ON AN AUTHENTICATION SCHEME BASED ON THE ROOT PROBLEM IN THE BRAID GROUP

BOAZ TSABAN

Abstract. Lal and Chaturvedi proposed two authentication schemes based on the difficulty of the Root Problem in the braid group. We point out that the first scheme is not really as secure as the Root Problem, and describe an efficient way to crack it. The attack works for any group.

1. The first authentication scheme

The basic definitions are given in [2]. We only describe the scheme itself. We work in the braid group B_n where n is even. Let $LB_n = \langle \sigma_1, \dots, \sigma_{n/2-1} \rangle$ and $UB_n = \langle \sigma_{n/2+1}, \dots, \sigma_n \rangle$. In the sequel, multiplication of elements of B_n means concatenation and reduction to left canonical form.

Key Generation. Alice chooses integers $r, s \geq 2$, $a \in LB_n$, and $b \in UB_n$. The public key is $(X = a^r b^s, r, s)$, and the secret key is (a, b).

Authentication. Bob chooses $c \in UB_n$ and $d \in LB_n$, and sends Alice the challenge $Y = c^r d^s$. Alice responds with $Z = a^r Y b^s$. Bob verifies that $Z = c^r X d^s$.

Lal and Chaturvedi argue that the scheme is secure if the Root Problem of finding x given x^e ($e \geq 2$ fixed) in B_n is difficult [2].

2. Cryptanalysis of the scheme

The scheme has nothing to do with the Root Problem.

Claim 1. *If one can, given xy where $x \in LB_n$, and $y \in UB_n$, find (x, y), then one can authenticate as Alice.*

Proof. Take $x = a^r$ and $y = b^s$. Then xy is known. Find $(x, y) = (a^r, b^s)$, and note that this suffices for the authentication. □

Claim 1 together with the following proposition implies that the scheme is insecure.

Proposition 2. *Given xy where $x \in LB_n$, and $y \in UB_n$, there is an efficient algorithm to find (x, y).*

Proof. xy is in left canonical form, and therefore written explicitly as a product of Artin generators. As all generators of LB_n commute with all generators of UB_n, we have that $xy = zw$ where $z \in LB_n$ is the product of all the generators in the list xy which come from LB_n, and $w \in UB_n$ is the product of the remaining generators. Note that z, w are known.

Lemma 3. *Assume that $x, z \in LB_n$, and $y, w \in UB_n$. If $xy = zw$, then $x = z$ and $y = w$.*

Proof. Assume that $xy = zw$. Then $xyw^{-1} = z$, and therefore $yw^{-1} = x^{-1}z \in LB_n \cap UB_n = \{e\}$. Thus, $yw^{-1} = e$, that is, $y = w$, and similarly $z = x$. □

Thus, we have found in linear time a presentation of x and y as a product of Artin generators. □

3. Additional remarks

The attack works for any group G with LB_n and UB_n replaced by any two commuting subgroups L, U of G, provided that elements xy where $x \in L$ and $y \in U$ are (or can effectively be) presented as products of elements of L and U.

Lal and Chaturvedi also propose a second scheme in [2]:

Key Generation. Alice chooses integers $r, s \geq 2$, $a \in LB_n$, and $c \in B_n$. The public key is $(X = a^r c a^s, c, r, s)$, and the secret key is a.

Authentication. Bob chooses $b \in UB_n$, and sends Alice the challenge $Y = b^r c b^s$. Alice responds with $Z = a^r Y a^s$. Bob verifies that $Z = b^r X b^s$.

Our attack does not apply to this second scheme. To crack this scheme, it suffices to solve the following problem:

> Given xcx where $x \in LU_n$ is unknown and $c \in B_n$ is known, find x.

Note that this problem is at least as difficult as the *Square* Root Problem in LB_n (which is the same as $B_{n/2}$). In principle, the generic attack described in [1] applies to this problem, and it seems that for practical parameters required to make the system usable, its success probability will not be negligible–see [1]. However, the generic attack is much more time consuming than the one suggested here, and will be debated

until practical parameters are suggested and the attack actually tried for them.

Acknowledgments. We thank Uzi Vishne for double-checking the correctness of this paper.

References

[1] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, and U. Vishne, *Probabilistic solutions of equations in the braid group*, Advances in Applied Mathematics, to appear. http://arXiv.org/math.GR/0404076

[2] S. Lal and A. Chaturvedi, *Authentication schemes using braid groups*, eprint http://arXiv.org/cs.CR/0507066

Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel

E-mail address: boaz.tsaban@weizmann.ac.il

URL: http://www.cs.biu.ac.il/~tsaban