Structure-Preserving Cryptography

(Invited talk in Asiacrypt 2015)

Masayuki ABE

NTT Secure Platform Laboratories

Modular Design in General

(mostly from Wikipeida)

Modular design:
A design approach that subdivides a system into smaller parts that can be independently created and then used in different systems.

Modular Design in General

Benefit:

Reduction in cost

less customization,

shorter learning time

Modular Design in General

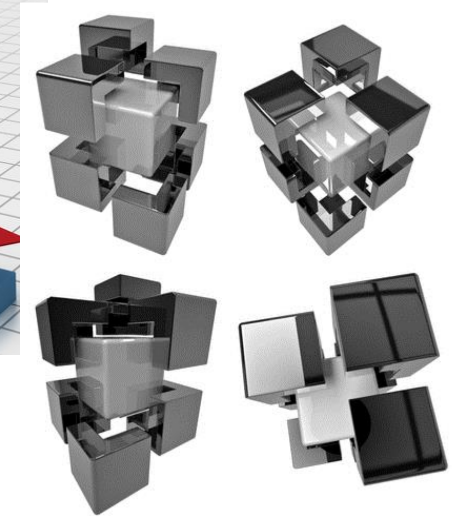
Benefit:

Reduction in cost

less customization,

shorter learning time

Flexibility in design



Modular Design in General

Benefit:

Reduction in cost

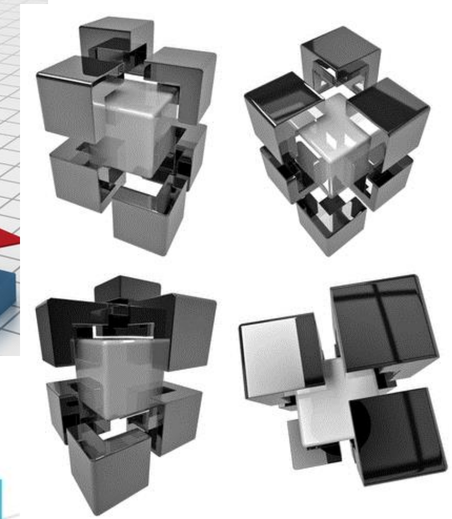
less customization,

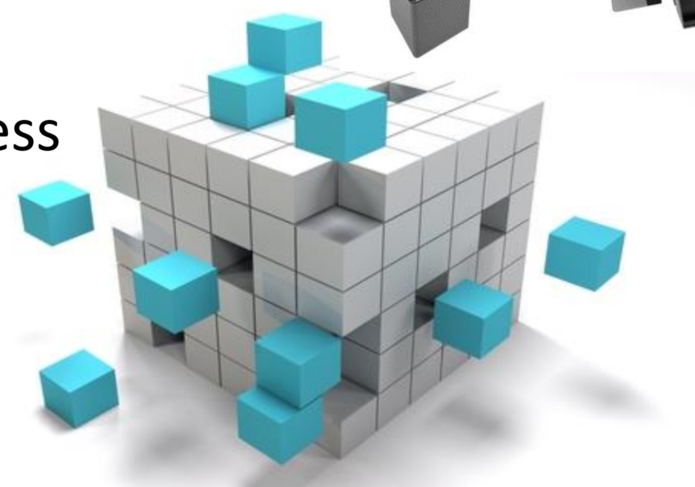
shorter learning time

Flexibility in design

Augmentation

adding new solution by merely plugging in a new module, making the manufacturing process more adaptive to change

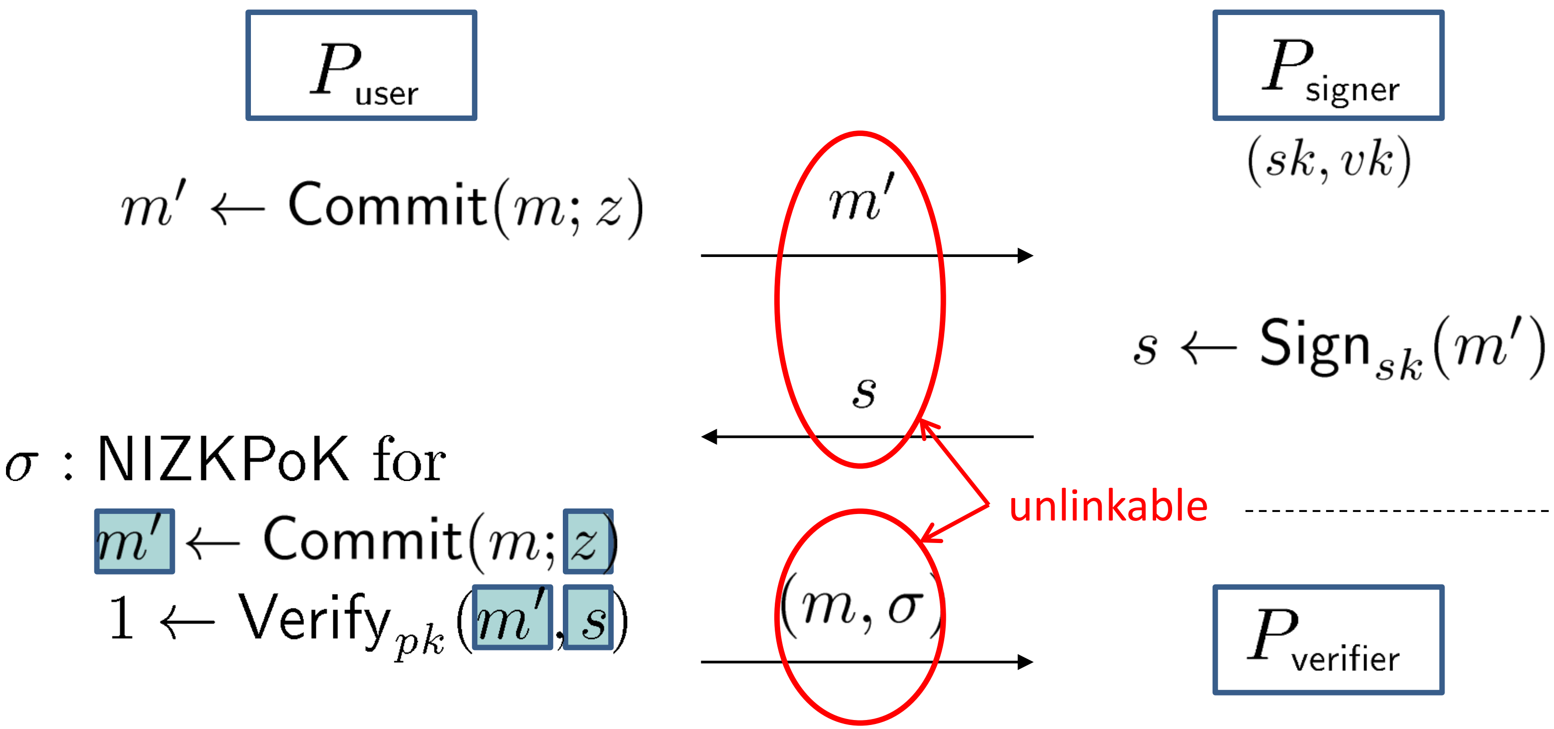




Modular Design in General

Downside:
Low quality modular systems are not optimized for performance. This is usually due to the cost of putting up interfaces between modules.

Blind Signatures [Fis06]



Generic Construction in Cryptography

Generic construction in cryptography is a design approach that constructs a cryptographic system by combining smaller and abstract cryptographic primitives that conform to independent security notions.

Benefit:

Reduction in cost: Simper, easy-to-follow security proofs.

Flexibility in design: Off-the-shelf building blocks. Choice of assumptions.

Augmentation: New solution by plugging in a new building block

Generic Construction in Cryptography

Generic construction in cryptography is a design approach that constructs a cryptographic system by combining smaller and abstract cryptographic primitives that conform to independent security notions.

MODULALITY

SECURITY

BENEFITS
Easy-to-read security proofs, choice of assumptions, etc.

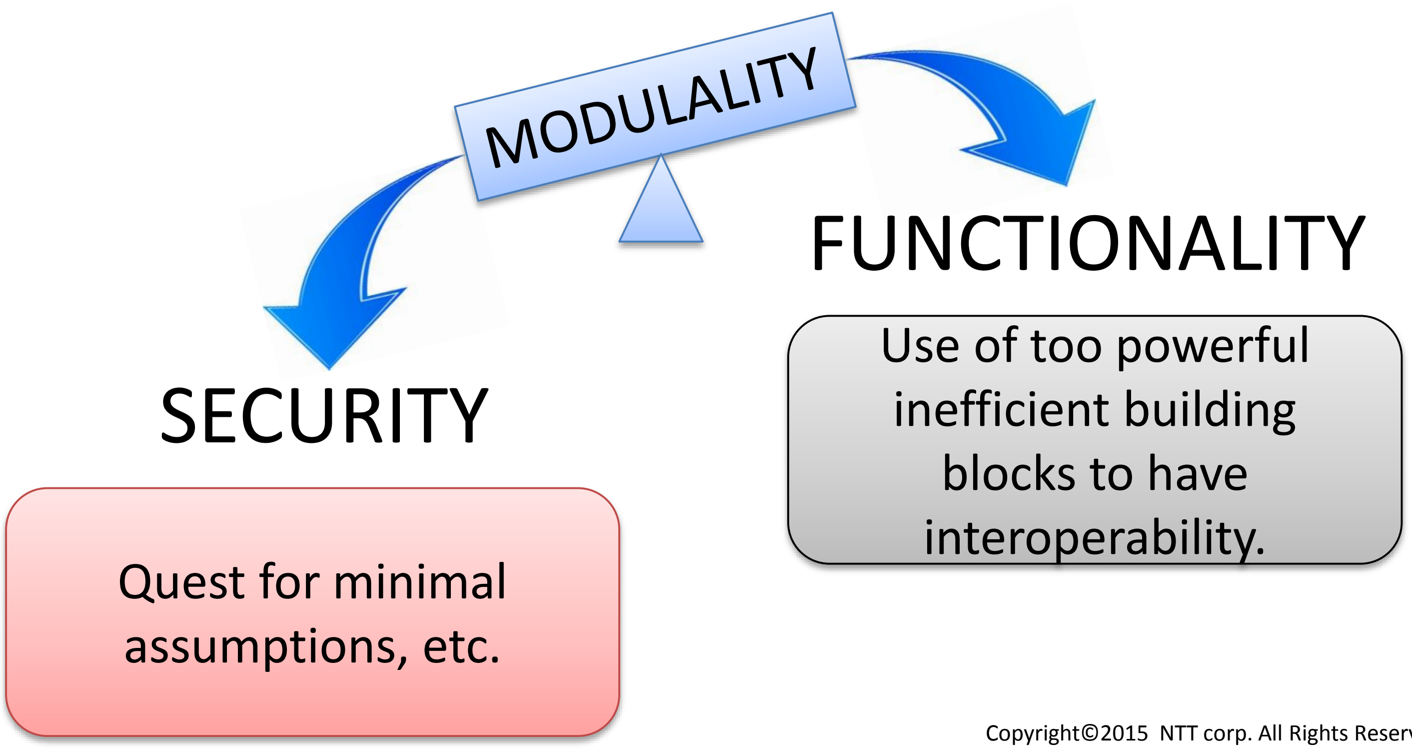
FUNCTIONALITY

BENEFITS
Less learning time, use of existing schemes, efficiency improvement, etc.

Generic Construction in Cryptography

Downside:

Mainly used to show feasibility under minimal assumptions, or to show the underlying ideas. Often hard or ignored to find an efficient instantiation.



Structure-Preserving Cryptography

Structure-Preserving Cryptography is a framework for efficiently instantiating generic constructions using bilinear groups as a common ground for building blocks.

Bilinear Groups

$$\Lambda = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G_1, G_2)$$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$: groups of prime order p

$G_1, G_2, e(G_1, G_2)$ generate $\mathbb{G}_1, \mathbb{G}_2,$ and $\mathbb{G}_T$, respectively

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

$$^\forall X \in \mathbb{G}_1, ^\forall Y \in \mathbb{G}_2, ^\forall a, b \in \mathbb{Z}_p,\ e(X^a, Y^b) = e(X, Y)^{ab}$$

Structure-Preserving Schemes

A cryptographic scheme is structure-preserving if:

- (Group elements as interface) All public objects such as public-keys, messages, commitments, etc, merely consist of elements in $\mathbb{G}_1$ and $\mathbb{G}_2$.

- (Correctness via PPEs) Verifying relations of interest can be done only by group operations, membership testing, and evaluating pairing product equations of the form

$$\prod_{i}^{n} e(A_i, Y_i) \prod_{i}^{m} e(X_i, B_i) \prod_{i}^{m} \prod_{j}^{n} e(X_i, Y_j)^{c_{ij}} = T.$$

where c_{ij} and T are system-defined constants.

Structure-Preserving Schemes

A cryptographic scheme is structure-preserving if:

- (Group elements as interface) All public c
keys, messages, commitments, etc, merely
in $\mathbb{G}_1$ and $\mathbb{G}_2$.

- (Correctness via PPEs) Verifying relations of interest can be done only by group operations, membership testing, and evaluating pairing product equations of the form

$$\prod_{i}^{n} e(A_i, Y_i) \prod_{i}^{m} e(X_i, B_i) \prod_{i}^{m} \prod_{j}^{n} e(X_i, Y_j)^{c_{ij}} = T.$$

where c_{ij} and T are system-defined constants.

Aim for high interoperability and use of efficient Groth-Sahai proof system.

Structure-Preserving Schemes

A cryptographic scheme is structure-preserving if:

- (Group elements as interface) All public c… keys, messages, commitments, etc, merely … in $\mathbb{G}_1$ and $\mathbb{G}_2$.

- (Correctness via PPEs) Verifying relations of interest … n be done only by group operations, membershi… evaluating pairing product equations of the …

$$\prod_{i}^{n} e(A_i, Y_i) \prod_{i}^{m} e(X_i, B_i) \prod_{i}^{m} \prod_{j}^{n} e(X_i, \ldots$$

where c_{ij} and T are system-defined constants.

Aim for high interoperability and use of efficient Groth-Sahai proof system.

Constraints that make it hard to build efficient building blocks.

Difficulty in Designing SP Primitives

Example: Signature Scheme

$$\begin{tikzcd}
 & \mathbb{Z}_p \arrow[r, "\text{One-Way}"] & \mathbb{G} \arrow[r, "\text{One-Way}"] & \mathbb{G}_T \\
\text{Key generation:} & sk \arrow[r] & vk & \\
\text{Signing:} & m, r, sk \arrow[r] & \sigma & \\
\text{Verification:} & m \arrow[dr] & vk & \\
 & & \sigma &
\end{tikzcd}$$

Must find a one-way structure within the same group (without hash functions).

(In)Feasibility of SP Primitives

Feasible	• NIWI, NIZK, CCA PKE, Non-shrinking Commitments, Shrinking TCR Commitments, (One-time/ Homormophic/ Automorphic/ Equivalence Class) Signatures, Oblivious Transfer
Unknown	• ID-based Encryption, Functional Encryption, …
Infeasible	• Unique signatures, (V)PRF, Deterministic Encryption, Shrinking CR Commitments

Known Structure-Preserving Primitives

Proof Systems

- NIWI, NIZK [Gro06, GS08, GSW10, EG14]
- Properties of GS-proofs [BCCKLS09,Fuc11,CKLM12]
- Simulation-Sound NIZK [Gro06, CCS08, HJ12]

Signatures

- Constructions [Gro06, GH08, CLY09, AFGHO10, AHO10, AGHO11, CK11, ACD+12, CDH12, CK12, ADKNO13, LPJY13, ALP13, AGOTia14, AGOTib14, HS14, LJ14, CM14, BFFSST15, LPY15, AKOTi15, KPW15, Groth15]
- Bounds [AGHO11, AGO11, AGOTia14, AGOTib14]

Public-Key Encryption

- CPA [ElG85,HK07,Sha07]
- CCA2 [CHKLN11]

Commitments

- Constructions [Gro09, AFGHO10, AHO10, AHO12, AKOTi15]
- Bounds [AHO12]

Oblivious Transfer

- Construction [DDvMNP15]

Known Structure-Preserving Primitives

Proof Systems

- NIWI, NIZK [Gro06, GS08]
- Properties of GS-proofs [BCCKLS09,Fuc11,CKLM12]
- Simulation-Sound NIZK [Gro06, CCS08, HJ12]

Signatures

- Constructions [Gro06, GH08, CLY09, AFGHO10, AHO10, AGHO11, CK11, ACD+12, CDH12, CK12, ADKNO13, LPJY13, ALP13, AGOTia14, AGOTib14, HS14, LJ14, CM14, BFFSST15, LPY15, AKOTi15, KPW15, Groth15]
- Bounds [AGHO11, AGO11, AGOTia14, AGOTib14]

Public-Key Encryption

- CPA [ElG85,HK07,Sha07]
- CCA2 [CHKLN11]

Commitments

- Constructions [Gro09, AFGHO10, AHO10, AHO12, AKOTi15]
- Bounds [AHO12]

Oblivious Transfer

- Construction [DDvMNP15]

Structure-Preserving Signatures

- The public keys, messages, and signatures consist of elements of $\mathbb{G}_1$ and $\mathbb{G}_2$, and
- signature verification is done only by group operations, membership testing, and evaluation of pairing product equations.

Advances of Research on SPS

($|\mathrm{msg}| = k$, 2^x sigs.)

Scheme	Assumptions	Signature Size	Group Type	Notes
[Fuc09]	q-DHSDH	$21k + 11$	I	
[CLY09]	q-HSDH, Flex-DH, DLIN	$9k + 4$	I	
[AFGHO10]	q-SFP	7	Any	Unilateral
[AGHO11]	q-type, SXDH	6	III	
		4	III	Unilateral
	interactive, SXDH	3	III	Unilateral
[AGOTi$_a$14]	interactive	3	Any	$k = 1$
[AGOTi$_b$14]	interactive	3	III	$k = 1$
	interactive	2	II	$k = 1$
[Gro06]	DLIN	$\mathcal{O}(k)$	I	
[CK12]	DLIN	$24k + 100 + 9x$	I	
	SXDH, RCDH	$18k + 77 + 6x$	III	Unilateral
[CDH12]	DLIN	$6k + 53$	I	
[ACDKNO12]	DLIN	17	I	
	SXDH, XDLIN	14	III	
		11	III	Unilateral
[ADKNO13]	DLIN	14	I	
[KPW15]	2-LIN	10	I	
	SXDH	7	III	Unilateral

Static v.s. q-Type Assumptions

Static assumptions

- Simple as DLIN, SXDH
- Widely used.

Security of [ADKNO13, KPW15] is reduced to static assumptions with loss factor of $1/q$ and $1/q^2$

Security of [AFGHO10, AGHO11] is tightly reduced to q-type assumptions.

q-Type Assumptions

- Consists of huge number of group elements
- Some are widely used, some are just ad-hoc.

Static v.s. q-Type Assumptions

Static Assumptions

- Simple as DLIN, SXDH
- Widely used.
- Tight generic security

$$\mathrm{CDH}\colon \mathcal{O}(\ell^2)/|\mathbb{G}|$$

Any generic adversary after ℓ steps wins at most with this probability.

q-Type Assumptions

- Consist of huge number of group elements
- Some are widely used, some are just ad-hoc.
- Loose generic security?

$$q\text{-SDH}\colon \mathcal{O}(q\,\ell^2)/|\mathbb{G}|$$

$$\text{Given: } G,\ G^x,\ G^{x^2},\ \ldots,\ G^{x^q}$$
$$\text{Find: } G^{\frac{1}{x+c}},\ c$$

q-Type Assumption: Example

Simultaneous Flexible Pairing Assumption (SFP) [AFGHO10]

Given: $(A, A', B, B', G_z, H_z, G_r, H_u) \in \mathbb{G}^8$ and

$(Z_i, R_i, S_i, T_i, U_i, V_i, W_i) \in \mathbb{G}^7$ for $i = 1, \ldots, q$ constrained that

$$e(A, A') = e(G_z, Z_i)\, e(G_r, R_i)\, e(S_i, T_i)$$

$$e(B, B') = e(H_z, Z_i)\, e(H_u, U_i)\, e(V_i, W_i)$$

Find: (Z, R, S, T, U, V, W) with $Z \notin \{Z_1, \ldots, Z_q\}$ and $Z \neq 1$

Tight Generic Hardness of SFP

Theorem.[AGFHO15] Any generic algorithm $\mathcal{A}$ performing up to ℓ group operations and pairings solves the q-SFP problem with probability at most $\mathcal{O}(\ell^2 + q^2)/|\mathbb{G}|$.

Tight Generic Hardness of SFP

Theorem.[AGFHO15] Any generic algorithm $\mathcal{A}$ performing up to ℓ group operations and pairings solves the q-SFP problem with probability at most $\mathcal{O}(\ell^2 + q^2)/|\mathbb{G}|$.

CDH: $\mathcal{O}(\ell^2)/|\mathbb{G}|$

[Sho97]

q-SDH: $\mathcal{O}(q\,\ell^2)/|\mathbb{G}|$

[BB04,Che06]

Tight Generic Hardness of SFP

Theorem.[AGFHO15] Any generic algorithm $\mathcal{A}$ performing up to ℓ group operations and pairings solves the q-SFP problem with probability at most $\mathcal{O}(\ell^2 + q^2)/|\mathbb{G}|$.

Proof intuition:
Recall that reference ansers satisfy

$$e(A, A') = e(G_z, Z_i)\, e(G_r, R_i)\, e(S_i, T_i)$$
$$e(B, B') = e(H_z, Z_i)\, e(H_u, U_i)\, e(V_i, W_i).$$

Taking the discrete log wrt G_r, the relations are written as

$$a\, a' = g_z z_i + 1\, r_i + s_i t_i$$
$$b\, b' = h_z z_i + h_u u_i + v_i w_i.$$

Tight Generic Hardness of SFP

Proof intuition (cont'd):

The j-th group element viwed by the generic adversary is represented by a function F_j of a linear combination of variables a, a', b, b', g_z, 1, h_z, h_u, z_i, r_i, s_i, t_i, u_i, v_i, w_i where

$$r_i := a\,a' - g_z z_i - s_i t_i$$
$$u_i := (b\,b' - h_z z_i - v_i w_i)/h_u.$$

For every $j, j' < \ell+q$, $F_j - F_{j'}$ and $F_j \cdot F_{j'}$ are Laurent polynomials with total degree of at most some small constants. Thus any of them vanishes at a random assignment to the variables only with probability at most ${}_2C_{\ell+q}(const/|\mathbb{G}|) = \mathcal{O}(\ell^2 + q^2)/|\mathbb{G}|$ as claimed.

Lower Bounds on Signature Size

Group type	Messages	Lower bounds: Interactive	Lower bounds: Non-interactive	Upper Bounds: Interactive	Upper Bounds: Non-interactive: q-type	Upper Bounds: Non-interactive: Static
Type-III	Unilateral	3 [AGHO11]	4 [AGO11]	3 [AGHO11]	4 [AGHO11]	7 [KPW15]
	Bilateral	3 [AGHO11]		3 [AGHO11]	6 [AGHO11]	14 [ACDKNO12]
Type-II	$M \in \mathbb{G}_1$, Bilateral	3 [AGOTib14]		3^{*1} [AGOTia14]		
	$M \in \mathbb{G}_2$	2 [AGOTib14]		2^{*2} [AGOTib14]	3 [AGOTib14]	
Type-I	N/A	3 [AGOTia14]		3^{*2} [AGOTia14]	7 [AFGHO10]	10 [KPW15]

*1: Single-element message. Vector mssage possible.
*2: Single-element message.

Extensions of SPS

Linearly homomorphic SPS [LPJY13]

- Application to Quasi-adaptive NIZK

Selectively randomizable SPS [AGOTi14a]

- Flexibly change signatures from strongly unforgeable to randomizable ones

SPS for equivalence classes [HS14,FHS15]

- Can sign on equivalence classes defined by vector of group elements
- Application to optimal-round blind signatures without using GS-proofs

Fully SPS [AKOTi15,Gro15(tomorrow!)]

- Even secret-keys are group elements

Open Problems on SPS

- Find more lower bounds for the case of non-interactive assumptions.
- Separately show lower bounds for static assumptions. Are they different from those for q-type assumptions?
- Show constant-size SPS with a tight reduction to simple assumptions.

Structure-Preserving Commitments

- The commitment keys, messages, commitments, and opening informations consist of elements of $\mathbb{G}_1$ and $\mathbb{G}_2$, and
- opening verification is done only by group operations, membership testing, and evaluation of pairing product equations.

State of The Art

Performance of Structure-Preserving Commitment Schemes

Group	Scheme	$\|msg\|$	$\|key\|$	$\|com\|$	$\|open\|$	$\#(PPE)$	asmpt.
Type-I	[Gro09]	k	$2k+4$	$2_{(\mathbb{G}_T)}$	2	2	STP
	[AHO10]	k	$2k+2$	$2_{(\mathbb{G}_T)}$	2	2	SDP
	[CLY09]	k	5	$3k$	$3k$	$3k$	DLIN
	[AHO10]	k	$2k+2$	$2k+2$	2	2	SDP
	[AHO12]	k	$2k+3$	$k+2$	2	2	SDP
Type-III	[AHO12]	$(0,\ k)$	$(k+1,\ 1)$	$(1,\ k)$	$(0,\ 1)$	1	DBP

|msg| < |com|

Abe, Haralambiev, Ohkubo, “Group to Group Commitments Do Not Shrink”, Eurocrypt 2012

SPCs Do Not Shrink?

Theorem 9 [AHO12]. If the discrete-logarithm problem is hard in the base groups, key generation and commitment algorithms are algebraic, and $|com| < |msg|$, then the commitment scheme is not binding.

Binding Property (Collision Resistance)

$$ck$$

$$\downarrow$$

$$\boxed{\mathcal{A}_{\mathsf{cr}}}$$

$$\downarrow$$

$$(com, msg, open, msg', open')$$

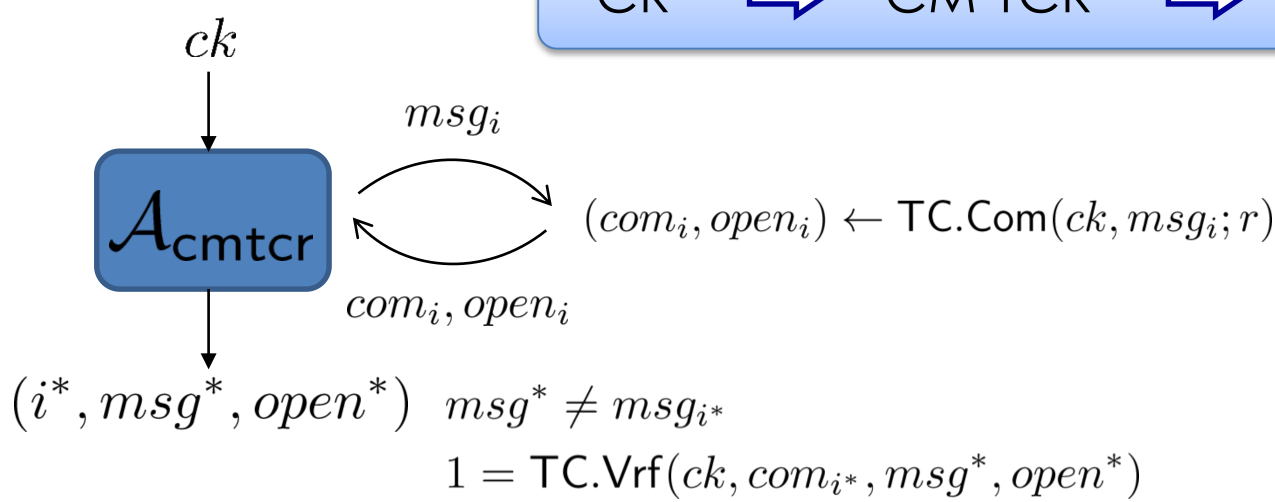
$$1 = \mathsf{TC.Vrf}(ck, com, msg, open) = \mathsf{TC.Vrf}(ck, com, msg', open')$$

SPCs Do Shrink, Sometimes

Theorem [AKOTi14]. There exists a shrinking homomorphic trapdoor structure-preserving commitment scheme that is chosen message target collision resistant (CMTCR) if there exist a one-time non-adaptive chosen message secure strucuture-preserving partially one-time signature scheme (POS) and a γ target collision resistant trapdoor commitment scheme (γ-TC) exists.

Notion of CMTCR

CR $\Rightarrow$ CM-TCR $\Rightarrow$ TCR



Impossibility Argument for CR

If TC.Com is algebraic, commitment $\vec{C}$ and opening $\vec{D}$ are computed by linear combination of message $\vec{M}$ and commitment key $\vec{V}$. Coefficient matrix B may depend on $\vec{M}$, $\vec{V}$ and internal random coins.

$$\begin{pmatrix}\vec{C}\\ \vec{D}\end{pmatrix} = \left(\begin{array}{c|c} B_1 & B_2 \\ \hline B_3 & B_4\end{array}\right)\begin{pmatrix}\vec{M}\\ \vec{V}\end{pmatrix}$$

If $|\vec{C}| < |\vec{M}|$, there exists $\vec{M}'(\neq \vec{M})$ that $\vec{C} = (\vec{B}_1|\vec{B}_2)(\vec{M}'|\vec{V})^T$.

To compute such $\vec{M}'$, matrix $\vec{B}$ must be known to the adversary.

Impossibility Argument for CR

If TC.Com is algebraic, commitment $\vec{C}$ and opening $\vec{D}$ are computed by linear combination of message $\vec{M}$ and commitment key $\vec{V}$. Coefficient matrix B may depend on $\vec{M}$, $\vec{V}$ and internal random coins.

$$\begin{pmatrix} \vec{C} \\ \vec{D} \end{pmatrix} = \left(\begin{array}{c:c} B_1 & B_2 \\ \hdashline B_3 & B_4 \end{array}\right) \begin{pmatrix} \vec{M} \\ \vec{V} \end{pmatrix}$$

In the CR game, it is the adversary that chooses the random coins. Hence it knows matrix B.

If $|\vec{C}| < |\vec{M}|$, there exists $\vec{M}'(\neq \vec{M})$ that $\vec{C} = (\vec{B}_1|\vec{B}_2)(\vec{M}'|\vec{V})^T$.

To compute such $\vec{M}'$, matrix $\vec{B}$ must be known to the adversary.

Impossibility Argument for CR

If TC.Com is algebraic, commitment $\vec{C}$ and opening $\vec{D}$ are computed by linear combination of message $\vec{M}$ and commitment key $\vec{V}$. Coefficient matrix B may depend on $\vec{M}$, $\vec{V}$ and internal random coins.

$$\begin{pmatrix}\vec{C}\\ \vec{D}\end{pmatrix} = \left(\begin{array}{c|c} B_1 & B_2 \\ \hline B_3 & B_4 \end{array}\right)\begin{pmatrix}\vec{M}\\ \vec{V}\end{pmatrix}$$

In the CR game, it is the adversary that chooses the random coins. Hence it knows matrix B.

In CM-TCR game, it is the challenger that chooses the random coins. Thus matrix B is unknown to the adversary.

The impossibility argument does not apply to CM-TCR.

If $|\vec{C}| < |\vec{M}|$, there exists $\vec{M}'(\neq \vec{M})$ that $\vec{C} =$

To compute such $\vec{M}'$, matrix $\vec{B}$ must be know

Shrinking SPTC : Generic Construction

Building blokcs

- Partial one-time signature scheme (POS)
- γ-target collision resistant commitment scheme (TC_γ)

$\mathsf{Com}(ck, msg)$

1. $(M^{(1)}, \ldots, M^{(\kappa)}) \in \mathcal{M}_{\mathsf{pos}}^{\kappa} \leftarrow msg$ — Divide message into k blocks
2. $(vk_{\mathsf{pos}}, sk_{\mathsf{pos}}) \leftarrow \mathsf{POS.Key}(\mathsf{gk})$ — Generate one-time key
3. For $i = 1, \ldots, \kappa$

   $(ovk_{\mathsf{pos}}^{(i)}, osk_{\mathsf{pos}}^{(i)}) \leftarrow \mathsf{POS.Ovk}(\mathsf{gk})$

   $\sigma_{\mathsf{pos}}^{(i)} \leftarrow \mathsf{POS.Sign}(sk_{\mathsf{pos}}, osk_{\mathsf{pos}}^{(i)}, M^{(i)})$ — Sign each message block
4. $(com_{\mathsf{gbc}}, open_{\mathsf{gbc}}) \leftarrow \mathsf{TC}_\gamma.\mathsf{Com}(sk_{\mathsf{gbc}}, osk_{\mathsf{gbc}}^{(1)}, \cdots, osk_{\mathsf{pos}}^{(\kappa)}))$ — Commit to the one-time keys
5. $com := com_{\mathsf{gbc}}$

   $open := (open_{\mathsf{gbc}}, vk_{\mathsf{pos}}, ovk_{\mathsf{pos}}^{(1)}, \cdots, ovk^{(\kappa)}, \sigma_{\mathsf{gbc}}^{(1)}, \cdots, \sigma^{(\kappa)})$

Shrinking SPTC : sketch

Concrete SPTC from POS and TC_γ in Type-III groups

Commitment-key : $ck = \left(G, \tilde{G}, \tilde{X}, \tilde{X}_1, \ldots, \tilde{X}_k, \tilde{Y}_1, \cdots, \tilde{Y}_\ell\right)$

Message : $M = (\tilde{M}_1, \cdots, \tilde{M}_{k\cdot\ell})$

Commitment : $C = \tilde{G}_u$

Opening : $D = \left(R, \{\tilde{Z}_j, \tilde{R}_j\}_{j=1}^{k}, A_1, \ldots, A_k, G_z, G_1, \cdots, G_\ell\right)$

Verification(ck, M, C, D)

$$e(G, \tilde{G}_u) = e(R, \tilde{G})\, e(G_z, \tilde{X}) \prod_{i=1}^{k} e(A_i, \tilde{X}_i) \prod_{i=1}^{\ell} e(G_i, \tilde{Y}_i)$$

for $j = 1, \ldots, k$

$$e(A_j, \tilde{G}) = e(G_z, \tilde{Z}_j)\, e(G, \tilde{R}_j) \prod_{i=1}^{\ell} e(G_i, \tilde{M}_{(j-1)\ell+i})$$

Message:	$k \cdot \ell$
Commit key:	$1 + k + \ell$
Trapdoor:	$1 + k + \ell$ (in $\mathbb{Z}_p$)
Commitment:	1
Opening info:	$2 + 3k + \ell$
# of PPEs:	1 + k

Usefulness of CM-TCR

CM-TCR is still useful in constructing CMA-secure signature schemes.

CMA-security Game

Adversary's choice

Challenger's choice (not seen by the adversary)

pk

$\mathcal{A}_{\text{cma}}$

msg_i

σ_i

$(com_{\text{tc}}, open_{\text{tc}}) \leftarrow \text{TC.Com}(ck_{\text{tc}}, msg_i; r)$

$\sigma_{\text{xsig}} \leftarrow \text{xSIG.Sign}(sk_{\text{xsig}}, com_{\text{tc}})$

$\sigma_i := (\sigma_{\text{xsig}}, com_{\text{tc}}, open_{\text{tc}})$

(σ^*, msg^*)

$msg^* \notin \{msg_i\}$

$1 \leftarrow \text{SIG.Vrf}(pk, msg^*, \sigma^*)$

Applications

Works on Structure-Preserving Crypto

Proof Systems

- NIWI, NIZK [Gro06, GS08, GSW10, EG14]
- Properties of GS-proofs [BCCKLS09,Fuc11,CKLM12]
- Simulation-Sound NIZK [Gro06, CCS08, HJ12]

Signatures

- Constructions [Gro06, GH08, CLY09, AFGHO10, AHO10, AGHO11, CK11, ACD+12, CDH12, CK12, ADKNO13, LPJY13, ALP13, AGOTia14, AGOTib14, HS14, LJ14, CM14, BFFSST15, LPY15, AGKOTi15, KPW15, Groth15]
- Bounds [AGHO11, AGO11, AGOTia14, AGOTib14]

Public-Key Encryption

- CPA [ElG85,HK07,Sha07]
- CCA2 [CHKLN11]

Commitments

- Constructions [Gro09, AFGHO10, AHO10, AHO12, AKOTi15]
- Bounds [AHO12]

Oblivious Transfer

- Construction [DDvMNP15]

Applications(Blind signature, Group signature, Credential system, etc,...)

- [AFGHO10, CHKLN11, Kris11, ALP12, LPY12, HJ12, CKLM12, FKMV12, AJ13, BFG13, LPJY13, KR13, CMA13, SEHKMO13, ZLG13, ACDN14, LJYP14, LPJM14, AEHS14, LPDW14, ABGSS14, HRS15, FHS15, KM15, Ghada15]

General Idea for Group Signatures

[AFGHO10] Signatures
[BB04] one-time Signatures

Groth-Sahai Proof System

Encryption/ Anonymous Tag System

"Group/Traceable Signature" = "Signature" + "Revocation Mechanism"

- Guarantees integrity of messages.
- Authenticate the signer.

- Opening, Tracing
- Claiming, Denial

Glued by NIZK that guarantees correct computation while hiding privacy related objects in each part.

Comparison

Scheme	Construction Type	Claim & Trace	Deny Function	Anonymity w/ Trace	Anonymity Level	Concurrent Join	Sig. Size
[AHO10]	generic	no	no	no	CCA	yes	58
[LY09]	Tailor-made	yes	no	no	CPA	no	83
[ACHO11]	generic	yes	yes	yes	CCA	yes	107

Table: Summary of properties among group signature and traceable signature schemes that provide non-frameability (the signature size conunts the number of group elements).

Wrap Up

Conclusion

- There are proof systems, signatures, encryption, and commitments over bilinear groups that are structure-preserving and thus interoperable each other.
- They can be used for modular construction of intricate cryptographic tasks. And the efficiency of the resulting scheme can be evaluated with concrete figures.
  - There is room for hand-crafted optimization by carefully choosing which elements are hidden and which are put in the clear.
- There are interesting open problems both in practice (efficiency improvements) and theory (lower bounds), and missing important tools like IBE, FE, etc.

People

Authors of papers that study or use SP primitives.

Laila El Aimani, Emmanuelle Anceaume, Nuttapong Attrapadung, Gilles Barthe, Mihir Bellare, Nasima Begum, Pedro Bibiloni, Jan Camenisch, Dario Catalano, Melissa Chase, Sanjit Chatterjee, Chen Chen, Sherman S. M. Chow, Bernardo David, David Derler, Rafael Dowsley, Maria Dubovitskaya, Ali El Kaafarani, Keita Emura, Robert R. Enderlein, Alex Escala, Edvard Fagerholm, Xiao Feng, Dario Fiore, Georg Fuchsbauer, Nobuo Funabiki, Sanjam Garg, Eddsam Ghadafi, Jens Groth, Gilles Guette, Hua Guo, Divya Gupta, Goichiro Hanaoka, Christian Hanser, Kristiyan Haralambiev, Dennis Hofheinz, Lina Huo, Tibor Jager, Marc Joye, Yutaka Kawai, Dalia Khader, Aggelos Kiayias, Eike Kiltz, Markulf Kohlweiss, Paul Lajoie-Mazenc, Jorn Lapon, Anja Lehmann, Xian Li, Xia Liu, Zhoujun Li, Benoît Libert, Muqing Lin, Anna Lysyanskaya, Jinxin Ma, Matteo Maffei, Takahiro Matsuda, Antonio Marcedone, Paul Lajoie-Mazenc, Sarah Meiklejohn, Alfred Menezes, Paz Morillo, Hirofumi Muratani, Vincent Naessens, Toru Nakanishi, Gregory Neven, Ryo Nishimaki, Kazuma Ohara, Miyako Ohkubo, Kazumasa Omote, Murat Osmanoglu, Jiaxin Pan, Kim Pecina, Thomas Peters, David Pointcheval, Orazio Puglisi, Max Rabkin, Samuel Ranellucci, Manuel Reinert, Alfredo Rial, Joeri de Ruiter, Yusuke Sakai, Olivier Sanders, Andre Scedrov, Benedikt Schmidt, Dominique Schröder, Thomas Sirvent, Daniel Slamanig, W. Su, Chunrong Sui, Takeya Tango, Qiang Tang, Alain Tapp, Mehdi Tibouchi, Thomas Unterluggauer, Valérie Viet Triem Tong, Hoeteck Wee, Xing Wei, J. Weng, Zheng Yuan, Moti Yung, Jiangxiao Zhang, Fucai Zhou, ….