Real-HEAAN: Approximate Homomorphic Encryption over the Conjugate-invariant Ring

Duhyeong Kim[1] Yongsoo Song[2]
[1]Seoul National University (SNU)
[2]University of California, San Diego (UCSD)

Nov 28, 2018

Contributions of Real-HEAAN

- An approximate Homomorphic Encryption of which the plaintext space is (purely) real number field

$\Longrightarrow$ NO waste of the plaintext space for real-number arithmetic contrary to HEAAN

$\Longrightarrow$ Prevent the potential problem of HEAAN

- Real-HEAAN supports twice more parallel computations compared to HEAAN under the same security level, speed, and memory (with new NTT method)

An Approxmiate HE Scheme
HEAAN

HEAAN: an Approximate HE scheme

HEAAN: **H**omomorphic **E**ncryption for **A**rithmetic over **A**pproximate **N**umbers

- Proposed by Cheon-Kim-Kim-Song in Asiacrypt'17
- Natural fit in real-world applications which require approximate computations of real numbers
- Abandoning exact computations, it gains a lot of advantages in efficiency:

  Ctxt/Ptxt expansion ratio, # Ptxt slots, rounding operation (for free)

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$
- Public Key: pk = $(a, b = a \cdot s + e) \in R_q^2$

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$
- Public Key: pk = $(a, b = \ a \cdot s + e) \in R_q^2$
- Ciphertext of $m \in R := Z[X]/(X^n + 1)$: ct = $(r \cdot a + e_1, r \cdot b + e_2 + m) \in R_q^2$

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$
- Public Key: pk = $(a, b = a \cdot s + e) \in R_q^2$
- Ciphertext of $m \in R := Z[X]/(X^n + 1)$: ct = $(r \cdot a + e_1, r \cdot b + e_2 + m) \in R_q^2$

$$\langle \text{ct}, \text{sk} \rangle = m + e'(\approx m)$$

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$
- Public Key: pk = $(a, b = \ a \cdot s + e) \in R_q^2$
- Ciphertext of $m \in R := Z[X]/(X^n + 1)$: ct = $(r \cdot a + e_1, r \cdot b + e_2 + m) \in R_q^2$

$$\boxed{\langle \mathrm{ct}, \mathrm{sk} \rangle} = m + e'(\approx m)$$

The Decryption Circuit!
(No Additional Modulo Operation)

HEAAN: an Approximate HE scheme

- Secret Key: sk = $(-s, 1) \in R_q^2$ where $R_q = Z_q[X]/(X^n + 1)$
- Public Key: pk = $(a, b = a \cdot s + e) \in R_q^2$
- Ciphertext of $m \in R := Z[X]/(X^n + 1)$: ct = $(r \cdot a + e_1, r \cdot b + e_2 + m) \in R_q^2$

$$\langle \text{ct}, \text{sk} \rangle = m + \boxed{e'} (\approx m)$$

Evaluation error + Decryption error

Encoding/Decoding of HEAAN

Then how are the complex numbers packed into an element of $R = Z[X]/(X^n + 1)$?

Encoding/Decoding of HEAAN

Then how are the complex numbers packed into an element of $\boldsymbol{R = Z[X]/(X^n + 1)}$?

- Let ϕ be an isomorphism (induced by canonical embedding) from $\mathrm{C}^{\frac{n}{2}}$ to $\mathrm{R}[X]/(X^n + 1)$

  (C and R denote complex/real number fields resp.)

Encoding/Decoding of HEAAN

Then how are the complex numbers packed into an element of $\boldsymbol{R = Z[X]/(X^n + 1)}$?

- Let ϕ be an isomorphism (induced by canonical embedding) from $\mathrm{C}^{\frac{n}{2}}$ to $\mathrm{R}[X]/(X^n + 1)$

  (C and R denote complex/real number fields resp.)

- Given $\frac{n}{2}$ complex numbers $z_1, z_2, \dots, z_{\frac{n}{2}}$ and a scaling factor $\Delta > 0$,

$$\mathbf{Ecd}\left(\boldsymbol{z_1, \dots, z_{n/2}; \Delta}\right) = \left\lfloor \boldsymbol{\Delta \cdot \phi\left(z_1, \dots, z_{n/2}\right)} \right\rceil := m$$

- The decoding process is very simple, just evaluating a half of m-th primitive roots of unities

$$\mathbf{Dcd(m; \Delta)} = \left(\frac{\mathbf{1}}{\boldsymbol{\Delta}} \cdot \boldsymbol{m(\zeta_{4i+1})}\right)_{\boldsymbol{0 \le i < n/2}}$$

- The scaling factor controls the Encoding/Decoding error

Impact of HEAAN to real-world

iDASH Privacy & Security Workshop

- A Privacy & Security workshop holding competitions on secure genome analysis
- One of 3 tasks: secure genome analysis based on HE (e.g., Logistic Regression, GWAS,…)

Impact of HEAAN to real-world

iDASH Privacy & Security Workshop

- A Privacy & Security workshop holding competitions on secure genome analysis
- One of 3 tasks: secure genome analysis based on HE (e.g., Logistic Regression, GWAS,…)
- HEAAN-based solutions won the 1st place both on 2017 and 2018
- All the submitted solutions of HE-based secure GWAS computation used HEAAN!

Some Limitations of HEAAN

Limitations of HEAAN

1. The Waste of the Plaintext Space

- The Plaintext space of HEAAN is

$$\mathrm{R}[X]/(X^n + 1) \simeq \mathrm{C}^{\frac{n}{2}}$$

where R and C denote the real / complex number field respectively.

Limitations of HEAAN

1. The Waste of the Plaintext Space

- The Plaintext space of HEAAN is

$$\mathrm{R}[X]/(X^n + 1) \simeq \mathrm{C}^{\frac{n}{2}} \supset \mathrm{R}^{\frac{n}{2}}$$

where R and C denote the real / complex number field respectively.

- In real-number applications, we only use the subring $\mathrm{R}^{\frac{n}{2}}$ of the plaintext space $\mathrm{C}^{\frac{n}{2}}$!

Limitations of HEAAN

2. The Complex Explosion Problem

- In real-number applications, we only care about the real part of a plaintext.
- However, the complex part of a plaintext is "internally growing up" in every operation!

Limitations of HEAAN

2. The Complex Explosion Problem

- In real-number applications, we only care about the real part of a plaintext.
- However, the complex part of a plaintext is "internally growing up" in every operation!

$$(a+bi)(c+di) = ac - bd + \boxed{(ad+bc)i}$$

The new cplx part after a multiplication

Limitations of HEAAN

2. The Complex Explosion Problem

- In real-number applications, we only care about the real part of a plaintext.
- However, the complex part of a plaintext is "internally growing up" in every operation!

$$(a+bi)(c+di) = ac - bd + \boxed{(ad+bc)i}$$

Let $a, c \approx 2^p$ and $b, d \approx 2^r$ for $r \ll p$.

$$\Longrightarrow \frac{b}{a}, \frac{d}{c} \approx 2^{r-p} \;\&\; \frac{ad+bc}{ac-bd} \approx 2^{r-p+1}$$

The new cplx part after a multiplication

Limitations of HEAAN

2. The Complex Explosion Problem

- In real-number applications, we only care about the real part of a plaintext.
- However, the complex part of a plaintext is "internally growing up" in every operation!

$$(a+bi)(c+di) = ac - bd + \boxed{(ad+bc)i}$$

Let $a, c \approx 2^p$ and $b, d \approx 2^r$ for $r \ll p$.

$$\Longrightarrow \frac{b}{a}, \frac{d}{c} \approx 2^{r-p} \ \& \ \frac{ad+bc}{ac-bd} \approx 2^{r-p+1}$$

The new cplx part after a multiplication

- The complex part essentially explodes in large-depth circuit evaluations

Real-HEAAN

The core idea of Real-HEAAN

Use the subring of the cyclotomic ring!

- The plaintext space of original HEAAN

$$\mathbb{R}[X]/(X^n + 1) \simeq \mathbb{C}^{\frac{n}{2}}$$

The core idea of Real-HEAAN

Use the subring of the cyclotomic ring!

- The plaintext space of original HEAAN

$$\mathbb{R}[X]/(X^n + 1) \simeq \mathbb{C}^{\frac{n}{2}}$$

- The NEW plaintext space

$$\cup$$

$$\mathbb{R}^{\frac{n}{2}}$$

The core idea of Real-HEAAN

Use the subring of the cyclotomic ring!

- The plaintext space of original HEAAN

$$\mathbb{R}[X]/(X^n+1) \simeq \mathbb{C}^{\frac{n}{2}}$$

- The NEW plaintext space

$$\cup \qquad\qquad \cup$$

$$\mathbb{R}[X+X^{-1}]/(X^n+1) \simeq \mathbb{R}^{\frac{n}{2}}$$

Here $X^{-1} := -X^{n-1}$ denotes the inverse of X modulo X^n+1

The core idea of Real-HEAAN

- Let $R' \coloneqq Z[X + X^{-1}]/(X^n + 1)$

The core idea of Real-HEAAN

- Let $R' := Z[X + X^{-1}]/(X^n + 1)$
- Every element of Real-HEAAN is built over R' instead of $R = \mathrm{Z}[X]/(X^n + 1)$
  - Secret Key: sk = $(-s, 1) \in R_q'^2$ where $R_q' = Z_q[X + X^{-1}]/(X^n + 1)$
  - Public Key: pk = $(a, b = a \cdot s + e) \in R_q'^2$
  - Ciphertext of $m \in R'$: ct = $(r \cdot a + e_1, r \cdot b + e_2 + m) \in R_q'^2$

Encoding/Decoding of Real-HEAAN

Then how are the real numbers packed into an element of $R' = Z[X + X^{-1}]/(X^n + 1)$?

Encoding/Decoding of Real-HEAAN

Then how are the real numbers packed into an element of $R' = \mathbb{Z}[X + X^{-1}]/(X^n + 1)$?

- Let τ be an isomorphism (induced by canonical embedding) from $\mathbb{R}^{\frac{n}{2}}$ to $\mathbb{R}[X + X^{-1}]/(X^n + 1)$

  (Note that τ is just a simple domain-restriction of $\phi \Longrightarrow \tau = \phi|_{\mathbb{R}^{n/2}}$)

Encoding/Decoding of Real-HEAAN

Then how are the real numbers packed into an element of $\boldsymbol{R' = Z[X + X^{-1}]/(X^n + 1)}$?

- Let τ be an isomorphism (induced by canonical embedding) from $\mathrm{R}^{\frac{n}{2}}$ to $\mathrm{R}[X + X^{-1}]/(X^n + 1)$

  (Note that τ is just a simple domain-restriction of $\phi \Longrightarrow \tau = \phi|_{\mathrm{R}^{n/2}}$)

- Given $\frac{n}{2}$ real numbers $x_1, x_2, \dots, x_{\frac{n}{2}}$ and a scaling factor $\Delta > 0$,

$$\mathbf{Ecd}\left(\boldsymbol{x_1, \dots, x_{n/2}; \Delta}\right) = \left\lfloor \boldsymbol{\Delta \cdot \tau\left(x_1, \dots, x_{n/2}\right)} \right\rceil \coloneqq m$$

- The decoding process is exactly same with HEAAN:

$$\mathbf{Dcd(m; \Delta)} = \left(\boldsymbol{\frac{1}{\Delta} \cdot m(\zeta_{4i+1})}\right)_{\boldsymbol{0 \le i < n/2}}$$

Real-HEAAN vs HEAAN

Real-HEAAN vs HEAAN

Our Claim

Real-HEAAN over $Z[X+X^{-1}]/(X^{2n}+1) \approx$ HEAAN over $Z[X]/(X^{n}+1)$

w.r.t. Security, Ring operation speed, and memory

#Ptxt Slots: n vs $n/2 \Longrightarrow$ twice more Parallel Computations!

Security of Real-HEAAN

[Security Reduction] Real-HEAAN is IND-CPA secure under the hardness assumption of RLWE over the number field $K := \mathrm{Q}[X + X^{-1}]/(X^{2n} + 1)$ (of which the extension degree $[K: Q] = n$)

[Cryptanalysis] RLWE over the number field K resists all known algebraic attacks on RLWE so that the best known attack is essentially the general attacks on LWE of dimension n

Efficiency of Real-HEAAN

1. Memory

- Every element of $R_q{}' = Z_q[X + X^{-1}]/(X^{2n} + 1)$ is express as $a(X) = a_0 + \sum_{i=1}^{n-1} a_i\,(X^i - X^{2n-i})$ for $a_i \in Z_q$

  $\Longrightarrow$ $n \cdot \log q$ bits are required to store each element

2. Speed

- Number Theoretical Transform (NTT): mapping between $Z_q[X]/(X^m - 1) \simeq Z_q^m$ with $O(m \log m)$ complexity
- Current best NTT method for $R_q = Z_q[X]/(X^n + 1)$ asymptotically requires $O(n \log n)$ complexity
- Our new NTT method for $R_q{}' = Z_q[X + X^{-1}]/(X^{2n} + 1)$ also requires $O(n \log n)$ complexity!

NTT method for R_q'

- Assume q is a prime

Trivial Approach:

$$
\begin{tikzcd}
R_q' = Z_q[X + X^{-1}]/(X^{2n}+1) \arrow[r, "\text{embedding}"] & Z_q[X]/(X^{4n}-1) \arrow[d, "\textbf{NTT of dim } 4n"] \\
\text{(Computations over } Z_q^{4n}\text{)} & Z_q^{4n} \arrow[d, "\textbf{Inverse NTT of dim } 4n"] \\
R_q' = Z_q[X + X^{-1}]/(X^{2n}+1) & Z_q[X]/(X^{4n}-1) \arrow[l, "\text{Mod } X^{2n}+1"']
\end{tikzcd}
$$

NTT method for R'_q

- Assume q is a prime

Trivial Approach:

$$\begin{tikzcd}
R'_q = Z_q[X+X^{-1}]/(X^{2n}+1) \arrow[r, "\text{embedding}"] & Z_q[X]/(X^{4n}-1) \arrow[d, "\textbf{NTT of dim } 4n"] \\
\text{(Computations over } Z_q^{4n}\text{)} & Z_q^{4n} \arrow[d, "\textbf{Inverse NTT of dim } 4n"] \\
R'_q = Z_q[X+X^{-1}]/(X^{2n}+1) & Z_q[X]/(X^{4n}-1) \arrow[l, "\text{Mod } X^{2n}+1"']
\end{tikzcd}$$

Requires
NTT of dimension $4n$!

NTT method for R'_q

Our New Approach:

- Find a "simply computable" invertible linear transformation from R'_q to $Z_q[X]/(X^n - 1)$

$$R'_q \xrightarrow[]{\text{Simply Computable Linear map}} Z_q[X]/(X^n - 1)$$

$$a(X) = a_0 + \sum_{i=1}^{n-1} a_i\,(X^i - X^{2n-i}) \longrightarrow \tilde{a}(X) = \sum_{i=0}^{n-1} \tilde{a}_i X^i$$

where $\widetilde{a_0} = a_0$ and $\tilde{a}_i = a_i \cdot w^i + a_{n-i} \cdot w^{i-n}$ for $1 \le i \le n-1$ (w: $4n$-th prim. root of unity mod q)

- The inverse mapping is also simply computable with $O(n)$ complexity

NTT method for R'_q

Our New Approach:

$$\begin{tikzcd}
R'_q = Z_q[X + X^{-1}]/(X^{2n}+1) \arrow[r, "\text{Simply Computable Linear map}"] & Z_q[X]/(X^n - 1) \arrow[d, "\textbf{NTT of dim } \boldsymbol{n}"] \\
\text{(Computations over } Z_q^n\text{)} & Z_q^n \arrow[d, "\textbf{Inverse NTT of dim } \boldsymbol{4n}"] \\
R'_q = Z_q[X + X^{-1}]/(X^{2n}+1) & Z_q[X]/(X^{4n} - 1) \arrow[l, "\mathrm{Mod}\ X^{2n}+1"']
\end{tikzcd}$$

NTT method for R'_q

Our New Approach:

$$\begin{tikzcd}
R'_q = Z_q[X+X^{-1}]/(X^{2n}+1) \arrow[r, "\text{Simply Computable Linear map}"] & Z_q[X]/(X^n-1) \arrow[d, "\textbf{NTT of dim } \boldsymbol{n}"] \\
\text{(Computations over } Z_q^n\text{)} & Z_q^n \arrow[d, "\textbf{Inverse NTT of dim } \boldsymbol{4n}"] \\
R'_q = Z_q[X+X^{-1}]/(X^{2n}+1) & Z_q[X]/(X^{4n}-1) \arrow[l, "\text{Mod } X^{2n}+1"']
\end{tikzcd}$$

Requires
NTT of dimension n!

Conclusion

- Real-HEAAN provides twice more parallel computations compared to the original HEAAN while preserving the same level of security, ring operation speed, and memory.
- In other words, with the same number of parallel computations, Real-HEAAN is asymptotically twice faster than the original HEAAN.
- Moreover, Real-HEAAN prevents the complex explosion problem of HEAAN.
- The generalization of our new NTT method would be very interesting open topic!

Table 1. Comparison of our scheme and HEAAN

Approximate HE	$\texttt{OurScheme}(2n, q)$	$\mathrm{HEAAN}(n, q)$
Number of plaintext slots	n	$n/2$
NTT dimension	n	n
Bit size of ciphertexts	$2n \log q$	$2n \log q$

thank you!

Homomorphic Encryption

Homomorphic Encryption

Homomorphic Encryption (HE) :

An Encryption scheme which allows computations on encrypted data

$$
\begin{tikzcd}
\mathrm{enc}(m) \arrow[r, "\mathrm{eval}"] & \mathrm{enc}(f(m)) \\
m \arrow[u, "\mathrm{enc}"] \arrow[r, "f"] & f(m) \arrow[u, "\mathrm{enc}"']
\end{tikzcd}
$$

Homomorphic Encryption

Homomorphic Encryption (HE) :

An arbitrary circuit over encrypted data can be evaluated w/o decryption!

Selected as 10 Emerging Technologies (MIT Technical Review 2011)

Ciphering: Gentry's system allows encrypted data to be analyzed in the cloud. In this example, we wish to add 1 and 2. The data is encrypted so that 1 becomes 33 and 2 becomes 54. The encrypted data is sent to the cloud and processed: the result (87) can be downloaded from the cloud and decrypted to provide the final answer (3). Credit: Steve Moors

Pros / Cons of HE

- **Pros**

- HE allows us to evaluate an arbitrary circuit (w/ bootstrapping)
- Data Leakage Prevention against hackers (w/o decryption key)
- Various Real-World Applications: Statistical Analysis, Searching, Machine Learning (over encrypted data)

- **Cons**

- Large Ciphertext/Plaintext Expansion ratio (40 ~ 1000 for FHE)
- Evaluation Speed: more than hundreds of times slower than one on unencrypted state

$\Longrightarrow$ **Individualized Optimization** is going on for each operation!

Various Lattice-based HE schemes

Scheme	Plaintext	Good	Bad	Library
Wordwise Encryption - Brakerski-Gentry-Vaikuntanathan'12 - Gentry-Halevi-Smart'12a,b,c - Brakerski'12, Fan-Vercauteren'12 - Halevi-Shoup'13,14,15	$GF(p^d)$ (Z_p)	Polylog overhead (Amortized time & Expansion rate)	Bootstrapping	HElib SEAL …
Linear Error growth & Quad. Ctxt size - Gentry-Sahai-Waters'13	Z, Z[X] ({0,1})	Toolkit for FHEW	Inefficient	-
Bitwise Encryption - Ducas-Micciancio'15 - Chillotti-Gama-Georgieva-Izabachene'16,17	{0,1}, $(\{0,1\}^*)$	Evaluation with Bootstrapping Latency	Amortized time & Expansion rate	FHEW TFHE

Application Researches on HE (2017 ~ Mar. 2018)

"Homomorphic Encryption" in ePrint and IEEE Xplore

Machine Learning:	11	(2018/233,202,139,074, 2017/979,715. SSCI, IEEE Access, IEEE Journal, ICCV, SMARTCOMP)
Neural Network:	2	(2018/073, 2017/1114)
Genomic Data:	7	(2017/955,770,294,228. EUSIPCO, SMARTCOMP, IEEE Journal)
Health Data:	2	(IBM Journal, IEEE Journal)
Biometric Data:	2	(IEEE Access, IEEE Conference)
Energy Management:	3	(2017/1212. IEEE Big Data, IET Journal)
Big Data:	1	(ICBDA)
Advertising:	1	(WIFS)
Internet of Things:	1	(IWCMC)
Election:	1	(2017/166)

The Construction of HEAAN

Idea 1: Every number contains an Approximation Error (from the unknown true value).

$\Longrightarrow$ Consider the error e of a ciphertext c as a part of the approximation error

$$c = \mathrm{Enc}(m) \quad \text{if} \quad \langle c, \mathrm{sk} \rangle \pmod{q} = m + e \approx m$$
$$(= m^*)$$

Simple Example:

$1.234 \Rightarrow$ (scale-up by $p = 10^4$) $\Rightarrow$ $12{,}340.$

$\Rightarrow$ (Encrypt) $\Rightarrow$ $[\langle c, \mathrm{sk} \rangle]_q$ = $12{,}344$ $\approx 1.234 \times 10^4$ $\Rightarrow$ (scale-down by p) $\Rightarrow$ 1.234

The Construction of HEAAN

The Construction of HEAAN

Idea 1: Every number contains an Approximation Error (from the unknown true value).

$\Longrightarrow$ Consider the error e of a ciphertext c as a part of the approximation error

$$c = \mathrm{Enc}(m) \quad \text{if} \quad \boxed{\langle c, \mathrm{sk}\rangle \pmod q} = m + e \approx m$$

$$(= m^*)$$

The Decryption Circuit!
(No Additional Modulo Operation)

Simple Example:

$1.234 \Rightarrow$ (scale-up by $p = 10^4$) $\Rightarrow$ $12{,}340.$

$\Rightarrow$ (Encrypt) $\Rightarrow [\langle c, \mathrm{sk}\rangle]_q$ = $12{,}344 \approx 1.234 \times 10^4 \Rightarrow$ (scale-down by p) $\Rightarrow 1.234$

The Construction of HEAAN

Idea 2: Approximate **Rounding** (ReScaling; RS) for (almost) Free!

- Assume that the secret key sk has sufficiently small coefficients.
- For a ciphertext c of the message m, define $c' = \lfloor p^{-1} \cdot c \rceil$.
- Then, it holds that

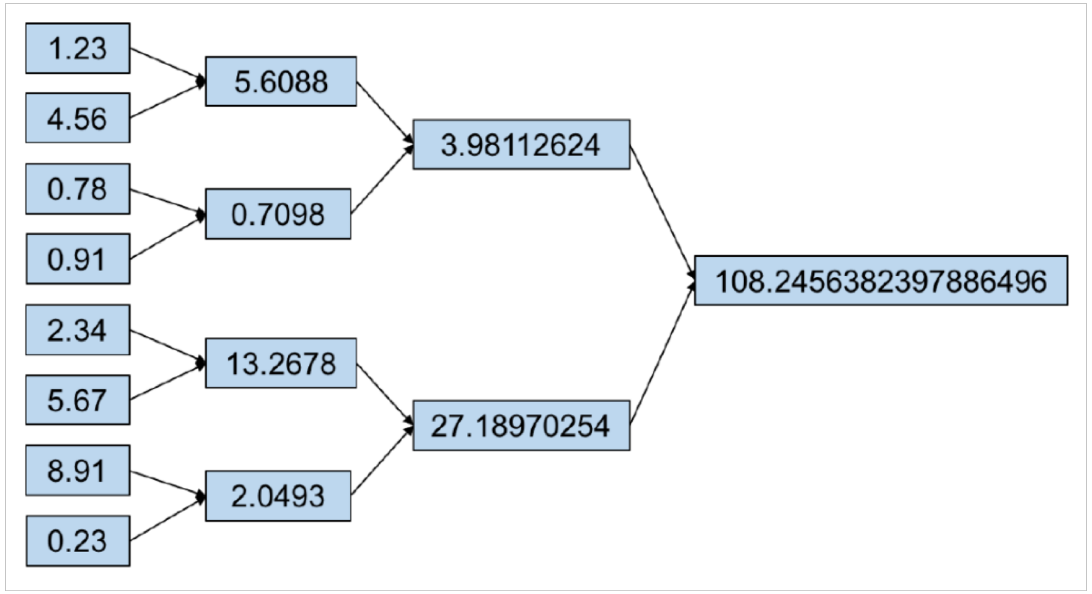
$$\langle c, \mathrm{sk} \rangle \pmod q = m^*$$

$$\Longrightarrow \langle c', \mathrm{sk} \rangle \pmod{\mathrm{p}^{-1} q} \approx p^{-1} m^* \text{ (an approximate rounding of } m^*\text{)}$$

- Rounding of a ciphertext directly derives an approximate rounding of the message!

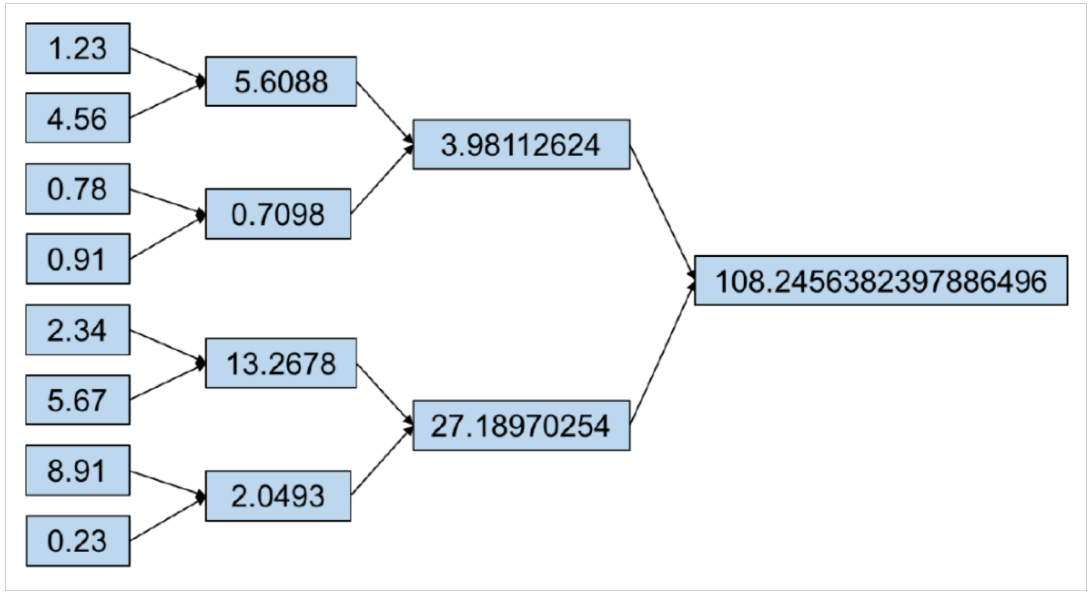
Real Number Computations in HEs

Q1) What is the main problem of previous wordwise HEs in computation of real numbers?



Real Number Computations in HEs

Q1) What is the main problem of previous wordwise HEs in computation of real numbers?

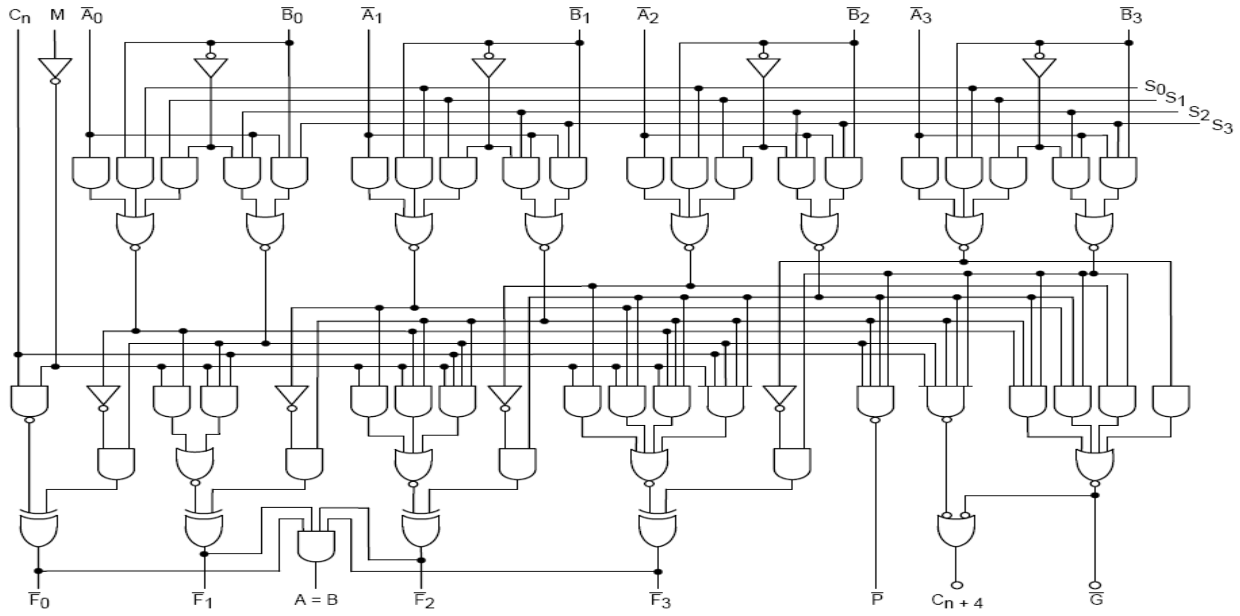


Ans) The exponential growth of the plaintext size (millions of bits after 20-depth multiplications)

- Ctxt size $\approx O(2^L)$, or other new techniques are required (L : level parameter)
- One solution is to extract MSBs and store them, but very expensive!

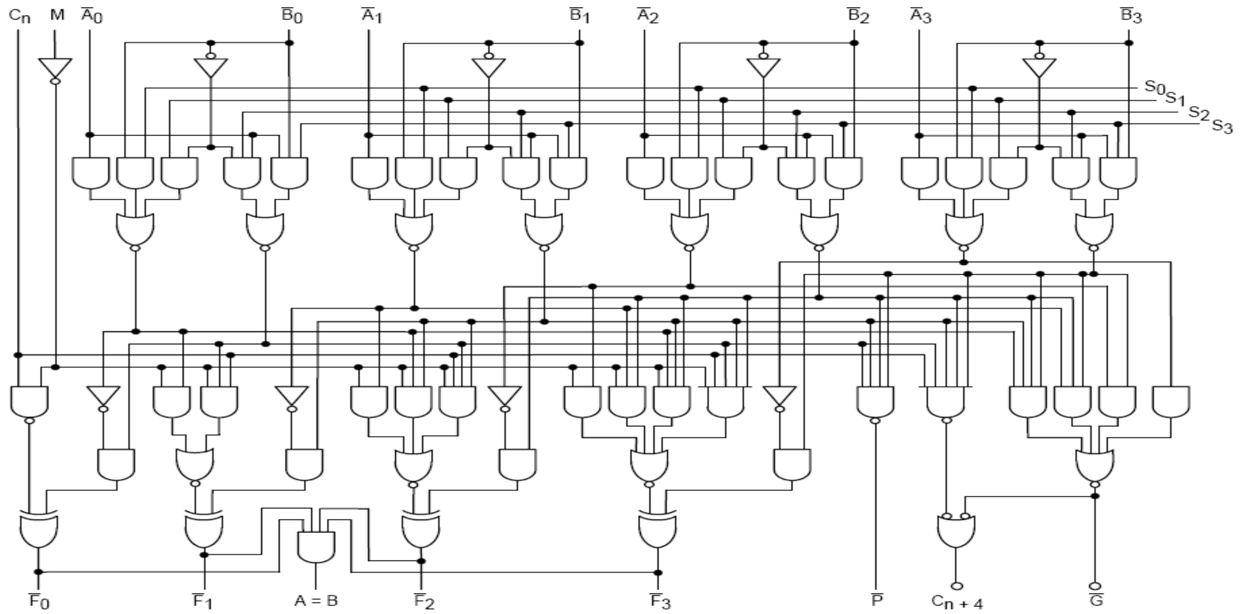
Real Number Computations in HEs

Q2) How about bitwise HE schemes?



Real Number Computations in HEs

Q2) How about bitwise HE schemes?

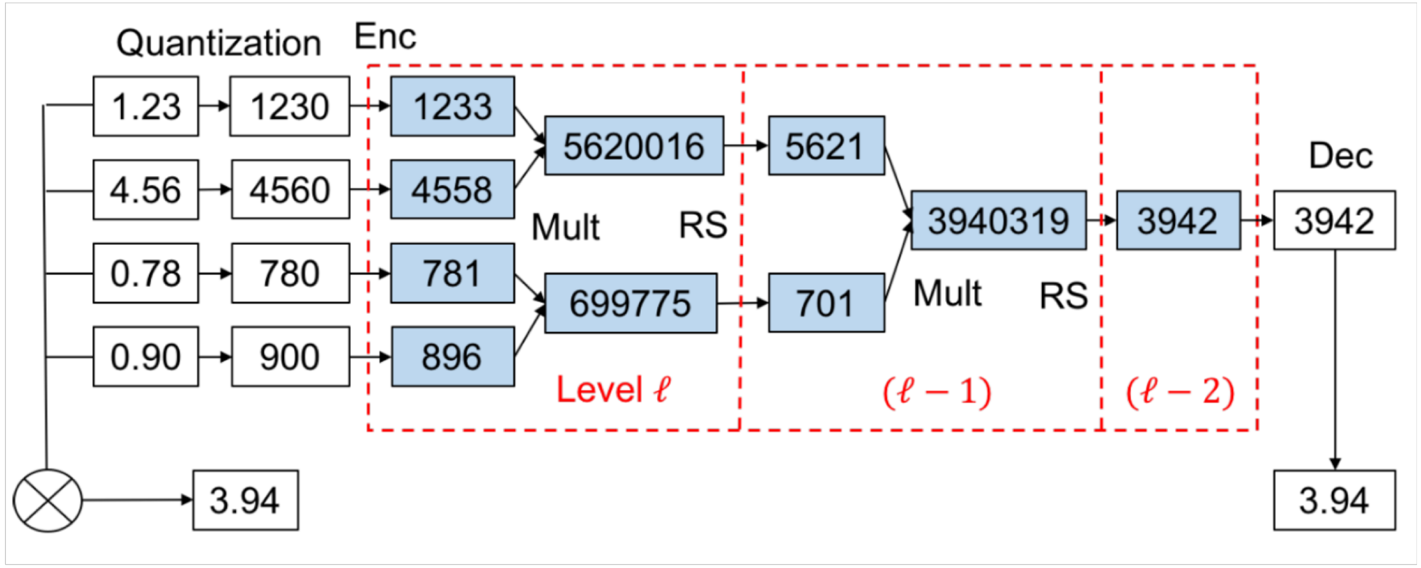


Ans) Too many gates required to represent an operation between large-precision numbers!

- 0.06 sec for (2-to-1) gate, 10 sec for (6-to-6) circuit.
- 75 gates for an operation between 4-bit strings.
- Then, how many gates for 16-bit / 32-bit precision multiplication?

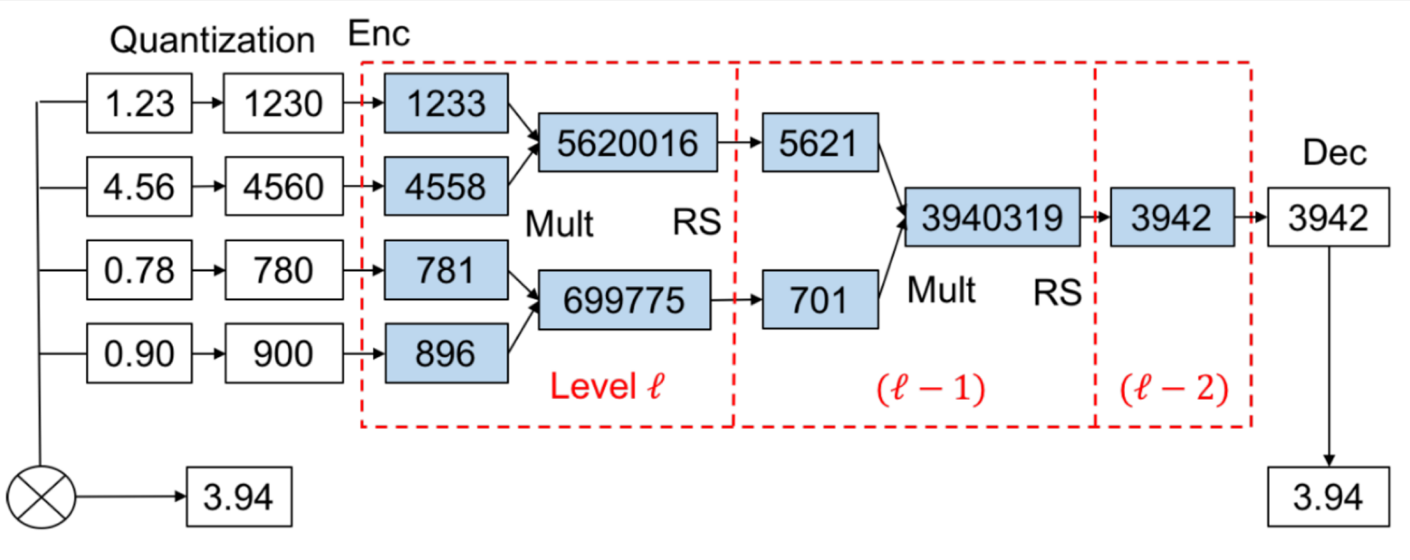
Real Number Computations in HEAAN

Q3) Then, how does it work in HEAAN?



Real Number Computations in HEAAN

Q3) Then, how does it work in HEAAN?



- Imitating the procedure of approximate arithmetic on computer system
- No additional cost for the "rounding"(RS) process!
- Ctxt size $\approx O(L)$ (L : level parameter), since HEAAN only stores most significant bits