Homomorphic Encryption for Arithmetic of Approximate Numbers

Jung Hee Cheon*, Andrey Kim*, Miran Kim†, Yongsoo Song*

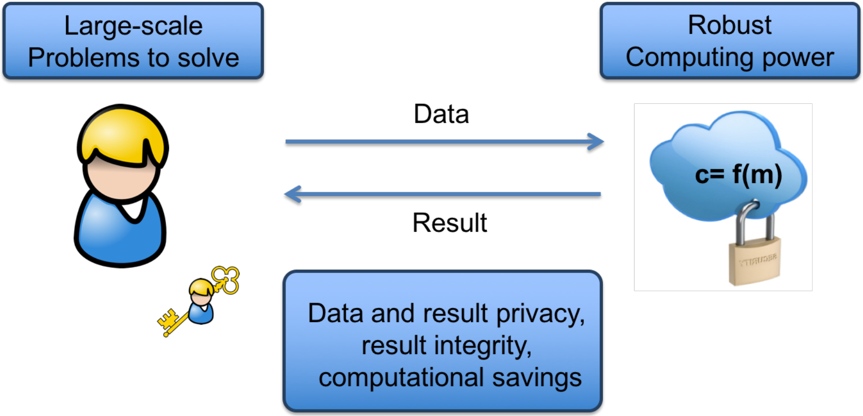
*Seoul National University
†University of California - SD

2017. 07. 12.

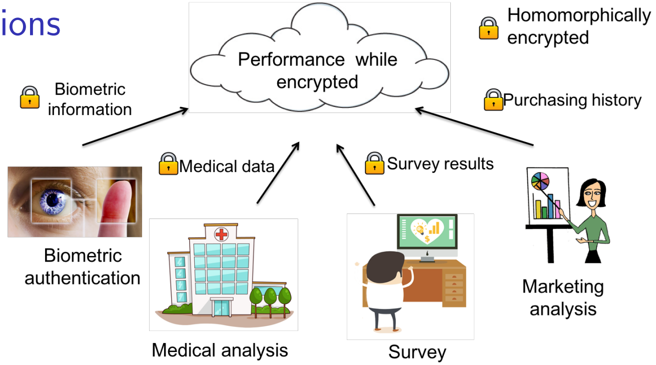
Table of contents

Homomorphic Encryption

- $c_1 \leftarrow Enc(m_1), \ldots, c_t \leftarrow Enc(m_t)$.
- $c^* \leftarrow Eval(f, c_1, \ldots, c_t), Dec(c^*) = f(m_1, \ldots, m_t)$.

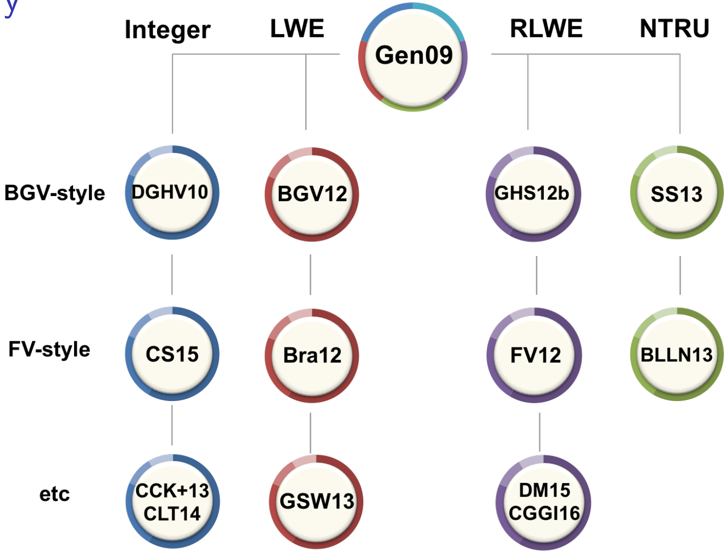


Applications



- Cloud Computing
- Medical Applications (Private data, Public functions)
- Financial Applications
- Advertising and Pricing
- Data Mining
- Biometric Authentication

History

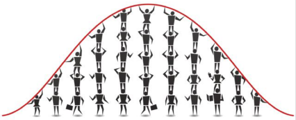

Integer
LWE
Gen09
RLWE
NTRU
BGV-style
DGHV10
BGV12
GHS12b
SS13
FV-style
CS15
Bra12
FV12
BLLN13
etc
CCK+13
CLT14
GSW13
DM15
CGGI16

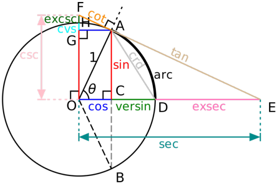
Previous Homomorphic Encryption

- An encryption c has a decryption structure $\langle c, sk \rangle = \hat{m} \pmod{q}$ for a random encoding $\hat{m}$ of message m.
  - BGV style: $\hat{m} = m + pe \xrightarrow{\text{mod } p} m$
  - FV style: $\hat{m} = \frac{q}{p}m + e \xrightarrow{\lfloor \frac{p}{q} \cdot \rceil} m$
- Support operations over *finite characteristic* plaintext spaces.
  - $\mathbb{Z}_p$, $\mathbb{Z}_p[X]/\Phi_M(X)$
  - $GF(p^d)$
- Somewhat practical implementations based on Ring structure
  - HElib (IBM), SEAL (Microsoft Research).
  - Theoretically every Boolean circuit can be evaluated in a polynomial time.

Limitation

- Many of real-world data belong to continuous spaces (e.g. $\mathbb{R}^N, \mathbb{C}^N$).
- They should be discretized (quantized) to an approximate value to be stored and used in computer systems.





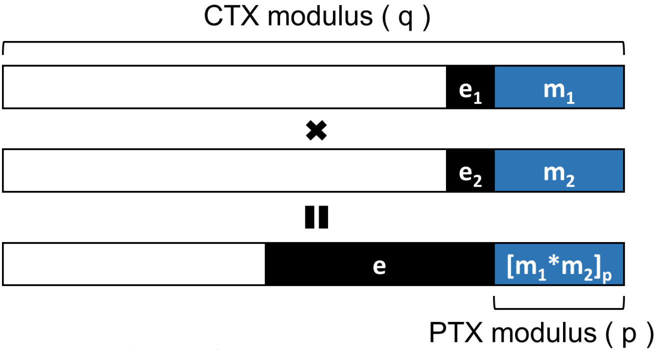
Limitation

- Current HE schemes are not adequate to the approximate arithmetic.
- Floating-point operation
  - $x = \pm(\mathit{significand}) * (\mathit{base})^{(\mathit{exponent})}$
  - Remove some inaccurate LSBs of significand after operations
  - e.g. $(2.313 * 10^4) * (3.127 * 10^{-7}) = 7.232751 * 10^{-3} \approx 7.233 * 10^{-3}$

Approximate arithmetic in HE

1. Extraction of MSBs: huge depth or expensive cost
2. Exact operations:
   - Evaluation of depth L circuit with $\eta = \log p$-bit inputs requires a large plaintext space ($\approx p^{2^L}$) and ciphertext modulus of $\log q = \Omega(2^L L \cdot \eta)$.

BGV style multiplication

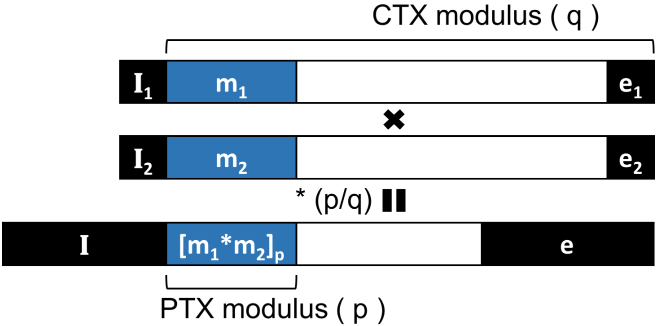


$\langle c_i, sk \rangle = m_i + pe_i \pmod{q}$.

$\langle c_{mult}, sk \rangle = (m_1 + pe_1)(m_2 + pe_2) + pe_{mult} = [m_1 m_2]_p + pe$

The MSBs of $m_1 * m_2$ is destroyed by ciphertext error.

FV style multiplication



$$\langle c_i, sk\rangle = (q/p)\cdot m_i + e_i \pmod q \Longrightarrow \langle c_i, sk\rangle = q\cdot I_i + (q/p)\cdot m_i + e_i.$$

$$\begin{aligned}\langle c_{mult}, sk\rangle &= \tfrac{p}{q}(q\cdot I_1 + (q/p)\cdot m_1 + e_1)(q\cdot I_2 + (q/p)\cdot m_2 + e_2) + e_{mult}\\ &= q\cdot I + (q/p)\cdot [m_1 m_2]_p + e.\end{aligned}$$

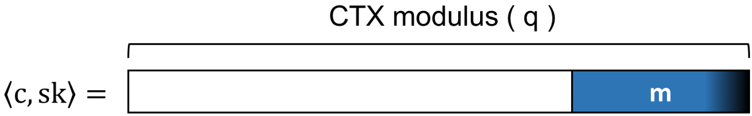
The MSBs of $m_1 * m_2$ is destroyed by ciphertext error.

Section 2

Main idea

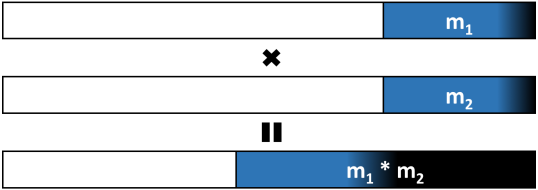
Idea 1: Embracing Noise

- An encryption of significand m satisfies $\langle c, sk \rangle = m + e \pmod q$ for some small error e.
- Consider the error added to the plaintext for security to be part of the error that occurred during approximate computations.
- The decryption structure $\hat{m} = m + e$ itself is an approximate value of the original message m.
- If $|e|$ is small enough not to destroy the significand of m, the precision is almost preserved (e.g. $m = 1.23 * 10^4, e = -17$. $\hat{m} = 12283 \approx m$).



HE Operations and Noise Estimation

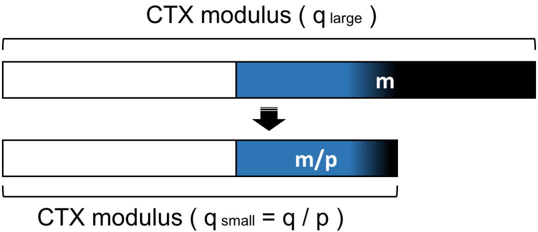
- Homomorphic operations between ciphertexts can be done by known techniques such as key-switching.



- An encryption c of m has a relative error β if $\langle c, sk \rangle = m \cdot (1 \pm \beta)$.
  - $m_1 \cdot (1 \pm \beta_1) + m_2 \cdot (1 \pm \beta_2) = (m_1 + m_2) \cdot (1 \pm \max_i \beta_i)$.
  - $m_1 \cdot (1 \pm \beta_1) * m_2 \cdot (1 \pm \beta_2) + e_{mult} \approx m_1 m_2 \cdot (1 \pm (\beta_1 + \beta_2))$.

Bit size of required modulus still increases exponentially on depth: evaluation of depth L circuit with η-bit inputs requires $\log q = \Omega(2^L \cdot \eta)$.

Idea 2: Rescaling Process

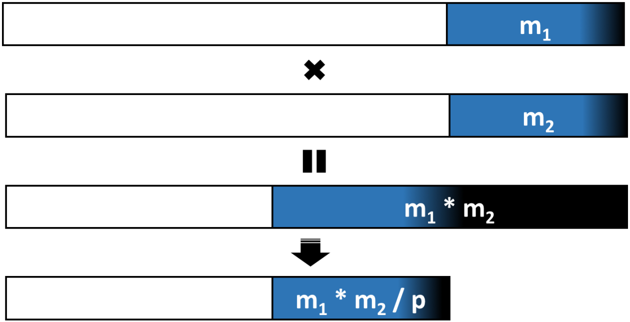


- Send a ciphertext (mod q_{large}) to a smaller modulus $q_{small} = q_{large}/p$.
- $Rescale(c) = \lfloor c/p \rceil$
- If $\langle c, sk \rangle = m + e \pmod{q_{large}}$, then we have

$$\langle Rescale(c), sk \rangle = (m/p) + e' \pmod{q_{small}}$$

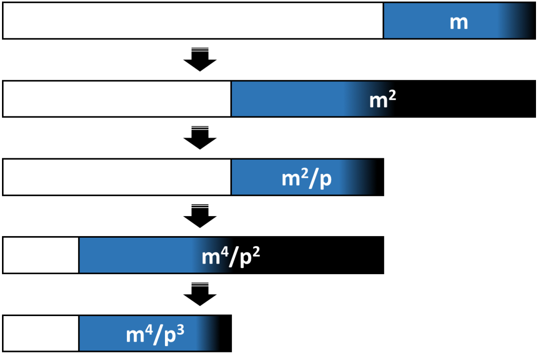
  for some $e' = (e/p) + e_{scale} \approx e/p$.
- The relative error of ciphertext is almost preserved.

Rescaling after Multiplication



- Rescaling procedure results in *rounding* of plaintext.

Leveled HE scheme



- Suppose that $m \approx p$. Given an encryption of m, we compute (m^d/p^{d-1}) in level $\log d$ within $(\log d + 1)$ bits of precision loss.
- Size of ciphertext modulus grows linearly on depth L
  - $\log q$: $\underline{O(L \cdot \eta)}$ vs $\Omega(2^L L \cdot \eta)$

Idea 3: Batching Technique

- Encrypt a message vector in a single ciphertext for SIMD operation.
- RLWE-based construction over a cyclotomic ring $\mathcal{R} = \mathbb{Z}[X]/\Phi_M(X)$.
  - Let $N = \phi(M)$.
  - Previous method: Use the factorization $\Phi_M(X) = \prod_{i=1}^{\ell} F_i(X) \pmod{p}$

$$\begin{array}{ccccc} \mathcal{R}_p & \rightarrow & \prod_{i=1}^{\ell} \mathbb{Z}_p[X]/(F_i(X)) & \rightarrow & \prod_{i=1}^{\ell} GF(p^d) \\ m(X) & \mapsto & (m(X) \pmod{F_i(X)})_{1 \le i \le \ell} & \mapsto & (m(\alpha_i))_{1 \le i \le \ell} \end{array}$$

  - Evaluation at non-conjugate roots $(\alpha_1, \ldots, \alpha_\ell)$ of $\Phi_M(X)$ over $\mathbb{Z}_p$.
  - Cannot be applied to the characteristic zero plaintext spaces.

Idea 3: Batching Technique

- Roughly, a plaintext space is the set of small polynomials in $\mathcal{R}$.
- Canonical embedding map $\sigma : \mathbb{Q}[X]/(\Phi_M(X)) \to \mathbb{C}^N$ defined by $a(X) \mapsto (a(\zeta^j))_{j\in\mathbb{Z}_M^*}$ where $\zeta = \exp(-2\pi i/M)$.
  - Cannonical embedding norm $||a||_\infty^{can} = ||\sigma(a)||_\infty$.
  - An image of σ is contained in the subring $\mathbb{H} = \{(z_j)_{j\in\mathbb{Z}_M^*} : z_{-j} = \overline{z_j}\}$.
  - Let $S \leq \mathbb{Z}_M^*$ be a subgroup such that $\mathbb{Z}_M^*/S = \{\pm 1\}$.
- Our method: Adapt the complex canonical embedding (isometric ring homomorphism) preserving the error size.

$$\begin{array}{ccccc} \mathcal{R} = \mathbb{Z}[x]/(\Phi_M(X)) & \xrightarrow{\sigma} & \mathbb{H} \leq \mathbb{C}^N & \xrightarrow{\iota} & \mathbb{C}^{N/2} \\ m(X) & \longmapsto & \sigma(m) & \longmapsto & (m(\zeta^j))_{j\in S} \end{array}$$

Encoding/Decoding and Rounding Error

$$\begin{array}{ccccc} \mathcal{R} = \mathbb{Z}[x]/(\Phi_M(X)) & \xrightarrow{\sigma} & \mathbb{H} \leq \mathbb{C}^N & \xrightarrow{\iota} & \mathbb{C}^{N/2} \\ m(X) & \longmapsto & \sigma(m) & \longmapsto & (m(\zeta^j))_{j \in S} \end{array}$$

- Encoding:

$$\begin{aligned} \vec{z} = (z_j)_{j \in S} \in \mathbb{Z}[i]^{N/2} \quad &\longmapsto \quad z(X) = \sigma^{-1} \circ \iota^{-1}(\vec{z}) \in \mathbb{R}[X]/(\Phi_M(X)) \\ &\longmapsto \quad m(X) = \lfloor \Delta \cdot z(X) \rceil \in \mathbb{Z}[X]/(\Phi_M(X)) \end{aligned}$$

  for a scaling factor Δ and rounding $\lfloor \cdot \rceil$ w.r.t. $||\cdot||_\infty^{can}$.
- Decoding:

$$\begin{aligned} m(X) \in \mathbb{Z}[X]/(\Phi_M(X)) \quad &\longmapsto \quad \vec{m} = (m(\zeta^j))_{j \in S} \in \mathbb{C}^{N/2} \\ &\longmapsto \quad \vec{z} = \lfloor \Delta^{-1} \cdot \vec{m} \rceil \in \mathbb{Z}[i]^{N/2}. \end{aligned}$$

- Encoding/Decoding preserves the size of errors.
- Rounding error is relatively small.

Example of Encoding & Encryption

Suppose that $M = 8$ ($\Phi_M(x) = x^4 + 1$) and $\Delta = 64$. Then

$$C_M = \begin{pmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & \zeta^3 & \zeta^6 & \zeta \\ 1 & \zeta^5 & \zeta^2 & \zeta^7 \\ 1 & \zeta^7 & \zeta^6 & \zeta^5 \end{pmatrix}, \quad C_M^{-1} = \frac{1}{4}\overline{C_M^T} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ \zeta^7 & \zeta^5 & \zeta^3 & \zeta \\ \zeta^6 & \zeta^2 & \zeta^6 & \zeta^2 \\ \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 \end{pmatrix}$$

where $\zeta = \exp(-2\pi i/8) = (1+i)/\sqrt{2}$.

$$\begin{aligned} \vec{z} = (3+4i, 2-i) \quad &\mapsto \quad \iota^{-1}(\vec{z}) = (3+4i, 2-i, 2+i, 3-4i) \\ &\mapsto \quad z(X) = \tfrac{1}{4}(10 + 4\sqrt{2}X + 10X^2 + 2\sqrt{2}X^3) \\ &\mapsto \quad m(X) = 160 + 91X + 160X^2 + 45X^3. \end{aligned}$$

$$m(\zeta) = 64(3.0082.. + i * 4.0026..), m(\zeta^3) = 64(1.9918.. - i * 0.9974..).$$

- $Enc(m) = (b + m, a)$ for $b = as + e_{enc}$.
- $Dec(m) = 64 \cdot z(X) + e_{enc} + e_{rd}$.
  (About $\log ||e_{enc}||_\infty^{can}$ bits of precision loss.)

Additional Operations

- Let $c = (b(X) = \hat{m}(X) + a(X) \cdot s(X), a(X))$ be a ciphertext with decryption structure $\hat{m}(X)$.
- Slot exchange
  - $c^{(i)} = (b(X^i), a(X^i))$ is an encryption of $\hat{m}(X^i)$ w.r.t. the secret $s(X^i)$.
  - Permutaion on plaintext slots: $(\hat{m}_j = \hat{m}(\zeta^j))_{j \in S} \mapsto (\hat{m}_{ij})_{j \in S}$ for $i \in S$.
- Slotwise conjugtation
  - $c^{(-1)} = (b(X^{-1}), a(X^{-1}))$ is an encryption of $\hat{m}(X^{-1})$ w.r.t. the secret $s(X^{-1})$.
  - Conjugation on plaintext slots: $(\hat{m}_j = \hat{m}(\zeta^j))_{j \in S} \mapsto (\overline{\hat{m}_j})_{j \in S}$.
- Key switching technique from $s^{(i)}(X) = s(X^i)$ to $s(X)$.

Section 3

Evaluation of Circuits & Applications

Analytic Functions

- Approximate evaluation of (complex) polynomials

Lemma (Polynomials)

FPHE scheme of depth $L = \log d$ *evaluates a polynomial of degree* d *in* $O(d)$ *multiplications and precision loss* $< (\log d + 1)$ *bits.*

- Transcendental functions
  - Exponential function: $\exp(x) \approx \sum_{j=0}^{d} \frac{1}{j!} x^j$.
  - Trigonometric functions: $\cos x, \sin x, \ldots$
  - Logistic function: $(1 + \exp(-x))^{-1}$

Lemma (Exponential Function)

FPHE scheme of depth $L = \log \eta$ *evaluates the exponential function with* $\eta = \log p$ *bits of precision input* $x = m/p \in [-1, 1]$ *in* $O(\eta)$ *multiplications and precision loss* < 1 *bit.*

Multiplicative Inverse

- Use the approximate polynomials of power-of-two degrees.
  - Let $y = 1 - x$ with $|y| \leq 1/2$.
  - $x^{-1} \approx (1+y)(1+y^2)\cdots(1+y^{2^{L-1}}) = x^{-1} \cdot (1 \pm 2^{-2^L})$.

Lemma (Multiplicative Inverse)

FPHE scheme of depth $L = \log \eta$ evaluates the exponential function with $\eta = \log p$ bits of precision input $x = m/p$ with $|1 - x| \leq 1/2$ in $O(L)$ multiplications and precision loss < 1 bit.

Ideal Applications

- FFT algorithm
  - Identifying the monomial X to the primitive M-th root of unity ζ reduces the parameter and complexity [CSV16].
  - $X \mapsto \zeta^j$ in the slot of index j, but the whole pipeline (FFT-Hadamard-iFFT) does not depend on the choice of j.
- Exact computation using approximate arithmetic
  - Multiplication of integral polynomials
- Convergence property of recursive algorithm
  - Newton's method
  - Gradient descent algorithm (machine learning)
  - Matrix factorization (PCA)
  - Control of cyber-physical system

Experimental Result

Intel Single Core i5 2.9GHz processor

Function	N	$\log q$	$\log p$	Consumed levels	Bit precision of input	Total time	Amortized time
x^{16}	2^{13}	150	30	4	15	0.43s	0.10ms
x^{1024}	2^{15}	440	40	10	22	8.53s	0.52ms
x^{-1}	2^{13}	150	25	5	9	0.69s	0.17ms
$\exp(x)$	2^{13}	175	35	5	20	0.98s	0.24ms

Function	N	$\log q$	$\log p$	Degree of polynomial	Total time	Amortized time
Logistic	2^{13}	175	35	7	0.79s	0.19ms
	2^{14}	210	35	9	2.36s	0.29ms

Experimental Result

Method	FFT Dim	N	$\log q$	Degree	Amortization amount	Total time	Amortized time
[CSV16][1]	2^4	2^{13}	150	2	-	0.46s	-
	2^{13}	2^{14}	192	2	-	17min	-
Ours[2]	2^4	2^{13}	100	2	2^{12}	0.88s	0.22ms
	2^{13}	2^{13}	100	2	2^{12}	19min	0.28s
	2^{13}	2^{14}	200	8	2^{13}	2.5h	1.10s

1. Six Intel Xeon E5 2.7GHz processors with 64 GB RAM
2. Four Intel Core i7 2.9 GHz processors with 16 GB RAM


감사합니다
Thank you~!

Reference

- Brakerski, Gentry, and Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping, 2012.
- Gentry, Halevi, and Smart. Homomorphic evaluation of the AES circuit, 2012.
- Bos et al. Improved security for a ring-based fully homomorphic encryption scheme, 2013.
- Costache, Smart, and Vivek. Faster homomorphic evaluation of discrete fourier transforms, 2016.
- Images
  - http://www.ibmsystemsmag.com/ibmi/trends/whatsnew/Biometric-Authentication-101/
  - https://www.societyofvirtualassistants.co.uk/va-products/uk-va-industry-survey-take-part/
  - https://en.wikipedia.org/wiki/Trigonometry
  - https://iq.intel.com/dr-you-handheld-medical-devices/