ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Applied Mathematics 130 (2003) 3–12

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

Non-abelian key agreement protocols

Iris Anshel[a], Michael Anshel[b], Dorian Goldfeld[c]

[a] *Arithmetica Inc., 31 Peter Lynas Ct, Tenafly, NJ 07670, USA*

[b] *Department of Computer Science, City College of New York, New York, NY 10031, USA*

[c] *Department of Mathematics, Columbia University, New York, NY 10027, USA*

Received 13 February 2001; received in revised form 21 November 2001; accepted 7 May 2002

Abstract

A key-agreement protocol (KAP) is a multi-party algorithm defined by a sequence of steps specifying the actions required for two or more individuals to each obtain a shared secret. A brief introduction to an axiomatic basis for non-abelian KAPs is presented. The security of these protocols is related to the difficulty of solving equations in non-linear algebraic structures. In particular, it is shown that well known hard problems in group theory can be used to generate key agreement protocols. Concrete examples of such KAPs are discussed and the axiomatic method is shown to subsume other braid group KAPs. The paper concludes with a snapshot of methods and examples currently under investigation.

Keywords: Public-key cryptography; Key-agreement protocol; Braid group; Conjugacy problem

1. Axiomatics for non-abelian key agreement protocols

A protocol is a multi-party algorithm, defined by a sequence of steps, specifying the actions required of two or more individuals in order to achieve a specified objective. A key-agreement protocol (KAP) is a protocol whereby a shared secret becomes available to two or more individuals for further cryptographic applications. A new class of non-abelian key agreement protocols was introduced in [2,3] and further developed in [4]. The security of these protocols is based on the difficulty of solving systems of equations over algebraic structures, in particular groups, a well known class of hard problems. Solutions of equations over algebraic structures are generally thought to be very hard and in some cases even provably unsolvable. We review the non-abelian key agreement protocols and later discuss some specific examples.

0166-218X/03/$ - see front matter
PII: S0166-218X(02)00585-1

Consider the 5-tuple:

$$(\mathbf{U}, \mathbf{V}, \beta, \gamma_1, \gamma_2),$$

where $\mathbf{U}$ and $\mathbf{V}$ are feasibly computable monoids, and

$$\beta : \mathbf{U} \times \mathbf{U} \to \mathbf{V},$$

$$\gamma_i : \mathbf{U} \times \mathbf{V} \to \mathbf{V} \quad (i = 1, 2)$$

satisfy the following axioms:

Axiom (i): For all $x, y_1, y_2 \in \mathbf{U}$

$$\beta(x, y_1 \cdot y_2) = \beta(x, y_1) \cdot \beta(x, y_2).$$

Axiom (ii): For all $x, y \in \mathbf{U}$

$$\gamma_1(x, \beta(y, x)) = \gamma_2(y, \beta(x, y)).$$

Axiom (iii): Assume $y_1, y_2, \ldots, y_k \in \mathbf{U}$,

$$\beta(x, y_1), \beta(x, y_2), \ldots, \beta(x, y_k)$$

are publicly known for some secret element $x \in \mathbf{U}$. Then, in general, determining x is not feasible.

We now describe the protocol as a sequence of steps. Alice and Bob are each assigned public submonoids,

$$S_A, S_B \subseteq U,$$

respectively.

Suppose S_A is generated by the elements

$$\{s_1, \ldots, s_m\}$$

and S_B is generated by

$$\{t_1, \ldots, t_n\}.$$

Alice begins by secretly choosing an element $a \in S_A$ and publicly announces the list:

$$\beta(a, t_1), \beta(a, t_2), \ldots, \beta(a, t_n).$$

Likewise, Bob secretly chooses an element $b \in S_B$ and publicly announces the list:

$$\beta(b, s_1), \beta(b, s_2), \ldots, \beta(b, s_m).$$

Alice, knowing a as an element in S_A,

$$a = \prod_i s_i^{e(i)} \quad (e(i) \text{ are secret})$$

can compute

$$\beta(b,a) = \prod_i \beta(b,s_i)^{e(i)}.$$

Bob, knowing b as an element in S_B,

$$b = \prod_i t_i^{f(i)} \quad (f(i) \text{ are secret})$$

can compute

$$\beta(a,b) = \prod_i \beta(a,t_i)^{f(i)}.$$

At this point Alice knows a and $\beta(b,a)$. Likewise, Bob knows b and $\beta(a,b)$.

They can now both compute the *shared secret* κ where

$$\kappa = \gamma_1(a,\beta(b,a))$$
$$= \gamma_2(b,\beta(a,b)).$$

We now compare the well-known Diffie–Hellman key agreement protocol and the new non-abelian key agreement protocol.

Diffie–Hellman KAP

Public information:

u,
$\mathscr{C} = large\ class\ of\ commuting\ one\text{-}way\ functions.$

Alice's:

Secret key: $f \in \mathscr{C}$
Public key: $f(u)$

Bob's:

Secret key: $g \in \mathscr{C}$
Public key: $g(u)$

Shared secret: $f(g(u))$.

Non-abelian KAP

Public information:

$U, V, \beta, \gamma_1, \gamma_2, \quad S_A, S_B$ satisfying axioms (i)–(iii).

Alice's:

Secret key: $a \in S_A$
Public key: $\beta(a, t_i)$

Bob's:

Secret key: $b \in S_b$
Public key: $\beta(b, s_j)$

Shared secret: $\gamma_1(a, \beta(b, a))$.

2. Intractable problems in combinatorial group theory

Informally, a finitely presented group $\mathbf{G}$ is specified by a finite set of generators

$$g_1, g_2, \ldots, g_n,$$

where every $g \in \mathbf{G}$ is a word in the generators and their inverses (product of g_i's and their inverses). Further, there are finitely many words

$$r_1, r_2, \ldots, r_m$$

called relators and each r_i defines the identity element of $\mathbf{G}$.

It is usual to suppress the trivial relations such as

$$g_i g_i^{-1} = g_i^{-1} g_i = e.$$

A presentation is written as $\{g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m\}$.

Examples. The *finite cyclic group* of order n has presentation: $\{g \mid g^n\}$. The *modular group* on two generators:

$$\{g_1, g_2 \mid g_1^2, g_2^3\}.$$

The study of equations in finitely presented groups took on significance with the work of Max Dehn (1910–1912) [6] who formulated several now well-known problems.

Fix a presentation

$$\mathbf{G} = \{g_1, \ldots, g_n \mid r_1, \ldots, r_m\}.$$

Word problem. *Is there an algorithm to determine if an arbitrary word in* $\mathbf{G}$ *defines the identity element*?

Conjugacy problem. *Is there an algorithm to determine if two arbitrary words* $v, w \in \mathbf{G}$ *define conjugate elements, i.e. to determine if there exists* $x \in \mathbf{G}$ *such that*

$$w = x^{-1} v x.$$

The following important progress has been made on these conjectures. In 1955 Novikov and Boone [6] constructed finitely presented groups whose word problem is algorithmically unsolvable. In 1971 Miller III [7] constructed a finitely presented residually finite group (this means $g_1 \neq g_2$ can be distinguished in some finite image) with an algorithmically unsolvable conjugacy problem. Note that residually finite groups have a solvable word problem.

3. Concrete examples of non-abelian key agreement protocols

We now present concrete examples of the above general non-abelian protocol (based on the theory of infinite non-abelian groups) for secret key establishment between two parties whose only means of communication is a public channel. The security of the method is founded on the difficulty of solving the conjugacy problem in infinite non-abelian groups.

Recall that the general non-abelian KAP (key agreement protocol) was based on the existence of a 5-tuple

$$U, V, \beta, \gamma_1, \gamma_2$$

satisfying axioms (i)–(iii). We now present two examples of this KAP in the case that $U = V = G$ where G is an infinite finitely presented non-abelian group.

We now choose

$$U = V = G = \text{group},$$

$$\beta(x, y) = x^{-1} y x,$$

$$\gamma_1(u, v) = u^{-1} v, \quad \gamma_2(u, v) = v^{-1} u.$$

Non-abelian KAP I

Public information:

G = finitely generated non-abelian group.

Two subgroups of G:

$$S_A = \langle s_1, s_2, \ldots, s_m \rangle,$$

$$S_B = \langle t_1, t_2, \ldots, t_n \rangle.$$

Secret keys:

Alice's secret key $a \in S_A$,
Bob's secret key $b \in S_B$.

Public keys:

Alice's public key

$$a^{-1}t_1a, a^{-1}t_2a, \ldots, a^{-1}t_na,$$

Bob's public key

$$b^{-1}s_1b, b^{-1}s_2b, \ldots, b^{-1}s_mb.$$

Shared secret:

$$a^{-1}b^{-1}ab.$$

Security of the method:

The Simultaneous Conjugacy Problem.

Non-abelian KAP II

Let G denote a non-abelian group with an intractable conjugacy problem. Assume G contains two commuting subgroups

$$S_A = \langle s_1, s_2, \ldots, s_m \rangle,$$

$$T_B = \langle t_1, t_2, \ldots, t_n \rangle$$

i.e., for all $h \in S_A$ and $k \in T_B$

$$hk = kh.$$

Public information:

$p \in G$ = finitely generated non-abelian group.

Two commuting subgroups of G:

$$S_A = \langle s_1, s_2, \ldots, s_m \rangle,$$

$$S_B = \langle t_1, t_2, \ldots, t_n \rangle.$$

Secret keys:

Alice's secret key $a \in S_A$,
Bob's secret key $b \in S_B$.

Public key:

Alice's public key

$$a^{-1}pa,$$

Bob's public key

$$b^{-1}pb.$$

Shared secret:

$$a^{-1}b^{-1}pab.$$

Security of the method:

Conjugacy Problem.

The above method in the special case of the braid group, was first presented by Ko et al. [5]. We will now show that this scheme is, in fact, a special case of the general non-abelian KAP for a suitable choice of the 5-tuple: $(\mathbf{U}, \mathbf{V}, \beta, \gamma_1, \gamma_2)$ satisfying the axioms (i)–(iii).

Let S be a set which contains an element e. We can make S into a monoid by defining a law of composition $\circ$ as follows:

$$e \circ x = x \circ e = x \quad (\text{for all } x \in S),$$

$$x \circ y = x \quad (\text{for all } x, y \in S,\ x \neq e, y \neq e).$$

Choose U to be the braid group B_N. Fix a public element $p \in B_N$. Define V (first as a set) to be the set of conjugates

$$V = \{xpx^{-1} \mid x \in B_N\}.$$

Then V is a monoid with identity p and law of composition $\circ$ as defined above. We now define $\beta, \gamma_1, \gamma_2$.

Definition. We define

$$\beta(x, y) = xpx^{-1} \in V$$

for all $x, y \in B_N$.

Clearly, β satisfies axiom (i). We now let $C(p)$ denote the centralizer of p in B_N. Let $x_1, x_2, \ldots, x_{N-1}$ denote the Artin generators for B_N, and for some $1 < \ell < N-1$ define subgroups A, B, where A is generated by $x_1, \ldots, x_{\ell-1}$ and B is generated by $x_{\ell+1}, \ldots, x_{N-1}$.

Definition. We define

$$\gamma_1(u, v) = \begin{cases} p & \text{if } u \notin A \cdot C(p), \\ p & \text{if } u \in A \cdot C(p) \text{ and } v \neq bpb^{-1} \text{ for all } b \in B, \\ ava^{-1} & \text{otherwise (where } u \in a \cdot C(p)). \end{cases}$$

One checks that this definition is well defined and independent of the choice of a. Similarly,

Definition. We define

$$\gamma_2(u,v) = \begin{cases} p & \text{if } u \notin B \cdot C(p), \\ p & \text{if } u \in B \cdot C(p) \text{ and } v \neq apa^{-1} \text{ for all } a \in A, \\ bvb^{-1} & \text{otherwise (where } u \in b \cdot C(p)). \end{cases}$$

One easily checks that axiom (ii) is satisfied. With these choices one obtains precisely the public-key scheme introduced in [5]. This demonstrates that the public key scheme introduced in [5] is a special case of the general algebraic protocol given in [2,3].

4. Requirements for a group theory KAP

The minimum requirements for a group theory KAP based on an infinite non-abelian group G are:

- A fast method is required to rewrite a set of conjugates in G:

  $$a^{-1}t_1a, a^{-1}t_2a, \ldots, a^{-1}t_ma$$

  so they become unrecognizable.
- A key extractor is required.

A key extractor E is determined by a set K (Keyspace) and is a map

$$E : G \to K$$

from the group G to K, such that each element $g \in G$ (regardless of the way it is expressed in the generators of G) is mapped to a unique key $E(g)$. In order to insure that the process of key extraction should eventually give a bitstring which is distributed close to uniformly, it is necessary, in practice, to apply a hash function to the internal bit representation of one of the invariants. We shall simply assume that this is incorporated in E and not discuss it further.

4.1. Rewriting methods

There are two basic methods for rewriting. The first method is the canonical form method. This method requires the existence of a canonical form on the group G.

Examples of groups with canonical forms include:

- Fundamental groups of graphs of groups (via Bass–Serre theory, see [8]).
- One relator groups (via the Magnus approach see [6]).
- Classes of two relator groups (see [1]).

- Groups which come from low dimensional topology (via Thurston's work on three manifolds (see [9]).

The second method for rewriting is the subgroup method. This method requires the existence of a subgroup

$$H \leqslant G,$$

where a method of rewriting (i.e., a method to make words in H unrecognizable) is already known in the subgroup H. For example, the subgroup could have a canonical form.

Now, every $g \in G$ can be written in the form

$$g = \sigma(g) \cdot \bar{g},$$

where $\sigma(g)$ is a word in H (i.e., it is expressed in the generators of H) and $\bar{g} \in G$ is a coset representative.

Method. Rewrite $\sigma(g)$ and then express $\sigma(g)$ as a word in the generators of G.

Remark. If one subgroup H with rewriting method exists, then one usually has a family of such subgroups given by the orbit of the action of the automorphism group of G acting on H. Since the choice of H is entirely private, an attacker cannot use properties of H to try to break the system. Since the result of this method is a word in the generators of the group G, this process can be iterated several times, using various subgroups where one has methods of rewriting, to strengthen the system.

Examples of groups where this subgroup rewriting is a natural choice arise from the theory of extensions of groups, i.e., groups with non-trivial higher cohomology groups.

4.2. Key extraction methods

- Canonical forms.
- In the case of the Braid group, knot polynomials.
- Applying a homomorphism to a very large finite group.
- Computing an invariant in an image group.

Examples of group invariants include:

- The Nielsen invariant of groups with infinite cyclic abelianizations.
- The relation module and its applications.
- The nilpotent quotients of classes of solvable groups and Burnside groups.
- Low-dimensional homology and cohomology.

Acknowledgements

The authors wish to thank Arithmetica Inc. for its support of this research.

References

[1] I. Anshel, An introduction to a class of two relator groups, in: C.M. Campbell, E.F. Robertson (Eds.), Groups St. Andrews 1989, Vol. 1, London Mathematical Society, Lecture Note Series, Vol. 159, Cambridge University, Cambridge, 1991, pp. 14–29.
[2] I. Anshel, M. Anshel, D. Goldfeld, A method and apparatus for cryptographically secure algebraic key establishment protocols, International Patent Application Number: WO 99/44324. U.S. patent allowed.
[3] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, Math. Research Lett. 6 (1999) 287–291.
[4] I. Anshel, M. Anshel, B. Fisher, D. Goldfeld, in: D. Naccacne (Ed.), New Key Agreement Protocols in Braid Group Cryptography, CT-RSA 2001, Lecture Notes in Computer Science, Vol. 2020, Springer, Berlin, 2001, pp. 13–27.
[5] K.H. Ko, S.J. Lee, J.H. Chean, J.W. Han, J.S. Kang, C. Park, New public-key cryptosystem using braid groups, in: M. Bellare (Ed.), Advances in Cryptology-Crypto 2000, Lecture Notes in Computer Science, Vol. 1880, Springer, Berlin, 2000, pp. 166–183.
[6] W. Magnus, A. Karrass, D. Solitar, Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Defining Relators, 2nd Revised Edition, Dover, New York, 1976.
[7] C.F. Miller, On Group-Theoretic Decision Problems and their Classification, in: Annals of Mathematics Studies, Vol. 68, Princeton University, Princeton, NJ, 1971.
[8] J.P. Serre, Trees, Springer, Berlin, 1980.
[9] W.P. Thurston, Three-dimensional Geometry and Topology, Vol. 1, Princeton University, Princeton, NJ, 1997.