Lattice-based Signcryption without Random Oracles

Shingo Sato Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University, Japan

Overview

- Lattice-based Cryptography
  - The cryptosystem is based on lattice problems and has quantum-resistance.
  - It is possible to realize a lot of functionalities of cryptosystems.
- Signcryption
  - Cryptosystem meeting both securities of public key encryption (PKE) and digital signatures (DSs)
  - The public-key based "authenticated encryption"

We propose

- A construction of signcryption based on lattice problems, and
- Hybrid encryption of signcryption based on this construction with data encapsulation mechanism (DEM)

Lattice

The lattice generated by n linearly independent vectors $\boldsymbol{b_1}, \boldsymbol{b_2}, \dots, \boldsymbol{b_n} \in \mathbb{R}^m$ is defined as

$$L(\boldsymbol{b_1}, \dots, \boldsymbol{b_n}) = \{ \sum x_i \boldsymbol{b_i} \mid x_i \in \mathbb{Z} \}.$$

It is often written by

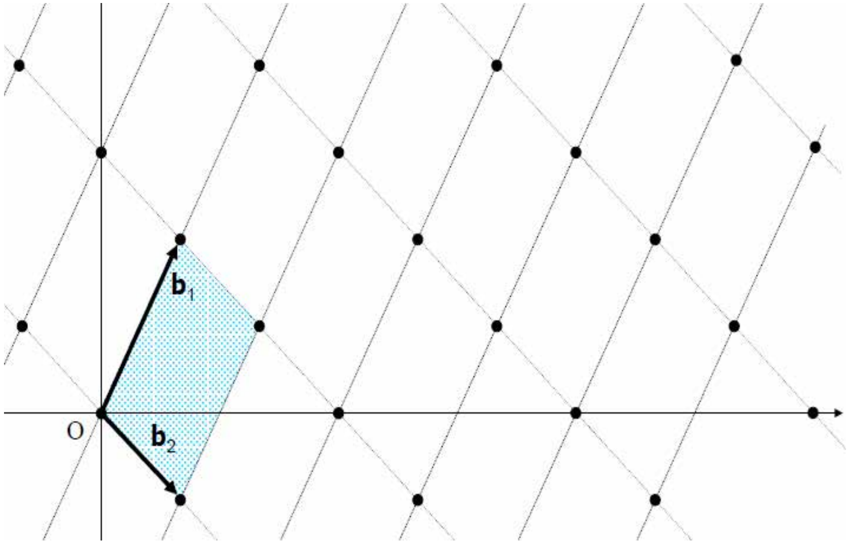
$$L(\boldsymbol{B}) = \{ \boldsymbol{Bx} \mid \boldsymbol{x} \in \mathbb{Z}^n \},$$

where $\boldsymbol{B} := [\boldsymbol{b_1}, \dots, \boldsymbol{b_n}] \in \mathbb{R}^{m \times n}$ is the lattice basis.

As the norm of vectors, we consider the Euclid norm:

$$\|\boldsymbol{v}\| = \sqrt{v_1^2 + \cdots + v_n^2}$$

for $\boldsymbol{v} = (v_1, \dots, v_n) \in \mathbb{R}^n$.



Lattice Problems

- $GapSVP_{\gamma}$:
  - Given a lattice basis $\boldsymbol{B}$, $r \in \mathbb{R}$,
  - Decide whether the shortest vector $\boldsymbol{v}(\in L(\boldsymbol{B}) \setminus \{\boldsymbol{O}\})$ fulfills $||v|| \leq r$ or $||v|| > \gamma \cdot r$

- Learning with Errors and Small Integer Solution

  (LWE and SIS)

  - ✓ It is possible to reduce from lattice problems to these problems.
  - ✓ The average-case problems are at least as hard as the worst-case problems.
  - ✓ It is possible to realize a lot of cryptosystems such as fully homomorphic encryption, attribute-based encryption, searchable encryption and so on.

Definitions of LWE and SIS

- $\boldsymbol{LWE}_{q,\alpha}$ (Decisional version)
  - The LWE distribution $A(\boldsymbol{s},\phi)$:
    - Input: $\boldsymbol{s} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}}$ and a Gaussian distribution ϕ with the center 0 and the standard deviation αq
    - Output (*): $(\boldsymbol{a}_1, b_1), \dots, (\boldsymbol{a}_m, b_m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$,

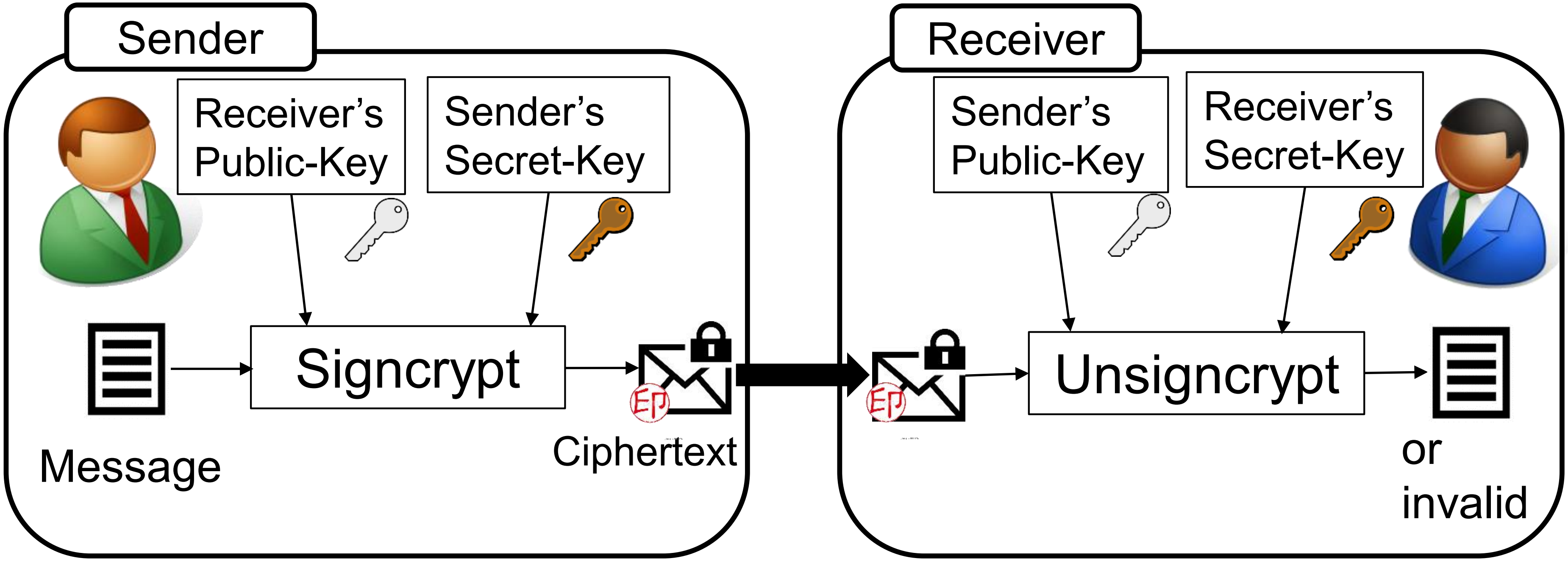
      where $b_i = \boldsymbol{s}^\top \boldsymbol{a}_i + e_i, \boldsymbol{a}_i \overset{U}{\leftarrow} \mathbb{Z}_q^n, e_i \leftarrow \phi$ for $i \in \{1, \dots, m\}$
  - Input: $(\boldsymbol{a}_1, b_1), \dots, (\boldsymbol{a}_m, b_m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$,
  - Decide whether the input sequence is sampled from the LWE distribution or uniformly at random in $\mathbb{Z}_q^n \times \mathbb{Z}_q$

  (*) Let $\boldsymbol{A} \coloneqq [\boldsymbol{a}_1, \dots, \boldsymbol{a}_m]$ and $\boldsymbol{e}^\top \coloneqq [e_1, \dots, e_m]$, then the LWE samples can be expressed by $\boldsymbol{b} = \boldsymbol{s}^\top \boldsymbol{A} + \boldsymbol{e}^\top \bmod q$

- $\boldsymbol{SIS}_{q,\beta}$
  - Input: $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$,
  - Find: $\boldsymbol{e} \in \mathbb{Z}^m$ s.t. $\boldsymbol{Ae} = \boldsymbol{0} \bmod q$ and $||\boldsymbol{e}|| \le \beta$

Signcryption [Z97]

- Signcryption schemes meet both functionalities of PKE and DS (both of confidentiality and integrity).
- It is used to construct secure channels from insecure ones such as the Internet

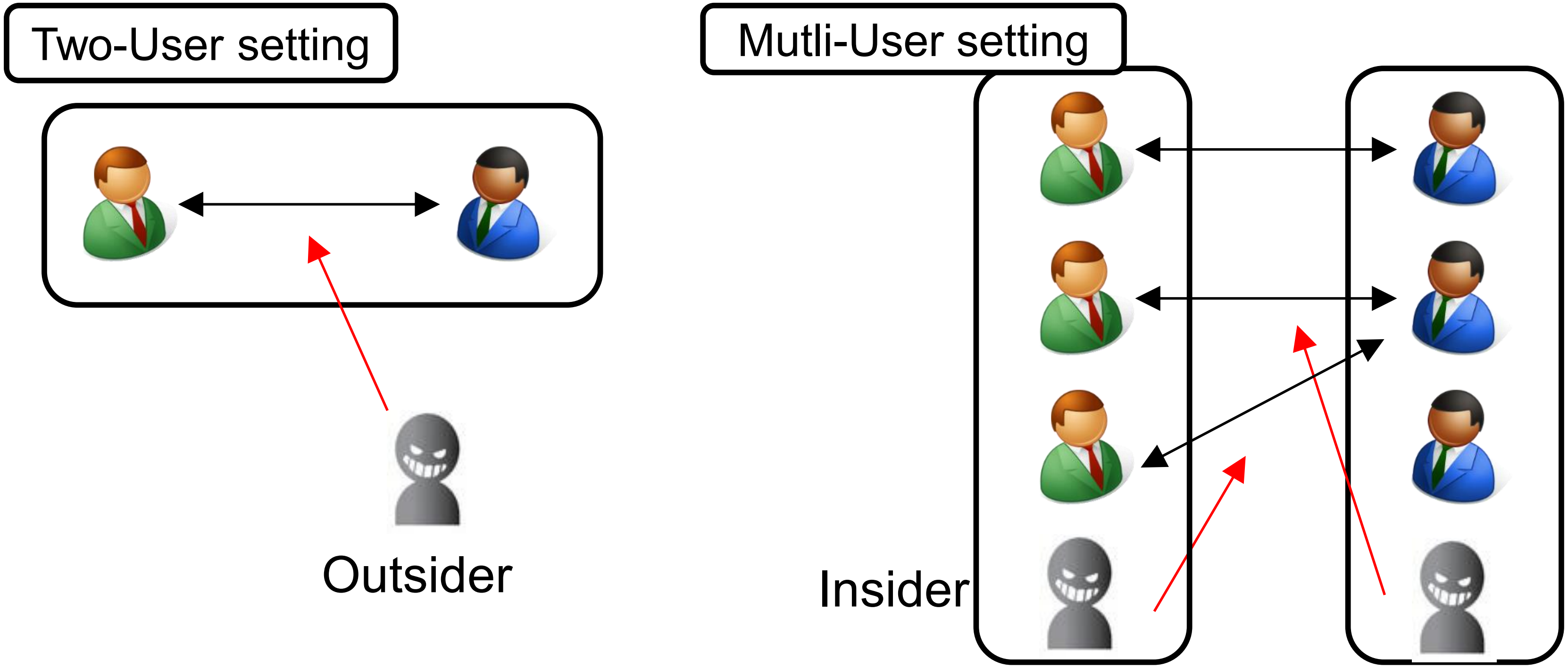


[Z97] Y. Zheng, "Digital Signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)," CRYPTO 1997.

The Security Model [ADR02]

We consider IND-CCA and sUF-CMA security against insiders in the multi-user setting (MU-IND-iCCA and MU-sUF-iCMA).

- Securities in the two-user setting doesn't always imply ones in the multi-user setting.
- Inside adversaries are stronger than outside ones.



[ADR02] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," EUROCRYPT 2002.

Our Proposal

Main purpose:

To construct a lattice-based signcryption scheme

- Meeting both of MU-IND-iCCA and MU-sUF-iCMA security
- More efficient than the existing constructions in terms of key-sizes and ciphertext-size

To achieve these, we propose the following constructions

1. A direct construction based on lattice problems
2. Hybrid encryption variant of signcryption (hybrid signcryption) obtained by combining this construction and an IND-OT secure DEM.

The existing constructions [CMSM11,NS13]:

- These are generic constructions satisfying both securities of MU-IND-iCCA and MU-sUF-iCMA.
- We can obtain lattice-based ones by applying lattice-based primitives.

The Model

Setup phase：

$prm \leftarrow \mathrm{Setup}(1^n)$

Sender

Receiver

Key-Generation:

$(pk_S, sk_S) \leftarrow \mathrm{KeyGen}_S(prm)$

Signcrypt:

$C \leftarrow \mathrm{SC}\ (pk_R, sk_S, \mu)$

C →

Key-Generation:

$(pk_R, sk_R) \leftarrow \mathrm{KeyGen}_R(prm)$

Unsigncrypt:

$\mu/\bot \leftarrow \mathrm{USC}\ (pk_S, sk_R, C)$

n:	Security parameter,	prm:	Public parameter,
pk_S:	Sender's public key,	pk_R:	Receiver's public key,
sk_S:	Sender's secret key,	sk_R:	Receiver's secret key,
μ:	Message,	C:	Ciphertext
$\bot$:	Invalid		

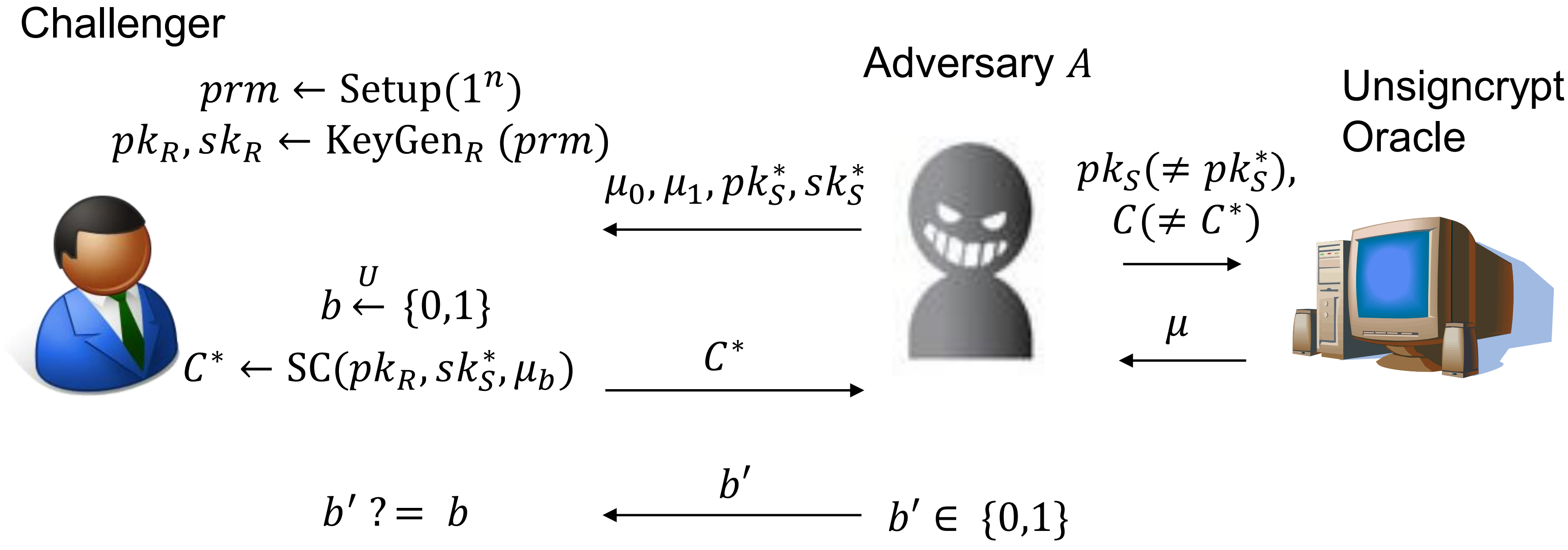
The Security Definition (1/2)

MU-IND-iCCA security

In the following game, if any adversary $A's$ advatage

$Adv_A^{\mathrm{MU-IND-iCCA}}(n) := |\Pr[b' = b] - \frac{1}{2}| < \mathrm{negl}(n)$ holds,

Signcryption meets MU-IND-iCCA security.



Challenger

$prm \leftarrow \mathrm{Setup}(1^n)$

$pk_R, sk_R \leftarrow \mathrm{KeyGen}_R\ (prm)$

Adversary A

Unsigncrypt Oracle

$\xleftarrow{\mu_0, \mu_1, pk_S^*, sk_S^*}$

$\xrightarrow{pk_S(\neq pk_S^*),\ C(\neq C^*)}$

$\xleftarrow{\mu}$

$b \overset{U}{\leftarrow} \{0,1\}$

$C^* \leftarrow \mathrm{SC}(pk_R, sk_S^*, \mu_b)$

$\xrightarrow{C^*}$

$b'\ ?=\ b$

$\xleftarrow{b'}$

$b' \in \{0,1\}$

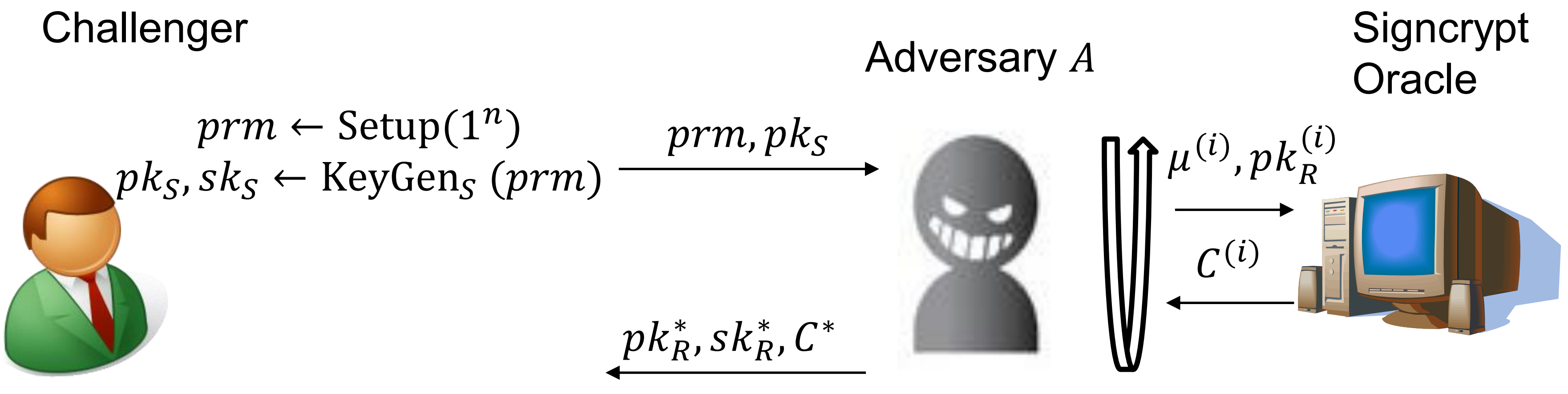
MU-IND-iCCA=Multi-User Indistinguishability against insider Chosen Ciphertext Attack

The Security Definition (2/2)

MU-sUF-iCMA security

In the following game, if any adversary A's advantage

$Adv_A^{\mathrm{MU-sUF-iCMA}}(n) \coloneqq \Pr[A \text{ wins}] < \mathrm{negl}(n)$ holds,
Signcryption meets MU-sUF-iCMA security.



Challenger

Adversary A

Signcrypt Oracle

$prm \leftarrow \mathrm{Setup}(1^n)$
$pk_S, sk_S \leftarrow \mathrm{KeyGen}_S\ (prm)$

$\xrightarrow{prm,\ pk_S}$

$\mu^{(i)}, pk_R^{(i)}$ $\longrightarrow$

$C^{(i)}$ $\longleftarrow$

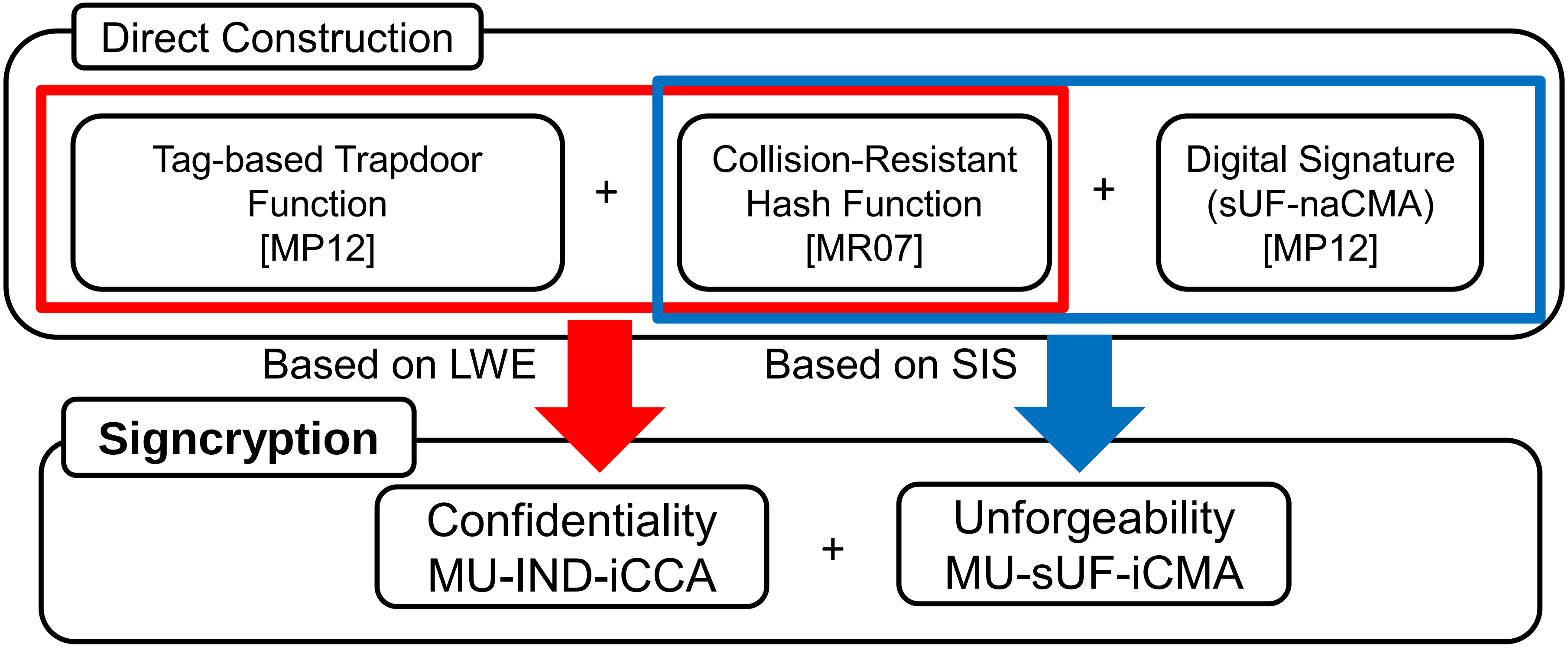
$\xleftarrow{pk_R^*,\ sk_R^*,\ C^*}$

Q queries

[A wins]:
$\mathrm{USC}(prm, pk_S, sk_R^*, C^*) = \mu^* \ \wedge$
$\forall i \in \{1, \ldots, Q\}, (pk_R^*, \mu^*, C^*) \neq \left(pk_R^{(i)}, \mu^{(i)}, C^{(i)}\right)$

MU-sUF-iCMA=Multi-User strong Unforgeability against insider Chosen Message Attack

Primitives used in Our Construction


Direct Construction
Tag-based Trapdoor Function [MP12]
+
Collision-Resistant Hash Function [MR07]
+
Digital Signature (sUF-naCMA) [MP12]
Based on LWE
Based on SIS
Signcryption
Confidentiality MU-IND-iCCA
+
Unforgeability MU-sUF-iCMA

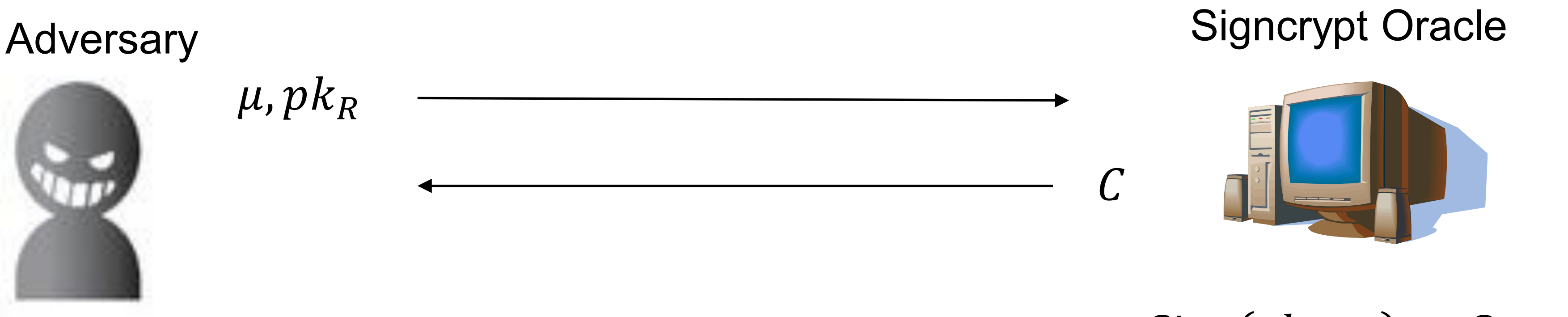
[MP12] D. Micciancio, C. Peikert: "Trapdoor for lattices: Simpler, tighter, faster, smaller," EUROCRYPT 2012.

[MR07] D. Micciancio, O. Regev: "Worst-case to average-case reductions based on gaussian measures," SIAM J. Comput. 2007.

The Problem of Sign-then-Encrypt paradigm

In the MU-sUF-iCMA game, inside adversaries can generate forgeries as follows:

1. Submit a query to the signcrypt oracle and receive the response,
2. Decrypt the message/signature-pair (μ, S) by using sk_R,
3. Encrypt (μ, S) again and output a forgery C^*.



Adversary

Signcrypt Oracle

μ, pk_R

C

$\mathrm{Dec}(sk_R, \sigma\ ) \rightarrow \mu || S$

$\mathrm{Enc}(pk_R, (\mu || S); r') \rightarrow C^*$

$\downarrow$

A valid forgery (pk_R, sk_R, C^*)
in the MU-sUF-iCMA game

$\mathrm{Sign}(sk_S, \mu\ ) \rightarrow S$

$\mathrm{Enc}(pk_R, (\mu || S); r) \rightarrow C$

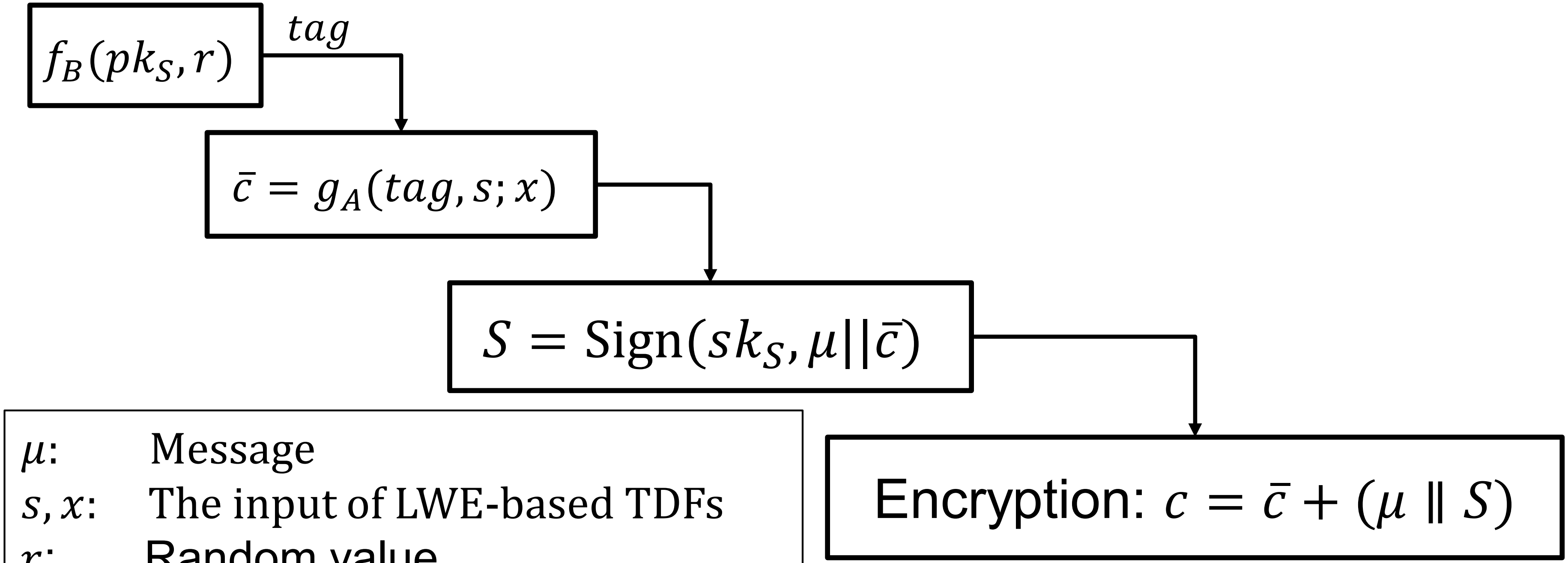
where r is a random number

Basic Idea of Our Construction

Our Idea to solve the problem:

Generate a signature on injective tag-based trapdoor functions (TDFs) of LWE $g_A(tag, s; x) = s^\top A_{tag} + x^\top \in \mathbb{Z}_q^m$ [MP12]

Overview of SC algorithm



$f_B(pk_S, r)$

tag

$\bar{c} = g_A(tag, s; x)$

$S = \mathrm{Sign}(sk_S, \mu || \bar{c})$

Encryption: $c = \bar{c} + (\mu \parallel S)$

⇒ ciphertext $C = (c, r)$

μ: Message

s, x: The input of LWE-based TDFs

r: Random value

$f_B(\cdot)$: Lattice-based collision-resistant hash function (with a parameter B)

Why can the Idea solve the Problem ?

- The reason that simple Sign-then-Encrypt constructions are broken:

  By using a new random number, it is possible to compute a ciphertext on the message/signature pair generated by the SC oracle.

- The process of our Construction

  Our SC algorithm generates a signature on both of a message and the input (random number) of the LWE-based trapdoor function [MP12]

⇒ To use new random numbers, adversaries have to break the underlying digital signature.

Our Lattice-based Signcryption (1/3)

$prm \leftarrow Setup(1^n)$:

- $q = poly(n)$
- $\bar{m} = O(n\log q)$
- $m = \bar{m} + n\lceil \log q \rceil$
- $\alpha^{-1} = O(n\log q) \cdot \omega(\sqrt{\log n})$
- $\delta = O(n\log q) \cdot \omega(\sqrt{\log n})$
- ℓ: the bit-length of messages
- $p = \Omega(q\delta^{-1})$
- G: a gadget matrix [MP12]
- $A_1, \ldots, A_{n\lceil \log q \rceil} \leftarrow \mathbb{Z}_q^{n\times m}$
- $B \leftarrow \mathbb{Z}_q^{n\times m}$
- Output

$prm =$
$(n, q, \bar{m}, m, \alpha, \delta, \ell, p, G, A_1, \ldots, A_{n\lceil \log q \rceil}, B)$

$(pk_R, sk_R) \leftarrow KeyGen_R(prm)$

1. $\bar{A}_R \leftarrow \mathbb{Z}_q^{n\times m}$,
2. $T_R \leftarrow D_\delta^{\bar{m}\times n\lceil \log q \rceil}$
3. $A_R = [\bar{A}_R \mid -\bar{A}_R \cdot T_R]$
4. Output $pk_R = A_R, sk_R = T_R$

$(pk_S, sk_S) \leftarrow KeyGen_S(prm)$

1. $\bar{A}_S \leftarrow \mathbb{Z}_q^{n\times m}$,
2. $T_S \leftarrow D_\delta^{\bar{m}\times n\lceil \log q \rceil}$
3. $A_S = [\bar{A}_S \mid G - \bar{A}_S \cdot T_S]$
4. Output $pk_S = A_S, sk_S = T_S$

Our Lattice-based Signcryption (2/3)

$C \leftarrow SC(pk_R, sk_S, \mu)$:

1. $r_e, r_s \leftarrow D^m_{\omega(\log n)}$,
2. $t = f_{\overline{A_R}}(pk_s) + f_B(r_e) \in \mathbb{Z}_q^n$,
3. $A_R = [\overline{A_R} \mid H(t)G - \overline{A_R} \cdot T_R]$
4. $s \leftarrow \mathbb{Z}_q^n,\ x_0 \leftarrow D^m_{\alpha q}, x_1 \leftarrow D^{\ell}_{\alpha q}$,
5. $\bar{c_0} = s^\top A_{R,t} + p x_0^\top \in \mathbb{Z}_q^m$,
6. $\bar{c_1} = s^\top U + p x_1^\top \in \mathbb{Z}_q^\ell$
7. $\bar{C} = (\bar{c_0}, \bar{c_1}, r_e)$,
8. Generate a signature on $\mu \parallel pk_R \parallel \bar{C}$,
   - $h = f_{A_S}(\mu \parallel pk_R \parallel \bar{C}) + f_B(r_s) \in \mathbb{Z}_q^n$,
   - $A_{S,h} = \left[A_S \,\middle|\, A_0 + \sum_{i=1}^{n\lceil \log q \rceil} h_i \cdot A_i \right]$,
   - $e \leftarrow Sample(T_S, A_{S,h}, u_S, \delta)$,
   - (e, r_s) is the signature,
9. $c_0 = \bar{c_0} + r_s \in \mathbb{Z}_q^m, c_1 = \bar{c_1} + p \cdot \mu \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q^\ell$
10. Output $C = (c_0, c_1, r_e, e)$

Our Lattice-based Signcryption (3/3)

$\mu/\perp \leftarrow USC(pk_S, sk_R, C)$:

1. $t = f_{\overline{A_R}}(pk_S) + f_B(r_e) \in \mathbb{Z}_q^n$,
2. $(z, r_s) \leftarrow Invert\left(T_R, A_{R,t}, c_0\right)$,
3. $E \leftarrow Sample\left(T_R, A_{R,t}, U, \delta\right)$,
4. $v^\top = c_1^\top - c_0^\top E = p\left(x_1^\top + \mu\left\lfloor\frac{q}{2}\right\rfloor - x_0^\top E\right)$,
5. Recover μ from v/p
6. Output μ if $A_{S,h} \cdot e = u_S \bmod q$ and $\|\boldsymbol{e}\| \leq \delta\sqrt{m + n\lceil\log q\rceil}$, or output ⊥ otherwise.

where

- $\bar{c_0} := c_0 - r_s, \bar{c_1} := c_1 - p \cdot \mu\left\lfloor\frac{q}{2}\right\rfloor, \bar{C} := (\bar{c_0}, \bar{c_1}, r_e)$,
- $h := f_{\overline{A_S}}(\mu \parallel pk_R \parallel \bar{C}) + f_B(r_s)$,
- $A_{S,h} := [A_S \mid A_0 + \sum_{i=1}^{\lceil n\log q\rceil} A_i]$,

The Security of the Lattice-based Signcryption

Theorem 1.

- Our lattice-based signcryption meets MU-IND-iCCA security, if the $LWE_{q,\alpha}$ assumption holds for

$$\alpha^{-1} = O(n^2 \log^2 q) \cdot \omega(\log n).$$

- Our lattice-based signcryption meets MU-sUF-iCMA security, if the $SIS_{q,\beta}$ assumption holds for

$$\beta = O(n^{2.5} \log^{2.5} q) \cdot \omega(\log n).$$

Hybrid enc. version of Our Signcryption (HSC)

$C \leftarrow SC(pk_R, sk_S, \mu)$:

1. $K \leftarrow \{0,1\}^{\ell}, r_e, r_s \leftarrow D^m_{\omega(\log n)}$,
2. $t = f_{\overline{A_R}}(pk_s) + f_B(r_e) \in \mathbb{Z}_q^n$,
3. $A_R = [\overline{A_R} \mid H(t)G - \overline{A_R} \cdot T_R]$
4. $s \leftarrow \mathbb{Z}_q^n,\ x_0 \leftarrow D^m_{\alpha q}, x_1 \leftarrow D^{\ell}_{\alpha q}$,
5. $\bar{c_0} = s^{\top} A_{R,t} + p x_0^{\top} \in \mathbb{Z}_q^m$,
6. $\bar{c_1} = s^{\top} U + p x_1^{\top} \in \mathbb{Z}_q^{\ell}$
7. $\bar{C} = (\bar{c_0}, \bar{c_1}, r_e)$,
8. Generate a signature on

   $\mu \parallel pk_R \parallel \bar{C} \parallel K$,

   - $h = f_{A_S}(\mu \parallel pk_R \parallel \bar{C} \parallel K) + f_B(r_s) \in \mathbb{Z}_q^n$,
   - $A_{S,h} = \left[A_S \,\middle|\, A_0 + \sum_{i=1}^{n\lceil \log q \rceil} h_i \cdot A_i \right]$,
   - $e \leftarrow Sample(T_S, A_{S,h}, u_S, \delta)$,
   - (e, r_s) is the signature,
9. $c_0 = \bar{c_0} + r_s \in \mathbb{Z}_q^m$,

   $c_1 = \bar{c_1} + p \cdot K \left\lfloor \frac{q}{2} \right\rceil \in \mathbb{Z}_q^{\ell}$,
10. $c_2 = DEM.Enc(K, \mu)$,
11. Output $C = (c_0, c_1, c_2, r_e, e)$

$Setup, KeyGen_R, KeyGen_S, USC$ are almost the same as those of the lattice-based construction.

The Security of HSC

Theorem 2.

- HSC meets MU-IND-iCCA security, if the $LWE_{q,\alpha}$ assumption holds for $\alpha^{-1} = O(n^2 \log^2 q) \cdot \omega(\log n)$ and DEM satisfies IND-OT security.
- HSC meets MU-sUF-iCMA security, if the $SIS_{q,\beta}$ assumption holds for $\beta = O(n^{2.5} \log^{2.5} q) \cdot \omega(\log n)$ and DEM is one-to-one (*).

(*) one-to-one property: DEM is one-to-one if for any message μ and any key K, there is only one ciphertext c such that $\mu = DEM.Dec(K, c)$.

Lattice-based Constructions

To compare lattice-based schemes fairly, we compare our hybrid Signcryption (HSC) scheme with others, because other constructions [CMSM11] are based on the KEM/DEM framework.

Construction	Primitive
SC_{TK} [CMSM11]	• IND-Tag-CCA secure Tag-based KEM • IND-CCA secure DEM • sUF-CMA secure DS
SC_{KEM} [CMSM11]	• IND-CCA secure KEM • IND-OT secure DEM • sUF-CMA secure DS • sUF-OT secure MAC
SC_{CHK} [NS13]	• IND-sID-CPA secure ID-based Encryption • UF-CMA secure DS • sUF-OT secure One-time Signature
Our Construction HSC	• The First Lattice-based Construction • IND-OT secure DEM

Concrete Existing Constructions

Existing Construction	Applied Constructions of Primitives
SC_{TK} [CMSM11]	• Tag-based KEM ([MP12] and [CHKP12]) • DEM • DS ([MP12] and [CHKP12])
SC_{KEM} [CMSM11]	• KEM ([MP12] and [BCHK07]) • DEM • DS ([MP12] and [CHKP12]) • MAC
SC_{CHK} [NS13]	• ID-based Encryption [ABB10] • DS [B10] • One-time Signature [LM08]

[ABB10] S. Agrawal, D. Boneh, X. Boyen, "Efficient lattice (H)IBE in the standard model," EUROCRYPT 2010.

[B10] X. Boyen, "Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more," PKC 2010.

[CHKP12] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert: "Bonsai trees, or how to delegate a lattice basis," J. Cryptology 2012.

[LM08] V. Lyubashevsky, D. Micciancio, "Asymptotically efficient lattice-based digital signatures," TCC 2008.

Comparison

Construction	Receiver's key size		Sender's key size		Ciphertext size
	Public key	Secret key	Public key	Secret key	
SC_{TK}	$3nm\log q$ $+ nK\log q$	$nm\log q\log d$	$3nm\log q$	$nm\log q\log d$	$(m+K)\log q$ $+ 3m\log d + \ell$
SC_{KEM}	$2nm\log q$ $+ nK\log q$				$(2m+K)\log q$ $+ 2m\log d$ $+ 2n\log q + \ell$
SC_{CHK}	$nm\log q$ $+ nK\log q$ (Best)		$nm\log q$ (Best)		$(2m+K)\log q$ $+ m\log d + \ell$ $+ \lvert vk\rvert$
Our Const. HSC					$(m+K)\log q$ $+ 2m\log d + \ell$

n: security parameter, q: a large enough prime, $|\mu|$: the bit-length of a message

$m = \Omega(n\log q)$, K: DEM's symmetric key, $d < q$: a positive integer

$|vk|$: the bit-lenthg of One-Time Signature's verification key size

Comparison Based on Parameters of [LP11]

Parameters	Size [bits]
n	256
q	4093
m	9215
K	512
d	49148
$\|vk\| \approx n^2 \log^2 n$	42.0×10^5

Comparison of ciphertext	Ciphertext-Size (Bit-length)
SC_{TK}	5.5×10^5
SC_{KEM}	5.2×10^5
SC_{CHK}	45.3×10^5
Our Const. HSC	4.0×10^5 (Best)

Note: We can observe that our construction is best, even if we apply other parameters in [ACF+15].

[ACF+15] M.R. Albrecht, C. Cid, J. Faugère, R. Fitzpatrick, L. Perret: “On the complexity of the BKW algorithm on LWE,” Des. Codes Cryptography 2015.

[LP11] R. Lindner, C. Peikert: “Better ey sizes (and attacks) for LWE-based encryption,” CT-RSA 2011.

Conclusion

We did the following:

- Proposing a lattice-based construction meeting both MU-IND-iCCA and MU-sUF-iCMA security;
- Constructing a hybrid signcryption by combining the lattice-based construction and an IND-OT secure DEM;
- Showing that public-key sizes and ciphertext size of the hybrid signcryption are smaller than those of the existing constructions.