EMBLEM and R.EMBLEM

1st NIST PQC Conference

2018.04.12.

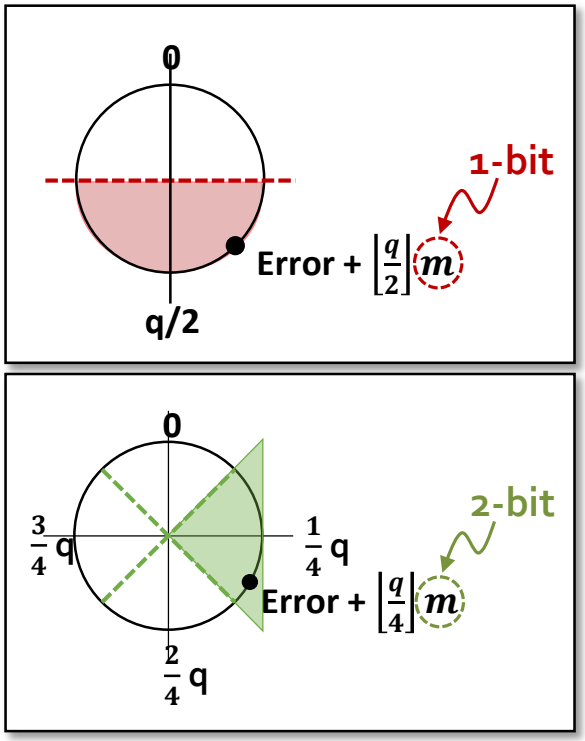
Minhye Seo, Suhri Kim, Dong Hoon Lee,
Seokhie Hong, Jongsun Park, Jong Hwan Park

KOREA UNIVERSITY

Learning with Errors

- **LWE-based encryption schemes***
  - public key : $(A, B = AS + E)$ Gaussian errors
  - ciphertext : $(C_1, C_2) = \left(R^T A + E_1, R^T B + E_2 + \left\lfloor \frac{q}{2} \right\rfloor m\right)$

→ Decryption : $C_2 - C_1 S = \underbrace{(R^T E + E_2 - E_1 S)}_{\text{Decryption error}} + \left\lfloor \frac{q}{2} \right\rfloor \cdot m$

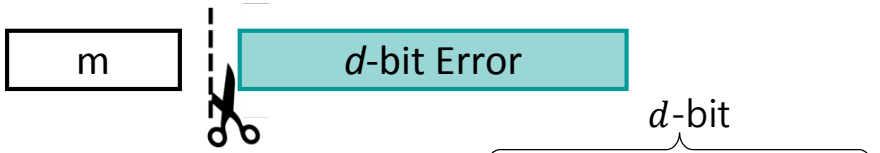


  - » **1-bit** message encoding : $\left\lfloor \frac{q}{2} \right\rfloor \cdot \boldsymbol{m}$
    - If **|error|** $< \frac{q}{4}$, we can distinguish whether m is 0 or 1
  - » ***t*-bit** message encoding : $\left\lfloor \frac{q}{2^t} \right\rfloor \cdot \boldsymbol{m}$ (generalized)
    - If **|error|** $< \frac{q}{2^{t+1}}$, we can recover the message correctly
  - Operations (required for decryption)
    - » 1 matrix multiplication + 1 matrix subtraction + ***rounding operations***

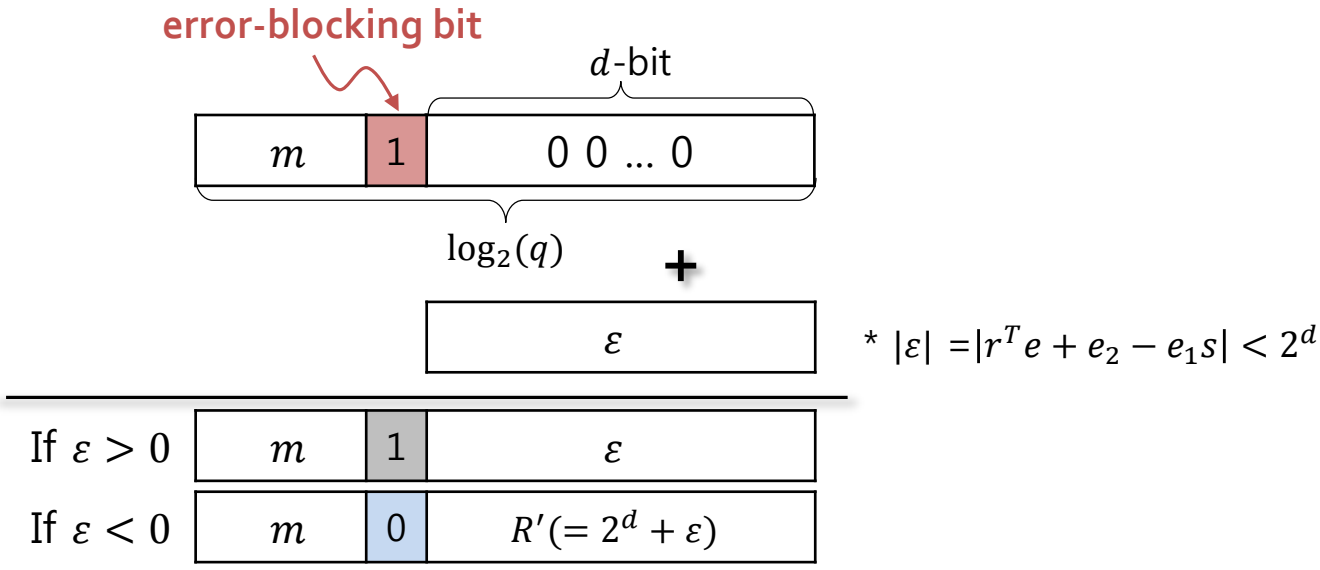
* [LP11] Better Key Sizes (and Attacks) for LWE-Based Encryption, CT-RSA 2011.

New Encoding Method

- ***Separate*** **the message *from* the error!**



  - Estimate the absolute size of the error (d-bit) →
  - Concatenate $(1||0^d)$ on each message block

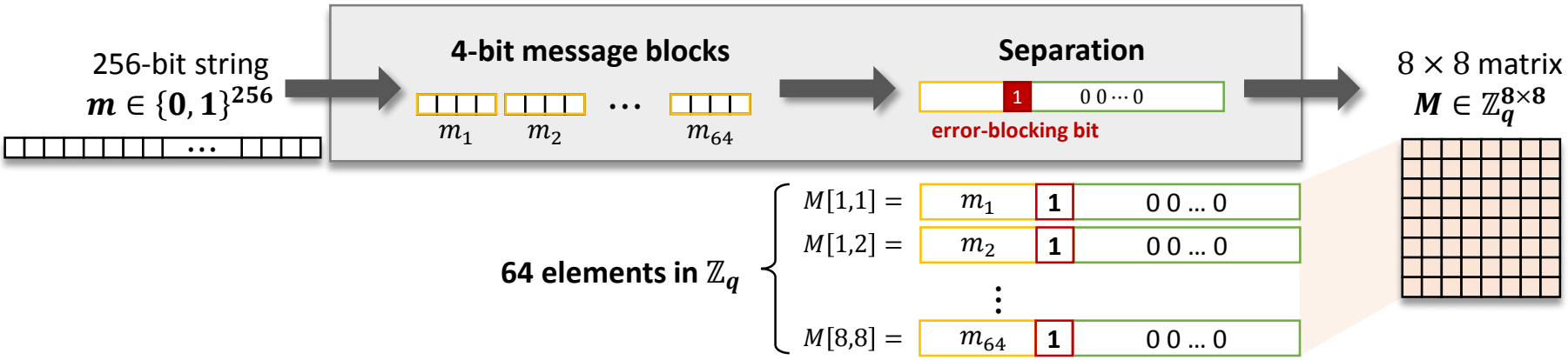


→ In the **decryption** phase, the error does ***not affect*** the message

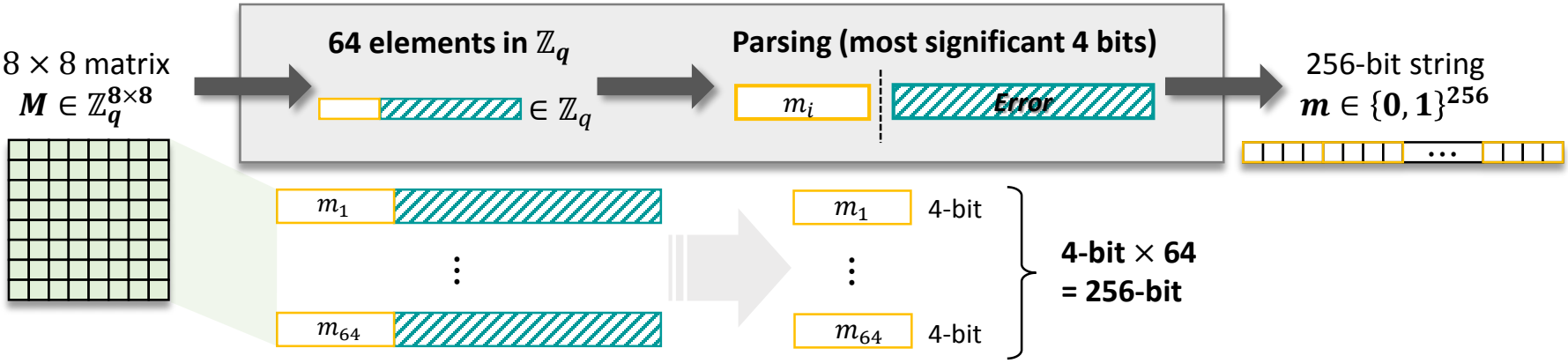
→ Intuitively extend to **multi-bit** encoding ***by prefixing*** it with the error-blocking bit

New Encoding Method

- **Encoding**



- **Decoding**



EMBLEM

(**E**rror-blocked **M**ulti-**B**it **L**WE-based Key **E**ncapsulation **M**echanism)

KOREA UNIVERSITY

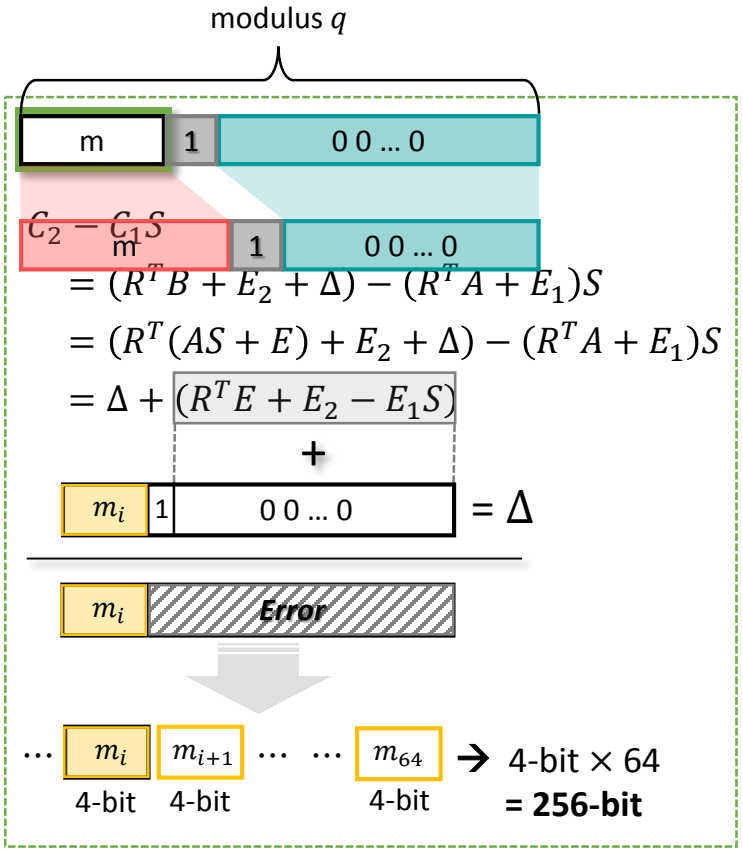
EMBLEM (Error-blocked Multi-Bit Lwe-based kEM)

❖ IND-CPA secure Public Key Encryption scheme

- **KeyGen (1^λ) → (pk,sk)**
  - **pk** = $(A, B = AS + E) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^{m\times k}$
  - **sk** = $s \in \{0,1\}^{256}$ → $S \in [-B, B]^{n\times k}$ (B = 1,2)

- **Encrypt (pk,m) → CT**
  - $r \leftarrow_R \{0,1\}^{256}; (R, E_1, E_2) \leftarrow Sample(r)$
    - » $R \in [-B, B]^{m\times v}$, $(E_1, E_2) \in \mathcal{D}_\sigma^{v\times n} \times \mathcal{D}_\sigma^{v\times k}$
  - $\Delta \leftarrow$ **Encode**(m, t, q)
  - $C_1 = R^T A + E_1,\ C_2 = R^T B + E_2 + \Delta$

- **Decrypt (CT,sk) → m**
  - $m \leftarrow$ **Decode**$(C_2 - C_1 S, t, q)$

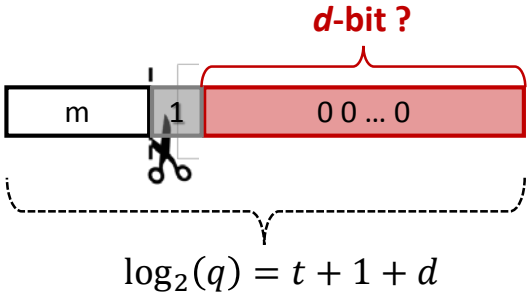


IND-CPA secure **PKE** scheme (under binary LWE) → **Fujisaki-Okamoto transformation** → **IND-CCA** secure **KEM** ***"EMBLEM"***

Parameter Selection

- **Binary LWE***
  - Binary LWE problem is ***as hard as*** LWE problem as long as increasing the dimension n **by a factor of** $log(log(n))$

- **Measure decryption error (*d*-bit)** : $|R^T E + E_2 - E_1 S| \in \mathbb{Z}_q^{v \times k}$
  - Probability of decryption failure : 2^{-140}
  - $|r^T e + e_2 - e_1 s| < |\langle r, e \rangle| + |e_2| + |\langle e_1, s \rangle| < 2^d$



  - » **Lemma 1.** $\Pr[|\langle x, \mathcal{GD}_s \rangle| \geq Q \cdot s\|x\|] < 2e^{-\pi Q^2}$ for $x \in \mathbb{R}^n$
    - $2e^{-\pi Q^2} = 2^{-140} \rightarrow Q \approx 5.5776$
    - $|\langle r, e \rangle| = Q \cdot s\|r\| = Q \cdot \sigma\sqrt{2\pi} \cdot \|r\| = 5.5776 \times 25\sqrt{2\pi} \times \sqrt{\frac{2}{3} \cdot m} \approx 2^{13.15}$
    - $|\langle e_1, s \rangle| = Q \cdot s\|s\| = Q \cdot \sigma\sqrt{2\pi} \cdot \|s\| = 5.5776 \times 25\sqrt{2\pi} \times \sqrt{\frac{2}{3} \cdot n} \approx 2^{13}$
  - » **Lemma 2.** $\Pr[|z| > T\sigma] < 2e^{-T^2/2}$ for $z \leftarrow \mathcal{GD}_\sigma$
    - $2e^{-T^2/2} = 2^{-140} \rightarrow T \approx 13.98$
    - $|e_2| = T\sigma = 13.98 \times 25 \approx 2^{8.45}$

[m=1008, n=824, σ=25] → $|\langle r, e \rangle| + |e_2| + |\langle e_1, s \rangle| < 2^{13.15} + 2^{8.45} + 2^{13} \approx 2^{14.1} < 2^d \rightarrow d = 15$

If we encode the message by 4-bit → $log_2(q) = 4 + 1 + 15 = 20$**-bit**

* [BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, Classical Hardness of Learning with Errors, STOC 2013.
* [BG14] S. Bai and S. D. Galbraith, Lattice Decoding Attacks on Binary LWE, ACISP 2014
* [APS15] M. R. Albrecht, R. Player, and S. Scott, On the Concrete Hardness of Learning with Errors, J. Math. Crypt. 2015

R.EMBLEM

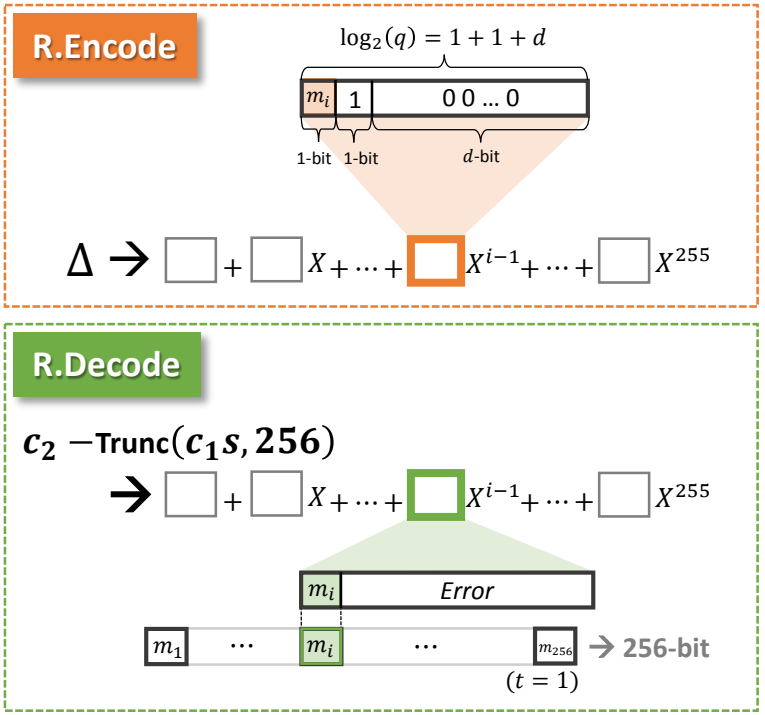
(EMBLEM over Rings)

KOREA UNIVERSITY

R.EMBLEM

❖ IND-CPA secure Public Key Encryption scheme (over Rings)

- **KeyGen (1^λ) → (pk,sk)**
  - **pk** = $(a, b = as + e) \in R_q^2$
  - **sk** = $\{0,1\}^{256}$ → $s \in R_q$
    - » $(s_1, \dots, s_n) \in_R [-1,1]^n$
- **Encrypt (pk,m) → CT**
  - $z \leftarrow_R \{0,1\}^{256}$; $(r, e_1, e_2) \leftarrow Sam(z)$
    - » $(r_1, \dots, r_n) \in [-1,1]^n$
  - $\Delta \leftarrow$ **R.Encode**(m, t, q)
  - $c_1 = r \cdot a + e_1,\ c_2 = \textbf{Trunc}\left(r \cdot b + e_2 + \Delta, \frac{256}{t}\right)$
- **Decrypt (CT,sk) → K**
  - $m \leftarrow$ **R.Decode**$\left(c_2 - \textbf{Trunc}\left(c_1 \cdot s, \frac{256}{t}\right), t, q\right)$



IND-CPA secure **PKE** scheme (under binary RLWE) → **Fujisaki-Okamoto transformation** → **IND-CCA** secure **KEM** ***"R.EMBLEM"***

Parameter Selection

- Parameter setting ***(changed!)***
  - Target security level : 128-bit [APS15], Message space : $\{0,1\}^{256}$
  - Adopted binary (or small secret) LWE [BG14,APS15]

	EMBLEM				R.EMBLEM			
(Secret distribution)	[-1,1]		[-2,2]		[-1,1]		[-2,2]	
m	1186	1008	1210	1016	-	-	-	-
n	1024	824	984	784	512	1024	512	1024
$\approx \log_2(q)$	24	20	24	20	16	14	16	14
σ	25	25	25	25	29	3	29	3
t (encoding unit)	8	4	8	4	1	1	1	1
PK size (bytes)	28,496	20,192	29,072	20,352	1,056	1,824	-	1,824
SK size (bytes)	32	32	32	32	32	32	-	32
CT size (bytes)	12,416	16,672	11,936	15,872	1,568	2,272	-	2,272

* [APS15] M. R. Albrecht, R. Player, and S. Scott, On the Concrete Hardness of Learning with Errors, J. Math. Crypt. 2015
* [BG14] S. Bai and S. D. Galbraith, Lattice Decoding Attacks on Binary LWE, ACISP 2014

Performance Analysis

- **Software** (Intel core i7-6700 (Skylake) @ 3.40GHz)

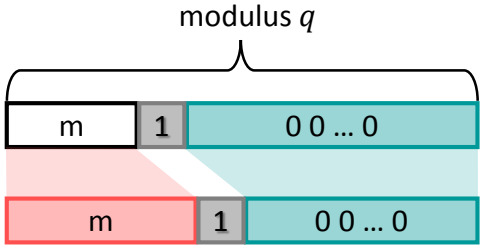
EMBLEM			
	KeyGen	**Encap**	**Decap**
[-1,1], 8-bit encoding	21.005 ms	5.247 ms	5.115 ms
[-1,1], 4-bit encoding	13.063 ms	4.000 ms	3.919 ms
[-2,2], 8-bit encoding	19.082 ms	5.445 ms	5.275 ms
[-2,2], 4-bit encoding	14.515 ms	4.055 ms	3.977 ms
R.EMBLEM			
[-1,1], 1-bit encoding	**KeyGen**	**Encap**	**Decap**
n=512, σ=29	0.055 ms	1.015 ms	1.045 ms
n=1024, σ=3	0.128 ms	2.363 ms	2.431 ms

- **Hardware** (FPGA : DE2-115)
  - R.EMBLEM : $[-1,1], t = 1, \boldsymbol{\sigma = 25}$

	KeyGen	**Encap**	**Decap**
R.EMBLEM	0.0063 ms	0.0093 ms	0.0162 ms

Summary

- **Security assumption : Binary (or Small secret) LWE**
  - – Increasing the size of dimension n
  - + Reducing the size of decryption error
    - → Encode "*more*" bits at a time using the *same* modulus q
    - → Encoding multiple bits at a time can *offset* the inefficiency of increasing n
  - + Making a secret key shorter
    - → Store a 256-bit string as a secret key



- **New *alternative* of encoding for LWE-based encryption schemes**
  - – Comprehensible for encoding multiple bits
    - → Can be useful for designing more advanced cryptographic primitives

- **Parameter selection**
  - – Negligible probability of decryption failure ($\approx 2^{-140}$)
  - – Providing a 128-bit security level

Q&A