# A Simple Framework for Noiseless Fully Homomorphic Encryption on Special Classes of Non-Commutative Groups

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

August 26, 2015

**Abstract**

We propose a new and simple framework for constructing fully homomorphic encryption (FHE) which is completely different from the previous work. We show that, the AND operator on plaintext bits is emulatable, with negligible error probability, by the commutator operator on a finite non-commutative group with appropriately rerandomized inputs, provided the group is large and "far from being commutative" in a certain sense. The NOT operator is also easily emulated on such a group; hence the FHE functionality is realized. Finally, in order to realize security, we propose some possible strategies for concealing the core structure of the FHE functionality, based on techniques in combinatorial or computational group theory. In contrast to the previous noise-based constructions of FHE, our proposed construction does not suffer from increasing noise in ciphertexts and therefore needs no bootstrapping procedures, which is the most inefficient part in the previous schemes.

## 1 Introduction

Until the pioneering work by Gentry [13], it had been a long-standing open problem to construct *fully homomorphic* (public key) *encryption* (*FHE*) that enables, without revealing any information on encrypted plaintexts, anyone to perform arbitrary operations on the plaintexts through the corresponding "homomorphic operations" on the ciphertexts. After that, studies of FHE to improve the efficiency (e.g., [11, 14, 16, 19, 27]) and to give various frameworks of construction (e.g., [3, 4, 5, 6, 7, 8, 9, 10, 15, 22]) have been one of the main research topics in cryptology (see [26] for a survey). Now we note that, all the previous FHE schemes (with compact ciphertexts) rely on Gentry's bootstrapping framework. Namely, any ciphertext involves noise, which is increased by homomorphic operations and will collapse the ciphertext after a number of operations, therefore a "bootstrapping" procedure is required to cancel the noise before the collapse. This additional procedure is a major bottleneck for efficiency improvement and makes the syntax of FHE less analogical to the classical homomorphic encryption. Therefore, a new approach to construct FHE schemes that does not require bootstrapping is really valuable.

### 1.1 Our Contributions and Related Work

In this paper, we propose a new framework for construction of FHE, which is completely different from the previous work and realizes the FHE functionality without bootstrapping. Our approach follows the direction of so-called "group-based cryptography" (see e.g., [2] for a survey), where *non-commutative groups* with some special properties are used as the underlying mathematical structure. We also emphasize that, the non-commutativity of groups in our construction is essential for the *functionality* of the scheme; our homomorphic operation uses the commutator operator in the group (see below for the definition), which becomes just a constant function if the group is commutative. This is a contrast to the major previous group-based cryptographic schemes (e.g., [21, 24]), where the functionality is realized on a *commutative* subset (e.g., by the technique of Diffie–Hellman key exchange) and the non-commutativity is used only for *security* purpose to conceal the commutative subset. The author hopes that this work shows a new possibility of group-based cryptography which is left unexplored.

Our proposed approach to FHE is twofold; we first realize the functionality of homomorphic operators on a non-commutative "base" group (denoted by $\overline{G}$), and then "lift" it (in a way compatible to the homomorphic operations) to a larger "obfuscated" group (denoted by $G$) to conceal the base structure. More precisely, we use a surjective group homomorphism $\varphi\colon G \to \overline{G}$, $g \mapsto \overline{g}$, whose values are difficult to guess when the map $\varphi$ is not announced (see below). The "base" structure consists of pairs $(\overline{c_1}, \overline{c_2})$ of elements of $\overline{G}$, which satisfies that $\overline{c_2} = 1$ (the identity element) and $\overline{c_2} = \overline{c_1}$ if the pair is associated to plaintext $m = 0$ and $m = 1$, respectively; we call such a pair a *class-$m$ pair*. An additional condition $\overline{c_1} \neq 1$ is also required to separate the two classes. Now our homomorphic NOT operator for the pair $(\overline{c_1}, \overline{c_2})$ replaces the component $\overline{c_2}$ with $\overline{c_1} \cdot (\overline{c_2})^{-1}$; this exchanges the two states $\overline{c_2} = 1$ and $\overline{c_2} = \overline{c_1}$ successfully.

On the other hand, the key tool for constructing our homomorphic AND operator is the *commutator* operator $[\cdot,\cdot]$, which is defined for any group $H$ by

$$[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1} \in H \text{ for any } g, h \in H \enspace .$$

The key property is the following: If $g = 1$ or $h = 1$, then $[g, h] = 1$. This is similar to the AND operator for bits (denoted by $\wedge$)[1], i.e., if $b = 0$ or $b' = 0$, then $b \wedge b' = 0$. Motivated by this analogy, we want to define the homomorphic AND operator for class-$m$ pair $(\overline{c_1}, \overline{c_2})$ and class-$m'$ pair $(\overline{d_1}, \overline{d_2})$ as outputting the pair $(\overline{e_1}, \overline{e_2})$ with $\overline{e_i} = [\overline{c_i}, \overline{d_i}]$ for $i = 1, 2$. By the above-mentioned property of commutator (as well as the "synchronized" definition for two components), the output satisfies *almost* all requirements for class-$(m \wedge m')$ pairs regardless of the choices of $m$ and $m'$, but only the requirement $\overline{e_1} \neq 1$ is in general *not* guaranteed even if $\overline{c_1} \neq 1$ and $\overline{d_1} \neq 1$ (for example, consider the case $\overline{c_1} = \overline{d_1}$, which always yields $\overline{e_1} = 1$).

Our idea to resolve the issue is to "rerandomize" the inputs of the commutator operator in a "synchronized" manner. Namely, we modify the definition of $\overline{e_i}$ in the following manner:

$$\overline{e_1} = [\overline{g} \cdot \overline{c_1} \cdot (\overline{g})^{-1} \,,\, \overline{d_1}] \quad \text{and} \quad \overline{e_2} = [\overline{g} \cdot \overline{c_2} \cdot (\overline{g})^{-1} \,,\, \overline{d_2}] \enspace ,$$

where $\overline{g}$ is a uniformly random element of $\overline{G}$ commonly used for the two components. This does not affect the already satisfied conditions for $(\overline{e_1}, \overline{e_2})$, since $\overline{c_2} = 1$ implies $\overline{g} \cdot \overline{c_2} \cdot (\overline{g})^{-1} = 1$. Then we prove that, if the group $\overline{G}$ is appropriately chosen (for example, $\overline{G}$ is the group of $2 \times 2$ matrices with determinant one over a sufficiently large finite field $\mathbb{F}$, denoted by $\mathrm{SL}_2(\mathbb{F})$), then the remaining condition $\overline{e_1} \neq 1$ is satisfied with sufficiently high probability (with respect to the random choice of $\overline{g}$), therefore our homomorphic AND operator works correctly. We also propose more complicated rerandomizing functions for inputs of commutator, which enlarges the possibilities of $\overline{G}$ significantly. We note that, this FHE functionality can be lifted to $G$ since the functionality is realized by using group operators in $\overline{G}$ only; i.e., a pair $(c_1, c_2)$ of elements of $G$ is regarded as a ciphertext for plaintext $m$ if $(\varphi(c_1), \varphi(c_2)) = (\overline{c_1}, \overline{c_2})$ is a class-$m$ pair.

Towards secure instantiation of the proposed scheme (i.e., to choose a group homomorphism $\varphi\colon G \to \overline{G}$ for which it is difficult to decide if a given element $x \in G$ satisfies $\varphi(x) = 1 \in \overline{G}$), our candidate strategy proposed in this paper is based on the theory of presentations of groups in terms of generators and fundamental relations satisfied by the generators. First we note that, the candidates for $\overline{G}$ given in this paper (including $\mathrm{SL}_2(\mathbb{F})$ mentioned above) admit efficient

[1]From the property of commutators, one may be reminded of the proof of the Barrington's theorem [1].

group presentations (e.g., [17]). We choose $G$ to be the direct product $N \times \overline{G}$ of $\overline{G}$ and another group $N$ and define the map $\varphi$ to be the natural projection to the second factor. Here we take a non-commutative group $N$ having efficient group presentation, which (together with the above-mentioned group presentation of $\overline{G}$) yields a group presentation of $G$. Examples of such groups $N$, as well as some necessary condition for security purpose, will be presented in later sections. Then we "obfuscate" the structure of $G$ by repeatedly applying Tietze transformations, which is an invertible transformation of group presentations that keeps the underlying group structure unchanged. Now the structure of $G$ would be suitably concealed if the transformations are applied randomly and sufficiently many times; detailed theoretical and experimental analyses of this construction will be a future research topic. We note that the proposed strategy would be also applicable to construct homomorphic encryption schemes with plaintext spaces being non-commutative groups, which (as mentioned in [23]) can be also converted to FHE schemes by choosing the plaintext group appropriately.

### 1.2 Organization of the Paper

In Section 2, we summarize some notations, terminology and basic definitions. In Section 3, we present our new framework for construction of FHE schemes. Two proposed choices of the rerandomization functions for inputs of the commutator operator in our framework are studied in Section 4 and 5. Finally, in Section 6, we describe some strategies for instantiating the proposed scheme. Some basic facts about group theory are supplied in Appendix A.

## 2 Preliminaries

In this section, we summarize some basic definitions and notations used throughout the paper. Unless otherwise specified, a group $G$ is written in multiplicative form with identity element denoted by $1_G$ (or simply by 1, if the group $G$ is obvious from the context) and is not commutative. The *commutator* $[g,h]$ of two elements $g,h \in G$ is defined by

$$[g,h] = g \cdot h \cdot g^{-1} \cdot h^{-1} \in G \enspace .$$

Note that, $[g,h] = 1$ if and only if $gh = hg$, i.e., $g$ and $h$ commute. The reader may refer to a textbook of group theory (e.g., [25]) for other definitions and basic facts for groups (see also Appendix A). Let $a \leftarrow_R X$ mean that an element $a$ is chosen from a finite set $X$ uniformly at random, and let $a \leftarrow \mathcal{A}(x)$ mean that $a$ is an output of an algorithm $\mathcal{A}$ with input $x$. We use a similar notation for outputs of probability distributions. Let $\Pr_{a \leftarrow_R X}[\cdots]$ denotes the probability of the specified event, taken over uniformly random element $a \in X$. Let $\lambda$ denote the security parameter unless otherwise specified. We say that a quantity $\varepsilon = \varepsilon(\lambda) \geq 0$ depending on $\lambda$ 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 $\lambda > \lambda_0$; $\varepsilon \in [0,1]$ is *overwhelming*, if $1 - \varepsilon$ is negligible; and $\varepsilon$ is *noticeable*, if there exist integers $n \geq 1$ and $\lambda_0 > 0$ with the property that we have $\varepsilon > \lambda^{-n}$ for every $\lambda > \lambda_0$. The *statistical distance* between two probability distributions $\mathcal{X}, \mathcal{Y}$ over a finite set $Z$ is defined by $\sum_{z \in Z} |\Pr[z \leftarrow \mathcal{X}] - \Pr[z \leftarrow \mathcal{Y}]|/2$. We say that two probability distributions (parameterized by $\lambda$) are *statistically close*, if their statistical distance is negligible.

A *public key encryption* (*PKE*) scheme consists of the following three algorithms. The key generation algorithm $\mathsf{Gen}(1^\lambda)$ outputs a pair $(\mathsf{pk}, \mathsf{sk})$ of a public key $\mathsf{pk}$ and a secret key $\mathsf{sk}$. The encryption algorithm $\mathsf{Enc}(\mathsf{pk}, m)$ with plaintext $m$ outputs a ciphertext as the encryption result of $m$. Finally, the decryption algorithm $\mathsf{Dec}(\mathsf{sk}, c)$ with ciphertext $c$ outputs either a plaintext $m$ as the decryption result of $c$, or a distinguished symbol $\perp$ indicating decryption failure. In the paper, any PKE scheme has 1-bit plaintext space $\{0,1\}$. The *correctness* of a PKE scheme means that, for any plaintext $m$, the probability $\Pr[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) \neq m]$ is negligible, where the probability is taken over the randomness in the encryption algorithm. In particular, negligible probabilities of decryption errors are tolerated in the paper.

A *homomorphic* PKE scheme (with 1-bit plaintexts) is a PKE scheme endowed with another algorithm that, given any map of the form $f\colon \{0,1\}^n \to \{0,1\}^{n'}$ in some specified class and any ciphertexts $c_i \leftarrow \mathsf{Enc}(\mathsf{pk}, m_i)$ for plaintexts $m_i$ ($i \in \{1,2,\dots,n\}$) as inputs, efficiently outputs ciphertexts $c'_1,\dots,c'_{n'}$ satisfying that $(\mathsf{Dec}(\mathsf{sk}, c'_i))_{i=1}^{n'} = f((m_i)_{i=1}^n)$ with overwhelming probability. In particular, if the $f$ can be any circuit with polynomially many gates, then the scheme is called an FHE scheme. The proposed FHE scheme in the paper calculates the circuit $f$ by combining AND and NOT operators, hence it is endowed with two algorithms $\mathsf{AND}$ and $\mathsf{NOT}$ for homomorphically computing AND and NOT operators, respectively.

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

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)\,;\, b^* \leftarrow_R \{0,1\}\,;\, c^* \leftarrow \mathsf{Enc}(\mathsf{pk}, b^*) \,:\, b \leftarrow \mathcal{A}(1^\lambda, \mathsf{pk}, c^*) \enspace .$$

We note that other advanced security notions for FHE, such as the circuit privacy (e.g., [20]), are out of the scope of the paper and are left as future research topics.

# 3 Our Proposed Framework for FHE Schemes

In this section, we present our proposed framework for non-commutative group-based FHE schemes. In Section 3.1, we summarize some basic properties of the underlying groups which are assumed throughout our argument below. Then in Section 3.2, we describe the proposed framework and show a part of the correctness property of the resulting scheme. Our framework involves some (probabilistic) functions on the underlying group, and the required conditions for the underlying groups to achieve the remaining part of the correctness property depend on a concrete choice of the functions, discussed in the following sections.

## 3.1 Common Properties of Underlying Groups

Here we summarize some basic properties of the underlying groups to be assumed in all of our proposed constructions. We suppose that, we are given (certain descriptions of) two finite groups[2] $G$ and $\overline{G}$ and a surjective group homomorphism $\varphi\colon G \to \overline{G}$. We assume that the group $\overline{G}$ (hence $G$ as well) is sufficiently large, or more precisely, $|\overline{G}|^{-1}$ is negligible in the security parameter $\lambda$. We denote the kernel of $\varphi$ by $N = \ker\varphi = \{g \in G \mid \varphi(g) = 1_{\overline{G}}\}$.

We will also use some functions and algorithms associated to these groups. First, we suppose that we are given two algorithms $\mathsf{Sample}_G$ and $\mathsf{Sample}_N$ which output uniformly random (or more generally, statistically close to uniform) elements of $G$ and of $N$, respectively. A typical implementation of these algorithms will be as follows: Given a generating set of $G$ (respectively, $N$), the algorithm computes a random product of random powers of generators chosen randomly from the generating set, and outputs the resulting element. Secondly, we also suppose that we are given two probabilistic functions $F_1, F_2\colon G \to G$, which we call *shuffling functions*, satisfying the following conditions, where $* \in \{1,2\}$ and $r$ denotes any fixed internal randomness for $F_*$:

$$\varphi(F_*(1_G; r)) = 1_{\overline{G}} \enspace . \tag{1}$$

$$\text{If } g_1, g_2 \in G \text{ and } \varphi(g_1) = \varphi(g_2) \text{ then } \varphi(F_*(g_1; r)) = \varphi(F_*(g_2; r)) \enspace . \tag{2}$$

[2]The argument in Section 3 can be extended to more general cases where $G$ or $\overline{G}$ has *non-associative* multiplication. It can be also extended even to the cases of *infinite* $G$, though the resulting scheme will be just a somewhat encryption scheme and its conversion to FHE (if possible) will require bootstrapping.

Examples of shuffling functions will be presented in later sections. Moreover, we suppose that we are given an algorithm $\mathsf{Ker}_\varphi$ to determine whether its input $g \in G$ is an element of $\ker \varphi$ or not. An obvious implementation of the algorithm is to calculate the value $\varphi(g)$ itself, provided $\varphi$ is efficiently computable. Further conditions for these objects required to realize correctness and security in each of our proposed construction will be discussed later.

### 3.2 Description of Our Framework

Here we give the description of our proposed framework to construct FHE schemes. We write the resulting FHE scheme as $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{NOT}, \mathsf{AND})$. Each of the algorithms in $\Pi$ is defined as follows, where $\varepsilon = \varepsilon(\lambda)$ denotes any fixed function which is negligible in $\lambda$:

$\mathsf{Gen}(1^\lambda)$**:** According to the security parameter $\lambda$, the algorithm generates groups $G$ and $\overline{G}$, a surjective group homomorphism $\varphi \colon G \to \overline{G}$, algorithms $\mathsf{Sample}_G$, $\mathsf{Sample}_N$ and $\mathsf{Ker}_\varphi$ and probabilistic functions $F_1$ and $F_2$, as in Section 3.1. In particular, $|\overline{G}|^{-1} \leq \varepsilon$. Then the algorithm outputs a public key $\mathsf{pk}$ and a secret key $\mathsf{sk}$ defined by

$$\mathsf{pk} = (G, \mathsf{Sample}_G, \mathsf{Sample}_N, F_1, F_2)\ ,\ \mathsf{sk} = \mathsf{Ker}_\varphi \ .$$

$\mathsf{Enc}(\mathsf{pk}, m)$ **for** $m \in \{0,1\}$**:** The algorithm outputs $c = (c_1, c_2) \in G \times G$ generated by

$$c_1 \leftarrow \mathsf{Sample}_G\ ,\ c_2 \leftarrow \begin{cases} h & \text{if } m = 0\ , \\ c_1 h & \text{if } m = 1\ , \end{cases} \text{ where } h \leftarrow \mathsf{Sample}_N \ .$$

The ciphertext space is defined as $\mathcal{C} := G \times G$.

$\mathsf{Dec}(\mathsf{sk}, c)$ **for** $c = (c_1, c_2) \in \mathcal{C}$**:** The algorithm decides whether $\varphi(c_2) = 1_{\overline{G}}$ or not, by using the algorithm $\mathsf{Ker}_\varphi$. Then it outputs 0 if $\varphi(c_2) = 1_{\overline{G}}$; and outputs 1 otherwise.

$\mathsf{NOT}(\mathsf{pk}, c)$ **for** $c \in \mathcal{C}$**:** The algorithm outputs

$$(c_1\ ,\ {c_2}^{-1} c_1) \in \mathcal{C} \ .$$

$\mathsf{AND}(\mathsf{pk}, c, c')$ **for** $c, c' \in \mathcal{C}$**:** The algorithm outputs

$$\Big( [F_1(c_1; r_1), F_2(c'_1; r_2)]\ ,\ [F_1(c_2; r_1), F_2(c'_2; r_2)] \Big) \in \mathcal{C}$$

(recall that $[x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1}$), where $r_1$ and $r_2$ denote internal randomness for $F_1$ and $F_2$, respectively, chosen uniformly at random. (We emphasize that computations for the two components are "synchronized", i.e., the randomness used in the functions $F_1$ and $F_2$ for the computation of the first component of the output are the same as ones for the second component.)

We show some basic properties of the proposed framework. We use the following fact:

**Lemma 1.** *If $f \colon H \to K$ is a surjective group homomorphism, $|H|, |K| < \infty$ and $g$ is a uniformly random element of $H$, then $f(g)$ is also a uniformly random element of $K$.*

*Proof.* This follows from the fact that, for any element $x$ of the image of $f$, the number of elements $g \in H$ satisfying $f(g) = x$ is equal to $|\ker f|$, regardless of the choice of $x$. □

To show the correctness of the proposed scheme, we introduce an auxiliary terminology:

**Definition 1.** For a ciphertext $c = (c_1, c_2) \in \mathcal{C}$, we say that $c$ is *class*-0 if $\varphi(c_1) \neq 1_{\overline{G}}$ and $\varphi(c_2) = 1_{\overline{G}}$, and $c$ is *class*-1 if $\varphi(c_1) \neq 1_{\overline{G}}$ and $\varphi(c_2) = \varphi(c_1)$.

By the definition of the decryption algorithm, for $b \in \{0,1\}$, we have $\mathsf{Dec}(\mathsf{sk}, c) = b$ if $c$ is a class-$b$ ciphertext. This implies the following result:

**Proposition 1.** *For any $m \in \{0,1\}$, the algorithm $\mathsf{Enc}(\mathsf{pk}, m)$ outputs a class-$m$ ciphertext with overwhelming probability. Hence, the scheme $\Pi$ satisfies the correctness as a PKE scheme.*

*Proof.* Let $c = (c_1, c_2) \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$. First, since $c_1 \leftarrow \mathsf{Sample}_G$, Lemma 1 implies that $\varphi(c_1)$ is uniformly random over $\overline{G}$, therefore we have $\varphi(c_1) \neq 1_{\overline{G}}$ with probability $1 - |\overline{G}|^{-1} \geq 1 - \varepsilon$ which is overwhelming. Now, assuming the overwhelming case $\varphi(c_1) \neq 1_{\overline{G}}$, if $m = 0$, then we have $\varphi(c_2) = \varphi(h) = 1_{\overline{G}}$ since $h \in N$, therefore $c$ is class-0. On the other hand, if $m = 1$, then we have $\varphi(c_2) = \varphi(c_1 h) = \varphi(c_1)\varphi(h) = \varphi(c_1)$ since $h \in N$, therefore $c$ is class-1. Hence the assertion holds. □

Secondly, we prove a part of the homomorphic property of the proposed scheme:

**Proposition 2.** *For any $m \in \{0,1\}$, if $c$ is a class-$m$ ciphertext, then $\mathsf{NOT}(\mathsf{pk}, c)$ always outputs a class-$(\neg m)$ ciphertext, where $\neg m = 1 - m$ denotes the NOT operator.*

*Proof.* First, we note that the algorithm $\mathsf{NOT}$ does not change the first component of a ciphertext. Now if $\varphi(c_2) = 1_{\overline{G}}$, then we have $\varphi({c_2}^{-1} c_1) = \varphi(c_2)^{-1}\varphi(c_1) = \varphi(c_1)$. On the other hand, if $\varphi(c_2) = \varphi(c_1)$, then we have $\varphi({c_2}^{-1} c_1) = \varphi(c_2)^{-1}\varphi(c_1) = 1_{\overline{G}}$. Hence the assertion holds. □

**Proposition 3.** *Let $m, m' \in \{0,1\}$, $c$ be a class-$m$ ciphertext, and $c'$ be a class-$m'$ ciphertext. Let $c^\dagger = (c_1^\dagger, c_2^\dagger) \leftarrow \mathsf{AND}(\mathsf{pk}, c, c')$. Then:*

- *If $m = 0$ or $m' = 0$, then we always have $\varphi(c_2^\dagger) = 1_{\overline{G}}$.*
- *If $m = m' = 1$, then we always have $\varphi(c_2^\dagger) = \varphi(c_1^\dagger)$.*

*Namely, the component $c_2^\dagger$ satisfies the condition for class-$(m \wedge m')$ ciphertexts in any case, where $m \wedge m'$ denotes the AND operator.*

*Proof.* When $m = 0$, since $\varphi(c_2) = 1_{\overline{G}} = \varphi(1_G)$, we have $\varphi(F_1(c_2)) = \varphi(F_1(1_G)) = 1_{\overline{G}}$ by (1) and (2) regardless of the randomness in $F_1$. Now we have

$$\begin{aligned}
\varphi(c_2^\dagger) &= \varphi([F_1(c_2), F_2(c_2')]) \\
&= \varphi(F_1(c_2) \cdot F_2(c_2') \cdot F_1(c_2)^{-1} \cdot F_2(c_2')^{-1}) \\
&= \varphi(F_1(c_2)) \cdot \varphi(F_2(c_2')) \cdot \varphi(F_1(c_2))^{-1} \cdot \varphi(F_2(c_2'))^{-1} \\
&= 1_{\overline{G}} \cdot \varphi(F_2(c_2')) \cdot 1_{\overline{G}} \cdot \varphi(F_2(c_2'))^{-1} = \varphi(F_2(c_2')) \cdot \varphi(F_2(c_2'))^{-1} = 1_{\overline{G}} \ .
\end{aligned}$$

When $m' = 0$, the same argument implies that $\varphi(F_2(c_2')) = 1_{\overline{G}}$ and

$$\varphi(c_2^\dagger) = \varphi(F_1(c_2)) \cdot \varphi(F_1(c_2))^{-1} = 1_{\overline{G}} \ .$$

Finally, when $m = m' = 1$, since $\varphi(c_2) = \varphi(c_1)$ and $\varphi(c_2') = \varphi(c_1')$, by (2), we have

$$\varphi(F_1(c_1; r_1)) = \varphi(F_1(c_2; r_1)) \quad \text{and} \quad \varphi(F_2(c_1'; r_2)) = \varphi(F_2(c_2'; r_2)) \ .$$

Therefore, we have

$$\begin{aligned}
\varphi(c_2^\dagger) &= \varphi(F_1(c_2; r_1)) \cdot \varphi(F_2(c_2'; r_2)) \cdot \varphi(F_1(c_2; r_1))^{-1} \cdot \varphi(F_2(c_2'; r_2))^{-1} \\
&= \varphi(F_1(c_1; r_1)) \cdot \varphi(F_2(c_1'; r_2)) \cdot \varphi(F_1(c_1; r_1))^{-1} \cdot \varphi(F_2(c_1'; r_2))^{-1} \\
&= \varphi([F_1(c_1; r_1), F_2(c_1'; r_2)]) = \varphi(c_1^\dagger) \ .
\end{aligned}$$

Hence the assertion holds. □

Proposition 2 showed that the algorithm $\mathsf{NOT}(\mathsf{pk}, c)$ behaves as a homomorphic NOT operator for class-0 and class-1 ciphertexts. On the other hand, Proposition 3 showed that the algorithm $\mathsf{AND}(\mathsf{pk}, c, c')$ will behave as a homomorphic AND operator for class-0 and class-1 ciphertexts, *provided the condition $\varphi(c_1^\dagger) \neq 1_{\overline{G}}$ for the first component is satisfied.* The requirements for the groups $G$ and $\overline{G}$ to guarantee the condition $\varphi(c_1^\dagger) \neq 1_{\overline{G}}$ (with overwhelming probability) depend on the choices of shuffling functions $F_1$ and $F_2$. We propose two choices of these functions in the following two sections.

On the other hand, the following holds for the CPA security of the proposed scheme $\Pi$:

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

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

*Proof.* First, to convert this adversary $\mathcal{A}^\dagger$ to a CPA adversary $\mathcal{A}$ for $\Pi$, given a challenge ciphertext $c^* = (c_1^*, c_2^*)$ with challenge bit $b^*$, the simulator simply inputs $c_2^*$ (as well as $1^\lambda$ and $\mathsf{pk}$) to $\mathcal{A}^\dagger$ and outputs the output bit of the $\mathcal{A}^\dagger$. Now $c_2^*$ is uniformly random over $N$ if $b^* = 0$, and $c_2^*$ is uniformly random over $G$ if $b^* = 1$ (since $c_2^* = c_1^* h$ and $c_1^*$ is uniformly random over $G$). Hence we have $\mathsf{Adv}_{\mathcal{A}} = \mathsf{Adv}_{\mathcal{A}^\dagger}$.

Secondly, to convert a CPA adversary $\mathcal{A}$ for $\Pi$ to this adversary $\mathcal{A}^\dagger$, given a challenge element $g^\dagger$ with challenge bit $b^\dagger$, the simulator generates $c_1^* \leftarrow \mathsf{Sample}_G$ and $b^* \leftarrow_R \{0,1\}$; computes $c_2^* = g^\dagger$ if $m^* = 0$ and $c_2^* = c_1^* g^\dagger$ if $m^* = 1$; inputs $c^* = (c_1^*, c_2^*)$ (as well as $1^\lambda$ and $\mathsf{pk}$) to $\mathcal{A}$ and receives the output bit $b'$; and outputs $b = b^* \oplus b'$ where $\oplus$ denotes the XOR operator. Now if $b^\dagger = 0$, then $g^\dagger$ is a uniformly random element of $N$, therefore the input distribution for $\mathcal{A}$ is correct and we have

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

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

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

Summarizing, we have

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

This completes the proof of Theorem 1. $\square$

# 4 First Candidate of Shuffling Functions

In this section, we present one of the two proposed choices of the shuffling functions $F_1$ and $F_2$ for our construction in Section 3. We define

$$F_1(x) = gxg^{-1} \text{ with } g \leftarrow \mathsf{Sample}_G \quad \text{and} \quad F_2(x) = x \ .$$

Now conditions (1) and (2) for $F_2$ are trivially satisfied, and condition (1) for $F_1$ is also satisfied since $g \cdot 1_G \cdot g^{-1} = 1_G$. Moreover, for condition (2) for $F_1$, if $\varphi(g_1) = \varphi(g_2)$, then we have

$$\varphi(g \cdot g_1 \cdot g^{-1}) = \varphi(g)\varphi(g_1)\varphi(g)^{-1} = \varphi(g)\varphi(g_2)\varphi(g)^{-1} = \varphi(g \cdot g_2 \cdot g^{-1}) \ .$$

Hence the shuffling functions satisfy the two conditions.

In this case, a sufficient condition for our proposed scheme to have the fully homomorphic functionality can be formulated as follows:

**Definition 2** (Commutator-separable group)**.** We say that the family of groups $\overline{G}$ used in our proposed scheme, parameterized by the security parameter $\lambda$, is *commutator-separable*, if there exists a subset $X$ of $\overline{G}$ satisfying the following conditions, where $\varepsilon = \varepsilon(\lambda)$ is the negligible function appeared in Section 3.2:

1. We have $1_{\overline{G}} \in X$.
2. We have $|X| \leq \varepsilon \cdot |\overline{G}|$.
3. For any $x, y \in \overline{G} \setminus X$, we have $\Pr_{g \leftarrow_R \overline{G}}[\ [gxg^{-1}, y] \in X\ ] \leq \varepsilon$.

Examples of commutator-separable groups will be shown in Section 6.1. We note that, only the *existence* of the subset $X$ as in Definition 2 matters in the proofs below, therefore $X$ need *not* be efficiently computable. Then, assuming that $\overline{G}$ is commutator-separable, the homomorphic functionality holds for class-0 and class-1 ciphertexts $c = (c_1, c_2)$ *with the additional property* $c_1 \notin X$. More precisely, we have the following result:

**Theorem 2.** *Assume that $\overline{G}$ is commutator-separable with the subset $X \subset \overline{G}$. Then:*

- *For any $m \in \{0,1\}$, the algorithm $\mathsf{Enc}(\mathsf{pk}, m)$ outputs, with probability at least $1 - \varepsilon$, a class-$m$ ciphertext $c = (c_1, c_2)$ satisfying $\varphi(c_1) \notin X$.*
- *For any $m \in \{0,1\}$, if $c$ is a class-$m$ ciphertext and $\varphi(c_1) \notin X$, then the output $c^\dagger$ of $\mathsf{NOT}(\mathsf{pk}, c)$ is a class-$(\neg m)$ ciphertext satisfying $\varphi(c_1^\dagger) \notin X$.*
- *Let $m, m' \in \{0,1\}$, $c$ be a class-$m$ ciphertext satisfying $\varphi(c_1) \notin X$, and $c'$ be a class-$m'$ ciphertext satisfying $\varphi(c_1') \notin X$. Then $\mathsf{AND}(\mathsf{pk}, c, c')$ outputs, with probability at least $1 - \varepsilon$, a class-$(m \wedge m')$ ciphertext $c^\dagger$ satisfying $\varphi(c_1^\dagger) \notin X$.*

*Hence, the proposed scheme $\Pi$ is an FHE scheme.*

*Proof.* First, since $1_{\overline{G}} \in X$ and $|\overline{G} \setminus X|/|\overline{G}| = 1 - |X|/|\overline{G}| \geq 1 - \varepsilon$, the same argument as the proof of Proposition 1 implies that $\Pr[\varphi(c_1) \notin X] \geq 1 - \varepsilon$ for $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$ and the assertion for $\mathsf{Enc}(\mathsf{pk}, m)$ holds. Secondly, the assertion for $\mathsf{NOT}(\mathsf{pk}, c)$ follows from Proposition 2 and the fact that $\mathsf{NOT}(\mathsf{pk}, c)$ does not change the first component $c_1$. Finally, for the assertion for $\mathsf{AND}(\mathsf{pk}, c, c')$, we have

$$\varphi(c_1^\dagger) = \varphi([gc_1g^{-1}, c_1']) = [\varphi(g)\varphi(c_1)\varphi(g)^{-1}, \varphi(c_1')] \ .$$

Since $\varphi(c_1), \varphi(c_1') \in \overline{G} \setminus X$ and $\varphi(g)$ is a uniformly random element of $\overline{G}$ by Lemma 1, Definition 2 implies that we have $\varphi(c_1^\dagger) \notin X$ with probability at least $1 - \varepsilon$. Therefore, the assertion holds by Proposition 3. This completes the proof of Theorem 2. □

## 5 Second Candidate of Shuffling Functions

In this section, we present another proposed choice of the shuffling functions $F_1$ and $F_2$ for our construction in Section 3. We define

$$F_1(x) = (g_1 x {g_1}^{-1})^{e_1} \cdot (g_2 x {g_2}^{-1})^{e_2} \cdot \dots \cdot (g_\ell x {g_\ell}^{-1})^{e_\ell} \quad \text{and} \quad F_2 = F_1 \ ,$$

where $\ell > 0$ is an integer parameter (independent of $x \in G$), $e_1, \dots, e_\ell$ are random integers, and $g_1, \dots, g_\ell \leftarrow \mathsf{Sample}_G$. Now condition (1) is satisfied since $g_i \cdot 1_G \cdot {g_i}^{-1} = 1_G$, and condition (2) is satisfied since $F_1$ is constructed from multiplications and inverses of elements of $G$ only, in a way similar to the case of Section 4. Hence the shuffling functions satisfy the two conditions.

We suppose that $\overline{G}$ has a non-commutative simple quotient group $\overline{G}_*$ satisfying $|\overline{G}_*|^{-1} \leq \varepsilon$. Let $\varphi_* \colon G \to \overline{G}_*$ be the composite map of $\varphi \colon G \to \overline{G}$ followed by the natural projection $\overline{G} \to \overline{G}_*$, hence $\varphi_*$ is a surjective group homomorphism as well as $\varphi$. For example, we may take $\overline{G}$ itself as the $\overline{G}_*$ if $\overline{G}$ is a non-commutative simple group (since we have assumed that $|\overline{G}|^{-1} \leq \varepsilon$). We note that, only the *existence* of the quotient group $\overline{G}_*$ matters in the proofs below, therefore $\overline{G}_*$ need *not* be efficiently computable. Then, for any $\overline{x}_* \in \overline{G}_* \setminus \{1_{\overline{G}_*}\}$, the simple group $\overline{G}_*$ is generated by the elements $h \cdot \overline{x}_* \cdot h^{-1}$ with $h \in \overline{G}_*$. Now for $x \in G$, we have

$$\varphi_*(F_1(x)) = (\varphi_*(g_1)\varphi_*(x)\varphi_*(g_1)^{-1})^{e_1} \cdot \dots \cdot (\varphi_*(g_\ell)\varphi_*(x)\varphi_*(g_\ell)^{-1})^{e_\ell}$$

and each $\varphi_*(g_i)$ is a uniformly random element of $\overline{G}_*$ by Lemma 1. If $\varphi_*(x) \neq 1_{\overline{G}_*}$, then $\varphi_*(F_1(x))$ is a product of powers of randomly chosen generators of $\overline{G}_*$ by the argument above. Therefore, we may expect that the following would hold by choosing a sufficiently large (but still polynomially bounded) parameter $\ell$:

**Assumption 1.** For any $x \in G$, if $\varphi_*(x) \neq 1_{\overline{G}_*}$, then the statistical distance between the probability distribution of $\varphi_*(F_1(x))$ and the uniform distribution over $\overline{G}_*$ is at most $\varepsilon$.

A concrete estimate of the sufficient number $\ell$ to guarantee Assumption 1 will be a future research topic. On the other hand, the following result by Guralnick and Robinson [18] is the key fact in our argument:

**Proposition 4** ([18], Theorem 9)**.** *For any finite non-commutative simple group $H$, we have*

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

In this setting, the homomorphic functionality holds for class-0 and class-1 ciphertexts $c = (c_1, c_2)$ *with the additional property* $\varphi_*(c_1) \neq 1_{\overline{G}_*}$. More precisely, we have the following result:

**Theorem 3.** *Assume that $\overline{G}$ has a non-commutative simple quotient group $\overline{G}_*$ satisfying $|\overline{G}_*|^{-1} \leq \varepsilon$. Then, under Assumption 1, we have:*

- *For any $m \in \{0,1\}$, the algorithm $\mathsf{Enc}(\mathsf{pk}, m)$ outputs, with probability at least $1 - \varepsilon$, a class-$m$ ciphertext $c = (c_1, c_2)$ satisfying $\varphi_*(c_1) \neq 1_{\overline{G}_*}$.*
- *For any $m \in \{0,1\}$, if $c$ is a class-$m$ ciphertext satisfying $\varphi_*(c_1) \neq 1_{\overline{G}_*}$, then the output $c^\dagger$ of $\mathsf{NOT}(\mathsf{pk}, c)$ is a class-$(\neg m)$ ciphertext satisfying $\varphi_*(c_1^\dagger) \neq 1_{\overline{G}_*}$.*
- *Let $m, m' \in \{0,1\}$, $c$ be a class-$m$ ciphertext satisfying $\varphi_*(c_1) \neq 1_{\overline{G}_*}$, and $c'$ be a class-$m'$ ciphertext satisfying $\varphi_*(c_1') \neq 1_{\overline{G}_*}$. Then $\mathsf{AND}(\mathsf{pk}, c, c')$ outputs, with probability at least $1 - (\sqrt{\varepsilon} + 2\varepsilon)$, a class-$(m \wedge m')$ ciphertext $c^\dagger$ satisfying $\varphi_*(c_1^\dagger) \neq 1_{\overline{G}_*}$.*

*Hence, the proposed scheme* $\Pi$ *is an FHE scheme.*

*Proof.* First, the same argument as the proof of Proposition 1 implies that $\Pr[\varphi_*(c_1) \neq 1_{\overline{G}_*}] \geq 1 - \varepsilon$ for $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$ and the assertion for $\mathsf{Enc}(\mathsf{pk}, m)$ holds. Secondly, the assertion for $\mathsf{NOT}(\mathsf{pk}, c)$ follows from Proposition 2 and the fact that $\mathsf{NOT}(\mathsf{pk}, c)$ does not change the first component $c_1$. Finally, for the assertion for $\mathsf{AND}(\mathsf{pk}, c, c')$, we have (since $F_2 = F_1$)

$$\varphi_*(c_1^\dagger) = \varphi_*([F_1(c_1), F_1(c_1')]) = [\varphi_*(F_1(c_1)), \varphi_*(F_1(c_1'))] \enspace .$$

Now if $\varphi_*(F_1(c_1))$ and $\varphi_*(F_1(c_1'))$ were uniformly random elements of $\overline{G}_*$, then the probability that $\varphi_*(c_1^\dagger) = 1_{\overline{G}_*}$ would be at most $|\overline{G}_*|^{-1/2} \leq \sqrt{\varepsilon}$ by Proposition 4 since $|\overline{G}_*|^{-1} \leq \varepsilon$. Then, by Assumption 1, the true probability $\Pr[\varphi_*(c_1^\dagger) = 1_{\overline{G}_*}]$ is at most $\sqrt{\varepsilon} + 2\varepsilon$, which is still negligible. Therefore, the assertion holds by Proposition 3. This completes the proof of Theorem 3. □

# 6 Towards Instantiation of the Proposed Scheme

In Section 6.1, we give examples of commutator-separable groups used in Section 4. Then in Section 6.2, we describe a candidate strategy for constructing instantiations of our proposed scheme.

## 6.1 Examples of Commutator-Separable Groups

Here we give examples of commutator-separable groups in Definition 2. For an element $g$ of any group $H$, let $Z_H(g)$ denote the centralizer of $g$ in $H$ defined by

$$Z_H(g) = \{h \in H \mid gh = hg\} \enspace .$$

Then the following holds for the probability appeared in Definition 2:

**Lemma 2.** *Let $H$ be a finite group, and let $X \subset H$. Then for any $x_1, x_2 \in H$, we have*

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

*Proof.* We put $H_y = \{g \in H \mid [g x_1 g^{-1}, x_2] = y\}$ for $y \in X$. Then we have

$$\Pr_{g \leftarrow_R H}[\ [g x_1 g^{-1}, x_2] \in X\ ] = \sum_{y \in X} \Pr_{g \leftarrow_R H}[\ [g x_1 g^{-1}, x_2] = y\ ] = \sum_{y \in X} \frac{|H_y|}{|H|} \enspace .$$

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

$$\begin{aligned}(g x_1 g^{-1}) x_2 (g x_1 g^{-1})^{-1} {x_2}^{-1} &= [g x_1 g^{-1}, x_2] \\ &= [g_y x_1 {g_y}^{-1}, x_2] = (g_y x_1 {g_y}^{-1}) x_2 (g_y x_1 {g_y}^{-1})^{-1} {x_2}^{-1} \enspace ,\end{aligned}$$

therefore $(g_y x_1 {g_y}^{-1})^{-1}(g x_1 g^{-1}) \in Z_H(x_2)$. Now for each $h \in Z_H(x_2)$, we put

$$H_{y,h} = \{g \in H_y \mid (g_y x_1 {g_y}^{-1})^{-1}(g x_1 g^{-1}) = h\} \enspace .$$

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 $g x_1 g^{-1} = g_y x_1 {g_y}^{-1} \cdot h = g_{y,h} x_1 {g_{y,h}}^{-1}$, therefore ${g_{y,h}}^{-1} g \in Z_H(x_1)$. This implies that $|H_{y,h}| \leq |Z_H(x_1)|$ for any $h \in Z_H(x_2)$. Summarizing, we have

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

Hence Lemma 2 holds. □

By using the result, we prove that the group

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

and its quotient group $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$, where $\mathbb{F}_q$ denotes the finite field with $q$ elements and $I$ denotes the identity matrix, are commutator-separable if $q$ is a function of $\lambda$ with sufficiently large values. For the purpose, we study the sizes of $Z_H(A)$ for $H \in \{\mathrm{SL}_2(\mathbb{F}_q), \mathrm{PSL}_2(\mathbb{F}_q)\}$ and each $A \in H$. First we show the following properties:

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

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

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

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 of Lemma 3. □

**Lemma 4.** *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.* First we note the following fact: For any finite group $H$ and its element $x$, we have $|Z_H(x)| = |H|/|x^H|$, where $x^H = \{hxh^{-1} \mid h \in H\}$ denotes the conjugacy class of $x$ in $H$. Now let $\pi\colon \mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ denote the natural projection. Then for each $\pi(x) \in \mathrm{PSL}_2(\mathbb{F}_q)$ with $x \in \mathrm{SL}_2(\mathbb{F}_q)$, the image of $x^{\mathrm{SL}_2(\mathbb{F}_q)}$ via the map $\pi$ is included in $\pi(x)^{\mathrm{PSL}_2(\mathbb{F}_q)}$. Since $\pi$ is a two-to-one map, this implies that $|\pi(x)^{\mathrm{PSL}_2(\mathbb{F}_q)}| \geq |x^{\mathrm{SL}_2(\mathbb{F}_q)}|/2$, therefore

$$|Z_{\mathrm{PSL}_2(\mathbb{F}_q)}(\pi(x))| = \frac{|\mathrm{PSL}_2(\mathbb{F}_q)|}{|\pi(x)^{\mathrm{PSL}_2(\mathbb{F}_q)}|} \leq \frac{|\mathrm{SL}_2(\mathbb{F}_q)|/2}{|x^{\mathrm{SL}_2(\mathbb{F}_q)}|/2} = \frac{|\mathrm{SL}_2(\mathbb{F}_q)|}{|x^{\mathrm{SL}_2(\mathbb{F}_q)}|} = |Z_{\mathrm{SL}_2(\mathbb{F}_q)}(x)| \ .$$

Hence the assertion follows from Lemma 3. □

By combining the results above, we have the following:

**Theorem 4.** *If the finite field* $\mathbb{F}_q$ *satisfies that*

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

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

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

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

by the condition for $\mathbb{F}_q$ in the statement. On the other hand, for any $x_1, x_2 \in H \setminus X$, Lemmas 3 and 4 imply that $|Z_H(x_1)|, |Z_H(x_2)| \leq 2q$. Therefore, by Lemma 2, we have

$$\Pr_{g \leftarrow_R H}[\ [g x_1 g^{-1}, x_2] \in X\ ] \leq \frac{(2/\eta) \cdot 2|\mathbb{F}| \cdot 2|\mathbb{F}|}{|\mathbb{F}|(|\mathbb{F}|^2-1)/\eta} = \frac{8|\mathbb{F}|}{|\mathbb{F}|^2-1} \leq \varepsilon$$

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

## 6.2 Candidate Strategy to Instantiate Our Scheme

Here we propose a strategy to give a candidate instantiation of the proposed scheme. An outline of the strategy is explained as follows:

1. We choose a surjective group homomorphism $\varphi_0 \colon G_0 \to \overline{G}$, where $\overline{G}$ satisfies the requirement in Section 4 or Section 5. In this step, it is not yet assumed that the subgroup membership problem for $\ker \varphi_0 \subset G_0$ is computationally hard.

2. We choose a (possibly infinite) group $\widetilde{G}_0$ containing $G_0$ as a subgroup, and randomly choose a group $\widetilde{G}$ isomorphic to $\widetilde{G}_0$ and a group isomorphism $\rho \colon \widetilde{G}_0 \xrightarrow{\sim} \widetilde{G}$. Then we define the group $G$ and the homomorphism $\varphi \colon G \to \overline{G}$ by $G = \rho(G_0)$ and $\varphi(g) = \varphi_0(\rho^{-1}(g))$ for $g \in G$. We conceal $\rho$ to make the subgroup membership problem $N = \ker \varphi \subset G$ computationally hard.

3. We randomly choose a generating set $\{\mathsf{gen}_{G_0,i}\}_{i=1}^{L_G}$ of $G_0$, and put $\mathsf{gen}_{G,i} = \rho(\mathsf{gen}_{G_0,i})$, therefore $\mathsf{gen}_G = \{\mathsf{gen}_{G,i}\}_{i=1}^{L_G}$ is a generating set of $G$. In a public key $\mathsf{pk}$, the group $G$ is specified by the pair of $\widetilde{G}$ and $\mathsf{gen}_G$. The algorithm $\mathsf{Sample}_G$ is defined as outputting a random product of random powers of elements randomly chosen from $\mathsf{gen}_G$, where the number of the multiplied elements is set to be sufficiently large in order to make the output of $\mathsf{Sample}_G$ statistically close to the uniform distribution on $G$. The algorithm $\mathsf{Sample}_N$ is defined similarly, by using a randomly chosen generating set $\mathsf{gen}_N$ of $N$ instead of $\mathsf{gen}_G$.

4. We construct the algorithm $\mathsf{Ker}_\varphi$. For example, $\mathsf{Ker}_\varphi$ may consist of $\varphi_0$ and $\rho^{-1}$, which enable one to compute the value $\varphi(g) = \varphi_0(\rho^{-1}(g))$ itself.

A possible way to do this is as follows. First, we define the homomorphism $\varphi_0 \colon G_0 \to \overline{G}$ by setting $G_0 = N_0 \times \overline{G}$ with some finite group $N_0$ and by taking the projection to the factor $\overline{G}$ as the map $\varphi_0$. Secondly, we choose a group $\widetilde{G}_0$ containing $G_0$ as above, which may be simply the group $G_0$ itself, together with a group presentation of $\widetilde{G}_0$ in terms of generators and their fundamental relations (see Appendix A for the terminology). Then we construct the group $\widetilde{G}$ by "obfuscating" the group presentation of $\widetilde{G}_0$ by a random composition of transformations, called Tietze transformations. More precisely, starting from a given group presentation of $\widetilde{G}_0$, we apply a sufficiently large number of the following transformations successively. Suppose that the group presentation at the current step is of the form $\langle g_1, \dots, g_n \mid r_1, \dots, r_m \rangle$. Then:

1. We randomly choose a generator $g_i$ and a word $w$ on the letters $g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n$, and take a new letter $g'$.

2. For each $r_j$, we substitute $g'w$ into each letter $g_i$ in $r_j$ and substitute $w^{-1}g'^{-1}$ into each letter ${g_i}^{-1}$ in $r_j$; let $\widetilde{r_j}$ denote the resulting word.

3. Then we define the new group presentation to be $\langle g_1, \dots, g_{i-1}, g', g_{i+1}, \dots, g_n \mid \widetilde{r_1}, \dots, \widetilde{r_m} \rangle$.

The record of the transformation process above gives a description of the isomorphism $\rho\colon \widetilde{G}_0 \to \widetilde{G}$, by which an element of $\widetilde{G}_0$ can be recovered from its "obfuscated" version in $\widetilde{G}$.

**On Efficient Computation in $\widetilde{G}$.** We note that, since each element of $\widetilde{G}$ can be represented by more than one words on the specified generating set of $\widetilde{G}$, it may be in general not efficient to decide whether given two elements of $\widetilde{G}$ are equal or not. To avoid the problem, it is desirable to provide (and specify in the public key) a way of calculating the normal form for each element (i.e., representatives of words representing each element). For example, we can apply Knuth–Bendix completion algorithm for term rewriting systems to the group presentation of $\widetilde{G}$. Unfortunately, Knuth–Bendix algorithm does not always halt for arbitrary inputs; therefore, we should either repeat the algorithm several times with various choices of parameters (reduction orderings), or change the original group presentation of $\widetilde{G}$, until the algorithm succeeds.

**On the Security.** A possible attack strategy against an instantiation of our proposed scheme obtained in the above-mentioned manner is to find a non-identity element $x \in \widetilde{G}$ with the property that $gx = xg$ for every $g \in N = \rho(N_0)$. If such an element is found, then for a given $g \in G = N \times \rho(\overline{G})$, $gx = xg$ holds for every $g \in N$ and $gx \neq xg$ would hold for a large fraction of $g \in G \setminus N$, which will enable the adversary to solve the subgroup membership problem. For example, any non-identity element $x$ of $\rho(\overline{G})$ satisfies the condition above, therefore such an element should not be efficiently found for security purpose. In particular, we consider the following strategy to find such an element: Sample elements $g = (g_0, g_1)$ of $G = N \times \rho(\overline{G})$ randomly and repeatedly, and check, for each pair of distinct elements $g = (g_0, g_1)$ and $g' = (g'_0, g'_1)$ obtained in this way, if $x = g^{-1}g'$ satisfies the condition (by checking whether $\mathsf{gen}_{N,i} \cdot x = x \cdot \mathsf{gen}_{N,i}$ for every generator $\mathsf{gen}_{N,i}$ of $N$ or not). Now the condition is satisfied if and only if $g_0 = g'_0$. By the birthday paradox, the order of the number of the sampled elements of $G$ until the suitable $x$ is found is expected to be $\sqrt{|N|}$, which is e.g., at least $2^{80}$ if $|N|$ is set to be at least $2^{160}$.

On the other hand, there may be a more direct attack that distinguishes distributions over $G = N \times \rho(\overline{G})$ and over $N$ without using such a special element $x$ as above. For example[3], suppose that both $N$ and $\rho(\overline{G})$ are alternating group $A_\lambda$ on $\lambda$ letters with $\lambda \geq 4$. Let $p$ be the largest odd prime with $p \leq \lambda$. Note that $p > \lambda/2$. Then the number of elements of $A_\lambda$ which are cyclic permutations on $p$ letters is $\binom{\lambda}{p}(p-1)! = \dfrac{2}{p \cdot (\lambda - p)!} \cdot |A_\lambda|$. This implies that, the probability (denoted by $P$) that $x^p = 1$ for a uniformly random element $x$ of $N = A_\lambda$ is $P = \dfrac{2}{p \cdot (\lambda - p)!} + \dfrac{1}{|A_\lambda|!}$. On the other hand, the probability that $x^p = 1$ for a uniformly random element $x$ of $G = A_\lambda \times A_\lambda$ is $P^2$. Since $\lambda - p$ is small for reasonable choices of $\lambda$ (e.g., $\lambda - p \leq 6$ for $\lambda \leq 80$), $P$ is significantly larger than $P^2$, therefore the uniform distributions over $G$ and over $N$ can be distinguished with non-negligible advantage by checking if $x^p = 1$ for a given element $x$.

The observation in the previous paragraph can be generalized as follows: If it is possible to efficiently find an integer $k$ satisfying that both $\Pr_{x \leftarrow_R N_0}[x^k = 1]$ and $1 - \Pr_{y \leftarrow_R \overline{G}}[y^k = 1]$ are non-negligible and at least one of them is noticeable, then an adversary can distinguish the uniform distributions over $G$ and over $N$ with non-negligible advantage by checking if a given element $z$ of $G$ or of $N$ satisfies $z^k = 1$. Therefore, such a $k$ should be difficult to find for security purpose.

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

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

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

**Candidates of the Groups.** Here we take $N_0 = \mathrm{SL}_2(\mathbb{F}_q)$ with $q$ odd and $\overline{G} = \mathrm{SL}_2(\mathbb{F}_{q'})$, where $1/q$ and $1/q'$ are negligible in $\lambda$, as a candidate of the underlying group $G_0 = N_0 \times \overline{G}$ for our proposed scheme satisfying the requirements in Section 4. Based on the argument in the previous paragraph, here we investigate the distribution of the orders of elements of $\mathrm{SL}_2(\mathbb{F}_q)$. Following the argument in Section 5.2 of [12], we choose a generator $\zeta$ of the cyclic group $(\mathbb{F}_q)^\times$. Then for an integer $i$ with $0 \le i \le q-2$, put $A_i = \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix}$. On the other hand, by considering the quadratic extension field $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, $\zeta$ has a square root in $(\mathbb{F}_{q^2})^\times$ (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 $\upsilon$ of the cyclic group $(\mathbb{F}_{q^2})^\times$. Then for an integer $i$ with $0 \le i \le q^2-2$, put $B_i = \begin{pmatrix} a & b \\ b\zeta & a \end{pmatrix}$ where $\upsilon^i = a + b\sqrt{\zeta}$. By using these notations, the list of conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ is obtained as in Table 1, where the second column (showing a representative element $x$ for each conjugacy class) and the third column (showing the size $\lvert x^{\mathrm{SL}_2(\mathbb{F}_q)}\rvert$ of the conjugacy class of $x$) are quoted (with slightly different notations) from Section 5.2 of [12]. The fourth column gives the order of an element of each conjugacy class, which is constant on each conjugacy class. Note that, for elements of type 8, 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 $\lvert x^{\mathrm{SL}_2(\mathbb{F}_q)}\rvert / \lvert \mathrm{SL}_2(\mathbb{F}_q)\rvert$ of the size of each conjugacy class of type 1 to 6 to the size of the whole group is at most $\dfrac{(q^2-1)/2}{q(q^2-1)} = \dfrac{1}{2q}$ which is negligible, therefore these 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 $\dfrac{(q-1)/2}{(q-1)/k}(q^2+q) = \dfrac{k}{2}(q^2+q)$, whose ratio to the size $q(q^2-1)$ of the whole group is $\dfrac{k}{2(q-1)}$. 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, by the choice of groups $N_0$ and $\overline{G}$, the attack strategy described above will be not effective provided the size of the coefficient field is appropriately concealed (e.g., by "obfuscating" the group presentation of $N_0 \times \overline{G}$ as above). We also note that, instead of $\mathrm{SL}_2(\mathbb{F}_q)$ itself, some more complicated group having $\mathrm{SL}_2(\mathbb{F}_q)$ as a quotient group may be taken as $N_0$ for safety; e.g., the semidirect product $\mathrm{SL}_2(\mathbb{F}_q) \rtimes \mathrm{SL}_2(\mathbb{F}_q)$ of two copies of $\mathrm{SL}_2(\mathbb{F}_q)$ via the conjugate action of the right-side $\mathrm{SL}_2(\mathbb{F}_q)$ on the left-side $\mathrm{SL}_2(\mathbb{F}_q)$.

For the construction above, we can use the following fact for short group presentations of $\mathrm{SL}_2(\mathbb{F}_q)$:

**Proposition 5** ([17], Section 3.2)**.** *If $q$ is prime and $q > 3$, then $\mathrm{SL}_2(\mathbb{F}_q)$ has a group presentation with four generators and eight relations, where each relation is represented by a word of length $O(\log q)$ in the generators.*

We also note that, several finite non-commutative simple groups also admit short group presentation as shown in the same paper [17]; owing to this fact, we can also use those simple groups such as $\mathrm{PSL}_2(\mathbb{F}_q)$ instead of $\mathrm{SL}_2(\mathbb{F}_q)$ in the construction above.


### Acknowledgments

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


## References


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

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

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

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

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

[6] Z. Brakerski and 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 and A. Yun, Batch Fully Homomorphic Encryption over the Integers, in: Proceedings of EUROCRYPT 2013, LNCS 7881, 2013, pp.315–335.

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

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

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

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

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

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

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

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

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

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

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

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

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

[21] K. H. Ko, S. Lee, J. H. Cheon, J. W. Han, J.-S. Kang and C. Park, New Public-Key Cryptosystem Using Braid Groups, in: Proceedings of CRYPTO 2000, LNCS 1880, 2000, pp.166–183.

[22] K. Nuida and 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.

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

[24] S.-H. Paeng, K.-C. Ha, J. H. Kim, S. Chee and C. Park, New Public Key Cryptosystem Using Finite Non Abelian Groups, in: Proceedings of CRYPTO 2001, LNCS 2139, 2001, pp.470–485.

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

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

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

# A Preliminaries for Group Theory

Here we summarize some definitions and facts used in the main text; see e.g., [25] for more details. For any group $G$, we say that a subgroup $N$ of $G$ is *normal*, if we have $g \cdot x \cdot g^{-1} \in N$ for any $x \in N$ and $g \in G$. For example, for any group homomorphism $\varphi \colon G \to H$ from $G$ to another group $H$, the *kernel* $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$ of $\varphi$ is a normal subgroup of $G$. If $N$ is normal, we define $G/N = \{gN \mid g \in G\}$ where $gN = \{gx \mid x \in N\} \subset G$. Note that $gN = hN$ (as subsets of $G$, or as elements of $G/N$) if and only if $g^{-1}h \in N$. Then the set $G/N$ forms a group, called the *quotient* of $G$ by $N$, with multiplication operator defined by $(gN) \cdot (hN) = ghN$ for $g, h \in G$. Now the (*natural*) *projection* $\pi$ from $G$ to $G/N$ is defined by $\pi(g) = gN$, $g \in G$. This is a surjective group homomorphism, and its kernel is equal to $N$, hence $G/\ker \varphi$ is (trivially) isomorphic to $G/N$. Similarly, given a surjective group homomorphism $\varphi \colon G \to H$, it is known that the quotient group $G/\ker \varphi$ is isomorphic to $H$, via a map $g \ker \varphi \mapsto \varphi(g)$ for $g \in G$.

We say that a group $G$ is *simple*, if $G$ does not have normal subgroups other than $G$ itself and $\{1_G\}$. For example, let $S_n$ denote the symmetric group on $n$ letters, i.e., the group of permutations $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ with multiplication operator given by the composition of maps. Let $A_n$ denote the alternating group on $n$ letter, i.e., the (normal) subgroup of $S_n$ of permutations that can be written as the product of an even number of transpositions $(a\ b)$, $a, b \in \{1, 2, \dots, n\}$ (which is the permutation exchanging $a$ and $b$ and fixing other elements of $\{1, 2, \dots, n\}$). Then $A_n$ is a simple group if $n \geq 5$.

For a subset $X$ of a group $G$, the subgroup of $G$ *generated* by $X$, denoted by $\langle X \rangle$, is defined to be the set of elements of $G$ written in the form ${x_1}^{e_1} \cdots {x_n}^{e_n}$ with $n \geq 0$, $x_i \in X$ and $e_i \in \mathbb{Z}$ (the element is regarded as $1_G$ if $n = 0$). On the other hand, the normal subgroup generated by $X$ or the *normal closure* of $X$, denoted by $\langle X \rangle_{\mathrm{normal}}$, is defined to be the subgroup generated by $\{gxg^{-1} \mid x \in X\,,\, g \in G\}$. Then $\langle X \rangle$ is the unique minimal subgroup of $G$ containing $X$, and $\langle X \rangle_{\mathrm{normal}}$ is the unique minimal normal subgroup of $G$ containing $X$. We say that $X$ is a *generating set* of $G$ or $X$ *generates* $G$, if $\langle X \rangle = G$. For example, the symmetric group $S_n$ is generated by the adjacent transpositions $(a\ a+1)$ for $a \in \{1, 2, \dots, n-1\}$. We note that, for any simple group $G$ and any $x \in G \setminus \{1_G\}$, $\langle x \rangle_{\mathrm{normal}}$ is a normal subgroup of $G$ different from $\{1_G\}$, therefore we have $\langle x \rangle_{\mathrm{normal}} = G$, i.e., $G$ is generated by the elements $gxg^{-1}$ with $g \in G$.

For any set $X$, let $X^{\pm}$ denote the disjoint union $X \cup X^{-1}$ of $X$ and the set of symbolic inverses $X^{-1} = \{x^{-1} \mid x \in X\}$ of elements of $X$. Let $F(X)$ be the set of finite-length words on the alphabet $X^{\pm}$, where two words are regarded as the same element in $F(X)$ if and only if, any of the two words can be converted to the other by successively inserting or removing subwords of the form $xx^{-1}$ or $x^{-1}x$ with $x \in X$. Then $F(X)$ forms a group, where multiplication is defined by concatenation of words, and the empty word, denoted by 1, is the identity element of $F(X)$. Now for any subset $R$ of $F(X)$, the group defined by the *group presentation* $\langle X \mid R \rangle$ is defined as the quotient group $F(X)/\langle R \rangle_{\mathrm{normal}}$. Intuitively, each element of this group is represented by a word on $X^{\pm}$ of finite length, the multiplication in this group corresponds to concatenation of words, and two words represent the same element of this group if and only if, any of the two words can be converted to the other by successively inserting or removing subwords of the form $xx^{-1}$, $x^{-1}x$ or $r$ with $x \in X$, $r \in R$. For example, it is known that $S_n$ has the following group presentation $\langle s_1, \dots, s_{n-1} \mid {s_i}^2\ (\forall i)\,,\, (s_i s_j)^3\ (|j-i| = 1)\,,\, (s_i s_j)^2\ (|j-i| \geq 2) \rangle$, where $s_i$ denotes the adjacent transposition $(i\ i+1)$.