1. Introduction

In public-key cryptography, the problem is to produce a cryptosystem that contains the following ingredients: a public key \( k_e \), a secret key \( k_d \), a public encrypting function \( f_e \), and a decrypting function \( f_d \). If somebody (usually named Bob) wants to send a message \( m \) to another person (usually named Alice) via a public channel, then he transmits the encryption \( u = f_e(m, k_e) \). To decrypt the message, Alice calculates \( m = f_d(u, k_d) \). It is assumed that \( k_d \) is known only to Alice, while \( k_e \) and \( f_e \) are known publicly and the function \( f_d \) is known to Alice (sometimes it may be known publically as well). Another important property of a cryptosystem is that an unauthorized person (named Charlie) should be unable to learn \( m \) (without knowing \( k_d \) and \( f_d \)).

A lot of efforts were made to design cryptosystems (some literature can be found in [17, 13, 11]). Still the security is proved for no cryptosystem, and the issue of security remains a challenging problem. All the existing results on security concern the impossibility of breaking a cryptosystem by certain fixed means, say, in frames of NP-hard problems.

In these notes, we study cryptosystems that involve ideas from the theory of group invariants. Several known cryptosystems rely on groups (below we give a short overview of them), but, surprisingly, the concept of a group representation invariant was never exploited, although it fits quite well the aims of cryptography. The most recognized cryptosystems are based on number-theoretical ideas, in particular, RSA, Diffie–Hellman, or the elliptic curves cryptosystems (see, e.g., [17]; this book contains also some cryptosystems involving combinatorial-algebraic NP-hard problems).

In these notes, we study cryptosystems that involve ideas from the theory of group invariants. Several known cryptosystems rely on groups (below we give a short overview of them), but, surprisingly, the concept of a group representation invariant was never exploited, although it fits quite well the aims of cryptography. Still, applying invariants to cryptography encounters the same difficulties as other known approaches; however, the purpose of these notes is to introduce invariants into cryptography, to design possible cryptosystems, and to discuss problems concerning their security.

The general idea behind using groups (and their invariants) is as follows. Let \( E \) denote the set of encrypted messages, and let a group \( G \) act on \( E \). Some examples of \( E \) are the set of words in a certain alphabet or a vector space. In addition, there is a distinguished subset \( M \subset E \) of plaintext messages, which is transversal to the orbits of \( G \), i.e., no two distinct messages \( m_1, m_2 \in M \) belong to the same orbit of \( G \).

Then the action of \( G \) is used for a probabilistic encryption (see [14, 13]), which is more efficient in “hiding information” than a deterministic one. Thus to encrypt a message \( m \in M \), Bob picks an element \( g \) from the group \( G \) at random and transmits \( gm \in E \) via the public channel. To learn \( m \), Alice has to decrypt \( gm \) by applying her secret key. And Charlie must be unable to learn \( m \) from \( gm \).

Usually, the latter two properties of the cryptosystem are achieved by a special choice of \( G \). In the widely used quadratic residue cryptosystem (see [14, 13]), one takes the integer \( n = pq \) for large primes \( p \) and \( q \) (which are the secret key of Alice). Then one takes \( (\mathbb{Z}_n^*)^2 \) as the group \( G \) and sets \( E = \{ g \in \mathbb{Z}_n^* : J_n(g) = 1 \} \), where \( J_n \) denotes the Jacobi symbol. One takes also a nonsquare element \( a \in E - G \) and puts \( M = \{ \{1, a\} \} \). The public key consists of \( n \) and \( a \). Thus to encrypt 1, Bob first picks a random element \( g \in \mathbb{Z}_n^* \); then the cyphertext of 1 is the square \( g^2 \in G \subset E \) of this element, and the cyphertext of \( a \) is \( g^2a \), which is a random nonsquare in \( E \); clearly, \( E = G \cup Gn \).

The task of Alice is to verify whether an element \( b \in E \) (this is a transmitted encrypted message) is a square. Alice can easily do this using \( p \), \( q \), and the Legendre–Jacobi symbols \( J_p \) and \( J_q \). On the other hand, it is a common belief that Charlie is unable to verify whether \( b \) is a square without knowing \( p \) and \( q \).

The described quadratic residue cryptosystem was generalized to a class of cryptosystems called homomorphic. Namely, let \( f : E \to H \) be a group epimorphism, which is the secret key of Alice. There is an exact sequence of
group homomorphisms

\[ qB \xrightarrow{\pi} E \xrightarrow{f} H \to \{1\}, \]

and the public key is \(B, s, E, H\), and a subset \(M \subset E\) that is transversal to the (normal) subgroup \(G = \ker(f)\) (thus \(f\) provides a bijection between \(M\) and \(H\)). This is consistent with the above notation: \(G\) acts (by left multiplication) on \(E\), and the set of plaintext messages \(M\) is transversal to this action; but here the group \(G\) is given implicitly as the image \(s(B)\). To encrypt a message \(m \in M\), Bob picks an element \(b \in B\) at random and transmits \(s(b)m\). Alice decrypts \(s(b)m\) by applying \(f\), taking into account that \(f(s(b)m) = f(m)\). It is difficult for Charlie to decrypt the ciphertext without knowing \(f\). In the quadratic residue cryptosystem described above, we have \(H = \mathbb{Z}_2, B = E, s(b) = b^2,\) and \(f\) is the epimorphism of the quadratic residue.

In [9, 33], a question was posed for what groups \(H\) homomorphic systems can be constructed (more generally, if one may consider ring homomorphisms rather than group homomorphisms)? For some abelian groups \(H\), cryptosystems were designed in [4, 23–25, 27]. For certain dihedral groups \(H\), cryptosystems were designed in [28]. In [15], a homomorphic system was designed for an arbitrary solvable group \(H\). For cryptosystems over elliptic curves, see [18, 17].

What is common in all the mentioned constructions is that decrypting relies on the knowledge of the secret primes \(p\) and \(q\). In these notes, we suggest another way of decrypting (and encrypting), which is based on an invariant \(w : E \to F\), i.e., on a function \(w\) that is constant on the orbits of \(G\). Then Alice is able to decrypt an encrypted message \(gm\) by means of calculating \(w(gm) = w(m)\), provided that \(w\) takes distinct values on the elements (plaintext messages) from \(M\).

The theory of invariants (see, e.g., [7, 30, 31]) is developed mostly in the situation where \(G : E \to E\) is a linear representation, so \(E\) is a vector space, \(G \subset GL(E)\) is a subgroup of matrices over a field \(F\), and \(w\) is a polynomial. But perhaps it would be also worthwhile to look at other group actions and their invariants.

Since the invariants \(w\) are known explicitly and can be calculated fast for only few infinite series of linear representations \(G \subset GL(E)\) (see [31]), we suggest to hide \(G\) by considering its conjugation \(a^{-1}Ga \subset GL(E)\) for a secret matrix \(a \in GL(E)\). Then an invariant \(e \to w(ae)\) of the conjugation \(a^{-1}Ga\) enables Alice to decrypt the message \(a^{-1}gam\), where \(a^{-1}ga\) is a random element from \(a^{-1}Ga\) chosen by Bob for encrypting a message \(m\). Usually, the group \(a^{-1}Ga\) (which constitutes the public key together with \(E\) and \(M \subset E\)) is given by a set of matrices from \(GL(E)\) that are its generators. To represent a group by a set of its generators is a quite succinct way; in particular, the known finite simple groups are representable just by two generators, and any finite group \(G\) is representable by \(\log_2 |G|\) generators. In calculations with a group \(G\) represented by a set of generators, it is not necessary to assume that \(G\) is finite (which is the case, in particular, if the field \(F\) is finite), because for encrypting Bob has just to pick a certain product of generators of \(a^{-1}Ga\) at random.

In the next sections, we describe cryptosystems based on group invariants and discuss the issues of their security, but first we complete the overview by describing two families of cryptogaphic tools that involve groups.

Another particular problem of cryptography, apart from designing cryptosystems, is the key agreement protocol (see, e.g., [13, 11, 17]). Now Alice and Bob want to agree about a common key by communicating via a public channel. The usual approach suggests that each of them chooses secret commuting operators \(f_A\) (Alice) and \(f_B\) (Bob) on the same set \(E\), and, in addition, they choose a certain (public) element \(e \in E\). Then Alice communicates \(f_A(e)\), Bob communicates \(f_B(e)\), and they agree on the common key \(f_A(f_B(e)) = f_B(f_A(e))\). In the first key agreement protocol due to Diffie and Hellman (see, e.g., [13, 17]), the commuting operators were \(f_A(e) = e^a\) and \(f_B(e) = e^b (\text{mod } p)\) for integers \(a\) and \(b\). Thus decrypting (by Charlie) of the Diffie–Hellman protocol relates to computing the discrete logarithm, which is believed to be difficult; the complexity of this problem was studied in [6, 22].

This general approach was considered in the following setting (see [3, 26, 16]). Let \(E\) be a group with two subgroups \(E_A, E_B \subset E\) commuting with each other (elementwise). Then \(f_A\) is the conjugation \(e \to a^{-1}ea\) for a randomly picked \(a \in E_A\); respectively, \(f_B(e) = b^{-1}eb\) for \(b \in E_B\). In [16], the braid group is used as \(E\), and the difficulty of breaking this key agreement protocol relates to the difficulty of the conjugacy problem in the braid group.

Several cryptosystems based on the difficulty of the word problem in appropriate groups were suggested in [2, 8, 10, 32].

The last family of cryptosystems we mention rely on lattices (which are discrete abelian subgroups of \(\mathbb{R}^n\)). The first such construction is due to [1]. Let \(L \subset \mathbb{R}^n\) be an \(n\)-dimensional lattice that contains a (hidden) \((n - 1)\)-dimensional sublattice \(L'\) whose linear span is a hyperplane \(H\) satisfying the following property. The coset hyperplanes \(H_i\) parallel to \(H\) such that \(\bigcup_i H_i \supset L\) are well separated: the distance between every adjacent