Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory

Koji Nuida

Abstract In CRYPTO 2008, 1 year earlier than Gentry's pioneering "bootstrapping" technique for the first fully homomorphic encryption (FHE) scheme, Ostrovsky and Skeith III had suggested a completely different approach towards achieving FHE. They showed that the NAND operator can be realized in some *non-commutative* groups; consequently, homomorphically encrypting the elements of the group will yield an FHE scheme, without ciphertext noise to be bootstrapped. 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. 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 $\pi : \widetilde{G} \to G$ 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 G. 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. Concretely realizing FHE schemes based on our proposed framework is left as a future research topic.

Keywords Fully homomorphic encryption · Non-commutative group · Combinatorial group theory

K. Nuida (✉)
Graduate School of Information Science and Technology,
The University of Tokyo, Tokyo, Japan
e-mail: nuida@mist.i.u-tokyo.ac.jp

National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan

T. Takagi et al. (eds.), *International Symposium on Mathematics, Quantum Theory, and Cryptography*, Mathematics for Industry 33,
https://doi.org/10.1007/978-981-15-5191-8_8

1 Introduction

Until the pioneering work by Gentry (2009) in 2009, it had been a long-standing open problem to construct *fully homomorphic encryption* (*FHE*) that enables arbitrary "computation on encrypted data" via "homomorphic" operations on the ciphertexts. After Gentry's work, studies of FHE to improve the efficiency (e.g. Chillotti et al. 2016; Ducas and Micciancio 2015; Gentry et al. 2012; Stehlé and Steinfeld 2010) and to give various frameworks of construction (e.g. Brakerski and Vaikuntanathan 2011; Cheon and Stehlé 2015; van Dijk et al. 2010; Gentry and Halevi 2011; Nuida and Kurosawa 2015) have been one of the main research topics in cryptology (see, e.g. Silverberg 2013 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, makes the syntax of FHE less analogical to the classical homomorphic encryption, and causes somewhat unclear treatments regarding so-called circular security.

On the other hand, in 2008 (1 year earlier than Gentry 2009), Ostrovsky and Skeith III (2008) 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. Consequently, if the elements of the underlying 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

In Sect. 3, we revisit the approach towards constructing FHE suggested in Ostrovsky and Skeith (2008). We give a formalization of "realizations of bit operators in groups" in a slightly generalized manner (e.g. our formalization can also handle probabilistic realizations of bit operators, which were not considered in Ostrovsky and Skeith 2008). Then we reduce the problem of "homomorphically encrypting the elements of a group G" to finding a surjective homomorphism $\pi : \widetilde{G} \to G$ from another finite group $\widetilde{G}$ (which plays the role of the ciphertext space) satisfying certain conditions and prove that the resulting FHE scheme is CPA-secure if the elements of the kernel

of π ($\ker \pi$) 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 Sect. 4, we propose new methodologies to realize bit operators in some groups, which are different from the previous methodology in Ostrovsky and Skeith (2008) analogous to Barrington's theorem (Barrington 1986) (recalled in Sect. 4.1). Our result enlarges the possibility of the underlying group G to find a suitable construction.

Finally, in Sect. 5, we give some observations and discussions on how to find a suitable homomorphism $\pi : \widetilde{G} \to G$. In Sect. 5.2, we give an observation that a naive approach to construct the group $\widetilde{G}$ by using embedding of a matrix group G into a larger matrix group and then taking its random conjugate would never yield a secure FHE scheme, due to the existence of a kind of "linear" constraint that separates the elements of $\ker \pi$ from general elements of $\widetilde{G}$ (where the "linearity" causes that such a constraint does not disappear even by taking random conjugate). This observation shows an importance of finding a homomorphism $\pi : \widetilde{G} \to G$ onto a given underlying group G without linear constraints for elements of $\ker \pi$. Towards constructing such a homomorphism π, in Sect. 5.3, we propose another approach using combinatorial group theory, i.e. the properties of presentations of groups in terms of generators and fundamental relations. Then, in Sect. 5.4, we discuss several problems to be resolved in order to realize our proposed approach, many of which would be of independent interest from mathematical viewpoints.

2 Preliminaries

Let $a \leftarrow \mathcal{X}$ mean that a random variable $\mathcal{X}$ takes a value a. Let $a \leftarrow_R X$ mean that an element a is chosen uniformly at random from a finite set X. The *statistical distance* between two probability distributions $\mathcal{X}, \mathcal{Y}$ over a finite set A is defined by $\Delta(\mathcal{X}, \mathcal{Y}) = (1/2) \sum_{z \in A} |\Pr[z \leftarrow \mathcal{X}] - \Pr[z \leftarrow \mathcal{Y}]|$. For $\varepsilon \geq 0$, we say that $\mathcal{X}$ is ε-*close* to $\mathcal{Y}$, if $\Delta(\mathcal{X}, \mathcal{Y}) \leq \varepsilon$. We say that a function $\varepsilon = \varepsilon(\lambda) \geq 0$ is *negligible*, if $\varepsilon = \lambda^{-\omega(1)}$. We say that $\varepsilon \in [0, 1]$ is *overwhelming*, if $1 - \varepsilon$ is negligible; and ε is *noticeable*, if there exist integers $n \geq 1$ and $\lambda_0 > 0$ for which 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 for a plaintext m. The *decryption algorithm* $\mathsf{Dec}(c) = \mathsf{Dec}_{\mathsf{sk}}(c)$ for a ciphertext c outputs either a plaintext or a "failure" symbol $\perp$. The *correctness* of a PKE scheme means that, for any plaintext m, the probability $\Pr[\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m)) \neq m]$ (taken over the internal randomness for the algorithms) is negligible.

For a finite set $\mathcal{M}$, we say that a set $\mathcal{F}$ of operators on $\mathcal{M}$ is *functionally complete*, if any (multivariate) 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:

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

The reader may refer to a textbook of group theory (e.g. Robinson 1996) for definitions and basic facts for groups mentioned without explicit references.

3 Our Framework for FHE

In this section, we describe our framework towards constructing FHE free from ciphertext noise. This can be seen as formalizing a framework suggested in Khamsemanan et al. (2016) and Ostrovsky and Skeith (2008).

3.1 Group-Theoretic Realization of Functions

Roughly speaking, a group-theoretic realization of a function in a group is emulating the function "by using the group operators only". To formalize it, we prepare some definitions. Let $w = w(x_1, \ldots, x_n)$ be a sequence of finite length over alphabet $\{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\}$, called a *group word* with variables $x_1, \ldots, x_n$. Then one can *substitute* given elements $g_1, \ldots, g_n$ of a group into the variables $x_1, \ldots, x_n$ in $w(x_1, \ldots, x_n)$ to yield an element of the same group, denoted by $w(g_1, \ldots, g_n)$.

Then we define a group-theoretic realization of functions as follows. In comparison to a similar definition in Khamsemanan et al. (2016) that was deterministic with a single component, our formulation here also covers probabilistic situations with multiple components.

Definition 1 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 $X_m \subseteq G^n$ for all $m \in \mathcal{M}$;
- for $f \in \mathcal{F}$, a collection $\vec{w}_f(\vec{x}_1, \ldots, \vec{x}_{\ell_f}, \vec{y})$ of n group words $w_{f,i}(\vec{x}_1, \ldots, \vec{x}_{\ell_f}, \vec{y})$ $(i = 1, \ldots, n)$ of polynomially bounded lengths, where $\vec{x}_j = (x_{j,1}, \ldots, x_{j,n})$ for $j = 1, \ldots, \ell_f$ and $\vec{y} = (y_1, \ldots, y_k)$;
- a collection $\vec{r} = (r_1, \ldots, r_k)$ of polynomial-time samplable random variables on G;

satisfying the following condition, where negl is some negligible value: 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 not larger than negl.

For each $f \in \mathcal{F}$, we denote by $\mathcal{A}_f$ 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, in the formulation above, some of the random variables r_h may take a constant value in G. When all the random variables appearing in a realization are constant, we call the realization *deterministic*, or else call it *probabilistic*.

3.2 *Lift of Realization of Functions*

Given a group homomorphism $\widetilde{G} \to G$ and a realization of functions in the target group G, the notion of a "lift" of the realization up to the source group $\widetilde{G}$ defined below plays a role of homomorphic operations in our proposed framework for FHE. We note that such a notion was not introduced in the previous work (Khamsemanan et al. 2016; Ostrovsky and Skeith 2008).

Definition 2 We suppose that a set $\mathcal{F}$ of functions on $\mathcal{M}$ has a realization in a group G as in Definition 1. Let $\pi : \widetilde{G} \to G$ be a surjective group homomorphism. We define a *lift* of the realization up to $\widetilde{G}$ to be a collection of polynomial-time samplable random variables $\widetilde{r}_1, \ldots, \widetilde{r}_k$ on $\widetilde{G}$ with the property that each value $\pi(\widetilde{r}_h) \in G$ has the same probability distribution as r_h. Then for each $f \in \mathcal{F}$, we denote by $\widetilde{\mathcal{A}}_f$ 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.

In the following, we also write as π the map $(\widetilde{G})^n \to G^n$ with $\pi(\widetilde{g}_1, \ldots, \widetilde{g}_n) = (\pi(\widetilde{g}_1), \ldots, \pi(\widetilde{g}_n))$.

Lemma 1 *In the situation of Definition 2, 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 negl as in Definition 1.*

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

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

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

3.3 The Proposed Framework

Based on the definitions above, here we describe our proposed framework for constructing FHE:

$\mathsf{Gen}(1^\lambda)$: Choose the following objects according to the security parameter λ, where $\mathcal{M}$ is the set of plaintexts and $\mathcal{F}$ is a functionally complete set of operators on $\mathcal{M}$:

- a group-theoretic realization (of some degree n) of $\mathcal{F}$ on a group G;
- a surjective group homomorphism $\pi : \widetilde{G} \to G$ and a lift of the realization of $\mathcal{F}$ up to $\widetilde{G}$;
- a polynomial-time samplable random variable $r_{\ker}$ on the kernel $\ker \pi$ of π;
- for each $m \in \mathcal{M}$, a tuple $\vec{\mathsf{gen}}_m = (\mathsf{gen}_{m,1}, \ldots, \mathsf{gen}_{m,n}) \in (\widetilde{G})^n$ with $\pi(\vec{\mathsf{gen}}_m) \in X_m$.

Then output a public key pk consisting of $\widetilde{G}$, $r_{\ker}$, $\vec{\mathsf{gen}}_m$ 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 $\vec{r}_{\ker} = (r_{\ker,1}, \ldots, r_{\ker,n})$ of the random variable $r_{\ker}$ independently, and then output $\vec{c} = (c_1, \ldots, c_n) \leftarrow \vec{\mathsf{gen}}_m \cdot \vec{r}_{\ker} \in (\widetilde{G})^n$.

$\mathsf{Dec}_{\mathsf{sk}}(c)$ 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, then output $\perp$.

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

The correctness of Enc is obvious; when $\vec{c} = \vec{\mathsf{gen}}_m \cdot \vec{r}_{\ker} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$, we have

$$\pi(\vec{c}) = \pi(\vec{\mathsf{gen}}_m) \cdot (\pi(r_{\ker,1}), \ldots, \pi(r_{\ker,n})) = \pi(\vec{\mathsf{gen}}_m) \cdot (1_G, \ldots, 1_G) = \pi(\vec{\mathsf{gen}}_m) \in X_m$$

as $r_{\ker,i} \in \ker \pi$ for each i. The correctness of Eval is just a restatement of Lemma 1. On the other hand, 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*

distribution over $\widetilde{G}$ is polynomial-time samplable. Then, our proposed FHE scheme is CPA-secure if the subgroup membership problem for $\ker\pi \subseteq \widetilde{G}$ *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:*

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

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 $i \leftarrow_R \{1, \ldots, n\}$ and executes $\mathcal{A}(\text{submit}, 1^\lambda, \mathsf{pk})$ to obtain a tuple (m_0, m_1, st).
2. The adversary $\mathcal{A}^\dagger$ chooses $b^* \leftarrow_R \{0,1\}$ and executes $\mathcal{A}(\text{guess}, 1^\lambda, \mathsf{pk}, \mathsf{st}, c^{b^*,b^\dagger,i})$ 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 $u_{i+1}, \ldots, u_n \leftarrow_R \widetilde{G}$.
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

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

and

$$\begin{aligned}\Pr[b = 0 \mid b^\dagger = 0] &= \Pr[b' = b^* \mid b^\dagger = 0] \\ &= \sum_{i=1}^{n} \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\text{guess}, 1^\lambda, \mathsf{pk}, \mathsf{st}, c^{b^*,0,i})]\ ,\end{aligned}$$

while

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

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 an identical probability distribution. Therefore, we have

$$\Pr[b = 0 \mid b^\dagger = 0] + \Pr[b = 1 \mid b^\dagger = 1] - 1$$
$$= \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\text{guess}, 1^\lambda, \mathsf{pk}, \mathsf{st}, c^{b^*,0,n})] - \frac{1}{n} \Pr[b^* \leftarrow \mathcal{A}(\text{guess}, 1^\lambda, \mathsf{pk}, \mathsf{st}, c^{b^*,1,1})] \ .$$

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

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

and

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

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

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

As 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 of Theorem 1. □

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) was proved in the previous work (Khamsemanan et al. 2016; Ostrovsky and Skeith 2008) (see, e.g. Theorem 2.1 of Ostrovsky and Skeith 2008).

Proposition 1 (Khamsemanan et al. 2016; Ostrovsky and Skeith 2008) *Let G be any non-commutative finite simple group. Then there exists a deterministic, degree-*1 *group-theoretic realization of* NAND *in G.*

We note that its proof, utilizing the commutators $[g, h] = ghg^{-1}h^{-1}$ in a way analogous to Barrington's theorem (Barrington 1986), is in general not constructive. A concrete construction was given in Sect. 6 of Khamsemanan et al. (2016) only for the smallest case $G = A_5$, where the group word has a length 65.

4.2 Deterministic Case: Proposed Constructions

Here, we propose a completely different approach, which we call *approximate-then-adjust method*, to obtain deterministic realizations of operators in some small groups. An intuitive explanation is as follows. For example, the operations $b_1 \,\mathsf{OR}\, b_2$ and $b_1 + b_2 \bmod 3$ have equal outputs for all but one input pairs $(b_1, b_2) \neq (1, 1)$ in $\{0, 1\}^2$, and $1 + 1 \bmod 3 = 2$ (instead of $1 \,\mathsf{OR}\, 1 = 1$) is "overflowed" from the correct output set $\{0, 1\}$. As the operation $b_1 + b_2 \bmod 3$ is easily realizable by using a cyclic subgroup of order 3, the problem has been reduced to realize the "adjusting function" $0 \mapsto 0$, $1 \mapsto 1, 2 \mapsto 1$ in a group.

In fact, by putting $\sigma_b = (1, 2, 3)^b \in S_5$ for $b \in \{0, 1, 2\}$ (where S_k denotes the symmetric group on k letters) and identifying each σ_b with b, the adjusting function mentioned above can be realized by a group word

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

(formally, the left-hand side is an abbreviation of $w^{\mathsf{out}}(g, \vec{y})$ where the variables in $\vec{y}$ take constant values over $G = S_5$ appearing in the right-hand side). This adjusting function defined by w^{out} is also applicable to other operations NAND, XOR, and EQ ($= \mathsf{NOT} \circ \mathsf{XOR}$). Namely, by putting

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

an output of each w^{in}_f for inputs in $\{\sigma_0, \sigma_1\}$ becomes either equal (via the identification $\sigma_b \leftrightarrow b$) to f, or σ_2 ($\leftrightarrow 2$) instead of σ_1 ($\leftrightarrow 1$). Hence, the composition $w^{\mathsf{out}}(w^{\mathsf{in}}_f(g_1, g_2))$ gives a correct group word to realize the operator f with $X_0 = \{\sigma_0 = 1_{S_5}\}$ and $X_1 = \{\sigma_1\}$. We also note that NOT is easily realized with the same X_0 and X_1 by $w^{\mathsf{NOT}}(g) = g^{-1}\sigma_1$.

This method is also applicable to realizing arithmetic operations for $\mathbb{F}_3$. We put $\sigma_b = (1, 2, 3)^b \in S_5$ for $b \in \{0, 1, 2\}$ again, and set $X_b = \{\sigma_b\}$ for each b. Then the addition $+$ is easily realized by $w_+(g_1, g_2) = g_1 g_2$. For the multiplication $\times$, the following group word

$$w_{\times}^{\mathsf{in}}(g_1, g_2) = g_1((1,4)(2,3,5))^{-1} g_2 (1,4)(2,3,5)$$

satisfies that $w_{\times}^{\mathsf{in}}(\sigma_{b_1}, \sigma_{b_2}) \in X'_{b_1 \times b_2 \bmod 3}$ for any $b_1, b_2 \in \{0,1,2\}$, where

$$\begin{aligned} X'_0 &= \{1_{S_5}, (2,4,5), (2,5,4), (1,2,3), (1,3,2)\} \ , \\ X'_1 &= \{(1,2,4,5,3), (1,3,2,5,4)\} \ , \\ X'_2 &= \{(1,2,5,4,3), (1,3,2,4,5)\} \ . \end{aligned}$$

On the other hand, by putting

$$\begin{aligned} &w'_1(g) = g^3 \ , \ w'_2(g) = w'_3(g) = (2,3,4)^{-1} g^{-1} (3,4,5) g^2 (3,4,5)^{-1} g (2,3,4) \ , \\ &w'_4(g) = g(1,5,3,4,2) g^{-1} (1,5,3,4,2)^{-1} g (1,4,2,3,5) g^{-1} (1,4,2,3,5)^{-1} \ , \end{aligned}$$

the composed group word $w^{\mathsf{out}}(g) = w'_4(w'_3(w'_2(w'_1(g))))$ satisfies that $w^{\mathsf{out}}(g) = \sigma_b$ for any $b \in \{0,1,2\}$ and any $g \in X'_b$. Hence, the group word $w_{\times}(g_1, g_2) = w^{\mathsf{out}}(w_{\times}^{\mathsf{in}}(g_1, g_2))$ realizes the operator $\times$ for $\mathbb{F}_3$, as desired. We note that the group words in the arguments above are found by heuristic searches; a systematic method to find such group words is a future research topic.

4.3 Preliminaries: On Random Sampling of Group Elements

In the probabilistic constructions described below, the following result by Dixon (2008) on almost uniform sampling over any finite group G would be useful in implementation. We introduce a notation: for any $g_1, \ldots, g_L \in G$, let $\mathsf{Sample}[g_1, \ldots, g_L]$ denote the random variable that takes the value $g_1^{e_1} \cdots g_L^{e_L} \in G$ with $e_1, \ldots, e_L \leftarrow_R \{0,1\}$.

Proposition 2 (Dixon 2008, Theorem 3) *Let G be a finite group, let $0 \leq \varepsilon < 1$, and let $\mathcal{U}$ be a random variable over G that is ε-close to the uniform random variable on G. Let L be a positive integer, and let $h, k \geq 0$. If*

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

then we have $\Pr_{g_1, \ldots, g_L \leftarrow \mathcal{U}} [\, \mathsf{Sample}[g_1, \ldots, g_L] \text{ is not } 2^{-k}\text{-close to uniform} \,] < 2^{-h}$.

4.4 Probabilistic Case: "Commutator-Separable" Groups

We propose a degree-2 probabilistic realization of $\{\mathsf{NOT}, \mathsf{AND}\}$ in the following class of groups.

Definition 3 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

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

Moreover, we say that a family of finite groups $G = G_\lambda$ indexed 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.

Let G be an ε-commutator-separable group. We put

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

where $Y \subseteq G \setminus \{1_G\}$ is as in Definition 3. Then NOT is easily realized by the group words (where $\vec{g} = (g_1, g_2)$)

$$\vec{w}_{\mathsf{NOT}}(\vec{g}) = (w_{\mathsf{NOT},1}(\vec{g}), w_{\mathsf{NOT},2}(\vec{g})) = (g_1, g_2^{-1} g_1)\ .$$

On the other hand, we define the (probabilistic) group words for AND by

$$\begin{aligned} \vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'}) &= (w_{\mathsf{AND},1}(\vec{g}, \vec{g'}), w_{\mathsf{AND},2}(\vec{g}, \vec{g'})) \\ &= ([ug_1u^{-1}, g_1'], [ug_2u^{-1}, g_2']) \text{ with } u \leftarrow_R G\ . \end{aligned}$$

For any $\vec{g}, \vec{g'} \in X_0 \cup X_1$, the condition (1) implies that $\Pr[w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) \notin Y] \leq \varepsilon$ where the probability is taken over the random choice of u in $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'})$. Moreover, when $\vec{g} \in X_0$ or $\vec{g'} \in X_0$, we have $g_2 = 1_G$ or $g_2' = 1_G$; therefore, $w_{\mathsf{AND},2}(\vec{g}, \vec{g'}) = 1_G$. On the other hand, when $\vec{g}, \vec{g'} \in X_1$, we have $g_2 = g_1$ and $g_2' = g_1'$; therefore, $w_{\mathsf{AND},2}(\vec{g}, \vec{g'}) = w_{\mathsf{AND},1}(\vec{g}, \vec{g'})$. Summarizing, $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'})$ is a realization of AND with error probability $\leq \varepsilon$.

Remark 1 Although only the *existence* of such a subset Y is concerned in Definition 3, 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, we show that the groups $\mathrm{SL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ are commutator-separable if the order q of the coefficient field $\mathbb{F}_q$ satisfies that $1/q$ is negligible. In the following, let $Z_H(g) = \{h \in H \mid gh = hg\}$ denote the centralizer of g in a group H. We note that $|Z_H(g)| = |H|/|g^H|$ for any $g \in H$, where $g^H = \{hgh^{-1} \mid h \in H\}$ denotes the conjugacy class of g in H.

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

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

Proof For $y \in X$, we have $[gx_1g^{-1}, x_2] = y$ if and only if $(gx_1g^{-1})x_2(gx_1g^{-1})^{-1} = yx_2$. As the mapping $h \mapsto hzh^{-1}$ is a $|Z_H(z)|$-to-1 mapping for any $z \in H$, there are at most $|Z_H(x_2)|$ possibilities of the value of gx_1g^{-1} to satisfy the condition $(gx_1g^{-1})x_2(gx_1g^{-1})^{-1} = yx_2$; and for each of them, there are at most $|Z_H(x_1)|$ possibilities of the value of g. This completes the proof. □

Lemma 3 *Let $\varphi\colon H_1 \to H_2$ be a surjective group homomorphism between two finite groups, and let $x \in H_1$. Then we have $|Z_{H_2}(\varphi(x))| \leq |Z_{H_1}(x)|$.*

Proof As φ is a surjective homomorphism, it is a $(|H_1|/|H_2|)$-to-1 mapping and we have $\varphi(x^{H_1}) = \varphi(x)^{H_2}$. Therefore $|x^{H_1}| \leq (|H_1|/|H_2|) \cdot |\varphi(x)^{H_2}|$, or equivalently $|H_2|/|\varphi(x)^{H_2}| \leq |H_1|/|x^{H_1}|$. Hence the claim holds. □

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 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$ with $A \neq \pm I$, and let $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in Z_{\mathrm{SL}_2(\mathbb{F}_q)}(A)$; therefore, $\det(X) = 1$ and $XA = AX$. Then we have

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

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 condition $A \neq \pm I$ 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 4. □

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 Apply Lemma 3 to the natural projection $\mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ and use Lemma 4. □

Theorem 2 *If $\dfrac{8q}{q^2 - 1} \leq \varepsilon$, or equivalently $q \geq \dfrac{4 + \sqrt{16 + \varepsilon^2}}{\varepsilon} \approx \dfrac{8}{\varepsilon}$, then $\mathrm{SL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q)$ are ε-commutator-separable with $Y = \mathrm{SL}_2(\mathbb{F}_q) \setminus \{\pm I\}$ 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 $|H \setminus Y| = 2/\eta$. 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

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

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

4.5 Probabilistic Case: Simple Groups

We also give a variant of the probabilistic realization described in Sect. 4.4. Although the correctness below relies on a heuristic assumption, the underlying group G for the realization can be taken as any sufficiently large non-commutative finite simple group.

The realization of NOT is similar to Sect. 4.4. Namely, we put

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

and, for $\vec{g} = (g_1, g_2)$,

$$\vec{w}_{\mathsf{NOT}}(\vec{g}) = (w_{\mathsf{NOT},1}(\vec{g}), w_{\mathsf{NOT},2}(\vec{g})) = (g_1, g_2^{-1} g_1)\ .$$

From now, we consider the realization of AND. First we note that, for any $g \in G \setminus \{1_G\}$, the normal closure of $\{g\}$ in G is equal to the whole G as G is simple; hence, G is generated by the set g^G. Keeping this property in mind, we put the following heuristic assumption:

Assumption 1 Let $\varepsilon > 0$ be a negligible value, 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 $u_1 g u_1^{-1} \cdots u_L g u_L^{-1}$, where $u_1, \ldots, u_L \leftarrow_R G$, is ε-close to the uniform distribution over G.

Now we define $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'}) = (w_{\mathsf{AND},1}(\vec{g}, \vec{g'}), w_{\mathsf{AND},2}(\vec{g}, \vec{g'}))$ by

$$w_{\mathsf{AND},i}(\vec{g}, \vec{g'}) = [r_1 g_i r_1^{-1} \cdots r_L g_i r_L^{-1}, r_{L+1} g'_i r_{L+1}^{-1} \cdots r_{2L} g'_i r_{2L}^{-1}] \text{ for } i = 1, 2$$

where $r_1, \ldots, r_{2L} \leftarrow_R G$ are common to both $i = 1, 2$. Then an argument similar to Sect. 4.4 implies that, for $\vec{g} \in X_b$ and $\vec{g'} \in X_{b'}$, we have $\vec{w}_{\mathsf{AND}}(\vec{g}, \vec{g'}) \in X_{b\,\mathsf{AND}\,b'}$ *provided* $w_{\mathsf{AND},1}(\vec{g}, \vec{g'}) \neq 1_G$. To evaluate the latter probability, we use the following result by Guralnick and Robinson (Guralnick and Robinson 2006):

Proposition 3 (Guralnick and Robinson 2006, Theorem 9) *For any non-commutative finite simple group H, we have*

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

Then we have the following result, implying that $\vec{w}_{\mathsf{AND}}$ realizes AND:

Theorem 3 *Assume that Assumption 1 holds. Then for any $\vec{g}, \vec{g}' \in X_0 \cup X_1$, we have*

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

which is negligible when both $1/|G|$ and ε are negligible.

Proof First, if $h_1 = r_1 g_1 r_1^{-1} \cdots r_L g_1 r_L^{-1}$ and $h_2 = r_{L+1} g_1' r_{L+1}^{-1} \cdots r_{2L} g_1' r_{2L}^{-1}$ were uniformly random over G, then 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 $|G|^{-1/2}$ by Proposition 3. Now note that $g_1, g_1' \neq 1_G$ as $\vec{g}, \vec{g}' \in X_0 \cup X_1$; 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 realization of operators that will yield a secure FHE scheme based on our framework in Sect. 3; concrete candidates for the secure construction are not yet obtained and are an open problem.

5.1 A Remark on the Choice of Random Variables

Here, we give a remark on random variables $\widetilde{r}_h$ involved in a lift of a realization of functions. First, for realizations of functions using a uniform random variable on a given target group G, such as those in Sects. 4.4 and 4.5, it may happen that sampling a uniformly random element of the source group $\widetilde{G}$ is not easy even if uniformly random sampling on G is easy. In such a case, owing to Proposition 2, a uniform random variable on G may be approximated as follows: random elements $g_1,\ldots,g_L$ of G are chosen at the beginning, and each random sampling on G is done by taking $g_1^{e_1}\cdots g_L^{e_L}$ with $e_1,\ldots,e_L \leftarrow_R \{0,1\}$. Provided L is sufficiently large, this approximation will work well except for a negligible probability in choosing $g_1,\ldots,g_L$. Then the corresponding random variable on $\widetilde{G}$ is easily obtained by

first taking elements $\widetilde{g}_1, \ldots, \widetilde{g}_L$ of $\widetilde{G}$ with $\pi(\widetilde{g}_i) = g_i$ for each i and then, for each sampling, generating $\widetilde{g}_1{}^{e_1} \cdots \widetilde{g}_L{}^{e_L}$ with $e_1, \ldots, e_L \leftarrow_R \{0, 1\}$.

On the other hand, for the random variable $r_{\ker}$ used by the algorithm Gen, it may also happen that uniformly random sampling over the subgroup $\ker \pi \subseteq \widetilde{G}$ seems not easy. In this case, we may choose a large number of elements $g'_1, \ldots, g'_{L'}$ of $\ker \pi$ first and then sample an element of $\ker \pi$ by randomly multiplying elements from $g'_1, \ldots, g'_{L'}$. 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 AND and NOT in $G = \mathrm{SL}_2(\mathbb{F}_q)$ proposed in Sect. 4.4. 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 $\pi : \widetilde{G} \to G$ 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 $T^{-1}gT$ (i.e. A in the description of $\widetilde{G}$ above). The conjugation by the random T in the definition of $\widetilde{G}$ intends to hide the internal block upper triangular structure 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 $(2, 1)$-component is zero", which is a *linear* constraint in terms of matrix components. By taking conjugation by T, this constraint is changed to another one, which is unknown but still a *linear* constraint in terms of matrix components. We denote the resulting constraint by "$F(g) = 0$", namely, any element g of $\ker \pi$ 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 the space $V = \{g \in M_{k+2,k+2}(\mathbb{F}_q) \mid F(g) = 0\}$. 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 $h_1, \ldots, h_L$. In this case, for a given element $g \in \widetilde{G}$, if $g \in \ker \pi$, then adding g to the subspace $\mathsf{span}(h_1, \ldots, h_L)$ (which is now equal to $\mathsf{span}(\ker \pi)$) does not increase the dimension of the subspace. 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 when g is added to $\mathsf{span}(h_1, \ldots, h_L)$, as $\mathsf{span}(h_1, \ldots, h_L) \subseteq V$ 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 Observation for Avoiding Linear Constraints

In order to realize group homomorphisms in our framework without linear constraints for the kernel discussed in Sect. 5.2, our idea here is to utilize combinatorial group theory. Roughly speaking, we say that a group H has a *presentation* $\langle X \mid R \rangle$, if X is a generating set of H, R is a set of group words with variables in X, and H is (isomorphic to) the quotient group of the free group generated by X modulo the relations "$r(\vec{x}) = 1$" for all words $r(\vec{x}) \in R$. See, e.g. Johnson (1997) for basics in combinatorial group theory. For example, it is well known that the symmetric group S_n on n letters admits a presentation of the form $\langle s_1, \ldots, s_{n-1} \mid (s_i s_j)^{\Gamma(i,j)}\ (i, j = 1, \ldots, n-1) \rangle$ where each s_i is the adjacent transposition $(i, i+1)$ and Γ is a matrix given by $\Gamma(i, i) = 1$, $\Gamma(i, i+1) = \Gamma(i+1, i) = 3$, and $\Gamma(i, j) = 2$ when $|i - j| \geq 2$. (This is actually the Coxeter group of type A_{n-1}; see, e.g. Humphreys 1990 for basic theory of the Coxeter groups.) On the other hand, it is known that for any prime $p > 3$, the groups $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ admit "compact" presentations with four generators and eight relations of lengths $O(\log p)$; see Theorem 3.6 and Remark 3.7 of Guralnick et al. (2008).

Our idea is based on the following fact implied by the fundamental theorem on homomorphisms for groups; if two groups H_1 and H_2 have presentations $\langle X \mid R_1 \rangle$ and $\langle X \mid R_2 \rangle$ with the same generating set X, and if every $r \in R_1$ is also equal to the unit element in H_2, then the identity map $X \to X$ induces a surjective group homomorphism $H_1 \to H_2$. As this kind of group homomorphism is obtained by a mechanism completely different from linear algebra, it is (naively) expected that such an approach would yield a desired group homomorphism without linear constraints.

Based on the argument above, we propose the following approach towards constructing a secure group homomorphism for our framework for FHE:

1. Take the group G associated to a realization of operations for plaintexts.
2. Take a semidirect product $H \rtimes G$ with a certain (possibly trivial) finite group H. Here, we require that a presentation of $H \rtimes G$ is efficiently computable. For example, when it is the direct product $H \times G$ and presentations for G and H are known, a presentation of $H \times G$ is obtained by introducing additional relations "generators of G and generators of H are mutually commutative" (see, e.g. Johnson 1997).

3. Let $\langle X \mid R_2 \rangle$ be the presentation of $H \rtimes G$. Then find a finite group $\widetilde{G}_0$ with presentation of the form $\langle X \mid R_1 \rangle$ and the associated surjective group homomorphism $\widetilde{G}_0 \to H \rtimes G$ as above.
4. Finally, randomly choose a group isomorphism from another group $\widetilde{G}$ to $\widetilde{G}_0$ in a certain way, subject to the condition that the group $\widetilde{G}$ admits a "compact" expression that yields efficient group operators for $\widetilde{G}$. Then the composition $\widetilde{G} \xrightarrow{\sim} \widetilde{G}_0 \to H \rtimes G \to G$ (where the last mapping is the natural projection) gives a candidate of the surjective homomorphism $\pi : \widetilde{G} \to G$.

In Step 4 of the approach described above, an easiest candidate of the "compact" expressions for the groups $\widetilde{G}_0$ and $\widetilde{G}$ is matrix expressions, i.e. embedding these groups into some matrix group. Now a candidate of the random isomorphism between them is taking the conjugation by a random secret matrix, just as in Sect. 5.2. In this case, due to the argument in Sect. 5.2, the kernel of the homomorphism $\widetilde{G}_0 \to H \rtimes G$ must avoid a linear constraint. Here we note that, even though the homomorphism from $\widetilde{G}_0 = \langle X \mid R_1 \rangle$ to $H \rtimes G = \langle X \mid R_2 \rangle$ is based on the mechanism of combinatorial group theory, this does not always guarantee that the resulting homomorphism is free from linear constraints.

For example, let $\widetilde{G}_0$ be the Coxeter group of type B_n, with presentation

$$\langle s_1, \ldots, s_n \mid (s_i s_j)^{\Gamma'(i,j)} \ (i, j = 1, \ldots, n) \rangle,$$

where $\Gamma'(i, j) = \Gamma(i, j)$ for $i, j \in \{1, \ldots, n-1\}$, $\Gamma'(n, n) = 1$, $\Gamma'(n, n-1) = \Gamma'(n-1, n) = 4$, and $\Gamma'(n, i) = \Gamma'(i, n) = 2$ for $1 \le i \le n-2$. If the value of $\Gamma'(n, n-1) = \Gamma'(n-1, n)$ is changed from 4 to 2, then it results in the direct product $S_n \times H$ with $H = \langle s_n \rangle$ being the cyclic group of order two. This implies that there is a natural surjective homomorphism $\widetilde{G}_0 \to S_n \times H$; hence, we obtain a surjective homomorphism $\widetilde{G}_0 \to S_n \times H \to S_n = G$. Now by using the expression of $\widetilde{G}_0$ as a "signed" permutation group (see, e.g. Humphreys 1990), it can be proved that the kernel of $\widetilde{G}_0 \to G$ is an elementary abelian 2-group generated by the elements $s_j s_{j+1} \cdots s_{n-1} s_n s_{n-1} \cdots s_{j+1} s_j$ with $j = 1, \ldots, n$. Moreover, in the standard matrix representation for the Coxeter groups (see, e.g. Humphreys 1990), these elements $s_j s_{j+1} \cdots s_{n-1} s_n s_{n-1} \cdots s_{j+1} s_j$ are all expressed as lower triangular matrices. Hence, the kernel of the homomorphism above has a linear constraint "upper triangular components are 0", which is not desirable. We also note that, owing to the classification result on finite Coxeter groups (see, e.g. Humphreys 1990), the group of type B_n mentioned above is essentially (i.e. without using direct products) the unique choice for a surjective, but not bijective, homomorphism from a finite Coxeter group onto the group S_n with $n \ge 5$. Consequently, the candidates for the group $\widetilde{G}_0$ in the case $G = S_n$ should be searched from outside the class of the Coxeter groups. Finding a concrete candidate for $\widetilde{G}_0$ in this case is left as an open problem.

5.4 Another Trial Using Tietze Transformations

Another trial for realizing the approach in Sect. 5.3 is as follows. Recall that, we are supposing that the group $H \rtimes G$ has a presentation of the form $\langle X \mid R_2 \rangle$. When the presentation is constructed naively, it might happen that the natural projection $H \rtimes G \to G$ is easy to compute by using the presentation of the group. Now the idea is choosing $\widetilde{G}_0 = H \rtimes G$ and constructing the isomorphic group $\widetilde{G}$ by randomly rewriting the original presentation $\langle X \mid R_2 \rangle$ while keeping the isomorphic class of groups. By letting the rewriting process be a part of the secret key, it is expected to be difficult to compute the map $\widetilde{G} \xrightarrow{\sim} H \rtimes G \to G$ without the secret key, while the secret key enables to compute the map by reversing the rewriting process above.

Such a rewriting of presentations that keeps the group isomorphic can be performed by using *Tietze transformation*. Namely, the following fact is known:

Lemma 5 (see, e.g. Johnson 1997) *Given a presentation $\langle X \mid R \rangle$ of a group, let w be a group word with variables in 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 $\langle X \cup \{y\} \mid R \cup \{wy^{-1}\} \rangle$.*

We also have the following result, which utilizes presentations of the trivial group:

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 with a single element), and for each $y \in Y$, 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 with variables in 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 the free group $\mathsf{Free}(X)$ generated by 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' is a subset of the normal closure $\langle R \rangle_{\mathrm{normal}}$ of R. To prove the opposite relation $R \subseteq \langle R' \rangle_{\mathrm{normal}}$, it suffices to show that $r_y \in \langle R' \rangle_{\mathrm{normal}}$ for each $y \in Y$. Now as $\langle Y \mid T \rangle$ 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 note that the current idea of randomly rewriting the presentation of the group $H \rtimes G$ has (at least) one unsolved problem from the viewpoint of efficiency and two from the viewpoint of security. For the efficiency, we recall that the expression of the resulting group $\widetilde{G}$ should enable efficient computation for group operators. However, with a randomly chosen presentation $\langle X \mid R \rangle$ of $\widetilde{G}$, in general, it seems not easy to compute the product of two elements. More precisely, each element

of $\widetilde{G}$ is now expressed as a group word on X, and the product corresponds to the concatenation of the two words. This concatenation of words increases the length of the word; therefore, the word has to be replaced with a shorter equivalent word by using relations in R before the word length becomes too long. However, this process of reducing the word length by using the relations in R is not efficient in general. It is an open problem to develop rewriting methods for group presentations while keeping efficiency of group operations.

From the viewpoint of security, first, it has not been evaluated how many random rewriting steps for the presentation of the group are sufficient to securely conceal the structure of the group. On the other hand, even if the sufficient number of the rewriting steps has been estimated, it may still happen that the resulting FHE scheme is not secure when the component H in $H \rtimes G$ is not appropriately chosen.

Namely, let $E = E(g)$ be a (deterministic) group word, which we call an "equation" over groups. We suppose that both of the probabilities $\Pr_{u \leftarrow_R H}[E(u) = 1]$ and $\Pr_{u \leftarrow_R H \rtimes G}[E(u) \neq 1]$ are non-negligible and at least one of them is noticeable. Then an adversary can distinguish a random element of $\ker \pi \simeq H$ (where $\pi : \widetilde{G} \to G$) from a random element of $\widetilde{G} \simeq H \rtimes G$ by checking whether a given random element u satisfies $E(u) = 1$ or not. Hence, it should be difficult to find a non-trivial equation E for which $\Pr_{u \leftarrow_R H}[E(u) = 1]$ is non-negligible.

For example, when the underlying group is the direct product $H \times G$, it should not be feasible to find a non-identity element w of the group for which its H-component is an identity element. Indeed, for any such "target" element w, it commutes with every element of $H \subseteq H \times G$, while it is likely not commutative with a random element of $H \times G$. Hence, the equation $E(g) = [w, g]$ will satisfy the attacking condition above. In particular, H should satisfy $|H| \geq 2^{2\lambda}$ for security parameter λ due to Birthday Paradox, as a collision in the H-components of two elements yields a target element. Moreover, the center of H should not be large, as otherwise the commutator $[w_1, w_2]$ for random elements w_1, w_2 will yield a target element with high probability.

For a general case of the semidirect product $H \rtimes G$, a candidate of such an equation E is $E(g) = g^k$ for some fixed value k; therefore, it is important to study the distribution of the orders of elements in H. For example, suppose that $H = A_\ell$ with $\ell \geq 4$. Let p be the largest odd prime with $p \leq \ell$. Then the number of elements of A_ℓ that are cyclic permutations on p letters is $\binom{\ell}{p}(p-1)! = \dfrac{2}{p \cdot (\ell - p)!} \cdot |A_\ell|$. This implies that $\Pr_{u \leftarrow_R H}[u^p = 1] = \dfrac{2}{p \cdot (\ell - p)!} + \dfrac{1}{|H|!}$. As $\ell - p$ is small for reasonable choices of ℓ (e.g. $\ell - p \leq 6$ for $\ell \leq 80$), the probability above is significantly high, which is not desirable to avoid the attack above.

On the other hand, we consider the choice $H = \mathrm{SL}_2(\mathbb{F}_q)$ for an odd prime q for which $1/q$ is negligible, and study the element orders in the group. Following the argument in Sect. 5.2 of Fulton and Harris (1991), 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 $\sqrt{\zeta}$

Table 1 The conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ for odd prime $q > 3$ (see the text for notations)

Type	Representative x in the class	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	$\frac{q+1}{\gcd(q+1,i)}$

in $(\mathbb{F}_{q^2})^\times \setminus (\mathbb{F}_q)^\times$ (as q is odd). This yields 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 a, b satisfy $\upsilon^i = a + b\sqrt{\zeta}$. 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 and the third columns are quoted (with slightly different notations) from Sect. 5.2 of Fulton and Harris (1991).

In Table 1, the ratio to $|H|$ of the cardinality of each conjugacy class of type 1 to 6 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. 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 $|H| = q(q^2 - 1)$ 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 *provided 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 using the equations of the form $E(g) = g^k$ 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 concealed by the random rewriting of the presentation of the group. A further analysis of attacks using other kind of equations will be a future research topic.

Acknowledgements 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 this 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, JST CREST Grant Number JPMJCR14D6, and JSPS KAKENHI Grant Number JP19H01804.

References

D.A. Barrington, Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1, in *Proceedings of STOC 1986*, pp. 1–5 (1986)

Z. Brakerski, V. Vaikuntanathan, Efficient fully homomorphic encryption from (Standard) LWE, in *Proceedings of FOCS 2011*, pp. 97–106 (2011)

J.H. Cheon, D. Stehlé, Fully homomophic encryption over the integers revisited, in *Proceedings of EUROCRYPT 2015* (1), LNCS 9056, pp. 513–536 (2015)

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, pp. 3–33 (2016)

M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, Fully homomorphic encryption over the integers, in *Proceedings of EUROCRYPT 2010*, LNCS 6110, pp. 24–43 (2010)

J.D. Dixon, Generating random elements in finite groups. Electron. J. Comb. **15** (2008), no. R94

L. Ducas, D. Micciancio, FHEW: bootstrapping homomorphic encryption in less than a second, in *Proceedings of EUROCRYPT 2015* (1), LNCS 9056, pp. 617–640 (2015)

W. Fulton, J. Harris, *Representation Theory*, vol. 129 (Springer, Berlin, 1991)

C. Gentry, Fully homomorphic encryption using ideal lattices, in *Proceedings of STOC 2009*, pp. 169–178 (2009)

C. Gentry, S. Halevi, Fully homomorphic encryption without squashing using depth-3 arithmetic circuits, in *Proceedings of FOCS 2011*, pp. 107–109 (2011)

C. Gentry, S. Halevi, N.P. Smart, Better bootstrapping in fully homomorphic encryption, in *Proceedings of PKC 2012*, LNCS 7293, pp. 1–16 (2012)

R.M. Guralnick, W.M. Kantor, M. Kassabov, A. Lubotzky, Presentations of finite simple groups: a quantitative approach. J. Am. Math. Soc. **21**, 711–774 (2008)

R.M. Guralnick, G.R. Robinson, On the commuting probability in finite groups. J. Algebr. **300**, 509–528 (2006)

J.E. Humphreys, *Reflection Groups and Coxeter Groups* (Cambridge University Press, Cambridge, 1990)

D.L. Johnson, *Presentations of Groups*, vol. 15, 2nd edn., London Mathematical Society Student Texts (Cambridge University Press, Cambridge, 1997)

N. Khamsemanan, R. Ostrovsky, W.E. Skeith III, On the black-box use of somewhat homomorphic encryption in noninteractive two-party protocols. SIAM J. Discret. Math. **30**(1), 266–295 (2016)

K. Nuida, K. Kurosawa, (Batch) Fully homomorphic encryption over integers for non-binary message spaces, in *Proceedings of EUROCRYPT 2015* (1), LNCS 9056, pp. 537–555 (2015)

R. Ostrovsky, W.E. Skeith III, Communication complexity in algebraic two-party protocols, in *Proceedings of CRYPTO 2008*, LNCS 5157, pp. 379–396 (2008)

D.J.S. Robinson, *A Course in the Theory of Groups*, vol. 80, 2nd edn. (Springer, Berlin, 1996)
A. Silverberg, Fully homomorphic encryption for mathematicians. IACR Cryptology ePrint Archive 2013/250 (2013). http://eprint.iacr.org/2013/250
D. Stehlé, R. Steinfeld, Faster fully homomorphic encryption, in *Proceedings of ASIACRYPT 2010*, LNCS 6477, pp. 377–394 (2010)