RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-T06

Structure-Preserving Certificateless Encryption and Its Application

Prof. Sherman S. M. Chow

Department of Information Engineering
Chinese University of Hong Kong, Hong Kong
@ShermanChow

joint work with Tao Zhang and Huangting Wu

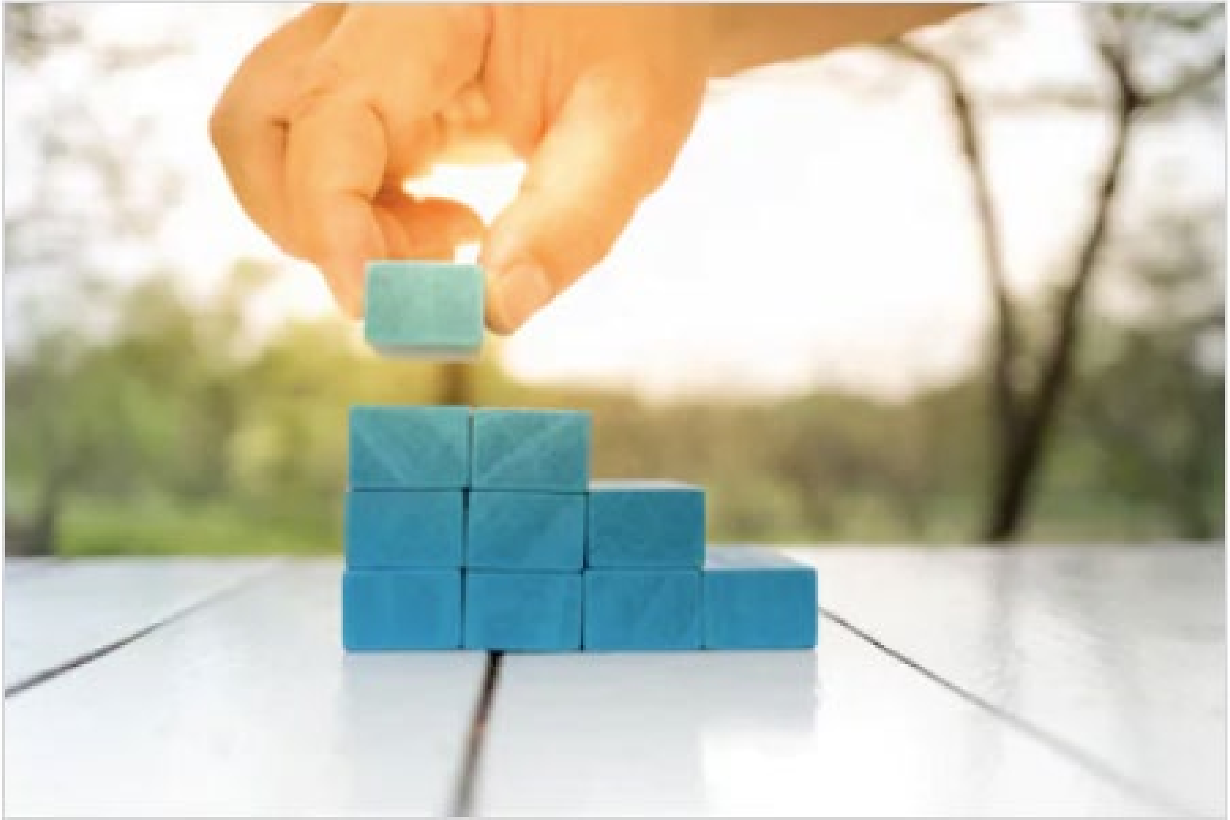
Tao Zhang: CUHK → Tencent
Huangting Wu: CUHK

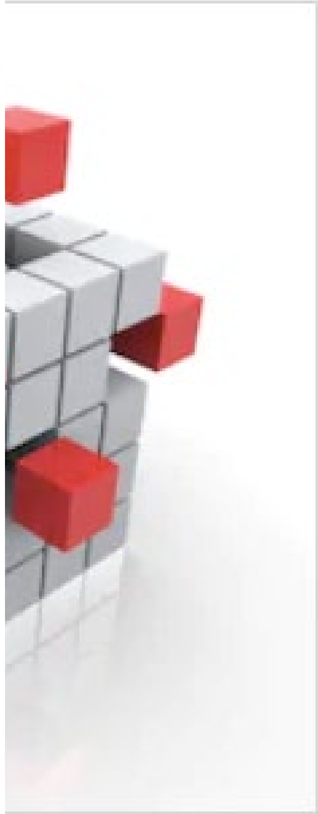
#RSAC

Modular Design

Reduction in Cost

Flexibility in Design





Some “Traditional Views”

- To use a modular approach in designing cryptosystem means…
  - it would be insecure since mix-and-match types of attack will succeed
  - it would be hopelessly inefficient when compared to a specific design
- To use public key encryption, we need public-key infrastructure.
- To issue a signature, everyone knows who is the signer.
- To ensure anonymity, we would lose accountability.

Modern Cryptography

- ***Structure-Preserving Cryptography*** **is a framework for *securely* & *efficiently* realizing a generic design.**
- ***Certificateless Encryption*** **does *not* require any PKI.**
- ***Group Signature*** **ensures *Signer-Anonymity* and *Accountability* simultaneously.**

Rundown

- Structure-Preserving Cryptography
- Certificateless Encryption

- Structure-Preserving Certificateless Encryption
- and Its *New* Application

  (in Group Signatures with “Certified Limited Opening”)

RSAConference2019

Structure-Preserving Cryptography

(and Bilinear Groups and Groth-Sahai Proof System)

Structure-Preserving Cryptography

- A framework for securely and efficiently instantiating a design
- But why it can be efficient?
- Because all of the building blocks use the same “structure”
- Suppose we compose encryption and signature together.
  - Encryption is based on a “group”
  - Signature is based on the same “group”
- What kind of group is popular?
- Bilinear group!

Bilinear Groups

- $\mathbf{G}$, $\mathbf{H}$, and $\mathbf{G}_T$ are 3 multiplicative cyclic group of prime order p.

- e: $\mathbf{G} \times \mathbf{H}$ (base groups) → $\mathbf{G}_T$ (target group) is bilinear:

$$\forall g \in \mathbf{G}, h \in \mathbf{H}, x, y \in \mathbf{Z}_p, \mathrm{e}(g, h) = \mathrm{e}(g, h)^{xy}$$

- Why is it useful? We can <u>multiply</u> the *secret exponents*!
  - Discrete logarithm is still hard: given g, g^x, cannot recover x.

Structure-Preserving Cryptography for Bilinear Groups

- All public objects (public-key, messages, signatures, *etc.*) merely consists of elements in **G** and **H**.
- Verifying relations of interest can be done only by group op.'s, membership testing, and evaluating *pairing product equations*:

$$\prod_i e(A_i, Y_i) \prod_i e(B_i, X_i) \prod_i \prod_j e(X_i, Y_j)^{c_{ij}} = T$$

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

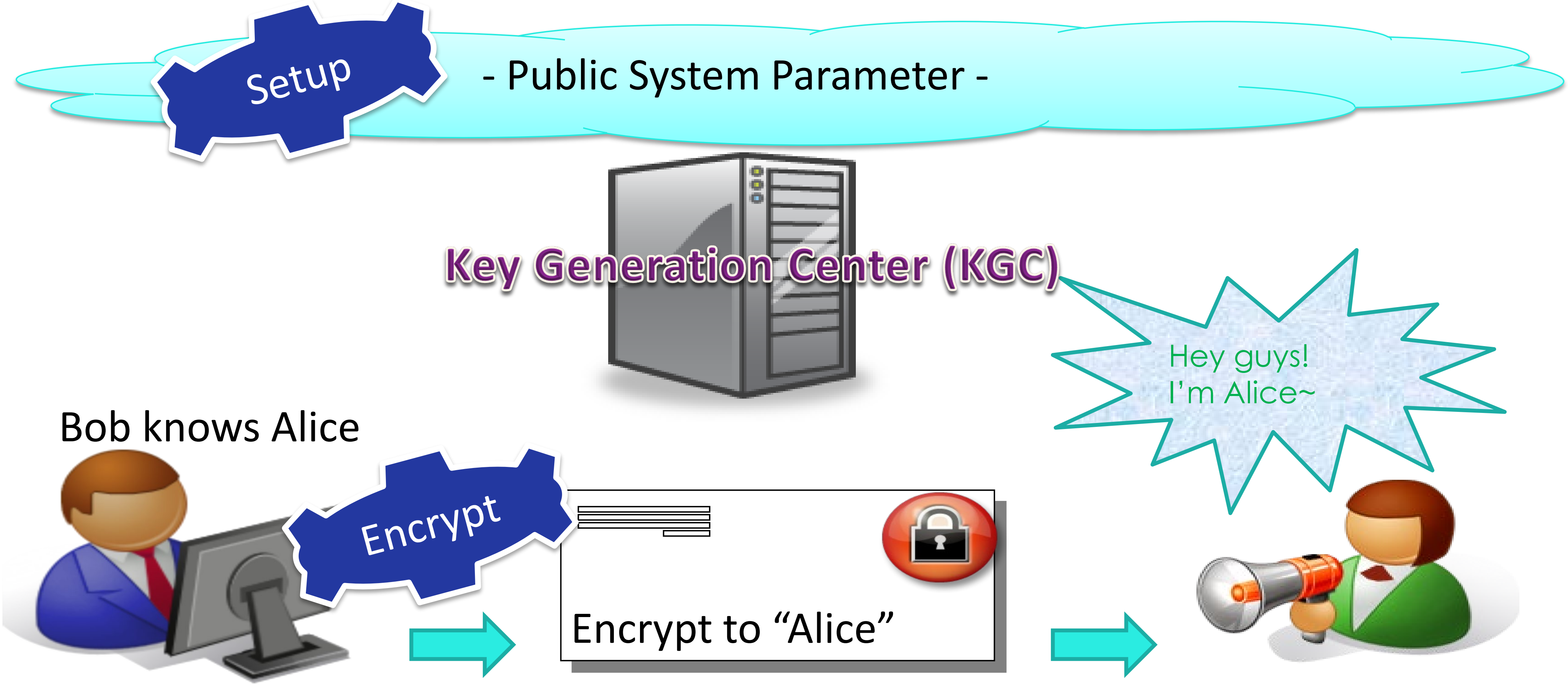
- Every building blocks follow the same form. But why it can be secure?
- Groth—Sahai proof system (Eurocrypt '08) can prove about it
  - without leaking $\{A_i\}$, $\{B_i\}$, $\{X_i\}$, $\{Y_i\}$!

RSAConference2019

Certificateless Encryption

(and why it is better than Identity-Based Encryption)

Identity-Based Encryption (IBE)



Who can decrypt? Authenticated Users and KGC

Generate *ID-based Secret Key*
(using Master Secret)

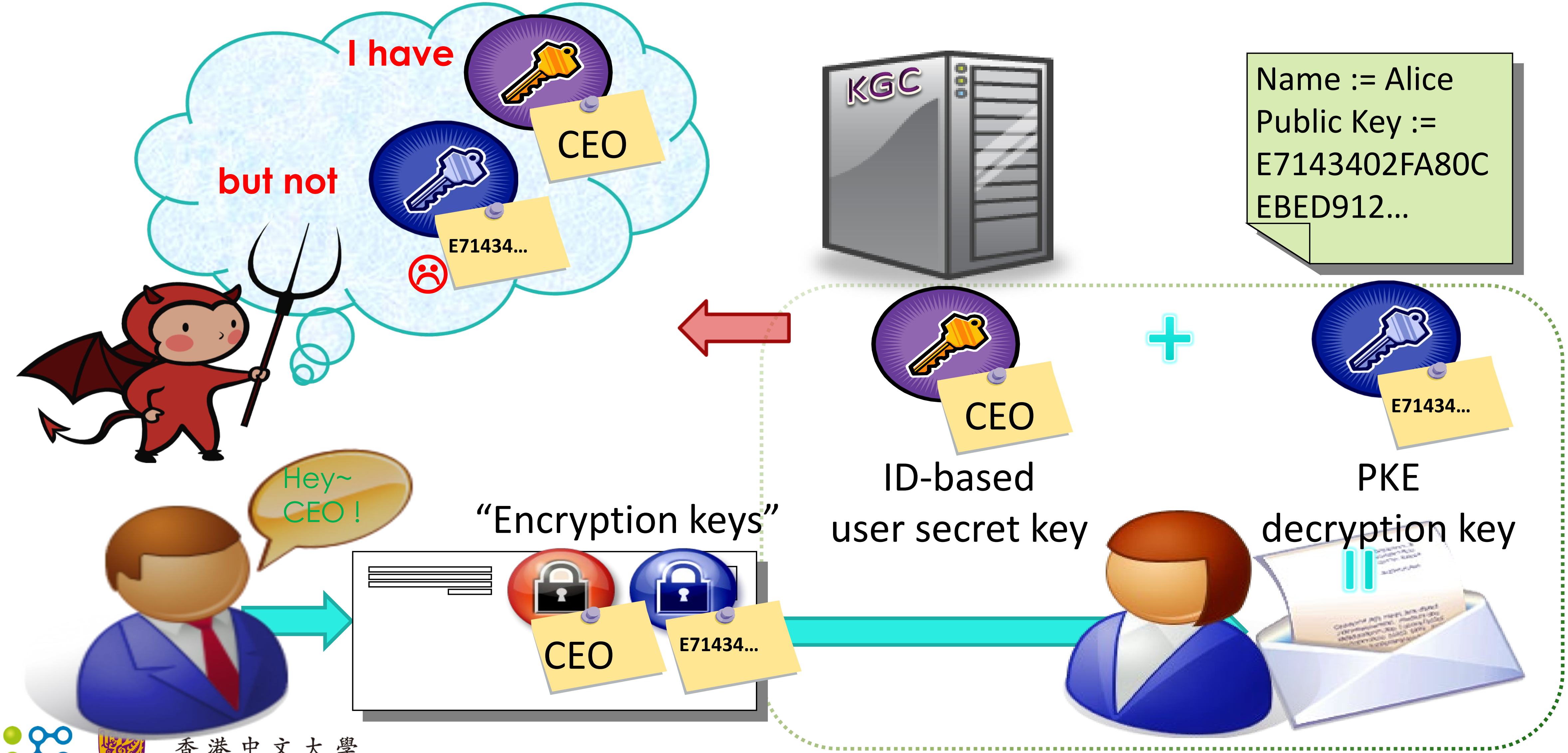
Key Generation Center (KGC)

KGC may turn **Evil** ?!

Escrowed Key!

Alice the Receiver
- Authenticated
- Get an ID-based secret key

Certificateless Encryption (CLE)



Benefits of Certificateless Encryption

- In essence, CLE = PKE + IBE
  - (+strong decryption oracle, *cf.*, Chow—Franklin—Zhang in CT-RSA ’14)
- Implicit certificate (better than PKE)
  - The encryptor does not need to verify any certificate.
  - Only the right person can get the “partial decryption key” from the KGC.
- Free from key-escrow (better than IBE)
  - The KGC does not know the “user private key”.

RSAConference2019

Structure-Preserving Certificateless Encryption

a new primitive in Structure-Preserving Cryptography

Upgrade from Structure-Preserving IBE?

- There is no known construction of structure-preserving (SP) IBE.
- Only partial SP-IBE exists (ID is not a group element).
  - proposed by Libert—Joye in CT-RSA ’14
- IBE → Signature, *i.e.*, the ID-based secret key is a signature on ID
- IBE decryption: <u>pairing</u> up this <u>signature</u> with the <u>ciphertext</u>.
- Can we upgrade structure-preserving signatures (SPS) to IBE?
- Verification of existing SPS requires computing a pairing where *both* of the input elements come from the signature.

Upgrade from Structure-Preserving PKE?

- If not SP-IBE, how about using SP-PKE?
- How to ensure that the user public key is still "related" to the master public key of the IBE system?
  - Otherwise, even if you are not the CEO, you can claim to be and decrypt.
- Ask the encryptor to somehow check the user public key?
- May work in principle… but it is rather meaningless…
- CLE is for relieving the encryptors from verifying a certificate…
- And now you are asking them to verify a public key?

Our Idea: upgrades from Structure-Preserving Signature

- We employ an SP signature scheme by Abe *et al.* in Crypto '11.
- For public key $(g, h, W_1, W_2, V_1, V_2)$, verification equations are:
- $\mathrm{e}(W_2, R)\ \mathrm{e}(g, S)\ \mathrm{e}(U, M_0) = \mathrm{e}(W_1, h)$
- $\mathrm{e}(T, R)\ \mathrm{e}(M_1, V_1)\ \mathrm{e}(M_2, V_2) = \mathrm{e}(g, h)$
- where (R, S, T) is a signature on the message vector (M_0, M_1, M_2)
- Trick 1: we use the signature (R, S, T) to also sign on $M_0 = R$
- Trick 2: we set M_1 as the identity and M_2 as a user public key

High-Level Idea of the Conversion

- Public Key of SPS → Master Public Key of SP-CLE
- Signature of SPS → Partial **Private** Key of the User

- We exploit the elements in the pairing product equations of SPS.
- Some elements embedded the encryption randomness.
- Only valid verification equations can recover the randomness.
- But how?

More Details of the Conversion

- $e(W_2, \underline{R})\, e(g, \underline{S})\, e(U, \underline{R}) = e(W_1, h)$ // R, S, T are now "<u>private</u>"
- $e(\underline{T}, \underline{R})\, e(ID, V_1)\, e(D, V_2) = e(g, h)$ // where D is a <u>user public key</u>
- The choice depends on the input elements of a pairing.
- *Both* elements are *public*: we make them the <u>session key</u>.
- *One* of the elements is *public*: we embed the <u>randomness</u>.
- *Both* elements are *private* (which is also why SP-IBE plan fails): we publish one element (R in our case) as a <u>user public key</u> too.

Spelling out the details…

- $e(W_2, R)\, e(g, \underline{S})\, e(U, R) = e(W_1, h)$ // $e(g, \underline{S})$: only S is private
- $e(\underline{T}, R)\, e(ID, V_1)\, e(D, V_2) = e(g, h)$ // $e(\underline{T}, R)$: only T is private

- $C_0 = M \cdot K$, $C_g = g^x$, $C_R = R^y$, $C_z = g^z$ // M is the message to encrypt
- $K = \{e(W_2, \underline{R})\, e(U, R) / e(W_1, h)\}^x$ // K is the session key
  - $\{e(ID, V_1)\, e(D, V_2) / e(g, h)\}^y$
  - $e(D, h^z)$

Making it preserving more structure

- Message is in the target group $\mathbf{G}_T$.
- Ciphertext has many elements in the target group $\mathbf{G}_T$.
- We can exploit the tricks of Libert—Joye to resolve these.

RSAConference2019

Group Signatures with Certified Limited Opening

a new primitive for Accountable Privacy

Group Signatures

- Group-oriented signatures with anonymity
  - but with an explicit group formation (diff. from ring signature)
- A *group manager* (GM) issues credentials
- Any *member* can sign for the group
  - remain <u>anonymous</u> within the group
  - signatures are <u>unlinkable</u>
  - but, unconditional anonymity may be abused, we want <u>accountability</u>
- An *opening authority* (OA) can “open” a group signature to <u>reveal its true signer</u>

Group Signatures with Message-Dependent Opening

- OA is too powerful.
- Message-dependent opening introduces another “admitter”.
- The admitter generates a message-dependent opening key.

- Opening only works with both “master” opening key and this message-dependent opening key.
- Good: opening power is restricted
- Bad: always bother the OA

Group Signatures with Certified Limited Opening (CLO)

- Opening in message-dependent opening depends on the *message*...
- We generalize it to "contexts".
- Instead of the "admitter", we introduce a "certifier".
- The certifier certifies the *opener* depending on the context.
  - *i.e.*, the opening power is limited to only the specified context.
- No need to bother the OA.
- The opener's opening power is limited.
- No (un-certified) opener can open signatures in other contexts.

Applications in Electronic Voting

- Consider using the group signatures for signing on votes.
- The government can be the master certifier.
- The openers can be those special party overseeing different districts/counties/provinces/states ← different contexts.
- Open when something bad happen, *e.g.*, when the voting software in one of the voting booths could be compromised.

Structure-Preserving CLE → Group Signatures with CLO

- SP-CLE's identity → Context in Group Sig. with CLO
- Group signature = Verifiable encryption of the signer's identity with respect to the corresponding context.
- SP-CLE key issuing → Certifying the opening power.
- SP-CLE decryption → Opening of identity limited to the context.

Conclusion

- Structure-Preserving Cryptography for Modular design
- Certificateless Encryption for Escrow-Free Encryption w/o PKI
- Structure-Preserving Certificateless Encryption
  - a new tool in structure-preserving cryptography
- and Its Application

  (in Group Signatures with “Certified Limited Opening”)
  - a new tool for accountable privacy
- *Sherman S. M. Chow* <{firstname}[at]ie.cuhk.edu.hk>