DEFEATING THE KOTOV, MENSHOV, USHAKOV ATTACK ON WALNUTDSA$^{\mathrm{TM}}$

IRIS ANSHEL, DEREK ATKINS, DORIAN GOLDFELD, AND PAUL E. GUNNELLS
SECURERF CORPORATION
100 BEARD SAWMILL RD #350, SHELTON, CT 06484

Abstract. The Walnut Digital Signature Algorithm (WalnutDSA) is a group-theoretic, public-key method that is part of the NIST Post-Quantum Cryptography standardization process. Kotov et al proposed a heuristic algorithm to search for and remove special elements (called cloaking elements) from a WalnutDSA signature to produce a surrogate signer private key that would enable an attacker to forge signatures of any message. We show that by using appropriately chosen cloaking elements with the WalnutDSA signature, we can easily defeat this attack without any significant degredation to size or performance. The use of these cloaking elements renders WalnutDSA completely secure against this attack.

1. Introduction

The digital signature algorithm known as WalnutDSA$^{\mathrm{TM}}$ was introduced in [1]. It is a group theoretic protocol which uses non linear operations in the Artin braid group B_N [2] together with operations in $GL(N, \mathbb{F}_q)$, the $N \times N$ matrix group over the finite field $\mathbb{F}_q$ with q elements.

Recently, Kotov et al [5] proposed a heuristic algorithm which searches and removes special braid elements (called cloaking elements) from a sequence of user generated WalnutDSA digital signatures to produce a surrogate signer private key that allows an attacker to forge signatures for any message. The attack is entirely group theoretic in nature and is independent of the finite field $\mathbb{F}_q$ and matrices over this field. The attack is easily defeated by putting appropriately chosen additional cloaking elements into the WalnutDSA digital signature.

2. Brief Introduction to WalnutDSA$^{\mathrm{TM}}$

A core tool in group theoretic cryptography is the fact that an element of a group can be rewritten (using the relations in the group) so that the original expression of the element cannot be recovered. Consider, for example (for $N \geq 2$), the N-strand braid group with Artin generators $\{b_1, b_2, \ldots, b_{N-1}\}$, subject to the following relations:

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}, \qquad (i = 1, \ldots, N-2), \tag{1}$$

$$b_i b_j = b_j b_i, \qquad (|i-j| \geq 2). \tag{2}$$

Let $\mathcal{R}\colon B_N \to B_N$ denote a rewriting algorithm. Well known examples are the Birman-Ko-Lee canonical form [3] or the Dehornoy handle reduction algorithm [4]. The security of WalnutDSA$^{\mathrm{TM}}$ is based on the hard problems known as Reversing E-multiplication (REM) as well as the cloaked conjugacy search problem. E-multiplication, in its simplest form, is a function which on input of a braid element in B_N outputs a pair consisting of a matrix in $GL(N, \mathbb{F}_q)$ together with a permutation in S_N. E-multiplication is based on the colored Burau representation of the B_N [6]. Cloaking elements of B_N are defined to be braids whose output on E-multiplication is the pair consisting of the identity matrix and the identity permutation.

Fix a hash function H. In brief, the protocol begins with a message m which is first hashed to $H(m)$ and then encoded as an element $E(H(m)) \in B_N$. The signer's private key consists of two nontrivial elements in B_N, denoted w, w' (satisfying certain technical properties), and the signer's public key will be an $N \times N$

matrix over a finite field together with a permutation on N symbols, i.e., an element in the symmetric group S_N. The signed message will be a braid in B_N of the form

$$\mathcal{R}\big(v_1 \cdot w^{-1} \cdot v \cdot E(H(m)) \cdot w' \cdot v_2\big),$$

where $\mathcal{R}$ denotes a rewriting algorithm on B_N and $v, v_1, v_2 \in B_N$ are appropriate cloaking elements. Signature verification can be executed rapidly by performing E-multiplication on the signature.

3. Colored Burau Representation of the Braid Group

Each braid $\beta \in B_N$ determines a permutation in S_N (group of permutations of N letters) as follows: For $1 \leq i \leq N-1$, let $\sigma_i \in S_N$ be the i^{th} simple transposition, which maps $i \to i+1,\ i+1 \to i$, and leaves $\{1, \ldots, i-1, i+2, \ldots, N\}$ fixed. Then σ_i is associated to the Artin generator b_i. Further, if $\beta \in B_N$ is written as in (**??**), we take β to be associated to the permutation $\sigma_\beta = \sigma_{i_1} \cdots \sigma_{i_k}$. A braid is called pure if its underlying permutation is trivial (i.e., the identity permutation).

Let $\mathbb{F}_q$ denote the finite field of q elements, and for variables $t_1, t_2, \ldots, t_N$, let

$$\mathbb{F}_q[t_1, t_1^{-1}, \ldots, t_N, t_N^{-1}]$$

denote the ring of Laurent polynomials in $t_1, t_2, \ldots, t_N$ with coefficients in $\mathbb{F}_q$. Next, we introduce the colored Burau representation

$$\Pi_{CB} \colon B_N \to GL\Big(N, \mathbb{F}_q[t_1, t_1^{-1}, \ldots, t_N, t_N^{-1}]\Big) \times S_N.$$

First, we define the $N \times N$ colored Burau matrix (denoted CB) of each Artin generator as follows[**?**].

$$CB(b_1) = \begin{pmatrix} -t_1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \tag{3}$$

For $2 \leq i \leq N-1$, the matrix $CB(b_i)$ is defined by

$$CB(b_i) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & t_i & -t_i & 1 & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}, \tag{4}$$

where the indicated variables appear in row i, and if $i = 1$ the leftmost t_1 is omitted.

We similarly define $CB(b_i^{-1})$ by modifying (4) slightly:

$$CB(b_i^{-1}) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & -\frac{1}{t_{i+1}} & \frac{1}{t_{i+1}} & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix},$$

where again the indicated variables appear in row i, and if $i = 1$ the leftmost 1 is omitted.

Recall that each b_i has an associated permutation σ_i. We may then associate to each braid generator b_i (respectively, inverse generator b_i^{-1}) a colored Burau/permutation pair $(CB(b_i), \sigma_i)$ (resp., $(CB(b_i^{-1}), \sigma_i)$). We now wish to define a multiplication of such colored Burau pairs. To accomplish this, we require the following observation. Given a Laurent polynomial $f(t_1, \dots, t_N)$ in N variables, a permutation in $\sigma \in S_N$ can act (on the left) by permuting the indices of the variables. We denote this action by $f \mapsto {}^{\sigma}f$:

$$ {}^{\sigma}f(t_1, t_2, \dots, t_N) = f(t_{\sigma(1)}, t_{\sigma(2)}, \dots, t_{\sigma(N)}). $$

We extend this action to matrices over the ring of Laurent polynomials in the t_i by acting on each entry in the matrix, and denote the action by $M \mapsto {}^{\sigma}M$. The general definition for multiplying two colored Burau pairs is now defined as follows: given $b_i^{\pm}, b_j^{\pm}$, the colored Burau/permutation pair associated with the product $b_i^{\pm} \cdot b_j^{\pm}$ is

$$ (CB(b_i^{\pm}), \sigma_i) \cdot (CB(b_j^{\pm}),\ \sigma_j) = \Big(CB(b_i^{\pm}) \cdot ({}^{\sigma_i}CB(b_j^{\pm})),\ \sigma_i \cdot \sigma_j \Big). $$

We extend this definition to the braid group inductively: given any braid

$$ \beta = b_{i_1}^{\epsilon_1} b_{i_2}^{\epsilon_2} \cdots b_{i_k}^{\epsilon_k}, $$

we can define a colored Burau pair $(CB(\beta), \sigma_\beta)$ by

$$ (CB(\beta), \sigma_\beta) \ = \ (CB(b_{i_1}^{\epsilon_1}) \cdot {}^{\sigma_{i_1}}CB(b_{i_2}^{\epsilon_2}) \cdot {}^{\sigma_{i_1}\sigma_{i_2}}CB(b_{i_3}^{\epsilon_3})) \quad \cdots \quad {}^{\sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_{k-1}}}CB(b_{i_k}^{\epsilon_k}), \quad \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_k}). $$

The colored Burau representation is then defined by

$$ \Pi_{CB}(\beta) := (CB(\beta), \sigma_\beta). $$

One checks that Π_{CB} satisfies the braid relations and hence defines a representation of B_N.

4. E-Multiplication and Cloaking Elements

In brief, E-Multiplication is an action of a group of ordered pairs associated with B_N on a direct product of two groups. Given an element $\beta \in B_N$, we can associate with β both the colored Burau matrix $CB(\beta)$ (whose entries are Laurent polynomials in N variables) and the natural permutation σ_β of the braid which is an element in S_N. Since permutations themselves act on the colored Burau matrices, the ordered pairs $(CB(\beta), \sigma_\beta)$ form a group under the semi-direct product operation. By fixing a field $\mathbb{F}_q$, and a collection of N invertible elements in $\mathbb{F}_q$, $\{\tau_1, \dots, \tau_N\}$, termed t-values, we can define the right action of $(CB(\beta), \sigma_\beta)$ on the ordered pair $(M, \sigma) \in GL_N(\mathbb{F}_q) \times S_N$:

$$ (M, \sigma) \star (CB(\beta), \sigma_\beta) \ = \ \big(M \cdot {}^{\sigma}\big(CB(\beta)\big) \downarrow_{t\text{-values}}, \sigma \circ \sigma_\beta \big), $$

where the $\downarrow_{t\text{-values}}$ indicates the polynomials are evaluated at the t-values. While the Laurent polynomials which would naturally occur as entries of the colored Burau matrices would become computationally unmanageable, the generators b_i of B_N have sparse colored Burau matrices, and, hence, E-Multiplication can be evaluated very efficiently and rapidly.

The above discussion of an infinite group acting on a finite group necessitates the existence of stabilizing elements in the group B_N. With this in mind, we have the following:

Definition (Cloaking element) *Let $m \in GL(N, \mathbb{F}_q)$ and $\sigma \in S_N$. An element v in the pure braid subgroup of B_N (i.e., the permutation associated to v is the identity) is termed a cloaking element of (m, σ) if it satisfies $(m, \sigma) \star v = (m, \sigma)$.*

Thus a cloaking element will essentially disappear when E-Multiplication is evaluated. Since stabilizing elements of a group action form a subgroup, the following proposition is immediate:

Proposition 4.1. *The set of braids that cloak a specific ordered pair (m, σ) forms a subgroup of B_N.*

It should be remarked that when cloaking elements are constructed in the manner above, such elements only depend on the permutation σ. Thus, with a small abuse of language, we can say the element v cloaks for the permutation σ without any ambiguity.

Definition (κ cloaking) *Given an element $\beta \in B_N$, the output of κ iterations of randomly inserting cloaking elements into the braid β is defined to be a κ–cloaking of β and is denoted by $\kappa(\beta)$.*

5. WalnutDSA$^{\text{TM}}$ Signature Generation and Verification

For $\beta \in B_N$ let $\mathcal{P}(\beta)$ denote the E-multiplication of β against the identity element, i.e.,

$$\mathcal{P}(\beta) = (\mathrm{Id}_N, \mathrm{Id}_{S_N}) \star \beta$$

where Id_N is the $N \times N$ identity matrix and Id_{S_N} is the identity element in the symmtric group S_N. The Signer's private key consists of two random freely reduced braids $w, w' \in B_N$. The Signer's public key is $\big(\mathcal{P}(w),\, \mathcal{P}(w')\big)$.

Fix a hash function H. To sign a message $m \in \{0,1\}^*$ the Signer performs the following steps:

Digital Signature Generation:

1. Compute $H(m)$.

2. Generate cloaking elements v, v_1, and v_2 such that

– v cloaks $(\mathrm{Id}_N, \mathrm{Id}_{S_N})$,

– v_1 cloaks $\mathcal{P}(w)$.

– v_2 cloaks $\mathcal{P}(w')$.

3. Generate the encoded message $E(H(m))$.

4. Compute $\mathrm{Sig} = \mathcal{R}\big(\kappa\left(v_1 \cdot w^{-1} \cdot v \cdot E(H(m)) \cdot w' \cdot v_2\right)\big)$, which is a rewritten braid.

5. The final signature for the message m is the ordered pair $(H(m), \mathrm{Sig})$.

Signature Verification: The signature (m, Sig) is verified as follows:

1. Generate the encoded message $E(H(m))$.

2. Evaluate $\mathcal{P}(E(H(m)))$.

3. Evaluate the E-Multiplication $\mathcal{P}(w) \star \mathrm{Sig}$.

4. Test the equality

$$\mathrm{Matrix}\Big(\mathcal{P}(w) \star \mathrm{Sig}\Big) \overset{?}{=} \mathrm{Matrix}\Big(\mathcal{P}\big(E(H(m))\big)\Big) \cdot \mathrm{Matrix}\Big(\mathcal{P}\big(w'\big)\Big), \tag{5}$$

where Matrix denotes the matrix part of the ordered pair in question, and the multiplication on the right is the usual matrix multiplication. The signature is valid if and only if (5) holds and the signature has length $\leq 2L$ where L is a certain positive integer such that all valid WalnutDSA$^{\text{TM}}$ signatures have length in the range $[L, 2L]$.

6. The Kotov, Menshov, Ushakov Attack

The attack proceeds by collecting a number of messages, together with their associated WalnutDSA signatures, which have all been generated by a single user whose private key is denoted by (w, w').

Next, a heuristic method is used on each of the signatures to search and remove the specified cloaking elements v, v_1, v_2 from each of the signatures. The search relies on the attacker knowing the permutations that each of the three cloaking elements v, v_1, v_2 are cloaking for.

Letting σ denote one of these permutations, the attacker searches for locations in a signature where $\sigma^{-1}(a)$ and $\sigma^{-1}(b)$ are switched (see [1] for the discussion of τ_a, τ_b). This can be explained as follows. Since a braid in B_N is a configuration of strands connecting N equally spaced points on a line with another N equally spaced points on a parallel line, one can search for subwords of the braid with the property that the strand starting at the point $\sigma^{-1}(a)$ crosses the strand starting at the point $\sigma^{-1}(b)$. The attack further assumes that cloaking elements are of the form $ub_i^{\pm 2}u^{-1}$ (i.e., a conjugate) where the permutation associated to u maps i to $\sigma^{-1}(a)$ and $i+1$ to $\sigma^{-1}(b)$. Writing $ub_i^{\pm 2}u^{-1} = ub_i^{\epsilon}b_i^{\epsilon}u^{-1}$ with $\epsilon = \pm 1$ the attack attempts to find the location of b_i^{ϵ} and replaces it with its inverse $b_i^{-\epsilon}$ resulting in the cloaking element turning into $ub_i^{-\epsilon}b_i^{\epsilon}u^{-1} = \mathrm{Id}$ where Id is the identity element in the braid group. If successful, this procedure effectively deletes the cloaking element. These manipulations do not always work. To make the attack more effective Kotov et al [5] perform the above procedure many times on a pair of signatures S_1, S_2 generating two lists of altered signatures $\{S_1^{(1)}, \ldots, S_1^{(k)}\}$, $\{S_2^{(1)}, \ldots, S_2^{(\ell)}\}$. The attack attempts to braid minimize

$$\left(S_1^{(i)}\right) \cdot \left(S_2^{(j)}\right)^{-1}, \qquad (\text{for } 1 \le i \le k,\ 1 \le j \le \ell),$$

which may remove the cloaking element. Since it is assumed that there are only three cloaking elements which cloak for known permutations the heuristic attack proceeds as above to systematically remove the three cloaking elements.

If the three cloaking elements are successfully removed it is then possible to construct a surrogate for the private key (w, w') of the signer as follows. With the cloaking elements removed, the signature of a message m_i takes the form

$$\mathrm{Sig}(m_i) = w^{-1} \cdot E(H(m_i)) \cdot w'.$$

Assuming that the attacker has signatures for k messages, $m_1, \ldots, m_k$, the sequence of products

$$\mathrm{Sig}(m_i) \cdot \mathrm{Sig}(m_{i+1})^{-1} = w^{-1} \cdot E(H(m_i)) \cdot E(H(m_{i+1}))^{-1} \cdot w,$$

yield a set of simultaneous conjugacy equations whose solution will be a surrogate of the signer's private key. This surrogate private key can then be used to forge signatures of further messages.

7. Defeating the attack

The heuristic attack of Kotov et al [5] can be easily defeated by introducing concealed cloaking elements into the WalnutDSA signature. Following [1], we fix a braid β, say

$$\beta = b_{i_1}^{\epsilon_1} \cdots b_{i_\ell}^{\epsilon_\ell},$$

and choose some point $1 \le k \le \ell$. Clearly, $\beta = x_1 \cdot x_2$ where $x_1 = b_{i_1}^{\epsilon_1} \cdots b_{i_{k-1}}^{\epsilon_{k-1}}$ and $x_2 = b_{i_k}^{\epsilon_k} \cdots b_{i_\ell}^{\epsilon_\ell}$, and, hence, for any matrix/permutation pair (m_0, σ_0), we have that $(m_0, \sigma_0) \star \beta = ((m_0, \sigma_0) \star x_1) \star x_2$.

We can generate a cloaking element v for the product of $\sigma_0 \cdot \sigma_{x_1}$ where σ_{x_1} deotes the permutation associated with x_1. By construction, given any matrix M we have that $(M, \sigma_0 \cdot \sigma_{x_1}) \star v = (M, \sigma_0 \cdot \sigma_{x_1})$. Since $(m_0, \sigma_0) \star x_1$ takes the form $(m_0, \sigma_0) \star x_1 = (M, , \sigma_0 \cdot \sigma_{x_1})$. It follows that

$$\begin{aligned}(m_0, \sigma_0) \star \beta &= ((m_0, \sigma_0) \star x_1) \star x_2 \\ &= (M, \sigma_0 \cdot \sigma_{x_1}) \star x_2 \\ &= (M, \sigma_0 \cdot \sigma_{x_1}) \star v \star x_2 \\ &= ((m_0, \sigma_0) \star x_1) \star v \star x_2 = (m_0, \sigma_0) \star x_1 \star v \star x_2.\end{aligned}$$

Hence we have generated a new braid β' which contains v,

$$\beta' = x_1 \cdot v \cdot x_2,$$

which has the property that $(m_0, \sigma_0) \star \beta = (m_0, \sigma_0) \star \beta'$. We shall refer to this inserted cloaking element as a *concealed* cloaking element.

It is the presence of κ concealed cloaking elements (for sufficiently large κ) that effectively blocks this attack. The key point is that for concealed cloaking elements we do not know the permutation that is being cloaked. In general, knowing that κ concealed cloaking elements have been placed in a nested fashion in a known braid, it would require $(N!)^\kappa$ searches to find them. To insure κ-bit security we would require

$$(N!)^\kappa > 2^\kappa,$$

and hence

$$\kappa > \text{Security Level}/\log_2(N!).$$

We have explored possible birthday attacks and have ruled out obvious ways to use a birthday attack to discover all the concealed cloaking elements. Indeed, multiple cloaking elements could use the same permutation but each would still need to individually be discovered. Without access to a birthday attack, in the case of $N = 10$, and a security level of 128 we can comfortably take $\kappa = 6$ (which results in a work factor of $2^{130.74}$). Likewise, when $N = 10$ and the security level is 256, taking $\kappa = 12$ is sufficient (resulting in a work factor of $2^{261.49}$).

We also note that concealed cloaking elements have a secondary purpose in blocking this attack. Recall that the attack not only relies on knowing the permutation being cloaked, but it also relies on a cloaking element being in the form of a conjugate. By placing a concealed cloaking element inside one side, e.g. converting $v = ub_i^{\pm 2}u^{-1}$ to $v = \kappa(u)b_i^{\pm 2}u^{-1}$, we block the attack in both ways. Specifically, while the permutation v is cloaking for is known, it is no longer a conjugate, and while the inner-most concealed cloaking element is a conjugate, the permutation it is cloaking for is not known.

With $N = 10$, a cloaking element using a random permutation for u averages 87.16 Artin generators (with a standard deviation of 22.03). This can be shortened by choosing the permutation of u carefully (note that this is different than the permutation being cloaked). If we add 6 concealed cloaking elements (necessary for 128-bit security), this implies an average signature-size increase of approximately 523 generators. However, after running BKL and Dehornoy, additional size reductions can be made. This results in an average signature increase from 1909 to 2037 Artin generators, or an increase in only 6.7%.

Because signature validation performance is linearly correlated with the length of the signature, this 6.7% average length increase results in a 6.7% increase in the average time required to validate signatures.

8. Conclusion

WalnutDSA is a group-theoretic, public-key method that is part of the NIST Post-Quantum Cryptography standardization process. Kotov et al proposed a heuristic algorithm to search for and remove cloaking elements from a WalnutDSA signature to produce a surrogate signer private key which allows an attacker to forge signatures of any message. We show that by putting in additional, concealed cloaking elements into the WalnutDSA signature we can easily defeat this attack without any significant degredation to size or performance, rendering WalnutDSA completely secure against this attack.

Specifically, we find that when we add a sufficient number of concealed cloaking elements to block the attack to a 128-bit security level we see only a 6.7% increase in signature size on average, which results in an equivalent 6.7% increase in signature verification time. This enables WalnutDSA to remain secure and performant on all supported platforms.

References

[1] Anshel, I., Atkins, D., Goldfeld, D., Gunnells, P.E.:WalnutDSA$^{\text{TM}}$: a quantum-resistant digital signature algorithm. Cryptology ePrint Archive, Report 2017/058 (2017).

[2] E. Artin, Theory of braids, *Ann. of Math.* (2) 48 (1947), 101–126.

[3] J. Birman; K. H. Ko; S. J. Lee, A new approach to the word and conjugacy problems in the braid groups, Adv. Math. 139 (1998), no. 2, 322–353.

[4] P. Dehornoy, A fast method for comparing braids, Adv. Math. 125 (1997), no. 2, 200–235.

[5] M. Kotov; A. Menshov; A. Ushakov, An attack on the Walnut digital signature algorithm, Cryptology ePrint Archive: Report 2018/393 (2018).

[6] H.R. Morton, The multivariable Alexander polynomial for a closed braid, Low-dimensional topology, (Funchal, 1998), 167–172, Contemp. Math., 233, Amer. Math. Soc., Providence, RI, 1999.

Email address: IANSHEL@SECURERF.COM, DATKINS@SECURERF.COM, DGOLDFELD@SECURERF.COM, PGUNNELLS@SECURERF.COM