Fully homomorphic encryption scheme using ideal lattices

Gentry’s STOC’09 paper - Part II
GGH cryptosystem

- Gentry’s scheme is a GGH-like scheme.
- GGH: Goldreich, Goldwasser, Halevi.
- Based on the hardness of ClosestVector Problem (CVP).
- Our discussion of GGH is variant by D. Micciancio:
Secret key

- The secret key is a "good" basis $R = (r_1, \ldots, r_n)$ of a lattice $L$.
  - For computational purpose, assume $L \subset \mathbb{Z}^n$.
  - The quantity $\rho_R = \frac{1}{2} \min \|r_i^*\|$ is relatively large.
  - We know: $\lambda_1(L) \geq \min \|r_i^*\|$; thus, $\lambda_1(L) \geq 2 \rho_R$.
  - Thus, the orthogonalized centered parallelepiped $C(R^*)$ is fat, containing a ball of radius $\rho_R$.
  - Any point $t \in \mathbb{Z}^n$ with $\text{dist}(t, L) < \rho_R$ can be corrected to the closest lattice point (using the nearest plane algorithm).
A good basis and the corresponding correction radius

Source: Daniele Micciancio's paper, CaLC 2001
Public key

- The public key is a "bad" basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of $L$.
- For example, $\mathbf{B} = \text{HNF}(\mathbf{R})$.
- Its orthogonalized parallelepiped, $P(\mathbf{B}^*)$, is skiny.
- $\rho_B = \frac{1}{2} \min \| \mathbf{b}_i^* \|$ is much smaller than $\rho_R$.
- CVP (BDDC) is hard (w/o knowing $\mathbf{R}$) even if $\text{dist}(\mathbf{t}, L) < \rho_R$.
- Denote by $\mathbf{t} \mod \mathbf{B}$ the unique $\mathbf{s} \in P(\mathbf{B}^*)$ s.t.
  - $\mathbf{s}$ is congruent to $\mathbf{t}$ modulo $L$ (i.e., $\mathbf{s} \equiv_L \mathbf{t}$ or $\mathbf{t} - \mathbf{s} \in L$).
- (Here we use $P(\mathbf{B}^*)$ as the representative system of $\mathbb{R}^n / L$.)
HNF basis and corresponding orthogonalized parallelepiped

Source: Daniele Micciancio's paper, CaLC 2001
Encryption and Decryption

- Encryption: to encrypt a message $m$,
  - Encode $m$ as a vector $r$, $\|r\| < \rho_R$.
  - $c \leftarrow r \mod B$.

- Decryption: to decrypt a ciphertext $c$,
  - Recover $r$ from $c$ by $r \leftarrow c \mod R$.
  - Recover $m$ from $r$. 
Correcting small errors using the private basis

From Micciancio's paper
Is GGH homomorphic?

• If the encoding scheme is such that

\[
\begin{align*}
  m_1 &\rightarrow r_1 \\
  m_2 &\rightarrow r_2
\end{align*}
\]

\[\Rightarrow m_1 + m_2 \rightarrow r_1 + r_2\]

and if \( \|r_1\|, \|r_2\| < \rho_R/2 \), then GGH is additively homomorphic:

\[
\text{GGH}(m_1 + m_2) = \text{GGH}(m_1) +_{\text{mod } B} \text{GGH}(m_2)
\]

• How to make it multiplicatively homomorphc?
  • Genty's answer: use ideal lattices.
Ideals

Gentry’s scheme uses ideal lattices, which are lattices corresponding to some ideals
Rings

• A ring $R$ is a set together with two binary operations $+$ and $\times$ satisfying the following axioms:
  - $(R, +)$ is an abelian group.
  - $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$.
  - Distributive laws hold: $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$.

• The ring $R$ is commutative if $a \times b = b \times a$.

• The ring $R$ is said to have an identity if there is an element $1 \in R$ with $a \times 1 = 1 \times a = a$ for all $a \in R$.

• We will only be interested in commutative rings with an identity.
Ideals

- An ideal $I$ of a ring $R$ is an additive subgroup of $R$ s.t. $r \times I \subseteq I$ for all $r \in R$. (I.e., a subset $I \subseteq R$ s.t. $a - b \in I$ and $r \times a \in I$ for all $a, b \in I, r \in R$.)

- Example:
  - Consider the ring $\mathbb{Z}$.
  - For any integer $a$, $I_a = \{na : n \in \mathbb{Z}\}$ is an ideal.
  - Conversely, any ideal $I \subseteq \mathbb{Z}$ is equal to $I_a$ for some $a \in \mathbb{Z}$.
  - The mapping $f : a \mapsto I_a$ is a bijective function from the set of nonnegative integers to the set of ideals of $\mathbb{Z}$.

- The name ideal comes from "ideal" numbers.
Some historical notes

- An algebraic integer is a number $x \in \mathbb{C}$ satisfying
  
  $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, where $a_i \in \mathbb{Z}$.

- The set of all algebraic integers forms a ring.

- For any algebraic integer $\alpha$, $\mathbb{Z}[\alpha]$ denote the closure of $\mathbb{Z} \cup \{\alpha\}$ under $+, -, \times$.

- Example: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Gaussian integers.

- $\mathbb{Z}[\alpha]$ resembles $\mathbb{Z}$, and many questions concerning $\mathbb{Z}$ can be answered by considering $\mathbb{Z}[\alpha]$. 
• For instance, **Format's theorem on sums of two squares**: an odd prime $p$ can be expressed as $p = x^2 + y^2$ ($x, y \in \mathbb{Z}$) iff $p \equiv 1 \mod 4$.

• This theorem can be proved by showing that in $\mathbb{Z}[i]$
  
  - if $p \equiv 1 \mod 4$, then $p$ factors into $p = (a + bi)(a - bi)$
  
  - if $p \equiv 3 \mod 4$, then $p$ cannot be factored.

• While $\mathbb{Z}$ has the **unique prime factorization** property, $\mathbb{Z}[\alpha]$ in general doesn't. For instance, in $\mathbb{Z} \left[ \sqrt{-5} \right]$, 6 has two prime factorizations: $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. 
• Eduard Kummer, inspired by the discovery of imaginary numbers, introduced \textit{ideal numbers}.

• For instance, in the example of $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, we may define \textit{ideal prime numbers} $p_1, p_2, p_3, p_4$, which are subject to the rules:

$$p_1p_2 = 2, \quad p_3p_4 = 3, \quad p_1p_3 = 1 + \sqrt{-5}, \quad p_2p_4 = 1 - \sqrt{-5}.$$ 

• Then, 6 would have the unique prime factorization:

$$6 = p_1p_2p_3p_4.$$ 

• Kummer's concept of \textit{ideal numbers} was later replaced by that of \textit{ideals}, by Richard Dedekind.
Operations on Ideals

- Let $I, J$ be ideals of the ring $R$.

- **Sum of ideals**: $I + J \triangleq \{a + b : a \in I, b \in J\}$, which is the smallest ideal containing both $I$ and $J$.

- **Product of ideals**: $I \times J \triangleq$ the set of all finite sums of the form $a \times b$ with $a \in I, b \in J$. I.e., the smallest ideal containing $\{a \times b : a \in I, b \in J\}$. Thus, $R$ is the identity.

- $I$ divides $J$ iff $I \supseteq J$. Thus, $\gcd(I, J) = (I, J) = I + J$.

- $I$ is a **prime ideal** if $\forall a, b \in R, ab \in I \Rightarrow a \in I$ or $b \in I$.

- Two ideal $I$ and $J$ are **relatively prime** if $I + J = R$. 


Generators and Bases of ideals

- Let $B$ be any subset of a ring $R$.

- Denote by $(B)$ the smallest ideal of $R$ containing $B$, called the ideal generated by $B$. We have:

  $$(B) = \left\{ r_1 b_1 + \cdots + r_n b_n : r_i \in R, \ b_i \in B, \ n \in \mathbb{Z}^+ \right\}$$

- The ideal $I = (B)$ is finitely generated if $B$ is finite, and is a principal ideal if $B$ contains a single element.

- $B$ is a basis of $I = (B)$ if it is linearly independent.
Cosets

- Let $I$ be an ideal of a ring $R$.
- $R$ is partitioned into cosets s.t. two elements $a, b \in R$ are in the same coset iff $a - b \in I$. $R = \bigcup_{a \in \mathbb{Z}} (I + a)$
- The coset containing $a$ is $[a]_I = a + I = \{a + i : i \in I\}$.
- Define $[a]_I + [b]_I = [a + b]_I$ and $[a]_I \times [b]_I = [a \times b]_I$.
- The cosets form a ring $R/I$, called the quotient ring.
- Choose an element from each coset as a representative, then we have a system of representatives for $R/I$.
- For $x \in R$, denote by $x \mod I$ the element representing $[x]_I$. 
Gentry’s Ideal-based Scheme
Notations

- Let $I$ be an ideal of the ring $R$, and $\mathbf{B}_I$ a basis of $I$.
- $R \mod \mathbf{B}_I$: a system of representatives for $R/I$ defined by $\mathbf{B}_I$.
- If $\mathbf{B}_1 \neq \mathbf{B}_2$ are two bases for the same ideal, we have in general $x \mod \mathbf{B}_1 \neq x \mod \mathbf{B}_2$ (not necessarily equal).
- $\text{Samp}(x, \mathbf{B}_I)$: samples the coset $x + I$ according to some probability distribution.
- $C$: a circuit whose gates perform $+$ and $\times$ operations $\mod \mathbf{B}_I$.
- $g(C)$: generalized $C$, the same as $C$ but without $\mod \mathbf{B}_I$.
- $C_{B_j}$: same as $C$, but gates perform $\mod \mathbf{B}_j$ operations instead.
Σ: an ideal-based encryption scheme

- **KeyGen**\( (R, B_I) \):
  - Input: a ring \( R \), a basis \( B_I \) of an ideal \( I \).
  - \( (B_{sk}^J, B_{pk}^J) \leftarrow_R \text{IdealGen}(R, B_I) \).
  - Public key \( pk := B_{pk}^J \). Secret key \( sk := B_{sk}^J \).
  - Parameters: \( (R, B_I, \text{Samp}) \), which are public info.
  - Plaintext space \( P := \) (a subset of) \( R \) mod \( B_I \)

- **Remarks**: As in GGH, \( B_{sk}^J \) is a good (fat) basis and \( B_{pk}^J \) a bad (skiny) one. The ideal \( I \) is used to encode plaintexts as ring elements.
• Encrypt($pk, \pi$): \hspace{1em} // $\pi \in P$ //

$$\pi' \leftarrow \text{Samp}(\pi, B_I) \hspace{1em} // \text{an element in coset } \pi + I //$$

$$\psi \leftarrow \pi' \mod B_{j}^{pk} \hspace{1em} // \text{the ciphertext //}$$

• Decrypt($sk, \psi$):

$$\pi \leftarrow (\psi \mod B_{j}^{sk}) \mod B_{I}$$

• Remarks:
  
  • $\pi$ is encoded as a random element $\pi'$ in the same coset.
  
  • $\pi'$ is then encrypted as in GGH.

  • Decryption is correct if $\pi' \in R \mod B_{j}^{sk}$. 
• **Evaluate**\((pk,C,\Psi)\):

  • Input: a public key \(pk\); a mod\(B_I\) circuit \(C\) composed of Add\(_{B_I}\) and Mult\(_{B_I}\) (and identity) gates; and ciphertexts \(\Psi = (\psi_1, \ldots, \psi_i)\), where \(\psi_i = \text{Encrypt}(pk, \pi_i)\), \(\pi_i \in P\).
  
  • Output: \(\psi := g(C)(\Psi) \mod B^{pk}_J\).  \(// = g(C)(\Pi') \mod B^{pk}_J //\)

• **Remarks:**

  • Evaluate\((pk, \text{Add}_{B_I}, \psi_1, \psi_2)\): outputs \(\psi_1 + \psi_2 \mod B^{pk}_J\).
  
  • Evaluate\((pk, \text{Mult}_{B_I}, \psi_1, \psi_2)\): outputs \(\psi_1 \times \psi_2 \mod B^{pk}_J\).
  
  • Evaluate circuit \(C\) by evaluating its gates in a proper order.
Correctness: informal

- Evaluating $C$ yields:

$$\psi := C_{B_j^{pk}}(\Psi) = g(C)(\Psi) \mod B_J^{pk} = g(C)(\Pi') \mod B_J^{pk}$$

where $\Pi = (\pi_1, \ldots, \pi_t)$

$$\xrightarrow{\text{encode}} \Pi' = (\pi'_1, \ldots, \pi'_t)$$

$$\xrightarrow{\mod B_J^{pk}} \Psi = (\psi_1, \ldots, \psi_t).$$

- Decrypting $\psi$ will yield: $\pi := (\psi \mod B_J^{sk}) \mod B_I$.

- Correct if $g(C)(\Pi') \in R \mod B_J^{sk}$.

- Thus, if we restrict $\pi'_1, \ldots, \pi'$ to be in certain region, the scheme will be homomorphic for circuits $C$ for which $g(C)(\Pi') \in R \mod B_J^{sk}$. 
Correctness of the ideal-based scheme $\Sigma$

- Let $X_{Enc} \triangleq \text{Samp}(B_I, M)$ and $X_{Dec} \triangleq R \mod B_{J}^{pk}$.

- A $\mod B_{I}$ circuit $C$ (including the identity circuit) with $t \geq 1$ inputs is a permitted circuit w.r.t. the scheme if:
  \[
  \forall x_1, \ldots, x_t \in X_{Enc}, \ g(C)(x_1, \ldots, x_t) \in X_{Dec}.
  \]

- **Theorem:** If $C_{\Sigma}$ is a set of permitted circuits containing the identity circuit, then the scheme is correct for $C_{\Sigma}$.
  - I.e., algorithm Decrypt correctly decrypts valid ciphertexts:
    \[
    C(\Pi) = \text{Decrypt}(sk, \text{Evaluate}(pk, C, \Psi)),
    \]
    where $C \in C_{\Sigma}$ and $\Psi \leftarrow \text{Encrypt}(sk, \Pi)$.
  - Valid ciphertexts: outputs of $\text{Evaluate}(pk, C, \Psi)$, $C \in C_{\Sigma}$. 

coset $\pi + I$

Encrypt: $\pi \xrightarrow{\text{Samp}(B_J, \pi)} \pi' \xrightarrow{\text{mod } B_J^{pk}} \psi$

Decrypt: $\pi \xleftarrow{\text{mod } B_J} \psi' \xleftarrow{\text{mod } B_J^{sk}} \psi$

It works if $\pi' = \psi'$, i.e. if $\pi' \in R \mod B_J^{sk}$.
Q: Is $C(\Pi) = \text{Decrypt}(sk, C_{B_p^k}(\Psi)) \triangleq (C_{B_p^k}(\Psi) \mod B_{sk}^J) \mod B_I$?

$C(\Pi) = g(C)(\Pi') \mod B_I$

$g(C)(\Pi') \mod B_{pk}^J = C_{B_p^k}(\Psi)$

$g(C)(\Pi') \mod B_{sk}^J = C_{B_p^k}(\Psi) \mod B_{sk}^J$

$(g(C)(\Pi') \mod B_{sk}^J) \mod B_I = (C_{B_p^k}(\Psi) \mod B_{sk}^J) \mod B_I$

Yes, if $g(C)(\Pi') = g(C)(\Pi') \mod B_{sk}^J$, i.e., $g(C)(\Pi') \in R \mod B_{sk}^J$. 
Security of the ideal-based scheme
Ideal Coset Problem (ICP)

- Let $R$ be a ring, $I$ an ideal, and $\mathbf{B}_I$ a basis.
- IdealGen: an algorithm that given $(R, \mathbf{B}_I)$ outputs two bases $\mathbf{B}^{\text{sk}}_J, \mathbf{B}^{\text{pk}}_J$ of the same ideal $J$.
- Samp$_1$: a random algorithm that samples $R$ (non-uniformly).
- Ideal Coset Problem: Fix $R, \mathbf{B}_I, \text{IdealGen}, \text{Samp}_1$.
  - Challenger: $(\mathbf{B}^{\text{sk}}_J, \mathbf{B}^{\text{pk}}_J) \leftarrow_R \text{IdealGen}(R, \mathbf{B}_I)$. $b \leftarrow_u \{0, 1\}$.
    - If $b = 0$, then $r \leftarrow_R \text{Samp}_1(R)$, $t \leftarrow r \mod \mathbf{B}^{\text{pk}}_J$.
    - If $b = 1$, then $t \leftarrow_{\text{uniformly}} R \mod \mathbf{B}^{\text{pk}}_J$.
  - Adversary: given $t$ and $\mathbf{B}^{\text{pk}}_J$, determine if $b = 0$ or 1.
- Essentially, the problem is to distinguish between:
  - \( b = 0 \): a coset \([t]_j\) is chosen according to some "Samp\(_1\)."
  - \( b = 1 \): a coset \([t]_j\) is chosen uniformly randomly.

- The hardness of ICP depends on Samp\(_1\).

- How does ICP connect to Gentry's encryption scheme \(\Sigma\)?
  - A ciphertext is essentially a coset \([\pi']_j\) chosen by Samp.
  - \(\Sigma\) is semantically secure if the ciphertext is random-like.
  - ICP is hard if coset \([t]_j\) chosen by Samp\(_1\) is random-like.

- Will show ICP \(\leq\) distinguishing ciphertexts of scheme \(\Sigma\).

- Will use Samp\(_1\) to define Samp.
Connect Samp to Samp$_1$

- $r \leftarrow \text{Samp}_1(R)$ samples an element in ring $R$.
- $x' \leftarrow \text{Samp}(x, B_I)$ samples an element in coset $[x]_I$.
- Wanted:
  
  $r$ random $\Rightarrow x'$ random

- Let $I = (s) = R \times s$ be a principal ideal generated by $s$.

  Then, $[x]_I = x + R \times s$.

- Let $\text{Samp}(x, B_I) \triangleq x + \text{Samp}_1(R) \times s$. 
Security of the ideal-based scheme $\Sigma$

- The Ideal Coset Problem is to distinguish between
  - $t \leftarrow \text{Samp}_1(R) \mod \mathcal{B}^\text{pk}_J$
  - $t \leftarrow \text{uniform}(R \mod \mathcal{B}^\text{pk}_J)$.

- Encrypt($pk, \pi$):
  \[
  \psi \leftarrow \text{Samp}(\pi, \mathcal{B}_I) \mod \mathcal{B}^\text{pk}_J \\
  (\pi + \text{Samp}_1(R) \times s) \mod \mathcal{B}^\text{pk}_J
  \]

  where $I = (s) = R \times s$ is a principal ideal generated by $s$. 
Theorem: If there is an algorithm $A$ that breaks the semantic security of $\Sigma$ with advantage $\varepsilon$ when it uses Samp, then there is an algorithm $B$, running in about the same time as $A$, that solves the ICP with advantage $\varepsilon/2$.

Proof: The challenger of ICP sends $B$ an instance $(t, B^j_{\mathbf{B}})$. $B$ chooses an ideal $I = \langle s \rangle$ relatively prime to $J$ and sets up the other parameters of $\Sigma$. We have two games:

1. the ICP game between Challenger and $B$ (adversary), and
2. the $\Sigma$ game between $B$ (challenger) and $A$ (adversary).

They run as follows.
where if \( b = 0 \), \( t \leftarrow \text{Samp}_1(R) \mod B_{J}^{pk} \); else, \( t \leftarrow_u R \mod B_{J}^{pk} \); and \( \psi_\beta \leftarrow (\pi_\beta + t \times s) \mod B_{J}^{pk} \).
• If $b = 0$, $t \leftarrow \text{Samp}_1(R) \mod B^p_k$ and $\psi_\beta = (\pi_\beta + t \times s) \mod B^p_k$  
$$= \left(\pi_\beta + \text{Samp}_1(R) \times s\right) \mod B^p_k = \text{Encrypt}\left(B^p_k, \pi_\beta\right).$$

$\pi'_\beta \leftarrow \text{Samp}(\pi_\beta, B_I)$

$$\Pr[b = b' \mid b = 0] = \Pr[\beta = \beta' \mid b = 0] = 1/2 + \varepsilon.$$

• If $b = 1$, $t \leftarrow_{\text{uniform}} R \mod B^p_k$, so $\psi_\beta = (\pi_\beta + t \times s) \mod B^p_k$

is uniformly random (for $I = (s)$ is relatively prime to $J$  
$s^{-1}$ exists  
$t \mapsto \pi_\beta + t \times s$ bijective  
$\pi_\beta + t \times s$ uniform.)

$$\Pr[b = b' \mid b = 1] = \Pr[\beta \neq \beta' \mid b = 1] = 1/2.$$

• Thus, $B$ has advantage $\varepsilon/2$. 