Fully Homomorphic Encryption over the Integers Revisited

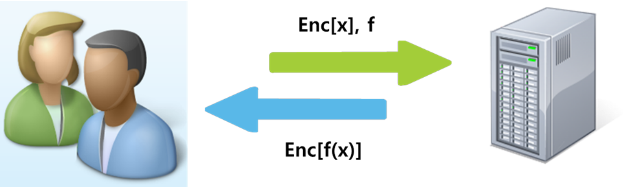
Jung Hee Cheon[1] and Damien Stehlé[2]

[1] SNU, Republic of Korea, [2] ENS de Lyon, France.

April 29, 2015

Privacy Homomorphism

- "Encryption functions which permit encrypted data to be operated on without preliminary decryption of the operands, for many sets of interesting operations" [RAD78]
- In 2009, Gentry proposed the first construction based on *ideal lattices*, which supports both of addition and multiplication.
    - Any circuit can be evaluated over encrypted data.
    - Keyword search, Statistical computations, Secure cloud computing



[RAD78] Rivest, Adleman, and Dertouzos, On data banks and privacy homomorphism," FOSC'78

Fully Homomorphic Encryption

- Over the Integers. AGCD-based:
  - [DGHV10] van Dijk, Gentry, Halevi, Vaikuntanathan: Fully Homomorphic Encryption over the Integers. Eurocrypt 2010.
  - CMNT11, CNT12, CCKLLTY13, CLT14, etc.
- Over $\mathbb{Z}_q$-modules. LWE-based:
  - [BV11a] Brakerski, Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011.
  - Bra12, BGV12, GSW13
- Over Polynomials over $\mathbb{Z}_q$.
  - Ideal lattice: SV10
  - Ring-LWE: BV11b, GHS13, BLLN13, etc.
  - NTRU: LTV12

Two Issues of AGCD-based FHE schemes

Issue 1: Hardness assumptions

- (Decisional) Approximate GCD problem (AGCD)
  - Parameters: γ, η and ρ
  - Secret: random η-bit integer p
  - Goal: distinguish between the distributions $U(\mathbb{Z} \cap [0, 2^\gamma))$ and

$$A_{\gamma,\phi}^{AGCD}(p) = \{pq + r : q \leftarrow \mathbb{Z} \cap [0, 2^\gamma/p), r \leftarrow U(\mathbb{Z} \cap (-2^\rho, 2^\rho))\}$$

- **No known reduction from classical lattice problems to AGCD.**

- An additional hardness assumption is required for bootstrapping.
  - The Sparse Subset Sum Problem is hard.

Issue 2: Ciphertext size (and Performance)

- Known Attacks (λ: security parameter)
  - Brute force attack: $\rho = \Omega(\lambda)$ and $\eta = \Omega(\lambda)$
  - Orthogonal lattice attack: $\gamma = \Omega\left(\frac{\lambda}{\log \lambda}\eta^2\right)$
  - Integer Factorization: $\eta = \log p = \Omega(\lambda^2)$ if a multiple of p is given.
- To resist the attacks, the ciphertext size is set to be
  - $\Theta(\lambda^5)$ for Partial AGCD [CMNT11,CNT12,CCKLLTY13]
  - $\Theta(\lambda^3)$ for General AGCD [DGHV10,CLT14]

Our contributions

1. LWE can be reduced to (general) AGCD.
   - AGCD is no easier than standard worst-case lattice problems.
2. The cost estimate of the orthogonal lattice attack is over-pessimistic:
   - $\gamma = \Omega\left(\frac{\lambda}{\log \lambda}(\eta - \rho)^2\right)$ suffices.
   - $\eta = \rho + L \log \lambda$, $\gamma = \Theta(L^2 \lambda \log \lambda)$ for multiplicative depth L.
3. We present a scale-invariant FHE based on the integers which:
   - is as secure as LWE,
   - has ciphertexts of bit-size $\widetilde{O}(\lambda)$, and
   - is bootstrappable without SSSP assumption.

Hardness of the AGCD problem

Learning with Errors

- (Decisional) Learning with Errors problem
  - Secret vector $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\alpha q} \subset \mathbb{Z}_q^n$ [ACPS09] (e.g. $n \approx \lambda$)
  - $\mathbb{T} = \mathbb{R}/\mathbb{Z} = [0,1)$, $\mathbb{T}_q = \dfrac{1}{q}\mathbb{Z}_q = \{0, \frac{1}{q}, \cdots, \frac{q-1}{q}\} \subseteq \mathbb{T}$
  - Distinguish between the distributions $U(\mathbb{T}_q^n \times \mathbb{T}_q)$ and

$$A_{q,\phi}^{\mathrm{LWE}}(\mathbf{s}) = \{(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) : \mathbf{a} \leftarrow \mathbb{T}_q^n, e \leftarrow \phi\}$$

  - There are reductions from *worst-case* SIVP_γ and GapSVP_γ to n-dim LWE [Reg05, Pei09, BLPRS13]

- Is 1-dimensional LWE insecure?
  - No, but the modulus q' should be exponentially large ($q' \approx q^n$).
  - There is a reduction from n-LWE to 1-LWE [BLPRS13].

Reduction to AGCD, in several steps

- 1-dim LWE problem: $1\text{-LWE}_{q,\phi}(\mathcal{D})$

$$\{(a, [as + e]_1) : a \leftarrow \mathbb{T}_q, e \leftarrow \phi\} \quad \text{versus} \quad U(\mathbb{T}_q \times \mathbb{T})$$

- 1-dim Scale-Invariant LWE: $\text{SILWE}_\phi(\mathcal{D})$

$$\{(a, [as + e]_1) : a \leftarrow \mathbb{T}, e \leftarrow \phi\} \quad \text{versus} \quad U(\mathbb{T} \times \mathbb{T})$$

- 0-dim LWE: $\text{ZDLWE}_\phi(\mathcal{D})$ Studied in [Regev03]

$$A_\phi^{\text{ZDLWE}}(s) = \{(k + e)/s : k \leftarrow \mathbb{Z} \cap [0, s), e \leftarrow \phi\} \quad \text{versus} \quad U(\mathbb{T})$$

- Approximate GCD: $\text{AGCD}_{\text{K},\phi}(\mathcal{D})$

$$\{qp + r : q \leftarrow \mathbb{Z} \cap [0, K/p), r \leftarrow \phi\} \quad \text{versus} \quad U(\mathbb{Z} \cap [0, K))$$

1-LWE to SILWE

- D_α is the Gaussian Distribution of param α. An element from D_α is in $[-\alpha, \alpha]$ with good prob. (e.g. $\alpha = 1/poly(n)$ or $2^{O(-\log^2 n)}$)
- Consider two distributions:

$$A^{\text{1-LWE}}_{q,D_\alpha}(s) = \{(a, [as+e]_1) : a \leftarrow \mathbb{T}_q, e \leftarrow D_\alpha\}$$

$$A^{\text{SILWE}}_{D'_\alpha}(s) = \{(a, [as+e]_1) : a \leftarrow \mathbb{T}, e \leftarrow D_{\alpha'}\}$$

- Idea: Add a noise to *a* and make it uniform over $\mathbb{T}$
  - Given a 1-LWE sample (a, b), output $(a+f, b)$ by sampling $f \leftarrow D_{\lesssim 1/q}$ since $|(as+e)-(a+f)s| \leq |e| + |fs|$ is small as s is small.
- Similar to Modulus Switching technique used in LWE-based FHE.

SILWE to ZDLWE

$$A_\phi^{\mathrm{SILWE}}(s) = \{(a, [as+e]_1) : a \leftarrow \mathbb{T}, e \leftarrow D_\alpha\}$$

$$A_\phi^{\mathrm{ZDLWE}}(s) = \{(k+e)/s : k \leftarrow \mathbb{Z} \cap [0, s), e \leftarrow D_{\alpha'}\}$$

- Given SILWE (a, b) with $b = as + e - k$ for $k \in \mathbb{Z}$, output

$$\left(a - \frac{b}{s}\right) = a - \frac{as+e-k}{s} = \frac{k-e}{s}.$$

- Idea: Guess $\log(1/\alpha) \approx \log n$ bits of s: $s' = s + \delta$ (see [Regev10]).

$$\left|\frac{b}{s} - \frac{b}{s'}\right| = \frac{b|\delta|}{ss'} \lesssim \frac{|\delta|}{s^2} \leq \frac{\alpha}{s}.$$

This discrepancy is swallowed up in e/s.

ZDLWE to AGCD

$$A_{\phi}^{\mathrm{ZDLWE}}(s) = \{(k+e)/s : k \leftarrow \mathbb{Z} \cap [0,s), e \leftarrow D_{\alpha}\}$$

$$A_{K,\phi}^{\mathrm{AGCD}}(p) = \{qp + r : q \leftarrow \mathbb{Z} \cap [0, K/p), r \leftarrow \lfloor D_{\beta} \rceil\}$$

- Idea: Rescale a sample in $\mathbb{T}$ to an integer
- Given a ZDLWE sample y, output $x = \lfloor Ky \rceil \bmod K$.

$$Ky = \frac{K}{s} \cdot k + \frac{ke}{s} = pk + r,$$

where $p = \lfloor K/s \rceil$, $r \leq ke/s + k$ is small as $0 \leq k < s$ and s is small.

A new FHE scheme over the integers

Additive homomorphic encryption scheme

- KeyGen(λ)
  - Secret key p of bit size $\approx \eta$
  - Sample $x_i \leftarrow A^{\mathrm{AGCD}}_{K,\lfloor D_\alpha \rceil}(p)$ for $0 \leq i \leq \tau$
  - Relabel so that x_0 is largest and $\lfloor x_1/p \rceil$ is odd
- $\mathrm{Enc}_{\mathrm{pk}}(\mathrm{m})$ of a given message $m \in \{0,1\}$
  - Sample a subset $S \subseteq \{1,2,\ldots,\tau\}$
  - Output $c = \left[\sum_{i \in S} x_i + \lfloor \frac{x_1}{2} \rceil m \right]_{x_0}$
  - This is of the form $c = pq + \dfrac{p}{2}m + r$ for some small $r \in \frac{1}{2}\mathbb{Z}$
- $\mathrm{Add}_{x_0}(c_1, c_2) = [c_1 + c_2]_{x_0}$
- $\mathrm{Dec}_{sk}(c) = [\lfloor 2c/p \rceil]_2 = m$ because

$$\frac{2}{p}\left(pq + \frac{p}{2}m + r\right) = 2p + m + \frac{2r}{p} \xrightarrow{\lfloor \cdot \rceil} 2p + m \xrightarrow{[\cdot]_2} m.$$

Multiplication

- Idea
  - $c_1 c_2$ has two large noise $> r_1 r_2$.
  - $c = pq + (p/2)m + r \Rightarrow (p/2)c = 2q + m + \epsilon$ for $\epsilon = 2r/p$
  - $(2/p)c_1 \cdot (2/p)c_2 \Rightarrow \overline{(2/p)(2/p)}(c_1 \cdot c_2)$
  - $\lfloor (2/p)c_1 c_2 \rceil = pq^* + \frac{p}{2} m_1 m_2 + r^*$ ... but r^* is large.
- Bit-Decomposition and Power-of-Two [Bra12]
  - Given $a = \sum_i 2^i a_i$ for $a_i \in \{0, 1\}$, $\mathrm{BD}(a) = (a_0, \ldots, a_{\gamma-1})$.
  - Given $s \in \mathbb{R}$, $\mathcal{P}(s) = (s, 2s, \ldots, 2^{\gamma-1}s)$.
  - $\langle \mathrm{BD}(c), \mathcal{P}(2/p) \rangle = 2c/p\,(= 2q + m + \epsilon)$
- $\langle \mathrm{BD}(c), [\mathcal{P}(2/p)]_2 \rangle = 2N + m + \epsilon$ for an integer N with $|N| \leq \gamma/2$

Multiplication (continued)

- Tensor Product
  - $\mathbf{u} = (u_1, \ldots, u_m), \mathbf{v} = (v_1, \ldots, v_n)$
  - $\mathbf{u} \otimes \mathbf{v} = (u_1\mathbf{v}, u_2\mathbf{v}, \ldots, u_m\mathbf{v})$
  - $\langle \mathbf{u} \otimes \mathbf{v}, \mathbf{u}' \otimes \mathbf{v}' \rangle = \langle \mathbf{u}, \mathbf{u}' \rangle \langle \mathbf{v}, \mathbf{v}' \rangle$

- Let $\mathbf{Y} = [\mathcal{P}(2/p)]_2 \otimes [\mathcal{P}(2/p)]_2$. Then

$$\langle \mathrm{BD}(c_1) \otimes \mathrm{BD}(c_2), \mathbf{Y} \rangle = \frac{p}{2}(2N_1 + m_1 + \epsilon_1)(2N_2 + m_2 + \epsilon_2),$$

  which becomes $m_1 m_2$ after $\lfloor \cdot \rceil$ and $[\cdot]_2$.

- Publish $\bar{\mathbf{Y}}$, an encryption of $\mathbf{Y}$. Then $\mathrm{Mul}(c_1, c_2)$ is

$$c_{mult} = [\langle \mathrm{BD}(c_1) \otimes \mathrm{BD}(c_2), \bar{\mathbf{Y}} \rangle]_{x_0}.$$

Performance

- After a multiplication, the noise increases ‘linearly’ (as in [Bra12]).
- Bit-size of noise is $\leq L \log \gamma$ after homomorphic evaluation of circuit of multiplicative depth L.
- The choice of $\rho = \Omega(\lambda)$, $\eta - \rho = \Omega(L \log \lambda)$ and $\gamma = O(L^2 \lambda \log \lambda)$ achieves the functionality and security reduction together.

  $\Rightarrow$ Ciphertexts have quasi-linear size $\gamma = \tilde{O}(\lambda)$.

Open Questions

- Truncation: $c = pq + \frac{p}{2}m + r$ for random $r \in \mathbb{Z} \cap [2^{-\rho}, 2^{\rho}]$. The lsb ρ bits does not need to be transmitted. How small can $(\gamma - \rho)$ be?
- How to improve the scheme?
  - Faster Multiplication
  - Batch scheme with ciphertexts of quasi-linear size
  - Bootstrapping with non-binary message space
- Integer version of Ring-LWE problem and a scheme based on this
- Any essential difference between AGCD and LWE?