COMBINATORIAL GROUP THEORY AND PUBLIC KEY CRYPTOGRAPHY

VLADIMIR SHPILRAIN AND GABRIEL ZAPATA

Abstract. After some excitement generated by recently suggested public key exchange protocols due to Anshel-Anshel-Goldfeld and Ko-Lee et al., it is a prevalent opinion now that the conjugacy search problem is unlikely to provide sufficient level of security if a braid group is used as the platform. In this paper we address the following questions: (1) whether choosing a different group, or a class of groups, can remedy the situation; (2) whether some other "hard" problem from combinatorial group theory can be used, instead of the conjugacy search problem, in a public key exchange protocol. Another question that we address here, although somewhat vague, is likely to become a focus of the future research in public key cryptography based on symbolic computation: (3) whether one can efficiently disguise an element of a given group (or a semigroup) by using defining relations.

Contents

1. Introduction

One of the possible generalizations of the *discrete logarithm problem* to arbitrary groups is the so-called *conjugacy search problem*: given two elements a, b of a group G and the information that $a^x = b$ for some $x \in G$, find at least one particular element x like that. Here a^x stands for xax^{-1}. The (alleged) computational difficulty of this problem in some particular groups (namely, in braid groups) has been used in several group based cryptosystems, most notably in [1] and [13]. However, after some initial excitement (which has even resulted in naming a new area of "braid group cryptography" — see [3], [4]), it seems now that the conjugacy search problem in a braid group cannot provide sufficient level of security; see [18] for explanations.

Therefore, one faces the following two natural questions:

Question 1. Is there a group, or a class of groups, where the public key exchange protocol suggested in [1] would be secure enough to be used in real-life applications?

Question 2. Is there another "hard" problem in combinatorial group theory that can be used, instead of the conjugacy search problem, in a public key exchange protocol?

Without a positive answer to at least one of these questions, it is unlikely that combinatorial group theory will have a significant impact on public key cryptography, which is now dominated by methods and ideas from number theory.

We point out one more question, which has not been getting sufficient attention so far, but is likely to become a focus of the future research in public key cryptography based on symbolic computation:

Question 3. Can one efficiently disguise an element of a given group (or a semigroup) by using defining relations?

Disguising an element before transmission is sometimes called "diffusion" — see e.g. [6]. The importance of this is rather obvious: if, for example, one transmits a conjugate xax^{-1} of a public element a "as is", i.e., without diffusion, then the opponent can determine the private element x just by inspection. Similar problem arises in any other public key exchange protocol. In protocols based on ideas from number theory, the diffusion is usually provided "automatically", due to various properties of the decimal or other numerical system that is used. For instance, in the product $7 \cdot 3{=}21$, the factors 7 and 3 cannot be determined just by inspection; this is provided simply by the way we multiply integers in the decimal system, or, equivalently, by the existence of a simple "normal form" for integers.

In abstract groups, we usually do not have this facility. In fact, in an abstract group (or a semigroup), the result of multiplication is simply concatenation: $a \cdot b = ab$, i.e., an extra effort is always required to disguise factors in a product. This is why a diffusion mechanism is of paramount importance in any public key exchange protocol based on symbolic computation.

We note here that recent work of Myasnikov and Ushakov [16] makes it appear likely that, speaking somewhat informally, in a "generic" group, the amount of work needed to disguise a "generic" element by using defining relations is about the same as needed to recover an element from its disguised form. This, of course, is unacceptable in cryptographic applications. It seems that the difficulty in disguising an element of a group (or a semigroup) by using defining relations might be a major obstacle for using symbolic computation in public key cryptography, and the problem of diffusion will therefore take the center stage in future research.

In this paper, we contribute toward a solution of this problem in Section 7 by breaking down defining relations of a group into "small pieces". More formally, we replace a given group by an isomorphic group where all relators have length at most 3. Intuitively, diffusion should be easier to achieve in groups with shorter defining relations, so we hope that our idea can be useful.

As far as other questions are concerned, we have to say up front that, in our opinion, Question 1 has a smaller chance for a positive answer, and it is unlikely that the conjugacy search problem will be used in real-life implementations. Nevertheless, we study Question 1 here in Section 6 by exploring the idea of using random groups from a sufficiently large *class of groups* instead of a single group. Technically, braid groups, too, are a class of groups, but this class is too narrow in the sense that, informally speaking, any (meaningful) algorithm that works for a particular group $B_n, n \geq 5$, would also work for B_m for any $m \geq 5$. We may call such a class of groups "algorithmically homogeneous". Here we draw attention to a more diverse class of *small cancellation groups* that satisfy small cancellation conditions $C(4)$, $T(4)$, but not $C'(\frac{1}{6})$ (see [14]). The latter is needed to try to avoid hyperbolic groups (all finitely presented $C'(\frac{1}{6})$ groups are hyperbolic), where the conjugacy search problem can be solved very quickly (see [10] and [11] for discussion).

In the class of groups with small cancellation conditions $C(4)$ and $T(4)$, the word problem is solvable in quadratic time (see [14, Theorem V.6.3]), which meets the necessary condition for an efficient common key extraction by authorized parties. We note in passing that the existence of a unique *normal form* for elements of a particular group G is not necessary for common key extraction, as observed in [1]. If Alice and Bob have arrived at a point where Alice has an element, say, u, and Bob has an element v such that $u = v$ in G, then they can establish a common key as follows. Alice chooses, privately, a finite binary sequence $b_1, b_2, ...$, which is going to be her common secret key with Bob. She then transmits a sequence of group elements $u_1, u_2, ...$ such that $u_i = u$ in G if and only if $b_i = 1$. Bob recovers the sequence $b_1, b_2, ...$ by comparing $u_1, u_2, ...$ to his v.

We note that there is no known polynomial time algorithm for solving the conjugacy search problem in an arbitrary group with small cancellation conditions $C(4)$ and $T(4)$.

In Section 2, we consider a different problem from combinatorial group theory that can be used in a public key exchange protocol. This is yet another generalization of the discrete logarithm problem. Given a group G with the semigroup of endomorphisms $End\ G$, suppose there are two subsemigroups, $A \subseteq End\ G$ and $B \subseteq End\ G$, such that for any $\alpha \in A$ and $\beta \in B$, one has $\alpha\beta = \beta\alpha$. Let $w \in G$ be a public element. Then the key exchange protocol is quite standard: Alice chooses, privately, some $\alpha \in A$ and sends $\alpha(w)$ to Bob. Bob chooses some $\beta \in B$ and sends $\beta(w)$ to Alice. Since $\alpha\beta = \beta\alpha$, both end up with a common private key $\alpha(\beta(w)) = \beta(\alpha(w))$.

The point is, of course, in selecting a platform group G and semigroups $A, B \subseteq End\ G$ wisely, so that the corresponding key exchange protocol is both secure and efficient. One special case of such arrangement appears in [13], where G is a braid group B_n, and A, B consist of inner automorphisms (i.e., conjugations). This arrangement however makes the cryptosystem vulnerable to so-called "length based" attacks (see e.g. [5], [7], [9]) because applying a generic automorphism to a generic element of a group tends to increase the length of (the normal form of) this element. To avoid attacks of this kind, we suggest here using non-injective endomorphisms; the effect of such an endomorphism on the length of an element is no longer predictable.

Again, in Section 4, we suggest using a large class of groups instead of a fixed group and selecting a random group from this class every time one wants to initiate a public key exchange protocol. A particular class of groups that we consider here is the class of *Artin groups of extra large type*. Groups in this class are known to be automatic [17], which implies, in particular, that the word problem in any group from this class is solvable in quadratic time. Further details are given in Section 5.

Finally, we note that, as a further generalization, one can use arbitrary well-defined mappings α, β (not necessarily endomorphisms) of a group G in the above context. A simple example of that kind was given in [12]; see also our Section 2.

2. Algebraic public-key cryptographic systems

The central requirement for an operational public-key cryptographic system (PKC) is a *one-way function*; in theory, it is the security core in the development and implementation of public-key cryptographic protocols. Let S and T be two sets. In essence, a one-way function is a feasibly computable function $f : S \to T$ such that given the *image* $y = f(x)$, it is computationally infeasible to determine a *preimage* $x \in S$.

For an algebraic characterization of a one-way function, we assume S and T to be associative algebraic structures with a single binary operation, e.g., semigroups. We call these structures *platforms* when used in the context of cryptography.

Let the pair $\langle X; R\rangle$ be a *presentation* of a semigroup S, where $X = \{x_1, x_2, \dots\}$ is a set of generators of S and $R = \{r_1 = r'_1, r_2 = r'_2, \dots\}$ a set of defining relations. The *full transformation semigroup* of S, denoted by $\mathcal{T}_S$, is the set of all functions $S \to S$ closed under composition, see e.g. [8]. A function $t \in \mathcal{T}_S$ is *well-defined* in S if for any $w, w' \in S$ such that $w = w'$, one has $t(w) = t(w')$.

The set of well-defined functions from $\mathcal{T}_S$ can be utilized to deliver *diffusion* in S, i.e., to dissemble an element of the platform S before transmission by using its defining relations. If a subset $T \subseteq \mathcal{T}_S$ consisting of well-defined functions acts on S, say,

$$f : S \times T \longrightarrow S \quad \text{described by} \quad f : (w, t) \longmapsto t(w),$$

such that recovering w from $t(w) = f(w, t)$ is computationally infeasible, then the action f satisfies the principal requirement of a one-way function.

A particular example of such a subset $T \subseteq \mathcal{T}_S$ would be $End\, S$, the set (which is actually a monoid) of endomorphisms of S. Let G be an arbitrary semigroup and let $\rho : G \to End\, S$ be a morphism. Then ρ determines an action of S by its image (denoted by $Im\, \rho$), i.e., $g \mapsto (t \mapsto t(w))$, for $g \in G$ and $t \in End\, S$. The function

$$f : S \times T \longrightarrow S \quad \text{given by} \quad (w, t) \longmapsto t(w) = w'$$

explicitly defines the action, where $T = Im\, \rho$. If the search for a $t \in T$ such that $f(w, t) = w'$ is computationally infeasible, then the action f is an intrinsic one-way function inherited by S via a semigroup T.

Therefore, an algebraic characterization of a one-way function can be determined through an action, as specified above, by algebraic properties of S and T. Without loss of generality, given feasibly computable algebraic structures S and T, if there exists an action $f : S \times T \to S$ such that f is a one-way, well-defined function for fixed values of T, then the elements of S can be manipulated for public-key encryption.

Definition 1. *An algebraic public-key cryptographic system is a tuple* $(S,\, T,\, f;\, \mathcal{H},\, h)$, *satisfying the following properties:*

- S *and* T *are feasibly computable algebraic structures (e.g. semigroups).*
- $f : S \times T \to S$ *is an action that is one-way and well-defined for fixed values of* T*: given a private* $t \in T$ *and any public* $w \in S$*, it is infeasible to determine* t *from* $f(w,\, t)$*, and for any* $w' \in S$ *such that* $w' = w$*, one has* $f(w', t) = f(w, t)$*.*
- $\mathcal{H}$ *is a set of auxiliary feasibly computable algebraic structures defined for specific protocols (i.e. key exchange, decryption, etc).*
- $h : X \times Y \to X$ *is an auxiliary action (defined for specific protocols), where* X *and* Y *are one of the algebraic structures* S, T, *or* $H \in \mathcal{H}$.

Let us now assume S to be a feasibly computable group G. With the developed analysis, we interpret the standard theory of PKC as arising from a *permutation representation* $\rho : G \to \mathcal{S}_G$, where $\mathcal{S}_G \subseteq \mathcal{T}_G$ is the symmetric group of G, such that $\rho : x \mapsto x^{\rho}$ and $Im\,\rho$ is a subgroup of the group of automorphisms of G, denoted by $Aut\,G$. Since the elements $x^{\rho} \in Im\,\rho$ are automorphisms, x^{ρ} acts by permuting words $g \in G$ with the capability of providing cryptographic confusion and diffusion (see e.g. [6]).

If for every $x^{\rho} \in Im\,\rho$ the recovery of g from $g' = x^{\rho}(g)$ is infeasible, then the representation ρ determines a one-way function; namely, the group action

$$f : G \times N \longrightarrow G \quad \text{defined by} \quad (g, x^{\rho}) \longmapsto x^{\rho}(g) = g',$$

where N is a subgroup of $Aut\,G$. Given $g' = f(g, x^{\rho})$, it should be noted that it suffices to "search" for $(x^{\rho})^{-1}$ in $Aut\,G$ to determine $g \in G$; this establishes an *automorphism search problem* for G.

Definition 2. *Let* $F(X)$ *be the free group with basis* X *and let* $\langle X; R\rangle$ *be a presentation of* G*.*

- *Given an arbitrary word* $g \in G$*,* the word problem *(WP) is the algorithmic problem of deciding whether or not* $g = 1$*.*
- *Given a word* $g \in G$ *such that* $g = 1$*, the word search problem (WSP) is the algorithmic problem of "searching" for an explicit expression of* g *as a product* $u_1\, r_1^{\epsilon_1} u_1^{-1} \cdots u_t\, r_t^{\epsilon_t} u_t^{-1} = g$*, where* $u_i \in F(X)$*,* $r_i \in R$*, and* $\epsilon_i \in \{\pm 1\}$*.*
- *Two words* $g, h \in G$ *are* conjugate *if there is an* $x \in G$ *such that* $xgx^{-1} = h$*. The algorithmic problem of deciding whether or not two arbitrary words* $g, h \in G$ *are conjugate is the* the conjugacy problem *(CP).*
- *Given two conjugate words* $g, h \in G$*, the conjugacy search problem (CSP) is the algorithmic problem of "searching" for an* $x \in G$ *satisfying* $xgx^{-1} = h$*.*

Example 1. The braid group on n strands, denoted by B_n, with presentation

$$B_n = \langle\, \sigma_1, \ldots, \sigma_{n-1}\,;\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \textit{for}\ |i-j| = 1,\ \sigma_i\sigma_j = \sigma_j\sigma_i \ \textit{for}\ |i-j| \geq 2\,\rangle,$$

has the word problem solvable in quadratic time. The braid group B_n is a suggested group-theoretic platform for the implementation of the conjugacy search problem, see [1], [13].

We note that the group $Aut\, B_n$ is equal to $\langle\, Inn\, B_n,\, \eta\,\rangle$, where $Inn\, B_n$ is the group of inner automorphisms of B_n and $\eta : \sigma \mapsto \sigma^{-1}$, for any $\sigma \in B_n$. Thus, the general automorphism search problem for B_n basically reduces to the inner-automorphism search problem for B_n, i.e., to the conjugacy search problem for braid groups.

3. Commuting Action Key Exchange (CAKE)

To change the standard methodology of working implicitly just with the automorphism group of G, we generalize an action $f : G \times Aut\, G \to G$, using Definition 1, to a well-defined action on an algebraic structure S by an algebraic structure N for fixed values of N. To manifest the advantage of the abstraction, we construct an algebraic PKC for the implementation of a key exchange protocol based on a generalization of the discrete logarithm problem:

Definition 3 (Commuting Action Key Exchange, CAKE)**.** *Select the platforms S and T to establish an algebraic PKC tuple $(S,\, T,\, f;\, \mathcal{H})$, where the auxiliary set $\mathcal{H}$ is $\{A, B \subseteq T \,|\, \forall\, \alpha \in A\ \forall \beta \in B\ \alpha\,\beta = \beta\,\alpha\,\}$. The key exchange protocol is set for two entities, Alice and Bob.*

Protocol:

1. *The semigroup S, a word $w \in S$, and a generating set for each semigroup in $\mathcal{H}$ are made public.*
2. *Alice chooses a private word $\alpha \in A$ satisfying $f(w, \alpha) \neq 1$ and transmits $f(w, \alpha) = w\alpha$ to Bob.*
3. *Bob chooses a private word $\beta \in B$ satisfying $f(w, \beta) \neq 1$ and transmits $f(w, \beta) = w\beta$ to Alice.*
4. *Alice computes $f(w\beta, \alpha) = w\,\beta\alpha$ and Bob computes $f(w\alpha, \beta) = w\,\alpha\beta$. Both entities establish $w\,\alpha\beta = w\,\beta\alpha$ as the common secret key.*

Example 2. The Diffie-Hellman protocol becomes an instance of the CAKE protocol if the multiplicative group of integers modulo a prime number and its standard automorphism group are the chosen platforms.

A simple, well-studied associative algebraic system S with a single binary operation and a commutative semigroup $T \subseteq End\, S$ generated by a large set of elements are good potential candidates for the implementation of CAKE. In this case, both α and β are endomorphisms of S, and $\alpha(\beta(w)) = \beta(\alpha(w))$ becomes the common key. Similarly, one can also use a commutative subsemigroup T of the full transformation semigroup $\mathcal{T}_S$ containing well-defined functions α, β (not necessarily endomorphisms) of S. A basic example of that kind was given in [12].

Example 3. Let $A, B \subseteq S$ be two subsemigroups of a semigroup S such that $ab = ba$ for any $a \in A,\ b \in B$. Given a public element $w \in S$, Alice computes $w \mapsto a_1 w a_2$, where $a_1, a_2 \in A$ are her private elements, and transmits this new element to Bob (after disguising it somehow). Similarly, Bob transmits $w \mapsto b_1 w b_2$, where $b_1, b_2 \in B$ are his private elements. The common key now is $a_1 b_1 w b_2 a_2 = b_1 a_1 w a_2 b_2$.

Note that if $A, B \subseteq S$ are groups, the protocol of Ko, Lee et. al. [13] can also be obtained as a special case of the above protocol where $a_2 = a_1^{-1}$ and $b_2 = b_1^{-1}$.

4. Classes of groups vs. particular groups

Let $\mathcal{B}$ be the class of braid groups. A generic element B_n from this class can be chosen from $\mathcal{B}$ simply by randomly selecting a natural number for the variable n. For general applications, once a choice for a braid group B_n is made, an algorithm that applies to this group also applies to other braid groups. Informally speaking, the braid groups are "algorithmically homogeneous" and this can be a drawback for cryptographic applications, as stated in the Introduction. In the following sections, we address this issue by considering wider classes of groups.

In particular, we introduce additional randomness to an algebraic PKC protocol, requiring that its platforms be selected at random from a wider class of groups at the beginning of the generation of keys. Moreover, isomorphic groups from a wider class provide a mechanism for diffusion, as examined in the last section of the paper. The use of isomorphic groups and random selections from a class of groups is a familiar scenario for cryptosystems; both in the RSA and in the discrete logarithm cryptosystems, primes are randomly selected for application, i.e., a multiplicative group of integers and a subgroup of its automorphism group are randomly selected.

To exemplify these ideas, we first consider the class of Artin groups of extra large type for the implementation of the Commuting Action Key Exchange protocol, via endomorphisms. Second, despite our belief that Question 1 in the Introduction is likely to have a negative answer, we give the conjugacy search problem (CSP) a benefit of the doubt; we consider the class of groups satisfying small cancellation conditions $C(4)$ and $T(4)$, but not $C'(\frac{1}{6})$ (to try to avoid hyperbolic groups), for the implementation of a cryptosystem relying on CSP. Furthermore, these classes of groups offer additional properties that can be utilized in other algebraic PKC protocols.

5. The class of Artin groups of extra large type

Let $G\Gamma$ be a group with presentation

$$G\Gamma = \langle\, g_1, \dots, g_n \,;\, r(g_i, g_j) = 1 \;\; (\textit{for} \;\; 1 \leq i, j \leq n \;\; \textit{and} \;\; i \neq j) \,\rangle\,,$$

where $n \geq 2$ and $r(g_i, g_j) = 1$ is a relator involving two generators. Given $G\Gamma$ there is an associated labeled graph Γ and vice versa. The vertices of the graph Γ are labeled by the generators of $G\Gamma$. Any two vertices $g_i, g_j \in \Gamma$ are connected by an edge if there is a relation $r(g_i, g_j) \in G\Gamma$ between the corresponding generators; in other words, edges are labeled by relations.

Example 4. An *Artin group* $A\Gamma$ is a group with presentation

$$A\Gamma = \langle\, a_1, \dots, a_n \,;\, \mu_{ij} = \mu_{ji} \;\; \textit{for} \;\; 1 \leq i < j \leq n) \,\rangle\,, \quad \text{where} \;\; \mu_{ij} = \underbrace{a_i\, a_j\, a_i \dots}_{m_{ij}}$$

and $m_{ij} = m_{ji}$. Artin groups arise as generalizations of braid groups, see e.g. [2]. For an Artin group $A\Gamma$, the associated labeled graph Γ has no multiple edges or loops. The vertices a_i of Γ are the generators of the Artin group. Any two vertices $a_i, a_j \in \Gamma$ are connected by an edge, labeled with the integer m_{ij} , associated to the relation $\mu_{ij} = \mu_{ji}$ (between the corresponding generators $a_i, a_j \in A\Gamma$).

In general, automorphisms (or endomorphisms) of the graph Γ induce automorphisms (or endomorphisms) of the group $G\Gamma$. Therefore, the graph associated to $G\Gamma$ gives us a direct procedure for the construction of a semigroup $T \subseteq End\, G\Gamma$ that can contain a large pool of commuting elements. This is a necessary condition for common key extraction by legitimate parties in the application of the Commuting Action Key Exchange protocol (CAKE, Definition 3). To construct the corresponding semigroup T with sufficiently many endomorphisms, a graph Γ can be chosen to be a tree. The procedure implemented for the Ko-Lee protocol can then be utilized to provide for commuting endomorphisms, i.e., one splits the vertices of the graph into two disjoint sets such that each of the entities, Alice and Bob, select endomorphisms which act on their own set.

Example 5. The relations of the braid groups B_n involve two generators. The corresponding graph associated to B_n is just a simple path, and it has only one automorphism that induces the following automorphism of B_n: $\sigma_i \mapsto \sigma_{n-i}$, which happens to be an inner automorphism of B_n. For other $G\Gamma$ groups, however, their corresponding graphs are more complex, and it is easy to arrange for a large semigroup (or a group) $T \subseteq End\, G\Gamma$ of endomorphisms (or automorphisms).

Artin groups $A\Gamma$ with the property that all the integers $m_{ij} \geq 4$ are called *Artin groups of extra large type*. A tree Γ can be associated to an Artin group of extra large type, providing a direct procedure for constructing a semigroup $T \subseteq End\, A\Gamma$. Moreover, Artin groups of extra large type are automatic [17], thus the word problem for groups in this class can be solved in quadratic time, and by a result of [11], the word problem is solvable in linear time on average. Therefore, we can suggest the class of Artin groups of extra large type as platforms for CAKE.

5.1. **Key exchange protocol based on Artin groups.** In this section we present the class of Artin groups of extra large type as an implementable class for CAKE.

Key generation: Randomly select a finite rooted tree Γ with l levels such that the degree of the root is equal to 2, and the degrees of all other vertices are between 2 and an integer m, with the exception of the end vertices whose degrees are 1. Associate to the tree Γ an Artin group $A\Gamma$ of extra large type by labelling each vertex of Γ with a letter a_i and numbering an edge by a (random) $m_{ij} \geq 4$ if there are two corresponding vertices a_i and a_j incident to this edge.

Let a_k be the root of the tree and let $\Gamma_0 = \Gamma - a_k$ be the subgraph obtained by deleting the root a_k. The graph Γ_0 consists of two finite disjoint subtrees, say, Γ_A and Γ_B, that are spliced by the root a_k. The associated subgroups are $A\Gamma_A$ and $A\Gamma_B$.

The sets of graph endomorphisms of Γ_A and Γ_B induce the submonoid of endomorphisms $End\, A\Gamma_A \times End\, A\Gamma_B \subseteq End\, A\Gamma$ such that for any $\alpha \in End\, A\Gamma_A$ and

$\beta \in End\,A\Gamma_B$ both α and β commute: $\alpha\,\beta = \beta\,\alpha$. In order for both submonoids to act non-trivially on a public word $w \in A\Gamma$, the word must involve some generating elements $a_1, \ldots , a_p \in A\Gamma_A$ and some generating elements $b_1, \ldots , b_q \in A\Gamma_B$, i.e., $w = w(a_1, \ldots , a_p, b_1, \ldots , b_q)$.

CAKE for Artin groups of extra large type. Choose a random Artin group $A\Gamma$ of extra large type to be the platform S for the CAKE tuple $(S, T, f; \mathcal{H})$, and let $T = End\,A\Gamma_A \times End\,A\Gamma_B$. Define $\mathcal{H}$ to be the set $\{End\,A\Gamma_A, End\,A\Gamma_B\}$. The protocol is set for Alice and Bob.

Protocol:

1. The random group $A\Gamma$, a word $w = w(a_1, \ldots , a_p, b_1, \ldots , b_q) \in A\Gamma$ and a generating set for each element of $\mathcal{H}$ are made public.
2. Alice chooses a private word $\alpha \in End\,A\Gamma_A$ and transmits $f(w, \alpha) = w^{\,\alpha}$ to Bob.
3. Bob chooses a private word $\beta \in End\,A\Gamma_B$ and transmits $f(w, \beta) = w^{\,\beta}$ to Alice.
4. Alice computes $f(w^{\,\beta}, \alpha) = w^{\,\beta\,\alpha}$ and Bob computes $f(w^{\,\alpha}, \beta) = w^{\,\alpha\,\beta}$. Alice and Bob set
$$w^{\,\alpha\,\beta} = w^{\,\beta\,\alpha}$$
as their common secret key.

Remark. By introducing randomness in the selection of the group $A\Gamma$, we make the present approach dynamic. The class of Artin groups of extra large type seems to be less "algorithmically homogeneous" than, say, the class of braid groups. In general, algorithmic non-homogeneity can disrupt general algorithmic methods an opponent might obtain for the purpose of acquiring a private key. For example, a typical endomorphism (non-automorphism) for $A\Gamma$ would be merging two terminal children vertices of the same parent, "confusing" the length of the word w. As a result, the effect of such an endomorphism on the length of a generic element of the group is no longer predictable, placing length attacks in question.

6. A class of small cancellation groups

In this section, we follow Lyndon and Schupp [14]. For facts about small cancellation theory the reader is referred to this source for further reading. Let $F(X)$ be the free group with a basis $X = \{\, x_i \,|\, i \in I \,\}$, where I is an indexing set. Let $\epsilon_k \in \{\pm 1\}$, where $1 \le k \le n$. A word $w(x_1, \ldots , x_n) = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n}$ in $F(X)$, with all x_{i_k} not necessarily distinct, is a *reduced X-word* if $x_{i_k}^{\epsilon_k} \neq x_{i_{k+1}}^{-\,\epsilon_{k+1}}$, for $1 \le k \le n-1$. In addition, the word $w(x_1, \ldots , x_n)$ is *cyclically reduced* if it is a reduced X-word and $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\,\epsilon_n}$. A set R containing cyclically reduced words from $F(X)$ is *symmetrized* if it is closed under cyclic permutations and taking inverses.

Let G be a group with presentation $\langle X; R\rangle$. A non-empty word $u \in F(X)$ is called a *piece* if there are two distinct relators $r_1, r_2 \in R$ of G such that $r_1 = uv_1$ and $r_2 = uv_2$. The group G belongs to the class $C(p)$ if no element of R is a product of fewer than p pieces. Also, the group G belongs to the class $C'(\lambda)$ if for every $r \in R$ such that $r = uv$ and u is a piece, one has $|u| < \lambda|r|$.

In particular, if G belongs to the class $C'(\frac{1}{6})$, then Dehn's algorithm solves the word problem for G. Thus, if G is a finitely presented group from the class $C'(\frac{1}{6})$, then it is *hyperbolic.*

Example 6. Let $\langle\, x_1, x_2, x_3\,;\, x_1^2x_2x_3^2x_2^{-1} = 1,\, x_2^2x_3x_1^2x_3^{-1} = 1\,\rangle$ be a presentation of a group G. Now, $x_1^{\pm 2}$, $x_2^{\pm 1}$, $x_2^{\pm 2}$, $x_3^{\pm 1}$, $x_3^{\pm 2}$, $(x_2x_3)^{\pm 1}$ and $(x_2x_3^{-1})^{\pm 1}$ are the pieces of G, and every relator is a product of four of these pieces. Therefore, the group G is in the class of $C(4)$ groups. However, G is not in the class of $C'(\frac{1}{6})$; for $i = 1$, 2 and 3, the pieces $x_i^{\pm 1}$, satisfy the property $|x_i^{\pm 1}| = \frac{1}{6}|x_1x_2x_3x_4^2x_2^{-1}|$ and $|x_i^{\pm 1}| = \frac{1}{6}|x_2^2x_3x_1x_4x_3^{-1}|$.

The solution of the conjugacy problem (CP) is irrelevant for the implementation of a cryptographic protocol utilizing the computational difficulty of the conjugacy search problem (CSP). However, reasonable evidence of a potentially computationally hard CSP is provided if there is no known polynomial time algorithm for CP.

For a class of small cancellation groups possessing the property of "no known polynomial time algorithm for CP", we need one more condition. A group G with finite presentation $\langle X; R\rangle$ belongs to the class $T(q)$ for a natural number q if for any sequence $r_1, \ldots, r_n \in R$, with $3 \le n < q$ and $r_i \neq r_{i+1}^{-1}$, at least one of the products $r_1r_2, \ldots, r_{n-1}r_n$, r_nr_1 is cyclically reduced without cancellation.

A group G with presentation $\langle\, X \mid R\,\rangle$ is said to be a small cancellation group of type $C(p)$-$T(q)$ if it belongs to the classes $C(p)$ and $T(q)$. By Theorem V.6.3 of [14], the word problem is solvable in the class of small cancellation groups of type $C(4)$-$T(4)$. If hyperbolic groups $C'(\frac{1}{6})$ are avoided, then, generally, there is no known polynomial time algorithm for solving the conjugacy search problem for groups in this class (even though the conjugacy problem is solvable by [14, Theorem V.7.6]).

Thus, in this class, legitimate entities can choose a random group and implement an algebraic PKC protocol, e.g. CAKE, that relies on the hardness of the conjugacy search problem or a harder problem that can potentially arise (as we indicated in Sections 2 and 3).

Example 7. Consider the presentation $\langle\, x_1, x_2, x_3\,;\, x_1^2x_2x_3^2x_2^{-1},\, x_2^2x_3x_1^2x_3^{-1}\,\rangle$ for G, the group of Example 6. For any r_1, r_2 and r_3, no two of which are inverse of one another, from the symmetrized set $\{x_1^2x_2x_3^2x_2^{-1},\, x_2^2x_3x_1^2x_3^{-1}\}$, no cancellation is possible in at least one of the words r_1r_2, r_2r_3 and r_3r_1. Therefore, G belongs to the class of $T(4)$ and $C(4)$ groups, but not the class of $C'(\frac{1}{6})$ groups.

7. Diffusion

In this section, we offer a method that can, in our opinion, substantially enhance the "diffusion", i.e., the process of disguising an element of a given group by using defining relations. This method is not brand new, but it was used before in a different context, namely, in attempts to attack the Andrews-Curtis conjecture, a notoriously difficult problem in low-dimensional topology and combinatorial group theory (see e.g. [15]).

The idea is to break down defining relations of a group into "small pieces". More formally, we replace a given group G by an isomorphic group where all relators have length at most 3. Intuitively, diffusion should be easier to achieve in groups with shorter defining relations, so we hope that our idea is useful.

The procedure itself is quite simple. Let G have a presentation $\langle x_1, ..., x_n; r_1, ..., r_k\rangle$ in terms of generators $x_1, ..., x_n$ and defining relations $r_1, ..., r_k$. We are going to obtain a different presentation for G by using *Tietze transformations* (see e.g. [14]); these are elementary isomorphism-preserving operations on presentations of groups.

Specifically, let, say, $r_1 = x_i x_j u$, $1 \le i, j \le n$. We introduce a new generator x_{n+1} and a new relator $r_{k+1} = x_{n+1}^{-1} x_i x_j$. The group with the presentation $\langle x_1, ..., x_n, x_{n+1}; r_1, ..., r_k, r_{k+1}\rangle$ is obviously isomorphic to G. Now if we replace r_1 with $r_1' = x_{n+1}u$, then the presentation $\langle x_1, ..., x_n, x_{n+1}; r_1', ..., r_k, r_{k+1}\rangle$ will again define a group isomorphic to G, but now the length of one of the defining relations (r_1) has decreased by 1. Continuing in this manner, we can eventually obtain a presentation where all relators have length at most 3, at the expense of introducing more generators.

Apparently, relators of length at most 3 can provide a very good diffusion, but the natural question now is: why cannot the opponent convert the new presentation back to the original one and take it from there? This, indeed, may work with some of the protocols, but let us have a look at the situation where applying an endomorphism of a group to an element is involved.

Suppose a group G' is isomorphic to a group G in the way described above. Let $w' \in G'$, and let φ be an endomorphism of G' applied to w'. The opponent can convert w' and $\varphi(w')$ to elements w and u, respectively, of the group G, by using relations of the form $x_s = x_{i_1}^{\pm 1} x_{i_2}^{\pm 1}$, where x_s are "new" generators and x_{i_1}, x_{i_2} are "old" generators. Then the opponent may try to find an endomorphism ψ of G such that $u = \psi(w)$ as follows.

Suppose we know that φ takes generators x_i' of the group G' to some y_i'. An obvious way to "lift" φ to an endomorphism of G would be to convert y_i' to $y_i \in G$ (again, by using relations of the form $x_s = x_{i_1}^{\pm 1} x_{i_2}^{\pm 1}$), then let ψ be the mapping of G that takes x_i to y_i.

This however may not work (and typically will not work) because the endomorphism φ, restricted to the "old" generators (i.e., to the generators of G) may not respect the original relations of the group G. We can therefore have an element $u \in G$ such that $\psi(w) = u$ in the group G, but $\varphi(w') \neq u$ in the group G'.

The only way to properly "lift" φ to an endomorphism of G would be to combine it with an isomorphism $f : G' \to G$, but the latter is by no means easy to explicitly compute, even if the whole chain of Tietze transformations is known to the opponent, which does not have to be the case. Incidentally, neither has the original group G to be known to the public.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), 287–291.

[2] K. Appel and P. Schupp, *Artin groups and infinite Coxeter groups,* Invent. Math. **72** (1983), 201–220.

[3] Cryptography and braid groups,
http://www.tcs.hut.fi/~helger/crypto/link/public/braid/

[4] P. Dehornoy, *Braid-based cryptography*, Contemp. Math., Amer. Math. Soc. **360** (2004).

[5] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, *Length-based conjugacy search in the braid group*, preprint
http://arXiv.org/abs/math.GR/0209267

[6] P. Garrett, *Making, breaking codes: an introduction to cryptology*, Prentice Hall, 2001.

[7] D. Hofheinz and R. Steinwandt, *A practical attack on some braid group based cryptographic primitives*, in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2003 Proceedings, Y.G. Desmedt, ed., Lecture Notes in Computer Science **2567**, pp. 187–198, Springer, 2002.

[8] J. M. Howie, *Fundamentals of Semigroup Theory*, London Mathematical Society Monographs, Vol. 12. Clarendon Press, 1995.

[9] J. Hughes and A. Tannenbaum, *Length-based attacks for certain group based encryption rewriting systems*, Workshop SECI02 Securitè de la Communication sur Intenet, September 2002, Tunis, Tunisia.
http://www.network.com/~hughes/

[10] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

[11] I. Kapovich, A. G. Myasnikov, P. Schupp, and V. Shpilrain, *Average-case complexity and decision problems in group theory*, Adv. Math., to appear.
http://xxx.lanl.gov/abs/math.GR/0206273

[12] K. H. Ko, *Conjugacy problem in braid groups and applications, I. Overview: Conjugacy problems, their variations, and their applications*, preprint.
http://kyokan.ms.u-tokyo.ac.jp/~topology/files/KS03a.pdf

[13] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 166–183, Lecture Notes in Comput. Sci. **1880**, Springer, Berlin, 2000.

[14] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Ergebnisse der Mathematik, band 89, Springer 1977. Reprinted in the Springer Classics in Mathematics series, 2000.

[15] A. D. Myasnikov, A. G. Myasnikov, V. Shpilrain, *On the Andrews-Curtis equivalence*, Contemp. Math., Amer. Math. Soc. **296** (2002), 183–198.

[16] A. G. Myasnikov and A. Ushakov, *Random van Kampen diagrams*, preprint.

[17] D. Peifer, *Artin groups of extra-large type are automatic*, J. Pure Appl. Alg. **110** (1996), 15–56.

[18] V. Shpilrain, *Assessing security of some group based cryptosystems*, Contemp. Math., Amer. Math. Soc. **360** (2004), 167–177.

Department of Mathematics, The City College of New York, New York, NY 10031

e-mail addresses: shpil@groups.sci.ccny.cuny.edu, nyzapata@verizon.net

http://www.sci.ccny.cuny.edu/~shpil/