Fully Homomorphic Encryption

Roman Walch

Graz, October 31, 2019

Homomorphic Encryption

- Homomorphic to operation $\oplus$

$$E(m_1) \otimes E(m_2) = E(m_1 \oplus m_2), \;\; \forall m_1, m_2 \in M$$

Note

$\otimes$ and $\oplus$ can be the same, but don't have to be!

Partial Homomorphic Encryption - RSA

- Encryption:

$$E(m) = m^e \bmod N$$

- Homomorphic to multiplication:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (m_1^e \bmod N) \cdot (m_2^e \bmod N) \\ &= (m_1 \cdot m_2)^e \bmod N \\ &= E(m_1 \cdot m_2) \end{aligned}$$

Partial Homomorphic Encryption - Paillier

- Encryption:

$$E(m) = g^m \cdot r^n \bmod n^2$$

... with random r

- Homomorphic to addition:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (g^{m_1} \cdot r_1^n \bmod n^2) \cdot (g^{m_2} \cdot r_2^n \bmod n^2) \\ &= g^{m_1+m_2} \cdot (r_1 \cdot r_2)^n \bmod n^2 \\ &= E(m_1 + m_2) \end{aligned}$$

Fully Homomorphic Encryption (FHE)

- Evaluate every circuit homomorphically
- Homomorphic
  - To addition and multiplication
  - Arbitrary times
- Nowadays: Somewhat HE or Levelled HE
  - Homomorphic to addition and multiplication
  - Limited number of times
  - Become FHE with bootstrapping

Learning With Errors

Learning With Errors (LWE)

- Search: Find secret $\boldsymbol{s} \in \mathbb{Z}_q^n$ given many noisy inner products
  - $\boldsymbol{a_i} \leftarrow \mathbb{Z}_q^n : b_i = \langle \boldsymbol{a_i}, \boldsymbol{s} \rangle + e_i \in \mathbb{Z}_q$

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{a_1} \leftarrow \mathbb{Z}_q^n \\ \boldsymbol{a_2} \leftarrow \mathbb{Z}_q^n \\ \cdots \\ \boldsymbol{a_k} \leftarrow \mathbb{Z}_q^n \end{pmatrix} : \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \in \mathbb{Z}_q^k$$

- Decision: Distinguish $(\boldsymbol{A}, \boldsymbol{b})$ from uniform $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{k \times n} \times \mathbb{Z}_q^k$

Ring Learning With Errors (R-LWE)

- Let $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^N$, and $R_q = R/qR$
  - Polynomials of deg $< n$ and coefficients mod q
- Search: Find secret ring element $s(X) \in R_q$ given:

$$
\begin{aligned}
a_1 \leftarrow R_q &: b_1 = a_1 \cdot s + e_1 \in R_q \\
a_2 \leftarrow R_q &: b_2 = a_2 \cdot s + e_2 \in R_q \\
&\cdots \\
a_k \leftarrow R_q &: b_k = a_k \cdot s + e_k \in R_q
\end{aligned}
$$

- Decision: Distinguish (a_i, b_i) from uniform $(a_i, b) \in R_q \times R_q$

(Ring -) Learning With Errors

- Lattice-based cryptography
- Applications:
  - FHE
  - (PQ) public key encryption
  - Key exchange protocols
- Encryption introduces noise
- Ring-LWE:
  - Smaller public keys ($\boldsymbol{A} \in \mathbb{Z}_q^{k \times n}$ vs. $a \in R_q$)
  - Efficient multiplication with NTT ($\mathcal{O}(n \log n)$)

FHE In Practice

FHE Schemes

- First FHE scheme by Gentry in 2009 [Gen09]
- Today's schemes:
  - BGV [BGV12]
  - BFV [Bra12; FV12]
  - CKKS (HEAAN) [Che+17]
- Based on R-LWE
- Different noise placement/handling

Noise Propagation

- Encryption introduces noise
- Homomorphic operations:
  - Addition: negligible noise growth
  - Multiplication: significant noise growth

  $\Rightarrow$ Limited amount of multiplications! (Leveled HE, Somewhat HE)
- Bootstrapping [Gen09]
  - Costly homomorphic decryption to reset noise
  - LHE, SWHE $\rightarrow$ FHE

BGV - FHE over Integers

BGV - FHE over Integers

- Gen: $s \leftarrow R_q, a \leftarrow R_q, b = a \cdot s + t \cdot e$, with $m \in R_t$
  - Keys: $pk = (b, a), sk = s$
- Encrypt: $c = Enc(m) = (c_0, c_1) = v \cdot pk + (m + t \cdot e_0, t \cdot e_1)$
- Decrypt: $m = Dec(c) = (c_0 - sk \cdot c_1 \bmod q) \bmod t$
  - Error if $\|c_0 - sk \cdot c_1\|_\infty >= q$ (wraparound)

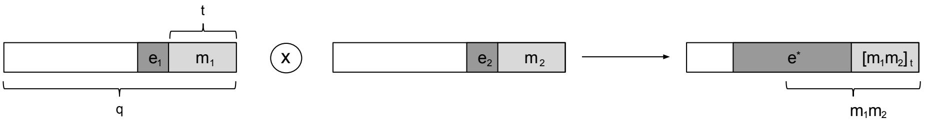

Fig.: Homomorphic multiplication of BGV [Che+17].

BGV - Multiplication

- Multiplication
  - $\text{Mult}(c, c') = (c_0 \cdot c'_0, c_0 \cdot c'_1 + c_1 \cdot c'_0, c_1 \cdot c'_1) = (\tilde{c}_0, \tilde{c}_1, \tilde{c}_2)$
  - triple decryptable by $s \otimes s$
    $\Rightarrow$ Key Switching (Relinearization) required
  - Quadratic noise growth
- Modulus Switching after multiplication
  - $c' = (p/q) \cdot c$
  - $m = (c_0 - sk \cdot c_1 \bmod q) = (c'_0 - sk \cdot c'_1 \bmod p) \bmod t$
  - Result: noise growth reduced to linear
  - But: different (smaller) modulus each level

CKKS - Approximate FHE

CKKS - Approximate FHE

- FHE problem: No floats
  $\Rightarrow$ Fixed-point arithmetic: 3.1415 $\rightarrow$ 314 at scale 100
- Multiplication:
  - Scale grows
  - Noise grows (R-LWE)
  - Big plaintext parts reserved for insignificant LSBs
- Idea:
  - Encode noise in LSBs
  - Rounding operation after multiplication

CKKS - Rescale

- Rescale operation:
  - Division by a base: $ct \to ct' = ct/p$ (scaling)
  - Consumes modulus: $q_\ell \to q_{\ell'} = q_\ell/p$
- Rescale achieves rounding
  - Discard insignificant LSBs
  - Discard noise
  - Similar to plain floating-point computation

CKKS Multiplication & Rescale

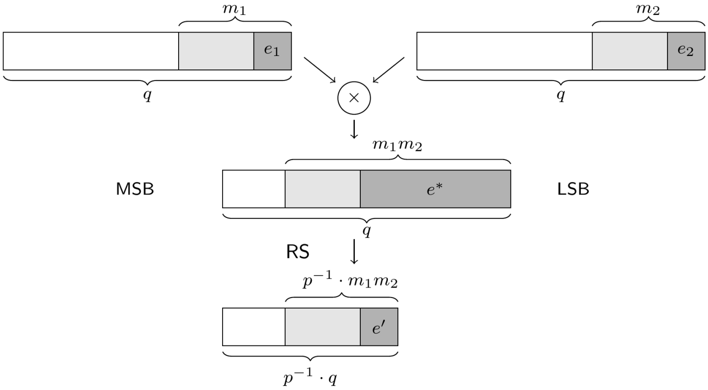

Fig.: Homomorphic multiplication and rescaling for approximate arithmetic [Che+17].

Outlook

- FHE problems:
  - Parameter tuning (maximize performance)
  - No branching
- Optimizations:
  - RNS variants using Chinese Reminder Theorem (CRT)
  - Natural SIMD encoding (packing multiple Ciphertext)
- BFV (FHE over integers):
  - Different noise encoding
  - Noise budget instead of modulus switching

Conclusion

- FHE is powerful, but
  - …difficult to use
  - …still slow
- Problem: managing LWE noise
- Different schemes with different noise management
  - BGV and BFV over integers
  - CKKS for approximate numbers

Fully Homomorphic Encryption

Questions?

Bibliography I

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. **(Leveled) fully homomorphic encryption without bootstrapping.** ITCS. ACM, 2012, pp. 309–325 (cit. on p. 11).

[Bra12] Zvika Brakerski. **Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP**. CRYPTO. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 868–886 (cit. on p. 11).

[Che+17] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. **Homomorphic Encryption for Arithmetic of Approximate Numbers.** ASIACRYPT (1). Vol. 10624. Lecture Notes in Computer Science. Springer, 2017, pp. 409–437 (cit. on pp. 11, 14, 19).

[FV12] Junfeng Fan and Frederik Vercauteren. **Somewhat Practical Fully Homomorphic Encryption.** IACR Cryptology ePrint Archive 2012 (2012), p. 144 (cit. on p. 11).

Bibliography II

[Gen09] Craig Gentry. **Fully homomorphic encryption using ideal lattices.** STOC. ACM, 2009, pp. 169–178 (cit. on pp. 11, 12).