# On non-abelian homomorphic public-key cryptosystems

Dima Grigoriev
IRM, Université de Rennes
Beaulieu, 35042, Rennes, France
dima@maths.univ-rennes1.fr

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

**Abstract**

An important problem of modern cryptography concerns secret public-key computations in algebraic structures. We construct homomorphic cryptosystems being (secret) epimorphisms $f : G \to H$, where $G, H$ are groups and $H$ is finite. A letter of a message to be encrypted is an element $h \in H$, while its encryption $g \in G$ is such that $f(g) = h$. A homomorphic cryptosystem allows one to perform computations (operating in a group $G$) with encrypted information (without knowing the original message over $H$).

In this paper certain homomorphic cryptosystems are constructed for the first time for non-abelian groups $H$ (earlier, homomorphic cryptosystems were known only for abelian groups $H$). In addition, a cryptosystem is designed for performing operations over a finite ring.

## 1 Definitions

In what follows all the groups are presented in a some natural way depending on the problem. For example, the special constructions of Section 3 are based on the groups $\mathbb{Z}_n^+$ and $\mathbb{Z}_n^*$ just given via $n$, whereas the general construction of Section 2 requires only that the multiplication and taking the inverse in the group in question could be performed efficiently. In the latter case the groups can be presented by generators and relations or even by generic algorithms (see e.g. [8]).

There is a lot of public-key cryptosystems using groups (see e.g. [1, 6, 7, 9]) 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 group. A triple $\mathcal{S} = (G, H, f(R, P, A))$ where $G$ is a finitely generated group, $f = f(R, P, A)$ is an epimorphism from $G$ onto $H$, $R \subset G$ is* *a set of distinct representatives of the left cosets of $G$ by* $\ker(f)$ *and $P$ is a surjection from the set $A$ to the group* $\ker(f)$, *is called a homomorphic cryptosystem over $H$ if the following condition are satisfied:*

(1) *appropriate presentations of $A$ and of the groups $G$ and $H$ are of size $O(N)$ for some $N \in \mathbb{N}$;*

(2) *in these presentations one can get random elements and compute the inverse of the element (in a group $G$ or $H$, respectively) and the product of two elements in probabilistic polynomial time on $N$;*

(3) $|R| = |H|$ *and the images of the elements of $R$ with respect to $f$ are given explicitely;*

(4) *the mapping $P$ is a trapdoor function.*

Condition (4) means (see [5]) that the values of $P$ can be computed in probabilistic polynomial time on $N$, whereas finding of the inverse mapping $P^{-1}$ is a hard computational problem which can be solved by means of some additional secret information (for instance, knowing some invariant of the group $G$). In a homomorphic cryptosystem $\mathcal{S}$ the elements of $H$ are encoded by the elements of $G$, all the computations are performed in $G$ and the result is decoded to $H$. More exactly:

**Public Key:** $G, H, P, R, A, f|_R$.

**Secret Key:** finding $P^{-1}$.

**Encryption:** given $h \in H$ take $g \in R$ such that $f(g) = h$, and a random element $g_0 \in \ker(f)$; the ciphertext of $h$ is the element $g_0 g \in G$.

**Decryption:** given $g \in G$ find the elements $g' \in R$ and $a \in A$ such that $g'g^{-1} = P(a)$; set $f(g) = f(g')$.

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 $g'$ one in fact has to solve the membership problem for $\ker(f)$ in $G$. 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 $P^{-1}$ is an intractable computation problem. On the other hand, our ability to compute $P^{-1}$ enables to efficiently implement the decryption algorithm. One can treat $P$ as a proof system for $\ker(f)$ in the sense of [2].

**Definition 1.2** $\mathcal{G}_{crypt}$ *is the class of all finite groups $H$ for which there exists a homomorphic cryptosystem over $H$.*

In the context of our definition of a homomorphic cryptosystem the main problem is to describe the class $\mathcal{G}_{crypt}$. To our knowledge at present all known homomorphic cryptosystems $(G, H, f(R, P, A))$ are more or less modifications of the following one with

$$G = \{g \in \mathbb{Z}_n^* : \ \mathbf{J}_n(g) = 1\}, \ H = \mathbb{Z}_2^+, \ \ker(f) = \{g^2 : \ g \in G\}, \ A = G, \ P(g) : g \mapsto g^2$$

where $n = pq$ with $p, q$ being distinct large primes of size $N = O(\log n)$, $\mathbf{J}_n$ is the Jacobi symbol and $R$ is a random set of representatives of cosets of $G$ by $\ker(G)$ (see [5]). We call it the *quadratic residue system*. It can be proved (see [5]) that in this case finding $P^{-1}$ is not easier than factoring $n$, whereas given $p$ and $q$ the computation of $P^{-1}$ can be done in polynomial time in $N$.

**Remark 1.3** It should be mentioned that a cryptosystem from [11] with $G = \mathbb{Z}_{n^2}^*$, $H = \mathbb{Z}_n^+$, $\ker(f) = \{g^n : \ g \in G\}$, $A = G$, $P : g \mapsto g^n$ and the same assumptions on $n$ and $N$ as in the quadratic residue system, is not homomorphic in the sense of Definition 1.1 because condition (3) of it does not hold. By the same reason the cryptosystem from [10] with $G = \mathbb{Z}_{p^2q}^*$, $H = \mathbb{Z}_p^+$, and $\ker(f) = \{g^{pq} : \ g \in G\}$ is also not homomorphic (besides, in this system only a part of the group $H$ is encoded).

# 2 Free products

Let us describe a construction producing new homomorphic cryptosystems from the old ones. To do this we recall some facts concerning the free products of groups. Let $G_i = \langle X_i; S_i \rangle$ be a group given by the set $X_i$ of generators and the set $S_i$ of relations, $i = 1, 2$. Without loss of generality we assume that $X_1 \cap X_2 = \emptyset$. Then the free product $G_1 * G_2$ of groups $G_1$ and $G_2$ is a group given by the presentation $\langle X_1 \cup X_2; S_1 \cup S_2 \rangle$. In particular, $G_1$ and $G_2$ are the subgroups of $G_1 * G_2$. If $X_1 = G_1$ and $X_2 = G_2$ then, obviously, any element of the group $G_1 * G_2$ can be reduced to the word in which no two adjacent letters belong to the same set among the sets $X_1$, $X_2$.

From the definition it follows that given epimorphisms $f_i : G_i \to H_i$, $i = 1, 2$, there exists the uniquely determined epimorphism

$$f_1 * f_2 : G_1 * G_2 \to H_1 * H_2 \tag{1}$$

such that $f_1 * f_2|_{G_i} = f_i$ for $i = 1, 2$ (we assume that $H_1 \cap H_2 = \emptyset$). Set $G_0 = \ker(f_1) * \ker(f_2)$. Then

$$\ker(f_1 * f_2) = \langle \{x^{-1} G_0 x : \ x \in X_1 \cup X_2, \ i = 1, 2\} \rangle \tag{2}$$

(it is the minimal normal subgroup of $G_1 * G_2$ containing $\ker(f_1)$ and $\ker(f_2)$). The following statement reflects the fact that given generators of the groups $\ker(f_1)$ and $\ker(f_2)$ the elements of $\ker(f_1 * f_2)$ can be efficiently recognized in the group $G_1 * G_2$.

**Lemma 2.1** *Let $A_i$ be a set and $P_i : A_i \to \ker(f_i)$, $i = 1, 2$, be a polynomial-time computable surjection. Set $A$ to be the set of all words in the alphabet $A_1 \cup A_2 \cup G_1 \cup G_2$. Then there exists a polynomial-time computable surjection $P = P(G_1, G_2, f_1, f_2)$ from $A$ onto* $\ker(f)$ *where $f = f_1 * f_2$, such that $P|_{A_i} = P_i$, $i = 1, 2$.*

**Proof**. Let us define a mapping $P : A \to \ker(f)$ recursively. Let $w \in A$. If $w$ is the empty word, then set $P(w) = 1_G$ where $G = G_1 * G_2$. If $w = w'x$ for some $w' \in A$ and $x \in A_1 \cup A_2 \cup G_1 \cup G_2$, then set

$$P(w) = \begin{cases} P(w')P_i(x), & \text{if } x \in A_i,\ i = 1, 2, \\ P(x^{-1})P(w')P(x), & \text{otherwise.} \end{cases}$$

Now, from (2) it follows that $P(A) \subset \ker(f_1 * f_2)$. Moreover, the mapping $P$ is efficiently computable whenever so are $P_1$ and $P_2$. On the other hand, from (2) it follows that any element $g \in \ker(f_1 * f_2)$ can be uniquely represented in the form

$$g = g_1^{-1} k_1 g_1 \cdots g_s^{-1} k_s g_s, \quad g_i \in X^*, k_i \in G_0$$

where $X^*$ is the set of all words over the alphabet consisting of letters belonging to the sets $G_i \setminus \ker(f_i)$, $i = 1, 2$. Assume by induction that $g_1^{-1} k_1 g_1 \cdots g_{s-1}^{-1} k_{s-1} g_{s-1} = P(w')$ for some $w' \in A$. Then for $w = w' g_s^{-1} a_s g_s$ with $a_s$ being the word of $(A_1 \cup A_2)^*$ such that $P(a_s) = k_s$, we have

$$P(w) = g_s^{-1} P(w' g_s^{-1} a_s) g_s = g_s^{-1} P(w' g_s^{-1}) k_s g_s = g_s^{-1} g_s P(w') g_s^{-1} k_s g_s = g.$$

Thus the mapping $P$ is a surjection and we are done.■

We need one more special homomorphism of a free product. Suppose that a finite group $H$ is a semidirect product of a group $H_1$ by a group $H_2$. Below we identify the group $H_i$ with the corresponding subgroup of $H$, $i = 1, 2$, and the elements of $H$ with the words $xy$, $x \in H_1$, $y \in H_2$. Then there exists a natural epimorphism

$$f(H_1, H_2) : H_1 * H_2 \to H \tag{3}$$

such that $f|_{H_i} = \mathrm{id}_{H_i}$, $i = 1, 2$, and

$$\ker(f) = \langle \{xyz^{-1} :\ x, y, z \in H,\ xy = z\} \rangle \tag{4}$$

where $f = f(H_1, H_2)$. Set $P(H_1, H_2)$ to be the identity mapping of the set $A(H_1, H_2) = \ker(f)$.

Let us describe the construction showing that the class $\mathcal{G}_{crypt}$ is closed with respect to semidirect produts. Let $\mathcal{S}_i = (G_i, H_i, f(R_i, P_i, A_i))$ be a homomorphic cryptosystem over a group $H_i$ with $G_i$ being a finite group, $i = 1, 2$. Suppose that a group $H$ is a semidirect product of $H_1$ by $H_2$. Set

$$G = G_1 * G_2, \quad f = (f_1 * f_2) f(H_1, H_2), \quad A = A(G_1, G_2, f_1, f_2) \times A(H_1, H_2)$$

where $f_i = f(R_i, P_i, A_i)$, $i = 1, 2$. Then due to the above definitions the mapping $f : G \to H$ is an epimorphism. Moreover, the group $\ker(f)$ contains the subgroup $\ker(f_1 * f_2)$ which is normal in $G$. So $\ker(f) = \ker(f_1 * f_2) \ker(f(H_1, H_2))$. Thus the mapping

$$P : A \to \ker(f), \quad (a, b) \mapsto P'(a) P''(b)$$

where $P' = P(G_1, G_2, f_1, f_2)$ and $P'' = P(H_1, H_2)$, is a polynomial-time computable surjection by Lemma 2.1. We claim that $\mathcal{S} = (G, H, f(R, P, A))$ where $R = R_1 R_2$, is a homomorphic cryptosystem over the group $H$. Indeed, the first three conditions of the definition are trivially satisfied. Thus it suffices to verify that the mapping $P$ is a trapdoor function. However, from the definition of the surjection $P$ it follows that the restriction of $P$ to $A_i \times \{1\}$ equals $P_i$, $i = 1, 2$. So the problem of finding $P_i^{-1}(g)$ with $g \in \ker(f_i)$ is a special case of the problem of finding $P^{-1}(g)$ with $g \in \ker(f)$. On the other hand, the mapping $(P'')^{-1}$ is obviously polynomial time computable. So, to find $P^{-1}(g)$ for $g \in \ker(f)$, it suffices to find $(P')^{-1}(g)$ with $g \in \ker(f_1 * f_2)$. Since the latter problem is obviously polynomial time reducible to finding $P_i^{-1}(g)$ with $g \in \ker(f_i)$, one can find $P^{-1}(g)$ by using a trapdoor information for $P_i$, $i = 1, 2$.

The above construction can be easily generalized to a finite set of homomorphic cryptosystems. Thus we obtain the following statement.

**Theorem 2.2** *Let $\{H_1, \ldots, H_k\}$ be a set of finite groups from $\mathcal{G}_{crypt}$ for some fixed $k \in \mathbb{N}$. Then any group $H = H_1 \cdots H_k$ such that the group $(H_1 \cdots H_i) H_{i+1}$ is a semidirect product of $H_1 \cdots H_i$ by $H_{i+1}$, $i = 1, \ldots, k-1$, belongs to the class $\mathcal{G}_{crypt}$.* $\blacksquare$

The special cases of a semidirect product are the direct and wreath products. (In the latter case the resulting group is a semidirect product of the direct power of the first group by the second group which acts on the product by permutations of direct factors, see e.g. [12]). Thus from Theorem 2.2 we obtain the following statement.

**Corollary 2.3** *The class $\mathcal{G}_{crypt}$ is closed under taking direct and wreath products.* $\blacksquare$

# 3 Explicit constructions

In this section we present an explicit homomorphic cryptosystem over a cyclic group which is in a sense a generalization of the quadratic residue cryptosystem over $\mathbb{Z}_2$. Given $m, N \in \mathbb{N}$ set

$$D_{N,m} = \{n \in \mathbb{N} : \ n = pq, \ p, q \text{ are primes}, \ |p| = |q| = N, \ m | p - 1, \ \text{GCD}(m, q - 1) = 1\}.$$

From the Dirichlet's theorem on primes in arithmetic progressions [3] it follows that given $m \in \mathbb{N}$, $m > 2$, the set $D_{N,m}$ is not empty for sufficiently large numbers $N$.

Let $n \in D_{N,m}$ for some natural numbers $N$ and $m > 2$. Then the group $G = \mathbb{Z}_n^*$ has a normal subgroup $G_0 = \{g^m : g \in G\}$ the factor by which is isomorphic to the group $H = \mathbb{Z}_m^+$. Denote by $f$ the corresponding epimorphism from $G$ to $H$. The mapping $P : A \to G_0$ with $A = G$ taking $g \in G$ to $g^m$ is obviously a polynomial time computable surjection (end even epimorphism). Next, any element of the set

$$R_{m,n} = \{(g_0, \dots, g_{m-1}) : \ g_i \in G, \ G_0 g_i \neq G_0 g_j \ \text{ for } \ i \neq j\}$$

is a system of distinct representatives of the cosets of $G$ by $G_0$. Now we claim that the triple $\mathcal{S}_{N,m,n} = (G, H, f(R, P, A))$ with randomly chosen $R \in R_{m,n}$ is a homomorphic cryptosystem over $H$ whenever the following statement is true:

**Assumption (*).** The problem $\mathcal{P}(m)$, of finding the $m$-root in $\mathbb{Z}_n^*$ for $n \in D_{N,m}$ given a random element $R \in R_{m,n}$ is not easier than the same problem without any such $R$.

Again conditions (1), (2), (3) of the definition of a homomorphic cryptosystem are trivially satisfied. In fact, all we need follows from the lemma below.

**Lemma 3.1** *Let $m, N \in \mathbb{N}$, $m > 2$, and $n \in D_{N,m}$. Then*

(1) *given primes $p$ and $q$ such that $n = pq$ and a number $g \in \mathbb{Z}_n^*$ being $m$-power, one can find an $m$-root of $g$ in probabilistic polynomial time in $N$;*

(2) *the factoring problem for $n$ is probabilistic polynomial time reducable to the problem of finding the $m$-root in $\mathbb{Z}_n^*$.*

**Proof**. Throughout the proof we will identify $\mathbb{Z}_n^*$ with $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. To prove statement (1) we make use Rabin's probabilistic polynomial-time algorithm for finding roots of polynomials over finite prime fields (see [13]). Namely, given $p, q$ and an $m$-power element $g \in \mathbb{Z}_n^*$ we proceed as follows:

**Step 1.** Find the numbers $g_p \in \mathbb{Z}_p^*$ and $g_q \in \mathbb{Z}_q^*$ such that $g = g_p g_q$.

**Step 2.** By Rabin's algorithm (for a prime field) find the roots $h_p \in \mathbb{Z}_p^*$ and $h_q \in \mathbb{Z}_q^*$ of the polynomials $x^m - g_p$ and $x^m - g_q$.

**Step 3.** Output $h = h_p h_q$.

Since, obviously, $h^m = h_p^m h_q^m = g_p g_q = g$, statement (1) is proved. To prove statement (2) suppose that we are given a probabilistic polynomial-time algorithm $Q_n$ that given $g \in \mathbb{Z}_n^*$ computes an $m$-root $Q_n(g)$ of $g$. The following procedure using well-known observations [5] shows how $Q_n$ helps to find the numbers $p$ and $q$.

**Step 1.** Randomly choose $x \in \mathbb{Z}_n^*$.

**Step 2.** Set $y = Q(x^m)$. If $x = y$, then go to Step 1.

**Step 3.** Output $q = \mathrm{GCD}(xy^{-1} - 1, n)$ and $p = n/q$.

Let $x = x_p x_q$ and $y = y_p y_q$ where $x_p, y_p \in \mathbb{Z}_p^*$ and $x_q, y_q \in \mathbb{Z}_q^*$. Since $\mathrm{GCD}(q-1, m) = 1$ and $x_q^m = y_q^m$, we conclude that $x_q = y_q$, So

$$xy^{-1} = (x_p x_q)/(y_p x_q) = x_p/y_p = 1 \pmod{q}.$$

Thus $xy^{-1} - 1$ is a multiple of $q$. To complete the proof we note that since $m = O(1)$, the loop of Steps 1,2 terminates with a large probability after a polynomial number of iterations.■

Unfortunately, we don't know how to apply this lemma without assumption (*) because in our case the system $\mathcal{S}_{N,m,n}$ includes the set $R \in R_{m,n}$. However, from it we obtain the following statement.

**Theorem 3.2** *Under assumption (*) the triple $\mathcal{S}_{N,m,n}$ for $m > 2$ is a homomorphic cryptosystem over $\mathbb{Z}_m^+$; in particular, $\mathbb{Z}_m^+ \in \mathcal{G}_{crypt}$ for all $m > 1$.*■

We complete the section by mentioning that $\mathcal{S}_{N,m,n}$ can be slightly modified to avoid the applying of Rabin's algorithm for finding roots of polynomials over finite fields. In principle, to implement the decryption algorithm it suffices to determine whether a given number $g \in G$ belongs to the group $G_0$ or not. However, this can be done by observing that $g \in G_0$ iff $g_p^{(p-1)/m} = 1 \pmod{p}$.

# 4 Cryptosystems over finite rings

The results of this paper can be applied to implement secure circuit evaluation introduced by Yao in [15]. To do this we construct a cryptosystem for secure computations over finite fields and the rings $\mathbb{Z}_n$, $n \in \mathbb{N}$. An alternative approach can be found in [14] (see also [4] where the problem of constructing a homomorphic cryptosystem over rings was posed).

Let $F$ be a finite field. Set $H$ to be the semidirect product of the additive group $F^+$ of $F$ by its multiplicative group $F^*$. Since the group $F^+$ is a direct product of cyclic groups and the group $F^*$ is cyclic itself, we conclude by Theorems 2.2 and 3.2 that $H \in \mathcal{G}_{crypt}$. Thus there exists a homomorphic cryptosystem $\mathcal{S}(F)$ over the group $H$. On the other hand, any computation in $F$ can be performed in the group $H$. Indeed, given $a, b \in F$ one can find the sum $a + b$ (resp. the product $ab$ if $ab \neq 0$) in $F$ by computing the product of translations $x + a$ and $x + b$ (resp. linear functions $ax$ and $bx$) in the group $H$ considered as the group of affine functions over $F$. This shows that the cryptosystem $\mathcal{S}(F)$ enables us to perform secret computations in a finite field. The similar trick with $H = \mathbb{Z}_n^+ \mathbb{Z}_n^*$ can be used to construct a cryptosystem for secret computations in the rings $\mathbb{Z}_n$.

# 5 Conclusions

From Theorems 2.2 and 3.2 it follows that the class $\mathcal{G}_{crypt}$ contains all finite groups which can be constructed from cyclic groups by taking semidirect products. In particular, there are homomorphic cryptosystems over the dihedral groups (which are semidirect products of a cyclic group with $\mathbb{Z}_2$) and so over symmetric groups $\mathrm{Sym}(n)$ for $n = 2, 3$. Moreover, by Corollary 2.3 all elementary Abelian groups belong to $\mathcal{G}_{crypt}$. So there exists a homomorphic cryptosystem over the group $\mathrm{Sym}(4) \approx ((\mathbb{Z}_2 \times \mathbb{Z}_2)\mathbb{Z}_3^+)\mathbb{Z}_2$. It would be interesting to construct a homomorphic cryptosystem over an arbitrary symmetric group.

**Acknowledgements.** The authors would like to thank the Max-Planck Institut fuer Mathematik (Bonn) during the stay in which this paper was done; also Eberhard Becker who has drawn the authors attention to homomorphic cryptosystems and Igor Shparlinski for useful discussions.

# References

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

[2] S. Cook, R. A. Reckhow, *The relative efficiency of propositional proof systems*, J. Symbolic Logic, **44** (1979), 36–50.

[3] H. Davenport, *Multiplicative number theory*, Springer, 1980.

[4] 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.

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

[6] 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.

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

[12] D. S. Passman, *Permutation groups*, W.A.Benjamin, Inc., New-York-Amsterdam, 1968.

[13] M. O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comput., **9** (1980), 273–280.

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

[15] A. Yao, *How to generate and exchange secrets*, Proc. 27th IEEE Symp. Found. Comput. Sci, 1986, 162–167.