Homomorphic public-key cryptosystems over groups and rings

Dima Grigoriev
IRMAR, Université de Rennes
Beaulieu, 35042, Rennes, France
dima@math.univ-rennes1.fr
http://name.math.univ-rennes1.fr/~dimitri.grigoriev

Ilia Ponomarenko
Steklov Institute of Mathematics,
Fontanka 27, St. Petersburg 191011, Russia
inp@pdmi.ras.ru
http://www.pdmi.ras.ru/~inp *

31.08.2003

Abstract

We propose a new homomorphic public-key cryptosystem over arbitrary non-identity finite group based on the difficulty of the membership problem for groups of integer matrices. Besides, a homomorphic cryptosystem is designed for the first time over finite commutative rings.

1 Introduction

1.1. The problem of constructing reliable cryptosystems for secret computations had been extensively studied last years (see [3, 5, 10, 14, 26]). Generally, it consists in encryption of a circuit over an algebraic structure H (e.g. group, ring, etc.). One of possible approaches to it is to find a publically known algebraic structure G and a secret homomorphism

*Partially supported by RFFI, grants, 03-01-00349, NSH-2251.2003.1 and a grant of NATO. The author would like to thank the Mathematical Institute of the University of Rennes during the stay in which this paper was initiated.

$f : G \to H$. If the inversion of f is efficiently computable and computing of f is a hard computational problem (i.e. f is a trapdoor function), one can design a homomorphic public-key cryptosystem in which an element $h \in H$ is encrypted by an element of the form gg_h where g is a random element of $\ker(f)$ and $f(g_h) = h$. Using such a cryptosystem one can efficiently implement a secret computation given by any circuit over the structure H. Some other applications of homomorphic public-key cryptosystems can be found in [3, 8, 9, 27]. We mention also that the group theory is a source of constructions (apart from homomorphic cryptosystems) in the cryptography, see e.g. [13, 16, 20, 21, 23].

It is well known that any boolean circuit of logarithmic depth can be efficiently simulated by a circuit over an arbitrary finite nonsolvable group, see [2] (another approach to encrypting boolean circuits was undertaken in [28]). Thus one of the first natural problems concerning secret computations is to design a homomorphic public-key cryptosystem over a finite group. The known examples of such systems include the quadratic residue cryptosystem (see [12, 11]) over the group of order 2 and the cryptosystems (see [22, 24, 25]) over some cyclic and dihedral groups. However, in these and some other cryptosystems the involved groups are solvable and so can not be used for the above cited simulation of boolean circuits. The first homomorphic public-key cryptosystem over an arbitrary nonidentity finite group was designed in [14].

It should be mentioned that the secrecy of all these cryptosystems was based on the difficulty of some problems closely related with that of integer factoring. However, "as long as factoring remains intractable, we are in a good position, but we are overindependent on the computational complexity of one particular problem" [31]. In addition, unlike factoring it is unknown whether there is a quantum machine which can decide the membership to a non-abelian matrix group, the problem on which relies the security of the cryptosystems in the present paper. In contrast to the cryptosystems based on the factoring problem the first main result of this paper is a new homomorphic public-key cryptosystem over arbitrary nonidentity finite group based on the difficulty of the membership problem for groups of integer matrices (for details see Section 2 and Theorem 2.1).

Theorem 1.1 *For a nonidentity finite group H given by generators and relations one can choose a group $G \leq \mathrm{GL}_2(\mathbb{Z})$ and a homomorphism $f : G \to H$ to obtain a homomorphic public-key cryptosystem over H.*

We may think of H to be a finite small group. On the other hand, the infiniteness of G is not an obstacle for performing algorithms of encrypting and decrypting (for the latter using the trapdoor information) since they involve just calculations with integer 2×2 matrices. In this connection we mention a public-key cryptosystem from [6] in which f was the natural epimorphism from a free group G onto the group H 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 epimorphism f is given on specially chosen generators of an appropriate subgroup G of a free group $F \subset \mathrm{GL}_2(\mathbb{Z})$, and the trapdoor consists in a polynomial-time algorithm (see Subsection 2.4) which allows one to represent an element of G (being an integer matrix) as a product of free generators of F. Publically in the cryptosystem from Theorem 1.1 a certain set of generators of G is exhibited, and the security of the cryptosystem relies on the difficulty (without knowledge of the trapdoor) of finding a representation of an element of G as a product of these generators, while in [6] an element of the free group G is given just by means of a product of its generators. (In fact, we keep a secret "good" basis of F which enables us to compute matrices of G easily; at the same time the public key is given by a "bad" basis of G for which the representation problem is supposedly hard.)

We mention also that two public-key cryptosystems (being not homomorphic) based on the group $\mathrm{SL}_2(\mathbb{Z})$ were suggested in [33, 34] which were subsequently broken in [30, 4]. These cryptosystems were hiding the generators of a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ by means of conjugating them with a secret matrix.

In [31, 15] two constructions of cryptosystems (being not homomorphic) were proposed with the difficulty of breaking relied on the word problem (in finitely generated groups). The common feature of both papers is that a public key is given by two words m_0, m_1 and a family $\mathcal{R}$ of words. Then encrypting of a bit $i \in \{0, 1\}$ is carried out by means of starting with m_i and subsequent random inserting polynomial number of times of the words from $\mathcal{R}$. Denote by G the group given by the relations $\mathcal{R}$. Then basically the trapdoor needs a solution of the word problem in G. To this end the epimorphisms of the form $f : G \to H$, provided that $f(m_0) \neq f(m_1)$ were suggested such that the word problem in the group H is easy, thereby this epimorphism plays a role of a trapdoor. In [31] the epimorphism f consists actually in adding some relations of commutativity of the generators. In [15] as a group H is taken the Grigorchuk group with 4 generators (and being not finitely presentable) corresponding to a certain fast computable infinite word χ. It is shown in [15] that the word problem in this group is easy, thus χ plays a role of a trapdoor. So, the principal difference of the cryptosystems proposed in [6, 31, 15] from our cryptosystem is that they perform calculations with words, whereas our cryptosystem deals with integer 2×2 matrices.

It seems to be an interesting open question whether for a non-abelian group H there exists a homomorphic cryptosystem with a finite group G?

1.2. The second topic of this paper is devoted to homomorphic public-key cryptosystems over finite rings. This problem was first posed in [26] (see also [10]) and in [5] it was demonstrated that a direct approach to it fails. At present there are only a few results in this direction. In particular, we mention the cryptosystem from [7] based on a homomorphism from the direct sum of rings isomorphic $\mathbb{Z}$. A finite version of this system [8] was

recently broken in [1]. As the second main result of this paper we present a homomorphic public-key cryptosystem over a finite commutative ring (for details see Section 3). Before formulating it we recall that any finite commutative ring with identity is isomorphic to a direct sum of local rings (see [19]).

Theorem 1.2 *Let R be a finite commutative ring with identity different from a direct sum of several copies of rings isomorphic to $\mathbb{Z}_2$. Then there exists a homomorphic public-key cryptosystem over R with respect to a homomorphism $f : \mathcal{A} \to R$ for an appropriate finite commutative ring $\mathcal{A}$.*

In the cryptosystem of Theorem 1.2 the ring $\mathcal{A}$ is a group ring of a finite Abelian group G and f is the epimorphism induced by a suitable secret epimorphism from G to the multiplicative group of R. The only commutative rings for which any homomorphism of such kind is trivial, have trivial multiplicative groups, and so are the direct sums of copies of the ring $\mathbb{Z}_2$. Thus the natural open question is to find a homomorphic public-key cryptosystem over the ring $\mathbb{Z}_2$. The way we construct the ring $\mathcal{A}$ gives a bound on the cardinality of $\mathcal{A}$ being *double exponential* in the cardinality of R. This condition is essential in the following sense. As we will see in Section 3 any finite ring of exponential cardinality is a subring of the ring $\mathrm{Mat}(n, \mathbb{Z}_m)$ of $n \times n$ matrices over $\mathbb{Z}_m$ with n and $\log m$ bounded by polynomials. The latter construction of embedding a ring into a matrix ring is not efficient a priori, in fact, its efficiency depends on the way in which the ring is given. On the other hand, Theorem 3.2 states that the homomorphisms of the rings given as subrings of $\mathrm{Mat}(n, \mathbb{Z}_m)$ can not be secret.

It should be remarked that secret homomorphisms from Theorem 1.2 can not be used for encrypting circuits over rings due to its size. The problem of finding cryptosystems suitable for such encrypting as well as constructing secret homomorphisms over noncommutative finite rings are still open. Theorem 3.2 shows that if there exists a homomorphic public-key cryptosystem over a finite ring R with the cardinality of the ring $\mathcal{A}$ being exponential in the cardinality of R , it should avoid *explicit* representing of $\mathcal{A}$ as a subring of some matrix ring $\mathrm{Mat}(n, \mathbb{Z}_m)$.

2 A homomorphic cryptosystem over a finite group

Throughout the section for a finite set X we denote by W_X the set of all the words in the alphabet $X^{\pm} = X \cup X^{-1}$. A word from W_X with no subword xx^{-1}, $x \in X^{\pm}$, is called irreducible. For an integer $a \in \mathbb{Z}$ we denote by $l(a)$ the bit size of it; for $S \subset \mathbb{Z}$ we set $l(S) = \sum_{a \in S} l(a)$.

2.1. Representation problem. Let Γ be a group and X be a finite subset of Γ. We are interested in the problem of finding an *X-representation* of an element $g \in G$ where $G = \langle X \rangle$ is a subgroup of Γ generated by X. By an X-representation of g we mean an

irreducible word $w_g \in W_X$ such that $\pi(w_g) = g$ where π is the epimorphism of the free group on X onto the group G with $\pi|_X = \mathrm{id}$. Obviously, if Γ is a free group on X, then $G = \Gamma$ and each element of Γ has the unique X-representation. If $w_g = x_1^{a_1} \cdots x_m^{a_m}$ where $x_i \in X$ and $a_i \in \mathbb{Z}$ for all i, then the number $l(w_g) = \sum_i l(a_i)$ is called the *bit size* of the X-representation w_g of g. We observe that the size of g as an element of the group Γ depending essentially on the nature of Γ can substantially differ from the bit size of an X-representation of it as well as the bit sizes of two different X-representations of g. In what follows we look for the algorithms finding X-representations of g efficiently, i.e. in polynomial time in size of g in Γ and in minimal bit size of its X-representation.

Representation Problem $\mathcal{P}(\Gamma, X)$. Let Γ be a group and $X \subset \Gamma$ be a finite set. Given $g \in \langle X \rangle$ presented as an element of Γ find an X-representation of g efficiently.■

It should be mentioned that the representation problem consists in finding a certificate for the membership problem when the group in question is given by generators. If Γ is a symmetric group of degree n, then both of these problems can be solved in time $n^{O(1)}$ by the sift algorithm (see e.g. [17]). However, if $\Gamma = \mathrm{GL}_n(\mathbb{Z}_m)$ then both of these problem are closely related with the discrete logarithm problem (when $n = 1$, m is a prime and X consists of a generator of the multiplicative group of the ring $\mathbb{Z}_m$). The representation problem is NP-hard *in average* in general even if Γ is a free group of a finite rank [32].

To adapt the representation problem to constructing public-key cryptosystems we have to describe a trapdoor information providing a polynomial-time solution of this problem. A general idea can be explained as follows. Let $G < F < \Gamma$ be groups and $F = \langle X' \rangle$, $G = \langle X \rangle$ for some finite sets $X, X' \subset \Gamma$. Suppose that both of the problems $\mathcal{P}(\Gamma, X')$ and $\mathcal{P}(F, X)$ can be solved efficiently. Then the problem $\mathcal{P}(\Gamma, X)$ can also be solved within the same time whenever using the corresponding algorithms one can find an X'-representation and an X-representation of an element from $\langle X \rangle$ the bit sizes of which are approximately the same. In this case one could use the set X' as a trapdoor for the problem $\mathcal{P}(\Gamma, X)$. In the next subsection we realize this idea for $\Gamma = \mathrm{GL}_2(\mathbb{Z})$ and apply it for constructing a homomorphic public-key cryptosystem over any nonidentity group given by generators and relations.

2.2. The main construction. Let us define a family of free subgroups of the group $\mathrm{GL}_2(\mathbb{Z})$. First we recall that given an integer $n \geq 2$ the matrices

$$A_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \quad B_n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \tag{1}$$

form a basis of a free subgroup of the group $\mathrm{GL}_2(\mathbb{Z})$ (see [18, p.232]). Next, from the proof of [18, Proposition 3.1] it follows that given a nonempty set $S \subset \mathbb{Z}$ the set

$$X(n, S) = \{A_n^{-s} B_n A_n^s : \ s \in S\}$$

is also a basis of a free group $G(n,S) \subset \mathrm{GL}_2(\mathbb{Z})$. The following statement proved in Subsection 2.4 enables us to define a homomorphic public-key cryptosystem with these groups.

Theorem 2.1 *Given an integer $n \geq 2$ and a finite set $S \subset \mathbb{Z}$ one can find the $X(n,s)$-representation w_g of an arbitrary matrix $g \in G(n,S)$ in polynomial time in $l(n) + l(S) + l(w_g)$.*

Let $H = \langle \mathcal{X}; \mathcal{R} \rangle$ be a nontrivial group given by the set $\mathcal{X}$ of at least two [1] generators and the set $\mathcal{R}$ of relations. Choose randomly $n \geq 2$, sets $S \subset \mathbb{Z}$, $R \subset W_{\mathcal{R}}$ such that $|S| = |R| = |\mathcal{X}|$, and bijections $h \mapsto x_h$, $h \mapsto r_h$ from $\mathcal{X}$ to $X(n,S)$ and to R respectively. Set

$$X = X(n,S,R) = \{x_h r_h : \ h \in \mathcal{X}\}, \quad G = \langle X \rangle.$$

Since $F = \langle X(n,S) \rangle$ is a free group on $X(n,S)$, there exists a uniquely determined epimomorphism $\varphi : F \to H$ coinciding with $f_{\mathcal{X}}^{-1}$ on $W_{X(n,S)}$ where $f_{\mathcal{X}} : W_{\mathcal{X}} \to W_{X(n.S)}$ is a bijection taking $h_1 \cdots h_k$ to $x_{h_1} \cdots x_{h_k}$. After identifying $W_{\mathcal{R}}$ with the subset of $W_{\mathcal{X}}$ we have $F = \varphi^{-1}(H) \supset \langle f_{\mathcal{X}}(\mathcal{X} \cup R) \rangle \supset \langle X \rangle = G$. Thus $G < F < \mathrm{GL}_2(\mathbb{Z})$ and the mapping

$$f : G \to H, \quad g \mapsto \varphi(g) \tag{2}$$

is a homomorphism such that $f(x_h r_h) = \varphi(x_h)\varphi(r_h) = h \cdot 1 = h$ for all $h \in \mathcal{X}$. Now we can define a homomorphic public-key cryptosystem $\mathcal{S}(H,n,S)$ over the group H with respect to the homomorphism (2) as follows:

Public Key: the subset $X = X(n,S,R)$ of $\mathrm{GL}_2(\mathbb{Z})$ where R is a random subset of $W_{\mathcal{R}}$, and a bijection $\mathcal{X} \to X, \ h \mapsto x_h r_h$.

Secret Key: the pair (n,S).

Encryption: given a plaintext $h \in H$ encrypt as follows:

Step 1. If $h = h_1 \cdots h_k$ with $h_i \in \mathcal{X}$ for all i, set $M_h = (x_{h_1} r_{h_1}) \cdots (x_{h_k} r_{h_k})$.

Step 2. Find an $\mathcal{X}$-representation $w_r = h'_1 \cdots h'_m$ of a random $r \in W_{\mathcal{R}}$. Set $M_r = x_{h'_1} \cdots x_{h'_m}$.

Step 3. Output the matrix $M_r M_h \in \mathrm{GL}_2(\mathbb{Z})$ as the ciphertext of h.

Decryption: given a cyphertext $g \in G$ decrypt as follows.

[1] This is rather technical restriction because even H is a cycle group one can choose as $\mathcal{X}$ nonminimal set of generators.

Step 1. Find the $X(n,S)$-representation $w_g = g_1 \cdots g_k$ of the element g (Theorem 2.1).

Step 2. Output $f_{\mathcal{X}}^{-1}(g_1) \cdots f_{\mathcal{X}}^{-1}(g_k)$ as the plaintext of g.

The correctness of the encryption and decryption algorithms immediately follows from the definitions. Moreover, by Theorem 2.1 the decryption of the cryptosystem $\mathcal{S}(H,n,S)$ can be done within time $(l(n)+l(S)+l(w_g)))^{O(1)}$.

2.3. Remarks on security of the cryptosystem $\mathcal{S}(H,n,S)$. First, we observe that the decryption problem, i.e. the problem of computing $f(g)$ for an element $g \in G$, is polynomial-time reducible to the representation problem $\mathcal{P}(\mathrm{GL}_2(\mathbb{Z}), X)$. Thus the difficulty of the direct way to break $\mathcal{S}(H,n,S)$ is based on that of the special case of this representation problem with the promise $X \subset G(n,S)$:

Problem 2.2 *Given a matrix belonging to a group $G \leq G(n,S)$ find a short X-representation of it under the assumption that such a representation does exist.*

One can make this problem even harder using for instance the Nielsen transformations [18] to replace $X(n,S)$ by other set of generators not necessarily being a basis of the group $G(n,S)$ (these transformations consist in succesive replacing elements of generating set for their inverses or products). A less direct way to break the cryptosystem $\mathcal{S}(H,n,S)$ could consist in finding the number n and the set X, in other words, the secret key. This seems to be difficult.

Finally, it should be remarked that the cryptosystem $\mathcal{S}(H,n,S)$ can be transformed to the homomorphic public-key cryptosystem in the sense of [14]. To do this it suffices to find a set A and a trapdoor function $P : A \to G$ such that $\mathrm{im}(P) = \ker(f)$, i.e. to get the exact sequence

$$A \xrightarrow{P} G \xrightarrow{f} H \longrightarrow \{1\}.$$

However, this can be done by choosing A to be the set W_K where $K = \{hh'(hh')^{-1} : h, h' \in H\}$, and $P = f_{\mathcal{X}}$ (we make use the fact that in this setting the group H has to be small). We do not dwell on details since we do not stick here with the definition of [14].

2.4. Proof of Theorem 2.1. The proof of the theorem is based on lemmas 2.3 and 2.4. In the first of them the free group $\mathcal{F}$ on $\mathcal{X}$ is considered as the subset of the set $W_{\mathcal{X}}$: any element of $\mathcal{F}$ is an irreducible word of $W_{\mathcal{X}}$ and the identity of $\mathcal{F}$ is the empty word $1_{\mathcal{X}} \in W_{\mathcal{X}}$. The length of the $\mathcal{X}$-representation of an element $g \in \mathcal{F}$ is denoted by $|g|$. For an arbitrary word $w \in W_{\mathcal{X}}$ we denote by $\overline{w}$ the element of $\mathcal{F}$ corresponding to w. Below we will use an observation from the proof of [18, Proposition 3.1] that if $\mathcal{X} = \{A, B\}$ and $S \subset \mathbb{Z}$ is a nonempty finite set, then the elements $A^{-s}BA^s$, $s \in S$, form a basis of a free subgroup of the group $\mathcal{F}$.

Lemma 2.3 *Let $\mathcal{F}$ be a free group of rank 2 on $\mathcal{X} = \{A, B\}$ and G be a subgroup of $\mathcal{F}$ generated by the set $X = \{A^{-s}BA^s : s \in S\}$ where $S \subset \mathbb{Z}$ is a nonempty finite set. Then given an element $g \in \mathcal{F}$ one can test whether $g \in G$ or not in time $(l(g) + l(S))^{O(1)}$ where $l(g)$ is the bit size of the $\mathcal{X}$-representation of g; moreover, if $g \in G$, then the X-representation w_g can be found within the same time and $l(g) \le 3l(w_g)l(S)$.*

Proof. To prove the lemma let us consider the following algorithm which for a given element $g \in \mathcal{F}$ by recursion on the length $|g|$ of its $\mathcal{X}$-representation produces a certain pair $(i_g, w_g) \in \{0, 1\} \times W_X$ such that $g \in G$ if and only if $i_g = 1$ and w_g is the X-representation of g.

Step 1. If $g = 1_{\mathcal{X}}$, then output $(1, 1_X)$. Otherwise, let $u = A^aB^bA^c\cdots$ for suitable $a, b, c, \ldots \in \mathbb{Z}$.

Step 2. If either $-a \notin S$ or $(-a, b) \in S \times \{0\}$, then output $(0, 1_X)$. Otherwise set $u = A^{a+c}\ldots$.

Step 3. Recursively find (i_h, w_h) where $h = \overline{u}$. If $i_h = 0$, then output (i_h, w_h).

Step 4. Output $(1, w_g)$ where $w_g = vw_h$ with $v = A^aB^bA^{-a}$. ∎

We observe that each recursive call at Step 3 is applied to the element $h \in \mathcal{F}$ with $|h| < |g|$, so the number of recursive calls is at most $|g|$ and each step can be implemented in time $O(l(g) + l(S))$. Thus the running time of the algorithm is $(l(g) + l(S))^{O(1)}$. Next, due to the obvious inequality $l(c) \le l(a + c) + l(a)$ we have

$$l(g) = l(A^aB^bA^c\cdots) \le 2l(a) + l(b) + l(A^{a+c}\ldots) = 2l(a) + l(b) + l(h). \tag{3}$$

Since $w_g = vw_h$ and $v = (A^aBA^{-a})^b$ we get that $l(w_g) = l(b) + l(w_h)$. On the other hand, $l(h) \le 3l(w_h)l(S)$ by the recursive hypothesis. Thus from (3) it follows that

$$l(g) \le 2l(a) + l(b) + 3l(w_h)l(S) = 2l(a) + l(b) + 3(l(w_g) - l(b))l(S) \le 3l(w_g)l(S)$$

(we use that $l(b) \ne 0$ and $\max\{l(a), l(b)\} \le l(S)$). This proves the required inequality $l(g) \le 3l(w_g)l(S)$.

To verify the correctness of the algorithm we need to show first that $g \in G$ if and only if $i_g = 1$, and second that if $i_g = 1$, then w_g is the X-representation of g. Using induction on $|g|$ suppose that $g \in G \setminus \{1_{\mathcal{X}}\}$. We observe that the first term of an arbitrary irreducible word $w \in W_{\mathcal{X}}$ such that $w = \overline{w'}$ for some $w' \in W_X$, is of the form A^a where $-a \in S$. So the output of Step 2 is correct. Moreover, from the definition of v at Step 4 it follows that $v \in X$ and so $g \in G$ iff $h \in G$. Besides, if the algorithm terminates at

Step 3 or 4, then $i_g = i_h$ and by the induction hypothesis w_h is the X-representation of h iff $i_h = 1$. Thus the output at Step 3 is correct and $w_g \in W_X$. Since obviously

$$g = \overline{vu} = \overline{v\overline{u}} = \overline{v\overline{w_h}} = \overline{vw_h} = \overline{w_g},$$

we conclude that w_g at Step 4 is the X-representation of g and the output of this step is correct.■

In the next lemma we deal with the subgroup of $\mathrm{GL}_2(\mathbb{Z})$ generated by the set $X_n = \{A_n, B_n\}$ (see (1)). Since this group is a free group on X_n, any element M of it has the uniquely determined X_n-representation coinciding with the irreducible word belonging to W_{X_n}.

Lemma 2.4 *Let $G = \langle X_n \rangle$ for some $n \geq 2$. Then given matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ belonging to G, the X_n-representation of M can be found in time $(l(n) + l)^{O(1)}$ where l is the bit size this representation.*

Proof. The algorithm below is similar to the one in [29] which yields a representation of a matrix with respect to a different (more standard in the theory of modular groups) family of generator, also in [29] one can find the basic facts on the group $\mathrm{SL}_2(\mathbb{Z})$ used in the proof below. We will employ the classical action of the group $\mathrm{GL}_2(\mathbb{Z})$ on the projective line (the Riemannian sphere) $\mathbb{C}^* = \mathbb{C} \cup \{\infty\}$ by means of linear fractional transformations

$$z \mapsto Mz = (M_{11}z + M_{12})/(M_{21}z + M_{22})$$

where $M = (M_{ij})$ is a matrix of $\mathrm{GL}_2(\mathbb{Z})$ (the kernel of this action is of order 2 and equal the subgroup of all diagonal matrices of $\mathrm{GL}_2(\mathbb{Z})$; the quotient group with respect to this subgroup is the projective group $\mathrm{PGL}_2(\mathbb{Z})$). We make use of the following key observation: if $n \geq 2$, then any power A^k of the matrix $A = A_n$ with nonzero $k \in \mathbb{Z}$ maps the unit open disk $D \subset \mathbb{C}$ centered at 0 *strictly* inside $D^c = \mathbb{C}^* - \overline{D}$, and reciprocately any power B^k of the matrix $B = B_n$ maps D^c *strictly* inside D. [2] A straightforward computation shows that given $z \in D \cup D^c$ there could exist at most one integer $k = k(z)$ such that

$$(z \in D^c \ \wedge \ A^k z \in D) \quad \vee \quad (z \in D \ \wedge \ B^k z \in D^c).$$

Below we set $C(z) = A^k$ if $z \in D^c$, and $C(z) = B^k$ if $z \in D$, provided that k does exist. In the following algorithm we suppose that I is the identity matrix, and $z \in D$ and $z' \in D^c$ are arbitrary fixed complex numbers of small sizes, say $z = 1/2$ and $z' = 2$.

Step 1. Set $(L, L') := (M, M)$ and $(u, u') := (1_{X_n}, 1_{X_n})$.

[2] This observation entails that G is the free group on $\{A, B\}$ (see [18, Proposition 12.2]).

Step 2. If $L = I$, then output u; if $L' = I$, then output u'.

Step 3. Set $(u, u') := (C^{-1}u, (C')^{-1}u')$ (in $W_{X_n} \times W_{X_n}$), and $(L, L') := (CL, C'L')$ (in $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$), where $C = C(Lz)$, $C' = C(L'z')$. Go to Step 2.■

Let us prove that the above algorithm finds the X_n-representation

$$M = A^{a_1}B^{b_1} \cdots A^{a_m}B^{b_m} \tag{4}$$

of a matrix $M \in G$ where m is a nonnegative integer and $a_i, b_i \in \mathbb{Z}$, $i \in \overline{m}$, such that $a_i \neq 0$ for $i \neq 1$, $b_i \neq 0$ for $i \neq m$. If $M = I$ ($m = 0$), then the statement is obvious (see Step 1). Let us show that if $b_m = 0$ (resp. $b_m \neq 0$), then after m iterations of the loop at Steps 2 and 3 the matrix L (resp. L') becomes the identity matrix and the word u (resp. u') is the X_n-representation of M. Indeed, let $b_m = 0$ (the case $b_m \neq 0$ is considered similarly). Then it is easy to see that $Mz \in D$ iff $a_1 = 0$. So after the first iteration according to Step 3 we have

$$k(Mz) = \begin{cases} -a_1, & \text{if } Mz \in D^c, \\ -b_1, & \text{if } Mz \in D, \end{cases}$$

whence $u = A^{a_1}$ if $Mz \in D^c$ and $u = B^{b_1}$ if $Mz \in D$. Since the number of factors in the X_n-representation of the matrix L after Step 3 equals $m - 1$, the required statement follows by induction on this number.

Let us estimate the running time of the algorithm. We observe that from the previous paragraph it follows that the algorithm terminates after m iterations. So to complete the proof it suffices to note that the sizes of all the intermediate matrices L and L' do not exceed $O(ml(n) + l)$.■

Let us complete the proof of Theorem 2.1. For an element $g \in G(n, S)$ by means of Lemma 2.4 one can find first its X_n-representation within time $(l(n)+l)^{O(1)}$ where $l = l(g)$ is the bit-size of this representation. Subsequently applying Lemma 2.3 one can find an $X(n, S)$-representation w_g of g within time $(l + l(S))^{O(1)} \leq (l(w_g) + l(S))^{O(1)}$.

3 Homomorphic cryptosystems over finite rings

Let R be a finite commutative ring with identity and G be a group. Then it is easy to see that any homomorphism $\varphi : G \to R^\times$ where $R^\times$ is the multiplicative group of R, can be extended to the homomorphism $\varphi' : R[G] \to R[R^\times]$ of the group rings taking $\sum_g r_g g$ to $\sum_g r_g \varphi(g)$. On the other hand, the natural injection $R^\times \to R$ can be extended to the ring homomorphism $\varphi'' : R[R^\times] \to R$. We will say that the homomorphism $f = \varphi' \circ \varphi''$,

$$f : R[G] \to R, \quad \sum_g r_g g \mapsto \sum_g r_g \varphi(g) \tag{5}$$

is induced by the homomorphism φ. From the computational point of view the homomorphisms φ and f are closely related; more exactly the problem of finding $\varphi(g)$ for $g \in G$ is polynomial time equivalent to the problem of finding $f(g)$ for $g \in G$ (here we suppose the elements of the group ring $R[G]$ are given by R-linear combinations of elements of G). This immediately implies the following statement.

Lemma 3.1 *Let R be a finite commutative ring with identity such that there exists a homomorphic public-key cryptosystem over the group $R^\times$ with respect to an epimorphism $\varphi : G \to R^\times$ for some group G. Then one can design a homomorphic public-key cryptosystem over the ring R. Moreover, the problems of breaking these two systems are polynomial-time equivalent.*■

Proof of Theorem 1.2. We recall that the ring R being a commutative one is isomorphic to a direct sum of local rings (see [19]). If among these local rings there is at least one not isomorphic to $\mathbb{Z}_2$ then the multiplicative group of this ring is nontrivial and hence $|R^\times| \neq 1$. Thus by Lemma 3.1 it suffices to find a homomorphic public-key cryptosystem over the group $R^\times$. To do this we observe that due to the commutativity of the ring R, we have $R^\times = H_1 \times \cdots \times H_k$ where H_i is a cyclic group, $i \in [k]$. So from [14, Section 2] it follows that for each i there exists a homomorphic public-key cryptosystem $\mathcal{S}_i$ over the group H_i with respect to an appropriate epimorphism $\varphi_i : G_i \to H_i$ with G_i being a finite Abelian group. Set $G = G_1 \times \cdots \times G_k$ and φ to be the epimorphism $G \to H$ induced by the epimorphisms $\varphi_1, \ldots, \varphi_k$. Now, using cryptosystems $\mathcal{S}_i$, $i \in [k]$, one can form a homomorphic public-key cryptosystem over the group $R^\times$ with respect to the epimorphism $\varphi : G \to R^\times$. Theorem is proved.■

Let R and $\mathcal{A}$ are finite rings as in Theorem 1.2. Then from the proof of this theorem it follows that the size of $\mathcal{A}$ is double exponential in the size of the ring R. Indeed, $\mathcal{A}$ is the group ring of the group G over R, whence $|\mathcal{A}| = |G|^{|R|}$, $|G| = |G_1| \cdots |G_k|$ and $|G_i|$ is exponential in $|H_i|$ (see construction in [14, Section 2]). We will see below that under the natural assumption on the presentation of $\mathcal{A}$ it is difficult to reduce the size of $\mathcal{A}$ preserving the secrecy of the homomorphism $f : \mathcal{A} \to R$ (this extends the observation from [5]).

Let $\mathcal{A}$ be a finite ring of characteristic m (i.e. the minimal integer which vanishes in $\mathcal{A}$) and $\mathcal{P}(m)$ be the set of the highest prime powers dividing m. Then it is easy to see that

$$\mathcal{A} = \bigoplus_{q \in \mathcal{P}(m)} \mathcal{A}_q \tag{6}$$

where $\mathcal{A}_q = q'\mathcal{A}$ with $q' = m/q$, is an ideal of $\mathcal{A}$ considered as a finite ring of characteristic q with the identity $q'1$. For each q the ring $\mathcal{A}_q$ is a linear space of the dimension $n_q = \log_p |\mathcal{A}_q|$ over the finite field $\mathbb{F}_p$ of the prime order p dividing q. This implies that $\mathcal{A}$ can be considered as a subring of the matrix ring $\mathrm{Mat}_n(\mathbb{Z}_m)$ where $n = \sum_q n_q$. To find a

basis of a linear space could be not easy a priori if a procedure of testing linear dependency is not known, that is why the efficiency of embedding of $\mathcal{A}$ into a matrix ring depends on the way how $\mathcal{A}$ is given. Now suppose that the size of $\mathcal{A}$ is at most exponential in $|R|$. Then the dimension n_q is polynomial in $|R|$ and hence n, $\log m$ are less than $|R|^{O(1)}$. In the following theorem we use a presentation of a ring homomorphism which is analogous to the presentation of a group homomorphism from [14].

Theorem 3.2 *Let R be a finite ring presented by the list of elements together with the Cayley tables of its additive and multiplicative groups and $\mathcal{A}$ be a subring of the ring $\mathrm{Mat}_n(\mathbb{Z}_m)$ where $\max\{n, \log m\} \leq |R|^{O(1)}$. Suppose that $f : \mathcal{A} \to R$ is a homomorphism given by generators of the ideal $\ker(f)$, a transversal X of $\ker(f)$ in $\mathcal{A}$ and the restriction of f to X. Then given $a \in \mathcal{A}$ the element $f(a)$ can be found in polynomial time in $|R|$.*

Proof. Using the decomposition (6) one can reduce the problem of computing $f(a)$, $a \in \mathcal{A}$, in polynomial time to $|\mathcal{P}(m)|$ problems of computing $f_q(a_q)$, $q \in \mathcal{P}(m)$, where $a_q = aq' \in \mathcal{A}_q$ and $f_q : \mathcal{A}_q \to R_q$ is the homomorphism induced by f. Thus without loss of generality we assume that the characteristic of $\mathcal{A}$ equals p^d for a prime p and $d \geq 1$. Since $d \leq \log m \leq |R|^{O(1)}$ one can find an embedding $\mathcal{A} \to \mathrm{Mat}_{nd}(\mathbb{Z}_p)$ in time $|R|^{O(1)}$. Then the ideal $\ker(f)$ becomes a linear space over a finite field $\mathbb{F}_p$ of dimension at most $(nd)^2$. Using linear algebra over $\mathbb{F}_p$ a linear basis of this space can be found within the same time. This enables us to solve efficiently whether or not an arbitrary element $a \in \mathcal{A}$ belongs to $\ker(f)$.

Let now $a \in \mathcal{A}$. Then there exists the uniquely determined element $x_a \in X$ such that $x_a - a \in \ker(f)$. Moreover, from the previous paragraph it follows that this element can be found in time $|R|^{O(1)}$ (it suffices to test for each $x \in X$ whether or not $x - a \in \ker(f)$). Since $f(a) = f(a + x_a - a) = f(x_a)$ and the element $f(x_a)$ is known as the part of presentation of f, the element $f(a)$ can be found within the same time.■

References

[1] F. Bao, *Cryptanalysis of a provable secure additive and multiplicative privacy homomorphism*, Proc. Workshop on Coding and Cryptography, Rocquencourt, INRIA, 2003, 43–49.

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

[3] J. Benaloh, *Dense probabilistic encryption*, First Ann. Workshop on Selected Areas in Cryptology, 1994, 120–128.

[4] S. Blackburn, S. Galbraith, *Cryptanalysis of two cryptosystems based of group actions*, Lecture Notes in Comput. Sci., **1716** (1999), 52–61.

[5] E. F. Brickell, Y. Yacobi, *On privacy homomorphisms*, Proc. EUROCRYPT 87, Lecture Notes in Comput. Sci. (1988), 117–125.

[6] 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.

[7] J. Domingo-Ferrer, *A new privacy homomorphism and applications*, Inform. Process Lett., **60** (1996), 277-282.

[8] J. Domingo-Ferrer, *A provable secure addition and multiplication privacy homomorphism*, Lecture Notes in Comput. Sci., **2433** (2002), 471–483.

[9] J. Domingo-Ferrer, R. X. Sanchez del Castillo, *An implementable scheme for secure delegation of statistical data*, Lecture Notes in Comput. Sci., **1334** (1997), 445–451.

[10] J. Feigenbaum, M. Merritt, *Open questions, talk abstracts, and summary of discussions*, DIMACS series in discrete mathematics and theoretical computer science, **2** (1991), 1–45.

[11] S. Goldwasser, M. Bellare, *Lecture Notes on Cryptography*, http://www-cse.ucsd.edu/users/mihir/papers/gb.html, 2001.

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

[13] D. Grigoriev, *Public-key cryptosystems and invariant theory*, Electronic Colloquium on Computational Complexity, 2002 `eccc.uni-trier.de/TR02-42`

[14] D. Grigoriev, I. Ponomarenko, *Homomorphic public-key cryptosystems and encrypting boolean circuits*, `arXiv:math.cs.CR/0301022`, 2003.

[15] M. Garzon, Y. Zalcstein, *The complexity of Grigorchuk groups with application to cryptography*, Theoret. Comput. Sci., **88** (1991), 83–98.

[16] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, 3, Springer, 1998.

[17] E. M. Luks, *Permutation groups and polynomial-time computation*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **11** (1993), 139–175.

[18] R. C. Lyndon, P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[19] B. R. MacDonald, *Finite Rings with Identity*, New York, Marcel Dekker, 1974.

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

[21] 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.

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

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

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

[25] D. K. Rappe, *Algebraisch homomorphe kryptosysteme*, Diplomarbeit, Dem Fachbereich Mathematik der Universität Dortmund, Oktober 2000, http://www.matha.-mathematik.uni-dortmund.de/~rappe/.

[26] R. Rivest, L. Adleman, M. Dertouzos, *On data banks and privacy homomorphisms*, Found. of Secure Computations, Academic Press, 1978, 169–179.

[27] T. Sander, C. F. Tschudin, *Protecting mobile agents against malicios hosts*, Lecture Notes in Comput. Sci., **1419** (1998), 44–60.

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

[29] J. P. Serre, *A course in arithmetic*, Springer, 1973.

[30] R. Steinwandt, *Loopholes in two public-key crytptosystems using the modular groups*, Preprint Universitaet von Karlsruhe, 2000.

[31] N. Wagner, M. Magyarik, *A public-key cryptosystem based on the word-problem*, Lect. Notes in Comput. Sci., **196** (1985), 19–36.

[32] J. Wang, *Average-Case Completeness of a Word Problem for Groups*, Proc. 27th ACM STOC, (1995), 325–334.

[33] A. Yamamura, *Public-key cryptosystems using the modular groups*, Lect. Notes in Comput. Sci., **1431**, (1998), 203–216.

[34] A. Yamamura, *A functional cryptosystem using a group action*, Lect. Notes in Comput. Sci., **1587**, (1999), 314–325.