November 9, 2011

Defeating the Kalka–Teicher–Tsaban Linear Algebra Attack on the Algebraic Eraser

Dorian Goldfeld
Paul E. Gunnells, *University of Massachusetts - Amherst*

DEFEATING THE KALKA–TEICHER–TSABAN LINEAR ALGEBRA ATTACK ON THE ALGEBRAIC ERASER

DORIAN GOLDFELD AND PAUL E. GUNNELLS

Abstract. The *Algebraic Eraser* (AE) is a public key protocol for sharing information over an insecure channel using commutative and noncommutative groups; a concrete realization is given by *Colored Burau Key Agreement Protocol* (CBKAP). In this paper, we describe how to choose data in CBKAP to thwart an attack by Kalka–Teicher–Tsaban.

1. Introduction

The *Algebraic Eraser* (AE), due to Anshel–Anshel–Goldfeld–Lemieux [1], is a public key protocol for sharing information over an insecure channel using commutative and noncommutative groups. The *Colored Burau Key Agreement Protocol* (CBKAP) is a concrete realization of the AE based on the braid group and finite general linear groups. The AE and CBKAP have been proposed as a public key protocol suitable for use in low-resource environments, such as passive RFID systems and remote-sensing networks.

In [4] Kalka–Teicher–Tsaban describe an attack on CBKAP based on probabilistic group theory that tries to recover part of the private data in CBKAP. This data consists of two matrices n_a, n_b in a large finite general linear group. Kalka–Teicher–Tsaban explain—under the assumption that n_a and n_b are chosen according to a certain probability distribution—how to detect nontrivial relations that n_a, n_b must satisfy. This then limits the spaces in which n_a, n_b live so that searching for them is feasible.

In this short note, we explain a simple technique for choosing n_a, n_b that defeats this attack.

2. The Algebraic Eraser Key Agreement Protocol and CBKAP

Following [1], we describe a protocol that allows two users (Alice and Bob) to create a shared secret over a public channel. The Algebraic Eraser protocol is built from the tuple

$$(G, M, N, \Pi, E, A, B, N_A, N_B),$$

where the *publicly known* elements are as follows:

Date: Nov. 9, 2011.

2010 *Mathematics Subject Classification.* 94A60, 20F36.

Key words and phrases. Algebraic eraser, colored Burau key agreement protocol, braid group cryptography, cryptography for RFID systems.

- G is a group, with identity element e.
- M, N are two monoids. The monoid M has a left G-action denoted by $(g, m) \mapsto^g m$. We denote the operation in M by a dot: $\cdot$. We denote the semidirect product of M and G by $M \rtimes G$, and write the binary operation using $\circ$:

$$(m_1, g_1) \circ (m_2, g_2) = (m_1 \cdot {}^g m_2,\ g_1 g_2)$$

  for all $(m_1, g_1), (m_2, g_2) \in M \times G$.
- $\Pi \colon M \to N$ is a monoid homomorphism.
- E is a function $E \colon (N \times G) \times (M \rtimes G) \to N \times G$, called *$E$-multiplication*, defined as follows. For all $(n, g) \in N \times G$ and all $(m, g') \in (M \rtimes G)$ we put

$$E((n, g), (m, g')) := \big(n \cdot \Pi\left({}^g m\right), g g'\big) \in N \times G.$$

  We denote E-multiplication by a star: $E((n, g), (m, g')) = (n, g) * (m, g')$.
- $A, B \subset M \rtimes G$ are two E-commuting submonoids. Here by E-commuting we mean

$$(\Pi(a),\ g_a) * (b, g_b) = (\Pi(b),\ g_b) * (a, g_a)$$

  holds for all $(a, g_a) \in A,\ (b, g_b) \in B$.
- Two commuting submonoids $N_A, N_B \subset N$.

Now we describe how this data is used to form the *AE Key Agreement Protocol*. The submonoids A, N_A are assigned to Alice, while B, N_B are assigned to Bob. Alice chooses *private keys*

$$n_a \in N_A, \quad (a_1, g_{a_1}), \ldots, (a_k, g_{a_k}) \in A$$

and then builds the *public key*

$$p_A = (n_a, e) * (a_1, g_{a_1}) * \cdots * (a_k, g_{a_k}) \in N \times G.$$

Similarly, Bob chooses private keys

$$n_b \in N_B, \quad (b_1, g_{b_1}), \ldots, (b_\ell, g_{b_\ell}) \in B$$

and the public key

$$p_B = (n_b, e) * (b_1, g_{b_1}) * \cdots * (b_\ell, g_{b_\ell}) \in N \times G.$$

Given this data, Alice and Bob can then each compute one side of the following equation, which constitutes the shared secret of the protocol:

$$(n_b, e) \cdot p_A * (b_1, g_{b_1}) * \cdots * (b_\ell, g_{b_\ell}) = (n_a, e) \cdot p_B * (a_1, g_{a_1}) * \cdots * (a_\ell, g_{a_\ell}).$$

We note that, in practice, all data in the protocol would be assigned to Alice and Bob by a trusted third party (TTP).

We now describe the *Colored Burau Key Agreement Protocol*, an explicit instance of the AE. Choose $n \geq 8$ even and let $t = (t_1, \ldots, t_n)$ be a tuple of variables. Define matrices $x_i(t)$ by

$$x_1(t) = \begin{pmatrix} -t_1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

and for $i = 2, \dots, n-1$ by

$$x_i(t) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_i & -t_i & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Fix a finite field $\mathbb{F}$. The matrices $x_i(t)$ generate a subgroup

$$M \subset GL(n, \mathbb{F}(t_1, \dots, t_{n-1})).$$

Let $G = S_n$, the symmetric group on n letters, act on the t_i by permutations, and let $s_i \in S_n$ be the simple transposition $(i, i+1)$. Then the pairs $\{(x_i(t), s_i)\}$ then generate the semidirect product $M \rtimes S_n$ inside $GL(n, \mathbb{F}(t_1, \dots, t_{n-1})) \rtimes S_n$. Let $N = GL(n, \mathbb{F})$ and choose $n-1$ nonzero elements $\tau_i \in N$. The assignment $t_i \mapsto \tau_i$ defines a map $\Pi\colon M \to N$.

To complete the description of CBKAP, we only need to specify the commuting monoids $A, B \subset M$ and the E-commuting monoids $N_A, N_B \subset N$. For the former, we can take A (respectively, B) to be the subgroup generated by the first (resp., last) $(n-2)/2$ matrices $x_i(t)$. For the latter, we can fix a matrix $m \in N$ and then define $N_A = N_B = \mathbb{F}[m]$, where the latter means all polynomials in m with coefficients in $\mathbb{F}$ that lie in N. How one chooses m will be explained below in §4.

3. The Kalka-Teicher-Tsaban Attack

In [KTT] a practical linear algebraic attack on the AE is developed. The attacker (called Eve) attempts to find Bob's first private key $n_b \in N_B$. The attack goes as follows. To attack the AE key agreement protocol, Eve creates a spurious element

$$(\alpha, e) \in A \subset M \rtimes G.$$

Then (α, e) E-commutes with every element in B. In particular it E-commutes with

$$(\beta, g) := (b_1, g_{b_1}) \circ \cdots \circ (b_\ell, g_{b_\ell}),$$

given by taking the semidirect product of Bob's second private keys. It follows that

$$\begin{aligned}(\Pi(\alpha), e) * (\beta, g) &= (\Pi(\alpha)\Pi(\beta),\ g) \\ &= (\Pi(\beta), g) * (\alpha, e) = (\Pi(\beta)\Pi({}^{g}\alpha),\ g)\,,\end{aligned}$$

and, therefore,

$$\pi(\alpha) \cdot \Pi(\beta) = \Pi(\beta) \cdot \Pi({}^{g}\alpha). \tag{1}$$

Now Eve also knows Bob's public key given by

$$p_B = (n_b, e) * (b_1, g_{b_1}) * \cdots * (b_\ell, g_{b_\ell}) = (n_b, e) * (\beta, g) = (n_b \Pi(\beta), g)\,. \tag{2}$$

Combining (1) and (2) Eve obtains

$$\Pi(\alpha) \cdot n_b^{-1} \cdot p_B = n_b^{-1} \cdot p_B \cdot \Pi({}^{g}\alpha),$$

which may be rewritten as

$$n_b \cdot \Pi(\alpha) = p_B \cdot \Pi\left({}^{g}\alpha\right) \cdot p_B^{-1} \cdot n_b. \tag{3}$$

The authors of [KTT] then assume that N is a subgroup of $GL(n, \mathbb{F})$ for some positive integer n and some finite field $\mathbb{F}$, as is done in CBKAP. With this assumption, and the assumption that it is possible to generate many spurious elements $(\alpha, e) \in A \subset M \rtimes G$, the authors show that it may be possible for Eve to find n_b by linear algebra: Eve uses the (α, e) to generate many equations of the form

$$n_b y_i = y_i' n_b \qquad y_i, y_i' \in GL(n, \mathbb{F}), i = 1, 2, 3, \ldots. \tag{4}$$

With many such equations she can then try to solve for n_b.

4. Defeating the Kalka-Teicher-Tsaban Attack

We now describe how the TTP can choose data so that Alice and Bob can thwart Eve's attack. The key is to take more care in choosing the matrix $m \in GL(n, \mathbb{F})$ that is used to construct the monoids N_A, N_B.

First, the TTP chooses E-commuting submonoids A, B by giving a set of generators for each of these monoids.

Next, the TTP chooses an element $(\beta, 1)$ out of the generators of B, chooses constants $c_\ell \in \mathbb{F}$, and defines a matrix

$$m = \sum_\ell c_\ell \cdot \Pi(\beta)^\ell.$$

This matrix m is made public.

Then the TTP defines $N_A = N_B = \mathbb{F}[m]$ to be the set of all polynomials in m with coefficients in $\mathbb{F}$. These two submonoids clearly commute with each other. Alice and Bob then choose first private keys n_a, n_b by choosing polynomials in the matrix m.

We claim that this defeats the attack. Indeed, suppose Bob chooses $n_b = \sum_\ell \nu_\ell m^\ell$ with $\nu_\ell \in \mathbb{F}$. This n_b will be a solution to all the equations of the form (3) and (4) that Eve can generate. But this does not give much information about n_b, since it is clear that any matrix of the form

$$n_b \cdot \sum_\ell w_\ell \cdot m^\ell, \qquad w_\ell \in \mathbb{F},$$

will also be a solution to (3) and (4) for any choice of $w_\ell \in \mathbb{F}$. In general this is such a large collection of matrices that the equations (3) and (4) give no useful information. Thus Eve cannot feasibly recover Bob's first private key via this attack.

Remark. There is a variant protocol that deserves mention, in which the TTP chooses commuting monoids A, B and gives B to Bob and only makes A public. Thus B is kept secret and is only known to Bob. The TTP also creates the matrix m out of a spurious element $(\beta, 1)$ in B as above, and makes m public. Using A and the matrix m, Alice can do a key exchange with Bob. This protocol is what is used in potential RFID applications, cf. [3, §1.4] and [2].

References

1. I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux, *Key agreement, the Algebraic Eraser*$^{\mathrm{TM}}$*, and lightweight cryptography*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 1–34.
2. I. Anshel, D. Goldfeld, and P. E. Gunnells, *Fast asymmetric encryption using the Algebraic Eraser*, in preparation.
3. P. E. Gunnells, *On the cryptanalysis of the generalized simultaneous conjugacy search problem and the security of the algebraic eraser*, 2011, arXiv:1105.1141.
4. A. Kalka, M. Teicher, and B. Tsaban, *Cryptanalysis of the Algebraic Eraser and short expressions of permutations as products*, 2008, arXiv:0804.0629v4.

Department of Mathematics, Columbia University, New York, NY 10027
E-mail address: goldfeld@columbia.edu

Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003-9305
E-mail address: gunnells@math.umass.edu