The 8-th International Workshop on Data Privacy Management (DPM 2013)
September 12th – 13th, 2013 (Egham, UK)

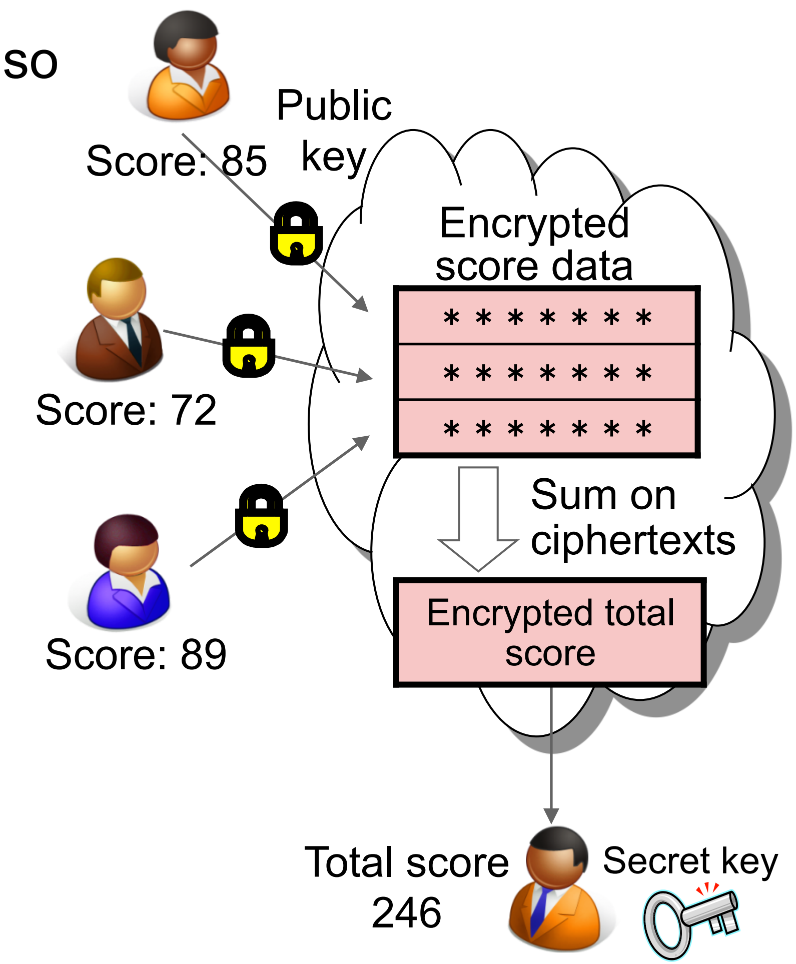
FUJITSU
shaping tomorrow with you

Practical Packing Method in Somewhat Homomorphic Encryption

Masaya Yasuda, Takeshi Shimoyama, Jun Kogure
(Fujitsu Laboratories Ltd.),
Kazuhiro Yokoyama (Rikkyo University), and
Takeshi Koshiba (Saitama University)

Homomorphic Encryption (HE)

- Public-key encryption supporting "some operations" on encrypted data
  - It enables us to compute the total score so that the cloud cannot know any score
- Additively HE
  - Practical in performance, but it can only support addition (e.g., Paillier scheme)
  - Limited applications (e.g., e-voting)
- FHE (fully HE)
  - Breakthrough by Gentry [1] in 2009
  - It supports any operations, and is expected to applied to cloud computing
  - But, difficulty on performance and size



[1] C. Gentry, "Fully homomorphic encryption using ideal lattices", STOC 2009.

Summary of Our Work

- SHE (Somewhat HE)
  - It supports “a limited number” of additions and multiplications
    - Well known as a building block for the FHE construction
  - Much faster and shorter than FHE
    - (Performance and Size) Additively HE < SHE << FHE
- Motivation: practical use of SHE in wider applications
- Contributions:
  - New packing method in SHE for the practical use
    - Use of the ring-LWE based LWE scheme
    - Our method can pack a vector into a single ciphertexts
    - It gives several efficient computations over packed ciphertexts
  - Application to privacy-preserving biometrics
    - Our method gives faster performance and shorter size for secret authentication in the HE approach

Ring-LWE Based SHE Scheme

Key Generation

- Secret key $\mathrm{sk}=s$, Public key $\mathrm{pk}=(a_0, a_1)$
  - $a_0=-(a_1 s+te)$ in R_q, s, a_1, e: small noises in R_q
  - $R=\mathbb{Z}[x]/(x^n+1)$: base ring, t: plaintext modulus, q: ciphertext modulus

Encryption

- For a palintext $m\in R_t$, $\mathrm{Enc}(m,\mathrm{pk})=(c_0, c_1)\in(R_q)^2$
  - $c_0=a_0 u+tg+m$, $c_1=a_1 u+tf$
  - u, g, f: small noises in R_q

Homomorphic Operations

- [Add] $\mathrm{Enc}(m,\mathrm{pk})+\mathrm{Enc}(m', \mathrm{pk}):=(c_0+c'_0, c_1+c'_1)$
- [Mul] $\mathrm{Enc}(m,\mathrm{pk})*\mathrm{Enc}(m', \mathrm{pk}):=(c_0\cdot c'_0, c_0\cdot c'_1+c'_0\cdot c_1, c_1\cdot c'_1)$

Decryption

- For a ciphertext $\mathrm{ct}=(c_0, c_1, \ldots, c_k)$, $\mathrm{Dec}(\mathrm{ct},\mathrm{sk})=[\sum c_i\cdot s^i]_q \bmod t$ in R_t
  - $[a]_q$: a modulo q in $[-q/2, q/2)$

Introduction of Our Packing Method

Strategy

1. Transform a vector of length n to a certain polynomial in R
2. Pack its polynomial into a single ciphertext

Our Trick: two types of polynomials in $R = \mathbb{Z}[x]/(x^n + 1)$

- [Type1] $A = (A_0, \cdots, A_{n-1}) \rightarrow F_1(A) := \sum A_i x^i$ (ascending order)
- [Type2] $B = (B_0, \cdots, B_{n-1}) \rightarrow F_2(B) := -\sum B_i x^{n-i}$ (descending order)

Packed ciphertexts

- [Type1] $\mathrm{vEnc}_1(A) := \mathrm{Enc}(F_1(A), \mathrm{pk})$
- [Type2] $\mathrm{vEnc}_2(B) := \mathrm{Enc}(F_2(B), \mathrm{pk})$
  - It does not change the security level of the SHE scheme

Efficient Secure Inner Product

Only one homomorphic multiplication

$$\mathrm{vEnc}_1(A) * \mathrm{vEnc}_2(B)$$

over packed ciphertexts gives the inner product between A and B on encrypted data

Sketch of Proof)

$F_1(A) \times F_2(B)$ over plaintexts ←corresponding→ $\mathrm{vEnc}_1(A) * \mathrm{vEnc}_2(B)$

performed on encrypted data

$$F_1(A) = A_0 + A_1 x + A_2 x^2 + \cdots + A_{n-1} x^{n-1}$$

$$\times)\quad F_2(B) = -B_{n-1} x - \cdots - B_1 x^{n-1} - B_0 x^n$$

$$F_1(A) \times F_2(B) = -(A_0 B_0 + A_1 B_1 + \cdots A_{n-1} B_{n-1}) x^n + \cdots$$

$x^n = -1$ in R

The constant term gives our desired inner product

Computations over Packed Ciphertexts

Combinations of our packed ciphertexts also give us the following computations:

- Private Statistic:
  - Sum, and Mean
  - Variance, and Standard deviation
- Statistical Analysis:
  - Covariance
  - Correlation
- Distances
  - Hamming distance
  - Euclid distance
- etc.,…

Remark: It is difficult to perform computations such as
- the median,
- the 1-norm distance

since we generally can not compare two values without decryption in the use of homomorphic encryption (irrespective of packing method).

Application to Privacy-Preserving Biometrics

Privacy-Preserving Biometrics

- Biometric authentication with protecting the privacy of biometric data

Homomorphic Encryption Approach

- **Secure Hamming distance**: metric to measure the similarity of feature vectors A, B on encrypted data
  - $d_H(A,B)=\sum_{i=0}^{2047}(A_i-B_i)^2 = \sum_{i=0}^{2047}(A_i+B_i-2A_i\cdot B_i)$
  - The authentication result is "OK" if $d_H(A,B)<\sigma$

Biometric Image

010101011
101001111
001100101
110101010

Feature Vector

Homomorphic Encryption

412ABCD11
124913FA12
FF121AB123
9192BBA112

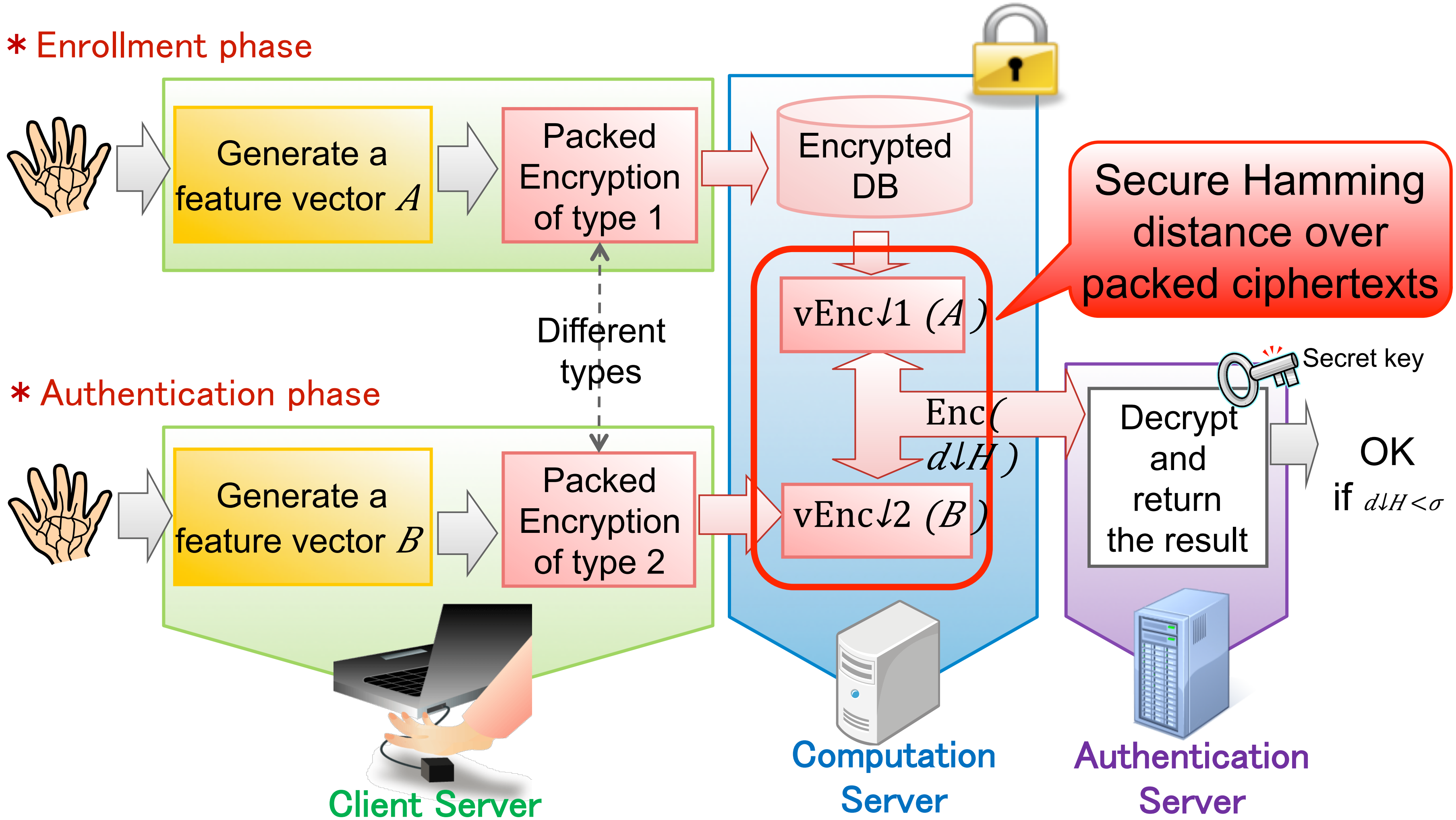
Assume 2048-bit for various biometrics (e.g., vein codes)

Secure Hamming distance in authentication

Secret Authentication with Our Method

FUJITSU

- Since all computations are performed on encrypted data, we hope that we would use “the cloud” as the computation server



Comparison with Related Work

FUJITSU

Table: A comparison on the performance and the encrypted data size

Protocols (feature vector size)	Performance of Secure Hamming	Size increase rate by encryption† (cipher. size)	Homomorphic encryption scheme
SCiFI [25] (900-bit)	310 ms[(a)]	2048 times (230 KByte)	Paillier-1024 (additive scheme)
Protocol of [2] (2048-bit)	150 ms[(b)]	1024 times (262 KByte)	DGK-1024 (additive scheme)
Previous work‡ [31] (2048-bit)	18.10 ms[(c)]	about 80 times (19 KByte)	ideal lattices-4096 (SHE)
This work (2048-bit)	**5.31 ms**[(c)]	**about 120 times (31 KByte)**	**ring-LWE-2048 (SHE)**

Only one feature vector is protected (SCiFI [25], Protocol of [2])

Two feature vectors are protected, which condition is tighter (Previous work [31], This work)

† denotes the ratio of (encrypted feature vector size)/(plain feature vector size)
‡ uses a similar packing method as in this work
(a) on an 8 core machine of 2.6 GHz AMD Opteron processors with 1 GByte memory
(b) on an Intel Core 2 Duo 2.13 GHz with 3 GByte memory
(c) on an Intel Xeon X3480 at 3.07 GHz with 16 GByte memory

[2] Osadchy et al, “SCiFI – A system for secure face identification”, IEEE Security & Privacy 2010.
[25] Blanton et al, “Secure and efficient protocols for iris and fingerprint identification”, ESORICS 2011.
[31] Yasuda et al., “Packed homomorphic encryption based on ideal lattices and its application to biometrics”, MoCrySEn 2013.

Conclusions and Future Work

FUJITSU

Conclusions

- We proposed a packing method in the ring-LWE based SHE scheme
  - Main trick: two types of packed ciphertexts
  - It gives us an efficient computation of secure inner product
- Our method gave a practical solution in privacy-preserving biometrics
  - It takes 5.31 ms for secure Hamming distance of 2048-bit vectors
  - Faster than additively schemes even under tighter condition
  - Lattice-based SHE with our packing method would be practical

Future Work

- Application of our packing method in wider applications
  - e.g., secure pattern matching for secret search

FUJITSU

shaping tomorrow with you