Homomorphic public-key cryptosystems and encrypting boolean circuits

Dima Grigoriev
IRMAR, Université de Rennes
Beaulieu, 35042, Rennes, France
dima@maths.univ-rennes1.fr
http://www.maths.univ-rennes1.fr/~dima

Ilia Ponomarenko
Steklov Institute of Mathematics,
Fontanka 27, St. Petersburg 191011, Russia
inp@pdmi.ras.ru

Abstract

In this paper homomorphic cryptosystems are designed for the first time over any finite group. Applying Barrington's construction we produce for any boolean circuit of the logarithmic depth its encrypted simulation of a polynomial size over an appropriate finitely generated group.

1 Homomorphic cryptography over groups

1.1. Definitions and results. An important problem of modern cryptography concerns secret public-key computations in algebraic structures. There is a lot of public-key cryptosystems using groups (see e.g. [7, 8, 9] and also Subsection 1.3) but only a few of them have a homomorphic property in the sense of the following definition.

Definition 1.1 *Let H be a finite nonidentity group, G a finitely generated group and $f: G \to H$ an epimorphism. Suppose that R is a right transversal of* $\ker(f)$ *in G, A is a set and $P: A \to G$ is a mapping such that* $\mathrm{im}(P) = \ker(f)$. *A triple $\mathcal{S} = (A, P, R)$ is called a homomorphic cryptosystem over H with respect to f, if the following conditions are satisfied for a certain integer $N \geq 1$ (called the size of $\mathcal{S}$):*

(H1) *the elements of the set A are represented by words in a certain alphabet; one can get randomly an element of A of size N within probabilistic time $N^{O(1)}$,*

(H2) *the elements of the group G are represented by words in a certain alphabet; one can test the equality of elements in G and perform group operations in G (taking the inverse and computing the product) in time $N^{O(1)}$, provided that the sizes of corresponding words are at most N,*

(H3) *the set R, the group H and the bijection $R \to H$ induced by f, are given by the list of elements, the multiplication table and the list of pairs $(r, f(r))$, respectively; $|R| = |H| = O(1)$,*

(H4) *the mapping P is a trapdoor function, i.e. given a word $a \in A$ of the length $|a|$ an element $P(a)$ can be computed within probabilistic time $|a|^{O(1)}$, whereas the problem* INVERSE(P) *is computationaly hard, while it can be solved by means of some additional secret information,* where for any mapping $P : A \to G$ we define INVERSE(P) to be the problem of testing whether given $g \in G$ belongs to $\mathrm{im}(P)$ and yielding a random element $a \in A$ such that $P(a) = g$ whenever $g \in \mathrm{im}(P)$.

Remark 1.2 *Having random generating in the set A one can easily generate elements of the group G in a form $P(a)r$, $a \in A$, $r \in R$.*

In a homomorphic cryptosystem $\mathcal{S}$ the elements of H playing the role of the alphabet of plaintext messages are publically encrypted in a probabilistic manner by the elements of G playing the role of the alphabet of ciphertext messages, all the computations are performed in G and the result is decrypted to H. More precisely:

Public Key: homomorphic cryptosystem $\mathcal{S}$.

Secret Key: INVERSE(P).

Encryption: given a plaintext $h \in H$ encrypt as follows: take $r \in R$ such that $f(r) = h$ (invoking (H3)) and a random element $a \in A$ (using (H1); the ciphertext of h is the element $P(a)r$ of G (computed by means of (H2) and (H4)).

Decryption: given a cyphertext $g \in G$ decrypt as follows: find the elements $r \in R$ and $a \in A$ such that $rg^{-1} = P(a)$ (using (H4)); the plaintext of g is the element $f(r)$ of H (computed by means of (H3)).

The main result of the present paper consists in the construction of a homomorphic cryptosystem over arbitrary finite nonidentity group; the security of it is based on the difficulty of the following slight generalization of the factoring problem FACTOR(n, m): given a positive integer $n = pq$ with p and q being primes (of the same size), a number $m \geq 2$ of a constant size such that $G/(\mathbb{Z}_n^*)^m \cong \mathbb{Z}_m^+$ where $G = \{g \in \mathbb{Z}_n^* : \ \mathbf{J}_n(g) \in \{1, (\Leftrightarrow 1)^{m \pmod 2}\}\}$ with $\mathbf{J}_n$ being the Jacobi symbol, and a transversal of $(\mathbb{Z}_n^*)^m$ in G, find the numbers p, q. In addition, we assume that $m | p \Leftrightarrow 1$ and $\mathrm{GCD}(m, q \Leftrightarrow 1) = \mathrm{GCD}(m, 2)$, although one could get rid of this extra assumption.

Theorem 1.3 *Let H be a finite nonidentity group and $N \in \mathbb{N}$. Then one can design a homomorphic cryptosystem $\mathcal{S}(H, N)$ of the size $O(N)$ over the group H; the problem* INVERSE(P) *where P is the trapdoor function, is probabilistic polynomial time equivalent to the problems* FACTOR(n, m) *for appropriate $n = \exp(O(N))$ and m running over the divisors of $|H|$.*

First a homomorphic cryptosystem for a cyclic group H is designed in Section 2, in this case the group G is a finite Abelian group. Then in Section 3 a homomorphic cryptosystem is yielded for an arbitrary H, in this case the group G being a free product of certain Abelian groups produced in Section 2. In Section 4 we recall the result from [1] designing a polynomial size simulation of any boolean circuit B of the logarithmic depth over an arbitrary unsolvable group H (in particular, one can take H to be the symmetric group Sym(5)). Combining this result with Theorem 1.3 provides an *encrypted simulation* of B over the group G: the output of this simulation at a particular input is a certain element $g \in G$, and thereby to know the output of B one has to be able to calculate $f(g) \in H$, which is supposedly to be difficult due to Theorem 1.3. We mention that a different approach to encrypt boolean circuits was undertaken in [13].

1.2. Discussion on complexity and security. One can see that the encryption procedure can be performed by means of public keys efficiently. However, the decryption procedure is a secret one in the following sense. To find the element r one has to solve in fact, the membership problem for the subgroup $\ker(f)$ of the group G. We assume that a solution for each instance $g' \in \ker(f)$ of this problem must have a "proof", which is actually an element $a \in P^{-1}(g')$. Thus, the secrecy of the system is based on the assumption that finding an element in the set $P^{-1}(g')$ i.e. solving INVERSE(P) is an intractable computation problem. On the other hand, our ability to compute P^{-1} enables us to efficiently implement the decryption algorithm. One can treat P as a proof system for membership to $\ker(f)$. Moreover, in case when A is a certain group and P is a homomorphism we have the following *exact* sequence of group homomorphisms

$$A \xrightarrow{P} G \xrightarrow{f} H \to \{1\} \tag{1}$$

(recall that the exact sequence means that the image of each homomorphism in it coincides with the kernel of the next one).

The usual way in the public-key cryptography of providing an evidence of the security of a cryptosystem is to fix a certain type of an attack (being an algorithm) of cryptosystems and to prove that a cryptosystem is resistant with respect to this type of an attack. The resistancy means usually that breaking a cryptosystem with the help of the fixed type of an attack implies a certain statement commonly believed to be unplausible. The most frequently used in the cryptography such statement (which we involve as well) is the possibility to factorize an integer being a product of a pair of primes. Thus a type of an attack we fix is that to break a homomorphic cryptosystem means to be able to solve INVERSE(P) (in other words, reveal the trapdoor).

Notice that in the present paper the group H is always rather small, while the group G could be infinite but being always finitely generated. However, the infinitness of G is not an obstacle for performing algorithms of encrypting and decrypting (using the trapdoor information) since G is a free product of groups of a number-theoretic nature like Z_n^*; therefore one can easily verify the condition (H2) and on the other hand this allows one to provide evidence for the difficulty of a decryption. In this connection we mention a public-key cryptosystem from [3] in which f was the natural epimorphism from a free group G onto the group H (infinite, non-abelian in general) given by generators and relations. In this case for any element of H one can produce its preimages (encryptions) by inserting in a word (being already a produced preimage of f) from G any relation defining H. In other terms, decrypting of f reduces to the word problem in H. In our approach the word problem is solvable easily due to a special presentation of the group G (rather than given by generators and relations).

1.3. Cryptosystems based on groups. To our best knowledge all known at present homomorphic cryptosystems are more or less modifications of the following one. Let n be the product of two distinct large primes of size of the order $\log n$. Set $G = \{g \in \mathbb{Z}_n^* : \mathbf{J}_n(g) = 1\}$ and $H = \mathbb{Z}_2^+$. Then given a non-square $r \in G$ the triple (A, P, R) where

$$R = \{1, r\}, \quad A = \mathbb{Z}_n^*, \quad P(g) : g \mapsto g^2,$$

is a homomorphic cryptosystem over H with respect to the natural epimorphism $f : G \to H$ with $\ker(f) = \{g^2 : g \in \mathbb{Z}_n^*\}$ (see [4]). We call it the *quadratic residue cryptosystem*. It can be proved (see [4]) that in this case solving the problem INVERSE(P) is not easier than factoring n, whereas given a prime divisor of n this problem can be solved in probabilistic polynomial time in $\log n$.

It is an essential assumption (being a shortcoming) in the quadratic residue cryptosystem as well as other cryptosystems cited below that its security relies on a fixed a priori (proof system) P. Indeed, it is not excluded that an adversary could verify whether an element of G belongs to $\ker(f)$ avoiding making use of P, for example, in case of the quadratic residue cryptosystem that would mean verifying that $g \in G$ is a square without providing a square root of g. Although, there is a common conjecture that verifying for an element to be a square (as well as some power) is also difficult.

Let us mention that a cryptosystem from [12] over $H = \mathbb{Z}_n^+$ (for the same assumptions on n as in the quadratic residue cryptosystem) with respect to the homomorphism $f : G \to H$ where $G = \mathbb{Z}_{n^2}^*$ and $\ker(f) = \{g^n : \ g \in G\}$, in which $A = G$ and $P : g \mapsto g^n$, is not homomorphic in the sense of Definition 1.1 because condition (H3) of it does not hold. (In particular, since $|G| \le |H|^2$, one can inverse P in a polynomial time in $|H|$.) By the same reason the cryptosystem from [10] over $H = \mathbb{Z}_p^+$ with respect to the homomorphism $f : G \to H$ where $G = \mathbb{Z}_{p^2q}^*$ and $\ker(f) = \{g^{pq} : \ g \in G\}$ (here the integers p, q are distinct large primes of the same size) is also not homomorphic (besides, in this system only a part of the group H is encrypted).

We note in addition that an alternative setting of a homomorphic (in fact, isomorphic) encryption E (and a decryption $D = E^{-1}$) was proposed in [7]. Unlike Definition 1.1 the encryption $E : G \to G$ is executed in the same set G (being an elliptic curve over the ring $\mathbb{Z}_n$) treated as the set of plaintext messages. If n is composite, then G is not a group while being endowed with a partially defined binary operation which converts G in a group when n is prime. The problem of decrypting this cryptosystem is close to the factoring of n. In this aspect [7] is similar to the well-known RSA scheme if to interprete RSA as a homomorphism (in fact, isomorphism) $E : Z_n^* \to Z_n^*$, for which the security relies on the difficulty of finding the order of the group Z_n^*.

We complete the section by mentioning some cryptosystems using groups but not being homomorphic in the sense of Definition 1.1. The well-known example is a cryptosystem which relies on the Diffie-Hellman key agreement protocol. It involves cyclic groups and relates to the discrete logarithm problem [8]; the complexity of this system was studied in [2]. Some generalizations of this system to non-abelian groups (in particular, the matrix groups over some rings) were suggested in [11] where secrecy was based on an analog of the discrete logarithm problems in groups of inner automorphisms. Certain variations of the Diffie-Hellman systems over the braid groups were described in [5]; here several trapdoor one-way functions connected with the conjugacy and the taking root problems in the braid groups were proposed. Finally it should be noted that a cryptosystem from [9] is based on the monomorphism $\mathbb{Z}_m^+ \to \mathbb{Z}_n^*$ by means of which x is encrypted by $g^x \pmod n$ where n, g constitute a public key; its decrypting relates to the discrete logarithm problem and is feasible in this situation due to special choice of n and m.

2 Homomorphic cryptosystems over cyclic groups

In this section we present an explicit homomorphic cryptosystem over a cyclic group of an order $m > 1$ whose decription is based on taking m-roots in the group $\mathbb{Z}_n^*$ for a suitable $n \in \mathbb{N}$. It can be considered in a sense as a generalization of the quadratic residue cryptosystem over $\mathbb{Z}_2^+$. Throughout this section given $n \in \mathbb{N}$ we denote by $|n|$ the size of the number n.

Given a positive integer $m > 1$ denote by D_m the set of all pairs (p, q) where p and q are distinct odd primes such that

$$p \Leftrightarrow 1 = 0\,(\mathrm{mod}\,m) \quad \text{and} \quad \mathrm{GCD}(m, q \Leftrightarrow 1) = \mathrm{GCD}(m, 2). \tag{2}$$

Let $(p, q) \in D_m$, $n = pq$ and $G_{n,m}$ be a group defined by

$$G_{n,m} = \{g \in \mathbb{Z}_n^* : \ \mathbf{J}_n(g) \in \{1, (\Leftrightarrow 1)^{m\,(\mathrm{mod}\,2)}\}\}. \tag{3}$$

Thus $G_{n,m} = \mathbb{Z}_n^*$ for an odd m and $[\mathbb{Z}_n^* : G_{n,m}] = 2$ for an even m. In any case this group contains each element $h = h_p \times h_q$ such that $\langle h_p \rangle = \mathbb{Z}_p^*$ and $\langle h_q \rangle = \mathbb{Z}_q^*$ where h_p and h_q are the p-component and the q-component of h with respect to the canonical decomposition $\mathbb{Z}_n^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. From (2) it follows that m divides the order of any such element h and $\{1, h, \cdots, h^{m-1}\}$ is a transversal of the group $G_{n,m}^m = \{g^m : \ g \in G_{n,m}\}$ in $G_{n,m}$. This implies that $G_{n,m}/G_{n,m}^m \cong \mathbb{Z}_m^+$ where the corresponding epimorphism is given by the mapping

$$f_{n,m} : G_{n,m} \to \mathbb{Z}_m^+, \quad g \mapsto i_g$$

with i_g being the element of $\mathbb{Z}_m^+$ such that $g \in G_{n,m}^m h^{i_g}$. From (2) it follows that $\ker(f_{n,m}) = G_{n,m}^m = \mathrm{im}(P_{n,m})$ where

$$P_{n,m} : A_{n,m} \to G_{n,m}, \quad g \mapsto g^m$$

is a homomorphism from the group $A_{n,m} = \mathbb{Z}_n^*$ to the group $G_{n,m}$. In particular, we have the exact sequence (1) with $A = A_{n,m}$, $P = P_{n,m}$, $f = f_{n,m}$, $G = G_{n,m}$ and $H = \mathbb{Z}_m^+$. Next, it is easily seen that any element of the set

$$\mathcal{R}_{n,m} = \{R \subset G_{n,m} : \ |f_{n,m}(R)| = |R| = m\}$$

is a right transversal of $G_{n,m}^m$ in $G_{n,m}$. Set

$$D_{N,m} = \{n \in \mathbb{N} : \ n = pq, \ (p, q) \in D_m, \ |p| = |q| = N\}.$$

Theorem 2.1 *Let H be a cyclic group of order $m > 1$. Then given $N \in \mathbb{N}$ and $n \in D_{N,m}$ one can design a homomorphic cryptosystem $\mathcal{S}_n(H, N)$ of the size $O(N)$ over the group H; the problem* INVERSE(P) *where P is the trapdoor function, is probabilistic polynomial time equivalent to the problem* FACTOR(n, m).■

3 Homomorphic cryptosystems using free products

Throughout the section we denote by W_X the set of all the words w in the alphabet X; the length of w is denoted by $|w|$. We use the notation $G = \langle X; \mathcal{R} \rangle$ for a presentation of a group G by the set X of generators and the set $\mathcal{R}$ of relations. Sometimes we omit $\mathcal{R}$ to stress that the group G is generated by the set X. The unity of G is denoted by 1_G and we set $G^{\#} = G \setminus \{1_G\}$. Finally, given a positive integer n we set $\overline{n} = \{1, \ldots, n\}$.

3.1. Calculations in free products of groups. Let us remind the basic facts on free products of groups (see e.g. [6, Ch. 4]). Let $G_1, \ldots, G_n$ be finite groups, $n \geq 1$. Given a presentation $G_i = \langle X_i; \mathcal{R}_i \rangle$, $i \in \overline{n}$, one can form a group $G = \langle X; \ \mathcal{R} \rangle$ where $X = \cup_{i \in \overline{n}} X_i$ (the disjoint union) and $\mathcal{R} = \cup_{i \in \overline{n}} \mathcal{R}_i$. It can be proved that this group does not depend on the choice of presentations of $\langle X_i; \mathcal{R}_i \rangle$, $i \in \overline{n}$. It is called the *free product* of the groups G_i and is denoted by $G = G_1 * \cdots * G_n$; one can see that it does not depend on the order of factors.

Without loss of generality we assume below that G_i is a subgroup of G and $X_i = G_i^{\#}$ for all i. In this case $G \subset W_X$ and 1_G equals the empty word of W_X. Moreover, it can be proved that

$$G = \{x_1 \cdots x_k \in W_X : \ x_j \in G_{i_j} \text{ for } j \in \overline{k}, \text{ and } i_j \neq i_{j+1} \text{ for } j \in \overline{k \Leftrightarrow 1}\}. \tag{4}$$

Thus each element of G is a word of W_X in which no two adjacent letters belong to the same set among the sets X_i, and any two such different words are different elements of G. To describe the multiplication in G let us first define recursively the mapping $W_X \to G$, $w \mapsto \overline{w}$ as follows

$$\overline{w} = \begin{cases} w, & \text{if } w \in G, \\ \overline{\ldots (x \cdot y) \ldots}, & \text{if } w = \ldots xy \ldots \text{ with } x, y \in X_i \text{ for some } i \in \overline{n}, \end{cases} \tag{5}$$

where $x \cdot y$ is the product of x by y in the group G_i. One can prove that the word $\overline{w}$ is uniquely determined by w and so the mapping is correctly defined. In particular, this implies that given $i \in \overline{n}$ we have

$$\overline{x_1 \cdots x_k} \in G_i \ \Leftrightarrow \ \overline{x_1 \cdots x_k} = \overline{x_{j_1} \cdots x_{j_{k'}}} \tag{6}$$

where $\{j_1, \ldots, j_{k'}\} = \{j \in \overline{k} : \ x_j \in G_i\}$. Now given $g, h \in G$ the product of g by h in G equals $\overline{gh}$.

Lemma 3.1 *Let $G = G_1 * \cdots * G_n$, $K = K_1 * \cdots * K_n$ be groups and f_i be an epimorphism from G_i onto K_i, $i \in \overline{n}$. Then the mapping*

$$\varphi : G \to K, \quad x_1 \cdots x_k \mapsto \overline{f_{i_1}(x_1) \cdots f_{i_k}(x_k)} \tag{7}$$

where $x_j \in G_{i_j}$, $j \in \overline{k}$, is an epimorphism. Moreover, $\varphi|_{G_i} = f_i$ for all $i \in \overline{n}$.∎

Let H be a finite nonidentity group and K be the free product of cyclic groups generated by all the nonidentity elements of H. Set

$$\mathcal{R}^{(0)} = \{h^{(m_h)} \in W_{H^{\#}} : h \in H^{\#}\},$$

$$\mathcal{R}^{(1)} = \{h^{(i)}h' \in W_{H^{\#}} : \ h, h' \in H^{\#}, \ 0 < i < m_h, \ h^i \cdot h' = 1_H\},$$

$$\mathcal{R}^{(2)} = \{hh'h'' \in W_{H^{\#}} : \ h, h', h'' \in H^{\#}, \ h' \notin \langle h \rangle, \ h \cdot h' \cdot h'' = 1_H\}$$

where $h^{(i)}$ is the word of length $i \geq 1$ with all letters being equal h, m_h is the order of $h \in H$ and $\cdot$ denotes the multiplication in H. Then one can see that

$$K = \langle H^{\#}; \mathcal{R}^{(0)} \rangle \tag{8}$$

and there is the natural epimorphism $\psi' : K \to H'$ where $H' = \langle H^{\#}; \mathcal{R}^{(0)} \cup \mathcal{R}^{(1)} \cup \mathcal{R}^{(2)} \rangle$. Since relations belonging to $\mathcal{R}^{(i)}$, $i = 0, 1, 2$, are satisfied in H, we conclude that $\ker(\psi')h_1 \neq \ker(\psi')h_2$ whenever h_1 and h_2 are different elements of H (we identify 1_K and 1_H). On the other hand, it is easy to see that any right coset of K by $\ker(\psi')$ contains a word of length at most 1, i.e. an element of H. Thus $K = \cup_{h \in H} \ker(\psi')h$, the mapping

$$\psi : K \to H, \quad k \mapsto h_k \tag{9}$$

where h_k is the uniquely detemined element of H for which $k \in \ker(\psi')h_k$, is an epimorphism and $\ker(\psi) = \ker(\psi')$.

3.2. Main construction of a homomorphic cryptosystem. Let H be a finite nonidentity group and N be a positive integer. We are going to describe a homomorphic cryptosystem $\mathcal{S}(H,N)$ of size $O(N)$ over the group H. Suppose first that H is a cyclic group of an order $m > 1$. Then we set $\mathcal{S}(H,N) = \mathcal{S}_n(H,N)$ where $n \in D_{N,m}$. If H is not a cyclic group, then $\mathcal{S}(H,N)$ is defined as follows.

Let $H^{\#} = \{h_1,\ldots,h_n\}$ where n is a positive integer (clearly, $n \geq 3$). Set $D_{N,H} = \cup_{i\in\overline{n}} D_{N,m_i}$ where m_i is the order of the group $K_i = \langle h_i\rangle$. Given $i \in \overline{n}$ choose $n_i \in D_{N,m_i}$ and set $\mathcal{S}_i = (A_i, P_i, R_i)$ to be the homomorphic cryptosystem $\mathcal{S}_{n_i}(K_i, N)$ with respect to the epimorphism $f_i : G_i \to K_i$. Without loss of generality we assume that G_i is a subgroup of the group $\mathbb{Z}^*_{n_i}$. Set

$$G = G_1 * \cdots * G_n, \quad f = \psi \circ \varphi, \tag{10}$$

where the mappings φ and ψ are defined by (7) and (9) respectively, with $K = K_1 * \cdots * K_n$. From Lemma 3.1 and the definition of ψ it follows that the mapping $f : G \to H$ is an epimorphism from G onto H.

To define a proof system for membership to $\ker(f)$ (see Subsection 1.2) we set

$$X_\varphi = X \cup A_0 \quad X = \cup_{i\in\overline{n}} G_i \setminus \ker(f_i), \quad A_0 = \cup_{i\in\overline{n}} A_i, \tag{11}$$

all the unions are assumed to be the disjoint ones. Denote by $\to$ the transitive closure of the binary relation $\Rightarrow$ on the set W_{X_φ} defined by

$$v \Rightarrow w \quad \text{iff} \quad w = x^{-1}x_0vx, \qquad v,w \in W_{X_\varphi} \tag{12}$$

where $x \in X \cup \{1_A\}$ and $x_0 \in A_0 \cup \{1_A\}$ with 1_A being the empty word of W_{X_φ}. Thus $v \to w$ if there exist words $w_1 = v, w_2, \ldots, w_l = w$ of W_{X_φ} such that $w_i \Rightarrow w_{i+1}$ for $i \in \overline{l \Leftrightarrow 1}$. We set

$$A_\varphi = \{a \in W_{X_\varphi} :\ 1_{A_\varphi} \to a\}, \quad P_\varphi : A_\varphi \to G,\ a_1\cdots a_k \mapsto \overline{P_\varphi(a_1)\cdots P_\varphi(a_k)} \tag{13}$$

where $P_\varphi|_X = \mathrm{id}_X$ and $P_\varphi|_{A_i} = P_i$ for all i. We observe that if $\overline{v} \in \ker(\varphi)$ and $v \Rightarrow w$ for some $v,w \in W_{X_\varphi}$ then obviously $\overline{w} \in \ker(\varphi)$ (see (12)). By induction on the size of a word this implies that $P_\varphi(A_\varphi) \subset \ker(\varphi)$. Next, set

$$A_\psi = \{r \in W_{R_\psi} :\ f(\overline{r}) = 1_H\}, \quad P_\psi : A_\psi \to G,\ a \mapsto \overline{a} \tag{14}$$

where $R_\psi = \cup_{i\in\overline{n}} R_i$. It is easily seen that the restriction of φ to the set $R_\varphi = G \cap W_R$ induces a bijection from this set to the group K. This shows that R_φ is a right transversal of $\ker(\varphi)$ in G. Finally we define

$$A = A_\varphi \times A_\psi, \quad P : A \to G,\ (a,b) \mapsto \overline{P_\varphi(a)P_\psi(b)}. \tag{15}$$

Let R be a right transversal of $\ker(f)$ in G, for instance one can take $R = \{1_G\} \cup \{r'_i\}_{i\in\overline{n}}$ where r'_i is the element of R_i such that $\psi(r'_i) = h_i$, $i \in \overline{n}$. One can prove that $\mathcal{S}(H,N) = (A,P,R)$ is a homomorphic cryptosystem satisfying the requirements of Theorem 1.3.

4 Encrypted simulating of boolean circuits

Let $B = B(X_1,\ldots,X_n)$ be a boolean circuit and H be a group. Following [1] we say that a word

$$h_1^{X_{l_1}} \cdots h_m^{X_{l_m}}, \quad h_1,\ldots,h_m \in H, \quad l_1,\ldots,l_m \in \overline{n}, \tag{16}$$

is a *simulation* of size m of B in H if there exists a certain element $h \in H^{\#}$ such that the equality

$$h_1^{x_{l_1}} \cdots h_m^{x_{l_m}} = h^{B(x_1,\ldots,x_n)}$$

holds for any boolean vector $(x_1, \ldots, x_n) \in \{0,1\}^n$. It is proved in [1] that given an arbitrary *unsolvable* group H and a boolean circuit B there exists a simulation of B in H, the size of this simulation is exponential in the depth of B (in particular, when the depth of B is logarithmic $O(\log n)$, then the size of the simulation is $n^{O(1)}$).

We say that the circuit B is *encrypted simulated* over a homomorphic cryptosystem with respect to an epimorphism $f : G \to H$ (we use the notations from Definition 1.1) if there exist $g_1, \ldots, g_m \in G$, and a certain element $h \in H^{\#}$ such that

$$f(g_1^{x_{l_1}} \cdots g_m^{x_{l_m}}) = h^{B(x_1,\ldots,x_n)} \qquad (17)$$

for any boolean vector $(x_1, \ldots, x_n) \in \{0,1\}^n$. Thus having a simulation (16) of the circuit B in H one can produce an encrypted simulation of B by choosing randomly $g_i \in G$ such that $f(g_i) = h_i$, $i \in \overline{m}$ (in this case, equality (17) is obvious). Now combining Theorem 1.3 with the above mentioned result from [1] we get the following statement.

Corollary 4.1 *For an arbitrary finite unsolvable group H, a homomorphic cryptosystem $\mathcal{S}$ of a size N over H and any boolean circuit of the logarithmic depth $O(\log N)$ one can design in time $N^{O(1)}$ an encrypted simulation of this circuit over $\mathcal{S}$.* ■

The meaning of an encrypted simulation is that given (publically) the elements $g_1, \ldots, g_m \in G$ and $h \in H^{\#}$ from (17) it should be supposedly difficult to evaluate $B(x_1, \ldots, x_n)$ since for this purpose one has to verify whether an element $g_1^{x_{l_1}} \cdots g_m^{x_{l_m}}$ belongs to $\ker(f)$. On the other hand, the latter can be performed using the trapdoor information. In conclusion let us mention the following two known schemes of interaction (cf. e.g. [13]) based on encrypted simulations.

The first scheme is called *evaluating an encrypted circuit*. Assume that Alice knows a trapdoor in a homomorphic cryptosystem over a group H with respect to an epimorphism $f : G \to H$ and possesses a boolean circuit B which she prefers to keep secret, and Bob wants to evaluate $B(x)$ at an input $x = (x_1, \ldots, x_n)$ (without knowing B and without disclosing x). To accomplish this Alice transmits to Bob an encrypted simulation (17) of B, then Bob calculates the element $g = g_1^{x_{l_1}} \cdots g_m^{x_{l_m}}$ and sends it back to Alice, who computes and communicates the value $f(g)$ to Bob.

In a different setting one could consider in a similar way evaluating an encrypted circuit $B_H(y_1, \ldots, y_n)$ over a group H (rather than a boolean one), being a sequence of group operations in H with inputs $y_1, \ldots, y_n \in H$. The second (dual) scheme is called *evaluating at an encrypted input.* Now Alice has an input $y = (y_1, \ldots, y_n)$ (desiring to conceal it) which she encrypts randomly by the tuple $z = (z_1, \ldots, z_n)$ belonging to G^n such that $f(z_i) = y_i$, $i \in \overline{n}$, and transmits z to Bob. In his turn, Bob who knows a circuit B_H (which he wants to keep secret) yields its "lifting" $f^{-1}(B_H)$ to G by means of replacing every constant $h \in H$ occurring in B_H by any $g \in G$ such that $f(g) = h$ and replacing the group operations in H by the group operations in G, respectively. Then Bob evaluates the element $(f^{-1}(B_H))(z) \in G$ and sends it back to Alice, finally Alice applies f and obtains $f((f^{-1}(B_H))(z)) = B_H(y)$ (even without revealing it to Bob).

References

[1] D. M. Barrington, H. Straubing, D. Therien, *Non-uniform automata over groups*, Information and Computation, **132** (1990), 89–109.

[2] D. Coppersmith, I. Shparlinski, *On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping*, J. Cryptology, **13** (2000), 339–360.

[3] Do Long Van, A. Jeyanthi, R. Siromony, K. Subramanian, *Public key cryptosystems based on word problems*, in ICOMIDC Symp. Math. of Computations, Ho Chi Minh City, April, 1988.

[4] S. Goldwasser. S. Micali, *Probabilistic encryption*, J.Comput.Syst.Sci., **28** (1984), 270–299.

[5] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, Lecture Notes in Computer Science, **1880** (2000), 166–183.

[6] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Interscience Publishers, New York-London-Sydney, 1966.

[7] K. Koyama, U. Maurer, T. Okamoto, S. Vanstone, *New public-key schemes based on elliptic curves over the ring* $\mathbb{Z}_n$, Lecture Notes in Computer Science, **576** (1991), 252–266.

[8] U. Maurer, S. Wolf, *Lower bounds on generic algorithms in groups*, Lecture Notes in Computer Science, **1403** (1998), 72–84.

[9] D. Naccache, J. Stern, A new public key cryptosystem based on higher residues, Proc. 5th ACM Conference on Computer and Communication Security, 1998, 59–66.

[10] T. Okamoto, S. Uchiyama, *A New Public-Key Cryptosystem as Secure as Factoring*, Lecture Notes in Computer Science, **1403** (1998), 308–317.

[11] S.-H. Paeng, D. Kwon, K.-C. Ha, J. H. Kim, *Improved public key cryptosystem using finite non-abelian groups*, Preprint NSRI, Korea.

[12] P. Paillier, *Public-Key Cryptosystem Based on Composite Degree Residuosity Classes*, Lecture Notes in Computer Science, **1592** (1999), 223-238.

[13] T. Sander, A. Young, M. Young, *Non-interactive cryptocomputing for* NC^1, Proc. 40th IEEE Symp. Found. Comput. Sci, 1999, 554–566.