

# New Developments in Commutator Key Exchange

Robert Gilman, Alex D. Miasnikov, Alexei G.  
Myasnikov and Alexander Ushakov

**Abstract.** We study the algorithmic security of the Anshel-Anshel-Goldfeld (AAG) key exchange scheme and show that contrary to prevalent opinion, the computational hardness of AAG depends on the structure of the chosen subgroups, rather than on the conjugacy problem of the ambient braid group. Proper choice of these subgroups produces a key exchange scheme which is resistant to all known attacks on AAG.

## 1. Introduction

Modern braid group cryptography begins with the public key exchange schemes introduced by Anshel, Anshel, and Goldfeld [1] and by Ko, Lee, Cheon, Han, Kang, and Park in [12]. Both schemes use  $B_n$ , the braid group on  $n$  strands, as their platform. Cryptanalysis of these schemes motivated investigation of the algorithmic complexity of the conjugacy problem in braid groups (written CP for short) [2, 3, 4, 7, 8, 13]. CP is known to be solvable in exponential time, but whether or not it is solvable in polynomial time is unknown. However, known algorithms work well in practice and solve most instances of CP in polynomial time [7]. Simple modifications of these algorithms solve the related problems CSP [18] and SCSP [14] in polynomial time on a generic set of inputs. In CSP, the conjugacy search problem, the task is to find a conjugating element, knowing that one exists, while in SCSP, the simultaneous conjugacy search problem one is required to find a solution to a system of conjugacy equations.

The fact that CP, CSP and SCSP are easily solved in practice seems to undermine the basic algorithmic security assumptions of the AAG protocol, and this conclusion has been strengthened by several subsequent attacks. However, in [17] it was argued that AAG could be improved by a better choice of the subgroups which appear as parameters in the protocol. We show here how to make such a choice. We obtain thereby a new variation of the commutator key

exchange which, we believe, foils all known attacks on AAG. To avoid confusion we refer to the new scheme as CKE (for commutator key exchange.)

## 2. Reduction of AAG

It is known that AAG, viewed as an algorithmic problem, is reducible in linear time to SCSP\*, which is yet another variation of CP (see [19, 21]). SCSP\* is like SCSP except that the conjugating element is required to lie in a fixed finitely generated subgroup  $A$  of the platform group,  $G$ . We refer to SCSP\* as SCSP with subgroup constraints.

We claim that CP, CSP and SCSP are not directly relevant to AAG. Indeed, all known attacks on AAG (or CKE for that matter) can be divided into two types. Attacks of the first type try to solve two instances of SCSP\* in  $G$  by employing the public information

$$a_1^x = \bar{a}_1, \dots, a_m^x = \bar{a}_m, \quad b_1^y = \bar{b}_1, \dots, b_n^y = \bar{b}_n. \quad (1)$$

to search for the private keys  $x$  (Alice's) and  $y$  (Bob's) in the subgroups  $A$  and  $B$ , generated in  $G$  by the elements  $t_A = (a_1, \dots, a_m)$  and  $t_B = (b_1, \dots, b_n)$ . This method includes the most powerful length-based and quotient attacks (see [11, 6, 18, 20, 19]). It should be noticed that in these cases the solutions  $x$  and  $y$  are sought as words in the generators of  $A$  and  $B$ , respectively.

Attacks of the second type seem to rely only on solutions of SCSP (1) without the constraints  $x \in B, y \in A$ . The most effective among them are

- 1) *Summit Set Attack* [14]. It starts by reducing the conjugates  $t_A, \bar{t}_A$  and  $t_B, \bar{t}_B$  of (1) to the minimal possible level with respect to their canonical length (called the summit set) and then performs the exhaustive search at that level.
- 2) *Hofheinz-Stainwandt Attack* [10] has the same first step as in the summit set attack but then uses heuristics to get a solution at the minimal level.
- 3) *Linear Attack* uses known presentations of braids by matrices (e.g., Burau or Kramer presentations (see [9]) , it produces first a solution of (1) in a matrix form and then lifts it into braids.

These methods are effective because quite often the solutions  $x = b, y = a$  of SCSP (1) either satisfy the SCSP\* constraints  $b \in B, a \in A$  or give the required commutator  $[a, b]$  (the shared private key of AAG). To understand this phenomenon, recall that all other solutions  $x = b', y = a'$  of (1) are of the form  $b' = db, a' = ca$ , where  $c \in C(B), d \in C(A)$ . If  $C(A) = C(B) = Z(G)$  where  $Z(G)$  is the center of  $G$  then  $[a', b'] = [a, b]$ . In particular, if the tuples  $t_A$  and  $t_B$  are chosen randomly (i.e., they components are randomly chosen words in the generators of  $G$ ), as is the case in AAG protocol, then, indeed,  $C(A) = C(B) = Z(G)$ , explaining effectiveness of these attacks.

More generally, one can employ the Narrow Centralizer Attack to reduce SCSP\* to SCSP. A centralizer  $C$  in  $G$  is *narrow* if it has, as a group, polynomial

growth, i.e.,  $C$  is generated by a finite set  $Y$  and the number of elements of length at most  $n$  (as words in the generators  $Y$ ) in  $C$  is bounded by  $p(n)$  for some fixed polynomial  $p$ . In the case when the centralizers  $C(A)$  and  $C(B)$  are narrow Eve can enumerate all possible elements in  $C(A)$  and in  $C(B)$  up to the lengths of the private keys of Alice and Bob, solve SCSP for (1) and get two lists of elements of polynomial sizes containing the private keys of Alice and Bob, which is a breach of security.

### 3. Hard Keys

The crucial mathematical fact that distinguishes SCSP\* from CSP, or SCSP is that the decision version SCP\* of SCSP\* (where one has to decide if a conjugating element exists in the fixed subgroup  $A$ ) is *undecidable* in  $B_n, n \geq 6$ . In contrast CP and SCP are decidable.

**Theorem.** There exists a finitely generated subgroup  $S$  of  $B_6$  such that the simultaneous conjugacy problem  $a_1^x = \bar{a}_1, \dots, a_m^x = \bar{a}_m$  in  $B_6$  (where the  $a_i$ 's and  $\bar{a}_i$ 's run over  $B_6$ ) with the subgroup constraint  $x \in S$  is undecidable.

It immediately follows from Theorem that there does not exist any recursive upper bound on the time complexity of SCSP\* in  $B_n, n \geq 6$ . In particular, any polynomial time algorithm for solving SCSP\* in  $B_n, n \geq 6$  is only partial, and hence fails on infinitely many inputs. This dramatically changes the whole security picture for commutator key exchange primitives, because we know now that hard keys exist with respect to properly chosen subgroups. Recall, that even in the RSA key exchange it is not known that hard keys exist, since it is not known whether the integer factorization problem is solvable in polynomial time or not.

In addition in the CKE case, the non-existence of recursive upper bounds for SCSP\* implies that, unlike RSA, there does not exist a polynomial time quantum algorithm to solve SCSP\* in  $B_n, n \geq 6$ .

Of course, the complexity arguments above concern only the worst-case complexity of the problems. The real issue is on how one can generate these hard instances of SCSP\* in  $B_n$  to be able to produce hard keys for CKE. The main mathematical idea is to reduce the Membership Problem (MP) in a given group  $G$  (which requires one to verify if a given element of  $G$  belongs to a fixed finitely generated subgroup of  $G$ ) to the decision version SCP\* of SCSP\* in  $G$ , thus making sure that SCP\* is as hard in  $G$  as MP. We were able to do this in  $B_n, n \geq 6$ , making use of the famous Mikhailova construction [15], which shows how one can construct finitely generated subgroups of the direct product  $F \times F$  of two non-abelian free groups  $F$ , hence in  $B_n, n \geq 6$ , with undecidable MP. In our talk we present a particular way to generate hard keys. A detailed description of key generation is rather technical, it requires a certain knowledge of modern group theory and familiarity with the known attacks on AAG. We cannot describe all the details of key generation in a short abstract; we leave a complete description for a longer

publication. The mathematical foundations of our approach were outlined in the paper [19], where authors gave a rigorous analysis of various length-based attacks, by far the most successful attacks on AAG scheme.

Our computer experiments indicate that the most effective attacks on AAG do fail to break CKE. The current hard keys are perhaps too long to be really practical: the average total length of the generating tuples  $t_A$  and  $t_B$  of the subgroups  $A$  and  $B$  is 4477, of the conjugates of the tuples  $t_A$  and  $t_B$  is 52113, and of the shared private key is 7347. However, they do demonstrate the feasibility of the method.

## References

- [1] I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. 6 (1999) 287–291.
- [2] J. Birman; V. Gebhardt, J. Gonzalez-Meneses, *Conjugacy in Garside groups I: Cyclings, powers, and rigidity*, Groups Geom. Dyn. 1 (2007), 221–279. (<http://arxiv.org/abs/math/0605230>.)
- [3] ———, *Conjugacy in Garside groups II: Structure of the ultra summit set*, Groups Geom. Dyn., to appear. (<http://arxiv.org/abs/math/0606652>.)
- [4] ———, *Conjugacy in Garside groups III: Periodic braids*, J. Algebra 316 (2007), 746–776.
- [5] D. Garbera, S. Kaplanc, M. Teicherc, B. Tsaband, U. Vishne. *Probabilistic solutions of equations in the braid group*, Advances in Applied Mathematics 35 (2005) 323-334.
- [6] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, *Length-based conjugacy search in the Braid group*, <http://arxiv.org/abs/math.GR/0209267>.
- [7] V. Gebhardt, *A New approach to the conjugacy problem in Garside groups*, J. Algebra 292 (2005), 282–302.
- [8] V. Gebhardt, *Conjugacy search in braid groups from a braid-based cryptography point of view*, Appl. Algebra Eng. Comm. 17 (2006) 219–238.
- [9] J. Hughes, *A linear algebraic attack on the AAFG1 braid broup cryptosystem*, ACISP 2002.
- [10] D. Hofheinz, R. Steinwandt, *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., LNCS 2567, Springer Verlag, (2002) 187-198.
- [11] Hughes, J., Tannenbaum, A., *Length-based attacks for certain group based encryption rewriting systems*, in Workshop SECI02 Sécurité de la Communication sur Intenet, September 2002, Tunis, Tunisia. <http://www.network.com/~hughes/>
- [12] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, in Advances in Cryptology – CRYPTO 2000 (Santa Barbara, CA), LNCS 1880) Springer Verlag (2000) 166–183.

- [13] S. J. Lee, *Algorithmic solutions to decision problems in the braid group*, Ph.D. thesis, KAIST, 2000.
- [14] S. J. Lee, E. Lee, *Potential weaknesses of the commutator key agreement protocol based on braid groups*, in *Advances in Cryptology – Eurocrypt 2002*, LNCS 2332, Springer Verlag (2002) 14–28.
- [15] K. A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR 119 (1958) 1103–1105.
- [16] A. G. Myasnikov, V. Shpilrain, A. Ushakov. *A practical attack on some braid group based cryptographic protocols*, in *CRYPTO 2005*, LNCS 3621, Springer Verlag, (2005), 86-96.
- [17] ———, *Random subgroups of braid groups: an approach to cryptanalysis of a braid group based cryptographic protocol*, in *PKC 2006*, LNCS 3958, Springer Verlag, (2006), 302-314.
- [18] A. D. Myasnikov and A. Ushakov, *Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol*, in *Advances in Cryptology – PKC 2007*, LNCS 4450, Springer Verlag (2007) 76–88.
- [19] ———, *Random subgroups and analysis of the length-based and quotient attacks*, *Journal of Mathematical Cryptology*, to appear.
- [20] D. Ruinsky, A. Shamir, and B. Tsaban, *Cryptanalysis of group-based key agreement protocols using subgroup distance functions*, in *Advances in Cryptology – PKC 2007*, LNCS 4450, Springer Verlag (2007) 61–75.
- [21] V. Shpilrain and A. Ushakov, *The conjugacy search problem in public key cryptography: unnecessary and insufficient*, *Applicable Algebra in Engineering, Communication and Computing*, to appear, <http://eprint.iacr.org/2004/321/>

Robert Gilman  
Stevens Institute of Technology,  
Hoboken NJ 07030-5991,  
USA  
e-mail: [Robert.Gilman@stevens.edu](mailto:Robert.Gilman@stevens.edu)

Alex D. Miasnikov  
Stevens Institute of Technology,  
Hoboken NJ 07030-5991,  
USA  
e-mail: [amyasnik@stevens.edu](mailto:amyasnik@stevens.edu)

Alexei G. Myasnikov  
Stevens Institute of Technology,  
Hoboken NJ 07030-5991,  
USA  
e-mail: [amiasnikov@gmail.com](mailto:amiasnikov@gmail.com)

Alexander Ushakov  
Stevens Institute of Technology,  
Hoboken NJ 07030-5991,  
USA  
e-mail: [aushakov@stevens.edu](mailto:aushakov@stevens.edu)