A Note on *P/poly* Validity of GVW15 Predicate Encryption Scheme*

Yupu Hu[1], Siyue Dong[1], Baocang Wang[1], and Jun Liu[1]

State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
yphu@mail.xidian.edu.cn; 359442088@qq.com; bcwang@xidian.edu.cn; jliu6@stu.xidian.edu.cn

Abstract. Predicate encryption (PE) is a cutting-edge research topic in cryptography, and an essential component of a research route: identity-based encryption (IBE)→attribute-based encryption (ABE)→predicate encryption (PE)→functional encryption (FE). GVW15 predicate encryption scheme is a major predicate encryption scheme. The bottom structure is BGG+14 attribute-based encryption scheme, which is combined with a fully homomorphic encryption (FHE) scheme. A crucial operation of the scheme is modulus reduction, by which the modulus Q of the fully homomorphic encryption ciphertext (also referred to as the inner modulus) is scaled down to the modulus q of the attribute ciphertext (also referred to as the outer modulus). 'Therefore', the noise in the fully homomorphic encryption ciphertext (also referred to as the inner noise) is reduced to polynomial size, allowing for the follow-up exhaustion of noise size and hence correct decryption.

We argue in this paper that there is no evidence to support the $P/poly$ validity of GVW15 predicate encryption scheme, that is, when addressing $P/poly$ functions, there is no evidence to show GVW15 scheme can be implemented. In specific, when addressing $P/poly$ functions, there is no indication that the modulus reduction in GVW15 predicate encryption scheme can scale the noise in the fully homomorphic encryption ciphertext (the inner noise) down to polynomial size. Our argument is separated into two parts.

First, under a compact inner modulus Q, an intuition is that modulus reduction should reduce the inner noise to about the same size as the outer noise (i.e. the noise in the attribute ciphertext), which is super-polynomial in size. Breaking this intuition requires a special proof which GVW15 predicate encryption (PE) scheme does not provide.

Second, under an enlarged inner modulus Q, the outer modulus is enlarged correspondingly. As a result, the static target of modulus reduction is lost. Even so, the size of inner noise can still be reduced to polynomial size by using proper modulus reduction, as long as it can be proved that the ratio of increments of outer modulus and inner modulus is smaller than the ratio of original outer modulus q and original inner modulus Q. However, GVW15

* Supported by National Natural Science Foundations of China (61972457, U19B2021); Key Research and Development Program of Shaanxi (2020ZDLGY08-04); Innovation Scientists and Technicians Troop Construction Projects of Henan Province.

PE scheme failed to provide such proof. Moreover, it appears hopeless to get such proof, based on our observations.

Keywords: learning with errors · attribute-based encryption · functional encryption.

1 Introduction

There is a famous route in cryptography research: identity-based encryption (IBE) [1–5] → attribute-based encryption (ABE) [6–10] → predicate encryption (PE) [12–14] → functional encryption (FE) [15–26]. Predicate encryption (PE) is an essential component of this route. PE is a level higher than attribute-based encryption (ABE), because it is 'attribute-based encryption with attribute hidden'. PE is a level lower than functional encryption (FE), because the latter is more focused on 'the security against collusion attack'. The predicate encryption (PE) scenario is as followed: an encryptor transforms a plaintext into a ciphertext that embedded with an attribute x; the ciphertext is received by a decryptor who has the decryption key corresponding to function f without knowing attribute x; only when $f(x) = 1$ the decryptor can transform the ciphertext back into plaintext, otherwise the decryptor can only transform the ciphertext into gibberish.

GVW15 predicate encryption scheme [12] is a major predicate encryption scheme. The bottom structure is BGG+14 attribute-based encryption scheme [6], which is combined with a fully homomorphic encryption (FHE) [27–29] scheme. A crucial operation of the scheme is modulus reduction, by which the modulus Q of the fully homomorphic encryption ciphertext (also referred to as the inner modulus) is scaled down to the modulus q of the attribute ciphertext (also referred to as the outer modulus). 'Therefore', the noise in the fully homomorphic encryption ciphertext (also referred to as the inner noise) is reduced to polynomial size. The modulus reduction's success is very important. Only when the noise in the FHE ciphertext (inner noise) is reduced to polynomial size can the noise size be exhausted subsequently. Furthermore, the inner modulus Q can only be reduced to the outer modulus q, rather than another small modulus p. This is clear from the description of GVW15 predicate

encryption scheme and the $P/poly$ invalidity of the Agr17 functional encryption scheme [15, 30].

We argue in this paper that there is no evidence to support the $P/poly$ validity of GVW15 predicate encryption scheme, that is, when addressing $P/poly$ functions, there is no evidence to show GVW15 scheme can be implemented. In specific, when addressing $P/poly$ functions, there is no indication that the modulus reduction in GVW15 predicate encryption scheme can scale the noise in the FHE ciphertext (the inner noise) down to polynomial size. Our argument is separated into two parts.

First, with a compact inner modulus Q, ratios of noise sizes and moduli are approximately equal: $E/Q \approx e/q$, where E and e are the size of the noise in FHE ciphertext (inner noise) and the noise in the attribute ciphertext (outer noise), respectively. One of them appears to be a polynomial multiple of the other even without this equation. As a result, an intuition is that modulus reduction should reduce the inner modulus Q to the outer modulus q while the inner noise size E is scaled down to nearly the same size as the outer noise size e. On the other hand, the corresponding outer noise size of the $P/poly$ function is super-polynomial from the explanation in [30]. In conclusion, the inner noise size after modulus reduction is super-polynomial rather than polynomial. Breaking this intuition requires a special proof which GVW15 predicate encryption (PE) scheme does not provide.

Second, we acknowledge the intuition in the first part, i.e. we have $E/Q \approx e/q$ with a compact inner modulus Q. Then we consider a non-compact inner modulus Q, i.e. we enlarge the inner modulus while keeping the inner noise unchanged. Such non-compact structure is surely practical, because it is supported by existing schemes of fully homomorphic encryption. The question is , with an enlarged inner modulus Q, the outer modulus q is enlarged correspondingly. As a result, the static target of modulus reduction is lost. Even so, the size of inner noise can still be reduced to polynomial size by using proper modulus reduction, as long as it can be proved that the ratio of increments of outer modulus and inner modulus is smaller than the ratio of original outer modulus q and original inner modulus Q: $\Delta q/\Delta Q < q/Q$. However, GVW15 predicate encryption scheme failed to provide such proof.

Moreover, it appears hopeless to get such proof, based on our observations. Our observations will be shown in detail in this paper.

2 Bottom Structure of GVW15 PE Scheme: BGG+14 ABE Scheme

2.1 Notations and Operations

Let (m, n, q) denote three positive integers such that $q = n^{\Theta(d_{max})}$ where q is prime, $m = n\lceil \log_2 q \rceil$, and d_{max} has been well explained. Let $\mathbb{Z}$ denote the set of integers. For two positive integers (m', m''), $(\mathbb{Z}^{m'}, \mathbb{Z}^{m' \times m''}, \mathbb{Z}_q^{m'}, \mathbb{Z}_q^{m' \times m''})$ have been well defined. Note that the output of the operation 'mod$q$' is within $\{\lceil -\frac{q}{2} \rceil, \lceil -\frac{q}{2} \rceil + 1, \ldots, \lceil \frac{q}{2} \rceil\}$, rather than $\{0, 1, \ldots, q-1\}$. For $a \in \mathbb{Z}_q$, the meanings of $\mathbf{A} \in \mathbb{Z}_q^{m' \times m''}$ and $a\mathbf{A} \in \mathbb{Z}_q^{m' \times m''}$ are clear. Let $\mathbf{G}$ denote the following special matrix

$$\mathbf{G} = \begin{pmatrix} 1\, 2 \cdots 2^{\lceil \log_2 q \rceil - 1} & & & \\ & 1\, 2 \cdots 2^{\lceil \log_2 q \rceil - 1} & & \\ & & \ddots & \\ & & & 1\, 2 \cdots 2^{\lceil \log_2 q \rceil - 1} \end{pmatrix} \in \mathbb{Z}_q^{n \times m}.$$

For any $\alpha \in \mathbb{Z}_q$, there is a unique Boolean matrix $\mathbf{G}^{(\alpha)} \in \mathbb{Z}^{m \times m}$ such that

$$\alpha \mathbf{G} = \mathbf{G}\mathbf{G}^{(\alpha)} (\mathrm{mod} q).$$

For any $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, there is a unique Boolean matrix $\mathbf{G}^{(\mathbf{B})} \in \mathbb{Z}^{m \times m}$ such that

$$\mathbf{B} = \mathbf{G}\mathbf{G}^{(\mathbf{B})} (\mathrm{mod} q).$$

Then, the following three algorithms are well known.

- $\mathsf{TrapGen}(n, m, q)$: Input (n, m, q) and output $(\mathbf{A}, \mathbf{T})$, where $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is a uniform matrix, $\mathbf{T} \in \mathbb{Z}^{m \times m}$ is a small Gaussian matrix, $\mathbf{A}\mathbf{T} = \mathbf{0} \in \mathbb{Z}_q^{n \times m}$, and $\mathbf{T}$ is of full rank. $\mathbf{T}$ is not of full rank regarding the modulus q. $\mathbf{T}$ is called a trapdoor of $\mathbf{A}$.

– $\mathsf{Encode}(\mathbf{A}, \mathbf{s})$: Input $(\mathbf{A}, \mathbf{s}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$ and output $\boldsymbol{\psi} = \mathbf{A}^T\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m$, where $\mathbf{e} \in \mathbb{Z}^m$ is a small Gaussian vector. $\mathbf{s}$ is the encoded vector, $\boldsymbol{\psi}$ is the encoding of $\mathbf{s}$, and $\mathbf{e}$ is the error vector. We say $\boldsymbol{\psi} = \mathsf{Encode}(\mathbf{A}, \mathbf{s})$.
– $\mathsf{ReKeyGen}(\mathbf{A}, \mathbf{B}, \mathbf{T}, \mathbf{D})$: Input $(\mathbf{A}, \mathbf{B}, \mathbf{T}, \mathbf{D})$ and output $\mathbf{R}$, where $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_q^{n\times m}$ are uniform matrices, $\mathbf{T} \in \mathbb{Z}^{m\times m}$ is a trapdoor of $\mathbf{A}$, $\mathbf{R} \in \mathbb{Z}^{2m\times m}$ is a small Gaussian matrix, and $\mathbf{D} = [\mathbf{A}, \mathbf{B}]\mathbf{R} \in \mathbb{Z}_q^{n\times m}$. In fact,

$$\mathbf{R} = \begin{bmatrix} \mathbf{R}_0 \\ \mathbf{R}_1 \end{bmatrix}, \mathbf{R}_i \in \mathbb{Z}^{m\times m}, i = 0, 1,$$

then $\mathbf{R}_1$ is the pre-sampled matrix, and $\mathbf{R}_0$ is the co-sampled matrix. The trapdoor matrix $\mathbf{T}$ satisfies that $\mathbf{A}\mathbf{R}_0 = \mathbf{D} - \mathbf{B}\mathbf{R}_1$.

2.2 Arithmetic Representation and Big Modulus Representation of Boolean Functions

In order to make BGG+14 ABE scheme available, Boolean functions need to be expressed as mod$q$ functions, i.e., big modulus functions. This can be easily achieved by firstly transforming each Boolean operation into an arithmetic operation and then transforming the arithmetic operation into a big modulus operation. For example, for two bit variables x_1 and x_2,

$$x_1 \cdot x_2 (\mathrm{mod} 2) = x_1 \cdot x_2 = x_1 \cdot x_2 (\mathrm{mod} q),$$

$$x_1 + x_2 (\mathrm{mod} 2) = x_1 + x_2 - 2x_1 \cdot x_2 = x_1 + x_2 - 2x_1 \cdot x_2 (\mathrm{mod} q).$$

Then, by generalizing these transformations, each operation of a Boolean function can be converted into an operation under a big modulus. Therefore, Boolean functions are described as mod$q$ functions, except that the variables are in $\mathbb{F}_2$ rather than $\mathbb{Z}_q$.

2.3 Quasi-homomorphic Operations of BGG+14 ABE Scheme

Let $\boldsymbol{x} = (x_1, x_2, \cdots, x_l)$ denote an l-dimensional attribute, where each x_i is a bit variable. Take l matrices $\mathbf{B}_1, \mathbf{B}_2, \cdots, \mathbf{B}_l \in \mathbb{Z}_q^{n\times m}$. Take another l matrices $x_1\mathbf{G} +$

$\mathbf{B}_1, x_2\mathbf{G}+\mathbf{B}_2, \cdots, x_l\mathbf{G}+\mathbf{B}_l \in \mathbb{Z}_q^{n\times m}$. For any *P/poly* Boolean function $f(x)$, there are some 'small-size linear combination operations' for the above matrices, resulting in a new matrix

$$f(x)\cdot\mathbf{G}+\mathbf{B}_f \in \mathbb{Z}_q^{n\times m},$$

where $\mathbf{B}_f$ is independent of x. Recalling Sect. 2.2, any Boolean operation can be viewed as operations in $\mathbb{Z}_q$, and any Boolean function can be viewed as a function in $\mathbb{Z}_q$. Furthermore, for this special function in $\mathbb{Z}_q$, the result of each operation belongs to $[-2, 2]$. We consider the following four simple cases.

Case I. If $f(x)=\alpha x_i$ where α is a constant, then the 'small-size linear combination operation' is

$$(x_i\mathbf{G}+\mathbf{B}_i)\mathbf{G}^{(\alpha)} = \alpha x_i\mathbf{G}+\mathbf{B}_i\mathbf{G}^{(\alpha)}(\mathrm{mod}q),$$

where $\mathbf{B}_f=\mathbf{B}_i\mathbf{G}^{(\alpha)}$.

Case II. If $f(x)=x_i+x_j$, then the 'small-size linear combination operation' is

$$(x_i\mathbf{G}+\mathbf{B}_i)+(x_j\mathbf{G}+\mathbf{B}_j)(\mathrm{mod}q) = (x_i+x_j)\mathbf{G}+(\mathbf{B}_i+\mathbf{B}_j)(\mathrm{mod}q),$$

where $\mathbf{B}_f=\mathbf{B}_i+\mathbf{B}_j$.

Case III. If $f(x)=x_i\cdot x_j$ where $i\le j$, then the 'small-size linear combination operation' is

$$x_j(x_i\mathbf{G}+\mathbf{B}_i)-(x_j\mathbf{G}+\mathbf{B}_j)\mathbf{G}^{(\mathbf{B}_i)} = x_ix_j\mathbf{G}+(-\mathbf{B}_j\mathbf{G}^{(\mathbf{B}_i)})(\mathrm{mod}q),$$

where $\mathbf{B}_f=-\mathbf{B}_j\mathbf{G}^{(\mathbf{B}_i)}$.

Case IV. If $f(x)=\alpha\cdot x_{j_1}\cdot x_{j_2}\cdot\cdots\cdot x_{j_k}, j_1\le j_2\le\cdots j_k$ and α is a constant, then the 'small-size linear combination operation' is

$$\sum_{i=1}^{k}\left(\prod_{h=i+1}^{k}x_{j_h}\right)\cdot(x_{j_i}\mathbf{G}+\mathbf{B}_{j_i})\cdot\mathbf{G}_i = \alpha\cdot x_{j_1}\cdot x_{j_2}\cdot\cdots\cdot x_{j_k}\cdot\mathbf{G}+(-\mathbf{B}_{j_k}\mathbf{G}_k),$$

where $\mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_k$ are Boolean matrices in $\mathbb{Z}^{m\times m}$ and are defined recursively as below:

$$\mathbf{G}_1=\mathbf{G}^{\alpha},$$

$$\mathbf{G}_i=\mathbf{G}^{(-\mathbf{B}_{j_{i-1}}\mathbf{G}_{i-1})}, i=2,3,\cdots,k,$$

where $\mathbf{B}_f = -\mathbf{B}_{j_k} \cdot \mathbf{G}$ is also independent of x.

Finally, we affirm that iterations of 'small-size linear combination operations' are still 'small-size linear combination operations', provided the time of iterations is at the polynomial level. Thus, we draw the conlusion by repeating the aforementioned four operations: any $P/poly$ Boolean function f can execute 'small-size linear combination operations' on the above matrices, resulting in $f(x)\mathbf{G} + \mathbf{B}_f$.

Next, we do the following encoding:

$$\mathbf{c}_1 = \mathsf{Encode}(x_1\mathbf{G} + \mathbf{B}_1, \mathbf{s}),$$

$$\mathbf{c}_2 = \mathsf{Encode}(x_2\mathbf{G} + \mathbf{B}_2, \mathbf{s}),$$

$$\cdots,$$

$$\mathbf{c}_l = \mathsf{Encode}(x_l\mathbf{G} + \mathbf{B}_l, \mathbf{s}).$$

By executing the same 'small-size linear combination operation' (only plus a transpose) on the codeword $(\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_l)$, we will obtain

$$\mathbf{c}_f = \mathsf{Encode}(f(x)\mathbf{G} + \mathbf{B}_f, \mathbf{s}).$$

We call such 'small-size linear combination operations' on $(\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_l)$ as quasi-homomorphic operations about the Boolean function f. Here, we need to emphasize two design techniques of BGG+14 scheme: (i) Case III indicates that when executing the quasi-homomorphic operations of multiplication, the accumulation form of errors is approximately the multiplication of an original error by a binary matrix, rather than the multiplication of two original errors. This decelerates the accumulation of errors to a large extent. (ii) Case III is a particular case of Case IV, whereas Case IV is not repeated operations of Case III. This design technique makes that when executing the quasi-homomorphic operations of continuous multiplication, the accumulation of errors by applying Case IV once is much smaller than by applying Case III multiple times.

When multiplying an original error by a random binary matrix, the size of the resulting error is about $\sqrt{\frac{m}{2}}$ times the size of the original error. Hence, when executing the quasi-homomorphic operations of multiplication, the size of the resulting

error is at least about $\sqrt{\frac{m}{2}}$ times the size of one original error, and this statement also holds when executing the quasi-homomorphic operations of continuous multiplication, i.e., Case IV. Continuous multiplications are uncommon for a $P/poly$ function, and even two adjacent operations are both multiplications in a $P/poly$ function, they do not necessarily can be merged into a continuous multiplication. In other words, quasi-homomorphic operations of continuous multiplication, i.e., Case IV, have a limited inhibitory effect on the accumulation of errors. To sum up, it is possible for BGG+14 scheme that when executing the quasi-homomorphic operations for $P/poly$ functions, the size of the final error reaches superpolynomial. Therefore, the modulus q of BGG+14 scheme has to be superpolynomially large for processing $P/poly$ functions.

2.4 BGG+14 ABE Scheme[6]

- Generating master key $(\mathbf{mpk}, \mathbf{msk})$: The key generator runs $\mathsf{TrapGen}(n, m, q)$ to obtain $(\mathbf{A}, \mathbf{T})$, then he randomly picks $\mathbf{B}_i \in \mathbf{Z}_q^{n\times m}, i = 1, 2, \cdots, l, \mathbf{D} \in \mathbf{Z}_q^{n\times m}$. The output is

$$\mathbf{mpk} = (\mathbf{A}, \mathbf{B}_1, \cdots, \mathbf{B}_l, \mathbf{D}), \mathbf{msk} = \mathbf{T}.$$

- Generating secret key $\mathbf{sk}_f$ for the Boolean function f: The key generator firstly generates $\mathbf{B}_f$. Note that $\mathbf{B}_f$ is generated by the method in Sect. 2.3. The attribute is randomly chosen, and the resulting $\mathbf{B}_f$ is independent of this attribute. Then, he runs $\mathsf{ReKeyGen}(\mathbf{A}, y_0\mathbf{G} + \mathbf{B}_f, \mathbf{T}, \mathbf{D})$ to obtain $\mathbf{R} \in \mathbb{Z}^{2m\times m}$. The output is

$$\mathbf{sk}_f = \mathbf{R}.$$

- Encryption: The plaintext $\mathbf{m}$ is an m-dimensional Boolean vector. The attribute $\boldsymbol{x} = (x_1, x_2, \cdots,$
  $x_l)$ is sent to the encryptor. The encryptor randomly picks $\mathbf{s} \in \mathbb{Z}_q^n$, and computes $(\mathsf{Encode}(\mathbf{A}, \mathbf{s}),\ \mathsf{Encode}(x_1\mathbf{G} + \mathbf{B}_1, \mathbf{s}),\ \mathsf{Encode}(x_2\mathbf{G} + \mathbf{B}_2, \mathbf{s}), \cdots,\ \mathsf{Encode}(x_l\mathbf{G} +$

$\mathbf{B}_l, \mathbf{s})$, $\mathsf{Encode}(\mathbf{D}, \mathbf{s}))$. The ciphertext is

$$\begin{aligned}\mathbf{C} &= (\mathbf{c}_{in}, \mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_l, \mathbf{c}_{out}) \\ &= (\mathsf{Encode}(\mathbf{A}, \mathbf{s}), \mathsf{Encode}(x_1\mathbf{G} + \mathbf{B}_1, \mathbf{s}), \cdots, \mathsf{Encode}(x_l\mathbf{G} + \mathbf{B}_l, \mathbf{s}), \mathsf{Encode}(\mathbf{D}, \mathbf{s}) + \lceil \frac{q}{2} \rceil \mathbf{m}) \\ &= (\mathbf{A}^T\mathbf{s} + \mathbf{e}_{in}, (x_1\mathbf{G} + \mathbf{B}_1)^T\mathbf{s} + \mathbf{e}_1, \cdots, (x_l\mathbf{G} + \mathbf{B}_l)^T\mathbf{s} + \mathbf{e}_l, \mathbf{D}^T\mathbf{s} + \mathbf{e}_{out} + \lceil \frac{q}{2} \rceil \mathbf{m}).\end{aligned}$$

- Decryption: By using his own f and the attribute $\boldsymbol{x} = (x_1, x_2, \cdots, x_l)$, the decryptor executes the quasi-homomorphic operation to obtain

$$\begin{aligned}\mathbf{c}_f &= \mathsf{Encode}(f(\boldsymbol{x})\mathbf{G} + \mathbf{B}_f, \mathbf{s}) \\ &= (f(\boldsymbol{x})\mathbf{G} + \mathbf{B}_f)^T\mathbf{s} + \mathbf{e}_f(\boldsymbol{x}).\end{aligned}$$

Then, by using $\mathbf{sk}_f = \mathbf{R}$, the decryptor computes

$$\begin{aligned}\mathbf{c}_{out} - \mathbf{R}^T \begin{pmatrix} \mathbf{c}_{in} \\ \mathbf{c}_f \end{pmatrix} &= \mathbf{D}^T\mathbf{s} - \mathbf{D}^T\mathbf{s} + \lceil \frac{q}{2} \rceil \mathbf{m} + ((y_0 - f(\boldsymbol{x}))\mathbf{G})^T \mathbf{s} + \mathbf{e}' \\ &= \lceil \frac{q}{2} \rceil \mathbf{m} + ((y_0 - f(\boldsymbol{x}))\mathbf{G})^T\mathbf{s} + \mathbf{e}'.\end{aligned}$$

When $f(\boldsymbol{x}) = y_0$, the plaintext $\mathbf{m}$ can be obtained by using "*Rounding*"; When $f(\boldsymbol{x}) \neq y_0$, gibberish is returned. Generally, $y_0 = 1$.

2.5 Hiding Attribute in BGG+14 ABE Scheme

The so-called 'hiding attribute' means that the encryptor only knows the attribute and the decryptor does not know it. The key issue is whether the decryptor can execute the quasi-homomorphic operation of f when he does not know some part of the attribute.

It can be easily seen that when f is a mod$q$ linear function, the decryptor can finish the quasi-homomorphic operation without knowing the attribute $\boldsymbol{x}$. However, from Sect. 2.2, any Boolean function is not a mod$q$ linear function. In other words, as a mod$q$ function, any Boolean function contains mod$q$ additions and mod q multiplications. When executing multiplications, i.e., the quasi-homomorphic operation of multiplications, one attribute bit can be secret, while another one has to be visible to the decryptor.

3 GVW15 PE Scheme

3.1 Overview of GVW15 PE Scheme[12]

Let $\mathbf{m}$ denote the plaintext, u denotes the attribute hidden from the decryptor, the encryption process can be divided into two steps: (1) u is encrypted to an FHE ciphertext u^* by the encryption algorithm of an FHE scheme. It is worth noting that now the modulus of the FHE ciphertext (the inner modulus) is Q; (2) u^* is taken as the public part of the attribute, and t, the secret key of the FHE scheme, is taken as the hidden part of the attribute. Then, for the attribute (u^*, t), $\mathbf{m}$ is encrypted to an 'ABE ciphertext' $\mathbf{C}$ by BGG+14 ABE scheme. Finally, the obtained 'ABE ciphertext' $\mathbf{C}$ is the ciphertext of GVW15 PE scheme. It is worth noting that now the modulus of the attribute ciphertext (the outer modulus) is q.

Now, the decryptor knows the following three items: (1) The ciphertext $\mathbf{C}$ of GVW15 PE scheme. In fact, this item is the 'ABE ciphertext' $\mathbf{C} = (\mathbf{c}_{in}, \mathbf{c}_1, \cdots, \mathbf{c}_l, \mathbf{c}_{out})$, where $(\mathbf{c}_1, \cdots, \mathbf{c}_l) = (\mathbf{C}_{u^*}, \mathbf{C}_t)$, $\mathbf{C}_{u^*}$ is the 'ABE ciphertext' of u^* (the public part of the attribute), and $\mathbf{C}_t$ is the 'ABE ciphertext' of t (the hidden part of the attribute); (2) The FHE ciphertext u^*. In fact, this item is exactly the public part of the attribute; (3) The secret key of GVW15 PE scheme, which is corresponding to the Boolean function f. In fact, this item is the secret key of BGG+14 scheme, which is corresponding to the composite function Df^*, where f^* is the homomorphic operation of f and D is the FHE decryption algorithm. In other words, there is $Df^*(u^*, t) = D(f^*(u^*), t) = f(u)$. The decryptor knows neither the hidden attribute u nor the secret key t of the FHE scheme.

The rough decryption process of the decryptor is as follows. He executes the 'predicate decryption' (i.e., 'attribute decryption') on the ciphertext $\mathbf{C}$ by using his secret key of GVW15 PE scheme, i.e., the secret key of BGG+14 scheme. If $f(u) = 1$, $\mathbf{m}$ is obtained, otherwise gibberish is obtained.

Note that the ciphertext $\mathbf{C}$ includes two parts $(\mathbf{C}_{u^*}, \mathbf{C}_t)$. Therefore, the detailed decryption process of the decryptor includes the following four steps.

First step, $\mathbf{C}_{u^*}$ is transformed into a new ciphertext $\mathbf{C}_{f^*(u^*)}$ by the homomorphic operation of f, where $\mathbf{C}_{f^*(u^*)}$ is the 'ABE ciphertext' of the new attribute $f^*(u^*)$.

In other words, this step is the 'quasi-homomorphic operation of the homomorphic operation of f' (cf. Sect. 2.3). We have two notes on the first step. Note (1), $u^* \to f^*(u^*)$ is mod$Q$ operation, while its quasi-homomorphic operation is mod$q$ operation, $Q \neq q$. Therefore, the operation mode will undergo three transformations: mod Q operation $\to$ Boolean operation $\to$ arithmetic operation of small value $\to$ mod$q$ operation. Note (2), the first two transformations of operation mode reduce the operation efficiency; the third transformation is a natural transformation, hence the operation efficiency remains unchanged.

Second step, modulus reduction. We transform $\mathbf{C}_{f^*(u^*)}$ into $\mathbf{C}_{f^{**}(u^*)}$, where $f^{**}(u^*)$ is the message obtained by the modulus reduction of $f^*(u^*)$. In other word, by using the modulus reduction in FHE, we transform a mod Q message $f^*(u^*)$ into a mod q message $f^{**}(u^*)$. We have three notes on the second step. Note (1), by modulus reduction, the inner modulus Q cannot be reduced to another small modulus p ($p \neq q$). Otherwise the subsequent operation cannot proceed[30]. Q can only be reduced to outer modulus q. Note (2), modulus reduction operation has to undergo a series of transformations, modulus reduction $\to$ Boolean operation $\to$ arithmetic operation of small value $\to$ mod q operation, before it can be used for quasi-homomorphic operation. Therefore, increasing computational complexity and decreasing efficiency are unavoidable. Note (3), it is claimed in GVW15 scheme that the modulus reduction can scale the noise in the fully homomorphic encryption ciphertext down to polynomial size.

Third step, with $\mathbf{C}_{f^{**}(u^*)}$ and $\mathbf{C}_t$ we perform the quasi-homomorphic operation of mod q inner product $\langle t, f^{**}(u^*)\rangle$ (mod q), obtaining a new ciphertext $\mathbf{C}_{\langle t, f^{**}(u^*)\rangle (\bmod q)}$. We have three notes on the second step. Note (1), although the decryptor do not know t, the third step is still realizable, because the inner modulus is equal to the outer modulus. Note (2), the noise in the FHE ciphertext $\langle t, f^{**}(u^*)\rangle$ (mod q) is still polynomial size, as long as the noise in $f^{**}(u^*)$ is polynomial size.

Final step, noise exhaustion. After the third step we have $\mathbf{C}_{\langle t, f^{**}(u^*)\rangle (\bmod q)}$, where $\langle t, f^{**}(u^*)\rangle$ (mod q) is an integer range from $[-B, B] \cup \left[-\frac{q}{2}, -\frac{q}{2} + B\right] \cup \left[\frac{q}{2} - B, \frac{q}{2}\right]$, B is a polynomial size value claimed in GVW15 scheme. For any integer w in the range,

the decryptor asks for BGG+14 ABE decryption key corresponding to function

$$f_w(u^*) = \begin{cases} 1 \ \langle t, f^{**}(u^*)\rangle \ (\bmod q) = w \\ 0 \ \langle t, f^{**}(u^*)\rangle \ (\bmod q) \neq w \end{cases}$$

and runs the test. By such exhaustion, the decryptor learns the exact value of $\langle t, f^{**}(u^*)\rangle \, (\mathrm{mod} q)$ and hence proper decryption.

3.2 Analysis of the Reasonability of Assuming '$Q > q$'

A precondition of modulus reduction operation is $Q > q$. It is not explained in GVW15 scheme why $Q > q$. Two possible reasons are based on the nature of FHE and BGG+14 ABE scheme.

(1) When performing multiplicative homomorphic operation in FHE, the noise size in the product is approximately the product of the noise sizes of two factors; when performing multiplicative quasi-homomorphic operation in BGG+14 ABE scheme, the noise size in the product is only about $\sqrt{\frac{m}{2}}$ times the noise size of one factor. Therefore, if a quasi-homomorphic operation of an FHE multiplicative homomorphic operation is only a multiply operation, the size of the inner noise accumulates faster than the size of the outer noise, hence we assume $Q > q$.

(2) When performing the k continued multiplicative quasi-homomorphic operation in BGG+14 ABE scheme, the accumulation of noise is more conservative. the noise size in the product is not $\left(\sqrt{\frac{m}{2}}\right)^{k-1}$ times the noise size of one factor, but only $(k-1)\sqrt{\frac{m}{2}}$ times of it. It is not as 'economical' as such when performing the k continued multiplicative homomorphic operation in FHE. As a result, if the quasi-homomorphic operation of the k continued multiplicative homomorphic operation in FHE is only a k continued multiplicative operation, the size of the inner noise accumulates much faster than the size of the outer noise, hence we assume $Q > q$.

The above two reasons are rough, because the loss brought by the transformations of operation mode 'mod$Q$ operation $\rightarrow$ Boolean operation $\rightarrow$ arithmetic operation of small value $\rightarrow$ mod$q$ operation' is completely ignored. Here we notice two facts.

(1) For multiplication operation in FHE evaluation, corresponding quasi-homomorphic operation of BGG+14 ABE scheme is not a multiplication, but rather a combination of several multiplications and additions. It is a complicated scenario.

(2) Even for addition operation in FHE evaluation, corresponding quasi-homomorphic operation of BGG+14 ABE scheme is still a combination of multiplications and additions.

In conclusion, the reasonability of the precondition '$Q > q$' is questionable, at the very least, a lengthy proof is necessary.

4 Analysis of *P/poly* Validity of GVW15 PE Scheme

Even if we assume '$Q > q$', there is no proof that supports the $P/poly$ validity of GVW15 PE scheme. In specific, when dealing with $P/poly$ functions, even if we assume '$Q > q$', there is still no evidence showing that the modulus reduction operation in GVW15 PE scheme can reduce the noise in FHE ciphertext (the inner noise) to polynomial size. Our intuition is that we should now consider the ratio of noise size and modulus size, rather than the modulus size. Our discussion is divided into two parts. First, we consider the scenario with a compact inner modulus Q; second, we consider the scenario with an enlarged inner modulus Q.

4.1 The Scenario with a compact inner modulus *Q*

The so-called compact inner modulus denotes the inner Q as the optimal compromise among FHE security, efficiency and decryption failure rate, without taking into account other parameter coordinations. Because the outer modulus q is almost certain to be compact, and because FHE and BGG+14 scheme share same or equivalent security (based on hard problems on lattice or LWE), they appear to have similar modulus to noise ratios: $E/Q \approx e/q$, where E and e are the size of the noise in FHE ciphertext (inner noise) and the noise in the attribute ciphertext (outer noise), respectively. One of them appears to be a polynomial multiple of the other even without this equation. As a result, an intuition is that modulus reduction should reduce the inner modulus Q to the outer modulus q while the inner noise size E is

scaled down to nearly the same size as the outer noise size e. On the other hand, the corresponding outer noise size of the $P/poly$ function is super-polynomial from the explanation in [30]. In conclusion, the inner noise size after modulus reduction is super-polynomial rather than polynomial. Breaking this intuition requires a special proof which GVW15 predicate encryption (PE) scheme does not provide.

4.2 The Scenario with an enlarged inner modulus Q

Now we acknowledge the intuition in the first part, i.e. we have $E/Q \approx e/q$ with a compact inner modulus Q. Then we consider a non-compact inner modulus Q, i.e. we enlarge the inner modulus while keeping the inner noise unchanged. Such non-compact structure is surely practical, because it is supported by existing schemes of fully homomorphic encryption. The question is, with an enlarged inner modulus Q, the outer modulus q is enlarged correspondingly. As a result, the static target of modulus reduction is lost. Even so, the size of inner noise can still be reduced to polynomial size by using proper modulus reduction, as long as it can be proved that the ratio of increments of outer modulus and inner modulus is smaller than the ratio of original outer modulus q and original inner modulus Q: $\Delta q/\Delta Q < q/Q$. In other words, we need to prove when the inner modulus Q increases by one bit (i.e. by two times), correspondingly the average increase of the outer q is smaller than q/Q bits (i.e. smaller than $2^{q/Q}$ times). However, GVW15 PE scheme did not provide such proof.

A further question is whether such proof exists? If it does, how complicated is the proof? Now we consider a weaker problem: when the inner modulus Q increases by one bit (i.e. by two times), is the average increase of the outer q less than one bit (i.e. less than 2 times bigger) correspondingly? We assume that an FHE ciphertext $f^*(u^*)$ with a compact inner modulus Q is obtained, and that another FHE ciphertext $f'^*(u'^*)$ is obtained when the inner modulus Q increases by about one bit. We assume an FHE ciphertext is a d dimension vector, then u'^* is about d bits larger than u^*. Considering the scenario when the independent variable is d bits larger, how many more Boolean operations does Boolean function $f'^*(u'^*)$ performs than

$f^*(u^*)$? Even if there is only one extra Boolean operation, the size of the outer noise is at least doubled (noting that the Boolean operation need to be transformed into arithmetic operation of small value, and there is arithmetic multiply operation in both arithmetic expressions of Boolean additive operation and Boolean multiply operation). That the size of the outer noise is at least doubled means the increase of the outer modulus q is at least one bit (i.e. two times bigger). In other words, this weaker problem is hard to prove.

In conclusion, it appears hopeless to get the proof of '$\Delta q/\Delta Q < q/Q$'.

References

1. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
2. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_32
3. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_17
4. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
5. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_27
6. Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G.,Vaikuntanathan, V., and Vinayagamurthy, D.: Fully key-homomorphic encryption, arithmetic circuit ABE, and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_30
7. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: CCS 2006. pp. 89–98. ACM (2006). https://doi.org/10.1145/1180405.1180418
8. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute based encryption for circuits. In: STOC 2013. pp. 545–554. ACM (2013). https://doi.org/ [DOI: 10.1145/2488608.2488677
9. Garg, S., Gentry, C., Halevi, S., Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 479–499. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_27

10. Agrawal, S., Maitra, M., Yamada, S.: Attribute based encryption (and more) for nondeterministic finite automata from LWE. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 765–797. Springer, Cham (2019) https://doi.org/10.1007/978-3-030-26951-7_26
11. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy 2007. pp. 321–334. IEEE (2007). https://doi.org/10.1109/SP.2007.11
12. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Predicate encryption for circuits from LWE. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 503–523. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_25
13. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_9
14. Datta, P., Okamoto, T., Takashima, K.: Adaptively simulation-secure attribute-hiding predicate encryption. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11273, pp. 640–672. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_22
15. Agrawal, S.: Stronger security for reusable garbled circuits, general definitions and attacks. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 3–35. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_1
16. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16
17. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. pp. 197–206. ACM (2008) https://doi.org/10.1145/1374376.1374407
18. Agrawal, S., Rosen, A.: Functional encryption for bounded collusions, revisited. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10677, pp. 173–205. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70500-2_7
19. Agrawal, S., Libert, B., Maitra, M., Titiu, R.: Adaptive simulation security for inner product functional encryption. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020. LNCS, vol. 12110, pp. 34–64. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45374-9_2
20. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_4
21. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product predicates from learning with errors. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 21–40. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_2
22. Waters, B.: Functional encryption for regular languages. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 218–235. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_14

23. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS 2013. pp. 40–49. IEEE (2013). https://doi.org/10.1109/FOCS.2013.13
24. Lai, Q., Liu, FH., Wang, Z.: New lattice two-stage sampling technique and its applications to functional encryption – stronger security and smaller ciphertexts. In: Canteaut, A., Standaert, FX. (eds.) EUROCRYPT 2021. LNCS, vol. 12696, pp. 498–527. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77870-5_18
25. Wang, Z., Fan X., Liu FH.: FE for inner products and its application to decentralized ABE. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11443, pp. 97–127. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17259-6_4
26. Ananth, P., Vaikuntanathan, V.: Optimal bounded-collusion secure functional encryption. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019. LNCS, vol. 11891, pp. 174–198. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36030-6_8
27. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: ITCS 2012. pp. 309–325. ACM (2012). https://doi.org/10.1145/2090236.2090262
28. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_5
29. Brakerski, Z., Vaikuntanathan, V.: Lattice-based FHE as secure as PKE. In: ITCS 2014. pp. 1–12. ACM (2014). https://doi.org/10.1145/2554797.2554799
30. Hu, Y.P., Liu J., Wang, B.C., and Pan, Y.B.: $P/poly$ Invalidity of the Agr17 Functional Encryption Scheme. In: IACR Cryptol. ePrint Arch. 2021: 1442 (2021)