Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory

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

December 18, 2017

Abstract

In CRYPTO 2008, one year earlier than Gentry's pioneering "bootstrapping" technique on constructing the first fully homomorphic encryption (FHE) scheme, Ostrovsky and Skeith III had suggested a completely different approach towards achieving FHE. Namely, they showed that the NAND operator can be realized in some *non-commutative* groups; consequently, in combination with the NAND operator realized in such a group, homomorphically encrypting the elements of the group will yield an FHE scheme. However, no observations on how to homomorphically encrypt the group elements were presented in their paper, and there have been no follow-up studies in the literature based on their approach.

The aim of this paper is to exhibit more clearly what is sufficient and what seems to be effective for constructing FHE schemes based on their approach. First, we prove that it is sufficient to find a surjective homomorphism $\pi\colon \widetilde{G} \to G$ between finite groups for which bit operators are realized in G and the elements of the kernel of π are indistinguishable from the general elements of $\widetilde{G}$. Secondly, we propose new methodologies to realize bit operators in some groups, which enlarges the possibility of the group G to be used in our framework. Thirdly, we give an observation that a naive approach using matrix groups would never yield secure FHE due to an attack utilizing the "linearity" of the construction. Then we propose an idea to avoid such "linearity" by using combinatorial group theory, and give a prototypical but still *incomplete* construction in the sense that it is "non-compact" FHE, i.e., the ciphertext size is unbounded (though the ciphertexts are noise-free as opposed to the existing FHE schemes). Completely realizing FHE schemes based on our proposed framework is left as a future research topic.

1 Introduction

Until the pioneering work by Gentry [16] 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 "homomorphic" operations on the ciphertexts. After that, studies of FHE to improve the efficiency (e.g., [9, 13, 17, 19, 22, 30]) and to give various frameworks of construction (e.g., [3, 4, 5, 6, 7, 8, 10, 11, 18, 26]) have been one of the main research topics in cryptology (see e.g., [29] for a survey). Here we emphasize that, all the previous FHE schemes in the literature rely on Gentry's "bootstrapping" framework. Namely, ciphertexts for these FHE schemes involve "noise" terms to conceal plaintexts, and the noise is increased by homomorphic operations and will finally collapse the ciphertext; hence the increased noise must be cancelled before the collapse. The bootstrapping, which is the additional procedure for noise cancellation, is a major bottleneck for efficiency improvement and makes the syntax of FHE less analogical to the classical homomorphic encryption.

On the other hand, in 2008, which is one year earlier than Gentry's work, Ostrovsky and Skeith III [27] had suggested a completely different, group-theoretic approach towards achieving FHE. Namely, they showed that the NAND operator (which is sufficient for constructing arbitrary bit operators) can be realized (in a certain suitable sense) in some *non-commutative* groups. In combination with the NAND operator realized in such a group, if the elements of the non-commutative group can be homomorphically encrypted, then it will yield an FHE scheme where the ciphertexts involve no noise terms, hence the bootstrapping procedure will no longer be required. However, no observations on how to homomorphically encrypt the group elements were presented in their paper and, to the author's best knowledge, there have been no follow-up studies in the literature based on their approach. The aim of this paper is to exhibit more clearly what is sufficient and what seems to be effective for constructing "noise-free" FHE schemes based on their approach.

1.1 Our Contributions

Our results in this paper are summarized as follows. First, in Section 3, we revisit the approach towards constructing FHE suggested in the previous paper [27]. We give a formalization of "realizations of bit operators in groups" in a slightly generalized manner (e.g., our formalization can handle probabilistic realizations of bit operators as well, which were not considered in [27]). Then we reduce the problem of "homomorphically encrypting the elements of a group G" (where the bit operators are realized in G) to finding a surjective homomorphism $\pi\colon \widetilde{G} \to G$ to G from another finite group $\widetilde{G}$ (where elements of $\widetilde{G}$ play the role of ciphertexts) and prove that, the resulting FHE scheme is CPA-secure if the elements of the kernel $\ker \pi$ of π are indistinguishable from the general elements of $\widetilde{G}$ even when a certain generating set of $\ker \pi$ is publicly given. This clarifies the problem to be solved from a group-theoretic viewpoint.

In Section 4, we propose new methodologies to realize bit operators in some groups, which are different from the previous methodology in [27] (recalled in Section 4.1 below) analogous to Barrington's theorem [1]. Our result enlarges the possibility of the group G to be used in our framework, which is beneficial in order to search for a suitable homomorphism $\pi\colon \widetilde{G} \to G$. For example, we are now able to choose the matrix group $G = \mathrm{SL}_2(\mathbb{F}_p)$ with exponentially large prime p, for which the previous methodology in [27] is not efficient.

In the final Section 5, we give several observations and discussions on how to find a suitable homomorphism $\pi\colon \widetilde{G} \to G$. First, in Section 5.2, we give an observation that a naive approach to construct the group $\widetilde{G}$ as a random conjugate of block upper-triangular matrices (where the map π extracts the upper-left block) would never yield a secure FHE scheme, due to the existence of the following kind of attacks[1]. We start with the simplified situation where $\widetilde{G}$ is just a set of some block upper-triangular matrices (without taking a random conjugate) and the value of the map π is the upper-left block of the matrix. In this case, all the elements of $\ker \pi$ satisfy the constraint "the off-diagonal components of the upper-left block are zero", which is a *linear* constraint in terms of the matrix components. This linear constraint separates the elements of $\ker \pi$ and general elements of $\widetilde{G}$ in the sense that, a general element of $\widetilde{G}$ does not belong to the linear space spanned by $\ker \pi$ while any element of $\ker \pi$ does belong to this linear space; hence these two kinds of elements become easily distinguishable. Now, even when a random conjugate is taken in the construction of $\widetilde{G}$, the aforementioned constraint for elements of $\ker \pi$ still remains *linear* after taking the conjugate, which enables one to easily distinguish the two kinds of elements in the same way as above. This observation suggests that, in order to find a suitable $\pi\colon \widetilde{G} \to G$, such a linear constraint for $\ker \pi$ should be avoided.

In order to avoid such a linear constraint for $\ker \pi$, in Section 5.4, we propose an idea of making the map $\pi\colon \widetilde{G} \to G$ "non-linear" by utilizing properties from combinatorial group theory.

[1] This attack was pointed out by an anonymous reviewer at a previous submission of this work.

More precisely, we try to establish a homomorphism $\pi\colon \widetilde{G} \to G$ as a quotient map between two *Coxeter groups* (see e.g., [23] for the terminology), which is expected to be "non-linear" in a general case. It is useful for us that any Coxeter group admits a well-studied realization as a subgroup of the matrix group $\mathrm{GL}_n(\mathbb{R})$; this enables one to take a conjugate by a random matrix for the group $\widetilde{G}$ realized in $\mathrm{GL}_n(\mathbb{R})$ in order to hide the information on the very detailed structure of $\widetilde{G}$. However, an appropriate choice of $\widetilde{G}$ as a *finite* group following this approach has not yet been found. The group $\widetilde{G}$ in our prototypical construction described in that section is an *infinite* group, which results in a so-called *non-compact* FHE scheme, i.e., the sizes of ciphertexts are not bounded. A realization of our proposed approach with a *finite* group $\widetilde{G}$, which will yield a *compact* FHE scheme, is left as a future research topic.

We also discuss in Section 5.5 another possible approach that highly relies on techniques in combinatorial group theory. In this alternative approach, the group $\widetilde{G}$ is described in terms of a *group presentation* consisting of a generating set and a set of fundamental relations for generators. Then the group presentation for $\widetilde{G}$ is randomly modified (without changing the group structure itself) in order to conceal the detailed structure of $\widetilde{G}$. However, even if such a random modification of a group presentation provides sufficient security, the lack of efficient group operators for $\widetilde{G}$ based on the random presentation implies that the resulting FHE is again *non-compact* FHE so far. Overcoming this issue of inefficient group operators for such a group $\widetilde{G}$ is also left as a future research topic.

2 Preliminaries

In this section, we summarize some basic definitions and notations used throughout the paper. For a probability distribution (or a random variable) $\mathcal{X}$, let $a \leftarrow \mathcal{X}$ mean that an element a is randomly chosen according to $\mathcal{X}$. For a finite set X, let $a \leftarrowtail X$ mean that an element a is chosen uniformly at random from the 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. The *statistical distance* between two probability distributions $\mathcal{X}, \mathcal{Y}$ over a finite set Z is defined by

$$\Delta(\mathcal{X}, \mathcal{Y}) = \frac{1}{2} \sum_{z \in Z} |\Pr[z \leftarrow \mathcal{X}] - \Pr[z \leftarrow \mathcal{Y}]| \ .$$

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 $\lambda > \lambda_0$.

A *public key encryption* (*PKE*) scheme consists of the following three algorithms. The *key 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. Let the *correctness* of a PKE scheme mean 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 $\mathcal{F}$ of operators on $\mathcal{M}$ is *functionally complete*, if any function with inputs and outputs in $\mathcal{M}$ can be computed by combining operators in $\mathcal{F}$. We say that a PKE scheme with plaintext space $\mathcal{M}$ is a *fully homomorphic encryption* (*FHE*) scheme, if there exist a functionally complete set $\mathcal{F}$ of operators on $\mathcal{M}$ and an efficient *homomorphic evaluation algorithm* Eval with the property that, for each, say n-ary operator $f \in \mathcal{F}$

$(f\colon \mathcal{M}^n \to \mathcal{M})$ and for given ciphertexts c_i for plaintexts m_i $(i = 1, \ldots, n)$, the algorithm $\mathsf{Eval}_{\mathsf{pk}}(f; c_1, \ldots, c_n)$ outputs a ciphertext for plaintext $f(m_1, \ldots, m_n) \in \mathcal{M}$ 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 $b = b^*$ holds in the following game:

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

2.1 Preliminaries on Group Theory

Unless otherwise specified, a (not necessarily commutative) group G is written in multiplicative form and its identity element is denoted by 1_G (or by 1 if the group G is clear from the context). The reader may refer to a textbook of group theory (e.g., [28]) for definitions and basic facts for groups mentioned without explicit references. We say that a subgroup N of a group G is *normal*, if we have $gxg^{-1} \in N$ for any $x \in N$ and $g \in G$. Then the *quotient group* G/N of a group G by its normal subgroup N is uniquely determined (up to group isomorphisms) in a way that, there is a surjective group homomorphism $G \to G/N$ (here we write the map as $g \mapsto \overline{g}$), and for any group H and any homomorphism $\varphi\colon G \to H$ satisfying $\varphi(N) = \{1_H\}$, there exists a homomorphism $\overline{\varphi}\colon G/N \to H$ satisfying $\overline{\varphi}(\overline{g}) = \varphi(g)$ for any $g \in G$. We say that a group G is *simple*, if G does not have normal subgroups other than G itself and $\{1_G\}$. For a subset X of a group G, let $\langle X \rangle$ denote the subgroup of G generated by X. We define the *normal closure* of a subset X, denoted by $\langle X \rangle_{\mathrm{normal}}$, to be the subgroup generated by $\{gxg^{-1} \mid x \in X, g \in G\}$.

For any integer $n \geq 1$, let S_n denote the symmetric group on n letters, i.e., the group of permutations $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ with multiplication defined by the composition of maps. Let A_n denote the alternating group on n letters, i.e., the (normal) subgroup of S_n of permutations that can be written as the product of an even number of transpositions (a, b), $a \neq b$. It is known that A_n is a simple group if $n \geq 5$.

For any field F and any integers $k, \ell \geq 1$, let $M_{k,\ell}(F)$ denote the set of matrices with components in F having k rows and ℓ columns. Let $\mathrm{GL}_k(F)$ denote the general linear group, consisting of the multiplicatively invertible matrices in $M_{k,k}(F)$. Let $\mathrm{SL}_k(F)$ denote the special linear group defined by $\mathrm{SL}_k(F) = \{A \in \mathrm{GL}_k(F) \mid \det(A) = 1\}$. Moreover, let $\mathrm{PSL}_k(F)$ denote the projective special linear group defined by $\mathrm{PSL}_k(F) = \mathrm{SL}_k(F)/N$ where N denotes the normal subgroup of $\mathrm{SL}_k(F)$ consisting of scalar matrices in $\mathrm{SL}_k(F)$. For example, we have $\mathrm{PSL}_2(F) = \mathrm{SL}_2(F)/\{\pm I\}$ where I denotes the identity matrix.

We also give a summary of some basic definitions and facts from combinatorial group theory; see e.g., [24] for those mentioned without explicit references. By a *group word* on a set X we mean a finite-length sequence of symbols of the form x or x^{-1} with $x \in X$. The empty word, denoted by $\emptyset$ or 1, is also regarded as a group word. Let $\mathsf{Free}(X)$ denote the set of group words on X with an additional rule that, two words are identified with each other in $\mathsf{Free}(X)$ if and only if one of the two words can be converted to the other word by a finite number of steps of inserting or deleting a subword of the form xx^{-1} or $x^{-1}x$ with $x \in X$. The set $\mathsf{Free}(X)$ forms a group, with multiplication defined by the concatenation of two words. Moreover, for any set R of group words on X, we define $\langle X \mid R \rangle$ to be the quotient group $\mathsf{Free}(X)/\langle R \rangle_{\mathrm{normal}}$ where the normal closure $\langle R \rangle_{\mathrm{normal}}$ is taken in the group $\mathsf{Free}(X)$. If a group G is isomorphic to $\langle X \mid R \rangle$, then $\langle X \mid R \rangle$ is called a *presentation* of the group G with *generating set* X and set of *fundamental relations* R. In the group $\langle X \mid R \rangle$, two words are identified with each other if and only if one of the two words can be converted to the other word by a finite number of steps of inserting or deleting a subword of the form xx^{-1} or $x^{-1}x$ with $x \in X$ or a subword r belonging to R.

3 Our Framework for FHE

In this section (in particular Section 3.3), we describe our proposed generic framework towards constructing FHE free from ciphertext noise. This is based on the notion of group-theoretic realization of functions (or operators) on plaintext sets introduced in Sections 3.1 and 3.2, and is seen as a concretization of a framework suggested in the previous work [25, 27].

3.1 Group-Theoretic Realization of Functions

Roughly speaking, a group-theoretic realization of a function in a group G is a way to emulate the given function "by using the group operators of G only". To clarify the meaning, first we give the following definition.

Definition 1 (group word)**.** A *group word* $w(x_1, \ldots, x_n)$ with variables $x_1, \ldots, x_n$ is a finite-length sequence of symbols of the form x_i or x_i^{-1} with $i \in \{1, \ldots, n\}$ (cf. Section 2.1). Then one can *substitute* given elements $g_1, \ldots, g_n$ of a group into the variables $x_1, \ldots, x_n$ in the word $w(x_1, \ldots, x_n)$ to yield an element of the same group, denoted by $w(g_1, \ldots, g_n)$.

For example, $w(x_1, x_2) = x_1 x_2 x_2 {x_1}^{-1} {x_1}^{-1}$ is a group word, abbreviated as $x_1 {x_2}^2 {x_1}^{-2}$ in a usual way, and by substituting matrices $g_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ we obtain $w(g_1, g_2) = g_1 {g_2}^2 {g_1}^{-2} = \begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix}$.

By using the notion of group words, we define a group-theoretic realization of functions. We note that our definition here is a generalization of a similar definition made by the previous work [25] from the following two viewpoints. First, our definition is extended to the cases where the underlying group may be composed of two or more direct product components and these components may be dealt with separately in the realization of functions. Secondly, while the definition in [25] is restricted to realizing functions in a deterministic manner, our definition also allows probabilistic realizations of functions. Our definition is as follows:

Definition 2 (group-theoretic realization of functions)**.** Let G be a group and $\mathcal{M}$ be a set. Let $\mathcal{F}$ be a set of functions of the form $f\colon \mathcal{M}^{\ell_f} \to \mathcal{M}$ with $\ell_f \geq 1$. We define a *group-theoretic realization* (or simply a *realization*) *of* $\mathcal{F}$ *in* G to be a collection of the following objects:

- a polynomially bounded integer $n \geq 1$, which we call the *degree* of the realization;
- non-empty and mutually disjoint subsets $X_m \subset G^n$ for all $m \in \mathcal{M}$;
- a collection of n group words $w_{f,i}(\vec{x}_1, \ldots, \vec{x}_{\ell_f}, \vec{y})$ $(i = 1, \ldots, n)$, denoted by $\vec{w}_f(\vec{x}_1, \ldots, \vec{x}_{\ell_f}, \vec{y})$, of polynomially bounded lengths for each $f \in \mathcal{F}$, where we write $\vec{x}_j = (x_{j,1}, \ldots, x_{j,n})$ for $j = 1, \ldots, \ell_f$ and $\vec{y} = (y_1, \ldots, y_k)$ (we note that the latter list $\vec{y}$ of variables may be redundant so that some variable y_h may be not appearing in a group word $w_{f,i}$);
- a collection of n polynomial-time samplable random variables r_h with values in the group G for each $h = 1, \ldots, k$, denoted by $\vec{r}$;

satisfying the following condition:

> For any $f \in \mathcal{F}$, any $m_1, \ldots, m_{\ell_f} \in \mathcal{M}$, and any $\vec{g}_i = (g_{i,1}, \ldots, g_{i,n}) \in X_{m_i}$ $(i = 1, \ldots, \ell_f)$, the probability $\Pr[\vec{w}_f(\vec{g}_1, \ldots, \vec{g}_{\ell_f}, r_1, \ldots, r_k) \notin X_{f(m_1, \ldots, m_{\ell_f})}]$ taken over the random choices of values of $r_1, \ldots, r_k \in G$ is bounded by a common negligible value not depending on f, $m_1, \ldots, m_{\ell_f}$, and $\vec{g}_1, \ldots, \vec{g}_{\ell_f}$.

When it is the case, we denote by $\mathcal{A}_f$ with $f \in \mathcal{F}$ an algorithm that, for given inputs $\vec{g}_1, \ldots, \vec{g}_{\ell_f} \in G^n$, outputs $\vec{w}_f(\vec{g}_1, \ldots, \vec{g}_{\ell_f}, r_1, \ldots, r_k) \in G^n$ where the values of random variables $r_1, \ldots, r_k$ are sampled according to the specified distributions.

We note that the formulation above includes the special cases where some of the random variables r_h takes a constant value in G. When all the random variables appearing in a realization of functions are constant, we call the realization *deterministic*, or else call it *probabilistic*. Concrete examples of such (deterministic or probabilistic) realizations of functions will be given in Section 4.

3.2 Lift of Realization of Functions

Given a group homomorphism $\widetilde{G} \to G$ and a realization of functions in the group G, the notion of a "lift" of the realization up to the other group $\widetilde{G}$ plays a central role in our proposed framework. We note that such a notion is not introduced in the previous work [25, 27]. The notion is defined as follows:

Definition 3 (lift of realization of functions)**.** We suppose that a set $\mathcal{F}$ of functions on a set $\mathcal{M}$ has a group-theoretic realization in a group G as in Definition 2. Let $\pi\colon \widetilde{G} \to G$ be a group homomorphism from another group $\widetilde{G}$ onto G. We define a *lift* of the realization of $\mathcal{F}$ *up to* $\widetilde{G}$ to be a collection of polynomial-time samplable random variables $\widetilde{r}_h$ taking values in the group $\widetilde{G}$ for all $h = 1, \ldots, k$ with the property that each value $\pi(\widetilde{r}_h) \in G$ has the same probability distribution as the corresponding random variable r_h. When it is the case, we denote by $\widetilde{\mathcal{A}}_f$ with $f \in \mathcal{F}$ an algorithm that outputs $\vec{w}_f(\vec{\widetilde{g}}_1, \ldots, \vec{\widetilde{g}}_{\ell_f}, \widetilde{r}_1, \ldots, \widetilde{r}_k) \in (\widetilde{G})^n$ for given inputs $\vec{\widetilde{g}}_1, \ldots, \vec{\widetilde{g}}_{\ell_f} \in (\widetilde{G})^n$ where the values of random variables $\widetilde{r}_1, \ldots, \widetilde{r}_k$ are sampled according to the specified distributions.

For example, when the underlying realization of functions is deterministic, it suffices for constructing its lift to choose a constant element $\widetilde{r}_h$ of $\widetilde{G}$ with $\pi(\widetilde{r}_h) = r_h$ for each $h = 1, \ldots, k$.

Lifts of realizations of functions play a role of homomorphic operations in our proposed framework for FHE. The following is a key fact for this purpose; here we also write as π the map $(\widetilde{G})^n \to G^n$ given by $\pi(\widetilde{g}_1, \ldots, \widetilde{g}_n) = (\pi(\widetilde{g}_1), \ldots, \pi(\widetilde{g}_n))$.

Lemma 1. *In the situation of Definition 3, let $f \in \mathcal{F}$, $m_1, \ldots, m_{\ell_f} \in \mathcal{M}$, and let $\vec{\widetilde{g}}_i \in (\widetilde{G})^n$ satisfy $\pi(\vec{\widetilde{g}}_i) \in X_{m_i}$ for each $i = 1, \ldots, \ell_f$. Then the probability $\Pr[\pi(\widetilde{\mathcal{A}}_f(\vec{\widetilde{g}}_1, \ldots, \vec{\widetilde{g}}_{\ell_f})) \notin X_{f(m_1,\ldots,m_{\ell_f})}]$ is bounded by the same negligible value as in Definition 2; hence the bound is again independent of f, $m_1, \ldots, m_{\ell_f}$, and $\vec{\widetilde{g}}_1, \ldots, \vec{\widetilde{g}}_{\ell_f}$.*

Proof. As $\pi\colon \widetilde{G} \to G$ is a group homomorphism, we have

$$\pi(w_{f,i}(\vec{\widetilde{g}}_1, \ldots, \vec{\widetilde{g}}_{\ell_f}, \widetilde{r}_1, \ldots, \widetilde{r}_k)) = w_{f,i}(\pi(\vec{\widetilde{g}}_1), \ldots, \pi(\vec{\widetilde{g}}_{\ell_f}), \pi(\widetilde{r}_1), \ldots, \pi(\widetilde{r}_k))$$

for any $i = 1, \ldots, \ell_f$ and any values of the random variables $\widetilde{r}_h$. By Definition 2, the claim follows from the property in Definition 3 that the probability distribution for each $\pi(\widetilde{r}_h)$ is identical to that for r_h. □

3.3 The Proposed Framework

Based on the definitions in Sections 3.1 and 3.2, here we describe our proposed framework for constructing FHE. Roughly summarizing, the set of plaintexts $\mathcal{M}$ is encoded into the group G^n given as in the group-theoretic realization of functions. The set of ciphertexts is the product of the other group $(\widetilde{G})^n$. A lift up to $\widetilde{G}$ of a realization of operators on $\mathcal{M}$ in G plays a role

of homomorphic operations for the corresponding operators on $\mathcal{M}$. Moreover, a ciphertext of a plaintext $m \in \mathcal{M}$ is generated by rerandomizing an initially provided ciphertext of the m, which is performed by multiplying random elements of the kernel of the group homomorphism $\widetilde{G} \to G$.

Our proposed framework for constructing FHE is as follows:

$\mathsf{Gen}(1^\lambda)$**:** Choose the following objects according to the security parameter λ, where $\mathcal{M}$ denotes the set of plaintexts:

- groups $G, \widetilde{G}$ and a group homomorphism $\pi\colon \widetilde{G} \to G$ between them;
- a group-theoretic realization of a functionally complete set $\mathcal{F}$ of operators on $\mathcal{M}$ in the group G and its lift up to $\widetilde{G}$, where the degree n is dependent solely on λ;
- a polynomial-time samplable random variable $r_{\ker}$ taking values in the set $\ker \pi = \{\widetilde{g} \in \widetilde{G} \mid \pi(\widetilde{g}) = 1_G\}$;
- for each $m \in \mathcal{M}$, a tuple $\vec{\mathsf{gen}}_m = (\mathsf{gen}_{m,1}, \dots, \mathsf{gen}_{m,n}) \in (\widetilde{G})^n$ satisfying $\pi(\vec{\mathsf{gen}}_m) \in X_m$.

Then output a public key pk consisting of $\widetilde{G}$, n, $r_{\ker}$, $\vec{\mathsf{gen}}_m$ for all $m \in \mathcal{M}$, and the algorithms $\widetilde{A}_f$ for all $f \in \mathcal{F}$ appearing in the lift of the realization of $\mathcal{F}$; and output a secret key sk consisting of G, π, and X_m for all $m \in \mathcal{M}$.

$\mathsf{Enc}_{\mathsf{pk}}(m)$ **for** $m \in \mathcal{M}$**:** Sample n values $r_{\ker,1}, \dots, r_{\ker,n}$ of the random variable $r_{\ker}$ independently, and then output $\vec{c} = (c_1, \dots, c_n) \leftarrow \vec{\mathsf{gen}}_m \cdot \vec{r}_{\ker} \in (\widetilde{G})^n$ where $\vec{r}_{\ker} = (r_{\ker,1}, \dots, r_{\ker,n})$.

$\mathsf{Dec}_{\mathsf{sk}}(c)$ **for** $\vec{c} \in (\widetilde{G})^n$**:** Compute $\pi(\vec{c}) \in G^n$, and if $\pi(\vec{c}) \in X_m$ for an $m \in \mathcal{M}$, then output the m. If no such m exists, output $\perp$.

$\mathsf{Eval}_{\mathsf{pk}}(f; \vec{c}_1, \dots, \vec{c}_{\ell_f})$ **for** $f \in \mathcal{F}$ **and** $\vec{c}_1, \dots, \vec{c}_{\ell_f} \in (\widetilde{G})^n$**:** Output $\widetilde{A}_f(\vec{c}_1, \dots, \vec{c}_{\ell_f}) \in (\widetilde{G})^n$.

The correctness of $\mathsf{Enc}_{\mathsf{pk}}$ in the construction above follows easily from the choices of $r_{\ker}$ and $\vec{\mathsf{gen}}_m$; indeed, when $\vec{c} = \vec{\mathsf{gen}}_m \cdot \vec{r}_{\ker} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$ we have

$$\begin{aligned}\pi(\vec{c}) = \pi(\vec{\mathsf{gen}}_m) \cdot \pi(\vec{r}_{\ker}) &= \pi(\vec{\mathsf{gen}}_m) \cdot (\pi(r_{\ker,1}), \dots, \pi(r_{\ker,n})) \\ &= \pi(\vec{\mathsf{gen}}_m) \cdot (1_G, \dots, 1_G) = \pi(\vec{\mathsf{gen}}_m) \in X_m\end{aligned}$$

since $r_{\ker,i} \in \ker \pi$ for each i. The correctness of $\mathsf{Eval}_{\mathsf{pk}}$ is just a restatement of Lemma 1.

For the security, we have the following result:

Theorem 1. *In the setting above, suppose that $\widetilde{G}$ is a finite group with polynomial-time computable group operators, and suppose either $n = 1$ or that the uniform random variable over $\widetilde{G}$ is polynomial-time samplable. Then, our proposed FHE scheme is CPA-secure if the subgroup membership problem for $\ker \pi \subset \widetilde{G}$ with respect to the random variable $r_{\ker}$ with auxiliary input pk 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:*

$$\mathsf{pk} \leftarrow \mathsf{Gen}(1^\lambda)\,;\, b^\dagger \leftharpoonup \{0,1\}\,;\, \begin{cases} g^\dagger \leftharpoonup \widetilde{G} & \textit{(if } b^\dagger = 1\textit{)} \\ g^\dagger \leftarrow r_{\ker} & \textit{(if } b^\dagger = 0\textit{)} \end{cases} : b \leftarrow \mathcal{A}^\dagger(1^\lambda, \mathsf{pk}, g^\dagger)\ .$$

Proof. Let $\mathcal{A}$ be any PPT CPA adversary for our scheme. Then we define an adversary $\mathcal{A}^\dagger$ for the subgroup membership problem specified in the statement as follows:

1. Given inputs 1^λ, pk, and $g^\dagger$ chosen according to the random bit $b^\dagger$, the adversary $\mathcal{A}^\dagger$ chooses $i \leftharpoonup \{1, \dots, n\}$ and executes $\mathcal{A}(\mathrm{submit}, 1^\lambda, \mathsf{pk})$ to obtain a tuple $(m_0, m_1, \mathsf{state})$.

2. The adversary $\mathcal{A}^\dagger$ chooses $b^* \leftarrow\!\!\!\!\circ\ \{0,1\}$, and executes $\mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,b^\dagger,i})$ to obtain a bit b', where

$$c^{b^*,b^\dagger,i} = (\mathsf{gen}_{m_{b^*},1}\rho_1, \ldots, \mathsf{gen}_{m_{b^*},i-1}\rho_{i-1}, \mathsf{gen}_{m_{b^*},i}g^\dagger, \mathsf{gen}_{m_{b^*},i+1}u_{i+1}, \ldots, \mathsf{gen}_{m_{b^*},n}u_n)$$

with independent random values $\rho_1, \ldots, \rho_{i-1}$ of r_{ker} and $u_{i+1}, \ldots, u_n \leftarrow\!\!\!\!\circ\ \widetilde{G}$.

3. The adversary $\mathcal{A}^\dagger$ outputs $b = \mathsf{XOR}(b^*, b')$.

Note that this adversary $\mathcal{A}^\dagger$ is PPT as well as $\mathcal{A}$. Now we have

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

and

$$\Pr[b = 0 \mid b^\dagger = 0] = \Pr[b' = b^* \mid b^\dagger = 0] = \sum_{i=1}^{n} \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,0,i})] \ ,$$

while

$$\Pr[b = 1 \mid b^\dagger = 1] = 1 - \Pr[b' = b^* \mid b^\dagger = 1] = 1 - \sum_{i=1}^{n} \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,1,i})] \ .$$

By the choice of $g^\dagger$, for each $i = 1, \ldots, n-1$ and any choice of b^*, the two tuples $c^{b^*,0,i}$ and $c^{b^*,1,i+1}$ follow the identical probability distribution. Therefore, we have

$$\begin{aligned}
&\Pr[b = 0 \mid b^\dagger = 0] + \Pr[b = 1 \mid b^\dagger = 1] - 1 \\
&= \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,0,n})] - \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,1,1})] \ .
\end{aligned}$$

Now we have

$$c^{b^*,1,1} = (\mathsf{gen}_{m_{b^*},1}g^\dagger, \mathsf{gen}_{m_{b^*},2}u_2, \ldots, \mathsf{gen}_{m_{b^*},n}u_n)$$

and the element $g^\dagger$ when $b^\dagger = 1$ is a uniformly random and independent element of $\widetilde{G}$ as well as $u_2, \ldots, u_n$. This implies that $c^{b^*,1,1}$ is uniformly random over $(\widetilde{G})^n$ regardless of the choice of b^*, therefore we have

$$\Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,1,1}) = \frac{1}{2}$$

and

$$\mathsf{Adv}_{\mathcal{A}^\dagger}(\lambda) = \frac{1}{2n}\left|\Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, c^{b^*,0,n})] - \frac{1}{2}\right| \ .$$

Moreover, we have

$$c^{b^*,0,n} = (\mathsf{gen}_{m_{b^*},1}\rho_1, \ldots, \mathsf{gen}_{m_{b^*},n-1}\rho_{n-1}, \mathsf{gen}_{m_{b^*},n}g^\dagger)$$

and the element $g^\dagger$ when $b^\dagger = 0$ is a random value of r_{ker} as well as $\rho_1, \ldots, \rho_{n-1}$. This implies that $c^{b^*,0,n}$ follows the same probability distribution as $\mathsf{Enc}_{\mathsf{pk}}(m_{b^*})$, therefore we have

$$\mathsf{Adv}_{\mathcal{A}^\dagger}(\lambda) = \frac{1}{2n}\left|\Pr[b^* \leftarrow \mathcal{A}(\mathrm{guess}, 1^\lambda, \mathsf{pk}, \mathsf{state}, \mathsf{Enc}_{\mathsf{pk}}(m_{b^*}))] - \frac{1}{2}\right| = \frac{1}{2n}\mathsf{Adv}_{\mathcal{A}}(\lambda) \ .$$

Since the adversary $\mathcal{A}^\dagger$ is PPT, the assumption in the statement implies that $\mathsf{Adv}_{\mathcal{A}^\dagger}(\lambda)$ is negligible, therefore $\mathsf{Adv}_{\mathcal{A}}(\lambda)$ is also negligible as n is polynomially bounded. This completes the proof. □

4 Examples of Realizations of Functions in Groups

4.1 Deterministic Case: Known Result

The following result (which is restated according to our terminology here) is proved in the previous work [25, 27] (see e.g., Theorem 2.1 of [27]), which shows the existence of realizations of the NAND operator in various non-commutative finite groups.

Proposition 1 ([25, 27])**.** *Let G be any non-commutative finite simple group. Then there exists a deterministic group-theoretic realization of the* NAND *operator in G of degree $n = 1$.*

This result was proved by utilizing the property of the commutator operator $[g, h] = ghg^{-1}h^{-1}$ in a way analogous to Barrington's Theorem [1]. We note that NAND alone forms a functionally complete set of bit operators, therefore it is sufficient for the use in our proposed framework. However, although it is a beautiful result, the result above shows in general the *existence* of such a realization only; and it is expected that the realization implied by the proof might be inefficient when the group G is large, which would restrict the choice of the group G in practical situations. As an example of Proposition 1, Section 6 of [25] gives a concrete realization of NAND in the alternating group $G = A_5$, which is the smallest non-commutative simple group, where the group word for the realization has length 65.

4.2 Deterministic Case: Binary Plaintexts

Here we give another way of realizing bit operators in some small non-commutative groups with degree $n = 1$. Our approach, which we call *approximate-then-correct method*, is completely different from the approach in the previous work [25, 27] based on Barrington's Theorem.

An intuition for our approach can be explained as follows. The two-input OR operator has behavior similar to (or can be "approximated" by) the integer addition + and in fact differs at only one input pair $(1, 1)$ among the four possible input pairs; and the latter operator + is purely an additive group operator and hence seems to be suitable for group-theoretic realization. Now the operator OR will be realized if we can realize the addition + for inputs from $\{0, 1\}$ and then "correct" the output value $2 = 1 + 1$ to $1 = 1 \,\mathsf{OR}\, 1$ while not changing the output values for the other three input pairs. Moreover, according to the same correction function $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 1$, any other bit operator can be also realized provided it can be approximated by a mod-3 affine function in a way that some of the output values 1 may become 2 instead and the other output values are correct. For example, the function $2 - b_1 - b_2 \bmod 3$ approximates the NAND operator for inputs $b_1, b_2 \in \{0, 1\}$ in this sense; the input pair $(b_1, b_2) = (0, 0)$ yields the output 2 instead of 1, while the output is correct for any other input pair. Similarly, the functions $b_2 - b_1 \bmod 3$ and $b_1 + b_2 - 1 \bmod 3$ approximate the XOR operator and the equality operator denoted here by EQ (which returns 1 if two input bits are equal and 0 otherwise) in this manner, respectively.

Based on the observation above, we construct a realization (with parameter $n = 1$) of bit operations NOT, OR, NAND, XOR, and EQ in the symmetric group S_5 as follows. First of all, we define $X_0 = \{\sigma_0\}$ and $X_1 = \{\sigma_1\}$ where $\sigma_0 = 1_{S_5}$ and $\sigma_1 = (1, 2, 3) \in S_5$. For the NOT operator, we define $w_{\mathsf{NOT}} = {x_1}^{-1} y_1$ and $r_1 = \sigma_1$, i.e.,

$$w_{\mathsf{NOT}}(g) = g^{-1}\sigma_1$$

where we omit the constant value $r_1 = \sigma_1$ of y_1 in the input of $w_{\mathsf{NOT}}(x_1, y_1)$ in order to emphasize that w_{NOT} is essentially regarded as a function of x_1 only. Then we indeed have $w_{\mathsf{NOT}}(\sigma_b) = \sigma_{\mathsf{NOT}(b)}$ for any $b \in \{0, 1\}$ as desired.

For the remaining four operators (with two input bits), based on the observation above and the fact that the subgroup $\{\sigma_0, \sigma_1, \sigma_2\}$ of S_5 with $\sigma_2 = {\sigma_1}^2$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ via the map $\sigma_m \mapsto m$, first we define

$$w^{\mathsf{in}}_{\mathsf{OR}}(g_1, g_2) = g_1 g_2 \,,\; w^{\mathsf{in}}_{\mathsf{NAND}}(g_1, g_2) = {g_1}^{-1}{g_2}^{-1}{\sigma_1}^2 \,,$$
$$w^{\mathsf{in}}_{\mathsf{XOR}}(g_1, g_2) = {g_1}^{-1} g_2 \,,\; w^{\mathsf{in}}_{\mathsf{EQ}}(g_1, g_2) = g_1 g_2 {\sigma_1}^{-1}$$

(we note that the definition $w^{\mathsf{in}}_{\mathsf{NAND}}(g_1, g_2) = {g_1}^{-1}{g_2}^{-1}{\sigma_1}^2$ above is an abbreviation and should formally be the combination of $w^{\mathsf{in}}_{\mathsf{NAND}}(x_1, x_2, y_1) = {x_1}^{-1}{x_2}^{-1}{y_1}^2$ and $r_1 = \sigma_1$; and similarly for the other operators OR, XOR, and EQ). Secondly, to realize the "correction" function $\sigma_0 \mapsto \sigma_0$, $\sigma_1 \mapsto \sigma_1$, $\sigma_2 = {\sigma_1}^2 \mapsto \sigma_1$, we define

$$w^{\mathsf{out}}(g) = (1,5)(2,3,4)g(2,3,4)g(3,4)g^2(2,3)(4,5)g(2,3,4)g(3,4)g^2(1,4,2,5)$$

(which is again an abbreviation of the combination of a group word of the form $w^{\mathsf{out}}(x_1, \vec{y})$ and the elements $r_h \in S_5$ being appeared in the right-hand side). Then a straightforward calculation shows that we have $w^{\mathsf{out}}(\sigma_0) = \sigma_0$ and $w^{\mathsf{out}}(\sigma_1) = w^{\mathsf{out}}(\sigma_2) = \sigma_1$ as desired. Hence, for each operator $* \in \{\mathsf{OR}, \mathsf{NAND}, \mathsf{XOR}, \mathsf{EQ}\}$, by substituting the group word w^{in}_* into the variable in the group word w^{out} we obtain a group word $w_*(x_1, x_2) = w^{\mathsf{out}}(w^{\mathsf{in}}_*(x_1, x_2))$ for realizing the operator $*$ in the group S_5; we have $w_*(\sigma_{b_1}, \sigma_{b_2}) = \sigma_{b_1 * b_2}$ for any $b_1, b_2 \in \{0, 1\}$.

4.3 Deterministic Case: Ternary Plaintexts

The idea of our approximate-then-correct method explained in Section 4.2 can be extended to the case of realization of modular arithmetic operators $+, \times$ over $\mathbb{Z}/3\mathbb{Z}$. We take the group $G = S_5$ and choose the subsets $X_m = \{\sigma_m\}$ for $m = 0, 1, 2$ where $\sigma_0 = 1_{S_5}$, $\sigma_1 = (1,2,3) \in S_5$, and $\sigma_2 = {\sigma_1}^2 = (1,3,2) \in S_5$. Then, owing to the group isomorphism $\{\sigma_0, \sigma_1, \sigma_2\} \to \mathbb{Z}/3\mathbb{Z}$ given by $\sigma_m \mapsto m$, the operator $+$ can be realized by the group word $w_+(x_1, x_2) = x_1 x_2$.

On the other hand, to realize the other operator $\times$, first we define

$$w^{\mathsf{in}}_{\times}(x_1, x_2) = x_1((1,4)(2,3,5))^{-1} x_2 (1,4)(2,3,5) \;\; .$$

Then, by putting

$$X'_0 = \{1_{S_5}, (2,4,5), (2,5,4), (1,2,3), (1,3,2)\} \subset S_5 \;\; ,$$
$$X'_1 = \{(1,2,4,5,3), (1,3,2,5,4)\} \subset S_5 \;\; ,$$
$$X'_2 = \{(1,2,5,4,3), (1,3,2,4,5)\} \subset S_5 \;\; ,$$

we have $w^{\mathsf{in}}_{\times}(\sigma_{m_1}, \sigma_{m_2}) \in X'_{m_1 m_2}$ for any $m_1, m_2 \in \mathbb{Z}/3\mathbb{Z}$ by a straightforward calculation. Hence, it suffices to realize in S_5 a function that maps elements of X'_m to σ_m for each $m \in \mathbb{Z}/3\mathbb{Z}$. For the purpose, we define

$$w'_1(x) = x^3 \,,\; w'_2(x) = (2,3,4)^{-1}x^{-1}(3,4,5)x^2(3,4,5)^{-1}x(2,3,4) \,,\; w'_3(x) = w'_2(x) \,,$$
$$w'_4(x) = x(1,5,3,4,2)x^{-1}(1,5,3,4,2)^{-1}x(1,4,2,3,5)x^{-1}(1,4,2,3,5)^{-1}$$

and define

$$w^{\mathsf{out}}(x) = w'_4(w'_3(w'_2(w'_1(x)))) \;\; .$$

We verify that this w^{out} satisfies the required condition step by step. First, by putting

$$X^{(1)}_0 = \{1_{S_5}\} \,,\; X^{(1)}_1 = \{(1,5,2,3,4), (1,5,3,4,2)\} \,,$$
$$X^{(1)}_2 = \{(1,4,2,3,5), (1,4,3,5,2)\} \,,$$

we have $w'_1(g) \in X_m^{(1)}$ for any $m \in \mathbb{Z}/3\mathbb{Z}$ and any $g \in X'_m$. Secondly, by putting

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

we have $w'_2(g) \in X_m^{(2)}$ for any $m \in \mathbb{Z}/3\mathbb{Z}$ and any $g \in X_m^{(1)}$. Thirdly, 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, by putting

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

we have $w'_3(g) \in X_m^{(3)}$ for any $m \in \mathbb{Z}/3\mathbb{Z}$ and any $g \in X_m^{(2)}$. Finally, we have $w'_4(g) = \sigma_m$ for any $m \in \mathbb{Z}/3\mathbb{Z}$ and any $g \in X_m^{(3)}$. By summarizing the argument above, we have $w^{\mathsf{out}}(g) = \sigma_m$ for any $m \in \mathbb{Z}/3\mathbb{Z}$ and any $g \in X'_m$ as desired; hence the group word $w_\times(x_1,x_2) = w^{\mathsf{out}}(w^{\mathsf{in}}(x_1,x_2))$ realizes the operator $\times$ on $\mathbb{Z}/3\mathbb{Z}$.

4.4 Preliminaries: On Random Sampling of Group Elements

As a preliminary for constructing probabilistic realizations of bit operators in Sections 4.5 and 4.6, here we recall the following result by Dixon [12] on sampling an almost uniformly random element of any finite group G.

We introduce a notation to clarify the result. For any elements $g_1,\ldots,g_L$ of the group G, let $\mathsf{Sample}[g_1,\ldots,g_L]$ denote the random variable that takes the value ${x_1}^{e_1}\cdots{x_L}^{e_L} \in G$ where $e_1,\ldots,e_L \leftarrowtail \{0,1\}$. Then the result is as follows:

Proposition 2 ([12], Theorem 3)**.** *Let G be a finite group, let $0 \le \varepsilon < 1$, and let $\mathcal{U}$ be a random variable taking a value in G that is ε-close to the uniform random variable on G. Let L be a positive integer, and let $h,k \ge 0$. If*

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

then we have $\Pr_{x_1,\ldots,x_L \leftarrowtail \mathcal{U}}[\mathsf{Sample}[x_1,\ldots,x_L]$ *is not* 2^{-k}*-close to uniform* $] < 2^{-h}$.

4.5 Probabilistic Case: Some Matrix Groups

Here we give a probabilistic realization of degree $n = 2$ of bit operators NOT and AND in a certain appropriate group G specified below. First, we define

$$X_0 = \{\vec{g} \in G^2 \mid g_1 \ne 1_G\,,\ g_2 = 1_G\}\,,\ X_1 = \{\vec{g} \in G^2 \mid g_1 \ne 1_G\,,\ g_2 = g_1\}\ .$$

For the operator NOT, we define

$$w_{\mathsf{NOT},1}(\vec{x}) = x_1\,,\ w_{\mathsf{NOT},2}(\vec{x}) = {x_2}^{-1}x_1\ .$$

Then it follows immediately that $(w_{\mathsf{NOT},1}(\vec{g}), w_{\mathsf{NOT},2}(\vec{g})) \in X_{\mathsf{NOT}(b)}$ for any $b \in \{0,1\}$ and any $\vec{g} \in X_b$ as desired, regardless of the choice of the group G.

On the other hand, the correctness of the following construction for the operator AND depends on the choice of the group G. We define

$$w_{\mathsf{AND},1}(\vec{x},\vec{x'},y_1) = [y_1x_1{y_1}^{-1},x'_1]\,,\ w_{\mathsf{AND},2}(\vec{x},\vec{x'},y_1) = [y_1x_2{y_1}^{-1},x'_2]$$

where $[g,h] = ghg^{-1}h^{-1}$ denotes the commutator operator, and define r_1 to be the uniform random variable over G. Namely, for $\vec{g},\vec{g'} \in G^2$ we have

$$\vec{w}_{\mathsf{AND}}(\vec{g},\vec{g'}) = ([ug_1u^{-1},g'_1],[ug_2u^{-1},g'_2]) \in G^2 \text{ with } u \leftarrowtail G\ .$$

Now if $\vec{g} \in X_0$, then we have $g_2 = 1_G$ and hence

$$w_{\mathsf{AND},2}(\vec{g}, \vec{g'}) = [ug_2u^{-1}, g'_2] = [1_G, g'_2] = 1_G$$

by the property of the commutator. Similarly, if $\vec{g'} \in X_0$, then we have $g'_2 = 1_G$ and hence

$$w_{\mathsf{AND},2}(\vec{g}, \vec{g'}) = [ug_2u^{-1}, g'_2] = [ug_2u^{-1}, 1_G] = 1_G$$

by the property of the commutator again. Moreover, if $\vec{g}, \vec{g'} \in X_1$, then we have $g_2 = g_1$ and $g'_2 = g'_1$, therefore

$$w_{\mathsf{AND},2}(\vec{g}, \vec{g'}) = [ug_2u^{-1}, g'_2] = [ug_1u^{-1}, g'_1] = w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) \ .$$

By these properties, for any $b, b' \in \{0, 1\}$, $\vec{g} \in X_b$, and $\vec{g'} \in X_{b'}$, we have $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'}) \in X_{\mathsf{AND}(b,b')}$ as desired *provided* $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) = [ug_1u^{-1}, g'_1] \neq 1_G$ *holds*.

However, the condition $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) = [ug_1u^{-1}, g'_1] \neq 1_G$ for the correctness is not always satisfied for given $\vec{g}$, $\vec{g'}$, and random $u \in G$. For example, we must have $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) = 1_G$ when $\vec{g} = \vec{g'}$ and $u = 1_G$. In fact, whether the failure probability $\Pr[w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) = 1_G]$ can be bounded by a negligible value for any given $\vec{g}, \vec{g'} \in X_0 \cup X_1$ or not depends heavily on the structure of the group G (as an easy example, this condition is never satisfied by a commutative group G since now the commutator always takes the value 1_G). Regarding this issue, we introduce the following definition:

Definition 4 (commutator-separable groups)**.** Let $\varepsilon > 0$. We say that a finite group G is *ε-commutator-separable*, if there exists a non-empty subset Y of $G \setminus \{1_G\}$ satisfying

$$\Pr_{u \leftarrow G}[\ [ugu^{-1}, g'] \notin Y\ ] \leq \varepsilon \text{ for any } g, g' \in Y. \tag{1}$$

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

Now suppose that G is commutator-separable in this sense. Then, by modifying the definition of the subsets X_0, X_1 of G as

$$X_0 = \{\vec{g} \in G^2 \mid g_1 \in Y\ ,\ g_2 = 1_G\}\ ,\ X_1 = \{\vec{g} \in G^2 \mid g_1 \in Y\ ,\ g_2 = g_1\}$$

where Y is the subset of G yielded by Definition 4, it follows, by combining the argument above with the property (1), that the construction above indeed provides a probabilistic realization of degree 2 of the operators NOT and AND in the group G.

Remark 1. Although only the *existence* of such a subset Y is concerned in Definition 4, the efficient samplability of an element of Y is needed to be used as a part of our proposed framework for FHE. In general, this is at least probabilistically achievable if the ratio $|G \setminus Y|/|G|$ is negligible; now a uniformly random element of G is also an element of Y except for a negligible probability.

From now, as a concrete example, we show that the special linear group $\mathrm{SL}_2(\mathbb{F}_q)$ of size two over q-element finite field $\mathbb{F}_q$ and the projective special linear group $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ of size two are commutator-separable, if q is sufficiently large so that the value $1/q$ is negligible. We present some lemmas for the purpose. First we fix a notation: 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. Now we have the following result:

Lemma 2. *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

$$\begin{aligned}(gx_1g^{-1})x_2(gx_1g^{-1})^{-1}x_2{}^{-1} &= [gx_1g^{-1}, x_2] \\ &= [g_yx_1g_y{}^{-1}, x_2] = (g_yx_1g_y{}^{-1})x_2(g_yx_1g_y{}^{-1})^{-1}x_2{}^{-1} \ ,\end{aligned}$$

therefore $(g_yx_1g_y{}^{-1})^{-1}(gx_1g^{-1}) \in Z_H(x_2)$. Now for each $h \in Z_H(x_2)$, we put

$$H_{y,h} = \{g \in H_y \mid (g_yx_1g_y{}^{-1})^{-1}(gx_1g^{-1}) = h\} \ .$$

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 $gx_1g^{-1} = g_yx_1g_y{}^{-1} \cdot h = g_{y,h}x_1g_{y,h}{}^{-1}$, 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

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

This completes the proof. □

Before moving to 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 result:

Lemma 3. *Let $\varphi\colon H_1 \to H_2$ be a surjective group 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

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

This completes the proof. □

In contrast to the general argument above, the following result is specific to our choice of the group here.

Lemma 4. *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

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

therefore

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

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. □

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 3 and 4 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 2. *If the finite field $\mathbb{F}_q$ satisfies*

$$\frac{8q}{q^2-1} \leq \varepsilon \, , \quad \textit{or equivalently} \quad q \geq \frac{4 + \sqrt{16+\varepsilon^2}}{\varepsilon} \approx \frac{8}{\varepsilon} \ ,$$

then $\mathrm{SL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q)$ are ε-commutator-separable with the subsets $Y = \mathrm{SL}_2(\mathbb{F}_q) \setminus \{\pm I\}$ and $Y = \mathrm{PSL}_2(\mathbb{F}_q) \setminus \{1_{\mathrm{PSL}_2(\mathbb{F}_q)}\}$, 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 $H = \mathrm{PSL}_2(\mathbb{F}_q)$. We also note that $|H \setminus Y| = 2/\eta$ for this value η. Now for any $x_1, x_2 \in Y$, Lemma 4 and Corollary 1 imply that $|Z_H(x_1)|, |Z_H(x_2)| \leq 2q$. Therefore, by Lemma 2, we have

$$\Pr_{g \leftarrow\!\!\shortmid H}[\ [g x_1 g^{-1}, x_2] \notin Y\ ] = \Pr_{g \leftarrow\!\!\shortmid H}[\ [g x_1 g^{-1}, x_2] \in H \setminus Y\ ] \leq \frac{(2/\eta) \cdot 2q \cdot 2q}{q(q^2-1)/\eta} = \frac{8q}{q^2-1} \leq \varepsilon$$

by the condition for q in the statement. This completes the proof. □

4.6 Probabilistic Case: Simple Groups

We also give a variant of the probabilistic realization of bit operators NOT and AND described in Section 4.5. Although the correctness of the realization here relies on a heuristic assumption given below, the underlying group G for the realization can be taken as any non-commutative finite simple group that is sufficiently large, more precisely, provided $1/|G|$ is negligible.

Let G be a non-commutative finite simple group as mentioned above. The definitions of subsets X_0, X_1 and the group word for the operator NOT are similar to Section 4.5. Namely,

$$X_0 = \{\vec{g} \in G^2 \mid g_1 \neq 1_G \, , \, g_2 = 1_G\} \, , \, X_1 = \{\vec{g} \in G^2 \mid g_1 \neq 1_G \, , \, g_2 = g_1\}$$

and

$$w_{\mathsf{NOT},1}(\vec{x}) = x_1 \,,\; w_{\mathsf{NOT},2}(\vec{x}) = {x_2}^{-1} x_1 \;\; .$$

Then we have $(w_{\mathsf{NOT},1}(\vec{g}), w_{\mathsf{NOT},2}(\vec{g})) \in X_{\mathsf{NOT}(b)}$ for any $b \in \{0,1\}$ and any $\vec{g} \in X_b$.

To consider the AND operator, first we note that, for any $g \in G \setminus \{1_G\}$, the simple group G is generated by the elements of the form ugu^{-1} with $u \in G$; indeed, the normal closure of g must coincide with the whole G. Keeping this property in mind, we put the following heuristic assumption:

Assumption 1. Let $\varepsilon > 0$, and let L be a sufficiently large parameter. We assume that, for any $g \in G \setminus \{1_G\}$, the probability distribution of the element $u_1 g {u_1}^{-1} \cdots u_L g {u_L}^{-1} \in G$, where $u_1, \ldots, u_L \leftarrow\!\!\!\!\!\!\rightharpoonup G$, is ε-close to the uniform distribution over G.

Now let $\varepsilon > 0$ be a negligible value, and let the parameter L be as in Assumption 1. We define

$$\begin{aligned} w_{\mathsf{AND},1}(\vec{x}, \vec{x'}, y_1, \ldots, y_{2L}) &= [y_1 x_1 {y_1}^{-1} \cdots y_L x_1 {y_L}^{-1}, y_{L+1} x'_1 {y_{L+1}}^{-1} \cdots y_{2L} x'_1 {y_{2L}}^{-1}] \,, \\ w_{\mathsf{AND},2}(\vec{x}, \vec{x'}, y_1, \ldots, y_{2L}) &= [y_1 x_2 {y_1}^{-1} \cdots y_L x_2 {y_L}^{-1}, y_{L+1} x'_2 {y_{L+1}}^{-1} \cdots y_{2L} x'_2 {y_{2L}}^{-1}] \,, \end{aligned}$$

and define the random variables $r_1, \ldots, r_{2L}$ to be the uniform random variable over G. Then an argument similar to Section 4.5 implies that, for $b, b' \in \{0,1\}$, $\vec{g} \in X_b$ and $\vec{g'} \in X_{b'}$, we have $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'}) \in X_{\mathsf{AND}(b,b')}$ as desired *provided* $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) \neq 1_G$ *holds*. To evaluate the probability of not satisfying the condition $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) \neq 1_G$, we use the following result by Guralnick and Robinson [21]:

Proposition 3 ([21], Theorem 9)**.** *For any non-commutative finite simple group H, we have*

$$\Pr_{h_1, h_2 \leftarrow\!\!\!\!\!\!\rightharpoonup H}[\; [h_1, h_2] = 1_H \;] \leq |H|^{-1/2} \;\; .$$

Then we have the following result:

Theorem 3. *For the group G as above, assume that Assumption 1 holds. Then for any $\vec{g}, \vec{g'} \in X_0 \cup X_1$, we have*

$$\Pr_{r_1, \ldots, r_{2L} \leftarrow\!\!\!\!\!\!\rightharpoonup G}[w_{\mathsf{AND},1}(\vec{g}, \vec{g'}, r_1, \ldots, r_{2L}) = 1_G] \leq |G|^{-1/2} + 2\varepsilon \;\; .$$

Hence the definition above gives a probabilistic realization of degree 2 of the operators NOT *and* AND *in G if both $1/|G|$ and ε are negligible.*

Proof. The latter part of the claim follows from the former part and the argument above. For the former part of the claim, first, if the elements

$$h_1 = r_1 g_1 {r_1}^{-1} \cdots r_L g_1 {r_L}^{-1} \text{ and } h_2 = r_{L+1} g'_1 {r_{L+1}}^{-1} \cdots r_{2L} g'_1 {r_{2L}}^{-1} \tag{2}$$

were uniformly random over G, then by Proposition 3, we would have $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}, r_1, \ldots, r_{2L}) = [h_1, h_2] = 1_G$ with probability at most $|G|^{-1/2}$. Now we note that $g_1 \neq 1_G$ and $g'_1 \neq 1_G$ since $\vec{g}, \vec{g'} \in X_0 \cup X_1$, therefore Assumption 1 implies that the probability distributions of h_1 and h_2 are independent and both ε-close to the uniform distribution over G. Hence, in fact, we have $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}, r_1, \ldots, r_{2L}) = 1_G$ with probability at most $|G|^{-1/2} + 2\varepsilon$. This completes the proof. □

5 Towards Achieving Secure Lift of Realization

In this section, we give some observations towards constructing a lift of a group-theoretic realization of operators for plaintexts (see Section 4) that will yield a secure FHE scheme based on our framework in Section 3. More precisely, though we give a candidate construction of such a lift, the resulting FHE scheme has an issue that the sizes of ciphertexts are not bounded, hence the scheme is currently so-called *non-compact* FHE. Realization of *compact* FHE (i.e., FHE in the usual sense) based on the strategy in this paper is left as a future research topic.

5.1 A Remark on the Choice of Random Variables

Here we give a remark on the construction of random variables $\widetilde{r}_h$ involved in a lift of a group-theoretic realization of functions. First, for realizations of functions using a uniform random variable on a given group G, such as those in Sections 4.5 and 4.6, it may happen that sampling a uniformly random element of the other group $\widetilde{G}$ is not easy even if uniformly random sampling of elements of G is easy. In such a case, owing to Proposition 2, a uniform random variable on G may be approximated as follows: a sufficiently large number of random elements $g_1, \ldots, g_L$ of G are chosen at the beginning, and a random element of G is chosen for each time by taking ${g_1}^{e_1} \cdots {g_L}^{e_L}$ with $e_1, \ldots, e_L \leftarrow\!\!\!\!\!\rightarrow \{0,1\}$. Provided L is sufficiently large, this approximation will work well except for a negligible probability for the choice of $g_1, \ldots, g_L$, and now the uniform random variable on G is replaced by the collection of L random variables, the i-th of which takes values 1_G and g_i with probabilities $1/2$ each. Then the corresponding random variables on $\widetilde{G}$ can be constructed by choosing an element $\widetilde{g}_i \in \widetilde{G}$ with $\pi(\widetilde{g}_i) = g_i$ (yielding a random variable taking values $1_{\widetilde{G}}$ and $\widetilde{g}_i$ with probabilities $1/2$ each) for each $i = 1, \ldots, L$, which is expected to be not difficult.

On the other hand, for the random variable r_{ker} used by the algorithm $\mathsf{Gen}(1^\lambda)$ in our proposed framework, it may also happen that sampling a uniformly random element of the subgroup $\ker \pi$ of $\widetilde{G}$ seems not easy. An approach similar to the previous paragraph would be useful in such a case: namely, we may choose a large number of elements $g'_1, \ldots, g'_{L'}$ of $\ker \pi$ first and then generate an element of $\ker \pi$ for each time by randomly multiplying the elements $g'_1, \ldots, g'_{L'}$. It is naively expected that the probability distribution of the resulting element of $\ker \pi$ will be significantly random if L' is sufficiently large.

5.2 Insecurity of a Matrix-Based Naive Construction

In order to exhibit the difficult point in the problem, here we show an example of an *insecure* construction of a lift of a realization of functions and explain why the resulting FHE scheme based on this construction is not secure.

We start with the realization of the AND and NOT operators in the group $G = \mathrm{SL}_2(\mathbb{F}_q)$ proposed in Section 4.5. We define the corresponding group $\widetilde{G}$ by

$$\widetilde{G} = \left\{ T \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} T^{-1} \mid A \in \mathrm{SL}_2(\mathbb{F}_q), B \in M_{2,k}(\mathbb{F}_q), C \in \mathrm{GL}_k(\mathbb{F}_q) \right\}$$

where k is a parameter and $T \in \mathrm{GL}_{k+2}(\mathbb{F}_q)$ is a fixed, randomly chosen matrix that must be secret. Then the group homomorphism $\pi\colon \widetilde{G} \to G$ is defined as follows: for $g \in \widetilde{G}$, $\pi(g)$ is obtained by first computing the $(k+2) \times (k+2)$ matrix $T^{-1}gT$ and then extracting the upper-left 2×2 block of $T^{-1}gT$. The conjugation by the random T in the definition of $\widetilde{G}$ intends to hide the internal block upper-triangular structure (i.e., the part $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$) of elements of $\widetilde{G}$.

However, this construction is not secure by the following reason (this attack was pointed out by an anonymous reviewer in a previous submission of this work). First, any matrix of

the form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ with $A = I \in \mathrm{SL}_2(\mathbb{F}_q)$ satisfies a constraint "the first column of the second row is zero", which is a *linear* constraint in terms of the components of the matrix. By taking conjugation by the matrix T, this constraint is changed to another constraint, which is more complex but still a *linear* constraint in terms of the components of the matrix. We denote the resulting constraint by "$F(g) = 0$"; namely, any element g of $\ker \pi$ (i.e., element with the component A in the form above being I) satisfies $F(g) = 0$.

Now we consider the linear subspace $\mathsf{span}(\ker \pi)$ generated by the set $\ker \pi$ in the matrix *ring* $M_{k+2,k+2}(\mathbb{F}_q)$. By the choice of the *linear* constraint F, $\mathsf{span}(\ker \pi)$ is a linear subspace of $V := \{g \in M_{k+2,k+2}(\mathbb{F}_q) \mid F(g) = 0\}$. Now by collecting sufficiently many elements $h_1, \ldots, h_L$ of $\ker \pi$, it is expected that $\mathsf{span}(\ker \pi)$ is generated by these elements $h_1, \ldots, h_L$. In this case, for a given element $g \in \widetilde{G}$, if $g \in \ker \pi$, then by adding g to the subspace $\mathsf{span}(h_1, \ldots, h_L)$ generated by $h_1, \ldots, h_L$ (which is now equal to $\mathsf{span}(\ker \pi)$), the dimension of the subspace is not increased. On the other hand, if $g \notin \ker \pi$, then the constraint $F(g) = 0$ is not satisfied with high probability, and now the dimension is increased by one when g is added to $\mathsf{span}(h_1, \ldots, h_L)$ since $\mathsf{span}(h_1, \ldots, h_L) \subset V$ and $g \notin V$. This yields a way for an adversary to decide whether a given $g \in \widetilde{G}$ belongs to $\ker \pi$ or not (hence to break the proposed FHE) by only comparing the dimensions of $\mathsf{span}(h_1, \ldots, h_L)$ and $\mathsf{span}(h_1, \ldots, h_L, g)$ even if the actual constraint F is not known to the adversary. This example suggests that the existence of a non-trivial *linear* constraint for the set $\ker \pi$ will yield a powerful tool for the adversary.

5.3 Preliminaries on Combinatorial Group Theory

For the sake of arguments in the following subsections, here we summarize some more definitions and facts from combinatorial group theory; see e.g., [24] for those mentioned without explicit references.

First, the following efficient presentations of the groups $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ are given by Guralnick et al. [20]. Here we introduce a notation: for an integer $m > 0$ with base-4 expression $m = \sum_{j=0}^{k} m_j 4^j$ and symbols u, h_2, we write $E(u, m; h_2) = u^{m_0} {h_2}^{-1} \cdots u^{m_{k-1}} {h_2}^{-1} u^{m_k} {h_2}^{k}$.

Proposition 4 ([20], Theorem 3.6 and Remark 3.7)**.** *Let $p > 3$ be a prime. Let j be a generator of the group ${\mathbb{F}_p}^{\times}$. Let $\overline{2}$ and $\overline{j}$ denote the multiplicative inverses of 2 and j modulo p, respectively. Then the group $\mathrm{SL}_2(\mathbb{F}_p)$ admits a presentation $\langle S \mid R \rangle$, where $S = \{u, h_2, h, t\}$ and R consists of the following words*

$$E(u, p; h_2)\,,\ {h_2}^{-1} u h_2 u^{-4}\,,\ h^{-1} u h E(u, j^2; h_2)^{-1}\,,\ t^2 u t^{-2} u^{-1}\,,\ t^{-1} h t h\,,\ t^{-1} u t^{-1} u t u\,,$$
$$t^{-1} {h_2}^{-1} E(u, \overline{2}; h_2) t^{-1} u^2 t E(u, \overline{2}; h_2)\,,\ t^{-1} h^{-1} E(u, \overline{j}; h_2) t^{-1} E(u, j; h_2) t E(u, \overline{j}; h_2)\ .$$

In the presentation, the generators in S correspond to the following elements of $\mathrm{SL}_2(\mathbb{F}_p)$:

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ h_2 = \begin{pmatrix} \overline{2} & 0 \\ 0 & 2 \end{pmatrix},\ h = \begin{pmatrix} \overline{j} & 0 \\ 0 & j \end{pmatrix}\ .$$

Similarly, a presentation of the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is obtained by replacing the word $t^2 u t^{-2} u^{-1} \in R$ in the presentation above with the word t^2.

The following result on presentations of direct products of groups is known:

Proposition 5 (see e.g., [24])**.** *Let $\langle S_i \mid R_i \rangle$, $i = 1, 2$, be two presentations of groups with $S_1 \cap S_2 = \emptyset$. Then the direct product of these two groups admits a presentation $\langle S_1 \cup S_2 \mid R_1 \cup R_2 \cup \{{s_1}^{-1} {s_2}^{-1} s_1 s_2 \mid s_1 \in S_1\,,\ s_2 \in S_2\} \rangle$.*

We also have the following two results on generating a new presentation of a group from a given presentation. The former is a consequence of the property of *Tietze transformation* and intuitively means that we can add any element of the group to its generating set without changing the group structure.

Lemma 5 (see e.g., [24])**.** *Given a presentation $\langle X \mid R\rangle$ of a group, let w be a group word on X and let y be a symbol not belonging to X. Then the group $\langle X \cup \{y\} \mid R \cup \{wy^{-1}\}\rangle$ is isomorphic to $\langle X \mid R\rangle$ where each element of X in the group $\langle X \mid R\rangle$ corresponds to the same element in the group $\langle X \cup \{y\} \mid R \cup \{wy^{-1}\}\rangle$.*

Lemma 6. *Given a presentation $\langle X \mid R\rangle$ of a group, let $\langle Y \mid T\rangle$ be a presentation of the trivial group (i.e., the group of size one), and for each element $y \in Y$, choose an element r_y of R. Let $T(r_y \mid y \in Y)$ denote the set of words of the form $t(r_y \mid y \in Y)$ with $t(\vec{y}) \in T$, where $t(r_y \mid y \in Y)$ denotes the group word on X obtained by substituting the word r_y into the variable y in the word $t(\vec{y})$ for each $y \in Y$. Then the subsets R and $R' := (R \setminus \{r_y \mid y \in Y\}) \cup T(r_y \mid y \in Y)$ have the same normal closure in $\mathsf{Free}(X)$, therefore $\langle X \mid R'\rangle$ is isomorphic to $\langle X \mid R\rangle$.*

Proof. The definition of the words $t(r_y \mid y \in Y)$ implies that $R' \subset \langle R\rangle_{\mathrm{normal}}$. To prove the opposite relation $R \subset \langle R'\rangle_{\mathrm{normal}}$, it suffices to show that $r_y \in \langle R'\rangle_{\mathrm{normal}}$ for each $y \in Y$. Now by the assumption that $\langle Y \mid T\rangle$ is a trivial group, y is the product of words of the form $u(\vec{y})t(\vec{y})u(\vec{y})^{-1}$ with $u(\vec{y}) \in \mathsf{Free}(Y)$ and $t(\vec{y}) \in T$. By substituting the word $r_{y'}$ into the variable y' for each $y' \in Y$, it follows that r_y is the product of words of the form $u(r_{y'} \mid y' \in Y)t(r_{y'} \mid y' \in Y)u(r_{y'} \mid y' \in Y)^{-1}$ with $u(r_{y'} \mid y' \in Y) \in \mathsf{Free}(X)$ and $t(r_{y'} \mid y' \in Y) \in T(r_{y'} \mid y' \in Y)$. This implies that $r_y \in \langle R'\rangle_{\mathrm{normal}}$, as desired. This completes the proof. □

We also give a brief summary of the theory of Coxeter groups; see e.g., [23] for the definitions and facts mentioned without explicit references. A *Coxeter matrix* of size n is an $n \times n$ matrix $\Gamma = (\Gamma_{ij})_{i,j\in\{1,\dots,n\}}$ satisfying that $\Gamma_{ii} = 1$ for $i = 1, \dots, n$ and $\Gamma_{ij} = \Gamma_{ji} \in \{2, 3, \dots\} \cup \{\infty\}$ for any $i \neq j$. Then the *Coxeter group* $W(\Gamma)$ with Coxeter matrix Γ is the group defined by the presentation $\langle S \mid R\rangle$ with the generating set $S = \{s_1, \dots, s_n\}$ and the set of fundamental relations R consisting of the words $(s_i s_j)^{\Gamma_{ij}}$ for each $i \leq j$ with $\Gamma_{ij} \neq \infty$. In particular, the set R always involves the words ${s_i}^2$ for $i = 1, \dots, n$, which allows one to freely replace the symbol ${s_i}^{-1}$ in a given word with s_i and hence implies that any element of the group $W(\Gamma)$ can be expressed by a word with symbols $s_1, \dots, s_n$ only (not using symbols ${s_1}^{-1}, \dots, {s_n}^{-1}$). For any element w of $W(\Gamma)$, we define the *length* $\ell(w)$ of w to be the length ℓ of the shortest word $s_{i_1} \cdots s_{i_\ell}$ $(s_{i_j} \in S)$ that is equal to w in the group $W(\Gamma)$.

Example 1. We say that a Coxeter matrix Γ of size n is of *type* A, or more precisely *type* A_n, if we have $\Gamma_{i,i+1} = 3$ for $i = 1, \dots, n-1$ and $\Gamma_{ij} = 2$ for any i, j with $|i - j| \geq 2$. Let Γ_{A_n} denote the Coxeter matrix of type A_n. For example,

$$\Gamma_{A_4} = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 3 & 2 \\ 2 & 3 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{pmatrix}$$

and $W(\Gamma_{A_4}) = \langle s_1, s_2, s_3, s_4 \mid R\rangle$ where

$$R = \{{s_1}^2, {s_2}^2, {s_3}^2, {s_4}^2, (s_1s_2)^3, (s_1s_3)^2, (s_1s_4)^2, (s_2s_3)^3, (s_2s_4)^2, (s_3s_4)^3\} \ .$$

It is known that, the Coxeter group $W(\Gamma_{A_n})$ of type A_n is isomorphic to the symmetric group S_{n+1}, where the generator s_i of $W(\Gamma_{A_n})$ with $i \in \{1, \dots, n\}$ corresponds to the adjacent transposition $(i, i+1)$ in S_{n+1}.

Let Γ be a Coxeter matrix of size n. For each generator s_i of $W(\Gamma)$ with $i = 1, \ldots, n$, we define the corresponding matrix $\varphi(s_i) = (\varphi(s_i)_{jk})_{j,k \in \{1,\ldots,n\}}$ by

$$\varphi(s_i)_{ii} = -1\,,\ \varphi(s_i)_{jj} = 1 \text{ and } \varphi(s_i)_{ij} = 2\cos(\pi/\Gamma_{ij}) \text{ for any } j \neq i\,,$$
$$\varphi(s_i)_{jk} = 0 \text{ for any } j \neq i \text{ and } k \neq j\ ,$$

where we interpret $\cos(\pi/\infty) = \cos(0) = 1$ when $\Gamma_{jk} = \infty$. For example, for the Coxeter group $W(\Gamma_{A_4})$ of type A_4 appeared in Example 1, we have (since $\cos(\pi/2) = 0$ and $\cos(\pi/3) = 1/2$)

$$\varphi(s_1) = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ \varphi(s_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$
$$\varphi(s_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ \varphi(s_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}\ .$$

Then the following fact is known for any Coxeter matrix Γ.

Proposition 6 (see e.g., Sections 5.3 and 5.4 of [23])**.** *In the current situation, the map given by $\varphi(s_{i_1}s_{i_2}\cdots s_{i_\ell}) = \varphi(s_{i_1})\varphi(s_{i_2})\cdots\varphi(s_{i_\ell})$ for words $s_{i_1}s_{i_2}\cdots s_{i_\ell}$ with symbols $s_{i_1}, \ldots, s_{i_\ell} \in S$ defines a group isomorphism φ from the Coxeter group $W(\Gamma)$ to the subgroup of $\mathrm{GL}_n(\mathbb{R})$ generated by the matrices $\varphi(s_1), \ldots, \varphi(s_n)$.*

To compute the inverse of the group isomorphism φ yielded by Proposition 6, the following fact is useful.

Proposition 7 (see e.g., Section 5.4 of [23])**.** *In the current situation, let $w \in W(\Gamma)$ and let $i \in \{1, \ldots, n\}$. Then we have $\ell(ws_i) < \ell(w)$ if and only if the i-th column of the matrix $\varphi(w) \in \mathrm{GL}_n(\mathbb{R})$ involves at least one negative component.*

Proposition 7 yields the following recursive algorithm to, given a matrix $g \in \varphi(W(\Gamma))$ as input, construct a word w satisfying $g = \varphi(w)$:

- When $g = I$, the algorithm outputs the empty word.
- When $g \neq I$, the algorithm searches any index i satisfying that the i-th column of g involves at least one negative component. Proposition 7 ensures that such an index i is always found (provided $g \in \varphi(W(\Gamma))$) and then the element $\varphi^{-1}(g \cdot \varphi(s_i))$ of $W(\Gamma)$ has shorter length than $\varphi^{-1}(g)$. Now a recursive procedure yields a word $w' \in W(\Gamma)$ satisfying $g \cdot \varphi(s_i) = \varphi(w')$; then the algorithm outputs the word $w's_i$ (note that ${s_i}^2 = 1$ in $W(\Gamma)$).

We also summarize the following two well-known facts, which will be used in our argument below. The first fact follows immediately from the definition of the Coxeter group $W(\Gamma)$, and the second fact is included in, e.g., [2].

Proposition 8. *Let Γ be any Coxeter matrix, where the indices for the rows (as well as columns) are chosen from a set Λ. Let Λ' be a subset of Λ with the following property: if $i \in \Lambda'$ and $j \in \Lambda \setminus \Lambda'$ then Γ_{ij} is either an even integer or ∞. Moreover, let Γ' be a Coxeter matrix where the indices for the rows (as well as columns) are chosen from the set Λ', and suppose that for any $i, j \in \Lambda'$, we have either $\Gamma_{ij} = \infty$ or that Γ'_{ij} is a divisor (hence not ∞) of Γ_{ij}. For any word w of symbols s_i with $i \in \Lambda$, we denote by w' the word obtained from w by removing all symbols s_i with $i \in \Lambda \setminus \Lambda'$. Then the map that sends a word w in $W(\Gamma)$ to the corresponding word w' in $W(\Gamma')$ defines a surjective group homomorphism from $W(\Gamma)$ to $W(\Gamma')$.*

Example 2. We consider two Coxeter matrices Γ and Γ' given by

$$\Gamma = \begin{pmatrix} 1 & 4 & 2 & 2 \\ 4 & 1 & \infty & 2 \\ 2 & \infty & 1 & 6 \\ 2 & 2 & 6 & 1 \end{pmatrix}, \Gamma' = \begin{pmatrix} 1 & * & 2 & 2 \\ * & * & * & * \\ 2 & * & 1 & 3 \\ 2 & * & 3 & 1 \end{pmatrix}$$

where the symbols $*$ in Γ' means that the second row and the second column are deleted. This corresponds to the case $\Lambda = \{1, 2, 3, 4\}$ and $\Lambda' = \{1, 3, 4\}$ in Proposition 8. Then Proposition 8 yields a surjective group homomorphism $W(\Gamma) \to W(\Gamma')$. For example, this map sends $s_1 s_2 s_3 s_4 s_3 s_2 s_4 s_3 s_2 s_4 \in W(\Gamma)$ to $s_1 s_3 s_4 s_3 s_4 s_3 s_4 \in W(\Gamma')$ by removing all symbols s_2, which is equivalent to the word s_1 in $W(\Gamma')$ owing to the component $\Gamma'_{34} = 3$ of the Coxeter matrix Γ'.

Proposition 9 (see e.g., Theorem 3.3.1 of [2])**.** *Let $W(\Gamma)$ be a Coxeter group, and let w be a word in $W(\Gamma)$ that involves the symbols $s_i \in S$ only (not their inverses ${s_i}^{-1}$). Then w can be converted to an equivalent word w' with the minimal length by using the following kinds of operations only:*

- *for some generator $s_i \in S$, remove a subword of the form ${s_i}^2$;*
- *for some different generators $s_i \neq s_j \in S$ with $\Gamma_{ij} < \infty$, replace a subword of the form $s_i s_j s_i \cdots$ of length Γ_{ij} with a subword $s_j s_i s_j \cdots$ of length Γ_{ij}.*

Example 3. Let $W(\Gamma_{A_4})$ be the Coxeter group of type A_4. Then the element $s_2 s_1 s_2 s_1 s_2 s_4 s_1 s_4$ of $W(\Gamma_{A_4})$ is in fact the identity element (i.e., equivalent to the empty word $\emptyset$), which can be verified by using the two kinds of transformations specified in Proposition 9 as follows:

$s_2 s_1 s_2 s_1 s_2 s_4 \underline{s_1 s_4} \mapsto s_2 s_1 s_2 s_1 s_2 s_4 s_4 s_1$ (using transformation $s_1 s_4 \mapsto s_4 s_1$),
$s_2 s_1 s_2 s_1 s_2 \underline{s_4 s_4} s_1 \mapsto s_2 s_1 s_2 s_1 s_2 s_1$ (removing subword $s_4 s_4$),
$s_2 s_1 s_2 \underline{s_1 s_2 s_1} \mapsto s_2 s_1 s_2 s_2 s_1 s_2$ (using transformation $s_1 s_2 s_1 \mapsto s_2 s_1 s_2$),
$s_2 s_1 \underline{s_2 s_2} s_1 s_2 \mapsto s_2 s_1 s_1 s_2$ (removing subword $s_2 s_2$),
$s_2 \underline{s_1 s_1} s_2 \mapsto s_2 s_2$ (removing subword $s_1 s_1$),
$\underline{s_2 s_2} \mapsto \emptyset$ (removing subword $s_2 s_2$).

5.4 A Candidate Construction for *Non-Compact* FHE

The discussion in Section 5.2 showed that a naive matrix-based construction of the group homomorphism $\pi\colon \widetilde{G} \to G$ to lift the realization of functions in a group G will be insecure due to the existence of a non-trivial linear constraint for the elements of $\ker \pi$. Here we describe an idea aiming at violating such linear constraints among the map π by utilizing combinatorial group theory mentioned in Section 5.3. However, a concrete example of a *finite* group $\widetilde{G}$ constructed in this manner has not been discovered so far; accordingly, we choose an *infinite* group $\widetilde{G}$ in the following example and hence the resulting FHE is a so-called *non-compact* FHE. We note that, though an infinite group $\widetilde{G}$ is out of the scope of Theorem 1, it is still naively expected that the security of the resulting non-compact FHE is also closely related to the computational hardness of recognizing elements of $\ker \pi$. A more detailed analysis of the security of the proposed scheme and a search for a *finite* group $\widetilde{G}$ suitable for the proposed idea are left as future research topics.

To construct the homomorphism $\pi\colon \widetilde{G} \to G$, we start with the group $G = S_5$ in which the bit operators are realized as in Section 4.2. Let d be a sufficiently large integer depending on the security parameter. Let Γ be the Coxeter graph of size d determined by $\Gamma_{ij} = 6$ for any distinct i, j. We randomly choose five distinct indices $i_1, \ldots, i_5$ from the set $\Lambda = \{1, \ldots, d\}$, and define another Coxeter graph Γ', with row and column indices chosen from the set $\Lambda' = \{i_1, \ldots, i_5\}$,

by $\Gamma'_{i_j,i_{j+1}} = \Gamma'_{i_{j+1},i_j} = 3$ for $j = 1, \ldots, 4$ and $\Gamma'_{i_j,i_k} = 2$ for any $j, k \in \{1, \ldots, 5\}$ with $|j-k| \geq 2$. By Example 1, the Coxeter group $W(\Gamma')$ corresponding to the Coxeter graph Γ' is of type A_4 (except different numbering for the row and column indices) and is isomorphic to the group $G = S_5$; we identify $W(\Gamma')$ with G in the following argument. Now Proposition 8 yields a surjective group homomorphism $W(\Gamma) \to W(\Gamma') = G$, which we write as ψ. On the other hand, Proposition 6 yields a group isomorphism φ from $W(\Gamma)$ to a certain subgroup of $\mathrm{GL}_d(\mathbb{R})$. We note that the subgroup $\varphi(W(\Gamma))$ of $\mathrm{GL}_d(\mathbb{R})$ is in fact contained in $\mathrm{GL}_d(\mathbb{Q}(\sqrt{3}))$ by the construction of the map φ, since $\cos(\pi/6) = \sqrt{3}/2$. Moreover, we take a random matrix T from $\mathrm{GL}_d(\mathbb{Q}(\sqrt{3}))$, and define the group $\widetilde{G}$ by

$$\widetilde{G} = T \cdot \varphi(W(\Gamma)) \cdot T^{-1} = \{T \cdot \varphi(w) \cdot T^{-1} \mid w \in W(\Gamma)\} \ .$$

In the resulting (non-compact) FHE scheme, the elements of $\widetilde{G}$ required to implement the public key are announced (i.e., elements gen_0 and gen_1, elements of $\widetilde{G}$ appearing in the group words for the lift of the realization of bit operators, and elements of $\widetilde{G}$ used to sample the random variable r_{ker} as specified below), while the choice of the matrix T and the indices $i_1, \ldots, i_5$ are kept secret.

Given an element $g \in \widetilde{G}$, the value $\pi(g)$ of the map $\pi\colon \widetilde{G} \to G$ is computed as follows:

1. Compute the conjugate $T^{-1}gT$ of the matrix g by using the secret matrix T.
2. Compute the word $w = \varphi^{-1}(T^{-1}gT)$ in $W(\Gamma)$ corresponding to $T^{-1}gT$ by using the algorithm yielded by Proposition 7.
3. Compute a word $w' = \psi(w)$ in $W(\Gamma')$ by the rule specified in Proposition 8.
4. Compute a shortest word equivalent to w' in $W(\Gamma')$ by using Proposition 9; this enables us to determine the element $\pi(g) \in G = S_5$ that corresponds to the w' via the isomorphism $G \simeq W(\Gamma')$.

In the construction of the public key mentioned above, first, to choose an element $\widetilde{w} \in \widetilde{G}$ satisfying $\pi(\widetilde{w}) = w$ for a given element $w \in W(\Gamma) \simeq G$, we take an element r of $\ker\pi \subset \widetilde{G}$ and then compute the product $\widetilde{w} = \varphi(w) \cdot r$ where the word w is also regarded as an element of $W(\Gamma)$ (note that the generating set of $W(\Gamma')$ is a subset of the generating set of $W(\Gamma)$ by the construction). Secondly, to sample the random variable r_{ker} on the set $\ker\pi$, we choose sufficiently many elements of $\ker\pi$ in advance, and then take a random product of those elements for each time to sample a value of r_{ker}. For both purposes, it suffices to choose an element of $\ker\pi$ in a suitable way. Here we consider the following way of randomly choosing an element of $\ker\pi$:

1. Take one of the words s_j with $j \in \Lambda \setminus \Lambda'$, $(s_{i_j}s_{i_{j+1}})^3$ with $j \in \{1, \ldots, 4\}$, and $(s_{i_j}s_{i_k})^2$ with distinct indices $j, k \in \{1, \ldots, 5\}$. Let w_0 denote the resulting word in $W(\Gamma)$.
2. Take a sufficiently long random word u in $W(\Gamma)$, and compute the conjugate uw_0u^{-1}.
3. Compute the matrix $\varphi(uw_0u^{-1}) \in \mathrm{GL}_d(\mathbb{Q}(\sqrt{3}))$ and then output the conjugate $T \cdot \varphi(uw_0u^{-1}) \cdot T^{-1} \in \widetilde{G}$. This element satisfies $\pi(T \cdot \varphi(uw_0u^{-1}) \cdot T^{-1}) = 1$ by the construction.

For possible parameter choices, first, we would be able to choose $d = 4$ as the minimal possible choice of d, but it is naively expected that a larger value of d would yield stronger security by hiding the actual choice of the sequence $i_1, \ldots, i_5$. Secondly, we would be able to choose each component of the matrix $T \in \mathrm{GL}_d(\mathbb{Q}(\sqrt{3}))$, say $a+b\sqrt{3}$, in a way that each of a and b is a random integer of at least $(40/d)$-bit length; now approximately at least $((2^{40/d})^2)^d = 2^{80}$

choices exist for each row and each column of the matrix T. Thirdly, for each choice of a random element of $\ker \pi$ mentioned above, we would be able to choose the random word u appeared in the algorithm above in such a way that u has at least length 80; now approximately at least 2^{80} choices exist for each word u. However, a detailed analysis of the security of the proposed (non-compact) FHE in practical implementation is left as a future research topic.

Remark 2. One may be curious about whether or not the Coxeter group $W(\Gamma)$ in the construction above can be chosen as a *finite* group, which will yield a *compact* FHE (i.e., FHE in the ordinary sense) as desired. In fact, starting from the Coxeter matrix Γ' of type A_4 as above, or more generally the Coxeter matrix Γ' of type A_n with $n \geq 4$, there is essentially a unique irreducible Coxeter matrix Γ other than Γ' for which $W(\Gamma)$ is finite and a group homomorphism $W(\Gamma) \to W(\Gamma')$ exists as specified in Proposition 8. This is the Coxeter matrix of type B_{n+1}, which is the Coxeter matrix Γ of size $n+1$ determined by the following conditions: restricting to the first n rows/columns of Γ yields the Coxeter matrix of type A_n, and we also have $\Gamma_{i,n+1} = 2$ for $1 \leq i \leq n-1$ and $\Gamma_{n,n+1} = 4$. Now the group homomorphism $W(\Gamma) \to W(\Gamma')$ in Proposition 8 is given by removing the symbols s_{n+1} from a given word in $W(\Gamma)$.

However, by using the known expression of the Coxeter group $W(\Gamma)$ of type B_{n+1} as a "signed" permutation group (see e.g., [23]), it can be proved that the kernel of the group homomorphism $W(\Gamma) \to W(\Gamma')$ is an elementary abelian 2-group generated by the elements $s_j s_{j+1} \cdots s_n s_{n+1} s_n \cdots s_{j+1} s_j$ with $j = 1, \ldots, n+1$, and it follows further that the image of any element of the kernel of the map $W(\Gamma) \to W(\Gamma')$ above via the isomorphism $\varphi\colon W(\Gamma) \to \varphi(W(\Gamma)) \subset \mathrm{GL}_{n+1}(\mathbb{R})$ in Proposition 6 is a lower triangular matrix. This yields a linear constraint "each component at the upper triangular part is 0" for the kernel of the resulting map $\varphi(W(\Gamma)) \to W(\Gamma') \simeq G$, which is not desirable as discussed in Section 5.2. Moreover, it is also known (see e.g., [14]) that, for any group automorphism ρ of $\varphi(W(\Gamma))$, we have $\rho(g) \in \{\pm g\}$ for each $g \in \varphi(W(\Gamma))$; therefore the linear constraint cannot be violated even by considering the composition of a group automorphism of $\varphi(W(\Gamma))$ followed by the map $\varphi(W(\Gamma)) \to W(\Gamma')$. This argument suggests that, in order to construct an appropriate homomorphism $\widetilde{G} \to G = S_{n+1}$ with finite $\widetilde{G}$, the group $\widetilde{G}$ must be searched from outside the class of Coxeter groups.

5.5 Another Approach

We also propose another idea to avoid an undesirable linear constraint as in Section 5.2 for the kernel of the map $\pi\colon \widetilde{G} \to G$ by utilizing combinatorial group theory. In the idea, we start with a finite group G in which the bit operators are realized and for which an efficient presentation is known. All of the group $G = S_5$ used in Section 4.2 and the groups $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ used in Section 4.5 satisfy the condition (see Proposition 4 for the latter case). We take, in a certain suitable way discussed below, another finite group H that also admits an efficient presentation. Then we take the direct product $G \times H$ of these two groups, which also admits an efficient presentation due to Proposition 5. However, if we adopt the group $G \times H$ with the aforementioned presentation as the group $\widetilde{G}$ in our proposed framework and the projection $G \times H \to G$ to the first component as the corresponding map $\pi\colon \widetilde{G} \to G$, the construction in Proposition 5 of the presentation of $G \times H$ will leak the direct product structure of $G \times H$. This implies that the information on the map $\pi\colon \widetilde{G} \to G$ is not hidden and hence the resulting FHE will never be secure.

Our idea to prevent the leakage of the direct product structure of the group $G \times H$ is to randomly modify the aforementioned presentation of this group yielded by Proposition 5 without changing the abstract group structure itself, by utilizing the facts in Lemmas 5 and 6. It is naively expected that, if this modification is successfully executed, then the resulting presentation of the group will not leak the information on the direct product structure $G \times H$, hence the resulting group will be used as the group $\widetilde{G}$. The record of the modification process

will be a part of the secret key, which enables one to recover the original presentation of the direct product group $G \times H$ in order to compute the map $\pi\colon \widetilde{G} \to G$.

Here we note that there are (at least) three problems to be solved for this approach. The first problem is to analyze a suitable way of modifying the presentation of the group in order to achieve the security in practice, e.g., to evaluate the sufficient number of steps of the modification. The second problem is that, in the resulting group $\widetilde{G}$ with a randomly modified presentation, the multiplication of two elements given as group words can, *in theory*, be computed by first concatenating the two words and then simplifying the resulting word by using the given fundamental relations for the group $\widetilde{G}$. However, as the presentation of $\widetilde{G}$ has been randomly modified, it is not obvious how to simplify the resulting word in an *efficient* way. If an efficient simplification of the resulting word does not work, then the words representing the elements of $\widetilde{G}$ will be unboundedly long, which will again result in a *non-compact* FHE (though the group $\widetilde{G}$ itself is a finite group).

Moreover, even if the aforementioned two problems are completely solved, it may still happen that the resulting FHE is not secure if the group H is not appropriately chosen. From now, we give some discussions on appropriate choices of the group H.

The idea of a potential attack against our FHE is as follows. Any element of the group $\widetilde{G} \simeq G \times H$ can be decomposed into the "G-component" and the "H-component". The G-component of an element is nothing but the value of the map $\pi\colon \widetilde{G} \to G$, therefore the elements of $\ker \pi$ are those with G-components being the identity element, i.e., the elements of H. Now suppose that an adversary obtains an element w_0 of $\widetilde{G}$ whose H-component is the identity element but G-component is not the identity element. Then any element of $\ker \pi$ is commutative with w_0, while a random element of $\widetilde{G} \setminus \ker \pi$ is expected to be not commutative with w_0. This property would enable the adversary to distinguish the elements of $\ker \pi$ from the other elements, which will violate the security of the proposed scheme. Hence, such an element w_0 should not be efficiently found.

For conditions of the group H to prevent to efficiently find such an element w_0, first, H should not be a commutative group; indeed, if H were a commutative group, then the element w_0 could be obtained by $w_0 = [w, w']$ for randomly chosen $w, w' \in \widetilde{G}$. On the other hand, a pair of distinct elements $w, w' \in \widetilde{G}$ with the same H-component will yield the element w_0 by $w_0 = w^{-1}w'$. Therefore, due to the Birthday Paradox, the cardinality of the group H should be at least 2^{160} if we expect to achieve 80-bit security.

We also have to consider the following kind of attacks. Suppose that an integer k satisfies that both of the probabilities $\Pr_{w \leftarrow H}[w^k = 1]$ and $\Pr_{w \leftarrow \widetilde{G}}[w^k \neq 1]$ are non-negligible and at least one of them is noticeable. Then an adversary can distinguish a random element of $H = \ker \pi$ from a random element of $\widetilde{G}$ by checking whether a given random element w satisfies $w^k = 1$ or not. Therefore, such an integer k should not be efficiently found.

For example[2], suppose that $G = H = A_\lambda$ 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 $\Pr_{w \leftarrow H}[w^p = 1] = \dfrac{2}{p \cdot (\lambda - p)!} + \dfrac{1}{|A_\lambda|!}$, denoted here by P; while we have $\Pr_{w \leftarrow \widetilde{G}}[w^p = 1] = P^2$. 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 H and over $\widetilde{G} \simeq G \times H$ can be distinguished with non-negligible advantage by checking if $w^p = 1$ for a given random element w.

In order to avoid the aforementioned attack strategies, here we propose to use $H = \mathrm{SL}_2(\mathbb{F}_q)$ for an odd prime q satisfying that $1/q$ is negligible. Note that this H indeed admits an efficient presentation by Proposition 4. For the sake of preventing the attack in the previous paragraph,

[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	cardinality	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	$\frac{q+1}{\gcd(q+1,i)}$

we investigate the distribution of the orders of elements of H.

Following the argument in Section 5.2 of [15], 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 $i = 0, 1, \ldots, q-2$. 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 $i = 0, 1, \ldots, q^2-2$, 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 cardinality of the conjugacy class) are quoted (with slightly different notations) from Section 5.2 of [15]. 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 of the cardinality of each conjugacy class of type 1 to 6 to the cardinality 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 $H = \mathrm{SL}_2(\mathbb{F}_q)$, provided the size of the coefficient field $\mathbb{F}_q$ is appropriately hidden by the random modification of the presentation of the group. A further analysis of other possible attack

strategies will be a future research topic.

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, and Takashi Yamakawa, 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 reviewers of previous submissions of the paper for their careful reviews and valuable comments. This work was supported by JST PRESTO Grant Number JPMJPR14E8, Japan.

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] A. Björner, F. Brenti: Combinatorics of Coxeter Groups. Springer GTM vol.231, Springer, 2005.

[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] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène: Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds. In: Proceedings of ASIACRYPT 2016 (1), LNCS 10031, 2016, pp.3–33.

[10] 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.

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

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

[13] 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.

[14] W. N. Franzsen: Automorphisms of Coxeter Groups. Ph.D. thesis, University of Sydney, 2001, http://www.maths.usyd.edu.au/u/PG/Theses/franzsen.pdf

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

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

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

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

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

[20] 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.

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

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

[23] J. E. Humphreys, Reflection Groups and Coxeter Groups, Cambridge University Press, 1990.

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

[25] N. Khamsemanan, R. Ostrovsky, W. E. Skeith III: On the Black-Box Use of Somewhat Homomorphic Encryption in NonInteractive Two-Party Protocols. SIAM Journal of Discrete Mathematics vol.30, no.1, 2016, pp.266–295.

[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: Communication Complexity in Algebraic Two-Party Protocols. In: Proceedings of CRYPTO 2008, LNCS 5157, 2008, pp.379–396.

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

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

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