Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts

Benoît Libert[1] **Thomas Peters**[2] **Chen Qian**[3]

[1]CNRS, Laboratoire LIP (CNRS, ENSL, U. Lyon, Inria, UCBL)
ENS de Lyon (France)

[2]FNRS & UCLouvain, ICTEAM (Belgium)

[3]Université de Rennes 1, IRISA, Rennes (France)

April 24, 2017

Contents

Contents

Structure-Preserving Encryption (informal)

Structure-Preserving Encryption (informal)

- Over groups $(\mathbb{G}, \hat{\mathbb{G}})$ with efficiently computable bilinear map

$$e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T.$$

Structure-Preserving Encryption (informal)

- Over groups $(\mathbb{G}, \hat{\mathbb{G}})$ with efficiently computable bilinear map

$$e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T.$$

- Ciphertexts and public keys are elements of the source group $\mathbb{G}$ or $\hat{\mathbb{G}}$.

Structure-Preserving Encryption (informal)

- Over groups $(\mathbb{G}, \hat{\mathbb{G}})$ with efficiently computable bilinear map

$$e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T.$$

- Ciphertexts and public keys are elements of the source group $\mathbb{G}$ or $\hat{\mathbb{G}}$.
- All cryptographic operations are group operation and pairing (e.g. no hash function).

Structure-Preserving Encryption (informal)

- Over groups $(\mathbb{G}, \hat{\mathbb{G}})$ with efficiently computable bilinear map

$$e : \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T.$$

- Ciphertexts and public keys are elements of the source group $\mathbb{G}$ or $\hat{\mathbb{G}}$.
- All cryptographic operations are group operation and pairing (e.g. no hash function).

Motivation

Smooth combination with Groth-Sahai (NIWI) proofs.
(witness extraction always possible)

Structure-Preserving Encryption (informal)

- Over groups $(\mathbb{G}, \hat{\mathbb{G}})$ with efficiently computable bilinear map

$$e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T.$$

- Ciphertexts and public keys are elements of the source group $\mathbb{G}$ or $\hat{\mathbb{G}}$.
- All cryptographic operations are group operation and pairing (e.g. no hash function).

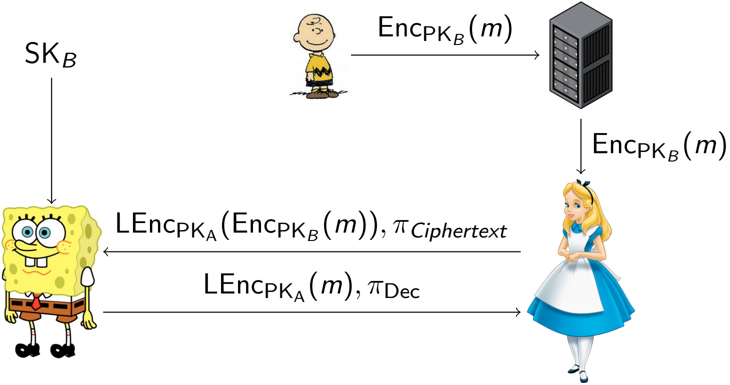
Motivation

Smooth combination with Groth-Sahai (NIWI) proofs.
(witness extraction always possible)

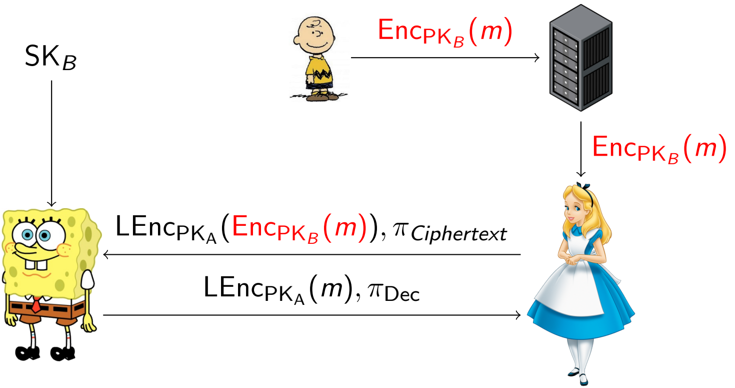
Example

1. Secure blind decryption [Gre11]
2. Oblivious 3rd parties protocols [CGH08]

Secure blind decryption [Gre11]



Secure blind decryption [Gre11]

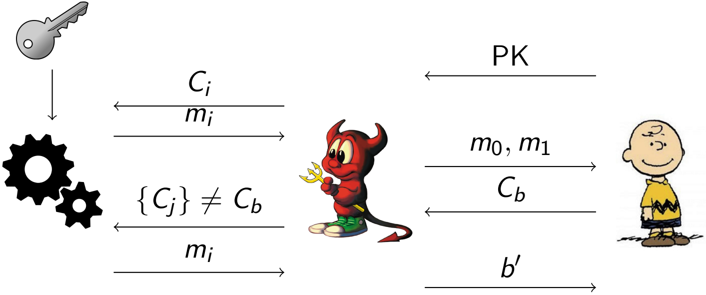


Public verifiability

- Allows adaptive OT with public contribution to database.
- Allows everyone to check the sanity of the database.
- Makes it possible to distribute senders.

Indistinguishable Chosen-Ciphertext security (IND-CCA)

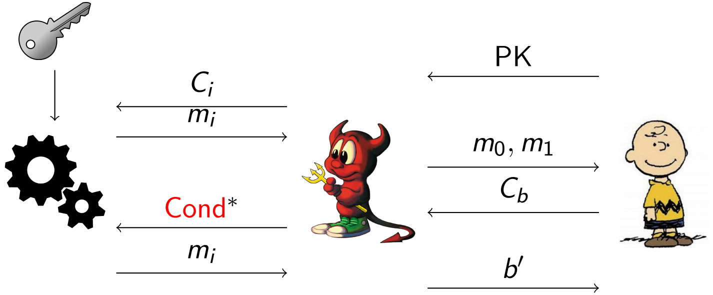
IND-CCA



Advantage: $Adv(\mathcal{A}) = |\Pr[b = b'] - \frac{1}{2}|.$

Replayable Chosen-Ciphertext security (RCCA)

RCCA



Advantage: $Adv(\mathcal{A}) = |\Pr[b = b'] - \frac{1}{2}|$.

- Motivation: Compatible with perfect rerandomizable encryption scheme.
- Optimal security notion for rerandomizable encryption schemes

* $Dec(k_d, \{C_j\}) \notin \{m_0, m_1\}$

Type-3 pairings and DDH (SXDH) assumption

Pairing

For three groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p and $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$.

$$e(A^\lambda, B) = e(A, B^\lambda) \qquad e(g, h) = 1 \text{ iff } g = 1 \vee h = 1$$

Type-3 pairings and DDH (SXDH) assumption

Pairing

For three groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p and $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$.

$$e(A^\lambda, B) = e(A, B^\lambda) \qquad e(g, h) = 1 \text{ iff } g = 1 \vee h = 1$$

- No computable isomorphism between $\mathbb{G}$ and $\hat{\mathbb{G}}$

Type-3 pairings and DDH (SXDH) assumption

Pairing

For three groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p and $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$.

$$e(A^\lambda, B) = e(A, B^\lambda) \qquad e(g, h) = 1 \text{ iff } g = 1 \vee h = 1$$

- No computable isomorphism between $\mathbb{G}$ and $\hat{\mathbb{G}}$
- Most efficient pairing configuration

Type-3 pairings and DDH (SXDH) assumption

Pairing

For three groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p and $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$.

$$e(A^\lambda, B) = e(A, B^\lambda) \qquad e(g, h) = 1 \text{ iff } g = 1 \vee h = 1$$

- No computable isomorphism between $\mathbb{G}$ and $\hat{\mathbb{G}}$
- Most efficient pairing configuration

DDH (SXDH) assumption

Let $g \in \mathbb{G}$ and $a, b, c \xleftarrow{R} \mathbb{Z}_p$

- Decisional Diffie-Hellman (DDH):

$$\{g, g^a, g^b, g^{ab}\} \approx_c \{g, g^a, g^b, g^c\}.$$

- Symmetric eXternal Diffie-Hellman (SXDH): DDH in $\mathbb{G}$ and $\hat{\mathbb{G}}$.

State of the art

Structure-Preserving Signatures

- [AHO10] Sign a message $\boldsymbol{M} = (m_1, m_2, \ldots, m_n) \in \hat{\mathbb{G}}^n$ with a signature $2\mathbb{G} + 5\hat{\mathbb{G}}$ under SXDH with asymmetric pairings.

State of the art

Structure-Preserving Signatures

- [AHO10] Sign a message $\boldsymbol{M} = (m_1, m_2, \ldots, m_n) \in \hat{\mathbb{G}}^n$ with a signature $2\mathbb{G} + 5\hat{\mathbb{G}}$ under SXDH with asymmetric pairings.

Structure-Preserving Public Key Encryption

- [CHK+11] Encryption of a message $m \in \mathbb{G}$ consists of $4\mathbb{G} + 1\mathbb{G}_T$ under DLIN with symmetric pairings; not publicly verifiable.
- [ADK+13] Structure-preserving publicly verifiable encryption with $321\mathbb{G}$ under DLIN.

State of the art

Structure-Preserving Signatures

- [AHO10] Sign a message $\boldsymbol{M} = (m_1, m_2, \ldots, m_n) \in \hat{\mathbb{G}}^n$ with a signature $2\mathbb{G} + 5\hat{\mathbb{G}}$ under SXDH with asymmetric pairings.

Structure-Preserving Public Key Encryption

- [CHK$^+$11] Encryption of a message $m \in \mathbb{G}$ consists of $4\mathbb{G} + 1\mathbb{G}_T$ under DLIN with symmetric pairings; not publicly verifiable.
- [ADK$^+$13] Structure-preserving publicly verifiable encryption with $321\mathbb{G}$ under DLIN.

Our goals

- Shorter ciphertexts under SXDH in asymmetric pairings (most efficient configuration)
- Public verifiability

Contents

Contributions

	Ciphertext Size[†]	Assumption	Security
[ADK$^+$13]	$321 \times \mathbb{G}$[‡]	DLIN	CCA
This work	$16 \times \mathbb{G} + 11 \times \hat{\mathbb{G}}$	SXDH	CCA
[CKLM12]	$93 \times \mathbb{G}$	DLIN	RCCA
[CKLM12]	$49 \times \mathbb{G} + 20 \times \hat{\mathbb{G}}$	SXDH	RCCA
This work[§]	$29 \times \mathbb{G} + 20 \times \hat{\mathbb{G}}$	SXDH	RCCA

[†] In the asymmetric setting, we assume $|\hat{\mathbb{G}}| \approx 2 \cdot |\mathbb{G}|$.

[‡] Only instantiable with symmetric pairing

[§] Instantiation of their generic construction with the more efficient tools to date.

Contents

Groth-Sahai Proof Systems

Only efficient NIZK proofs in the standard model for now.

Groth-Sahai Proof Systems

Only efficient NIZK proofs in the standard model for now.

Statement: Pairing Product Equation (PPE)

$$\prod_{j=1}^{n} e(\mathcal{A}_j, \mathcal{Y}_j) \prod_{i=1}^{m} e(\mathcal{X}_i, \mathcal{B}_i) \prod_{i=1}^{m} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{Y}_j)^{\gamma_{i,j}} = t_T$$

Statement: Multi-Exponentiation Equation

$$\prod_{j=1}^{n} \mathcal{A}_j^{y_j} \prod_{i=1}^{m} \mathcal{X}_i^{b_i} \prod_{i=1}^{m} \prod_{j=1}^{n} \mathcal{X}_i^{\gamma_{i,j} y_j} = t_T$$

Where for $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$

1. Variables: $\mathcal{X}_i$, $\mathcal{Y}_j$ and y_j.
2. Constants: $\mathcal{A}_j$, $\mathcal{B}_i$, t_T, $\gamma_{i,j}$ and b_i.

Groth-Sahai Proof Systems

A NIWI/NIZK proof system (Setup, Prove, Verify):

Groth-Sahai Proof Systems

A NIWI/NIZK proof system (Setup, Prove, Verify):

- Multi-exponentiation equation.

Groth-Sahai Proof Systems

A NIWI/NIZK proof system (Setup, Prove, Verify):

- Multi-exponentiation equation.
- Operate in two modes: Depending on the Common Reference String $CRS = (\boldsymbol{u}_1, \boldsymbol{u}_2, \hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2) \in \mathbb{G}^2 \times \mathbb{G}^2 \times \hat{\mathbb{G}}^2 \times \hat{\mathbb{G}}^2$.

Groth-Sahai Proof Systems

A NIWI/NIZK proof system (Setup, Prove, Verify):

- Multi-exponentiation equation.
- Operate in two modes: Depending on the Common Reference String $CRS = (\boldsymbol{u}_1, \boldsymbol{u}_2, \hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2) \in \mathbb{G}^2 \times \mathbb{G}^2 \times \hat{\mathbb{G}}^2 \times \hat{\mathbb{G}}^2$.
  - Perfect Zero-Knowledge (ZK) setting $\exists \zeta, \hat{\zeta} \in \mathbb{Z}_p$ s.t. $\boldsymbol{u}_2 = \boldsymbol{u}_1^{\zeta}$ and $\hat{\boldsymbol{u}}_2 = \hat{\boldsymbol{u}}_1^{\hat{\zeta}}$.
    1. Using $\zeta, \hat{\zeta}$, we can simulate a proof for false statement.
    2. Proofs using different valid witnesses are indistinguishable.

Groth-Sahai Proof Systems

A NIWI/NIZK proof system $(\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$:

- Multi-exponentiation equation.
- Operate in two modes: Depending on the Common Reference String $CRS = (\boldsymbol{u}_1, \boldsymbol{u}_2, \hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2) \in \mathbb{G}^2 \times \mathbb{G}^2 \times \hat{\mathbb{G}}^2 \times \hat{\mathbb{G}}^2$.
  - Perfect Zero-Knowledge (ZK) setting $\exists \zeta, \hat{\zeta} \in \mathbb{Z}_p$ s.t. $\boldsymbol{u}_2 = \boldsymbol{u}_1^{\zeta}$ and $\hat{\boldsymbol{u}}_2 = \hat{\boldsymbol{u}}_1^{\hat{\zeta}}$.
    1. Using $\zeta, \hat{\zeta}$, we can simulate a proof for false statement.
    2. Proofs using different valid witnesses are indistinguishable.
  - Perfect Soundness setting $(\boldsymbol{u}_1, \boldsymbol{u}_2)$ and $(\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2)$ are independent.
    1. Even unbounded adversaries cannot prove false statements.
    2. Trapdoor allows extracting witnesses from proofs.

Strictly Structure-Preserving Commitment [AKOT15]

SSPC $(\mathsf{Setup}, \mathsf{Commit}, \mathsf{Verify})$:

Strictly Structure-Preserving Commitment [AKOT15]

SSPC (Setup, Commit, Verify):

Properties

- Correctness: $\mathsf{Verify}(\mathsf{ck}, m, \mathsf{Commit}(\mathsf{ck}, m; \mathsf{open}), \mathsf{open}) = \mathsf{True}$.

Strictly Structure-Preserving Commitment [AKOT15]

SSPC (Setup, Commit, Verify):

Properties

- Correctness: $\mathsf{Verify}(\mathsf{ck}, m, \mathsf{Commit}(\mathsf{ck}, m; \mathsf{open}), \mathsf{open}) = \mathsf{True}$.
- Strictly Structure-Preserving: Commitment is also in $\mathbb{G}$ or $\hat{\mathbb{G}}$.

Strictly Structure-Preserving Commitment [AKOT15]

SSPC (Setup, Commit, Verify):

Properties

- Correctness: $\mathsf{Verify}(\mathsf{ck}, m, \mathsf{Commit}(\mathsf{ck}, m; \mathsf{open}), \mathsf{open}) = \mathsf{True}$.
- Strictly Structure-Preserving: Commitment is also in $\mathbb{G}$ or $\hat{\mathbb{G}}$.

  Remark: Binding impossible [AHO12], but weaker property suffices.

Strictly Structure-Preserving Commitment [AKOT15]

SSPC (Setup, Commit, Verify):

Properties

- Correctness: $\mathsf{Verify}(\mathsf{ck}, m, \mathsf{Commit}(\mathsf{ck}, m; \mathsf{open}), \mathsf{open}) = \mathsf{True}$.
- Strictly Structure-Preserving: Commitment is also in $\mathbb{G}$ or $\hat{\mathbb{G}}$.

  Remark: Binding impossible [AHO12], but weaker property suffices.

- Chosen-Message Target Collision Resistant (CM-TCR): Given $\mathsf{com}^*, m^*, \mathsf{open}^*$, hard to generate m s.t.

$$\mathsf{Verify}(\mathsf{ck}, m, \mathsf{com}^*, \mathsf{open}^*) = \mathsf{True} \wedge m \neq m^*$$

Strictly Structure-Preserving Commitment [AKOT15]

SSPC (Setup, Commit, Verify):

Properties

- Correctness: $\mathsf{Verify}(\mathsf{ck}, m, \mathsf{Commit}(\mathsf{ck}, m; \mathsf{open}), \mathsf{open}) = \mathsf{True}$.
- Strictly Structure-Preserving: Commitment is also in $\mathbb{G}$ or $\hat{\mathbb{G}}$.

  Remark: Binding impossible [AHO12], but weaker property suffices.

- Enhanced Chosen-Message Target Collision Resistant (ECM-TCR):
  Given $\mathsf{com}^*, m^*, \mathsf{open}^*$, hard to generate (m, open) s.t.

$$\mathsf{Verify}(\mathsf{ck}, m, \mathsf{com}^*, \mathsf{open}) = \mathsf{True} \land (m, \mathsf{open}) \neq (m^*, \mathsf{open}^*)$$

Contents

Construction ideas: Cramer-Shoup [CS02]

IND-CCA encryption: Cramer-Shoup

- Keys: PK $= g_1, g_2, X = g_1^{x_1} \cdot g_2^{x_2}$, SK $= x_1, x_2$.
- Ciphertext: $\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M \cdot X^r, g_1^r, g_2^r, \pi)$ where π is a proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ and $r \stackrel{R}{\leftarrow} \mathbb{Z}_q$.
- Decryption: $M = C_0/(C_1^{x_1} C_2^{x_2})$.

Proof intuitions

- Setup: PP_{GS} in perfect soundness setting.
- Challenge Ciphertext:

$$\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M_b \cdot X^r, g_1^r, g_2^r, \pi).$$

Construction ideas: Cramer-Shoup [CS02]

IND-CCA encryption: Cramer-Shoup

- Keys: PK $= g_1, g_2, X = g_1^{x_1} \cdot g_2^{x_2}$, SK $= x_1, x_2$.
- Ciphertext: $\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M \cdot X^r, g_1^r, g_2^r, \pi)$ where π is a proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ and $r \xleftarrow{R} \mathbb{Z}_q$.
- Decryption: $M = C_0/(C_1^{x_1} C_2^{x_2})$.

Proof intuitions

- Setup: PP_{GS} in perfect ZK setting.
- Challenge Ciphertext:

$$\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M_b \cdot X^r, g_1^r, g_2^r, \pi).$$

Construction ideas: Cramer-Shoup [CS02]

IND-CCA encryption: Cramer-Shoup

- Keys: $\mathrm{PK} = g_1, g_2, X = g_1^{x_1} \cdot g_2^{x_2}$, $\mathrm{SK} = x_1, x_2$.
- Ciphertext: $\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M \cdot X^r, g_1^r, g_2^r, \pi)$ where π is a proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ and $r \stackrel{R}{\leftarrow} \mathbb{Z}_q$.
- Decryption: $M = C_0/(C_1^{x_1} C_2^{x_2})$.

Proof intuitions

- Setup: PP_{GS} in perfect ZK setting.
- Challenge Ciphertext:

$$\boldsymbol{C} = (C_0, C_1, C_2, \pi_{sim}) = (M_b \cdot X^r, g_1^r, g_2^r, \pi_{sim}).$$

Construction ideas: Cramer-Shoup [CS02]

IND-CCA encryption: Cramer-Shoup

- Keys: $\mathrm{PK} = g_1, g_2, X = g_1^{x_1} \cdot g_2^{x_2}$, $\mathrm{SK} = x_1, x_2$.
- Ciphertext: $\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M \cdot X^r, g_1^r, g_2^r, \pi)$ where π is a proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ and $r \overset{R}{\leftarrow} \mathbb{Z}_q$.
- Decryption: $M = C_0/(C_1^{x_1} C_2^{x_2})$.

Proof intuitions

- Setup: PP_{GS} in perfect ZK setting.
- Challenge Ciphertext:

$$\boldsymbol{C} = (C_0, C_1, C_2, \pi_{sim}) = (M_b \cdot C_1^{x_1} C_2^{x_2}, g_1^r, g_2^r, \pi_{sim}).$$

Construction ideas: Cramer-Shoup [CS02]

IND-CCA encryption: Cramer-Shoup

- Keys: $\mathrm{PK} = g_1, g_2, X = g_1^{x_1} \cdot g_2^{x_2}$, $\mathrm{SK} = x_1, x_2$.
- Ciphertext: $\boldsymbol{C} = (C_0, C_1, C_2, \pi) = (M \cdot X^r, g_1^r, g_2^r, \pi)$ where π is a proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ and $r \xleftarrow{R} \mathbb{Z}_q$.
- Decryption: $M = C_0/(C_1^{x_1} C_2^{x_2})$.

Proof intuitions

- Setup: PP_{GS} in perfect ZK setting.
- Challenge Ciphertext:

$$\boldsymbol{C} = (C_0, C_1, C_2, \pi_{sim}) = (M_b \cdot C_1^{x_1} C_2^{x_2}, g_1^{r_1}, g_2^{r_2}, \pi_{sim}).$$

Construction ideas: All-but-one perfectly sound hash proof system [LY12]

ABO proof

Each proof is associated with a tag, prove with $\boldsymbol{u}_1 = \boldsymbol{u}_2 \cdot (1, \frac{1}{tag})$.

- Correct tag GS proof is in perfect soundness setting
- Wrong tag GS proof is in perfect ZK setting

Prove $log_{g_1}(C_1) = log_{g_2}(C_2)$

- Generate OTS keys $\mathsf{VK}_{OTS}, \mathsf{SK}_{OTS}$.
- Generate proof of $log_{g_1}(C_1) = log_{g_2}(C_2)$ with $tag = \mathsf{VK}_{OTS}$.

Difficulties

Problems

1. *OTS*.VK has several group elements.

Difficulties

Problems

1. OTS.VK has several group elements.
   - Hash verification key OTS.VK. (No for the structure-preserving)

Difficulties

Problems

1. *OTS*.VK has several group elements.
   - Hash verification key *OTS*.VK. (No for the structure-preserving)
   - Strictly structure-perserving commitment.
     (Binding impossible [AHO12])

Difficulties

Problems

1. *OTS*.VK has several group elements.
   - Hash verification key *OTS*.VK. (No for the structure-preserving)
   - Strictly structure-perserving commitment.
     (Binding impossible [AHO12])
   - Solution: Enhanced Chosen-Message Target Collision Resistant (ECM-TCR) suffices.

Difficulties

Problems

1. OTS.VK has several group elements.
   - Hash verification key OTS.VK. (No for the structure-preserving)
   - Strictly structure-perserving commitment. (Binding impossible [AHO12])
   - Solution: Enhanced Chosen-Message Target Collision Resistant (ECM-TCR) suffices.
2. Commitement scheme's ck and com are in $\mathbb{G}$ and $\hat{\mathbb{G}}$.

Difficulties

Problems

1. *OTS*.VK has several group elements.
   - Hash verification key *OTS*.VK. (No for the structure-preserving)
   - Strictly structure-perserving commitment. (Binding impossible [AHO12])
   - Solution: Enhanced Chosen-Message Target Collision Resistant (ECM-TCR) suffices.
2. Commitement scheme's ck and com are in $\mathbb{G}$ and $\hat{\mathbb{G}}$.
   - Solution: No need to sign the commitment. (Not trivial to prove)

Structure-Preserving Publicly Verifiable Encryption

- $\mathsf{SK} = (x_1, x_2)$.
- $\mathsf{PK} = (g_1, g_2, X = g_1^{x_1} g_2^{x_2}, \mathsf{PP}_{SPC}, \mathbf{ck}, CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2) \in \hat{\mathbb{G}}^2 \times \hat{\mathbb{G}}^2)$.

where $(g_1, g_2) \in \mathbb{G}^2$, $(x_1, x_2) \in \mathbb{Z}_p^2$ and $\exists \rho_u \in \mathbb{Z}_p$ such that $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Details of the Encryption algorithm

- Generate $\boldsymbol{C} = (C_0, C_1, C_2) = (M \cdot X^\theta, g_1^\theta, g_2^\theta)$.
- $\mathsf{OTS.KeyGen}(\mathsf{PP}) \rightarrow (\mathsf{SSK}, \mathsf{SVK})$.
- $\mathsf{Commit}(\mathbf{ck}, \mathsf{SVK}) \rightarrow (\hat{\mathsf{com}}, \mathsf{open})$.
- Compute $\hat{\boldsymbol{u}}_{\hat{\mathsf{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\mathsf{com}}) \in \hat{\mathbb{G}}^2$.
- $\mathsf{Prove}(CRS_{\hat{\mathsf{com}}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\mathsf{com}}), (C_1, C_2), \theta) \rightarrow \pi$ of statement
$$\exists \chi \text{ s.t. } (C_1, C_2) = (g_1^\chi, g_2^\chi).$$
- $\mathsf{OTS.Sign}(\mathsf{SSK}, (\boldsymbol{C}, \pi)) \rightarrow \sigma$.
- Output the ciphertext $(\boldsymbol{C}, \pi, \mathsf{SVK}, \hat{\mathsf{com}}, \mathsf{open}, \sigma) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2)$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot X^{\theta^*}, g_1^{\theta^*}, g_2^{\theta^*})$.
- OTS.KeyGen(PP) $\rightarrow$ (SSK*, SVK*).
- Commit(**ck**, SVK*) $\rightarrow$ (côm*, open*).
- Compute $\hat{\boldsymbol{u}}_{\text{côm}} = \hat{\boldsymbol{u}}_2 \cdot (1, \text{côm}^*) \in \hat{\mathbb{G}}^2$.
- Prove($CRS_{\text{côm}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\text{côm}}), x = (C_1^*, C_2^*), w = \theta^*) \rightarrow \pi^*$ of the statement "$\exists \chi$ such that $(C_1^*, C_2^*) = (g_1^{\chi}, g_2^{\chi})$".
- OTS.Sign(SSK*, $(\boldsymbol{C}^*, \pi^*)$) $\rightarrow \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \text{SVK}^*, \text{côm}^*, \text{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2)$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot X^{\theta^*}, g_1^{\theta^*}, g_2^{\theta^*})$.
- $\mathsf{OTS.KeyGen}(\mathsf{PP}) \rightarrow (\mathsf{SSK}^*, \mathsf{SVK}^*)$. Done at beginning
- $\mathsf{Commit}(\mathbf{ck}, \mathsf{SVK}^*) \rightarrow (\hat{\mathsf{com}}^*, \mathsf{open}^*)$. Done at beginning
- Compute $\hat{\boldsymbol{u}}_{\hat{\mathsf{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\mathsf{com}}^*) \in \hat{\mathbb{G}}^2$.
- $\mathsf{Prove}(CRS_{\hat{\mathsf{com}}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\hat{\mathsf{com}}}), x = (C_1^*, C_2^*), w = \theta^*) \rightarrow \pi^*$ of the statement "$\exists \chi$ such that $(C_1^*, C_2^*) = (g_1^{\chi}, g_2^{\chi})$".
- $\mathsf{OTS.Sign}(\mathsf{SSK}^*, (\boldsymbol{C}^*, \pi^*)) \rightarrow \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \mathsf{SVK}^*, \hat{\mathsf{com}}^*, \mathsf{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- $\mathsf{OTS.KeyGen}(\mathsf{PP}) \rightarrow (\mathsf{SSK}^*, \mathsf{SVK}^*)$.
- $\mathsf{Commit}(\mathsf{ck}, \mathsf{SVK}^*) \rightarrow (\hat{\mathsf{com}}^*, \mathsf{open}^*)$.
- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2)$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot X^{\theta^*}, g_1^{\theta^*}, g_2^{\theta^*})$.
- Compute $\hat{\boldsymbol{u}}_{\hat{\mathsf{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\mathsf{com}}^*) \in \hat{\mathbb{G}}^2$.
- Prove$(CRS_{\hat{\mathsf{com}}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\hat{\mathsf{com}}}), x = (C_1^*, C_2^*), w = \theta^*) \rightarrow \pi^*$ of the statement "$\exists \chi$ such that $(C_1^*, C_2^*) = (g_1^{\chi}, g_2^{\chi})$".
- $\mathsf{OTS.Sign}(\mathsf{SSK}^*, (\boldsymbol{C}^*, \pi^*)) \rightarrow \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \mathsf{SVK}^*, \hat{\mathsf{com}}^*, \mathsf{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- OTS.KeyGen(PP) $\rightarrow$ (SSK*, SVK*).
- Commit(ck, SVK*) $\rightarrow$ ($\hat{\text{com}}^*$, open*).
- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2 \cdot (1, \frac{1}{\hat{\text{com}}^*}))$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot X^{\theta^*}, g_1^{\theta^*}, g_2^{\theta^*})$.
- Compute $\hat{\boldsymbol{u}}_{\hat{\text{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\text{com}}^*) \in \hat{\mathbb{G}}^2$.
- Prove($CRS_{\hat{\text{com}}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\hat{\text{com}}}), x = (C_1^*, C_2^*), w = \theta^*) \rightarrow \pi^*$ of the statement "$\exists \chi$ such that $(C_1^*, C_2^*) = (g_1^{\chi}, g_2^{\chi})$".
- OTS.Sign(SSK*, ($\boldsymbol{C}^*, \pi^*$)) $\rightarrow \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \text{SVK}^*, \hat{\text{com}}^*, \text{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- $\mathsf{OTS.KeyGen}(\mathsf{PP}) \rightarrow (\mathsf{SSK}^*, \mathsf{SVK}^*)$.
- $\mathsf{Commit}(\mathsf{ck}, \mathsf{SVK}^*) \rightarrow (\hat{\mathsf{com}}^*, \mathsf{open}^*)$.
- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2 \cdot (1, \frac{1}{\hat{\mathsf{com}}^*}))$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot C_1^{x_1} \cdot C_2^{x_2}, g_1^{\theta^*}, g_2^{\theta^*})$.
- Compute $\hat{\boldsymbol{u}}_{\hat{\mathsf{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\mathsf{com}}^*) \in \hat{\mathbb{G}}^2$.
- $\mathsf{Prove}(CRS_{\hat{\mathsf{com}}} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_{\hat{\mathsf{com}}}), x = (C_1^*, C_2^*), w = \theta^*) \rightarrow \pi^*$ of the statement "$\exists \chi$ such that $(C_1^*, C_2^*) = (g_1^{\chi}, g_2^{\chi})$".
- $\mathsf{OTS.Sign}(\mathsf{SSK}^*, (\boldsymbol{C}^*, \pi^*)) \rightarrow \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \mathsf{SVK}^*, \hat{\mathsf{com}}^*, \mathsf{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Proof intuition

Setup

- $\mathsf{OTS.KeyGen}(\mathsf{PP}) \to (\mathsf{SSK}^*, \mathsf{SVK}^*)$.
- $\mathsf{Commit}(\mathsf{ck}, \mathsf{SVK}^*) \to (\hat{\mathsf{com}}^*, \mathsf{open}^*)$.
- $CRS_{GS} = (\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2 \cdot (1, \frac{1}{\hat{\mathsf{com}}^*}))$ with $\hat{\boldsymbol{u}}_1 = \hat{\boldsymbol{u}}_2^{\rho_u}$.

Encryption

- Generate $\boldsymbol{C}^* = (C_0^*, C_1^*, C_2^*) = (M_b \cdot C_1^{x_1} \cdot C_2^{x_2}, g_1^{\theta_1}, g_2^{\theta_2})$.
- Compute $\hat{\boldsymbol{u}}_{\hat{\mathsf{com}}} = \hat{\boldsymbol{u}}_2 \cdot (1, \hat{\mathsf{com}}^*) \in \hat{\mathbb{G}}^2$.
- Simulate proof of the false statement $log_{g_1}(C_1) = log_{g_2}(C_2)$ using ρ_u.
- $\mathsf{OTS.Sign}(\mathsf{SSK}^*, (\boldsymbol{C}^*, \pi^*)) \to \sigma^*$. **(No need to sign commitments)**
- Output the ciphertext $(\boldsymbol{C}^*, \pi^*, \mathsf{SVK}^*, \hat{\mathsf{com}}^*, \mathsf{open}^*, \sigma^*) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$.

Conclusion

- Publicly verifiable IND-CCA encryption: $321\mathbb{G} \to 16\mathbb{G} + 11\hat{\mathbb{G}}$.
- Publicly verifiable RCCA rerandomizable encryption: $93\mathbb{G}/49\mathbb{G} + 20\hat{\mathbb{G}} \to 29\mathbb{G} + 20\hat{\mathbb{G}}$.

Conclusion

- Publicly verifiable IND-CCA encryption: $321\mathbb{G} \rightarrow 16\mathbb{G} + 11\hat{\mathbb{G}}$.
- Publicly verifiable RCCA rerandomizable encryption: $93\mathbb{G}/49\mathbb{G} + 20\hat{\mathbb{G}} \rightarrow 29\mathbb{G} + 20\hat{\mathbb{G}}$.

Future Works

- Smaller ciphertext for rerandomization encryption scheme.
- More general malleability (e.g. Linear Homomorphism, HCCA security)?

Conclusion

- Publicly verifiable IND-CCA encryption: $321\mathbb{G} \to 16\mathbb{G} + 11\hat{\mathbb{G}}$.
- Publicly verifiable RCCA rerandomizable encryption: $93\mathbb{G}/49\mathbb{G} + 20\hat{\mathbb{G}} \to 29\mathbb{G} + 20\hat{\mathbb{G}}$.

Future Works

- Smaller ciphertext for rerandomization encryption scheme.
- More general malleability (e.g. Linear Homomorphism, HCCA security)?

References I

Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo.
Tagged one-time signatures: Tight security and optimal tag size.
In Kaoru Kurosawa and Goichiro Hanaoka, editors, Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings, volume 7778 of Lecture Notes in Computer Science, pages 312–331. Springer, 2013.

Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo.
Signing on elements in bilinear groups for modular protocol design.
IACR Cryptology ePrint Archive, 2010:133, 2010.

Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo.
Group to group commitments do not shrink.
In EUROCRYPT, volume 7237 of Lecture Notes in Computer Science, pages 301–317. Springer, 2012.

Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi.
Fully structure-preserving signatures and shrinking commitments.
In EUROCRYPT (2), volume 9057 of Lecture Notes in Computer Science, pages 35–65. Springer, 2015.

Jan Camenisch, Thomas Groß, and Thomas S. Heydt-Benjamin.
Rethinking accountable privacy supporting services: extended abstract.
In Digital Identity Management, pages 1–8. ACM, 2008.

Jan Camenisch, Kristiyan Haralambiev, Markulf Kohlweiss, Jorn Lapon, and Vincent Naessens.
Structure preserving CCA secure encryption and applications.
In ASIACRYPT, volume 7073 of Lecture Notes in Computer Science, pages 89–106. Springer, 2011.

Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn.
Malleable proof systems and applications.
In EUROCRYPT, volume 7237 of Lecture Notes in Computer Science, pages 281–300. Springer, 2012.

References II

Ronald Cramer and Victor Shoup.
Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption.
In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 45–64. Springer, 2002.

Matthew Green.
Secure blind decryption.
In Public Key Cryptography, volume 6571 of Lecture Notes in Computer Science, pages 265–282. Springer, 2011.

Benoît Libert and Moti Yung.
Non-interactive cca-secure threshold cryptosystems with adaptive security: New framework and constructions.
In TCC, volume 7194 of Lecture Notes in Computer Science, pages 75–93. Springer, 2012.