, s'_3 \leftarrow \mathbb{Z}_p^*$ such that $s_3 \neq s'_3$
- $\mathsf{ct}_1 = g^{s_2}, \;\; \mathsf{ct}_2 = h^{s_1}$
- $, \left\{ \begin{array}{ll} \mathsf{ct}_{3,i} = W_{1,i}^{s_1} \cdot F_{1,i}^{s_2} \cdot U_1^{x_i s_3} \quad , & \mathsf{ct}_{4,i} = W_{2,i}^{s_1} \cdot F_{2,i}^{s_2} \cdot U_2^{x_i s_3} \\ \mathsf{ct}_{5,i} = T_{1,i}^{s_1} \cdot H_{1,i}^{s_2} \cdot V_1^{x_i s_4} \quad , & \mathsf{ct}_{6,i} = T_{2,i}^{s_1} \cdot H_{2,i}^{s_2} \cdot V_2^{x_i s_4} \end{array} \right\}_{i \in [n]} ,$
- $\mathsf{ct}_7 = \mathbf{e}(g^{s_3}, g^{s_4}), \mathsf{ct}_8 = \Lambda^{-s_2} \cdot m.$

2- Variables

$$\mathcal{S}_1 = g^{s_1} \; , \; \mathcal{S}'_1 = g^{s'_1}$$
$$\mathcal{S}_3 = g^{s_3} \; , \; \mathcal{S}'_3 = g^{s'_3}$$
$$\mathcal{S}_4 = g^{s_4} \; , \; \mathcal{X}_i = g^{x_i}$$
$$\mathcal{U}_1 = U_1^{s_3} \; , \; \mathcal{U}_2 = U_2^{s_3}$$
$$\mathcal{V}_1 = V_1^{s_4} \; , \; \mathcal{V}_2 = V_2^{s_4}$$
$$\mathcal{U}_1 = U_1^{s'_3} \; , \; \mathcal{U}_2 = U_2^{s'_3}$$
$$\mathcal{K}_1 = K_1^{s_2} \; , \; \mathcal{K}'_1 = K_1^{s'_2}$$

3- System of equations:

$$
E_{\mathsf{ct}}: \begin{cases}
e(\mathsf{ct}_2, g) = e(h, \mathcal{S}_1), e(\mathsf{ct}'_2, g) = e(h, \mathcal{S}'_1), e(\hat{\mathsf{ct}}_2, \hat{g}) = e(\hat{h}, \hat{\mathcal{S}}_1), e(\hat{\mathsf{ct}}'_2, \hat{g}) = e(\hat{h}, \hat{\mathcal{S}}'_1) \\
e(\mathsf{ct}_{3,i}, g) \cdot e(F_{1,i}, \mathsf{ct}_1)^{-1} = e(W_{1,i}, \mathcal{S}_1) \cdot e(\mathcal{U}_1, \mathcal{X}_i) \\
e(\mathsf{ct}'_{3,i}, g) \cdot e(F_{1,i}, \mathsf{ct}'_1)^{-1} = e(W_{1,i}, \mathcal{S}'_1) \cdot e(\mathcal{U}'_1, \mathcal{X}_i) \\
e(\mathsf{ct}_{4,i}, g) \cdot e(F_{2,i}, \mathsf{ct}_1)^{-1} = e(W_{2,i}, \mathcal{S}_1) \cdot e(\mathcal{U}_2, \mathcal{X}_i) \\
e(\mathsf{ct}'_{4,i}, g) \cdot e(F_{2,i}, \mathsf{ct}'_1)^{-1} = e(W_{2,i}, \mathcal{S}'_1) \cdot e(\mathcal{U}'_2, \mathcal{X}_i) \\
e(\mathsf{ct}_{5,i}, g) \cdot e(H_{1,i}, \mathsf{ct}_2)^{-1} = e(T_{1,i}, \mathcal{S}_1) \cdot e(\mathcal{V}_1, \mathcal{X}_i) \\
e(\mathsf{ct}'_{5,i}, g) \cdot e(H_{1,i}, \mathsf{ct}'_2)^{-1} = e(T_{1,i}, \mathcal{S}'_1) \cdot e(\mathcal{V}'_1, \mathcal{X}_i) \\
e(\mathsf{ct}_{6,i}, g) \cdot e(H_{2,i}, \mathsf{ct}_2)^{-1} = e(T_{2,i}, \mathcal{S}_1) \cdot e(\mathcal{V}_2, \mathcal{X}_i) \\
e(\mathsf{ct}'_{6,i}, g) \cdot e(H_{2,i}, \mathsf{ct}'_2)^{-1} = e(T_{2,i}, \mathcal{S}'_1) \cdot e(\mathcal{V}'_2, \mathcal{X}_i) \\
\mathsf{ct}_7 = e(\mathcal{S}_3, \mathcal{S}_4), \mathsf{ct}'_7 = e(\mathcal{S}'_3, \mathcal{S}_4), \hat{\mathsf{ct}}_7 = e(\hat{\mathcal{S}}_3, \hat{\mathcal{S}}_4), \hat{\mathsf{ct}}'_7 = e(\hat{\mathcal{S}}'_3, \hat{\mathcal{S}}_4) \\
\mathsf{ct}_8^{-1} \cdot \mathsf{ct}'_8 = e(K_1, \mathcal{K}_2) \cdot e(K_1^{-1}, \mathcal{K}'_1), \hat{\mathsf{ct}}_8^{-1} \cdot \hat{\mathsf{ct}}'_8 = e(\hat{K}_1, \hat{\mathcal{K}}_2) \cdot e(\hat{K}_1^{-1}, \hat{\mathcal{K}}'_1) \\
e(\mathsf{ct}_1, K_1) = e(g, \mathcal{K}_1), e(\mathsf{ct}'_1, K_1) = e(g, \mathcal{K}'_1)
\end{cases}
$$

Groth-Sahai NIWI proof system: → **NIWI proofs: π**

[GS08]: Jens Groth and Amit Sahai. Ecient non-interactive proof systems for bilinear groups- EUROCRYPT 2008

Some applications of VIPE/IPE:

- Anonymous Identity-Based Encryption [KSW08]
- Predicate encryption schemes supporting polynomial evaluation
- Hidden-Vector Encryption
- Polynomial commitment scheme

[KSW08]: J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. EUROCRYPT 2008

Verifiable Polynomial commitment

Commitment Phase:

$$\mathsf{poly}(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}_p[X]$$

$$\vec{x} := (a_d, a_{d-1}, \ldots, a_1, a_0, 1) \in \mathbb{Z}_p^{d+2}$$

$$\mathsf{VIP.SetUp}(1^\lambda, d+2) \longrightarrow (\mathsf{MPK}, \mathsf{MSK})$$

$$\mathsf{VIP.Enc}(\mathsf{MPK}, \vec{x}) \rightarrow \mathsf{CT}$$

$$\mathsf{com} := (\mathsf{MPK}, \mathsf{CT})$$

Opening Phase:

$$(m, y), \qquad \mathsf{poly}(m) = y$$

$$\vec{v} = (m^d, m^{d-1}, \ldots, m, 1, -y),$$

$$\mathsf{TokGen}(\mathsf{MSK}, \vec{v}) \longrightarrow \mathsf{Tok}_{\vec{v}}$$

$$\begin{aligned}\langle \vec{x}, \vec{v} \rangle &= a_d m^d + \ldots + a_1 m + a_0 - y \\ &= \mathsf{poly}(m) - y\end{aligned}$$

$$\Rightarrow \mathsf{VIP.Dec}(\mathsf{CT}, \mathsf{Tok}_{\vec{v}}) = 0 \text{ iff } \mathsf{poly}(m) = y$$

Reference:

[Par11]: Jong Hwan Park. Inner-product encryption under standard assumptions.Des. Codes Cryptography, 58(3):235-257, 2011.

[BGJS16]: Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai. Verfiable functional encryption. In Proceedings, Part II, of the 22Nd International Conference on Advances in Cryptology | ASIACRYPT 2016

[GS08]: Jens Groth and Amit Sahai. Ecient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, Advances in Cryptology - EUROCRYPT 2008

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, Advances in Cryptology -CRYPTO 2006

[BSW11]: Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, TCC 2011: 8th Theory of Cryptography Conference

[KSW08]: Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Nigel P.Smart, editor, Advances in Cryptology - EUROCRYPT 2008

Thanks for your attention!

we're all in this together