Candidate Constructions of Fully Homomorphic Encryption on Finite Simple Groups without Ciphertext Noise

Koji Nuida[1][2]

[1] National Institute of Advanced Industrial Science and Technology (AIST), Japan
k.nuida@aist.go.jp
[2] Japan Science and Technology Agency (JST) PRESTO Researcher, Japan

November 3, 2015

Abstract

We propose constructions of fully homomorphic encryption completely different from the previous work, using special kinds of *non-commutative* finite groups. Unlike the existing schemes, our ciphertexts involve no "noise" terms, hence the inefficient "bootstrapping" procedures are not necessary. Our first scheme is based on improved results on embeddings of logic gates into (almost) simple groups [Ostrovsky and Skeith III, CRYPTO 2008]. Our second scheme is based on properties of the commutator operator (analogous to those used in Barrington's theorem) and a new idea of input rerandomization for commutators, effective for some (almost) simple matrix groups. Our main idea is to conceal the concrete structures of the underlying groups by randomly applying some special transformations famous in combinatorial group theory, called *Tietze transformations*, to a kind of symbolic representations of the groups. Ideally, the resulting group is expected to behave like a black-box group where only an abstract group structure is available; a detailed analysis of the true effect of random Tietze transformations on the security is a future research topic. We emphasize that such a use of Tietze transformations in cryptology has no similar attempts in the literature and would have rich potential for further applications to other areas in cryptology.

1 Introduction

Until the pioneering work by Gentry [14] in 2009, it had been a long-standing open problem to construct *fully homomorphic encryption* (*FHE*) that enables arbitrary "computation on encrypted data" through special kinds of operations on the ciphertexts called *homomorphic operations*. After that, studies of FHE to improve the efficiency (e.g., [12, 15, 17, 20, 31]) and to give various frameworks of construction (e.g., [3, 4, 5, 6, 7, 8, 9, 10, 16, 26]) have been one of the main research topics in cryptology (see [30] for a survey). However, all the previous FHE schemes (with compact ciphertexts) rely on Gentry's "bootstrapping" framework: Ciphertexts involve "noise" terms to conceal plaintexts but the noise is increased by homomorphic operations and will finally collapse the ciphertext, hence it must be cancelled before the collapse. This additional cancellation procedure is a major bottleneck for efficiency improvement and makes the syntax of FHE less analogical to the classical homomorphic encryption. Therefore, a new approach to construct FHE schemes without the bootstrapping framework is really valuable.

1.1 Our Contributions and Related Work

In this paper, we propose a completely different approach to construction of FHE by following the direction of so-called "group-based cryptography" (see e.g., [2] for a survey), where special kinds of *non-commutative groups* are used as the underlying mathematical structure. For example, a variation of our proposed FHE schemes utilizes some properties of *commutators* $[g, h] = ghg^{-1}h^{-1}$ for group elements (that were also used in Barrington's theorem [1]); here the non-commutativity of groups is indispensable, since the commutator operator becomes useless in commutative groups as it just outputs the identity element constantly. In our proposed FHE schemes, the ciphertexts involve no "noise" terms that were necessary for security in the previous FHE schemes, hence the "bootstrapping" procedures are not required.

Our new idea for achieving security without ciphertext noise is based on *Tietze transformations*, which is a notion famous in combinatorial group theory (see e.g., [21]). Roughly speaking, a *presentation* of group by generators and relators yields a definition of a group via a (one-to-many) correspondence between the group elements and words of finite lengths over a specified alphabet (generating set), where multiplication of group elements corresponds to concatenation of words and the *relators* determine when given two words define the same group element. Tietze transformations are a class of elementary transformations for group presentations that do not change the corresponding group (up to isomorphism). In our proposed schemes, the underlying group is specified by a group presentation, and to achieve security, its concrete structure (except the abstract group structure) is concealed or "obfuscated" by applying Tietze transformations randomly and successively. See Section 5 for the details. Here we emphasize that, such a use of Tietze transformations in cryptology has no similar attempts in the literature; this paper would open a door to develop a new general methodology based on combinatorial group theory that seems potentially applicable to wide areas in cryptology. We also note that, Tietze transformations are usually used in order to *simplify* a given group presentation. In contrast, these are used in this paper to make a group presentation more *complicated*, which seems also very rare in the literature.

Our proposed FHE schemes mainly have two variations, one with deterministic homomorphic operators (Section 3) and the other with probabilistic homomorphic operators (Section 4). For the deterministic case, recall that Ostrovsky and Skeith III [27, 28] showed the existence of embeddings of logic gates into non-commutative finite simple groups, especially into the alternating group A_5 on five letters where a concrete embedding is given in [27], and mentioned that an FHE scheme will be obtained if elements of A_5 can be homomorphically encrypted. Our construction follows this direction, where embeddings of logic gates are improved in terms of efficiency and the size of plaintext spaces (from 1-bit space to the three-element finite field).

On the other hand, for the probabilistic case, we utilize the following property of the commutator operator: We have $[x, y] = 1$ if $x = 1$ or $y = 1$, which is partially analogous to AND gate as we have $b \wedge b' = 0$ if $b = 0$ or $b' = 0$ (cf., Barrington's theorem [1]). However, these are not fully analogous, since $[x, y] \neq 1$ does not hold in general even when $x \neq 1$ and $y \neq 1$. To make it fully analogous, we introduce an idea of input rerandomization that results in the element $[gxg^{-1}, y]$ with uniformly random element g of the group. This idea is indeed effective (i.e., we have $[gxg^{-1}, y] \neq 1$ for a random g with probability close to 1 when $x \neq 1$ and $y \neq 1$) for a kind of matrix groups called projective special linear groups (of dimension two).

Then, as mentioned before, the presentations of the underlying groups for the two schemes above are "obfuscated" by random Tietze transformations. Ideally, the resulting group is expected to behave like a black-box group where only an abstract group structure is available; a detailed analysis of the true effect of random Tietze transformations on the security is a future research topic. We also note that, it is in fact not trivial to efficiently compute group operations from a given group presentation; more precisely, to efficiently derive normal forms for group elements and their multiplication rule. See Section 6. An algorithm called *Knuth–Bendix completion* (see e.g., [22, 23, 25]) can be used to derive such a system of normal forms, but it is not guaranteed in general to find the solution efficiently with high probability. Hence, it is an important future research topic to improve the algorithm in such a way that the algorithm will work efficiently for inputs relevant to our proposed schemes.

Finally, we observe that the proposed constructions of FHE schemes based on random Tietze transformations look somewhat "artificial"; more "natural" constructions of the underlying groups (analogous to the use of rational point groups of elliptic curves for instantiating abstract cyclic groups appeared in ElGamal cryptosystem) would be more desirable from the viewpoints of mathematical beauty as well as improvements of efficiency. Here we note, however, that such a natural instantiation of our schemes seems not easy to find. For example, a naive instantiation of our scheme may realize the ciphertext space as a group consisting of matrices. Then the ciphertext space is easily embedded into a matrix *ring*. Now the matrix ring forms a vector space (or module) over the coefficient ring, and it happens frequently that the two sets of ciphertexts for plaintext 0 and for plaintext 1 span subspaces (or submodules) of different dimensions; the difference of dimensions helps an adversary to break the scheme[1]. We note that, for the case of our proposed schemes, it seems hard to find an embedding of the underlying group into matrix group from the "obfuscated" group presentation. To find a "natural" instantiation of our schemes that avoids the powerful attack strategy explained above is an interesting future research topic.

2 Preliminaries

In this section, we summarize some basic definitions and notations used throughout the paper. Unless otherwise specified, any group G is finite, is not necessarily commutative, and is written in multiplicative form with identity element denoted by 1_G (or simply 1, if unambiguous from the context). The reader may refer to a textbook of group theory (e.g., [29]) for other definitions and basic facts for groups. Let S_n denote the symmetric group on n letters, i.e., the group of permutations $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ with multiplication defined by the composition of maps. Let A_n denote the alternating group on n letter, i.e., the subgroup of S_n of permutations that can be written as the product of an even number of transpositions (a, b), $a \neq b$. For any group G, we say that a subgroup N of G is *normal*, if we have $gxg^{-1} \in N$ for any $x \in N$ and $g \in G$. We say that a group G is *simple*, if G does not have normal subgroups other than G itself and $\{1_G\}$. For example, A_n is a normal subgroup of S_n for any n, and A_n is simple if $n \geq 5$. For a subset X of a group G, let $\langle X \rangle$ denote the subgroup of G generated by X. The normal subgroup generated by X or the *normal closure* of X, denoted by $\langle X \rangle_{\mathrm{normal}}$, is defined to be the subgroup generated by $\{gxg^{-1} \mid x \in X \,,\, g \in G\}$. We note that, if G is simple and $x \in G \setminus \{1_G\}$, then (since $\langle x \rangle_{\mathrm{normal}} \neq \{1_G\}$) we have $\langle x \rangle_{\mathrm{normal}} = G$.

For a probability distribution (or a random variable) $\mathcal{X}$, let $a \leftarrow \mathcal{X}$ mean that an element a is chosen according to $\mathcal{X}$. We write $a \leftarrow X$ instead of $a \leftarrow \mathcal{U}[X]$, where $\mathcal{U}[X]$ denotes the uniform distribution over a finite set X. We also write $a \leftarrow \mathcal{A}(x)$ for any algorithm $\mathcal{A}$ to indicate that a is chosen according to the output distribution of $\mathcal{A}$ with input x. Let $\Pr_{a \leftarrow X}[\cdots]$ denotes the probability of the event specified in the square bracket, taken over uniformly random element $a \in X$. The *statistical distance* between two probability distributions $\mathcal{X}, \mathcal{Y}$ over a finite set Z is defined by $\Delta(\mathcal{X}, \mathcal{Y}) = (1/2) \cdot \sum_{z \in Z} |\Pr[z \leftarrow \mathcal{X}] - \Pr[z \leftarrow \mathcal{Y}]|$. For $\varepsilon \geq 0$, we say that $\mathcal{X}$ is *ε-close* to $\mathcal{Y}$, if $\Delta(\mathcal{X}, \mathcal{Y}) \leq \varepsilon$.

Let λ denote the security parameter unless otherwise specified. We say that a function $\varepsilon = \varepsilon(\lambda) \geq 0$ is *negligible*, if for any integer $n \geq 1$, there exists a $\lambda_0 > 0$ with the property that we have $\varepsilon(\lambda) < \lambda^{-n}$ for every $\lambda > \lambda_0$. We say that $\varepsilon \in [0, 1]$ is *overwhelming*, if $1 - \varepsilon$ is negligible. We say that ε is *noticeable*, if there exist integers $n \geq 1$ and $\lambda_0 > 0$ with the property that we have $\varepsilon > \lambda^{-n}$ for every $\lambda > \lambda_0$. We say that two families of probability distributions parameterized by λ are *statistically close*, if their statistical distance is negligible.

A *public key encryption* (*PKE*) scheme consists of the following three algorithms. The key

[1] Such attacks was pointed out by an anonymous reviewer for a previous submission of this paper.

generation algorithm $\mathsf{Gen}(1^\lambda)$ outputs a pair of a public key pk and a secret key sk. The encryption algorithm $\mathsf{Enc}(m) = \mathsf{Enc}_{\mathsf{pk}}(m)$ outputs a ciphertext as the encryption result of plaintext m. The decryption algorithm $\mathsf{Dec}(c) = \mathsf{Dec}_{\mathsf{sk}}(c)$ outputs either a plaintext m as the decryption result of ciphertext c, or a distinguished symbol $\perp$ indicating decryption failure. The *correctness* of a PKE scheme means that, for any plaintext m, the probability $\Pr[\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m)) \neq m]$ is negligible, where the probability is taken over the internal randomness for the algorithms.

For a finite set $\mathcal{M}$, we say that a set of operators on $\mathcal{M}$ is *functionally complete*, if any function with inputs and outputs in $\mathcal{M}$ can be computed by combining these operators only. We say that a PKE scheme with plaintext space $\mathcal{M}$ is a *fully homomorphic encryption* (*FHE*) scheme, if there exists a functionally complete set of operators on $\mathcal{M}$, which we call the *fundamental operators*, and an efficient algorithm, which we call a *homomorphic operator*, associated to each fundamental operator $f \colon \mathcal{M}^n \to \mathcal{M}$ that, given ciphertexts for plaintexts m_i $(i = 1, \dots, n)$ as inputs, outputs a ciphertext for plaintext $f(m_1, \dots, m_n)$ with overwhelming probability.

We say that a PKE scheme with plaintext space $\mathcal{M}$ is *CPA-secure*, if for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, the *advantage* $\mathsf{Adv}_{\mathcal{A}}(\lambda) = |\Pr[b = b^*] - 1/2|$ of $\mathcal{A}$ is negligible, where $\Pr[b = b^*]$ is the probability that $b = b^*$ in the following game:

$$\begin{aligned}&(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)\,;\ (m_0, m_1, \mathsf{state}) \leftarrow \mathcal{A}(\text{submit}, 1^\lambda, \mathsf{pk})\,;\\ &b^* \leftarrow \{0,1\}\,;\ c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{b^*})\ :\ b \leftarrow \mathcal{A}(\text{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^*)\ .\end{aligned}$$

2.1 Algorithms for Sampling Group Elements

Here we recall a known result on sampling an almost uniformly random element of any finite group G. For any elements $x_1, \dots, x_n \in G$, let $\mathsf{Sample}[x_1, \dots, x_n]$ denote the algorithm that outputs ${x_1}^{e_1} \cdots {x_n}^{e_n} \in G$ for uniformly random and independent exponents $e_1, \dots, e_n \leftarrow \{0,1\}$. Then, for a sufficiently large n, the output distribution of $\mathsf{Sample}[x_1, \dots, x_n]$ becomes close to uniform for random elements $x_1, \dots, x_n$ with high probability. More precisely, the following result was given by Dixon [11]:

Proposition 1 ([11], Theorem 3)**.** *Let G be a finite group, let $0 \leq \varepsilon < 1$, and let $\mathcal{X}$ be a probability distribution over G with $\Delta(\mathcal{X}, \mathcal{U}[G]) \leq \varepsilon$. Let n be a positive integer, and let $h, k \geq 0$. If*

$$n \geq \frac{\log_2 |G| + h + 2k - 2}{\log_2(2/(1+\varepsilon))}\ ,$$

then we have $\Pr_{x_1,\dots,x_n \leftarrow \mathcal{X}}[\Delta(\mathsf{Sample}[x_1, \dots, x_n], \mathcal{U}[G]) > 2^{-k}] < 2^{-h}$.

3 Prototype Schemes with Deterministic Operators

In the following two sections, we describe "prototypes" of our proposed FHE schemes, where only the functionality is considered and the security is not concerned yet. A candidate methodology to make the scheme (conjecturally) secure will be proposed in Section 5. In this section, we deal with the schemes with deterministic homomorphic operators.

We set the plaintext space to be $\mathcal{M} = \{0,1\}$ (Section 3.1) or $\mathcal{M} = \mathbb{F}_3$ (Section 3.2). The ciphertext space is the direct product group $\mathcal{C} = N \times S_5$ of symmetric group S_5 and a certain appropriate group N (see Section 5.2). Let $\pi \colon \mathcal{C} \to S_5$ denote the projection function. We regard N as a subgroup of $\mathcal{C}$ in a natural manner. For any subset $X \subset S_5$, let $\pi^{-1}(X)$ denote the set of the elements $c \in \mathcal{C}$ with $\pi(c) \in X$; and we write $\pi^{-1}(\{g\})$ for $g \in S_5$ simply as $\pi^{-1}(g)$. For $g \in S_5$, let $\widetilde{g}$ denote any fixed element of $\pi^{-1}(g)$; hence $\pi(\widetilde{g}) = g$.

Let $\delta > 0$ be a sufficiently small parameter. For the sake of random sampling over N, we choose a number of random elements $x_1, \dots, x_n \in N$. Then by Proposition 1, by taking a sufficiently large n, the probability that $\mathsf{Sample}[x_1,\dots,x_n]$ is δ-close to $\mathcal{U}[N]$ becomes arbitrarily close to 1, where the probability is taken over the random choice of $x_1,\dots,x_n$. Owing to this, here we assume that $\mathsf{Sample}[x_1,\dots,x_n]$ is indeed δ-close to $\mathcal{U}[N]$.

Moreover, we choose elements $\sigma_m \in S_5$ for $m \in \mathcal{M}$ in a certain manner (see Sections 3.1 and 3.2) and choose any element $\widetilde{\sigma_m} \in \pi^{-1}(\sigma_m)$ for each $m \in \mathcal{M}$. Now the PKE part of the prototype scheme is defined as follows:

$\mathsf{Gen}(1^\lambda)$ Given a security parameter, the algorithm chooses the group N and elements $\widetilde{\sigma_m} \in \mathcal{C}$ for $m \in \mathcal{M}$ and $x_1,\dots,x_n \in N$ as above. Then it publicizes $\mathcal{M}$, $\mathcal{C} = N \times S_5$, the elements $\widetilde{\sigma_m}$, the elements x_i, and additional elements of $\mathcal{C}$ required for computation of the homomorphic operators (see Sections 3.1 and 3.2).

$\mathsf{Enc}(m)$ For $m \in \mathcal{M}$, it generates $x \leftarrow \mathsf{Sample}[x_1,\dots,x_n]$ and outputs $c = x \cdot \widetilde{\sigma_m} \in \mathcal{C}$.

$\mathsf{Dec}(c)$ For $c \in \mathcal{C}$, it outputs the element $m \in \mathcal{M}$ satisfying $\pi(c) = \pi(\widetilde{\sigma_m})$, or equivalently $c^{-1}\widetilde{\sigma_m} \in N$ (and output $\perp$ if such an element m does not exist).

Now the correctness holds since $\pi(x) = 1_{S_5}$ for any $x \in N$. We emphasize again that here the security is not concerned yet; the projection π in Dec is in general efficiently computable for a naive construction of the product group $\mathcal{C} = N \times S_5$. A candidate methodology to make the function π harder to compute (without trapdoor information) will be proposed in Section 5.

Remark 1. We consider additional rerandomization functionality for the scheme; given $c \in \mathcal{C}$, the algorithm outputs $x \cdot c$ where $x \leftarrow \mathsf{Sample}[x_1,\dots,x_n]$. Now if δ is negligible, then for any $c \in \mathcal{C}_m$ with $m \in \mathcal{M}$, the distribution of the element $x \cdot c$ above is statistically close to the output distribution of $\mathsf{Enc}(m)$. This implies that, the scheme is endowed with circuit privacy (see e.g., [24]) by appending the rerandomization procedure to the end of each homomorphic operator.

From now, we describe constructions of the homomorphic operators for the scheme.

3.1 Case of 1-Bit Plaintexts

Here we construct homomorphic operators for the case of 1-bit plaintext space $\mathcal{M} = \{0,1\}$. In [28], Ostrovsky and Skeith III proved that NAND gate is realizable in any non-commutative finite simple group. They also gave a concrete construction over alternating group A_5 in the full version [27] of [28]. More precisely, they constructed a function $f\colon A_5 \times A_5 \to A_5$ and specified two elements $\sigma_0, \sigma_1 \in A_5$, with the following properties: $f(\sigma_b, \sigma_{b'}) = \sigma_{\mathsf{NAND}(b,b')}$ for any $b, b' \in \{0,1\}$; and values of f are computed by group operations for inputs and some constant elements. Here we utilize similar but significantly simpler functions defined over the group S_5 instead of A_5, corresponding to fundamental operators NOT, OR, NAND, XOR, and EQ (where EQ denotes the equality test, i.e., $\mathsf{EQ}(b,b') = 1$ if and only if $b = b'$).

We put $\sigma_0 = 1_{S_5}$, $\sigma_1 = (1,2,3) \in S_5$, and $\mathcal{C}_m = \pi^{-1}(\sigma_m)$ for $m \in \mathcal{M}$. Note that $\mathcal{C}_m$ is nothing but the set of ciphertexts for $m \in \mathcal{M}$. For NOT operator, we define a map F_{NOT} by

$$F_{\mathsf{NOT}}(c) = c^{-1}\widetilde{\sigma_1} \in \mathcal{C} \text{ for } c \in \mathcal{C} \enspace .$$

Then we have $F_{\mathsf{NOT}}(\mathcal{C}_m) \subset \mathcal{C}_{\mathsf{NOT}(m)}$ for $m \in \mathcal{M}$ (i.e., $F_{\mathsf{NOT}}(\mathcal{C}_0) \subset \mathcal{C}_1$ and $F_{\mathsf{NOT}}(\mathcal{C}_1) \subset \mathcal{C}_0$) by definition, therefore the map F_{NOT} provides a homomorphic NOT operator for the scheme.

For the homomorphic operators for the remaining fundamental operators $\mathsf{op} = \mathsf{OR}$, NAND, XOR, EQ, first we define a map $F_{\mathsf{op},\mathrm{app}}$ that "approximates" the operator, by

$$\begin{aligned} &F_{\mathsf{OR},\mathrm{app}}(c_1,c_2) = c_1 c_2 \,,\; F_{\mathsf{NAND},\mathrm{app}}(c_1,c_2) = {c_1}^{-1}{c_2}^{-1}\widetilde{\sigma_1}^2 \,, \\ &F_{\mathsf{XOR},\mathrm{app}}(c_1,c_2) = {c_1}^{-1}c_2 \,,\; F_{\mathsf{EQ},\mathrm{app}}(c_1,c_2) = c_1 c_2 \widetilde{\sigma_1}^{-1} \text{ for } c_1,c_2 \in \mathcal{C} \enspace . \end{aligned}$$

Then a straightforward calculation shows that $F_{\mathsf{op},\mathrm{app}}(\mathcal{C}_{m_1},\mathcal{C}_{m_2}) \subset X_{\mathsf{op}(m_1,m_2)}$ for any $m_1, m_2 \in \mathcal{M}$, where $X_0 = \mathcal{C}_0$ and $X_1 = \mathcal{C}_1 \cup \pi^{-1}({\sigma_1}^2)$ (note that ${\sigma_1}^2 = {\sigma_1}^{-1}$). For example, we have $\pi(F_{\mathsf{EQ},\mathrm{app}}(c_1,c_2)) = \sigma_1\sigma_0{\sigma_1}^{-1} = \sigma_0$ and $F_{\mathsf{EQ},\mathrm{app}}(c_1,c_2) \in X_0 = X_{\mathsf{EQ}(1,0)}$ if $c_1 \in \mathcal{C}_1$ and $c_2 \in \mathcal{C}_0$; and we have $\pi(F_{\mathsf{OR},\mathrm{app}}(c_1,c_2)) = {\sigma_1}^2$ and $F_{\mathsf{OR},\mathrm{app}}(c_1,c_2) \in X_1 = X_{\mathsf{OR}(1,1)}$ if $c_1, c_2 \in \mathcal{C}_1$. Secondly, we define another function $F_{\mathrm{ad}} \colon \mathcal{C} \to \mathcal{C}$ by

$$F_{\mathrm{ad}}(c) = \widetilde{(1,5)}\widetilde{(2,3,4)}c\widetilde{(2,3,4)}c\widetilde{(3,4)}c^2\widetilde{(2,3)}\widetilde{(4,5)}c\widetilde{(2,3,4)}c\widetilde{(3,4)}c^2\widetilde{(1,4,2,5)}$$

for $c \in \mathcal{C}$ (see the beginning of Section 3 for the notation $\widetilde{g}$ with $g \in S_5$). Then a straightforward calculation shows that this function "adjusts" the sets X_m in such a way that $F_{\mathrm{ad}}(X_m) \subset \mathcal{C}_m$ for any $m \in \mathcal{M}$. Namely, we have

$$\begin{aligned}&(1,5)(2,3,4)g(2,3,4)g(3,4)g^2(2,3)(4,5)g(2,3,4)g(3,4)g^2(1,4,2,5)\\&= \begin{cases} 1_{S_5} = \sigma_0 & \text{if } g = \sigma_0 \ , \\ (1,2,3) = \sigma_1 & \text{if } g \in \{\sigma_1, {\sigma_1}^2\} \ . \end{cases}\end{aligned}$$

By the argument, the function

$$F_{\mathsf{op}} = F_{\mathsf{op},\mathrm{ad}} \circ F_{\mathsf{op},\mathrm{app}} \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

satisfies that $F_{\mathsf{op}}(\mathcal{C}_{m_1},\mathcal{C}_{m_2}) \subset \mathcal{C}_{\mathsf{op}(m_1,m_2)}$ for $m_1, m_2 \in \mathcal{M}$ and $\mathsf{op} = \mathsf{OR}, \mathsf{NAND}, \mathsf{XOR}, \mathsf{EQ}$, therefore the function F_{op} provides a homomorphic operator for op. These functions F_{op} have expressions with significantly smaller numbers of group elements than the function in [27], where the latter is composed of 65 group elements in total. We note that the elements $\widetilde{g}$ for $g \in S_5$ appeared in the definition of F_{op} must be also included in the public key for the scheme.

3.2 Case of Ternary Plaintexts

We also construct homomorphic operators for the case of non-binary plaintext space $\mathcal{M} = \mathbb{F}_3 = \{0,1,2\}$ of three elements in a similar manner, where the fundamental operators are the ring operators $\mathsf{op} \in \{+, \times\}$. We put $\sigma_0 = 1_{S_5}$, $\sigma_1 = (1,2,3) \in S_5$, $\sigma_2 = {\sigma_1}^2 = (1,3,2)$, and $\mathcal{C}_m = \pi^{-1}(\sigma_m)$ for $m \in \mathcal{M}$. Now since ${\sigma_1}^3 = 1_{S_5}$, the function F_+ for the homomorphic addition is simply defined by

$$F_+(c_1,c_2) = c_1c_2 \in \mathcal{C} \text{ for } c_1, c_2 \in \mathcal{C} \ ,$$

and it satisfies $F_+(\mathcal{C}_{m_1},\mathcal{C}_{m_2}) \subset \mathcal{C}_{m_1+m_2}$ for any $m_1, m_2 \in \mathcal{M}$.

For the homomorphic multiplication, first we define an "approximation" function $F_{\times,\mathrm{app}}$ by

$$F_{\times,\mathrm{app}}(c_1,c_2) = c_1\widetilde{(1,4)(2,3,5)}^{-1}c_2\widetilde{(1,4)(2,3,5)} \text{ for } c_1, c_2 \in \mathcal{C}$$

(see the beginning of Section 3 for the notation $\widetilde{g}$ with $g \in S_5$). Then, by putting

$$\begin{aligned}X_0 &= \pi^{-1}(\{1_{S_5}, (2,4,5), (2,5,4), (1,2,3), (1,3,2)\}) \ ,\\ X_1 &= \pi^{-1}(\{(1,2,4,5,3), (1,3,2,5,4)\}) \ ,\\ X_2 &= \pi^{-1}(\{(1,2,5,4,3), (1,3,2,4,5)\}) \ ,\end{aligned}$$

we have $F_{\times,\mathrm{app}}(\mathcal{C}_{m_1},\mathcal{C}_{m_2}) \subset X_{m_1m_2}$ for any $m_1, m_2 \in \mathcal{M}$ by a straightforward calculation. On the other hand, the "adjusting" function $F_{\mathrm{ad}} \colon \mathcal{C} \to \mathcal{C}$ is constructed as follows. First, the function $\varphi_1(c) = c^3$ and the following sets

$$\begin{aligned}X_0^{(1)} = \pi^{-1}(1_{S_5})\, , \ X_1^{(1)} &= \pi^{-1}(\{(1,5,2,3,4), (1,5,3,4,2)\}) \ ,\\ X_2^{(1)} &= \pi^{-1}(\{(1,4,2,3,5), (1,4,3,5,2)\})\end{aligned}$$

satisfy $\varphi_1(X_m) \subset X_m^{(1)}$ for any $m \in \mathcal{M}$. Secondly, the function $\varphi_2 \colon \mathcal{C} \to \mathcal{C}$ defined by

$$\varphi_2(c) = \widetilde{(2,3,4)}^{-1} c^{-1} \widetilde{(3,4,5)} c^2 \widetilde{(3,4,5)}^{-1} c \widetilde{(2,3,4)}$$

and the following sets

$$X_0^{(2)} = \pi^{-1}(1_{S_5}) \,,\, X_1^{(2)} = \pi^{-1}((1,4,2,3,5)) \,,\, X_2^{(2)} = \pi^{-1}(\{(1,5,3,4,2),(1,5,2,3,4)\})$$

satisfy $\varphi_2(X_m^{(1)}) \subset X_m^{(2)}$ for any $m \in \mathcal{M}$. Since $X_0^{(2)} = X_0^{(1)}$, $X_1^{(2)} \subset X_2^{(1)}$ and $X_2^{(2)} = X_1^{(1)}$, the same calculation implies that the function $\varphi_3 = \varphi_2$ and the following sets

$$X_0^{(3)} = \pi^{-1}(1_{S_5}) \,,\, X_1^{(3)} = \pi^{-1}((1,5,3,4,2)) \,,\, X_2^{(3)} = \pi^{-1}((1,4,2,3,5))$$

satisfy $\varphi_3(X_m^{(2)}) \subset X_m^{(3)}$ for any $m \in \mathcal{M}$. Finally, the function $\varphi_4 \colon \mathcal{C} \to \mathcal{C}$ defined by

$$\varphi_4(c) = c \widetilde{(1,5,3,4,2)} c^{-1} \widetilde{(1,5,3,4,2)}^{-1} c \widetilde{(1,4,2,3,5)} c^{-1} \widetilde{(1,4,2,3,5)}^{-1}$$

satisfies $\varphi_4(X_m^{(3)}) \subset \mathcal{C}_m$ for any $m \in \mathcal{M}$. Summarizing, the function

$$F_{\mathrm{ad}} = \varphi_4 \circ \varphi_3 \circ \varphi_2 \circ \varphi_1$$

satisfies that $F_{\mathrm{ad}}(X_m) \subset \mathcal{C}_m$ for any $m \in \mathcal{M}$, therefore the function

$$F_\times = F_{\mathrm{ad}} \circ F_{\times,\mathrm{app}} \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

satisfies that $F_\times(\mathcal{C}_{m_1}, \mathcal{C}_{m_2}) \subset \mathcal{C}_{m_1 m_2}$ for any $m_1, m_2 \in \mathcal{M}$. Hence this function provides a homomorphic multiplication. We note that the elements $\widetilde{g}$ for some $g \in S_5$ appeared in the definition of $F_\times$ must be also included in the public key for the scheme.

4 Prototype Schemes with Probabilistic Operators

In this section, we describe the prototype schemes with 1-bit plaintext spaces $\mathcal{M} = \{0,1\}$ and probabilistic homomorphic operators. Let $\varepsilon > 0$ be a sufficiently small parameter. The ciphertext space is the direct product group $\mathcal{C} = (N \times G) \times (N \times G)$, where G is a certain appropriate group with $|G| \geq 1/\varepsilon$ (see Sections 4.1 and 4.2) and N is another appropriate group N (see Section 5.2). We often express an element of $\mathcal{C}$ as $c = (c_1, c_2)$ with $c_1, c_2 \in N \times G$. We regard N as a subgroup of $N \times G$ in a natural manner. Let $\pi \colon N \times G \to G$ be the projection function. Now the sets $\mathcal{C}_m$ of ciphertexts for plaintexts $m \in \mathcal{M}$ are defined by

$$\begin{aligned} \mathcal{C}_0 &= \{c = (c_1, c_2) \in \mathcal{C} \mid \pi(c_1) \neq 1_G \,,\, \pi(c_2) = 1_G\} \ , \\ \mathcal{C}_1 &= \{c = (c_1, c_2) \in \mathcal{C} \mid \pi(c_1) \neq 1_G \,,\, \pi(c_2) = \pi(c_1)\} \ . \end{aligned}$$

Let $\delta > 0$ be a sufficiently small parameter. In the same way as Section 3, we may assume (by Proposition 1) that randomly chosen elements $x_1, \dots, x_n \in N$ and $y_1, \dots, y_{n'} \in G$ satisfy that $\mathsf{Sample}[x_1, \dots, x_n]$ is δ-close to uniform over N and $\mathsf{Sample}[y_1, \dots, y_{n'}]$ is δ-close to uniform over G. Moreover, we choose random elements $\widetilde{y_i} \in N \times G$ satisfying $\pi(\widetilde{y_i}) = y_i$ for $i = 1, \dots, n'$. Note that, outputs $\widetilde{y}$ of $\mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$ satisfy that $\pi(\widetilde{y})$ is δ-close to uniform over G. Now the PKE part of the prototype scheme and its homomorphic NOT operator are defined as follows:

$\mathsf{Gen}(1^\lambda)$ Given a security parameter, the algorithm chooses the groups N and G and elements $x_1, \dots, x_n \in \mathcal{C}$ and $\widetilde{y_1}, \dots, \widetilde{y_{n'}} \in \mathcal{C}$ as above. Then it publicizes $\mathcal{M} = \{0,1\}$, $\mathcal{C}$, the elements x_i and the elements $\widetilde{y_j}$.

$\mathsf{Enc}(m)$ For $m \in \mathcal{M}$, it generates $z_1, z_2 \leftarrow \mathsf{Sample}[x_1, \dots, x_n]$ and $\widetilde{y} \leftarrow \mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$. Then it outputs $c = (z_1\widetilde{y}, z_2) \in \mathcal{C}$ if $m = 0$, and outputs $c = (z_1\widetilde{y}, z_2\widetilde{y}) \in \mathcal{C}$ if $m = 1$.

$\mathsf{Dec}(c)$ For $c = (c_1, c_2) \in \mathcal{C}$, it outputs 0 if $\pi(c_2) = 1_G$, and outputs 1 otherwise.

$F_{\mathsf{NOT}}(c)$ For $c = (c_1, c_2) \in \mathcal{C}$, it outputs $(c_1, {c_2}^{-1}c_1) \in \mathcal{C}$.

For the correctness, we have $\pi(z_2) = 1_G$ and $\pi(z_1\widetilde{y}) = \pi(z_2\widetilde{y}) = \pi(\widetilde{y})$ in $\mathsf{Enc}(m)$. Now if $\pi(\widetilde{y})$ were uniformly random over G, then the output c of $\mathsf{Enc}(m)$ would satisfy $c \in \mathcal{C}_m$ (hence $\mathsf{Dec}(c) = m$) with probability at least $1 - 1/|G| \geq 1 - \varepsilon$. In fact $\pi(\widetilde{y})$ is δ-close to uniform, therefore we have $c \in \mathcal{C}_m$ with probability at least $1 - \varepsilon - \delta$. Hence the correctness holds if both ε and δ are negligible. Moreover, the algorithm F_{NOT} satisfies by definition that $F_{\mathsf{NOT}}(\mathcal{C}_m) \subset \mathcal{C}_{\mathsf{NOT}(m)}$, therefore it indeed provides a homomorphic NOT operator.

On the other hand, we show that the CPA security of the scheme is equivalent to hardness of the membership decision for the subgroup N in $N \times G$. We note that the latter problem is always easy for a naive construction of the product group $N \times G$; a candidate construction to make the membership decision for the subgroup N harder (without trapdoor information) will be proposed in Section 5. We have the following result:

Theorem 1. *Assume that all the algorithms in the scheme above are efficient, and both ε and δ are negligible. Then the scheme is CPA-secure if and only if, the subgroup membership problem for N in $N \times G$ is computationally hard; that is, for any PPT adversary $\mathcal{A}^\dagger$, the advantage $\mathsf{Adv}_{\mathcal{A}^\dagger}(\lambda) = |\Pr[b = b^\dagger] - 1/2|$ of $\mathcal{A}^\dagger$ in the following game is negligible:*

$$\mathsf{pk} \leftarrow \mathsf{Gen}(1^\lambda)\,;\, b^\dagger \leftarrow \{0,1\}\,;\, \begin{cases} g^\dagger \leftarrow N \times G & \text{if } b^\dagger = 1 \\ g^\dagger \leftarrow N & \text{if } b^\dagger = 0 \end{cases} \,:\, b \leftarrow \mathcal{A}^\dagger(1^\lambda, \mathsf{pk}, g^\dagger) \enspace .$$

Proof. We note that, by the hypothesis, an output x of $\mathsf{Sample}[x_1, \dots, x_n]$ is statistically close to uniform over N, and an output $\widetilde{y}$ of $\mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$ satisfies that $\pi(\widetilde{y})$ is statistically close to uniform over G. To simplify the argument, we suppose that x is uniformly random over N and $\pi(\widetilde{y})$ is uniformly random over G. Then it follows that $x\widetilde{y}$ is uniformly random over $N \times G$. Owing to this argument, we suppose without loss of generality that a uniformly random element of $N \times G$ can be efficiently computable.

First, we convert an adversary $\mathcal{A}^\dagger$ for the subgroup membership problem to a CPA adversary $\mathcal{A}$ for the scheme in the following manner. The algorithm $\mathcal{A}$ chooses challenge plaintexts $m_0 = 0$ and $m_1 = 1$. Given a challenge ciphertext $c^* = (c_1^*, c_2^*) \in \mathcal{C}$ with challenge bit b^*, $\mathcal{A}$ simply inputs c_2^* (as well as 1^λ and pk) to $\mathcal{A}^\dagger$, and outputs the output bit of the $\mathcal{A}^\dagger$. For the construction of $\mathcal{A}$, c_2^* is uniformly random over N if $b^* = 0$, and c_2^* is uniformly random over $N \times G$ if $b^* = 1$ (see the first paragraph of the proof). Hence we have $\mathsf{Adv}_{\mathcal{A}} = \mathsf{Adv}_{\mathcal{A}^\dagger}$.

Secondly, we convert a CPA adversary $\mathcal{A}$ for the scheme to an adversary $\mathcal{A}^\dagger$ for the subgroup membership problem in the following manner. Since the plaintext space is $\mathcal{M} = \{0,1\}$, we may assume without loss of generality that $\mathcal{A}$ always generates challenge plaintexts $m_0 = 0$ and $m_1 = 1$. Given a challenge element $g^\dagger$ with challenge bit $b^\dagger$, the algorithm $\mathcal{A}^\dagger$ generates $c_1^* \leftarrow N \times G$ (see the first paragraph of the proof) and $b^* \leftarrow \{0,1\}$; $\mathcal{A}^\dagger$ generates $c_2^* = g^\dagger (c_1^*)^{b^*}$; $\mathcal{A}^\dagger$ inputs $c^* = (c_1^*, c_2^*)$ (as well as 1^λ and pk) to $\mathcal{A}$ and receives the output bit b' of $\mathcal{A}$; and $\mathcal{A}^\dagger$ outputs $b = \mathsf{XOR}(b^*, b')$. Now if $b^\dagger = 0$, then $g^\dagger$ is a uniformly random element of N, therefore the input distribution for $\mathcal{A}$ is correct and we have

$$\left| \Pr[b = 0 \mid b^\dagger = 0] - \frac{1}{2} \right| = \left| \Pr[b' = b^* \mid b^\dagger = 0] - \frac{1}{2} \right| = \mathsf{Adv}_{\mathcal{A}}(1^\lambda) \enspace .$$

On the other hand, if $b^\dagger = 1$, then $g^\dagger$ is a uniformly random element of $N \times G$, therefore the distributions of c_2^* for $b^* = 0$ and for $b^* = 1$ are identical (uniform over $N \times G$) and independent of c_1^*. Hence we have

$$\Pr[b = 1 \mid b^\dagger = 1] = \Pr[b' \neq b^* \mid b^\dagger = 1] = \frac{1}{2} \ .$$

Summarizing, we have

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}^\dagger}(1^\lambda) &= \left| \Pr[b = b^\dagger = 1] + \Pr[b = b^\dagger = 0] - \frac{1}{2} \right| \\ &= \left| \frac{1}{2} \Pr[b = 1 \mid b^\dagger = 1] + \frac{1}{2} \Pr[b = 0 \mid b^\dagger = 0] - \frac{1}{2} \right| \\ &= \left| \frac{1}{4} + \frac{1}{2} \Pr[b = 0 \mid b^\dagger = 0] - \frac{1}{2} \right| \\ &= \frac{1}{2} \left| \Pr[b = 0 \mid b^\dagger = 0] - \frac{1}{2} \right| = \frac{1}{2} \mathsf{Adv}_{\mathcal{A}}(1^\lambda) \ .\end{aligned}$$

This completes the proof of Theorem 1. □

From now, we describe constructions of homomorphic AND operators for the scheme, whose correctness depends on the choice of the group G.

4.1 Construction over Matrix Groups

The first construction of homomorphic AND operator is given as follows:

$F_{\mathsf{AND}}(c, c')$ For $c = (c_1, c_2) \in \mathcal{C}$ and $c' = (c'_1, c'_2) \in \mathcal{C}$, it generates $g \leftarrow \mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$ and outputs $c^\dagger = (c_1^\dagger, c_2^\dagger) \in \mathcal{C}$ defined by $c_i^\dagger = [g c_i g^{-1}, c'_i]$ for $i = 1, 2$, where $[a, b] = aba^{-1}b^{-1}$ denotes the commutator operator.

For the correctness of the algorithm, suppose that $c \in \mathcal{C}_m$ and $c' \in \mathcal{C}_{m'}$ with $m, m' \in \mathcal{M}$. We expect that $c^\dagger \in \mathcal{C}_{\mathsf{AND}(m,m')}$. For the second component $c_2^\dagger$, if $m = 0$ or $m' = 0$, then we have $\pi(c_2) = 1_G$ or $\pi(c'_2) = 1_G$, therefore the element $\pi(c_2^\dagger) = [\pi(g)\pi(c_2)\pi(g)^{-1}, \pi(c'_2)]$ satisfies that $\pi(c_2^\dagger) = [1_G, \pi(c'_2)] = 1_G$ or $\pi(c_2^\dagger) = [\pi(g)\pi(c_2)\pi(g)^{-1}, 1_G] = 1_G$, respectively. On the other hand, if $m = m' = 1$, then we have $\pi(c_2) = \pi(c_1)$ and $\pi(c'_2) = \pi(c'_1)$, therefore we have $\pi(c_2^\dagger) = [\pi(g)\pi(c_2)\pi(g)^{-1}, \pi(c'_2)] = [\pi(g)\pi(c_1)\pi(g)^{-1}, \pi(c'_1)] = \pi(c_1^\dagger)$. Hence the condition for the second component $c_2^\dagger$ is satisfied. In contrast, for the first component $c_1^\dagger$, it is in general not guaranteed that the condition $\pi(c_1^\dagger) \neq 1_G$ is satisfied with high probability (for example, $\pi(c_1^\dagger)$ is always equal to 1_G when G is commutative), and we require some condition for the group G. Now we introduce the following definition:

Definition 1 (Commutator-separable groups)**.** Let $\varepsilon > 0$. We say that a finite group G is *ε-commutator-separable*, if there exists a subset $X \subset G$ satisfying that $1_G \in X$, $|X| \leq \varepsilon \cdot |G|$ (hence $|G| \geq 1/\varepsilon$), and for any $x, y \in G \setminus X$, we have

$$\Pr_{g \leftarrow G}[\ [gxg^{-1}, y] \in X\ ] \leq \varepsilon \ . \tag{1}$$

Moreover, we say that a family of finite groups $G = G_\lambda$ is *commutator-separable*, if there exists a negligible function $\varepsilon = \varepsilon(\lambda)$ for which G is ε-commutator-separable.

Examples of commutator-separable groups will be given below. We note that, only the *existence* of the subset X in Definition 1 matters in the argument below, therefore X need *not* be efficiently computable. Now assume that G is ε-commutator-separable. For each $m \in \mathcal{M}$, we define an auxiliary subset $\mathcal{C}_m^\dagger$ of $\mathcal{C}_m$ by $\mathcal{C}_m^\dagger = \{c = (c_1, c_2) \in \mathcal{C}_m \mid \pi(c_1) \notin X\}$ (note that $\pi(c_1) \notin X$ implies $\pi(c_1) \neq 1_G$, since $1_G \in X$). Then the following property holds:

Theorem 2. *Let G be ε-commutator-separable. Then:*

1. *For any $m \in \mathcal{M}$, the output of $\mathsf{Enc}(m)$ belongs to $\mathcal{C}_m^\dagger$ with probability at least $1 - \varepsilon - \delta$.*
2. *For any $m \in \mathcal{M}$, we have $F_{\mathsf{NOT}}(\mathcal{C}_m^\dagger) \subset \mathcal{C}_{\mathsf{NOT}(m)}^\dagger$.*
3. *Let $m, m' \in \mathcal{M}$, $c = (c_1, c_2) \in \mathcal{C}_m^\dagger$ and $c' = (c'_1, c'_2) \in \mathcal{C}_{m'}^\dagger$. Then the output $c^\dagger = (c_1^\dagger, c_2^\dagger)$ of $F_{\mathsf{AND}}(c, c')$ belongs to $\mathcal{C}_{\mathsf{AND}(m,m')}^\dagger$ with probability at least $1 - \varepsilon - \delta$, where the probability is taken over the internal randomness for F_{AND}.*

Proof. The first two parts follow from Definition 1 and the same argument as before Section 4.1. For the third part, by the argument above, we only need to consider the condition $\pi(c_1^\dagger) \not\in X$. Now we have $\pi(c_1^\dagger) = [\pi(g)\pi(c_1)\pi(g)^{-1}, \pi(c'_1)]$ where $g \leftarrow \mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$, while $\pi(g)$ is δ-close to uniform over G as mentioned above. Since $\pi(c_1), \pi(c'_1) \in G \setminus X$ by the hypothesis, if $\pi(g)$ were uniformly random over G, then condition (1) implies that we would have $\pi(c_1^\dagger) \not\in X$ with probability at least $1 - \varepsilon$. In fact $\pi(g)$ is δ-close to uniform, therefore we have $\pi(c_1^\dagger) \not\in X$ with probability at least $1 - \varepsilon - \delta$, as desired. This concludes the proof. □

By Theorem 2, if both δ and ε are negligible, then the outputs of Enc, F_{NOT} and F_{AND} will belong to a correct one of the two subsets $\mathcal{C}_m^\dagger$ of $\mathcal{C}_m$ except negligible error probability. Hence correct homomorphic NOT and AND operators are obtained.

Examples of Commutator-Separable Groups. Here we give examples of commutator-separable groups. For the purpose, first we present some lemmas. For an element g of any group H, let $Z_H(g) = \{h \in H \mid gh = hg\}$ denote the centralizer of g in H. Then, for condition (1), we have the following property:

Lemma 1. *Let H be a finite group, and let $X \subset H$. Then for any $x_1, x_2 \in H$, we have*

$$\Pr_{g \leftarrow H}[\ [gx_1g^{-1}, x_2] \in X\ ] \leq \frac{|X| \cdot |Z_H(x_1)| \cdot |Z_H(x_2)|}{|H|} \ .$$

Proof. We put $H_y = \{g \in H \mid [gx_1g^{-1}, x_2] = y\}$ for $y \in X$. Then we have

$$\Pr_{g \leftarrow H}[\ [gx_1g^{-1}, x_2] \in X\ ] = \sum_{y \in X} \Pr_{g \leftarrow H}[\ [gx_1g^{-1}, x_2] = y\ ] = \sum_{y \in X} \frac{|H_y|}{|H|} \ .$$

For each $y \in X$ with $H_y \neq \emptyset$, fix an element $g_y \in H_y$. Then for each $g \in H_y$, we have

$$\begin{aligned}(gx_1g^{-1})x_2(gx_1g^{-1})^{-1}{x_2}^{-1} &= [gx_1g^{-1}, x_2] \\ &= [g_yx_1{g_y}^{-1}, x_2] = (g_yx_1{g_y}^{-1})x_2(g_yx_1{g_y}^{-1})^{-1}{x_2}^{-1} \ ,\end{aligned}$$

therefore $(g_yx_1{g_y}^{-1})^{-1}(gx_1g^{-1}) \in Z_H(x_2)$. Now for each $h \in Z_H(x_2)$, we put

$$H_{y,h} = \{g \in H_y \mid (g_yx_1{g_y}^{-1})^{-1}(gx_1g^{-1}) = h\} \ .$$

Then we have $|H_y| = \sum_{h \in Z_H(x_2)} |H_{y,h}|$. If $H_{y,h} \neq \emptyset$, we fix an element $g_{y,h} \in H_{y,h}$. Now for any $g \in H_{y,h}$, we have $gx_1g^{-1} = g_yx_1{g_y}^{-1} \cdot h = g_{y,h}x_1{g_{y,h}}^{-1}$, therefore ${g_{y,h}}^{-1}g \in Z_H(x_1)$. This implies that $|H_{y,h}| \leq |Z_H(x_1)|$ for any $h \in Z_H(x_2)$. Summarizing, we have

$$\Pr_{g \leftarrow H}[\ [gx_1g^{-1}, x_2] \in X\ ] \leq \sum_{y \in X} \frac{\sum_{h \in Z_H(x_2)} |Z_H(x_1)|}{|H|} \leq \frac{|X| \cdot |Z_H(x_1)| \cdot |Z_H(x_2)|}{|H|} \ .$$

Hence Lemma 1 holds. □

Before giving the next lemma, we note the following fact: For any finite group H and $x \in H$, we have $|Z_H(x)| = |H|/|x^H|$, where $x^H = \{hxh^{-1} \mid h \in H\}$ denotes the conjugacy class of x in H. Then we have the following property:

Lemma 2. *Let $\varphi\colon H_1 \to H_2$ be a surjective homomorphism between two finite groups. Then we have $|Z_{H_2}(\varphi(x))| \leq |Z_{H_1}(x)| \leq |Z_{H_2}(\varphi(x))| \cdot |H_1|/|H_2|$ for any $x \in H_1$.*

Proof. First we note that, for each $h \in H_2$, the number of elements $g \in H_1$ with $\varphi(g) = h$ is constant independent of h, namely $|H_1|/|H_2|$. Moreover, we have $\varphi(x^{H_1}) = \varphi(x)^{H_2}$. By these arguments, we have $|\varphi(x)^{H_2}| \leq |x^{H_1}| \leq |\varphi(x)^{H_2}| \cdot |H_1|/|H_2|$, therefore

$$\frac{|H_2|}{|\varphi(x)^{H_2}|} \leq \frac{|H_1|}{|x^{H_1}|} \leq \frac{|H_1|}{|\varphi(x)^{H_2}|} = \frac{|H_1|}{|H_2|} \cdot \frac{|H_2|}{|\varphi(x)^{H_2}|} \enspace .$$

Hence Lemma 2 holds. □

From now, we prove that the special linear group of size two defined by

$$\mathrm{SL}_2(\mathbb{F}_q) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_q \,,\, \det(A) = ad - bc = 1\}$$

and the projective special linear group of size two defined by $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$, where $\mathbb{F}_q$ denotes the q-element finite field and I denotes the identity matrix, are commutator-separable if q is a sufficiently large function of the security parameter λ. In order to apply Lemma 1, we show the following property:

Lemma 3. *For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$ with $A \neq \pm I$, we have $|Z_{\mathrm{SL}_2(\mathbb{F}_q)}(A)| \leq 2q$ if $b \neq 0$ or $c \neq 0$, and $|Z_{\mathrm{SL}_2(\mathbb{F}_q)}(A)| = q - 1$ if $b = c = 0$.*

Proof. Let $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in Z_{\mathrm{SL}_2(\mathbb{F}_q)}(A)$, therefore $XA = AX$. Then we have

$$\det(X) = 1 \quad \text{and} \quad \begin{pmatrix} ax + cy & bx + dy \\ az + cw & bz + dw \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix} \enspace ,$$

therefore

$$xw - yz = 1 \,,\, cy = bz \,,\, bx + dy = ay + bw \,,\, az + cw = cx + dz \enspace .$$

First, suppose that $b \neq 0$. Then we have $z = b^{-1}cy$ and $w = x + b^{-1}(d - a)y$, therefore $x^2 + b^{-1}(d - a)xy - b^{-1}cy^2 = 1$. Now for each $y \in \mathbb{F}_q$, the quadratic equation in x has at most two solutions, and z and w are uniquely determined from x and y by the relations above. This implies that the number of the possible X is at most $2q$. The argument for the case $c \neq 0$ is similar; x and y are linear combinations of z and w, and w satisfies a quadratic equation when an element $z \in \mathbb{F}$ is fixed, therefore the number of the possible X is at most $2q$.

On the other hand, suppose that $b = c = 0$. By the condition $\det(A) = 1$, we have $ad = 1$, therefore $a \neq 0$ and $d \neq 0$. Now we have $dy = ay$ and $az = dz$, while the assumption $A \neq \pm I$ implies that $a \neq d$. Therefore, we have $y = 0$ and $z = 0$. This implies that $xw = 1$, therefore $w \neq 0$ and $x = w^{-1}$. Hence, the number of the possible X is $q - 1$. This completes the proof of Lemma 3. □

Corollary 1. *We have $|Z_{\mathrm{PSL}_2(\mathbb{F}_q)}(A)| \leq 2q$ for any non-identity element $A \in \mathrm{PSL}_2(\mathbb{F}_q)$.*

Proof. This follows from Lemmas 2 and 3 and the fact that there exists a surjective homomorphism $\mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ that maps $\pm I$ to the identity element. □

By combining the results above, we have the following:

Theorem 3. *If the finite field $\mathbb{F}_q$ satisfies*

$$\frac{8q}{q^2-1} \le \varepsilon \,, \quad \text{or equivalently} \quad q \ge \frac{4+\sqrt{16+\varepsilon^2}}{\varepsilon} \approx \frac{8}{\varepsilon} \ ,$$

then $\mathrm{SL}_2(\mathbb{F}_q)$ *and* $\mathrm{PSL}_2(\mathbb{F}_q)$ *are* ε*-commutator-separable with the subsets* $X = \{\pm I\}$ *and* $X = \{1_{\mathrm{PSL}_2(\mathbb{F}_q)}\}$*, respectively.*

Proof. Let $H \in \{\mathrm{SL}_2(\mathbb{F}_q), \mathrm{PSL}_2(\mathbb{F}_q)\}$. First, it is known that $|H| = q(q^2-1)/\eta$, where $\eta = 1$ if $H = \mathrm{SL}_2(\mathbb{F}_q)$ and $\eta = 2$ if $H = \mathrm{PSL}_2(\mathbb{F}_q)$. Therefore

$$\frac{|X|}{|H|} = \frac{2/\eta}{q(q^2-1)/\eta} = \frac{2}{q(q^2-1)} \le \varepsilon$$

by the condition for $\mathbb{F}_q$ in the statement. On the other hand, for any $x_1, x_2 \in H \setminus X$, Lemma 3 and Corollary 1 imply $|Z_H(x_1)|, |Z_H(x_2)| \le 2q$. Therefore, by Lemma 1, we have

$$\Pr_{g \leftarrow H}[\ [g x_1 g^{-1}, x_2] \in X\ ] \le \frac{(2/\eta) \cdot 2q \cdot 2q}{q(q^2-1)/\eta} = \frac{8q}{q^2-1} \le \varepsilon$$

by the condition for $\mathbb{F}_q$ in the statement. Hence Theorem 3 holds. □

4.2 Construction over Simple Groups

For the second construction of homomorphic AND operator, here we assume that G is a non-commutative finite simple group with $|G| \ge 1/\varepsilon$. Then for any $x \in G \setminus \{1_G\}$, G is generated by the elements of the form hxh^{-1} with $h \in G$. Due to this property, for a sufficiently small parameter $\rho > 0$, we may expect that the following property would hold by choosing a sufficiently large parameter ℓ (a concrete estimate of sufficient values of ℓ will be a future research topic):

Assumption 1. For any $x \in G \setminus \{1_G\}$, the probability distribution of the element $(h_1 x {h_1}^{-1})^{e_1} \cdot (h_2 x {h_2}^{-1})^{e_2} \cdots (h_\ell x {h_\ell}^{-1})^{e_\ell} \in G$, where $h_1, \dots, h_\ell \leftarrow G$ and the exponents $e_1, \dots, e_\ell$ are randomly chosen, is ρ-close to the uniform distribution over G.

Now we define the homomorphic AND operator as follows:

$F_{\mathsf{AND}}(c, c')$ For $c = (c_1, c_2) \in \mathcal{C}$ and $c' = (c'_1, c'_2) \in \mathcal{C}$, it generates $g_1, \dots, g_\ell, g'_1, \dots, g'_\ell \leftarrow \mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$, chooses exponents $e_1, \dots, e_\ell, e'_1, \dots, e'_\ell$ randomly, and outputs $c^\dagger = (c^\dagger_1, c^\dagger_2) \in \mathcal{C}$ defined by (for $i = 1, 2$)

$$c^\dagger_i = [(g_1 c_i {g_1}^{-1})^{e_1} \cdots (g_\ell c_i {g_\ell}^{-1})^{e_\ell}, (g'_1 c'_i {g'_1}^{-1})^{e'_1} \cdots (g'_\ell c'_i {g'_\ell}^{-1})^{e'_\ell}] \ .$$

For the correctness of the algorithm, suppose that $c \in \mathcal{C}_m$ and $c' \in \mathcal{C}_{m'}$ with $m, m' \in \mathcal{M}$. We expect that $c^\dagger \in \mathcal{C}_{\mathsf{AND}(m,m')}$. Now by an argument similar to Section 4.1, the condition for the second component $c^\dagger_2$ is always satisfied, and we only need to consider the condition $\pi(c^\dagger_1) \ne 1_G$ for the first component. For the purpose, we use the following group-theoretic result by Guralnick and Robinson [19]:

Proposition 2 ([19], Theorem 9). *For any non-commutative finite simple group H, we have*

$$\Pr_{x,y \leftarrow H}[\ [x, y] = 1_H\ ] \le |H|^{-1/2} \ .$$

Then, under Assumption 1, we have the following result:

Theorem 4. *For the group G as above, assume that Assumption 1 holds. Let $m, m' \in \mathcal{M}$, $c = (c_1, c_2) \in \mathcal{C}_m$ and $c' = (c'_1, c'_2) \in \mathcal{C}_{m'}$. Then an output $c^\dagger = (c^\dagger_1, c^\dagger_2)$ of $F_{\mathsf{AND}}(c, c')$ satisfies $c^\dagger \in \mathcal{C}_{\mathsf{AND}(m,m')}$ with probability at least $1 - \sqrt{\varepsilon} - 2\rho - 2\ell\delta$, where the probability is taken over the internal randomness for F_{AND}.*

Proof. First, if the elements

$$\pi\big((g_1 c_1 g_1{}^{-1})^{e_1} \cdots (g_\ell c_1 g_\ell{}^{-1})^{e_\ell}\big) = (\pi(g_1)\pi(c_1)\pi(g_1)^{-1})^{e_1} \cdots (\pi(g_\ell)\pi(c_1)\pi(g_\ell)^{-1})^{e_\ell} \tag{2}$$

and

$$\pi\big((g'_1 c'_1 g'_1{}^{-1})^{e'_1} \cdots (g'_\ell c'_1 g'_\ell{}^{-1})^{e'_\ell}\big) = (\pi(g'_1)\pi(c'_1)\pi(g'_1)^{-1})^{e'_1} \cdots (\pi(g'_\ell)\pi(c'_1)\pi(g'_\ell)^{-1})^{e'_\ell} \tag{3}$$

were uniformly random over G, then by Proposition 2, we would have $\pi(c^\dagger_1) \neq 1_G$ with probability at least $1 - |G|^{-1/2} \geq 1 - \sqrt{\varepsilon}$. From now, we investigate the true distributions of elements (2) and (3). Since $\pi(c_1), \pi(c'_1) \neq 1_G$, by Assumption 1, if the elements $\pi(g_1), \dots, \pi(g_\ell)$ and $\pi(g'_1), \dots, \pi(g'_\ell)$ were uniformly random over G, then the elements (2) and (3) would be ρ-close to uniformly random over G, therefore we would have $\pi(c^\dagger_1) \neq 1_G$ with probability at least $1 - \sqrt{\varepsilon} - 2\rho$. In fact, each of the elements $\pi(g_j)$ and $\pi(g'_j)$ is δ-close to uniform, therefore the true probability of $\pi(c^\dagger_1) \neq 1_G$ is at least $1 - \sqrt{\varepsilon} - 2\rho - 2\ell\delta$. Hence Theorem 4 holds. □

By Theorem 4, if Assumption 1 holds and all of ε, ρ, and $\ell\delta$ are negligible, then we obtain a correct homomorphic AND operator with negligible error probability.

Remark 2. We consider additional rerandomization functionality for the scheme; given $c = (c_1, c_2) \in \mathcal{C}$, the algorithm generates $z_1, z_2 \leftarrow \mathsf{Sample}[x_1, \dots, x_n]$, $g_1, \dots, g_\ell \leftarrow \mathsf{Sample}[\widetilde{y_1}, \dots, \widetilde{y_{n'}}]$ and random exponents $e_1, \dots, e_\ell$, and outputs $c^\dagger = (c^\dagger_1, c^\dagger_2)$ where $c^\dagger_i = z_i (g_1 c_i g_1{}^{-1})^{e_1} \cdots (g_\ell c_i g_\ell{}^{-1})^{e_\ell}$. Now if $c \in \mathcal{C}_m$ for $m \in \mathcal{M}$, then we have $\pi(c^\dagger_2) = 1_G$ when $m = 0$ ($\pi(c_2) = 1_G$), and we have $\pi(c^\dagger_2) = \pi(c^\dagger_1)$ when $m = 1$ ($\pi(c_2) = \pi(c_1)$). Moreover, if Assumption 1 holds and all of ε, ρ, and $\ell\delta$ are negligible, then by an argument similar to Theorem 4, $\pi(c^\dagger_1)$ is statistically close to uniform over G and z_1, z_2 are statistically close to uniform over N, therefore $c^\dagger$ is statistically close to the uniform distribution over $\mathcal{C}_m$. This implies that, the scheme is endowed with circuit privacy (see e.g., [24]) by appending the rerandomization procedure to the end of each homomorphic operator. The same also holds for the case of Section 4.1 (provided the group G is simple and Assumption 1 holds for the group).

5 Candidate Methodology to Achieve Security

In this section, we explain a candidate methodology to derive a secure FHE scheme from the prototype schemes given in Section 3 and 4. Recall that, the insecurity of the prototype schemes comes from the fact that the projection function $\pi\colon N \times G \to G$ for a direct product group $N \times G$ appeared in the scheme (where $G = S_5$ for the case of Section 3) is easily computable for a naive construction of the product group $N \times G$. To resolve this issue, in Section 5.1, we propose a countermeasure that, roughly speaking, "obfuscates" a symbolic expression of the group $N \times G$ by randomly applying a certain kind of transformations. Ideally, we expect that the resulting group would behave like a black-box group, hence the direct product structure of $N \times G$ is difficult to observe. Nevertheless, even if this is true, the scheme may be still insecure for an inappropriate choice of the group N. Then in Section 5.2, we give candidates for appropriate choices of the group N.

5.1 Obfuscation of Group Structures

Generator-Relator Presentations for Groups. Here we summarize some definitions and facts about the theory of presentations of groups in terms of generators and their fundamental relations; see e.g., [21] for some omitted details. For any set X, let $X^{\pm}$ denote the disjoint union of X and the set of symbols $X^{-1} = \{x^{-1} \mid x \in X\}$. Let R be some set of words of finite lengths with alphabet $X^{\pm}$, called *relators*. Then the *presentation* of group with generating set X and relators set R, denoted by $\langle X \mid R \rangle$, defines a group as follows: Each element of the group is specified by some (not necessarily unique) word of finite lengths with alphabet $X^{\pm}$. The multiplication of two elements is defined by concatenation of two words specifying these elements. Moreover, two words define the same group element if and only if, each of the two words can be converted to the other word by an iteration of the following kind of procedures: Insert or remove a subword of the form xx^{-1} with $x \in X^{\pm}$ (where we set $(x^{-1})^{-1} = x$ for $x^{-1} \in X^{-1}$) or a subword r in R. For a word $w = x_1 \cdots x_k$ with $x_1, \dots, x_k \in X^{\pm}$, we set $w^{-1} = {x_k}^{-1} \cdots {x_1}^{-1}$. In the presentation $\langle X \mid R \rangle$, each relator r in R may be expressed as "$r = 1$" or more generally "$w = v$" where w and v are two words satisfying $r = w^{-1}v$. We often identify the presentation $\langle X \mid R \rangle$ with the group which the presentation defines.

Remark 3. We note that, for any relator $r = x_1 \cdots x_k \in R$ with $x_1, \dots, x_k \in X^{\pm}$, the presentation $\langle X \mid (R \setminus \{r\}) \cup \{x_2 \cdots x_k x_1\} \rangle$ defines the same group as $\langle X \mid R \rangle$; for example, an insertion of a subword r is realized by an insertion of $x_1{x_1}^{-1}$, an insertion of $x_2 \cdots x_k x_1$ (to get $x_1 x_2 \cdots x_k x_1 {x_1}^{-1}$) and a removal of $x_1{x_1}^{-1}$ (to get $x_1 x_2 \cdots x_k$). Similarly, the presentation $\langle X \mid (R \setminus \{r\}) \cup \{r^{-1}\} \rangle$ also defines the same group as $\langle X \mid R \rangle$; for example, an insertion of a subword r is realized by an insertion of $x_1{x_1}^{-1}$, an insertion of $x_2{x_2}^{-1}$ (to get $x_1 x_2 {x_2}^{-1} {x_1}^{-1}$), and so on, and an insertion of $x_k{x_k}^{-1}$ (to get $x_1 x_2 \cdots x_k {x_k}^{-1} \cdots {x_2}^{-1}{x_1}^{-1}$) and a removal of r^{-1} (to get $x_1 x_2 \cdots x_k$).

For example, it is known that the symmetric group S_n admits a presentation $\langle s_1, \dots, s_{n-1} \mid {s_i}^2 = 1 \text{ (for any } i) \,,\, s_i s_j s_i = s_j s_i s_j \text{ (for } |j-i| = 1) \,,\, s_i s_j = s_j s_i \text{ (for } |j-i| \geq 2) \rangle$, where s_i denotes the adjacent transposition $(i, i+1) \in S_n$. On the other hand, Guralnick et al. [18] showed that $\mathrm{SL}_2(\mathbb{F}_q)$ admits a short presentation as follows:

Proposition 3 ([18], Section 3.2)**.** *If $q > 3$ is a prime, then $\mathrm{SL}_2(\mathbb{F}_q)$ admits a presentation with four generators and eight relators, where each relator has length $O(\log q)$.*

They also gave in [18] similar short presentations for several non-commutative finite simple groups, including $\mathrm{PSL}_2(\mathbb{F}_q)$. Moreover, we have the following result on the presentations for direct product groups:

Proposition 4 (See e.g., [21])**.** *Let $\langle X_i \mid R_i \rangle$, $i = 1, 2$, be two presentations with $X_1 \cap X_2 = \emptyset$. Then the direct product of the groups $\langle X_1 \mid R_1 \rangle$ and $\langle X_2 \mid R_2 \rangle$ admits a presentation $\langle X_1 \cup X_2 \mid R_1 \cup R_2 \cup \{{x_1}^{-1}{x_2}^{-1}x_1 x_2 \mid x_1 \in X_1 \,,\, x_2 \in X_2\} \rangle$.*

Tietze Transformations. There are some kinds of elementary transformations that converts a presentation $\langle X \mid R \rangle$ of a group to another presentation of the same (isomorphic) group, called *Tietze transformations* (see e.g., [21]). It consists of the following four kinds of transformations, where the first and the second ones are inverses of each other and the third and the fourth ones are inverses of each other:

1. Add a (redundant) relator r to R, as long as the word r defines the identity element in the group $\langle X \mid R \rangle$.
2. Remove a (redundant) relator r from R, as long as the word r defines the identity element in the group $\langle X \mid R \setminus \{r\} \rangle$.

3. Add a generator $y \notin X^{\pm}$ to X and add a relator $y^{-1}x_1 \cdots x_k$ to R with $x_1, \dots, x_k \in X^{\pm}$; i.e., add an element $x_1 \cdots x_k$ of the group to the generating set and write it as y.

4. Remove a generator y from X and remove a relator $y^{-1}x_1 \cdots x_k$ from R with $x_1, \dots, x_k \in (X \setminus \{y\})^{\pm}$, as long as no relators in R other than $y^{-1}x_1 \cdots x_k$ involve y or y^{-1}; i.e., remove a redundant generator y that can be expressed by the other generators as $y = x_1 \cdots x_k$.

We note that, for the fourth kind of transformations, any expression by word of an element of the group is also transformed in such a way that each appearance of the generator y is substituted by the subword $x_1 \cdots x_k$ (hence y^{-1} is substituted by ${x_k}^{-1} \cdots {x_1}^{-1}$).

Remark 4. The fourth kind of Tietze transformations above can be generalized to the following form: Remove a generator y from X, remove a relator $y^{-1}x_1 \cdots x_k$ from R with $x_1, \dots, x_k \in (X \setminus \{y\})^{\pm}$, and replace any other relator r in R with another relator $r^{\dagger}$ obtained by substituting $x_1 \cdots x_k$ into every appearance of y (hence ${x_k}^{-1} \cdots {x_1}^{-1}$ into every appearance of y^{-1}) in r. Indeed, a symbol y (respectively, y^{-1}) in any word can be replaced with $x_1 \cdots x_k$ (respectively, ${x_k}^{-1} \cdots {x_1}^{-1}$) by inserting a word $y^{-1}x_1 \cdots x_k$ to get $yy^{-1}x_1 \cdots x_k$ and then successively removing the subword yy^{-1} (respectively, by successively inserting a subword $x_1 \cdots x_k {x_k}^{-1} \cdots {x_k}^{-1}$ to get $y^{-1}x_1 \cdots x_k {x_k}^{-1} \cdots {x_k}^{-1}$ and then removing the subword $y^{-1}x_1 \cdots x_k$). The converse also holds by a similar argument. This implies that the relators r and $r^{\dagger}$ are equivalent under the existence of the relator $y^{-1}x_1 \cdots x_k$, therefore the generalized transformation is realized by first replacing every relator r with $r^{\dagger}$, the latter involving no y nor y^{-1}, and then applying the fourth kind of Tietze transformation.

Example 1. We start from a presentation $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$ of the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (written in multiplicative form) and its element $g = xy^2$, and apply Tietze transformations as follows:

1. We get $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\, z = xy \rangle$ by the third kind of transformation. We also replace the relator $z = xy$ with an equivalent one $x = zy^{-1}$ (see Remark 3).

2. We get $\langle y, z \mid (zy^{-1})^3 = y^5 = (zy^{-1})y(yz^{-1})y^{-1} = 1 \rangle$ by the fourth kind of transformation focusing on the relator $x = zy^{-1}$ (see Remark 4). This transformation changes $g = xy^2$ to $(zy^{-1})y^2 = zy$. We also replace the relator $(zy^{-1})y(yz^{-1})y^{-1}$ with an equivalent one $zyz^{-1}y^{-1}$.

3. We get $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$ by the first kind of transformation; the relator $zyz^{-1}y^{-1}$ allows to switch z and y^{-1} in the relator $(zy^{-1})^3$. Similarly, we get $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$ by the second kind of transformation.

4. We get $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1\,,\, y = z^6 \rangle$ by the first kind of transformation; we can insert z^6y^{-1} by the successive procedures $\emptyset \mapsto z^3y^{-3} \mapsto z^3z^3y^{-3}y^{-3} = z^6y^{-6} \mapsto z^6y^{-6}y^5 \mapsto z^6y^{-1}$.

5. We get $\langle z \mid z^3z^{-18} = z^{30} = zz^6z^{-1}z^{-6} = 1 \rangle$ by the fourth kind of transformation focusing on the relator $y = z^6$ (see Remark 4). This transformation changes $g = zy$ to $z(z^6) = z^7$. We also replace the relator z^3z^{-18} with an equivalent one z^{15}.

6. Finally, we get $\langle z \mid z^{15} = 1 \rangle$ by the second kind of transformation, which is a presentation of the group $\mathbb{Z}/15\mathbb{Z}$.

This process shows that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is isomorphic to $\mathbb{Z}/15\mathbb{Z}$, where $(1, 2) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ corresponds to $7 \in \mathbb{Z}/15\mathbb{Z}$ (note that $7 \bmod 3 = 1$ and $7 \bmod 5 = 2$).

Obfuscation of the Underlying Groups. Example 1 showed a process of converting a relatively complicated presentation of a given group to a simpler presentation of the same group. Here we emphasize that such a process is *reversible* (since every elementary Tietze transformation is reversible); a simpler presentation can be converted to a complicated presentation by using Tietze transformations. For example, the following kind of transformations can be realized by successive Tiezte transformations:

Lemma 4. *For any presentation of group $\langle X \mid R \rangle$, let $g \in X$ and let w be a word in alphabet $(X \setminus \{g\})^{\pm}$. Let g' be a symbol not in the set $X^{\pm}$, and set $X' = (X \setminus \{g\}) \cup \{g'\}$. Moreover, let R' denote the set obtained from R by substituting the word $g'w$ (respectively, $w^{-1}g'^{-1}$) into each appearance of the generator g (respectively, g^{-1}) in every relator in R. Then the presentation $\langle X' \mid R' \rangle$ defines the same group as $\langle X \mid R \rangle$.*

Proof. Starting from $\langle X \mid R \rangle$, first we apply the third kind of Tietze transformation to get $\langle X \cup \{g'\} \mid R \cup \{g'^{-1}gw^{-1}\} \rangle$. Secondly, we replace the relator $g'^{-1}gw^{-1}$ with an equivalent one $wg^{-1}g'$, and furthermore with $g^{-1}g'w$ (see Remark 3). Finally, we apply the fourth kind of Tietze transformation focused on the relator $g^{-1}g'w$ (see Remark 4), and the resulting presentation is nothing but $\langle X \mid R \rangle$. Hence Lemma 4 holds. □

Now we propose a candidate methodology to make the prototype schemes given in Sections 3 and 4 secure, by "obfuscating" a straightforward presentation of the product group $N \times G$ given by Proposition 4 (where we put $G = S_5$ for the case of Section 3) to a sufficiently complicated presentation by applying Tietze transformations randomly. We note that the group $G = S_5$ used in Section 3 admits a short presentation mentioned in Section 5.1. For the case of Section 4.1, the groups $G = \mathrm{SL}_2(\mathbb{F}_q)$ and $G = \mathrm{PSL}_2(\mathbb{F}_q)$ are commutator-separable (see Theorem 3) and admit short presentations (see Proposition 3). For the remaining case of Section 4.2, we may choose a non-commutative simple group G that admits a short presentation (see [18] and Proposition 3). For candidates of appropriate groups N with short presentations, see Section 5.2. Now the transformed key generation and decryption algorithms for our proposed FHE schemes are described as follows; while the other algorithms for encryption and homomorphic operators are essentially unchanged, except that the computations for group elements are performed on the obfuscated presentation instead of the original presentation:

$\mathsf{Gen}^*(1^\lambda)$ Given a security parameter, it first generates some elements of the group $\mathcal{C}$ specified in the original key generation algorithm. Secondly, the algorithm randomly chooses an "obfuscated" presentation of the group $N \times G$ by using Tietze transformations. The algorithm also records how the Tietze transformations are applied. Then the algorithm outputs a public key pk consisting of the plaintext space $\mathcal{M}$, the ciphertext space $\mathcal{C}$ with obfuscated presentation, and the elements of $\mathcal{C}$ chosen as above. The algorithm also outputs a secret key sk consisting of the record of the Tietze transformation above.

${\mathsf{Dec}^*}_{\mathsf{sk}}(c)$ Given an element $c \in \mathcal{C}$ in the obfuscated form, first the algorithm applies the reverse transformations of the Tietze transformations recorded in sk to the obfuscated presentation of the group $N \times G$; this results in the original presentation of the group, where the projection function π is easily computable. Then the algorithm calculates the decryption result in the same way as the original decryption algorithm.

For the security of the scheme, ideally, the obfuscated group $N \times G$ might behave like a kind of black-box groups if a sufficiently large number of random Tietze transformations are applied, hence it would be difficult (without the record of the transformations in the secret key) to compute the projection function π or the membership decision for the subgroup N (see Theorem 1); see Section 5.2 for a discussion on the choice of the group N. Due to the high flexibility of possible choices of random Tietze transformations, we may expect that a secure instantiation of our proposed FHE schemes would be available along this direction. A detailed analysis from both theoretical and experimental viewpoints will be a future research topic.

5.2 Choices of the Underlying Groups

Here we show that, even if the "obfuscation" methodology proposed in Section 5.1 works ideally to conceal the structure of the underlying product group, there still exist possibilities that our proposed scheme can be broken in a black-box manner if the subgroup N is not appropriately selected. We also give some candidates for appropriate choices of N.

Possible Attack Strategies. Let $\pi_N \colon N \times G \to N$ denote the projection function. A typical attack strategy against our proposed scheme is to find a non-identity element $g \in N \times G$ (where $G = S_5$ for the case of Section 3) satisfying $\pi_N(g) = 1_N$. If such an element g is found, then we always have $gx = xg$ for any $x \in N$, while the probability that $gx = xg$ holds for a random $x \in N \times G$ is low by the choice of the non-commutative group G, therefore the subgroup membership problem for $N \subset N \times G$ is now easily solvable. Hence, such an element g should not be efficiently found.

For example, a naive strategy to find a target element g as above is to generate a large number of random elements $h_1, \dots, h_L \in N \times G$ and then test for each pair (h_i, h_j) whether $\pi_N({h_i}^{-1} h_j) = 1_N$ or not. By the birthday paradox, the required number L of elements is expected to be of the order of $\sqrt{|N|}$, therefore $\sqrt{|N|}$ should be sufficiently large (e.g., we may set $\sqrt{|N|} \geq 2^{80}$, therefore $|N| \geq 2^{160}$). We also note that, given any element $h \in N \times G$, the elements $h_1, \dots, h_L$ may be sampled in such a way that each $\pi_N(h_i)$ belongs to the normal closure $\langle \pi_N(h) \rangle_{\mathrm{normal}}$ of $\pi_N(h)$ in N, by using a randomized function similar to Assumption 1 in Section 4.2. This suggests us to choose a group N for which the size of $\langle x \rangle_{\mathrm{normal}}$ is expected to be as large as possible for a random element x of N. From the viewpoint, it would be reasonable to use a non-commutative simple group N of large size, where we have $\langle x \rangle_{\mathrm{normal}} = N$ for any $x \in N \setminus \{1_N\}$. (We note that N may not be a commutative group, since $g = [h_1, h_2]$ becomes a target element when N is commutative.) It may be also reasonable to use an almost simple group such as $\mathrm{SL}_2(\mathbb{F}_q)$; note that $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ is a simple group for $q > 3$.

On the other hand, there are other possible attack strategies as follows. Suppose that an integer k satisfies that both probabilities $\Pr_{x \leftarrow N}[x^k = 1]$ and $\Pr_{y \leftarrow N \times G}[y^k \neq 1]$ are non-negligible and at least one of them is noticeable. Then an adversary can distinguish the uniform distributions over N and over $N \times G$ with non-negligible advantage by checking if a random element z of N or of $N \times G$ satisfies $z^k = 1$. Therefore, such an integer k should not be efficiently found.

For example[2], suppose that $N = G = A_\lambda$ with $\lambda \geq 4$. Let p be the largest odd prime with $p \leq \lambda$. Then the number of elements of A_λ that are cyclic permutations on p letters is $\binom{\lambda}{p}(p-1)! = \dfrac{2}{p \cdot (\lambda - p)!} \cdot |A_\lambda|$. This implies that $\Pr\limits_{x \leftarrow N}[x^p = 1] = \dfrac{2}{p \cdot (\lambda - p)!} + \dfrac{1}{|A_\lambda|!}$, denoted here by P; while we have $\Pr_{y \leftarrow N \times G}[y^p = 1] = P^2$. Since $\lambda - p$ is small for reasonable choices of λ (e.g., $\lambda - p \leq 6$ for $\lambda \leq 80$), P is significantly larger than P^2, therefore the uniform distributions over N and over $N \times G$ can be distinguished with non-negligible advantage by checking if $x^p = 1$ for a random element x of N or of $N \times G$.

Candidates for the Group. By the arguments above, it is reasonable to use a non-commutative (almost) simple group N of sufficiently large size for which an integer k yielding non-negligible

[2] This is the case of the candidate instantiation given in a previous version (20150819:140754) of this paper posted to `http://eprint.iacr.org/2014/097` on August 19, 2015.

Table 1: The conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ for odd prime $q > 3$ (here ζ denotes a generator of $(\mathbb{F}_q)^\times$, and matrices A_i and B_j are as defined in the text)

type	representative x	$\lvert x^{\mathrm{SL}_2(\mathbb{F}_q)}\rvert$	order of x
1	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	1	1
2	$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$	1	2
3	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	$\frac{q^2-1}{2}$	q
4	$\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix}$	$\frac{q^2-1}{2}$	q
5	$\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$	$\frac{q^2-1}{2}$	$2q$
6	$\begin{pmatrix}-1 & \zeta\\ 0 & -1\end{pmatrix}$	$\frac{q^2-1}{2}$	$2q$
7-i	A_i $(1 \le i < \frac{q-1}{2})$	q^2+q	$\frac{q-1}{\gcd(q-1,i)}$
8-i	$B_{(q-1)i}$ $(1 \le i < \frac{q+1}{2})$	q^2-q	$\frac{q+1}{\gcd(q+1,i)}$

probability $\Pr_{x \leftarrow N}[x^k = 1_N]$ is difficult to find. Here we propose to use $N = \mathrm{SL}_2(\mathbb{F}_q)$ for an odd prime q satisfying that $1/q$ is negligible in the security parameter λ. Note that this group N indeed admits a short presentation by Proposition 3. From now, we investigate the distribution of the orders of elements of $N = \mathrm{SL}_2(\mathbb{F}_q)$.

Following the argument in Section 5.2 of [13], we choose a generator ζ of the cyclic group $(\mathbb{F}_q)^\times$. Put $A_i = \begin{pmatrix}\zeta^i & 0\\ 0 & \zeta^{-i}\end{pmatrix}$ for $i = 0, 1, \dots, q-2$. On the other hand, by considering the quadratic extension field $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, ζ has a square root in $(\mathbb{F}_{q^2})^\times \setminus (\mathbb{F}_q)^\times$ (since q is odd), denoted by $\sqrt{\zeta}$. Then we have a bijection $\mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_{q^2}$, $(a, b) \mapsto a + b\sqrt{\zeta}$. Choose a generator υ of the cyclic group $(\mathbb{F}_{q^2})^\times$. For $i = 0, 1, \dots, q^2-2$, put $B_i = \begin{pmatrix}a & b\\ b\zeta & a\end{pmatrix}$ where $\upsilon^i = a + b\sqrt{\zeta}$. By using these notations, the list of conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ is obtained as in Table 1, where the second column (showing a representative element x for each conjugacy class) and the third column (showing the size of the conjugacy class $|x^{\mathrm{SL}_2(\mathbb{F}_q)}|$ of x) are quoted (with slightly different notations) from Section 5.2 of [13]. The fourth column gives the order of an element of each conjugacy class, which is constant on the conjugacy class. Note that, for elements of type 8 in the table, the map $\upsilon^i \mapsto B_i$ is a homomorphism from $(\mathbb{F}_{q^2})^\times$ to the matrix group.

In Table 1, the ratio $|x^{\mathrm{SL}_2(\mathbb{F}_q)}|/|\mathrm{SL}_2(\mathbb{F}_q)|$ of the size of each conjugacy class of type 1 to 6 to the size of the whole group is at most a negligible value $\frac{(q^2-1)/2}{q(q^2-1)} = \frac{1}{2q}$, therefore these conjugacy classes can be ignored in the current argument. On the other hand, for each divisor k of $q-1$, an element x of the conjugacy class of type 7-i satisfies $x^k = 1$ if and only if i is a multiple of $(q-1)/k$. Therefore, the number of such elements x is at most $\frac{(q-1)/2}{(q-1)/k}(q^2+q) = \frac{k}{2}(q^2+q)$, whose ratio to the size $q(q^2-1)$ of the whole group is $\frac{k}{2(q-1)}$. To make the ratio non-negligible, one must find a divisor k of $q-1$ which is almost as large as $q-1$; this is expected to be difficult *if the size q of the coefficient field $\mathbb{F}_q$ is not known.* The same also holds for conjugacy classes of type 8.

Summarizing, the attack strategy described above will be not effective for the group $N = \mathrm{SL}_2(\mathbb{F}_q)$, provided the size of the coefficient field $\mathbb{F}_q$ is appropriately concealed by the "obfuscating" methodology applied to the presentation of $N \times G$ in Section 5.1. A further analysis of other possible attack strategies will be a future research topic.

6 Concluding Remarks and Future Research Topics

The security of our proposed FHE schemes is based on the (conjectural) hardness of observing some significant information (e.g., the size of the coefficient field for a matrix group) from an "obfuscated" presentation of the underlying group obtained by applying random Tietze transformations. Since such a use of presentations for groups and Tietze transformations in cryptology is new, a detailed analysis of the reliability of this kind of hardness assumptions (as well as a study of possibilities for other applications of the proposed methodology) is left as a new research area where cryptology and combinatorial group theory intersect.

On the other hand, another issue about our proposed scheme is for the efficiency. Namely, in the underlying group with "obfuscated" presentation, any element is expressed as a word on the generating set (involving the inverses of generators) as the alphabet, where the expression is in general not unique. Since the length (as a word) of the product of group elements calculated naively is the sum of the lengths of the original elements, it is required to reduce the length of the word by using the relators; otherwise, the scheme might become a *somewhat* homomorphic encryption, where successive homomorphic operators would be available as long as the length of the resulting group element stays treatable by the implementation. To resolve the issue, a desirable situation is as follows: A unique representative of the set of expressions for each group element, called the *normal form* of the element, is determined, and an efficient algorithm to calculate the normal form of a given element is available. In fact, there exists an algorithm to find such a system of normal forms from a given presentation for group, called *Knuth–Bendix completion* (see e.g., [22, 23, 25]), but it is not guaranteed in general to find the solution efficiently with high probability. Hence, it is an important future research topic to improve the algorithm in such a way that the algorithm will work efficiently for inputs relevant to our proposed schemes.

Acknowledgments. The author thanks members of Shin-Akarui-Angou-Benkyou-Kai for their helpful comments. In particular, the author thanks Shota Yamada for inspiring the author with motivation to the present work; Takashi Yamakawa for pointing out the relation to Barrington's theorem; and Takahiro Matsuda, Keita Emura, Yoshikazu Hanatani, Jacob C. N. Schuldt and Goichiro Hanaoka for giving many precious comments on the work. The author also thanks the anonymous referees of previous conference submissions of the paper for their careful reviews and valuable comments.

References

[1] D. A. Barrington: Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC^1. In: Proceedings of STOC 1986, 1986, pp.1–5.

[2] S. R. Blackburn, C. Cid, C. Mullan: Group Theory in Cryptography. In: Proceedings of Group St Andrews 2009 in Bath, LMS Lecture Note Series 387, 2011, pp.133–149.

[3] Z. Brakerski: Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In: Proceedings of CRYPTO 2012, LNCS 7417, 2012, pp.868–886.

[4] Z. Brakerski, C. Gentry, V. Vaikuntanathan: (Leveled) Fully Homomorphic Encryption without Bootstrapping. In: Proceedings of ITCS 2012, 2012, pp.309–325.

[5] Z. Brakerski, V. Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. In: Proceedings of FOCS 2011, 2011, pp.97–106.

[6] Z. Brakerski, V. Vaikuntanathan: Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In: Proceedings of CRYPTO 2011, LNCS 6841, 2011, pp.505–524.

[7] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, A. Yun: Batch Fully Homomorphic Encryption over the Integers. In: Proceedings of EUROCRYPT 2013, LNCS 7881, 2013, pp.315–335.

[8] J. H. Cheon, D. Stehlé. Fully Homomophic Encryption over the Integers Revisited. In: Proceedings of EUROCRYPT 2015 (1), LNCS 9056, 2015, pp.513–536.

[9] J.-S. Coron, D. Naccache, M. Tibouchi: Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. In: Proceedings of EUROCRYPT 2012, LNCS 7237, 2012, pp.446–464.

[10] M. Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan: Fully Homomorphic Encryption over the Integers. In: Proceedings of EUROCRYPT 2010, LNCS 6110, 2010, pp.24–43.

[11] J. D. Dixon: Generating Random Elements in Finite Groups. The Electronic Journal of Combinatorics vol.15, 2008, no.R94.

[12] L. Ducas, D. Micciancio: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In: Proceedings of EUROCRYPT 2015 (1), LNCS 9056, 2015, pp.617–640.

[13] W. Fulton, J. Harris: Representation Theory. Springer GTM series vol.129, Springer, 1991.

[14] C. Gentry: Fully Homomorphic Encryption Using Ideal Lattices. In: Proceedings of STOC 2009, 2009, pp.169–178.

[15] C. Gentry, S. Halevi: Implementing Gentry's Fully-Homomorphic Encryption Scheme. In: Proceedings of EUROCRYPT 2011, LNCS 6632, 2011, pp.129–148.

[16] C. Gentry, S. Halevi: Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits. In: Proceedings of FOCS 2011, 2011, pp.107–109.

[17] C. Gentry, S. Halevi, N. P. Smart: Better Bootstrapping in Fully Homomorphic Encryption. In: Proceedings of PKC 2012, LNCS 7293, 2012, pp.1–16.

[18] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky: Presentations of Finite Simple Groups: A Quantitative Approach. Journal of the American Mathematical Society vol.21, 2008, pp.711–774.

[19] R. M. Guralnick, G. R. Robinson: On the Commuting Probability in Finite Groups. Journal of Algebra vol.300, 2006, pp.509–528.

[20] S. Halevi, V. Shoup: Bootstrapping for HElib. In: Proceedings of EUROCRYPT 2015 (1), LNCS 9056, 2015, pp.641–670.

[21] D. L. Johnson: Presentations of Groups, Second Edition. London Mathematical Society Student Texts vol.15, Cambridge University Press, 1997.

[22] J.-P. Jouannaud, H. Kirchner: Completion of a Set of Rules Modulo a Set of Equations. SIAM Journal of Computing vol.15, no.4, 1986, pp.1155–1194.

[23] D. Kapur, P. Narendran: The Knuth–Bendix Completion Procedure and Thue Systems. SIAM Journal of Computing vol.14, no.4, 1985, pp.1052–1072.

[24] J. Katz, A. Thiruvengadam, H.-S. Zhou: Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption. In: Proceedings of PKC 2013, LNCS 7778, 2013, pp.14–31.

[25] D. Knuth, P. Bendix: Simple Word Problems in Universal Algebra. In: Computational Problems in Abstract Algebra (J. Leech, ed.), Pergamon Press, 1970, pp.263–297.

[26] K. Nuida, K. Kurosawa: (Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces. In: Proceedings of EUROCRYPT 2015 (1), LNCS 9056, 2015, pp.537–555.

[27] R. Ostrovsky, W. E. Skeith III: Algebraic Lower Bounds for Computing on Encrypted Data. Electronic Colloquium on Computational Complexity (ECCC) 14(022), 2007.

[28] R. Ostrovsky, W. E. Skeith III: Communication Complexity in Algebraic Two-Party Protocols. In: Proceedings of CRYPTO 2008, LNCS 5157, 2008, pp.379–396.

[29] D. J. S. Robinson: A Course in the Theory of Groups, Second Edition. Springer GTM series vol.80, Springer, 1996.

[30] A. Silverberg: Fully Homomorphic Encryption for Mathematicians. IACR Cryptology ePrint Archive 2013/250, 2013, `http://eprint.iacr.org/2013/250`

[31] D. Stehlé, R. Steinfeld: Faster Fully Homomorphic Encryption. In: Proceedings of ASIACRYPT 2010, LNCS 6477, 2010, pp.377–394.