全同態加密發展與現狀的綜述

胡予濮，陳虎，連至助
西安電子科技大學 西安
yphu@mail.xidian.edu.cn

摘要

全同態密碼加密體制能對密文的任意函數進行同態計算。全同態加密長期被尊爲密碼學的“聖杯”，有著極其豐富的應用。自 Gentry 於 2009 年突破性實現了全同態加密體制（FHE）構造，開啓了這困擾密碼學家 30 餘年的大門。Gentry 這一突破性的工作和 FHE 不成熟的現狀極大激發了密碼學家的研究熱情，大批高水平的研究成果相繼湧現。本文主要對全同態加密取得突破以來的進展做一個粗線條的回顧，側重於介紹構造全同態方案中所湧現出的各種新方法和新技術。

關鍵字：全同態加密；Bootstrapping；Squashing

1 引言

Rivset，Adleman 和 Dertouzos 在 1978 年提出一個具有挑戰性的問題[45]：在不使用私鑰解密的情況下，我們能否對密文進行任意計算，且運算結果的解密值等於對應的明文運算的結果。具有這種性質的加密稱爲同態加密，如教科書式-RSA 和 ElGamal 體制屬乘法同態體制，可以支持任意次乘法同態操作，但不支持加法同態操作並且方案也不是語義安全的。這種同態性本來被視爲一種安全性缺陷，卻能夠提供一種極爲重要的服務：無信任委托計算，支持電子投票系統，保密信息檢索等。這個新穎獨特，但確如海市蜃樓般的困難問題被譽爲密碼學的“聖杯”。

1984 年，Goldwasser 和 Micali 提出第一個具有語義安全的加法同態密碼體制 GM，支持任意次加法（模 2）同態操作。2005 年 Boneh-Goh-Nissm 提出 BGN 同態加密體制[4]，可以支持任意次加法和一次乘法同態。2006 年，Fellows 和 Koblitz 提出“Polly Cracker”體制支持任意電路[20,37-39]，但是誤差隨密文尺寸指數增長。Sanders，Young 和 Yung，使用保密電路（**circuit-private**）加法同態加密構造的保密電路體制 SYY 能處理 NC_1 電路[47,3]。Ishai 和 Paskin 使用線路圖（braching programs），能同態處理 NC_1 電路[35]。

儘管歷經 30 餘年的艱辛探索，但是上述方案距離真正全同態方案還很遠。直到 2009 年 Gentry 實現了全同態加密構造的重大突破，使用理想格構造了可以支持任意深度電路的同態計算[21,22]。他所構造的方案 E 有四個算法：$KeyGen_{\mathrm{E}}, Encrypt_{\mathrm{E}}$，$Decrypt_{\mathrm{E}}$ 和 $Evaluate_{\mathrm{E}}$。其中 $Evaluate_{\mathrm{E}}$ 算法以公鑰 pk，屬允許電路集 C_{E} 的電路 C，和一組密文 $(c_1,\cdots,c_t)$ 爲輸入，輸出密文 c。上述所有算法都是多項式時間的，該全同態加密方案實現的是語義安全（CPA 安全）。因爲同態密碼是可展的，所以方案不能達到 CCA2 安全

性。儘管文獻[1,11,43]考慮了弱化的 CCA2 安全的概念，但尚需完善。至於構造 CCA-1 安全的全同態加密仍是個重要的公開問題。

此後，出現許多改進和變形的全同態加密體制。主要集中在：基於 Gentry 初始方案的改進構造[24,25,48,50,52]，基於整數全同態加密構造[15,17-19,36]，基於 LWE 和 RLWE 問題的構造[6,8-10,23]，及其運用擴展。其中，引入很多新的處理技術, 每個新技術的出現都帶來 FHE 方案效率的提高。但總起來看，已有的 FHE 方案依然遠遠無法滿足實用性的要求。

本文主要對全同態加密取得突破以來的進展做一個粗線條的回顧，側重於介紹構造全同態方案中所湧現出的各種新方法和新技術，將很少涉及全同態方案安全性方面的發展。文章第 2 節介紹 Gentry 基於理想格全同態構造方案，第 3 節介紹全同態加密的進一步發展。第 4 節總結全文。

2 全同態加密的突破

2009 年 Craig Gentry 在其博士論文中，至少在理論上解決了如何全同態構造這一問題，使得全同態密碼開始接近現實。Gentry 構造全同態加密方案分三步：第一步是基於理想格構造一個 somewhat 同態加密（SWHE）方案，即一個能同態計算“淺的電路”加密方案。然後是證明一個“Bootstrappable”同態體制（能同態計算自己解密電路）能通過遞歸嵌入構造全同態密碼。最後是提出 Squashing 技術，修改解密電路，降低解密電路複雜度，該體制獲得 Bootstrappable。

2.1 Somewhat 同態加密

Gentry 利用如下的基本加密方案去構造 SWHE。

基本加密方案

- $KeyGen(R, B_I)$：令 J 爲 n 維整數向量空間 $\mathbb{Z}^n$ 上大尺寸的理想格，生成其陷門基私鑰 B_J^{sk}，公開基 B_J^{pk}，令 I 爲 n 維整數向量空間 $\mathbb{Z}^n$ 上小尺寸的理想格，它是 2 的整數倍向量的全體。B_I 是 I 的基，它的所有列向量爲 $(2,0,0,\cdots,0)$，$(0,2,0,\cdots,0)$，…，$(0,0,0,\cdots,2)$。換句話說，$\mathbb{Z}^n \bmod B_I$ 是所有 n 維布爾向量全體。公鑰 pk 包含 B_J^{pk}，B_I。私鑰爲 $sk = B_J^{sk}$。
- $Encrypt(pk, m)$：明文 $m \in \{(1,0,\cdots,0),(0,0,\cdots,0)\}$，是 $\mathbb{Z}^n \bmod B_I$ 子集。（可以理解爲明文空間爲 $\{1,0\}$，不影響其加法和乘法。）對於明文 m，從 B_I 中隨機抽樣誤差向量 $e_i = (e_{i_1}, e_{i_2}, \cdots, e_{i_n})$。密文 $c = (m+e) \bmod B_J^{pk} = m + e + j$，$j$ 爲理想 J 中的某個向量。
- $Decrypt(sk, c)$：$m' \leftarrow (c \bmod B_J^{sk}) \bmod B_I$。
  解密算法正確性：$((m+e+j) \bmod B_j^{sk}) \bmod B_I = (m+e) \bmod B_I = m$。

基本方案的同態性

設密文 $c_i = (m_i + e_i) \bmod B_J^{pk} = m_i + e_i + j_i$ ， $i = 1, 2\cdots$ 。

加法同態：

$$c_{add} = (c_1 + c_2) \bmod B_J^{sk} = \left((m_1 + m_2) + (e_1 + e_2) + (j_1 + j_2)\right) \bmod B_J^{sk} \text{ ，}$$

解密得

$$\begin{aligned} & \left(c_{add} \bmod B_J^{sk}\right) \bmod B_I \\ = & \left(\left(m_1 + m_2 + (e_1 + e_2) + (j_1 + j_2)\right) \bmod B_J^{sk}\right) \bmod B_I \\ = & \left(m_1 + m_2 + (e_1 + e_2)\right) \bmod B_I \\ = & (m_1 + m_2) \bmod B_I \end{aligned}$$

這就是說，$(m_1 + m_2) \bmod B_I$ 是 $(c_1 + c_2) \bmod B_J^{pk}$ 的解密值，即方案是加法同態的。加密同態的充分條件爲 $\left(m_1 + m_2 + (e_1 + e_2)\right)$ 在陷門基 B_J^{sk} 所對應的“平行 2n 面體”的最大內含球之內，$\left\|\left(m_1 + m_2 + (e_1 + e_2)\right)\right\| \le R$ ， R 爲球半徑。換句話說，正確解密要求，明文 m 和誤差 e 滿足 $\|m + e\| \le R/2$ 。

乘法同態：

$$\begin{aligned} c_{mult} &= c_1 c_2 \bmod B_J^{pk} \\ &= \left((m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2) + (m_1 j_2 + m_2 j_1 + e_1 j_2 + e_2 j_1 + j_1 j_2)\right) \bmod B_j^{pk} \\ &= \left((m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2) + j\right) \bmod B_J^{pk} \end{aligned}$$

解密得

$$\begin{aligned} & \left(c_{mult} \bmod B_J^{sk}\right) \bmod B_I \\ = & \left(\left((m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2) + j\right) \bmod B_J^{sk}\right) \bmod B_I \\ = & \left((m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2)\right) \bmod B_I \\ = & (m_1 m_2) \bmod B_I \end{aligned}$$

這就是說，$(m_1 m_2) \bmod B_I$ 是 $(c_1 c_2) \bmod B_J^{pk}$ 的解密值，即方案是加法同態的。加密同態的充分條件爲 $(m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2)$ 在陷門基 B_J^{sk} 所對應的“平行 $2n$ 面體”的最大內含球之內，即

$$\left\|(m_1 m_2) + (m_1 e_2 + m_2 e_1 + e_1 e_2)\right\| \le R \text{ ，}$$

R 爲球半徑。換句話說，正確解密要求，明文 m 和誤差 e 滿足 $\|m + e\| \le \sqrt{R/\gamma}$ 。其中 γ 爲乘法規模。

若 k 個密文相加

$$\sum_{i=1}^{k} c_i \bmod B_J^{pk}$$

得到的新密文，其所含的誤差擴大到原來誤差的 k 倍。若 k 個密文相乘

$$\prod_{i=1}^{k} c_i \bmod B_J^{pk}$$

得到的新密文，其含有的誤差擴大到原來誤差尺寸的 k 次方。

因此，k 個密文相加

$$\sum_{i=1}^{k} c_i \bmod B_J^{pk} \ ,$$

想要讓其解密值總是對應的 k 個明文相加

$$\sum_{i=1}^{k} m_i \bmod B_I \ ,$$

要求 R 的尺寸是單純加密 R 尺寸的 k 倍。任何 k 個密文相乘

$$\prod_{i=1}^{k} c_i \bmod B_J^{pk} \ ,$$

要想讓其解密值總是對應的 k 個明文相乘

$$\prod_{i=1}^{k} m_i \bmod B_I \ ,$$

R 的尺寸大於單純加密的 R 的尺寸的 k 次方。故爲獲得全同態服務所付出的空間代價是不能承受的。這就是說，該同態加密不能做到全同態，只是一個“有點同態（somewhat 同態）”的加密方案。

2.2 bootstrapping 過程

對一個密文 c，它是由若干個密文的環運算 $\left(\bmod B_J^{pk}\right)$ 而得到的，其所含的誤差尺寸是原誤差尺寸的 k 倍。

如果有一種方法，將密文 c 變爲對應相同明文的另一個密文 m'，m' 所含的誤差尺寸僅僅是原誤差尺寸的 l 倍，其中 $l < k$。則密文的變換就意味著誤差尺寸的縮小。

於是，“有點同態”的加密方案就可以擴展爲以下的“全同態”的加密方案：密文運算到一定深度就做一次降低誤差尺寸的運算。

我們來觀察加密方案的解密電路 $m = Decrypt\left(sk, c\right)$，其中 c 是密文，m 是明文，sk 是私鑰，$Decrypt$ 是解密算法。 服務器知道密文 c，因此在服務器眼中 c 是“公開參數”。服務器知道解密算法 $Decrypt$。

服務器不知道私鑰 sk，因此在服務器眼中 sk 是“明文（或若干個明文）”。服務器不知道明文 m，因此在服務器眼中 m 是“明文”。

綜上所述，在服務器眼中

1）解密電路 $m = Decrypt\left(sk, c\right)$ 是若干個“明文”的運算，輸入若干個“明文” sk，輸出一個新的“明文” m。

2）該“明文”運算可以在對應的“密文”端做同態運算。“明文”運算 $m = Decrypt\left(sk, c\right)$ 對應的“密文”同態運算爲 $m' = Decrypt'\left(sk', c\right)$，其中 m' 是“明文” m 的對應“密文”，sk' 是

“明文”*sk* 的對應“密文”，*Dectry'*是“明文”運算所對應的“密文”運算。這就是說，“密文”同態運算輸入若干個“密文”*sk'*，輸出一個新的“密文”*m'*。

3）該“明文”運算是“深度有限的”。（比如，不超過 100000 個“明文”相加）

4）因此，該“明文”運算所對應的“密文”同態運算也是“深度有限的”。（比如，不超過 100000 個“密文”相加）

5）因此，該“明文”運算在對應的“密文”端進行的同態運算，其輸出值 *m'* 所含的誤差尺寸是有限的。（比如，不超過原誤差尺寸的 100000 倍）

6）另一方面，*m* 是 *c* 的解密值，但 *c* 是從前由若干密文運算得到的，*c* 所含的誤差尺寸是比較大的。（比如，超過原誤差尺寸的 200000 倍）

7）通過對“明文”運算進行“密文”同態運算，將原來的密文 *c* 變換爲新的“密文” *m'*，並縮小了誤差尺寸。（比如，從超過原誤差尺寸的 200000 倍，到不超過原誤差尺寸的 100000 倍）

以上過程就稱爲 Bootstrapping。

需要指出的是私鑰 *sk* 的加密值 *sk'*，是用什麼公鑰加密的？如果是用 *sk* 自己所對應的公鑰加密的，則加密方案必須具有更強的“KDM 安全性”。如果不能保證“KDM 安全性”，就必須用另一個公鑰加密 *sk* 。這就是說，進行一次 Bootstrapping，就要更換一次密鑰。

Bootstrapping 技術是把一個 SWHE 方案轉化爲 FHE 方案的關鍵技術，是目前可以在固定長度的密鑰和密文條件下對任何可以有效操作的函數進行同態運算的唯一途徑，但同時也是制約 FHE 方案的效率的“罪魁禍首”。提高 Bootstrapping 技術運行效率成爲 FHE 實用化道路上極需解決的問題。文獻[9,19,21,22,24,25]中 Bootstrapping 運行時間約 $O(\lambda^4)$，λ 爲安全參數,。文獻[7,29]把 Bootstrapping 效率向前推進了一大步，在約爲 $O(\lambda)$ 時間中同時對包含 $\Omega(\lambda)$ 比特的密文進行 Bootstrapping，實現 Bootstrapping 在時間和空間上漸進最優。 最近，在美密 2013 中，Jacob Alperin-Sheriff 和 Chris Peikert 指出文獻[7,29]中的算法在實際應用中有潛在的限制，他們推廣了文獻[26]中的換環技術，給出實用性強的，每個密文進行 Bootstrapping 的運行時間約爲 $O(\lambda)$ 的新方法[2]。

2.3 Squashing 解密電路

Gentry 的解密算法在理想格上運算如下：

$$\left(c \bmod B_J^{sk}\right) \bmod B_I = c - B_J^{sk} \cdot \text{鍵}_J^{sk})^{-1} \cdot c \bmod B_I$$

爲了把這個解密算法改造成“明文運算”，並且是可以在密文端進行同態運算的“明文運算”，Gentry 做了大量的工作。

構造步驟一

將 R 的尺寸擴大 $2n^{2.5}\|M(x)\|$ 倍，可以找到很多 $\left(v_J^{sk}\right)^{-1} \in J$ ，使得可以變形解密 $m = c - (v_J^{sk})^{-1} \cdot \text{鍵}^k \cdot c \bmod B_I$ 。

構造步驟二

注意：當 $v_J^{sk} \in J^{-1}$ 時，未必有 $\left(v_J^{sk}\right)^{-1} \in J$ 。我們只能說，當 v_J^{sk} 是 J^{-1} 的子理想格的生成元時，$\left(v_J^{sk}\right)^{-1}$ 是 J 的超理想格的生成元。

構造步驟二

將 R 的尺寸再擴大 2 倍（即總擴大 $4n^{2.5}\|M(x)\|$ 倍），可以找到更多的 $\left(v_J^{sk}\right)^{-1} \in J$ ，使得可以變形解密

$$m = \left(c - (v_J^{sk})^{-1} \cdot \text{鍖}_J^k \cdot c\ \right) \bmod B_I ,$$

而且保證對任何密文 c 都有 $\text{鍖}_J^k \cdot c$ 的每個分量都在 $v_J^{sk} \cdot c$ 的對於分量的 $\pm 1/4$ 之內，而不是 $\pm 1/2$ 。

構造步驟三

在很多 $v_J^{sk} \in J^{-1}$ 中可以找到一個 $v_J^{sk} \in J^{-1}$ 使得 $\left(v_J^{sk}\right)^{-1} \bmod B_I$ 等於單位向量 $(1,0,\cdots,0)$ ，因此變形解密形式爲

$$m = \left(c - (v_J^{sk})^{-1} \cdot \text{鍖}_J^k \cdot c\ \right) \bmod B_I = \left(c - \text{鍖}_J^k \cdot c\ \right) \bmod 2 。$$

新的解密算法 $m = \left(c - \text{鍖}_J^k \cdot c\ \right) \bmod 2$ 是變形私鑰 v_J^{sk} 的布爾函數（ v_J^{sk} 的二進制中各比特的布爾函數）。換句話說，變形解密運算正是“明文運算”。

似乎問題變得很直接：只要把這個“明文運算”簡單地翻譯成（同構成）“密文運算”即可。“明文”（即 v_J^{sk} 的二進制表示中各比特）用密文（即 v_J^{sk} 的二進制表示中各位的加密值）來代替。“明文加法”換成密文加法， “明文乘法”換成密文乘法。但是變形私鑰 v_J^{sk} 的布爾函數是表示不出來的，因爲有指數多個項。

解決方法：引入稀疏子集和問題，即將私鑰 v_J^{sk} 撕碎（Squashing），然後將碎片公開。取逆格 J^{-1} 上的 $\gamma_{set(n)}$ 個向量 $t_1, t_2, \cdots, t_{\gamma_{set(n)}}$ ，他們看起來像是從空間 $J^{-1} \bmod B_I$ 中均勻選取，但要求，$t_1, t_2, \cdots, t_{\gamma_{set(n)}}$ 中有 $\gamma_{subset(n)}$ 個向量 $u_1, u_2, \cdots, u_{\gamma_{subset(n)}}$ ，滿足

$$\sum_{i=1}^{\gamma_{subset(n)}} u_i \equiv v_J^{sk} \bmod B_I 。$$

此時公鑰包括公開基 B_J^{pk} ，基 B_I ，向量組 $t_1, t_2, \cdots, t_{\gamma_{set(n)}}$ （ v_J^{sk} 撕碎的碎片和其他無用的碎片的混合體）。私鑰變成 $\gamma_{subset(n)} \times \gamma_{set(n)}$ 階矩陣 M ，其中 $M_{ij} = 1$ 當且僅當 $u_i = t_j$ ，否則 $M_{ij} = 0$ ，已知 M 的每一行至多有一個 1，其餘都爲 0。

解密算法如下：

第零步　計算 $A = \left(a_1, a_2, \cdots, a_{\gamma_{set(n)}}\right)$ ，其中 $a_j = c \times t_j \bmod B_I$ 的第一個分量（向量模乘後的第一個分量。向量模乘即兩個向量的重模乘積）。置 $w_{ij} \leftarrow M_{ij} \cdot a_j$

第一步　輸出 $x_i = w_{i1} + w_{i2} + \cdots + w_{i,\gamma_{set(n)}}$ ，$i = 1 \square \gamma_{subset(n)}$ 。其中的加法可以換爲“同層次的比特抑或”，而不需要進位。即爲簡單的“明文運算”。

第二步　取 $\left(y_1, \cdots, y_{\gamma_{subset(n)}}\right)$ 分別爲 $\left(x_1, \cdots, x_{\gamma_{subset(n)}}\right)$ 的整數部分，取 $y_{\gamma_{subshet(n)+1}}$ 的是 $\left(x_1, \cdots, x_{\gamma_{subset(n)}}\right)$ 純小數部分的和的最近整數。於是有

$$錯_1 + x_2 \cdots + x_{\gamma_{subset(n)}} = y_1 + y_2 \cdots + y_{\gamma_{subset(n)}+1}$$

第三步 明文 $m = \left(c - \left(y_1 + y_2 \cdots + y_{\gamma_{subset(n)}+1}\right)\right) \bmod B_I$

$$= \left(c - \left(y_1 + y_2 \cdots + y_{\gamma_{subset(n)}+1}\right)\right) \bmod 2$$

到此爲止，Gentry 使用 Squashing 技術，壓縮 SWHE 方案的解密電路，將一部分解密任務交給加密者預先計算，減輕解密者的計算負擔，從而能夠實現同態計算過程中對自身解密電路的調用。

2.4 Gentry 構造的局限性

首先，構造方案是基於多個複雜的假設的。其中最大的問題是 squashing 解密電路時引入的稀疏子集和問題 SSSP，它是否必須？是否存在僅基於單個假設的全同態密碼體制？基於理想格上問題，他的近似因子能否是多項式的？

其次，Bootstrapping 中，每個門電路需同態調用解密電路，效率制約是固有的。是否可以有另一種輕量級的降低噪聲新方式？

正是 Gentry 傑出工作的示範性和內在的局限性，爲 FHE 的進一步發展提供了強大的推動力。

3 全同態加密的發展

自從 Gentry 里程碑式的工作以後，國際上掀起了對全同態密碼的研究熱潮，相繼出現一大批高水平研究成果。他們通過引入新的技術以逐步優化方案的效率或擴展全同態加密的功能。

3.1 基於Gentry 構造方法的FHE

Gentry 的傑出工作不僅給出了首個全同態加密方案，而且提供了構造全同態加密方案的一種通用模式。第一代的 FHE 都遵循著 Gentry 的構造模式，把方案構建在理想環上，並依賴於稀疏子集和問題困難假設[24,25,48,50,52]。

文獻[19]提出第二個全同態加密 DGHV，該方案使用了 Gentry 構造方案中所使用的多個構造工具，但他們使用一個非常簡單的基於整數的 SWHE 來替換 Gentry 構造中基於理想格的 SWHE。因此 DGHV 方案在概念上方案更簡潔，更易於理解。但是，它的公鑰尺寸高達 $O(\lambda^{10})$，因而不具有實用價值。後來，文獻[17]改進了 DGHV 中方案的公鑰生成方法，即只需存儲較少數量的小尺寸公鑰，由這些小尺寸的公鑰兩兩相乘，生成較大尺寸的全部的公鑰。這樣，他們把 SWHE 方案的公鑰尺寸成功降到 $O(\lambda^7)$。爲防止運

算中誤差過快增長，他們需要公鑰 $x_0 = q_0 p$ 不含任何的誤差，這似乎在某種程度上弱化近似 GCD 問題的困難性，即他們的方案的安全性基於 PACD 問題。在 EUROCRYPT 2012 中，Yuanmi Chen 和 Phong Q.Nguyen 提出了解決 PACD 和 GACD 問題的快速算法[12]，對上述在整數上構造的 FHE 方案構成嚴重威脅。

Smart 和 Vercauteren 提出首個對 Gentry 構造全同態思想的方案的實現體制 SV[50]。它的新穎之處是密文不是向量而是整數。SV 方案可以方便地把對單比特消息的同態加密擴展爲多比特，而且支持 SIMD(single-instruction multiple-data)操作[51]以實現並行再加密，極大地提高 FHE 的效率。但是，由於在實現過程中所使用的主理想的範數要求必須是個素數，導致密鑰生成過程太複雜。2011 年，Gentry 等人通過取消主理想的範數是素數的限制，提高了 SV 體制中公鑰生成算法效率[25]。文獻[48]又對該密鑰生成算法實施進一步優化。2012 年，Smart 等人進一步指出文獻[25]中密鑰生成算法不支持 SIMD。

SIMD 技術

Smart 和 Vercauteren 首先注意到：SV 體制中的明文空間利用關於多項式的中國剩餘定理，可以分解成若干個相同子域的直積，這些子域形成由“plaintext slots”組成的向量，每個“plaintext slot”含有子域中的一個元素。

例如，設 $f(x)$ 爲 $F[x]$ 上的 N 次不可約多項式，且 $f(x)$ 在 $F_2[x]$ 上可被分解爲 r 個次數爲 $d = N/r$ 的不可約多項式，即

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

定義數域 $K = \square[x]/(f(x)) = \square(\theta)$，這裏 θ 爲 $f(x) = 0$ 在有理數域的代數閉包上的根。明文空間 $A := F_2[x]/(f(x))$，據中國剩餘定理有：

$$A \cong F_2[x]/(f_1(x)) \otimes \cdots \otimes F_2[x]/(f_r(x)) \cong F_{2^d} \otimes \cdots \otimes F_{2^d}$$

令 θ_i 爲 $f_i(x) = 0$ 在有限域 F_2 的代數閉包上的根，並記 $L_i := F_2[x]/(f_i(x))$，$i = 1, 2, \cdots, r$，則子域 L_i 間具有同構關係：

$$\Lambda_{i,j} : L_i \to L_j, \alpha(\theta_i) \mapsto \alpha(\rho_{i,j}(\theta_i))\ ,$$

其中 $\rho_{i,j}(\theta_i)$ 爲 $f_i(x)$ 在有限域 L_j 中的一個根。

對整數 d 的每個正因子 n，定義有限域 $K_n := F_{2^n} \cong F_2[x]/(k_n(x)) \subset F_{2^d}$，$\psi$ 代表 n 次不可約多項式 $k_n(x)$ 在有限域 F_2 的代數閉包上的根。這樣，可得到如下同態映射：

$$\psi_{n,j} : K_n \to L_i, \alpha(\psi) \mapsto \alpha(\sigma_{n,i}(\theta_i))\ ,$$

其中 $\sigma_{n,i}(\theta_i)$ 爲 $k_n(x)$ 在有限域 L_i 中的一個根。

據上述同態映射和中國剩餘定理，可以得到如下同構映射：

$$\Gamma_{n,l} : K_n^{\ l} \to A, (\kappa_1(\psi), \cdots, \kappa_l(\psi)) \mapsto \sum_{i=1}^{l} \kappa_i(\sigma_{n,i}(x)) \cdot H_i(x) \cdot G_i(x)$$

其中，正整數 $l \le r$ ， $H_i(x) = f(x) / f_i(x), G_i(x) = 1/ f_i(x) (\mathrm{mod}\ f_i(x))$ 。

同構映射 $\Gamma_{n,l}$ 可把由“plaintext slots”組成的向量 $(\kappa_1(\psi),\cdots,\kappa_l(\psi))$，轉化到明文空間 A 中元素，對 A 中元素的每次同態操作就相當於對向量 $(\kappa_1(\psi),\cdots,\kappa_l(\psi))$ 中 l 個小明文並行操作了各一次，從而極大地提高了方案的效率。另外，SIMD 技術使得一個密文包含多個獨立的明文，更加有效地利用了密文尺寸，降低了計算代價。

文獻[7]進一步地把 Smart 和 Vercauteren 提出的 SIMD 技術應用於 Ring-LWE 困難問題的 FHE，並獲得較好的性能。在 PKC13 中，文獻[8]借鑒 Peikert 等人在文獻[44]提出的批處理方法，把 SIMD 技術應用於基於標準 LWE 困難問題的 FHE。在歐密 2013 中，文獻[16]巧妙利用中國剩餘定理，把基於整數上的 FHE 方案 DGHV 改造成可進行 SIMD 技術處理的 FHE 方案，並切實提高了方案的效率。SIMD 技術已經成爲提高 FHE 運行效率的重要技術之一。

3.2 基於LWE和Ring-LWE的FHE

爲了避免引入稀疏子集和問題，文獻[10]和[24]分別獨立地提出了不同的有效方法構造不需要對解密電路壓縮處理的 FHE。其中，文獻[10]，Brakerski 和 Vaikuntanathan 提出的基於帶誤差的學習(LWE)困難問題在一般的格上構造出一個 FHE，代表了 FHE 發展的主流趨勢。這是因爲安全性基於 LWE 或 Ring-LWE 的 FHE 比以前的 FHE 方案的效率高，且湧現出諸如再線性化，換模，換環和近似特徵向量法等新技術。

文獻[10]引入了再線性化技術，應用該技術在一般的格上構造了一個 SWHE 方案。然後，他們運用降維縮模技術來降低解密電路的複雜度，從而把 SWHE 轉成 FHE。

3.2.1 再線性化技術

考察一個基於 LWE 問題的加密方案 SHW：

設 q 爲大素數，n 爲正整數，按下列步驟用私鑰 $s \in Z_q^n$ 加密明文 $m \in \{0,1\}$。

加密：隨機選擇向量 $a \in Z_q^n$ 和小誤差量 $e \in Z_q$ ，則密文

$$c = (a, b = < a, s > + 2e + m) \in Z_q^n \times Z_q \text{ 。}$$

解密：給定一個密文 (a,b) ，定義線性函數 $f_{a,b} : Z_q^n \to Z_q$

$$f_{a,b}(x) = b - < a, x > (\mathrm{mod}\, q) = b - \sum_{i=1}^{n} a[i]x[i]$$

這裏 $x = (x[1], x[2], \cdots, x[n])$ 表示變量，(a,b) 組成函數的係數。顯然，解密方程可寫成 $m = f_{a,b}(s) \bmod 2$ 。

同態性：易知 $f_{a+a',b+b'}(x) = f_{a,b}(x) + f_{a',b'}(x)$ 是相應密文 $(a+a', b+b')$ 的線性函數。

類似地，兩個密文的乘積相應的線性函數的乘積爲：

$$\begin{aligned} f_{a,b}(x) \cdot f_{a',b'}(x) &= (b - \sum a[i]x[i])(b' - \sum a'[i]x[i]) \\ &= h_0 + \sum h_i x[i] + \sum h_{i,j} x[i]x[j] \end{aligned}$$

上述等式右端是關於變量 $x=(x[1],x[2],\cdots,x[n])$ 的二次多項式，若要完成解密必須知道這些二次項的係數，這意味著密文尺寸從 $n+1$ 增加到大約 $n^2/2$ —這是進行密文同態乘法運算遇到的嚴重挑戰。而再線性化技術可以將增大的密文尺寸重新降到 $n+1$。

考察 $f_{a,b}(s)\cdot f_{a',b'}(s)=h_0+\sum h_i s[i]+\sum h_{i,j}s[i]s[j]$

在新的私鑰 t 下，對所有的 $s[i],s[i]s[j]$ 項逐個加密。因此，這些密文具有如下形式：

$$b_i=<a_i,t>+2e_i+s[i]\approx<a_i,t>+s[i]\ ;$$

$$b_{i,j}=<a_{i,j},t>+2e_{i,j}+s[i]s[j]\approx<a_{i,j},t>+s[i]s[j]\ 。$$

於是，

$$h_0+\sum h_i s[i]+\sum h_{i,j}s[i]s[j]=h_0+\sum h_i(b_i-<a_i,t>)+\sum h_{i,j}(b_{i,j}-<a_{i,j},t>)\ ,$$

這可以看成含有至多 $n+1$ 項關於變量 $t=(t[1],t[2],\cdots,t[n])$ 的線性函數。

這裏需要指出：當係數 $h_{i,j}$ 很大時，則 $h_{i,j}(b_{i,j}-<a_{i,j},t>)\approx h_{i,j}s[i]s[j]$ 將再不成立。爲此，用二進制表示

$$h_{i,j}=\sum_{\tau=0}^{\lfloor\log q\rfloor}h_{i,j,\tau}2^{\tau}\ 。$$

對每個 τ，有 $(a_{i,j,\tau},b_{i.j,\tau})$ 滿足 $b_{i,j,\tau}=<a_{i,j,\tau},t>+2e_{i,j,\tau}+2^{\tau}s[i]s[j]\approx<a_{i,j,\tau},t>+2^{\tau}s[i]s[j]$。

這樣，有

$$h_{i,j}s[i]s[j]\approx\sum_{\tau=0}^{\lfloor\log q\rfloor}h_{i,j,\tau}(b_{i,j,\tau}-<a_{i,j,\tau},t>)$$

其中 $h_{i,j,\tau}\in\{0,1\}$。

再線性化技術使我們在不增加密文尺寸的條件下完成一次同態乘法運算，獲得在新私鑰下的消息乘積的密文。如果連續實施多次再線性化，可以獲得基於 LWE 問題的 SWHE 方案。

3.2.2 降維縮模技術

上述 SHW 方案的解密算法爲 $(b-\langle a,s\rangle \bmod q)\pmod 2$，其複雜度至少爲 $\max(n,\log q)$。設該 SHW 方案可進行的同態運算的深度爲 D，則 $\max(n,\log q)>D$。

注意到在上面的再線性化過程中，可以將密鑰 s 下的密文 $(a,b=<a,s>+2e+m)$ 轉化爲密鑰 t 下的密文 $(a',b'=<a,t>+2e'+m)$，而且密鑰 s 和 t 不必都是 n 維數。故可以考慮選擇 t 是 k 維向量，使得 $k<n$。這樣解密算法的複雜度從 $(n,\log q)$ 降到 $(k,\log q)$。

進一步地，若選擇 $t\in\mathbb{Z}_p$，使得模數 $p<q$，保證 $\max(k,\log p)<D$。

若 $(a_{i,\tau},b_{i,\tau})\in\mathbb{Z}_p^k\times\mathbb{Z}_p$，其中 $b_{i,\tau}=\langle a_{i,\tau},t\rangle+e+\lfloor\frac{q}{2}\rfloor 2^{\tau}\cdot s[i]$，則

$$2^{\tau} s[i] \approx \frac{q}{p}(b_{i,\tau} - \langle a_{i,\tau}, t\rangle)。$$

這樣，就保證把關於 s 的線性函數轉化爲關於 t 的線性函數。因此，實施降維縮模技術後，就得到新密文 $(\hat{a},\hat{b}) \in Z_p^k \times Z_p$，滿足 $\hat{b} - \langle \hat{a}, t\rangle = m + 2\hat{e}$。

文獻[10]構造的上述方案的最大亮點是取消了 Gentry 方案中使用的解密電路壓縮技術，從而避免引入稀疏子集和問題，效率也比 Gentry 方案有所提高。缺陷是需要很大的維數，導致方案的效率和安全性受到很大的影響。基於 LWE 全同態加密的提出，標誌著對 FHE 方案的構造進入到第二代。

2012 年，Brakerski，Gentry 和 Vaikuntanathan 給出了通用的 FHE[7]，即它的安全性可選擇基於 LWE 或 Ring-LWE 問題，但基於 Ring-LWE 問題的 FHE 效率更高。該方案是對文獻[10]中方案進行了進一步地優化，他們把再線性化技術應用到私鑰變換子程序中。他們注意到[10]中降維縮模技術是降低解密電路複雜度的利器，但也帶來方案在最初幾步運算中要求所依賴格的維數過大的問題。故他們只縮模不降維，採用更加靈活的噪聲處理方式——**梯狀逐次遞縮換模技術**(*a ladder of gradually decreasing moduli*)。該技術可以保證密文中噪聲的絕對大小不變，但模數逐漸變小，以此可以極大提高進行同態計算的次數。他們在密文刷新的子程序中順次使用模交換技術和私鑰變換技術實現不需 Bootstrapping 過程也可以對密文中的噪聲量進行有效的控制。該方案是第一個擺脫使用 Bootstrapping 過程的 FHE。

其 Somewhat 同態方案 *SH* 構造：

設 q 爲奇素數，$f(x)$ 爲一個 n 次不可約多項式，環 $R = Z[x]/(f(x))$ 和 $R_q = R/qR$。χ 爲環 R 上的一個“誤差”分布，用於產生多項式的“小”係數。消息空間爲 $R_2 = R/2R$

$SH.Keygen(1^{\kappa})$：$sk := s \leftarrow R_q$，其中 s 爲係數來自“誤差”分布 χ 的一個多項式。

$SH.Encrypt(sk, \mu \in R_2)$：$a \xleftarrow{R} R_q$，$e$ 爲係數來自“誤差”分布 χ 的一個多項式。輸出密文 $c := (a, as + 2e + \mu)$。

$SH.Decrypt(sk, c = (a,b))$：計算 $\hat{\mu} = b - as \bmod q$，輸出 $\mu = \hat{\mu} \bmod 2$。

解密成功的條件是密文中的噪聲應“充分小”。對密文同態操作會引起噪聲的增加，特別地，同態計算一個含有 M 個變量的 D 次多項式時，噪聲會變成 $O(M \cdot n^{O(D)})$。方案的高效性充分體現在其超強的噪聲處理技術。

3.2.3 換模技術

換模技術是處理噪聲的關鍵手段，是下面引理的直接應用。

引理 1 設 p、q 爲兩個奇素數，$a,b \in R_q$，$c = (a,b)$ 爲密文，定義 $c' = (a',b')$ 是整數向量接近於向量 $\frac{p}{q}c = (\frac{p}{q}a, \frac{p}{q}b)$，且滿足 $c' = c \bmod 2$，那麼對任何的 s 滿足 $|b - as \bmod q| < \frac{q}{2} - \frac{q}{p}\ell_1(s)$，必有

$$(b' - a's \bmod p) \bmod 2 = (b - as \bmod q) \bmod 2 \text{ 和 } |b' - a's \bmod p| < \frac{p}{q}|b - as \bmod q| + \ell_1(s)，$$

這裏$\ell_1(s)$表示多項式s對應係數形成向量的ℓ_1範數。

該引理說明了一個同態計算者在僅僅獲知私鑰s長度的範圍的情況下，就可以把密文$c \bmod q$轉化爲相同私鑰s下的另一個密文$c' \bmod p$，滿足$(c's \bmod P) \bmod 2 = (c \bmod q) \bmod 2$。

從密文c到c'轉化過程中僅涉及一個簡單的縮放p/q和取整操作。尤其是當私鑰s模很小，素數p比q充分小的情況下，c'中的噪聲的確比c中的小，即$|c's \bmod P| < |cs \bmod q|$。換句話說，換模技術爲全同態加密方案提供了一個非常有力的輕量級處理噪聲的手段。

3.2.4 梯狀逐次遞縮換模技術

咋一看，換模似乎並非降噪的有力工具。如上所述，當模數p比q小時，換模確實降低了噪聲，但是同比例地減少了模數。換句話說，新舊密文中噪聲與相應模數的比沒發生改變。

事實上，在噪聲處理過程中，不只是噪聲與模數的比是重要的，噪聲的絕對量也是重要的，特別在密文乘法操作中。下面通過具體的例子來說明。

設模$q \approx x^k$，密文c_1, c_2中的噪聲均爲x。經歷一次同態乘法運算後，密文中的噪聲約爲x^2。這樣，當密文經歷第4層同態乘法運算後，結果密文中的噪聲約爲x^{16}。這時，若想把該密文的噪聲降到x，則需要把模縮小x^{15}倍，這意味著噪聲的絕對量對縮小噪聲有很大的影響。如此這樣只需經歷$\log_2 k$層同態乘法運算後，結果密文的噪聲量就達到模數q。

如果每做一次同態乘法運算就把模數縮小，而不是連續做多次同態乘法等到噪聲積累到一定程度再把模數縮小，那將會有何效果呢？

選擇梯狀逐次遞縮模列$\{q_i \mid q_i \approx q / x^i, q \approx x^k, i < k\}$。密文$c_1, c_2$中的噪聲均爲$x$。經歷一次同態乘法運算後，密文中的噪聲約爲$x^2$。此時，利用引理 1 把結果密文的模換爲$q_1 \approx q / x$，則新密文的噪聲由原來的$x^2$變回到$x$。接著，我們把兩個噪聲爲$x$在模$q_1$的密文再做一次乘法，密文中的噪聲又增到約爲$x^2$。對該密文的模換爲$q_2 \approx q / x^2$，則該密文的噪聲又由原來的$x^2$變回到$x$。總之，按這種方式逐次遞縮換模，保證噪聲絕對量不變，經歷大約k層（而不是$\log_2 k$）同態乘法運算後，結果密文的噪聲量就達到模數q。

由此可見，利用梯狀逐次遞縮換模技術，我們把 SWHE 方案的乘法同態次數大大增強了指數倍，這種同態能力足以實現 leveled FHE 而無需借助 Bootstrapping 過程。

另外，文獻[7]還可以利用 Bootstrapping 和批處理等多種措施加以優化，與以往所有方案相比，效率極大提高。

Brakerski 分析發現上述方案中的梯狀逐次遞縮模換過程仍制約 FHE 的性能，進而構造出一個比例不變的(scale-invariant)FHE 方案[6]。該方案的性質只依賴於模數q和初始噪聲大小 B，而與它們的絕對值無關。因此，該方案不需要進行複雜的模數轉換。同時，由於方案性質與模數q的絕對值無關，可以通過設置模數大小使得建立從 GapSVP 到方案安全性的一個傳統歸約，並且 GapSVP 問題的近似因子是擬多項式的。

3.2.5 換環技術

基於 LWE 的 FHE 方案前幾層同態運算工作在維數很高的多項式環上以保障方案的安全，然而隨著模數的不斷減小，噪聲保持不變，後幾層同態運算工作在維數較低的多項式環上。因此，從安全角度來說，BGV 型 FHE 方案在後幾層同態運算中容許轉化到低維環中運行，以加速同態運算。文獻[7]僅在 Bootstrapping 過程中實現了這種換環技術，且僅局限於環族 $\mathbb{Z}[x]/(x^{2^n}+1)$。不久，Gentry 等人在文獻[26]中把換環技術推廣到任何分圓多項式環，不僅應用於 Bootstrapping 過程，而且可以配合密文批處理技術的使用，以達到降低計算代價之目的。

換環技術實質就是滿足一定條件的一個線性映射。設 $K=\mathbb{Q}(\zeta_m)\cong\mathbb{Q}[x]/\phi_m(x)$，$R=\mathbb{Z}(\zeta_m)\cong\mathbb{Z}[x]/\phi_m(x)$，其中

$$\phi_m(x)=\prod_{i\in\mathbb{Z}_m^*}(x-\zeta_m^i)$$

是 m 階分圓多項式。

設正整數 $\omega\mid m$，且 $u=m/\omega, u'=\phi(m)/\phi(\omega)$，$K'=\mathbb{Q}(\zeta_\omega)\subseteq K$，$R'=\mathbb{Z}[\zeta_\omega]\subseteq R$，則 $K=K'[\zeta_m]$ 是有限域 K' 的 u' 次擴域。這樣，K 可視爲 K' 上的 u' 維線性空間，設 $\zeta_m^0,\cdots,\zeta_m^{u'-1}$ 是其一組 $K'-$基。對任意的 $a\in K$，則有

$$a=\sum_{k=0}^{u'-1}a_k\zeta_m^k\ ,$$

其中 $a_k\in K'$。 上述 $a\in R$,當且僅當每個 $a_k\in R'$。

下面定義把高維環 R 中元素轉化爲低維環 R' 上元素的映射：

$$T:R\to(R')^{u'}, a\mapsto T(a)=(a_0,a_1,\cdots,a_{u'-1})$$

不難驗證映射 T 滿足如下性質：

性質 1 映射 T 是線性的，即對任意 $a,b\in K, r'\in K'$，必有 $T(a+b)=T(a)+T(b)$ 和 $T(r'a)=r'T(a)$。

性質 2 對環 R' 的任意理想 $\wp$，可誘導出線性雙射映射 $T_\wp:R_\wp\to(R_\wp')^{u'}$，即

$$T_\wp(a+\wp R)=T_\wp(a)+(\wp)^{u'}=(a_0+\wp,\cdots,a_{u'-1}+\wp)。$$

性質 3 近似保長度，即 T 把高維環 R 中短尺寸元素映射到低維環 R' 上短尺寸元素。

這裏指出僅依靠在 Bootstrapping 過程的換環技術並不能降低同態計算量，還需成功完成對高維環下批處理後的密文轉化爲低維批處理密文後的同態運算才能達到提高效率的目的。

在美密 2013 上，Gentry 等人指出，基於 LWE 或 Ring-LWE 問題的 FHE 都使用到再線性化技術[6,7,10]，這種技術很巧妙但不自然，很難給出直觀的解釋—它爲什麼可以和如何起作用。最令人傷神的是每次再線性化操作必然伴隨著尺寸爲 $\Omega(n^3)$ 的矩陣，公鑰中必須含有 L 個這樣的矩陣，其中 L 表示同態運算電路的最大乘法深度。從計算角度

來看，再線性化約需要$\Omega(n^3)$個操作，而且每個操作所耗費的代價是關於L的多項式。因此，再線性化操作代價昂貴。

能否以更自然的乘法方式構造基於 LWE 或 Ring-LWE 問題的 FHE 方案，能否不需要用於同態運算的公鑰，尤其是再線性化矩陣呢？

Gentry 等人利用近似特徵向量法構造了 FHE[23]。該 FHE 方案的同態加和乘就是對應矩陣的加和乘，且該 FHE 方案無需同態運算公鑰。這使得 FHE 方案效率更高，概念上更簡潔。

3.2.6 近似特徵向量法

設正整數q,N分別爲模數和維數，密文C爲Z_q上的$N\times N$矩陣，C的元素遠小於q。密鑰$\vec{v}$是Z_q上的一個N維向量，其至少含有一個大係數v_i。消息μ是一個小整數。當$C\cdot\vec{v}=\mu\cdot\vec{v}+\vec{e}$，且$\vec{e}$是一個小誤差向量時，稱$C$爲消息$\mu$的密文。

解密時，首先從密文矩陣C中抽取第i行C_i，計算$x\leftarrow\langle C_i,\vec{v}\rangle=\mu\cdot v_i+e_i$，輸出$\mu=$錯誤/$v_i$。

由此可見，密鑰$\vec{v}$是密文矩陣C的近似特徵向量，而消息μ就是其特徵值。

下面考察該方案的同態性質。設C_1,C_2分別爲消息μ_1,μ_2的密文，即存在小向量$\vec{e_i}$，滿足$C_i\cdot\vec{v}=\mu_i\cdot\vec{v}+\vec{e_i}$，這裏$i\in\{1,2\}$。

令$C^+=C_1+C_2$，則有$C^+\cdot\vec{v}=(\mu_1+\mu_2)\vec{v}+(\vec{e_1}+\vec{e_2})$。因爲$\vec{e_1},\vec{e_2}$爲小向量，所以$\vec{e_1}+\vec{e_2}$也爲小向量。於是，$C^+$就是消息$\mu_1+\mu_2$的密文。

令$C^\times=C_1\cdot C_2$，則有

$C^\times\cdot\vec{v}=C_1(\mu_2\vec{v}+\vec{e_2})=\mu_2(\mu_1\vec{v}+\vec{e_1})+C_1\vec{e_2}=\mu_2\mu_1\vec{v}+\mu_2\vec{e_1}+C_1\vec{e_2}$。

如果能保證$\mu_2\vec{e_1}+C_1\vec{e_2}$爲小向量，則$C^\times$就是消息$\mu_1\cdot\mu_2$的密文。這需要對密文平化處理以使矩陣$C_1$中元素變小。

3.2.7 密文平化技術（ciphertext flattening）

爲使$\mu_2\vec{e_1}+C_1\vec{e_2}$爲小向量，必要條件是密文矩陣$C_1$中的每個元素都是充分小的整數，如矩陣$C_1$爲 0,1 矩陣。他們借鑒再線性化技術中對向量使用兩個重要函數$Bitdecomp(\cdot)$和 $Powerof\,2(\cdot)$方法，給出處理矩陣的$Flatten(\cdot)$函數。

令向量$\vec{a},\vec{b}$是有限域Z_q中的k維向量，即$\vec{a}=(a_1,a_2,\cdots,a_k)$，$\vec{b}=(b_1,b_2,\cdots,b_k)$。令$\ell=\lceil\log_2 q\rceil+1$，$N=\ell k$。定義$BitDecomp\left(\vec{a}\right)=(a_{1,0},\cdots,a_{1,\ell-1},\cdots,a_{k,0},\cdots,a_{k,\ell-1})$爲$N$維向量，滿足

$$a_i=\sum_{j=0}^{\ell-1}a_{i,j}\cdot 2^j\ ,\ i=1,2,\cdots,k\ 。$$

定義$Powersof\,2\left(\vec{b}\right)=(b_1,2b_1,\cdots,2^{\ell-1}b_1,\cdots,b_k,2b_k,\cdots,2^{\ell-1}b_k)$。

設$\vec{a}'=(a_{1,0},\cdots,a_{1,\ell-1},\cdots,a_{k,0},\cdots,a_{k,\ell-1})$爲任意的$N$維向量，定義

$$Flatten\left(\vec{a}'\right) = BitDecomp\left(BitDecomp^{-1}\left(\vec{a}'\right)\right)。$$

$Flatten\left(\vec{a}'\right) = BitDecomp\left(BitDecomp^{-1}\left(\vec{a}'\right)\right)$是$Z_2$上的$N$維向量。

容易看出有如下等式成立。

$$\langle BitDecom(\vec{a}), Powersof\,2(\vec{b})\rangle = \langle \vec{a}, \vec{b}\rangle ，$$

$$\langle \vec{a}', Powersof\,2(\vec{b})\rangle = \langle BitDecomp^{-1}(\vec{a}'), \vec{b}\rangle = \langle Flatten(\vec{a}'), Powersof\,2(\vec{b})\rangle 。$$

若$C = (C_1, C_2, \cdots, C_k)^T$爲限域$Z_q$中$k \times k$矩陣，其中$C_i$表示矩陣的行向量，則定義

$BitDecomp(C) = (BitDecomp(C_1), BitDecomp(C_2), \cdots, BitDecomp(C_k))^T$;

$BitDecomp^{-1}(C) = (BitDecomp^{-1}(C_1), BitDecomp^{-1}(C_2), \cdots, BitDecomp^{-1}(C_k))^T$;

$Flatten(C) = (Flatten(C_1), Flatten(C_2), \cdots, Flatten(C_k))^T$ 。

這樣，對向量或矩陣進行平化處理，在不影響內積的情況下把其中的元素變小了。於是，在不要再線性化操作的情況下完成很自然的同態操作，進而避免了使用同態運算公鑰，從而大大降低了存儲代價，提高了方案的運行效率。更爲重要的是，無需同態運算公鑰這一重大突破爲構造基於身份和屬性的 FHE 打開了通道。

3.3 基於身份的FHE

基於身份的加密[5,19]和基於屬性的加密[32,46]可實現比傳統公鑰系統更加靈活的對加密數據的訪問控制。但構造基於身份的FHE（甚至SWHE）一直都是一個難以解決的公開問題[6,13,30,42]。儘管文獻[31]可以基於“dual-Regev" 系統構造格上基於身份的加密方案，生成基於身份的公私鑰。但是能產生基於身份的公私鑰在構造基於身份的FHE的征途中只解決了一半的問題，只能構造很“粗糙”的基於身份的FHE。主要障礙在於以前所有已知的FHE都需要同態運算公鑰，他們是無法身份化的。另外，構造基於屬性的FHE似乎更困難。

Gentry等人使用近似特徵向量法構造無需同態運算公鑰的FHE，這爲構造基於身份和屬性的FHE提供了可能。他們稱一個基於身份的加密方案，只要滿足如下3個性質就可以轉化爲基於身份HFE。

性質4 設身份爲ID，其對應的密文和解密密鑰分別爲$\vec{c}_{ID}, \vec{s}_{ID} \in Z_q^{n'}$，且$\vec{s}_{ID}$的第一個分量爲1。

性質5 若密文$\vec{c}_{ID}$爲0的密文，則$\langle \vec{c}_{ID}, \vec{s}_{ID}\rangle$是小整數。

性質6 若密文$\vec{c}_{ID}$爲0的密文，則$\vec{c}_{ID}$與從Z_q中均勻選擇的向量是不可區分的。

限於篇幅，至於基於屬性的HFE構造詳細過程請讀者參看文獻[10]。

3.4 基於NTRU-variant 的Multi-keys FHE

前面所提到的FHE都是在相同公鑰下的加密密文進行同態計算的，但許多場合需要對多用戶的加密數據進行同態操作，而每個用戶都獨立擁有其自己的公鑰。這就涉及到

如何構造多公鑰FHE問題。Lopez-Alt等人提出了多鑰FHE的概念[40]。一個多鑰FHE相比於常規FHE有兩點變化：其一是同態運算可輸入多項式個密文，這些密文至多是N個公鑰下的密文。其二是對同態運算結束後得到的密文進行解密需要所有涉及到的密鑰共同參與。他們基於 *NTRU* 加密方案[33]，借助再線性化、換模等技術構造了一個多鑰FHE。

他們還指出文獻[9,10,19,21,50]中的方案都可以用來構造多鑰FHE。下面給出構造多鑰FHE方案所依賴的NTRU方案及其所具有的同態性質。

設κ為安全參數，素數模$q=q(\kappa)$，χ為環$R=\mathbb{Z}[x]/\langle x^n+1\rangle$上 B-差錯分布，所有運算都在環$R_q=R/qR$，明文空間為$\mathbb{Z}_2$。

$KeyGen\left(1^\kappa\right)$：抽取受限係數多項式$f',g\leftarrow\chi$，令$f:=2f'+1$滿足$f\equiv 1(\mathrm{mod}\,2)$。公鑰$pk$為$h=2gf^{-1}\in R_q$，私鑰$sk$為$f\in R$。若$f$在$R_q$不可逆，則需重新抽取$f'$。

$Encrypt\left(pk,m\right)$：對明文加密，抽取受限係數多項式$s,e\leftarrow\chi$，輸出密文$c:=hs+2e+m\in R_q$。

$Decrypt\left(sk,c\right)$：因為$f\equiv 1\bmod 2$，當滿足$|2(gs+ef)+fm|<q/2$，則有

$$\begin{aligned}&fc \bmod q \bmod 2\\ &= f(hs+2e+m)(\mathrm{mod}\,q)(\mathrm{mod}\,2)\\ &= 2(gs+ef)+fm(\mathrm{mod}\,q)(\mathrm{mod}\,2)\\ &= 2(gs+ef)+fm(\mathrm{mod}\,2)\\ &= m\end{aligned}$$

多鑰同態性

設$c_1=h_1s_1+2e_1+m_1\in R_q$，$c_2=h_2s_2+2e_2+m_2\in R_q$分別明文$m_1,m_2$在公鑰$h_1,h_2$下的密文。若記$c^+=c_1+c_2$，$c^\times=c_1c_2$，則$c^+,c^\times$分別是消息$m_1+m_2$和$m_1m_2$在聯合公鑰$f_1f_2$下的密文。同態理由如下：

$$\begin{aligned}&f_1f_2(c_1+c_2)\bmod q\bmod 2\\ &=\underbrace{2[f_1f_2(e_1+e_2)+f_2g_1s_1+f_1g_2s_2]}_{2E_{add}}+f_1f_2(m_1+m_2)\bmod q\bmod 2\\ &=f_1f_2(m_1+m_2)+2E_{add}\bmod 2\\ &=m_1+m_2\end{aligned}$$

$$\begin{aligned}&f_1f_2(c_1c_2)\bmod q\bmod 2\\ &=\underbrace{2[2g_1g_2s_1s_2+f_1f_2(e_1m_2+e_2m_1+2e_1e_2)+f_1g_2s_2(2e_1+m_1)+f_2g_1s_1(2e_2+m_2)]}_{2E_{mult}}\\ &\quad+f_1f_2(m_1m_2)\bmod q\bmod 2\\ &=f_1f_2(m_1m_2)+2E_{add}\bmod 2\\ &=m_1m_2\end{aligned}$$

當然，在上述同態過程中，噪聲會不斷積累，因此同態運算的次數只是有限的。他們採用換模技術[7,10]來降低噪聲。構造多鑰 FHE 還會遇到特殊的困難——對同態運算後的密文解密，需知道該同態運算電路。例如，在兩個公鑰的 FHE 系統中，為正確解密

密文 $c_1^2 + c_2$，需要對應的公鑰爲 $f_1^2 f_2$，而解密密文 $c_1 + c_2^2$ 需要的聯合公鑰卻爲 $f_1 f_2^2$。這顯然與設計 FHE 需要保證同態電路的私密理念背道而馳。還有一個問題是對同態密文的解密所需的聯合公鑰個數隨著涉及參與用戶人數指數級增長。這也是該方案限定參與用戶個數的一個原因。

爲克服上述障礙，他們借用再線性化技術，遇到聯合公鑰中存在某個公鑰出現 2 次時，就做一次再線性化，把 2 次化爲 1 次。具體過程請讀者參看文獻[40]。

4 結論與展望

全同態加密的構造問題 30 年以來一直是個公開問題，直到 Gentry 在 2009 年提出了第一個構造方案，開啓了全同態設計的新篇章。近幾年，伴隨全同態加密的快速發展，各種新工具、新技術不斷湧現，其性能也在不斷改進。新穎獨特的應用場景是 FHE 發展的不竭動力。

廣義上講，可以將同態加密的絕大多數應用視作安全多方計算的範疇，即全同態加密機制在複雜密碼協議的構造和設計中具有重要的應用價值。例如，應用全同態加密方案可以構造較短的非交互式證明，可證明的外包計算，私密信息檢索（PIR），代理重加密，KDM 安全的加密體制等等。隨著當今流行的安全雲存儲與安全雲計算的廣泛認可和應用，人們對同態加密的應用前景充滿渴望。

但是，不容忽視的問題是：全同態加密是否可以實用，或者全同態加密能否實用？顯然，從目前已有的全同態加密體制來看，將其應用於解決實際問題尚有很長的路要走。而且除了效率之外，存在許多重要的公開問題極待解決[53]。例如，CCA1 安全的全同態加密構造，如何弱化不可展性以構造選擇性允許的同態運算等等。

5 參考文獻

[1] J. H. An, Y. Dodis, and T. Rabin. On the security of jointsignature and encryption. In Eurocrypt 2002, pp. 83–107.

[2] J. Alperin-Sheriff and C. Peikert. Practical Bootstrapping in Quasilinear Time，R. Canetti and J.A. Garay (Eds.): CRYPTO 2013, Part I, LNCS 8042, pp. 1–20, 2013.

[3] D. Beaver. Minimal-latency secure function evaluation. Eurocrypt ’00, pp. 335–350.

[4] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. TCC ’05, pp. 325–341.

[5] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM J. of Computing 32(3), 586–615 (2003); Extended abstract in Kilian, J. (ed.): CRYPTO 2001.

LNCS, vol. 2139, pp. 586–615. Springer, Heidelberg (2001)

[6] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In: Safavi-Naini, R. (ed.) CRYPTO 2012. LNCS, vol. 7417, pp. 868–886. Springer, Heidelberg (2012)

[7] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) Fully homomorphic without Bootstrapping. In: Goldwasser, S. (ed.) ITCS 2012, pp. 309–325. ACM (2012)

[8] Z. Brakerski, C. Gentry, and S. Halevi. Packed ciphertexts in LWE-based homomorphic encryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 1–13. Springer, Heidelberg (2013)

[9] Z. Brakerski and V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In CRYPTO'2011,505-524,2011.

[10] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In FOCS 2011, 97-106.

[11] R. Canetti, H. Krawczyk, and J.B. Nielsen. Relaxing chosen-ciphertext security. Crypto '03, pp. 565–582.

[12] Y. Chen and P. Q. Nguyen. Faster algorithms for approximate common divisors: Breaking fullyhomomorphic-encryption challenges over the integers. Cryptology ePrint Archive, Report 2011/436, 2011, http://eprint.iacr.org/2011/436.

[13] M. Clear, A. Hughes, and H. Tewari. Homomorphic encryption with access policies: Characterization and new constructions. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 61–87. Springer, Heidelberg (2013)

[14] H. Cohn and N. Heninger, Approximate common divisors via lattices. Cryptology ePrint Archive, Report 2011/437, 2011, http://eprint.iacr.org/2011/437.

[15] J.-S. Coron, T. Lepoint, M. Tibouchi, et al. Batch fully homomorphic encryption over the integers. In EUROCRYPT 2013, pp. 315-335.

[16] J.-S.Coron, T. Lepoint, and M. Tibouchi. Batch fully homomorphic encryption over the integers. In EUROCRYPT 2013, pp. 315-335

[17] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi. Fully Homomorphic Encryption over the Integers with Shorter Public Keys. In Crypto 2011. 487-504. 2011

[18] J.-S. Coron, D. Naccache, and M. Tibouchi. Public-key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. In Eurocrypto 2012，446-464.

[19] M. v. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In ASIACRYPT'2010, 24-43.

[20] M. Fellows and N. Koblitz. Combinatorial cryptosystems galore! Contemporary Mathematics, v. 168 of Finite Fields: Theory, Applications, and Algorithms, FQ2, pp.

51–61, 1993.

[21] C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC '2009, 169-178.

[22] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University (2009), http://crypto.stanford.edu/craig

[23] C. Gentry, A. Sahai, and B. Waters. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, in CRYPTO 2013, 75-92

[24] C. Gentry and S. Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In FOCS 2011, 107-109.

[25] C. Gentry and S. Halevi. Implementing Gentry's full homomorphic encryption scheme. In EUROCRYPT 2011, 129-148.

[26] C. Gentry, S. Halevi, C. Peikert, and N. P. Smart. Ring Switching in BGV-Style Homomorphic Encryption.Manuscript, http://eprint.iacr.org/2012/240.

[27] C. Gentry, S. Halevi and N. P. Smart. Homomorphic Evaluation of the AES Circuit. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 850–867. Springer, Heidelberg (2012)

[28] C. Gentry, S. Halevi and N. P. Smart. Fully Homomorphic Encryption with Polylog Overhead. In Eurocrypto 2012, 465-482.

[29] C. Gentry, S. Halevi, and N. P. Smart. Better bootstrapping for fully homomorphic encryption. In PKC'2012 Springer, LNCS 7293, PP:1–16.

[30] C. Gentry, S. Halevi, V. Vaikuntanathan. A simple BGN-type cryptosystem from LWE. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 506–522. Springer, Heidelberg (2010)

[31] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In: STOC, pp. 197–206. ACM (2008)

[32] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS, pp. 89–98 (2006)

[33] J. Hoffstein, J. Pipher, and J. H. Silverman. Ntru: A ring-based public key cryptosystem. In J. Buhler, editor, ANTS, volume 1423 of Lecture Notes in Computer Science, pages 267-288. Springer, 1998.

[34] N. Howgrave-Graham. Approximate integer common divisors. In CaLC, 2001, pp. 51–66.

[35] Y. Ishai and A. Paskin. Evaluating Branching Programs on Encrypted Data. TCC '07.

[36] J. Kim, M. S. Lee, A. Yun, and J. H. Cheon. CRT-based fully homomorphic encryption over the integers. Cryptology ePrint Archive, Report 2013/057 (2013), http://eprint.iacr.org

[37] F. Levy-dit-Vehel and L. Perret. A Polly Cracker system based on satisfiability. In Coding, Crypt. and Comb., Prog. In Comp. Sci. and App. Logic, v. 23, pp. 177–192.

[38] L Ly. A public-key cryptosystem based on Polly Cracker, Ph.D. thesis, Ruhr-Universit¨at Bochum, Germany, 2002.

[39] L. Ly. Polly two – a new algebraic polynomial-based public-key scheme. AAECC, 17(3-4), 2006.

[40] A. L´opez-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, pp. 1219–1234. ACM (2012)

[41] J. Loftus, A. May, N.P. Smart, and F. Vercauteren. On CCA-Secure Fully Homomorphic Encryption. In SAC 2011, LNCS 7118, pp.55-72, 2012.

[42] D. Naccache. Is theoretical cryptography any good in practice? Invited talk at Crypto/CHES 2010 (2010), http://www.iacr.org/workshops/ches/ches2010

[43] M. Prabhakaran and M. Rosulek. Homomorphic Encryption with CCA Security. ICALP '08.

[44] C. Peikert, V. Vaikuntanathan, and B. Waters. A Framework for Efficient and Composable Oblivious Transfer.In CRYPTO 2008, LNCS 5157, pp.554-571,2008.

[45] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On Data Banks and Privacy Homomorphism. Foundations of Secure Computation, 1978, PP: 452–473.

[46] A. Sahai and B. Waters. Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

[47] T. Sander, A. Young, and M. Yung. Non-interactive cryptocomputing for NC1. FOCS '99, pp. 554–567, 1999.

[48] P. Scholl and N.P. Smart. Improved Key Generation For Gentry's Fully Homomorphic Encryption Scheme. http://eprint.iacr.org/2011/471.

[49] A. Shamir. Identity-based cryptosystems and signature schemes.In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

[50] N. P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In PKC 2010, 420-443.

[51] N. P. Smart and F. Vercauteren. Fully homomorphic SIMD operations. Manuscript at http://eprint.iacr.org/2011/133, 2011.

[52] D. Stehl´e and R. Steinfeld. Faster Fully Homomorphic Encryption. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 377–394. Springer, Heidelberg (2010)

[53] V. Vaikuntanathan. How to Compute on Encrypted Data. In INDOCRYPT 2012, LNCS, 7668,pp.1-15,2012.