1

Representation Attacks on the Braid Diffie-Hellman Public Key Encryption

Arkadius G. Kalka*

Abstract

The Braid Diffie-Hellman Public Key Cryptosystem is based on the Diffie-Hellman version of a Decomposition Problem (DP) in the braid group B_n. We propose a linear algebra attack on DP via the faithful Lawrence-Krammer representation ρ'_n. For generic and sufficiently long instance braids we recover the ρ'_n-image of the private key using just one matrix inversion.

Keywords: Public-key cryptography, Braid group, Braid Diffie-Hellman key agreement protocol, Generalized conjugacy search problem, Decomposition problem, Linear algebra attack, Lawrence-Krammer representation

In section 1 we give a description of the Braid Diffie-Hellman key agreement protocol and its underlying algorithmic problems (DH-DP, DP). Representation attacks on these problems especially by Cheon, Jun [6] and E. Lee, Park [20] are discussed in section 2. In section 3 we develope our proposed linear algebra attack on DP for generic and sufficiently long instance braids via the faithful Lawrence-Krammer representation.
In the appendix we estimate the asymptotic complexity of this attack.

1 Braid Diffie-Hellman Key Agreement

Braid-based cryptography was introduced by Anshel, Anshel and Goldfeld in 1999 [1] and by Ko, Lee, Cheon, Han, Kang and Park at the CRYPTO 2000 [16]. Several attacks have been proposed for the AAG key agreement protocol (KAP) for braid groups [21, 13, 14, 8, 11] and for the Ko, Lee et al. braid Diffie-Hellman public key encryption scheme [12, 11, 6, 20] so far. An introducing, summarizing and outlooking survey on braid group cryptography is given by P. Dehornoy [7].
Here we deal with the revised version of the **Braid Diffie-Hellman KAP** suggested at the ASIACRYPT 2001 [5]:
Let LB_m and UB_{n-m} $(m < n)$ be the commuting subgroups of the n-braid group $B_n :=< \sigma_1, \ldots, \sigma_{n-1} | \, \sigma_i\sigma_j = \sigma_j\sigma_i \, , |i-j| > 1 \, , \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \forall i = 1, \ldots, n-2 >$ generated by $\sigma_1, \ldots, \sigma_{m-1}$ and $\sigma_{m+1}, \ldots, \sigma_{n-1}$ respectively. Then A(lice) and B(ob) have to perform the following protocol steps:

*Ruhr-Universität-Bochum, Fakultät für Mathematik, Lehrstuhl Prof. L. Gerritzen

0) A or B select (and publish) a generic, sufficiently complicated braid $x \in B_n$.
1A) A generates randomly $(a_l, a_r) \in LB_m^2$, and sends $y_A = a_l x a_r$ in a rewritten (normal) form to B.
1B) B generates randomly $(b_l, b_r) \in UB_{n-m}^2$, and sends $y_B = b_l x b_r$ to A.
2A) A receives y_B and computes $K := a_l y_B a_r$.
2B) B receives y_A and computes also the shared key $b_l y_A b_r = b_l(a_l x a_r)b_r = a_l(b_l x b_r)a_r = a_l y_B a_r = K$.

The security of this key agreement scheme and the corresponding PKC[1] depend on the following **Diffie-Hellman type Decompositon Problem (DH-DP):**

Instance: $(x, y_A, y_B) \in B_n^3$ such that $y_A = a_l x a_r$ and $y_B = b_l x b_r$ for some $a_l, a_r \in LB_m$ and $b_l, b_r \in UB_{n-m}$.
Objective: Find $K := a_l y_B a_r = b_l y_A b_r = a_l b_l x a_r b_r$.

To recover the private key $(a_l, a_r) \in LB_m^2$ of A(lice) it is sufficient to solve the following **Decompositon Problem (DP):**

Instance: $(x, y_A) \in B_n^2$ such that $y_A = a_l x a_r$ for some $a_l, a_r \in LB_m$.
Objective: Find $(a_l', a_r') \in LB_m^2$ such that $a_l' x a_r' = y_A$.

A solution for the DP induces a solution for the DH-DP. In the case $a_l = a_r^{-1}$ and $b_l = b_r^{-1}$ we obtain the original braid Diffie-Hellman key agreement scheme, which is based on a Diffie-Hellman version of the Generalized Conjugacy Search Problem (GCSP) [16]. The fact that in general $a_l \neq a_r^{-1}$ (and $b_l \neq b_r^{-1}$) for the revised scheme is indeed its advantage:
a_l and a_r are in general not in the same conjugacy class. So attacks, which (frequently) use conjugacy operations like Cycling attacks [11] and Gebhardt's computation of Ultra Summit Sets [10], don't work.
We can restrict to the monoid versions DP$^+$ and DH-DP$^+$, in which each braid group is replaced by the corresponding monoid of positive braids, because we can multiply the equations $y_A = a_l x a_r$, $y_B = b_l x b_r$ by a sufficiently high power of the square of the Garside element Δ_n^2, which generates the center of B_n.

2 Representation attacks and previous work

Linear algebra or representation attacks on braid-based cryptosystems work as follows:

I) Choose a linear representation $\rho : B_n \longrightarrow GL(k, R)$ of the n-braid group for some ring R and $k \in \mathbb{N}$, and compute the images of the instance braids for this representation.
II) Solve the base problem in the matrix group $GL(k, R)$. Keep in mind that there will be infinitely many solutions in general, and that not all solutions are in $\mathrm{im}\rho \subset GL(k, R)$.
III) Find preimage braids for solutions in $\mathrm{im}\rho$.

[1] Using an ideal hash function from the braid group into the message space $H : B_n \longrightarrow \{0,1\}^k$ a corresponding Public Key Encryption can be constructed ([5], chapter 6).

2.1 Linear algebra attack on DH-DP$^+$ via Lawrence-Krammer representation [6]

Let V denote the free $\mathbb{Z}[t^{\pm 1}, q^{\pm 1}]$-module of rank $\binom{n}{2}$ with basis $\{x_{ij} | 1 \leq i < j \leq n\}$. The Lawrence-Krammer (LK) representation [19]
$\rho_n : B_n \longrightarrow GL(\binom{n}{2}, \mathbb{Z}[t^{\pm 1}, q^{\pm 1}]) = Aut(V)$ defined $\forall k = 1, \ldots, n-1$ by

$$(\rho_n \sigma_k) x_{ij} = \begin{cases} tq^2 x_{k,k+1} & , i = k, j = k+1 \\ (1-q)x_{ik} + q x_{i,k+1} & , i < k = j \\ x_{ik} + tq^{k-i+1}(q-1)x_{k,k+1} & , i < k, j = k+1 \\ tq(q-1)x_{k,k+1} + q x_{k+1,j} & , i = k, k+1 < j \\ x_{kj} + (1-q)x_{k+1,j} & , i = k+1 < j \\ x_{ij} & , j < k \quad \text{or} \quad k+1 < i \\ x_{ij} + tq^{k-i}(q-1)^2 x_{k,k+1} & , i < k, k+1 < j \end{cases}$$

was proved to be faithful by Bigelow and Krammer [17, 3, 18] for all n and even if q is a real number with $0 < q < 1$.
We use the abbreviation $\rho'_n := \rho_n|_{q=1/2}$. Then the Cheon-Jun attack on DH-DP$^+$ works roughly as follows. For technical details see [6].

I) Compute $X = \rho'_n x, Y^A = \rho'_n y_A, Y^B = \rho'_n y_B \in Mat(\binom{n}{2}, \mathbb{Q}[t])$ for $x, y_A, y_B \in B_n^+$.

II) Compute $\binom{n}{2} \times \binom{n}{2}$-matrices A'_l, A'_r over $\mathbb{Q}[t]$ satisfying the following equations $\forall k = m+1, \ldots, n-1$:

$$X A'_r = A'_l Y^A \tag{1}$$

$$\left.\begin{array}{rcl} \rho'_n(\sigma_k) A'_l & = & A'_l \rho'_n(\sigma_k) \\ \rho'_n(\sigma_k) A'_r & = & A'_r \rho'_n(\sigma_k) \end{array}\right\} \tag{2}$$

A'_l is invertible with overwhelming probability, so we can compute
$(A'_l)^{-1} Y^B A'_r = (A'_l)^{-1}(B^l X B^r) A'_r \overset{(2)}{=} B^l ((A'_l)^{-1} X A'_r) B^r \overset{(1)}{=} B^l Y^A B^r = \rho'_n(K)$ with $B^l := \rho'_n b_l, B^r := \rho'_n b_r$.
Note that in general $(A'_l)^{-1} \neq A^l := \rho'_n a_l$ and $A'_r \neq A^r := \rho'_n a_r$, and $(A'_l)^{-1}$ and A'_r need not to lie in im ρ'_n.
We remark that we can change the system (1), (2) by vectorization into a highly overdetermined linear system with $(2n - 2m - 1)\binom{n}{2}^2$ equations and $2\binom{n}{2}^2$ variables, which are polynomials in $\mathbb{Q}[t]$[2]. The complexity of the Cheon-Jun attack is dominated by Gaussian elimination for such linear systems.

III) In [6] chapter 3.2 Cheon and Jun developed a polynomial time algorithm for inverting the LK-representation based on the ideas of Krammer [18]. Applying this algorithm to $(A'_l)^{-1} Y^B A'_r = \rho_n(K)$ we obtain the unique preimage braid K.

So the Cheon-Jun attack provides a polynomial time solution to the DH-DP. Nevertheless the complexity is too large to break the cryptosystem with the proposed parameters in [16, 5] efficiently.

[2] By precise analysis of Krammer matrices as in [6] we can reduce the number of variables and equations, but (in the case $m = O(n)$) they keep $O(n^4)$ and $O(n^5)$ (not $O(n^4)$!) respectively.

2.2 Linear algebra attack on DP$^+$ via Burau representation [20]

Let W denote the free $\mathbb{Z}[q^{\pm 1}]$-module of rank n with basis $\{w_i | 1 \leq i \leq n\}$. The (unreduced)[3] Burau representation [4] $\rho_n^{\text{Burau}} : B_n \longrightarrow GL(n, \mathbb{Z}[q^{\pm 1}]) = Aut(W)$ defined by

$$\rho_n^{\text{Burau}} \sigma_k = \mathbb{I}_{k-1} \oplus \begin{pmatrix} 1-q & q \\ 1 & 0 \end{pmatrix} \oplus \mathbb{I}_{n-k-1} \qquad \forall\, k = 1, \ldots, n-1$$

provides the following special attack on DP$^+$, but only in the symmetric case $2m = n$:

I) Compute $X = \rho_n^{\text{Burau}} x, Y = \rho_n^{\text{Burau}} y_A \in Mat(n, \mathbb{Z}[q])$ for $x, y_A \in B_n^+$.

II) Consider the DP-induced decomposition $W = \text{span} L \oplus \text{span} U$ with $L := \{w_i | 1 \leq i \leq m\}, U := \{w_i | m+1 \leq i \leq n\}$. Then we obtain the following block matrix equations:

$$\begin{aligned} Y = \begin{pmatrix} Y_{LL} & Y_{LU} \\ Y_{UL} & Y_{UU} \end{pmatrix} &= \begin{pmatrix} A_l & 0 \\ 0 & \mathbb{I}_{n-m} \end{pmatrix} \begin{pmatrix} X_{LL} & X_{LU} \\ X_{UL} & X_{UU} \end{pmatrix} \begin{pmatrix} A_r & 0 \\ 0 & \mathbb{I}_{n-m} \end{pmatrix} \\ &= \begin{pmatrix} A_l X_{LL} A_r & A_l X_{LU} \\ X_{UL} A_r & X_{UU} \end{pmatrix} \end{aligned}$$

Note that $A_l = \rho_m^{\text{Burau}} a_l, A_r = \rho_m^{\text{Burau}} a_r$. In the case $2m = n$ the offdiagonal blockmatrices X_{LU}, X_{UL} are quadratic. The probability that X_{LU} or X_{UL} have full rank for randomly chosen $x \in B_n^+$ increases for $n = \text{const}$ and increasing word length $|x|$, and for $|x| = \text{const}$ and decreasing braid index n ($n \geq 5$) [20]. If at least one of these two offdiagonal matrices is regular, so we obtain $A_l = Y_{LU} X_{LU}^{-1}$ or $A_r = X_{UL}^{-1} Y_{UL}$.
In [15] Ko suggests the following countermeasure: Choose a x, which contains just a few generators σ_m.

III) The Burau representation is proved to be not faithful for $n \geq 5$ [2]. The best known algorithms for computing preimage braids for the Burau representation are the heuristic Hughes algorithm [13] and its variations by Lee and Park [20]. Applying it to A_l or A_r we might obtain a_l or a_r, and that's sufficient to solve DP.
But the success rates of these heuristics decreases for $m = \text{const}$ with increasing word length $|a|$, and they are very low for the parameter values suggested in [5].

3 Cryptanalysis

Now we use ideas from Lee and Park [20] to develop an attack on DP$^+$ via LK-representation.

3.1 Symmetric case $2m = n$

Consider the DP-induced decomposition $V = \text{span}\, L \oplus \text{span}\, M \oplus \text{span}\, U$ with $L := \{x_{ij} | 1 \leq i < j \leq m\}, M := \{x_{ij} | 1 \leq i \leq m < m+1 \leq j \leq n\}$ and $U := \{x_{ij} | m+1 \leq i < j \leq n\}$ ($|L| = \binom{m}{2}, |M| = m(n-m), |U| = \binom{n-m}{2}$).

[3] It is also possible to use the reduced Burau representation $B_n \longrightarrow GL(n-1, \mathbb{Z}[q^{\pm 1}])$.

The basis is reordered according to the DP-induced decomposition of V by the transformation $\phi : \{x_{ij} | 1 \leq i < j \leq n\} \longrightarrow \{x_k | 1 \leq k \leq \binom{n}{2}\}$ defined by $x_{ij} \mapsto x_k$ with

$$k := \begin{cases} \binom{j-1}{2} & , x_{ij} \in L \\ \binom{m}{2} + (j-m-1)m + i & , x_{ij} \in M \\ \binom{m}{2} + m(n-m) + \binom{j-m-1}{2} + i - m & , x_{ij} \in U \end{cases}$$

So we get the following block matrix structures for embedded braids:

$$\rho_n a = \begin{pmatrix} A_{LL} & A_{LM} \\ 0 & A_{MM} \end{pmatrix} \oplus \mathbb{I}_{\binom{n-m}{2}} \quad \forall a \in LB_m \quad \text{and}$$

$$\rho_n b = \mathbb{I}_{\binom{m}{2}} \oplus \begin{pmatrix} B_{MM} & 0 \\ B_{UM} & B_{UU} \end{pmatrix} \quad \forall b \in UB_{n-m}\,.$$

Note that $A_{LL} = \rho_m a = \rho_m a(t,q)$, $A_{LM} = A_{LM}(t,q)$, rank $A_{LM} \leq m$, and $A_{MM} = A_{MM}(q) = (\rho_m^{\text{Burau-type}} a)^{\oplus(n-m)} \in Mat((n-m)m, \mathbb{Z}[q^{\pm 1}])$.
The commutativity equation $ab = ba \quad \forall a \in LB_m \forall b \in UB_{n-m}$ yields the following block matrix equations:

$$\rho_n ab = \begin{pmatrix} A_{LL} & A_{LM}B_{MM} & 0 \\ 0 & A_{MM}B_{MM} & 0 \\ 0 & B_{UM} & B_{UU} \end{pmatrix} = \begin{pmatrix} A_{LL} & A_{LM} & 0 \\ 0 & B_{MM}A_{MM} & 0 \\ 0 & B_{UM}A_{MM} & B_{UU} \end{pmatrix} \quad (3)$$

Our representation attack contains the following steps:

I) Compute the images of the instance braids:

$$\rho'_n x = \begin{pmatrix} X_{LL} & X_{LM} & X_{LU} \\ X_{ML} & X_{MM} & X_{MU} \\ X_{UL} & X_{UM} & X_{UU} \end{pmatrix}, \rho'_n y_A = \begin{pmatrix} Y_{LL} & Y_{LM} & Y_{LU} \\ Y_{ML} & Y_{MM} & Y_{MU} \\ Y_{UL} & Y_{UM} & Y_{UU} \end{pmatrix}.$$

II) The UL-block matrix from $\rho'_n a_l x a_r =$

$$\left(\begin{array}{c|c|c} A^l_{LL}X_{LL}A^r_{LL} + A^l_{LM}X_{ML}A^r_{LL} & (A^l_{LL}X_{LL} + A^l_{LM}X_{ML})A^r_{LM} + (A^l_{LL}X_{LM} + A^l_{LM}X_{MM})A^r_{MM} & A^l_{LL}X_{LU} + A^l_{LM}X_{MU} \\ \hline A^l_{MM}X_{ML}A^r_{LL} & A^l_{MM}(X_{ML}A^r_{LM} + X_{MM}A^r_{MM}) & A^l_{MM}X_{MU} \\ \hline X_{UL}A^r_{LL} & X_{UL}A^r_{LM} + X_{UM}A^r_{MM} & X_{UU} \end{array}\right)$$

yields the equation $Y_{UL} = X_{UL}A^r_{LL}$.
X_{UL} is quadratic for $2m = n$ and non-singular with increasing probability for increasing $|x|$ ($n = \text{const}$) and decreasing n ($|x| = \text{const}$) (**Table 1**).
If X_{UL} is regular, we can compute $\rho'_m a_r = A^r_{LL} = X^{-1}_{UL}Y_{UL}$.
If it is not, choose a generic, sufficiently long $u \in UB^+_{n-m}$ with $\rho'_n u = \mathbb{I}_{\binom{m}{2}} \oplus \begin{pmatrix} U_{MM} & 0 \\ U_{UM} & U_{UU} \end{pmatrix}$, and compute
$(\rho'_n u a_l x a_r)_{UL} = (UY)_{UL} = U_{UM}Y_{ML} + U_{UU}Y_{UL} = U_{UM}A^l_{MM}X_{ML}A^r_{LL} + U_{UU}X_{UL}A^r_{LL} \overset{(3)}{=} (U_{UM}X_{ML} + U_{UU}X_{UL})A^r_{LL}$.
Then $U_{UM}X_{ML} + U_{UU}X_{UL} = (\rho'_n ux)_{UL}$ has with high probability full rank for sufficiently long u, and we obtain

$$A^r_{LL} = (U_{UM}X_{ML} + U_{UU}X_{UL})^{-1}(U_{UM}Y_{ML} + U_{UU}Y_{UL}).$$

Table 1: $p := \text{Prob}(\text{rank}\, X_{UL}|_{t=3} = \binom{m}{2})$

$n = 2m$									
6	$\|x\|$	15	20	25	30	35	40	45	50
	p in %	6	30	41	62	77	90	92	95
8	$\|x\|$	30	40	50	60	70	80	90	100
	p in %	0	7	30	48	69	87	89	99
10	$\|x\|$	70	90	110	130	150	170		
	p in %	5	21	60	80	92	100		
12	$\|x\|$	100	140	180	220	260			
	p in %	1	20	65	88	99			

100 random experiments were executed for each entry. A randomly chosen $x \in B_n^+$ is rejected, if it doesn't contain all Artin generators.

Note that this regularization procedure does not work, if X_{ML} and X_{UL} have a common zero column, or if X_{UL} is the null matrix and X_{ML} doesn't have full rank. But for generic, sufficiently long and complicated x, which of course contains all Artin generators $\sigma_1, \ldots, \sigma_{n-1}$, this will not occur.

III) By Cheon-Jun algorithm we lift back $A_{LL}^r = \rho'_m a_r$ to $a_r \in B_m^+$.

3.2 Asymmetric cases

a) $\mathbf{m < n - m}$

Here we have to replace m by $m' := n/2$ (n even) or $m' := (n+1)/2$ (n odd) in the definitions of L, M, U. If n is even the problem is reduced to the symmetric case $n = 2m'$.
But if n is odd we have to embed the problem into $B_{2m'}$ and compute images of the instance braids for $\rho'_{2m'}$. Choose the decomposition $\text{span}\{x_{ij}|1 \le i < j \le 2m'\} = \text{span}L \oplus \text{span}\bar{M} \oplus \text{span}\bar{U}$ with $\bar{M} := \{x_{ij}|1 \le i \le m', m'+1 \le j \le 2m'\}$ and $\bar{U} := \{x_{ij}|m'+1 \le i < j \le 2m'\}$. Then $X_{\bar{U}L}$ is quadratic, but singular - it contains (at least) $m' - 1 = (n-1)/2$ zero rows, and $X_{\bar{M}L}$ has (at least) $m' = (n+1)/2$ zero rows. Nevertheless we can apply the above regularization procedure again:
Choose a generic, sufficiently long $u \in \bar{U}B^+_{2m'-m'} :=< \sigma_{m'+1}, \ldots, \sigma_{2m'-1} >^+ \subset B^+_{2m'}$ and compute

$$\begin{array}{rcl} (\rho'_{2m'} u y_A)_{\bar{U}L} & = & U_{\bar{U}\bar{M}} Y_{\bar{M}L} + U_{\bar{U}\bar{U}} Y_{\bar{U}L} = U_{\bar{U}M} Y_{ML} + U_{\bar{U}U} Y_{UL} = \\ (\rho'_{2m'} u a_l x a_r)_{\bar{U}L} & = & (\rho'_{2m'} u x a_r)_{\bar{U}L} = (U_{\bar{U}\bar{M}} X_{\bar{M}L} + U_{\bar{U}\bar{U}} X_{\bar{U}L}) A_{LL}^r \\ & = & (U_{\bar{U}M} X_{ML} + U_{\bar{U}U} X_{UL}) A_{LL}^r. \end{array}$$

$(\rho'_{2m'} ux)_{\bar{U}L} = U_{\bar{U}M} X_{ML} + U_{\bar{U}U} X_{UL}$ is quadratic, and regular for generic, sufficiently long $u \in \bar{U}B'^+_m, x \in LB^+_n$, and we obtain

$$A_{LL}^r = (U_{\bar{U}M} X_{ML} + U_{\bar{U}U} X_{UL})^{-1} (U_{\bar{U}M} Y_{ML} + U_{\bar{U}U} Y_{UL}) = \rho'_{m'} a_r.$$

b) $\mathbf{m > n - m}$

By half twist transformation $\tau_n : B_n \longrightarrow B_n$ def. by $\sigma_i \mapsto \sigma_{n-i}$ we reduce case b) to case a).

Note that we perform now an attack on Bob's private key, while in case a) we only can compute the private key of Alice.

c) Simple Generalizations

We can introduce some simple variations and generalizations of the DH-DP:
One way is to choose different partitions of the (l)eft and (r)ight areas, i.e. choose $a_l \in LB_{m_l}, b_l \in UB_{n-m_l}, a_r \in LB_{m_r}, b_r \in UB_{n-m_r}$ with $m_l \neq m_r$ $(m_l, m_r < n)$. By half twist transformation, reverse anti-automorphism of B_n and proper embeddings of the private keys we can transform the problem to the following standard form of l,r-asymmetric DP:

Instance: $(x', y') \in B_n^2$ such that $y' = p_l x p_r$ for some $p_l \in LB_{m'_l}, p_r \in LB_{m'_r}$ with $m'_r = n - m'_l < n/2$.
Objective: Find $p'_l \in LB_{m'_l}, p'_r \in LB_{m'_r}$ such that $p'_l x' p'_r = y'$.

Defining $L := \{x_{ij} | 1 \leq i < j \leq m'_r\}$ and $U := \{x_{ij} | n - m'_r + 1 \leq i < j \leq n\}$ we get $(\rho'_n y')_{UL} = (\rho'_n p_l x' p_r)_{UL} = X'_{UL} \rho'_{m'_r}(p_r)$. So recovering p_r depends on the regularity of the quadratic block matrix $X'_{UL} := (\rho'_n x')_{UL}$.
Another way is to choose $a_r \in UB_{n-m}, b_r \in LB_m$ (and keep $a_l \in LB_m, b_l \in UB_{n-m}$) or vice versa. But in this case we can attack the DP, if one of the quadratic matrices X_{UU} or X_{LL} is invertible.
Further generalizations e.g. by introducing refined partitions of each area, can be treated with similar methods.

References

[1] Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Mathematical Research Letters 6, 1-5 (1999)

[2] Bigelow, S.: The Burau representation is not faithful for $n = 5$. Geom. Topol. 3, 397-404 (1999)

[3] Bigelow, S.: Braid groups are linear. J. Amer. Math. Soc. 14, no. 2, 471-486 (2001)

[4] Burau, W.: Über Zopfgruppen und gleichsinnig verdrillte Verkettungen. Abh. Math. Sem. Univ. Hamburg 11, 179-186 (1936)

[5] Cha, J., Ko, K., Lee, S., Han, J., Cheon, J.: An efficient implementation of braid groups. In: Boyd, C. (ed.) Advances in Cryptology - ASIACRYPT 2001 (Lect. Notes. Comp. Sc., vol. 2248) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Tokyo: Springer 2001

[6] Cheon, J., Jun, B.: A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003 (Lect. Notes. Comp. Sc., vol. 2729) Berlin Heidelberg New York Hong Kong London Milan Paris Tokyo: Springer 2003

[7] Dehornoy, P.: Braid-based cryptography. Contemporary Mathematics 360, 5-33 (2004)

[8] Garber, D., Kaplan, S., Teicher, M., Tsaban, B., Vishne, U.: Length based conjugacy search in the braid group. Preprint, http://arXiv.org/abs/math.GR/0209267

[9] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press 1999

[10] Gebhardt, V.: A New Approach to the Conjugacy Problem in Garside Groups. Preprint, http://arxiv.org/abs/math.GT/0306199

[11] Hofheinz, D., Steinwandt, R.: A Practical Attack on Some Braid Group Based Cryptographic Primitives. In: Desmedt, Y. (ed.) Public Key Cryptography - PKC 2003 (Lect. Notes. Comp. Sc., vol. 2567) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Tokyo: Springer 2003

[12] Hughes, J.: The LeftSSS attack on Ko-Lee-Cheon-Han-Kang-Park Key Agreement Protocol in B_{45}. Presentation, Rump Session CRYPTO 2000, http://www.stortek.com/hughes/Crypt2000.pdf

[13] Hughes, J.: A linear algebraic attack on the AAFG1 braid group cryptosystem. In: Batten, L., Seberry, J. (eds.) Information Security and Privacy (Lect. Notes. Comp. Sc., vol. 2384) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Tokyo: Springer 2002

[14] Hughes, J., Tannenbaum, A.: Length-based attacks for certain group based encryption rewriting systems. Workshop SECI02 SEcurité de la Communication sur Internet Sept. 2002, Tunis

[15] Ko, K.: Conjugacy Problem in Braid Groups and Applications:
III. Cryptanalytic approach to conjugacy problem and its variations via representations and linear algebra. Presentation, 10th school of Knots and Links, University of Tokyo 2003, http://kyokan.ms.u-tokyo.ac.jp/~ topology/files/KS03b.pdf

[16] Ko, K., Lee, S., Cheon, J., Han, J., Kang, J., Park, C.: New Public-key Cryptosystem Using Braid Groups. In: Bellare, M. (ed.) Advances in cryptology - CRYPTO 2000 (Lect. Notes. Comp. Sc., vol. 1880) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Singapore Tokyo: Springer 2000

[17] Krammer, D.: The braid group B_4 is linear. Invent. Math. 142 no. 3, 451-486 (2000)

[18] Krammer, D.: Braid groups are linear. Ann. of Math. (2) 155 no. 1, 131-156 (2002)

[19] Lawrence, R.: Homological representations of the Hecke algebra. Comm. Math. Phys. 135 no. 1, 141-191 (1990)

[20] Lee, E., Park, J.: Cryptanalysis of the Public-key Encryption based on Braid Groups. In: Biham, E. (ed.) Advances in cryptology - EUROCRYPT 2003 (Lect. Notes. Comp. Sc., vol. 2656) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Tokyo: Springer 2003

[21] Lee, S., Lee, E.: Potential weaknesses in the commutator key agreement protocol based on braid groups. In: Knudsen, L. (ed.) Advances in Cryptology - EUROCRYPT 2002 (Lect. Notes. Comp. Sc., vol. 2332) Berlin Heidelberg New York Barcelona Hong Kong London Milan Paris Tokyo: Springer 2002

Appendix: Complexity Analysis

For simplicity we assume that $x, y_A \in B_{2m}^+$, $a_l, a_r \in LB_m^+$, and x, a_l, a_r have the same (Artin) canonical length l. Therefore the entries in $A_{LL}^r = \rho'_m a_r$ are polynomials in $\mathbb{Q}[t]$ with degree bounded above l. According to Corollary 1 in [6] the absolute values of the numerators and denominators of the coefficients of these polynomials are bounded by $2^{|a_r|}$ and $2^{2(m-1)l}$ respectively. Let p be a prime with $p > 2^{|a_r|+2(m-1)l}$ and $f(t)$ an irreducible polynomial of degree l over $\mathbb{Z}_p$. Then we have

$$\rho'_m a_r = \frac{1}{2^{2(m-1)l}}[2^{2(m-1)l}\rho'_m a_r \mod(p, f(t))].$$

So we can work in the residue class field $F = \mathbb{Z}_p[t]/(f) \cong \mathbb{F}_{p^l}$ rather than in $\mathbb{Q}[t]$. This allows us to estimate the costs of the ring operations. Using Schönhage-Strassen method one multiplication in $\mathbb{Z}_p$ takes $O(\log p \log\log p \log\log\log p) = O^\sim(\log p) = O^\sim(|a_r|) = O^\sim(m^2 l)$ bit operations[4], and a multiplication in $\mathbb{F}_{p^l}$ takes $O(l^2)$ multiplications in $\mathbb{Z}_p$[5]. Therefore an operation in F takes $O^\sim(l^2 \log p) = O^\sim(m^2 l^3)$bit operations.

Step II): Compute $\rho'_m a_r = X_{UL}^{-1} Y_{UL}$.
The matrix inversion has the same asymptotic complexity of $O(m^{2\tau})$ operations in F as matrix multiplication. The feasible matrix multiplication exponent τ is 3 for classical algorithms, $\log_2 7$ using Strassen's method, and the current world record is $\tau < 2.376$ ([9], section 12.1). Therefore the asymptotic complexity of step II is about $O^\sim(m^{2\tau+2} l^3)$.

Step III): Invert the Lawrence-Krammer representation.
In [6] the authors errouneously assume that the complexity of their Algorithm 1 for inverting the Lawrence-Krammer representation is dominated by the computation of a power of $\rho_n \Delta_n$. This is not the case, because we can compute even powers by formula $\rho_n \Delta_n^{2k} = t^{2k} q^{2nk} \mathbb{I}_{\binom{n}{2}}$ and $\rho_n \Delta_n$ is sparse - it has the support of a permutation matrix.
Therefore the complexity of Algorithm 1 [6] is dominated by step 3.4 (for $k = 1$ to l). So Inverting $A_{LL}^r = \rho'_m a_r$ has the same complexity as computing $\rho'_m a_r$[6].
In step 3.4 we have to perform $O((m^2)^\tau)$ operations in F. That are $O(m^{2\tau} l)$ operations in $\mathbb{Z}_p$, because the (Artin) canonical length of a permutation braid is 1. Therefore step 3.4 takes $O^\sim(m^{2\tau} l \log p) = O^\sim(m^{2\tau+2} l^2)$ and the whole Algorithm 1 $O^\sim(m^{2\tau+2} l^3)$ bit operations.
Note that the precomputation of the Krammer matrices of l permutation

[4] For a precise definition of the $O^\sim$-notation see definition 25.8 in [9].
[5] Using asymptotically fast algorithms this can be reduced to $O^\sim(l)$ multiplications in $\mathbb{Z}_p$.
[6] Because the (Artin) canonical length of y_A is bounded by $3l$, step I (compute $\rho'_n x, \rho'_n y_A$) has the same complexity as step III.

braids takes $O^{\sim}(m^6 l)$ bit operations:
The Krammer matrix of an Artin generator contains at most 2 nonzero entries per column. So multiplication with $\rho'_m \sigma_j$ $(j = 1, \ldots, m-1)$ takes $O((m^2)^2)$ field operations in F, and also in $\mathbb{Z}_p$, because the (Artin) canonical length of a permutation braid is 1. Because the word length of a permutation braid b_σ is $O(m^2)$, Schönhage-Strassen multiplication takes $O^{\sim}(|b_\sigma|) = O^{\sim}(m^2)$ bit operations.

Summary: Our proposed attack requires $O^{\sim}(m^{2\tau+2} l^3)$ bit operations using Schönhage-Strassen multiplication in $\mathbb{Z}_p$ and $O(m^{2\tau+4} l^4)$ bit operations using classical multiplication.