Bootstrapping for Approximate Homomorphic Encryption

Jung Hee Cheon, Kyoohyung Han, Andrey Kim (Seoul National University)

Miran Kim, Yongsoo Song (University of California, San Diego)

Landscape of Homomorphic Encryption

Landscape of Homomorphic Encryption

“Word Encryption”
(BGV12, Bra12, FV12)

Packing & SIMD operations on $GF(p^d)$
between RLWE ciphertexts

Long latency (Bootstrapping)

Landscape of Homomorphic Encryption

“Word Encryption”
(BGV12, Bra12, FV12)

Packing & SIMD operations on GF(p^d)
between RLWE ciphertexts

Long latency (Bootstrapping)

“Bitwise Encryption”
(DM15, CGGI16)

Eval. of LUTs on {0,1}* with bootstrapping
on LWE ciphertext (<-> RLWE <- RGSW)

Large expansion rate (storage, cost)

Landscape of Homomorphic Encryption

"Word Encryption"
(BGV12, Bra12, FV12)

Packing & SIMD operations on GF(p^d)
between RLWE ciphertexts

Long latency (Bootstrapping)

"Bitwise Encryption"
(DM15, CGGI16)

Eval. of LUTs on {0,1}* with bootstrapping
on LWE ciphertext (<-> RLWE <- RGSW)

Large expansion rate (storage, cost)

"Approximate Encryption"
(CKKS17)

Approximate HE

- Every approximate number contains an Error (from its unknown true value).

  Consider an RLWE error as part of it.

Approximate HE

- Every approximate number contains an Error (from its unknown true value).

  Consider an RLWE error as part of it.

  $ct = Enc(M)$ if $[\langle ct, sk \rangle]_q = M + e \approx M$.

Approximate HE

- Every approximate number contains an Error (from its unknown true value).

  Consider an RLWE error as part of it.

  ct = Enc (M) if $[\langle ct,sk \rangle]_q = M+e \approx M$.

- Approximate Rounding is easy!

Approximate HE

- Every approximate number contains an Error (from its unknown true value).

  Consider an RLWE error as part of it.

  ct = Enc (M) if $[\langle ct,sk\rangle]_q = M+e \approx M$.

- Approximate Rounding is easy!

  $[\langle ct, sk\rangle]_q = M$

  HomRnd : $ct \mapsto ct' = \lceil p^{-1} \cdot ct \rfloor$

  $\Rightarrow [\langle ct', sk\rangle]_{q/p} \approx M/p$

$(1.234) \times (5.678) = (1{,}234 \times 5{,}678) \times 10^{-6} = (7{,}006{,}652) \times 10^{-6} \approx (7{,}007) \times 10^{-3}$.

Functionality of Approximate HE

Packing Technique

- $K = Q[x]/(\Phi_m(x))$, $R = Z[x]/(\Phi_m(x))$.
- $\Phi_m(X) = \prod_i(x - \zeta_i)$ for the primitive m-th roots of unity ζ_i.
- Encoding map: $(M_i)_i \mapsto M(X)$ such that $M(\zeta_i) = M_i$

Approximate addition, multiplication, and rounding

- Every homomorphic operation includes a small noise

Evaluation of Analytic Functions

- exp (z),
- z^{-1}

Landscape of Homomorphic Encryption

"Word Encryption"
(BGV12, Bra12, FV12)

Packing & SIMD operations on GF(p^d)
between RLWE ciphertexts

Long latency (Bootstrapping)

"Bitwise Encryption"
(DM15, CGGI16)

Eval. of LUTs on {0,1}* with bootstrapping
on LWE ciphertext (<-> RLWE <- RGSW)

Large expansion rate (storage, cost)

"Approximate Encryption"
(CKKS17)

Landscape of Homomorphic Encryption

"Word Encryption"
(BGV12, Bra12, FV12)

Packing & SIMD operations on $GF(p^d)$ between RLWE ciphertexts

Long latency (Bootstrapping)

"Bitwise Encryption"
(DM15, CGGI16)

Eval. of LUTs on {0,1}* with bootstrapping on LWE ciphertext (<-> RLWE <- RGSW)

Large expansion rate (storage, cost)

"Approximate Encryption"
(CKKS17)

Packing & SIMD operation over the real/complex numbers (add, mult + rounding) between RLWE ciphertexts

Application Researches of HE (2017~)

- Machine Learning & Neural Networks: 7
- Biomedical & Health data analysis: 3
- Bioinformatics: 3
- Genomic data analysis: 3
- Cyber Physical System & Internet of Things: 4
- Smart Grid: 3
- Image processing: 3
- Voting: 2
- Advertising: 2

> 80 %

[Kim-Song-Kim-Lee-Cheon'18] iDASH Privacy & Security Competition 2017

Six minutes to train a logistic regression model from encrypted dataset of size 1579 * (18+1).

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

- Homomorphic operation of approximate HE induces a small "noise":

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

- Homomorphic operation of approximate HE induces a small "noise":

  Dec (ct) = M => HomEval (Dec (ct)) = Enc (M + e)

  Refreshed ciphertext encrypts an approximate value.

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

- Homomorphic operation of approximate HE induces a small "noise":

  Dec (ct) = M => HomEval (Dec (ct)) = Enc (M + e)

  Refreshed ciphertext encrypts an approximate value.

- Dec (ct, sk) = <ct, sk> (mod q).

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

- Homomorphic operation of approximate HE induces a small "noise":

  Dec (ct) = M => HomEval (Dec (ct)) = Enc (M + e)

  Refreshed ciphertext encrypts an approximate value.

- Dec (ct, sk) = $\langle ct, sk \rangle$ (mod q).

  Idea 1: $\langle ct, sk \rangle = q \cdot t + M$ for some small $|t| < K = |sk|_1$.

  ct = Enc $(q \cdot t + M)$ with a ciphertext modulus $q' \gg q$.

Bootstrapping of Approximate HE

Bootstrapping = Evaluation of Decryption circuit ?

- Homomorphic operation of approximate HE induces a small "noise":

  Dec (ct) = M   =>   HomEval (Dec (ct)) = Enc (M + e)

  Refreshed ciphertext encrypts an approximate value.

- Dec (ct, sk) = $\langle ct, sk \rangle \pmod q$.

  Idea 1: $\langle ct, sk \rangle = q \cdot t + M$ for some small $|t| < K = |sk|_1$.

  ct = Enc $(q \cdot t + M)$ with a ciphertext modulus $q' \gg q$.

  How to (efficiently) evaluate the modular reduction $(q \cdot t + M) \mapsto M$?

Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

- Naive solution: Lagrange interpolation on the domain $(-Kq, Kq)$

Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

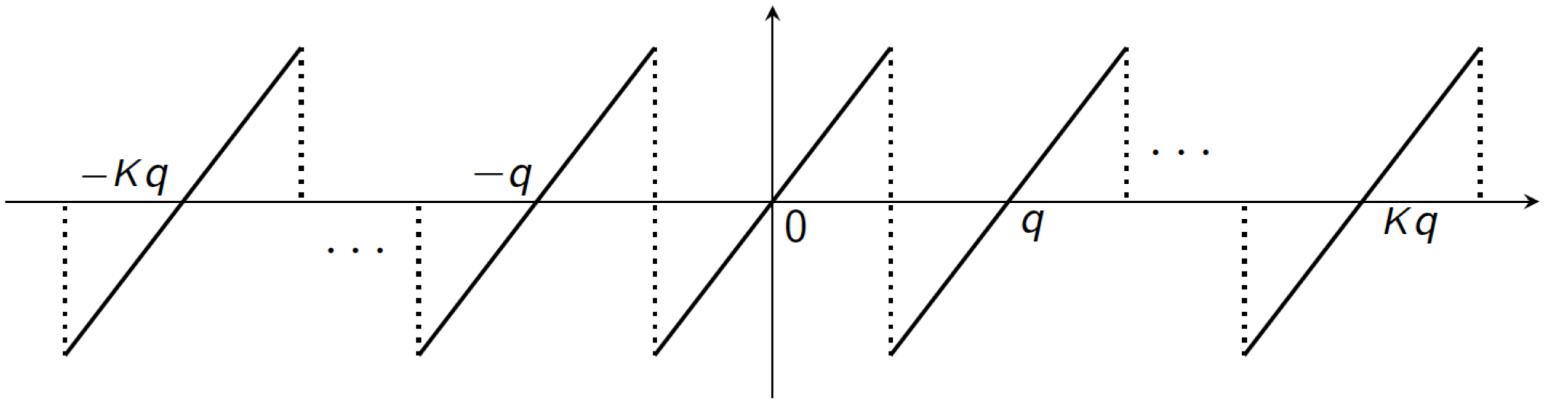
- Naive solution: Lagrange interpolation on the domain $(-Kq, Kq)$

Efficiency Degree $d = O(Kq)$, Complexity $O(d)$ operations - exp. on the depth!

Evaluation of Modular Reduction

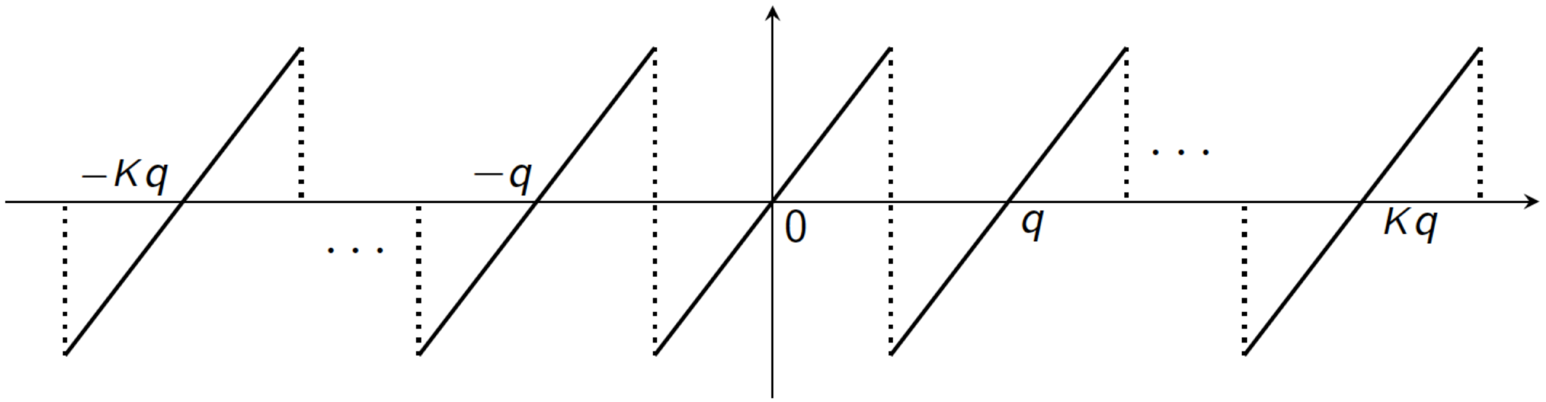
- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.
- Naive solution: Lagrange interpolation on the domain $(-Kq, Kq)$

Efficiency	Degree $d = O(Kq)$, Complexity $O(d)$ operations - exp. on the depth!
Correctness	Large error on the boundary



Evaluation of Modular Reduction

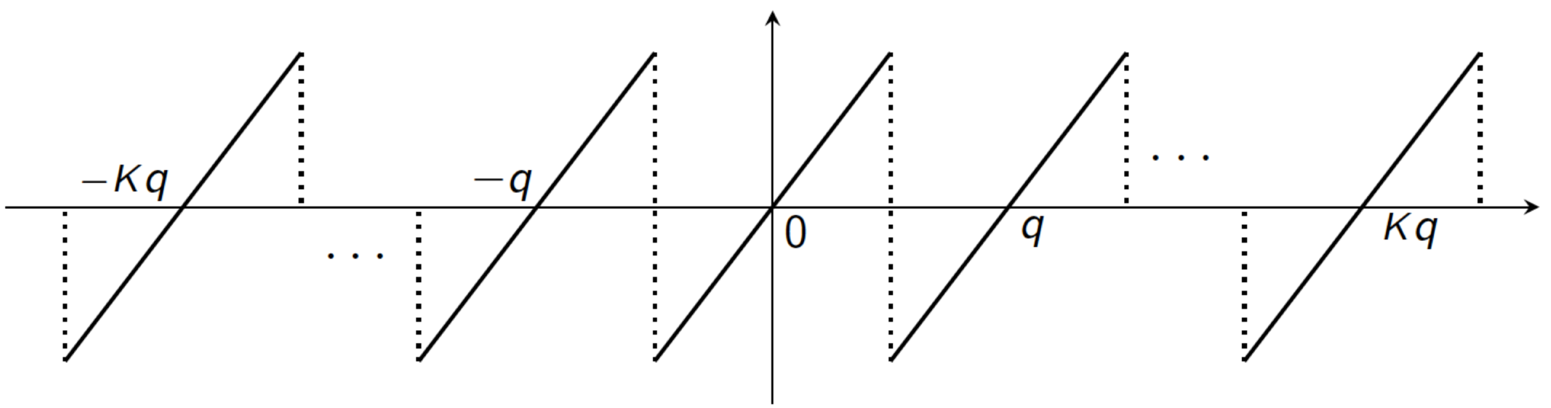
- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.



Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

- Modular Reduction is discontinuous when $|M| = q/2$.

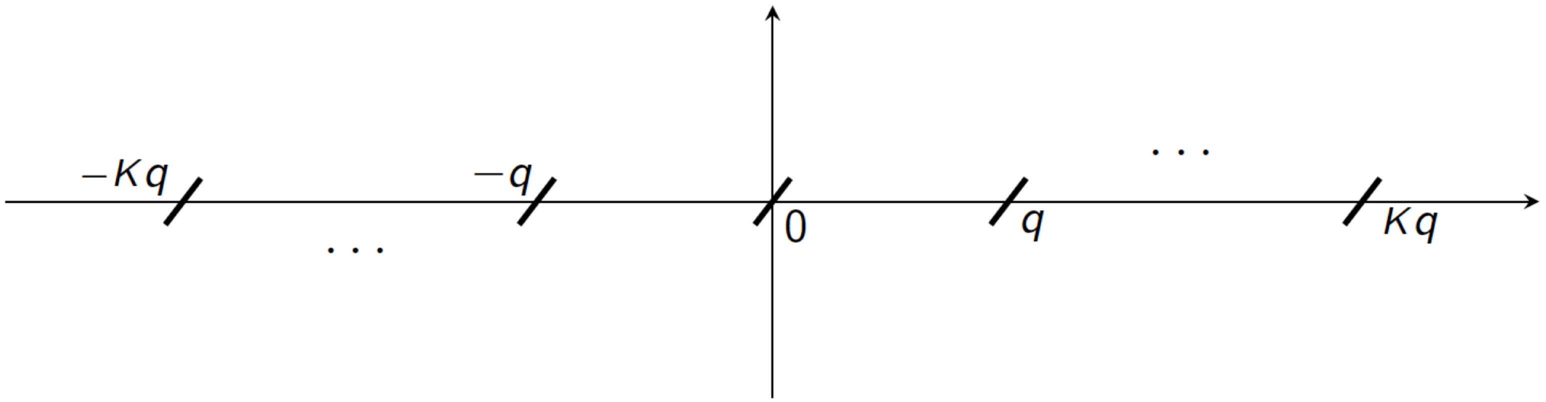


Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

- Modular Reduction is discontinuous when $|M| = q/2$.

  Idea 2: Start bootstrapping when $|M| << q$.



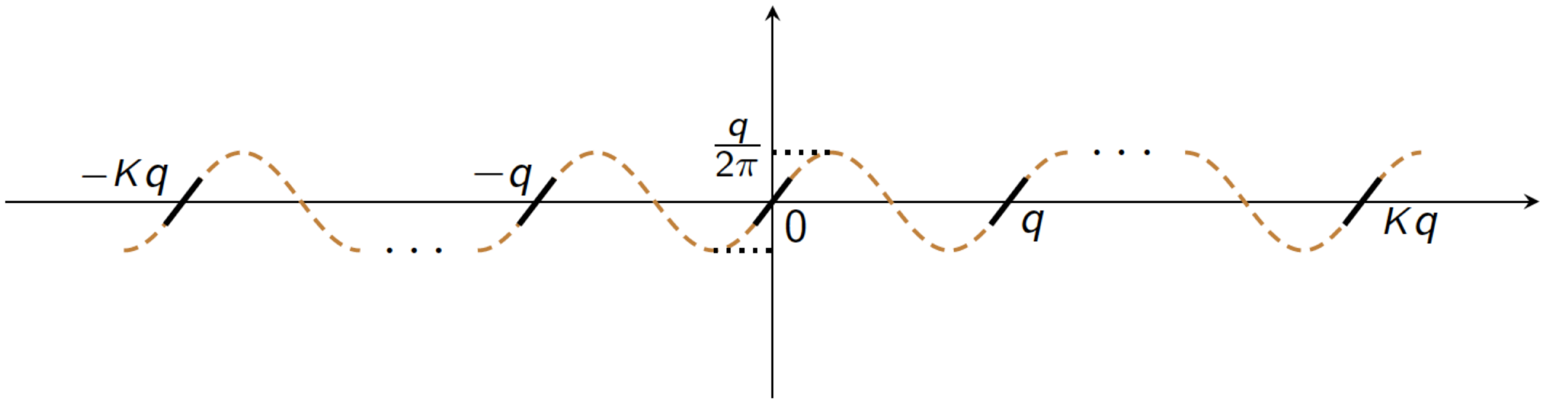
Evaluation of Modular Reduction

- Goal: Represent modular reduction $(q \cdot t + M) \mapsto M$ as a circuit over the complex numbers.

- Modular Reduction is discontinuous when $|M| = q/2$.

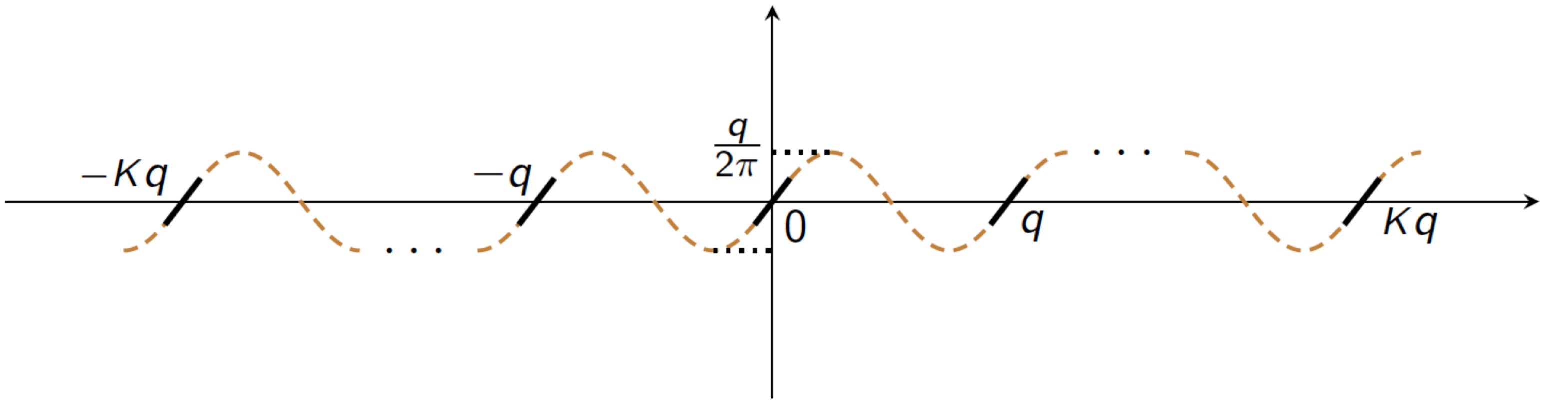
Idea 2: Start bootstrapping when $|M| << q$.

Use the formula $M \approx (q/2\pi) \cdot \sin\left[(2\pi/q)\,(q \cdot t + M)\right]$.



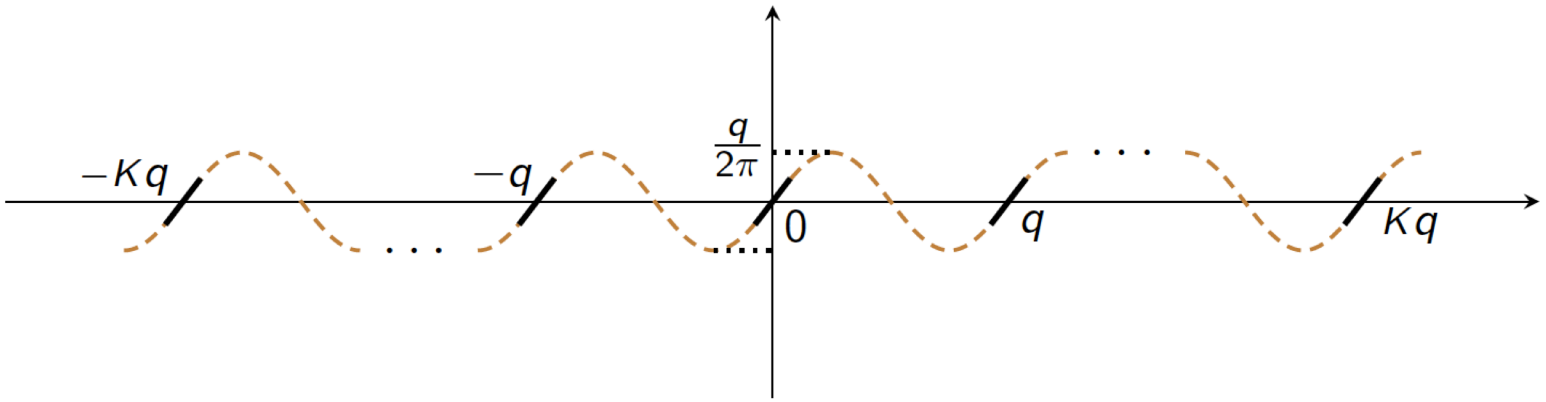
Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$



Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$
- Naive solution: Taylor series approximation $\sin\theta = \theta - (\theta^3/6) + (\theta^5/120) - \ldots$

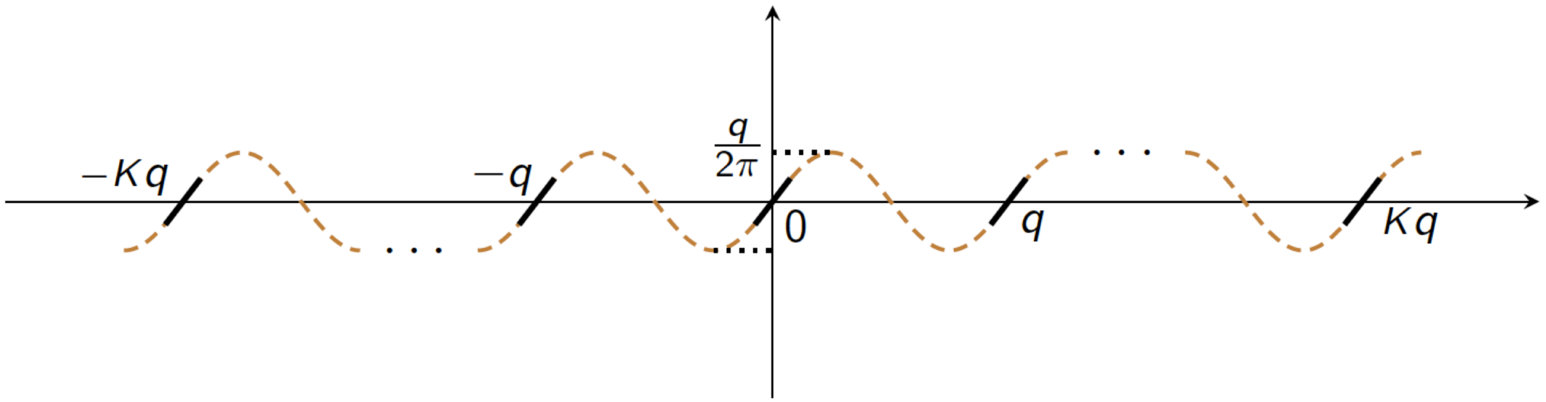


Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$

- Naive solution: Taylor series approximation $\sin\theta = \theta - (\theta^3/6) + (\theta^5/120) - \dots$

Degree	$d = O(Kq)$ to achieve $R_d = O(1)$.
Complexity	$O(Kq)$ operations.



Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$
- How to reduce the complexity?

Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$

- How to reduce the complexity?

  Idea 3: Double-angle formula

  $\cos\theta = \cos^2(\theta/2) - \sin^2(\theta/2)$, $\sin\theta = 2\cos(\theta/2) \cdot \sin(\theta/2)$.

Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$

- How to reduce the complexity?

  Idea 3: Double-angle formula

  $\cos\theta = \cos^2(\theta/2) - \sin^2(\theta/2)$, $\sin\theta = 2\cos(\theta/2) \cdot \sin(\theta/2)$.

  Low-degree Taylor series of $\cos(\theta/2^r)$, $\sin(\theta/2^r)$ for some $r = O(\log(Kq))$

  & Recursive evaluation (r iterations) to get an approximate value of $(\sin\theta)$.

Evaluation of Sine

- Goal: Evaluate $M \approx (q/2\pi) \cdot \sin\theta$ for $\theta = (2\pi/q)\,(q \cdot t + M)$ such that $|\theta| < 2\pi K$

- How to reduce the complexity?

  Idea 3: Double-angle formula

  $\cos\theta = \cos^2(\theta/2) - \sin^2(\theta/2)$, $\sin\theta = 2\cos(\theta/2) \cdot \sin(\theta/2)$.

  Low-degree Taylor series of $\cos(\theta/2^r)$, $\sin(\theta/2^r)$ for some $r = O(\log(Kq))$

  & Recursive evaluation (r iterations) to get an approximate value of ($\sin\theta$).

- Efficiency

  Depth: $L = r + O(1) = O(\log(Kq))$.

  Complexity: $O(L)$ operations. Linear on the depth!

Summary

- $ct = Enc(M) \pmod q$ is an encryption of $(q \cdot t + M)$ in a large modulus.
- Approximation of Modular reduction $(q \cdot t + M)_q = M$ using a trigonometric function.
- Recursive evaluation strategy to reduce the computational costs.

Summary

- $ct = Enc(M) \pmod q$ is an encryption of $(q \cdot t + M)$ in a large modulus.
- Approximation of Modular reduction $(q \cdot t + M)_q = M$ using a trigonometric function.
- Recursive evaluation strategy to reduce the computational costs.

  ✓ No Bootstrapping Key.

  ✓ Linear Complexity on the depth $L = O(\log(|sk|_1 \cdot q))$ of decryption circuit.

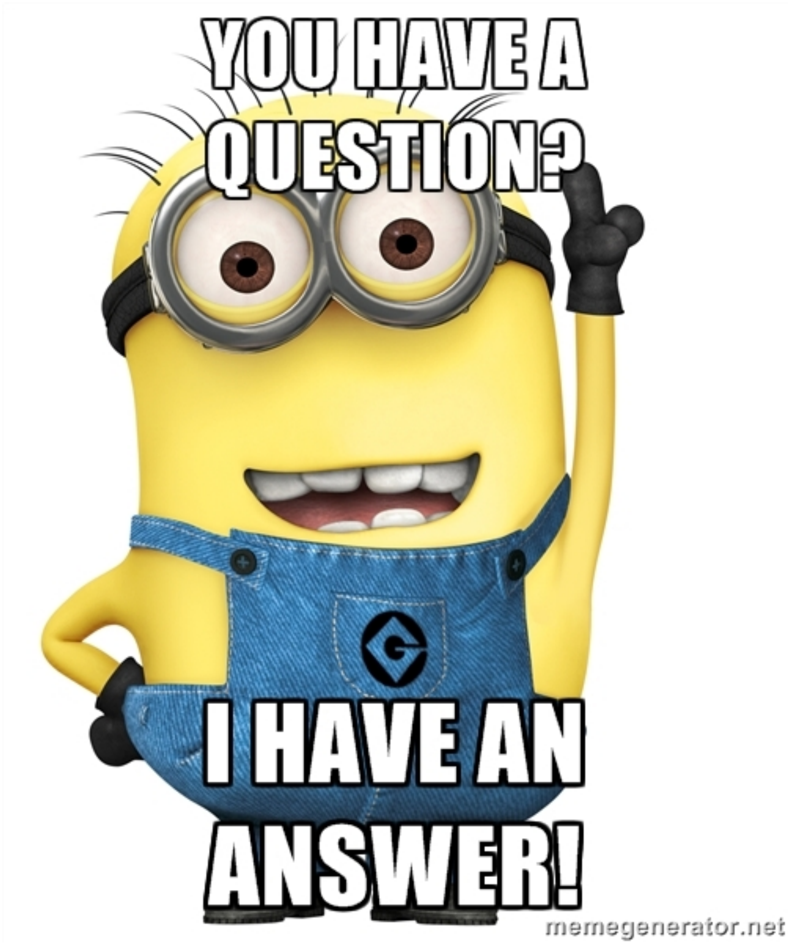
  ✓ Small Memory : 1 ciphertext encrypting $\exp(i \cdot \theta) = \cos\theta + i \sin\theta$.

  ✓ Implication : Machine Learning, Cyber-Physical System

Comparison & Experimental Results

HS15, CH18	Coeff To Slots $\tilde{O}(1)$ per slot	Bit/Digit Extraction	Slots To Coeff $\tilde{O}(1)$ per slot
Ours		**Sine Evaluation**	
DM15,CGGI16	Accumulator: O(n) operation / 1 slot		

- Digit Extraction: 6s (Z_{127}). 30s (Z_{127^2}). 15s (Z_{2^6}). 239s (Z_{2^8}).
- **Sine Evaluation**: 12.5s (12-bit precision). 68s (24-bit precision).
  [Song-Han-Kim-Kim-Cheon 18] Full Residue Number System: 8x ~ 12x speedup
- Accumulator: 0.06s (1 bit). 10s (6 bits)


YOU HAVE A QUESTION?
I HAVE AN ANSWER!
memegenerator.net