On the Algebraic Eraser and the Ben-Zvi, Blackburn, and Tsaban Attack

Elijah Soria, Lindsey Cioffi, Jiahui Liu

June 20, 2016

Faculty Advisor: Dr. Jonathan Katz

University of Maryland REU-CAAR, 2016

Abstract

The purpose of this paper is to give an overview to the Algebraic Eraser and the Colored Burau Key Agreement Protocol (CBKAP), following the method first displayed in [1]. Then an example of the protocol with small parameters is given to display the inner workings of the scheme. Lastly, we give an exposé on a recent attack on the CBKAP by Ben-Zvi, Blackburn, and Tsaban [2].

1 Colored Burau Key Agreement Protocol

We begin with a brief introduction into braid groups. For a more in-depth introduction into braid groups, see [4].

Definition 1.1. The Artin braid group B_m is the group generated by the generators $\sigma_1, \sigma_2, \ldots, \sigma_{m-1}$ that satisfy the "braid relations": For all $i, j \in \{1, 2, \ldots, m-1\}$ such that $|i-j| \geq 2$,

$$\sigma_i \sigma_j = \sigma_j \sigma_i,$$

and for all $k \in \{1, 2, \ldots, m-2\}$,

$$\sigma_k \sigma_{k+1} \sigma_k = \sigma_{k+1} \sigma_k \sigma_{k+1}.$$

Let $n \geq 7$ be an integer and let $q \in \mathbb{Z}^+$ be prime with the stipulation that $q > n$. Let $t = (t_1, t_2, \ldots, t_n)$ be a commutative indeterminate with an inverse element $t^{-1} = (t_1^{-1}, t_2^{-1}, \ldots, t_n^{-1})$. For each $i \in \{1, 2, 3, \ldots, n-1\}$, define

$$x_1(t) = \begin{bmatrix} -t_1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \text{ and}$$

$$x_i(t) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & 0 & 0 & & \\ & & t_i & -t_i & 1 & & \\ & & 0 & 0 & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \quad \text{where } 2 \leq i \leq n-1.$$

For each $i \in \{2, 3, \ldots, n-1\}$, $x_i(t)$ is thus the identity matrix I_k with the i^{th} row replaced with the successive entries $t_i, -t_i$, and 1, with $-t_i$ being the entry along the main diagonal. It is clear that $x_1(t), \ldots, x_{n-1}(t)$ satisfy the braid relations given in Definition 1.1 for the braid group on n strands B_n. The matrices $x_1(t), \ldots, x_{n-1}(t)$ thus form a representation of B_n, and are more commonly referred to as the reduced Burau representation of B_n. Let M be the group generated by the set $\{x_1(t), \ldots, x_{n-1}(t)\}$ with the operation being matrix multiplication i.e. $M \leq \mathrm{GL}_n(\mathbb{F}_q[t])$.

Let S_n denote the symmetric group on n elements with the identity permutation denoted as e. For each $i \in \{1, 2, \ldots, n-1\}$, let $s_i = \begin{pmatrix} i & i+1 \end{pmatrix}$; $s_i \in S_n$ is simply the transposition of the elements i and $i+1$. The elements $s_1, s_2, \ldots, s_{n-1}$ also satisfy the braid relations for B_n, so they form a representation of B_n as well.

Construct the set of ordered pairs

$$\{(x_1(t), s_1), \ldots, (x_{n-1}(t), s_{n-1})\}.$$

Let $\{(x_1(t), s_1), \ldots, (x_{n-1}(t), s_{n-1})\}$ be the generating set of the semi direct product $M \rtimes S_n$ with the operation defined as $(m_1, \sigma_1) \circ (m_2, \sigma_2) = (m_1^{\sigma_1} m_2, \sigma_1\sigma_2)$ for all $(m_1, \sigma_1), (m_2, \sigma_2) \in M \rtimes S_n$, where ${}^{\sigma_1}m_2$ denotes the permutation σ_1 acting on m_2 by permuting the indeterminants $t_1, \ldots, t_n$. Thus, $\{(x_1(t), s_1), \ldots, (x_{n-1}(t), s_{n-1})\}$ is also a representation of the braid group B_n, and is commonly referred to as the Colored Burau group. Also, let $\mathrm{GL}_n(\mathbb{F}_q) \times S_n$ be simply the direct product of the groups $\mathrm{GL}_n(\mathbb{F}_q)$ and S_n.

Fix elements $\kappa_1, \ldots, \kappa_n \in \mathbb{F}_q$. Create the evaluation homomorphism $\varphi : M \to \mathrm{GL}_n(\mathbb{F}_q)$ where the operation is defined by the mapping $\kappa_1 = t_1, \kappa_2 = t_2, \ldots, \kappa_n = t_n$. The operation known as $e-$ *multiplication* (or $*-$ *multiplication*) is the function $* : (\mathrm{GL}_n(\mathbb{F}_q) \times S_n) \times (M \rtimes S_n) \to \mathrm{GL}_n(\mathbb{F}_q)$ defined by

$$(n, \sigma_1) * (m, \sigma_2) = (n\varphi({}^{\sigma_1}m), \sigma_1\sigma_2)$$

for all $(n, \sigma_1) \in \mathrm{GL}_n(\mathbb{F}_q) \times S_n$ and $(m, \sigma_2) \in M \rtimes S_n$. Elements $(a, \sigma), (b, \sigma') \in M \rtimes S_n$ are said to $e-$ *commute* if

$$(\varphi(a), \sigma) * (b, \sigma') = (\varphi(b), \sigma') * (a, \sigma).$$

Let $m_0 \in \mathrm{GL}_n(\mathbb{F}_q)$ be a matrix of order $q^n - 1$. Let C and D be equivalent subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$ (i.e. $C = D$) where the elements of $C = D$ are all matrices of the form

$$\ell_1 m_0^{k_1} + \ell_2 m_0^{k_2} + \cdots + \ell_r m_0^{k_r},$$

where $\ell_1, \ell_2, \ldots, \ell_r \in \mathbb{F}_q$ and $k_1, k_2, \ldots, k_r \in \mathbb{Z}^+$. Note that the groups C and D are abelian.

With these definitions in hand, we are able to explicitly define the Colored Burau Key Agreement Protocol (CBKAP) as follows. (Alice and Bob take their usual roles)

Private System Data

- A fixed element $z \in M \rtimes S_n$.
- Choose two subsets $A' = \{(x_{l_1}, s_{l_1}), \ldots, (x_{l_\alpha}, s_{l_\alpha})\}$ and $B' = \{(x_{r_1}, s_{r_1}), \ldots, (x_{r_\beta}, s_{r_\beta})\}$ from the set of generators of $M \rtimes S_n$ such that $|\ell_i - r_j| \geq 2$ for all $1 \leq i \leq \ell_\alpha$ and $1 \leq j \leq r_\beta$.

Public Information

- The generating matrix $m_0 \in \mathrm{GL}_n(\mathbb{F}_q)$ from the groups $C = D$.

- The $*$-commuting groups

$$A = z \circ \langle (x_{l_1}, s_{l_1}), \ldots, (x_{l_\alpha}, s_{l_\alpha}) \rangle \circ z^{-1}$$
$$B = z \circ \langle (x_{r_1}, s_{r_1}), \ldots, (x_{r_\beta}, s_{r_\beta}) \rangle \circ z^{-1}$$

- The elements $\kappa_1, \ldots, \kappa_n \in \mathbb{F}_q$ and the corresponding evaluation homomorphism $\varphi : M \to \mathrm{GL}_n(\mathbb{F}_q)$.

Alice's Private Key

- A matrix $c \in C$ such that $c = \ell_1 m_0^{\alpha_1} + \ell_2 m_0^{\alpha_2} + \cdots + \ell_r m_0^{\alpha_r}$ where $\ell_1, \ell_2, \ldots, \ell_r \in \mathbb{F}_q$ and $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}^+$ are kept secret.

- An element $(a, g) \in A$.

Bob's Private Key

- A matrix $d \in d$ such that $d = \ell'_1 m_0^{\beta_1} + \ell'_2 m_0^{\beta_2} + \cdots + \ell'_t m_0^{\beta_t}$ where $\ell'_1, \ell'_2, \ldots, \ell'_t \in \mathbb{F}_q$ and $\beta_1, \beta_2, \ldots, \beta_t \in \mathbb{Z}^+$ are kept secret.

- An element $(b, h) \in B$.

Alice's Public Key

$$(c, e) * (a, g) = (c\varphi(a), g).$$

Bob's Public Key

$$(d, e) * (b, h) = (d\varphi(b), h).$$

Shared Secret

$$(c, e) \cdot ((d, e) * (b, h))) * (a, g) = (d, e) \cdot ((c, e) * (a, g)) * (b, h)$$

2 Example of CBKAP

Let $q = 11$ and $n = 7$. Thus we have the indeterminate $t = (t_1, \dots, t_7)$ and the generating matrices $x_1(t), \dots, x_6(t)$ for the group $M \leq \mathrm{GL}_7(\mathbb{Z}_{11}[t])$ as defined above. Similarly, the elements $s_1 = \begin{pmatrix} 1 & 2 \end{pmatrix}, s_2 = \begin{pmatrix} 2 & 3 \end{pmatrix}, \dots, s_6 = \begin{pmatrix} 6 & 7 \end{pmatrix}$ are the elements from S_7 that we care about. Thus, the set of ordered pairs $\{(x_1 t(t), s_1), (x_2(t), s_2), \dots, (x_6(t), s_6)\}$ generate the semi-direct product $M \rtimes S_7$.

We now turn to defining all public and private information given in the form used in Section 1.

Private System Data

- Select our conjugating element $z \in M \rtimes S_n$ to be

$$\begin{aligned} z &= (x_1(t), s_1)(x_6(t), s_6)(x_3(t), s_3) \\ &= \left(\begin{bmatrix} -t_1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & t_3 & -t_3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & t_6 & -t_6 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right) \end{aligned}$$

- Let the two subsets A' and B' from the set of generators of $M \rtimes S_n$ be

$$\begin{aligned} A' &= \{(x_1(t), s_1), (x_2(t), s_2)\} \\ B' &= \{(x_4(t), s_4), (x_5(t), s_5), (x_6(t), s_6)\} \end{aligned}$$

Public Information

- Let

$$m_0 = \begin{bmatrix} 0 & 10 & 6 & 2 & 0 & 10 & 7 \\ 5 & 4 & 8 & 3 & 9 & 5 & 10 \\ 4 & 0 & 3 & 4 & 9 & 6 & 1 \\ 10 & 8 & 7 & 4 & 2 & 9 & 10 \\ 4 & 7 & 5 & 4 & 8 & 4 & 3 \\ 3 & 10 & 5 & 5 & 2 & 4 & 7 \\ 8 & 10 & 1 & 9 & 2 & 9 & 0 \end{bmatrix}.$$

  Since the characteristic polynomial of m_0 is irreducible over $\mathbb{Z}_{11}$, we can assume (with probability greater than 1/2) that m_0 has order $11^7 - 1$. We have not been able to verify this directly, but will once we get the program for the CBKAP running. For this example, the subgroups $C = D$ of $\mathrm{GL}_n(\mathbb{Z}_q)$ are all matrices of the form

$$\ell_1 m_0^{k_1} + \ell_2 m_0^{k_2} + \cdots + \ell_r m_0^{k_r}$$

  such that $\ell_1, \ldots, \ell_r \in \mathbb{Z}_q$ and $k_1, \ldots, k_r \in \mathbb{Z}^+$.

- The $*$-commuting groups are

$$A = z \circ \langle (x_1(t), s_1), (x_2(t), s_2) \rangle \circ z^{-1}$$
$$B = z \circ \langle (x_4(t), s_4), (x_5(t), s_5), (x_6(t), s_6) \rangle \circ z^{-1}$$

- Let $\tau = (\tau_1, \tau_2, \ldots, \tau_7)$ where

$$\tau_1 = 1 \quad \tau_2 = 2 \quad \tau_3 = 3$$
$$\tau_4 = 4 \quad \tau_5 = 5 \quad \tau_6 = 6$$
$$\tau_7 = 7$$

  $\varphi : M \to \mathrm{GL}_n(\mathbb{F}_q)$ is the evaluation homomorphism using τ.

Alice's Private Key

- Let $c \in C$ be chosen to be

$$c = m_0 + 2m_0^2 + 3m_0^3 = \begin{bmatrix} 0 & 9 & 0 & 1 & 0 & 9 & 1 \\ 1 & 8 & 0 & 3 & 4 & 1 & 9 \\ 8 & 0 & 3 & 8 & 4 & 0 & 6 \\ 9 & 0 & 1 & 8 & 1 & 4 & 9 \\ 8 & 1 & 1 & 8 & 0 & 8 & 3 \\ 3 & 9 & 1 & 1 & 1 & 8 & 1 \\ 0 & 9 & 6 & 4 & 1 & 4 & 0 \end{bmatrix}$$

- Choose $(a, g) \in A$ to be

$$\begin{aligned} (a, g) &= z \circ (x_1(t), s_1) \circ z^{-1} \\ &= \left(\begin{bmatrix} -t_2 & t_2 - t_1 + 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & t_3 t_4^{-1} & -t_3 t_4^{-1} + 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & t_6 t_7^{-1} & -t_6 t_7^{-1} + 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \right) \end{aligned}$$

Bob's Private Key

- Let $d \in D$ be chosen to be

$$d = 4m_0^2 + m_0^5 + 2m_0^6 = \begin{bmatrix} 0 & 5 & 10 & 0 & 0 & 5 & 5 \\ 1 & 7 & 8 & 10 & 2 & 1 & 5 \\ 7 & 0 & 10 & 7 & 2 & 10 & 7 \\ 5 & 8 & 5 & 7 & 0 & 2 & 5 \\ 7 & 5 & 1 & 7 & 8 & 7 & 10 \\ 10 & 5 & 1 & 1 & 0 & 7 & 5 \\ 8 & 5 & 7 & 2 & 0 & 2 & 0 \end{bmatrix}$$

- Choose $(b,h) \in B$ to be

$$
\begin{aligned}
(b,h) &= z \cdot (x_6(t), s_6) \cdot z^{-1} \\
&= \left(\begin{bmatrix} t_1t_2^{-1} & 1-t_1t_2^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & t_3t_4^{-1} & 1-t_3t_4^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & t_6-t_6t_7 & -t_7 & t_7-t_6+1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{pmatrix} 6 & 7 \end{pmatrix} \right)
\end{aligned}
$$

Alice's Public Key

$$
(c,e) * (a,g) = (c\varphi(a), g) = \left(\begin{bmatrix} 0 & 9 & 0 & 1 & 0 & 3 & 7 \\ 9 & 10 & 0 & 3 & 4 & 4 & 6 \\ 6 & 5 & 5 & 6 & 4 & 0 & 6 \\ 4 & 7 & 9 & 0 & 1 & 5 & 8 \\ 6 & 6 & 9 & 0 & 0 & 10 & 1 \\ 5 & 4 & 9 & 4 & 1 & 10 & 10 \\ 0 & 9 & 10 & 0 & 1 & 5 & 10 \end{bmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \right).
$$

Bob's Public Key

$$
(d,e) * (b,h) = (d\varphi(b), h) = \left(\begin{bmatrix} 0 & 5 & 2 & 8 & 7 & 9 & 4 \\ 6 & 2 & 6 & 1 & 10 & 4 & 7 \\ 9 & 9 & 2 & 4 & 5 & 7 & 5 \\ 8 & 5 & 1 & 0 & 5 & 8 & 9 \\ 9 & 3 & 9 & 10 & 9 & 6 & 2 \\ 5 & 10 & 9 & 4 & 1 & 6 & 8 \\ 4 & 9 & 8 & 1 & 5 & 8 & 4 \end{bmatrix}, \begin{pmatrix} 6 & 7 \end{pmatrix} \right)
$$

Shared Secret

$$\begin{aligned}(c,e)\cdot((d,e)*(b,h))*(a,g) &= \left(\begin{bmatrix} 7 & 1 & 9 & 0 & 2 & 5 & 5 \\ 6 & 7 & 6 & 9 & 6 & 8 & 0 \\ 5 & 4 & 8 & 3 & 9 & 8 & 8 \\ 7 & 5 & 5 & 7 & 1 & 10 & 5 \\ 9 & 5 & 5 & 3 & 0 & 3 & 7 \\ 10 & 6 & 10 & 9 & 0 & 8 & 8 \\ 10 & 0 & 9 & 5 & 3 & 6 & 1 \end{bmatrix}, \begin{pmatrix} 6 & 7 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\right) \\ &= (d,e)\cdot((c,e)*(a,g))*(b,h)\end{aligned}$$

3 The Ben-Zvi, Blackburn, and Tsaban (BBT) Attack

Assume that Eve, the adversary, sees all public information. With the public information, Eve hopes to produce the Shared Secret between Alice and Bob, which is retrieved directly instead of through discovering each of their respective private keys. Before going through the attack specifically, a few definitions will be needed.

Let H be an arbitrary group of $n\times n$ matrices over $\mathbb{F}_q$. Let $\mathrm{Alg}(H)$ denote the $\mathbb{F}_q$-algebra generated by H; that is, $\mathrm{Alg}(H)$ is the collection of a $\mathbb{F}_q$-linear combinations of elements in H. Furthermore, let $\mathrm{Alg}^*(H)$ denote the set of all invertible matrices in $\mathrm{Alg}(H)$. Note that in the CBKAP, $C = \mathrm{Alg}^*(C)$.

Let $\gamma_1, \gamma_2, \ldots, \gamma_\rho \in C$ be a basis for C, which Eve will need to compute. Let $P \trianglelefteq A$ be the *pure subgroup* of A defined as

$$P = \{(\alpha, e) \in A\}.$$

Thus, $\varphi(P)$ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$.

Eve's main goal is to find $\tilde{c} \in C$, $(\tilde{a}, g) \in M \rtimes S_n$, and

$$\sum_{i=1}^{k} \ell_i \varphi(\alpha_i),$$

where $(\alpha_i, e) \in P$ and $\ell_i \in \mathbb{F}_q$ for all $i \in \{1, \ldots, k\}$, that satisfy

$$(c,e)*(a,g) = \tilde{c}\cdot\left(\sum_{i=1}^{k} \ell_i\varphi(\alpha_i), e\right) * (\tilde{a}, g),$$

where $(c, e) * (a, g)$ is Alice's public key. The reason is that, with these elements in hand, Eve can compute the shared secret as follows:

- First compute the matrix
$$\beta' = \sum_{i=1}^{k} \ell_i \varphi({}^{h}\alpha_i),$$
where h is the element from the symmetric group from Bob's public key.

- Eve can then compute
$$(\tilde{c} d\varphi(b)\beta', h) * (\tilde{a}, g),$$
which is exactly the shared secret between Alice and Bob. (See [2] for the proof of this claim)

The rest of the attack is devoted to finding the desired elements that allow Eve to construct the shared secret.

1. **Find the α_i's:** Eve needs to find the elements (α_i, e)'s from A such that the collection $\{\varphi(\alpha_1), \ldots, \varphi(\alpha_j)\}$ form a basis for $\mathrm{Alg}^*(\varphi(P))$. The authors note that this step can be carried out before the transmission of messages between Alice and Bob take place as this does not rely on their public keys.

   Following the method given in [3], Eve generates an element $(a', g') \in A$ such that the order of $g' \in S_n$ is smaller than n, and then computes $\alpha_1 = (a', g')^r$. Eve repeats this process to find $\alpha_2, \alpha_3, \ldots,$ until the dimension of the $\mathbb{F}_q$-linear span of the matrices $\varphi(\alpha_i)$ stops growing, usually when the dimension stops growing after four α_i's are added. Eve then fixes a linearly independent subset of these matrices, and thus we have that the matrices $\varphi(\alpha_1), \ldots, \varphi(\alpha_j)$ are a basis for a subspace V of $\mathrm{Alg}(\varphi(P))$. With high probability, we expect that $V = \mathrm{Alg}(\varphi(P))$, so this is assumed from now on.

2. **Find $\tilde{a}$:** Again using the method found in [3], we find a product of generators of A whose second component is equal to g, and this product will be $(\tilde{a}, g)$. Also, define $\delta \in \mathrm{GL}_n(\mathbb{F}_q)$ by
$$(\delta, e) = (c\varphi(a), g) * (\tilde{a}, g)^{-1}.$$

3. **Find $\tilde{c}$:** Assume that Eve has already found the elements $\gamma_1, \gamma_2, \ldots, \gamma_\rho \in C$ that form a basis for C (recall that $C = \mathrm{Alg}(C)$ by assumption). Eve then finds element $y_1, \ldots, y_\rho \in \mathbb{F}_q$ such that

$$\delta^{-1}(y_1\gamma_1 + y_2\gamma_2 + \cdots + y_\rho\gamma_\rho) \in \mathrm{Alg}(\varphi(P)), \text{ and} \tag{3.1}$$

$$y_1\gamma_1 + y_2\gamma_2 + \cdots + y_\rho\gamma_\rho \in \mathrm{GL}_n(\mathbb{F}_q) \tag{3.2}$$

   Let $\tilde{c} = y_1\gamma_1 + y_2\gamma_2 + \cdots + y_\rho\gamma_\rho \in C$. To find the elements $y_1, \ldots, y_\rho \in \mathbb{F}_q$, Eve randomly generates solutions y_i to the equation given in 3.1. Due to the linearity of 3.1, this turns out to be easy. If the solution that satisfies 3.1 also satisfies 3.2, then Eve stops; otherwise, Eve starts the process again. Ben-Zvi et al. show in [2] that the proportion of solutions to 3.1 that satisfy 3.2 is bounded by $1 - n/q$. The element $\tilde{c}$ is used in the calculation of the shared secret.

4. **Everything Else:** Since $\delta^{-1}\tilde{c} \in \mathrm{Alg}(\varphi(P))$, it follows that $\tilde{c}^{-1}\delta \in \mathrm{Alg}(\varphi(P))$ as well. Thus, Eve can calculate coefficients ℓ_i that satisfy

$$\sum_{i=1}^{k} = \ell_i\varphi(\alpha_i) = \tilde{c}^{-1}\delta.$$

   Therefore, Eve can calculate Alice's public key as follows.

$$(\delta, e) * (\tilde{a}, g) = ((p, g) * (\tilde{a}, g)^{-1}) * (\tilde{a}, g) = (c\varphi(a), g).$$

The BBT attack has been implemented and recovers the shared secret for a transmission where $n = 16$, $q = 256$, and generating words of A being length 650 in less than 8 hours, using only 64MB of memory and running on a 2GHz core. The attack has yet to be optimized, but the mathematical beauty of the scheme remains!

References

[1] I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux, *Key agreement, the algebraic erasertm, and lightweight cryptography*, Contemporary Mathematics **418** (2007), 1–34.

[2] A. Ben-Zvi, S. R. Blackburn, and B. Tsaban, *A practical cryptanalysis of the algebraic eraser*, 2015. `http://eprint.iacr.org/`.

[3] A. Kalka, M. Teicher, and B. Tsaban, *Short expressions of permutations as products and cryptanalysis of the algebraic eraser*, Advances in Applied Mathematics **49** (2012), no. 1, 57–76.

[4] C. Kassel, O. Dodane, and V. Turaev, *Braid groups*, Graduate Texts in Mathematics, Springer New York, 2008.