DEFEATING THE MERZ–PETIT ATTACK ON WALNUTDSA$^{\text{TM}}$

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 quantum-resistant, group-theoretic, public-key method. Merz and Petit found that by using the Garside Normal Form of a WalnutDSA signature they could discover traces of the Garside form of the original encoded message, and use that knowledge to create a forgery. We show (and Merz and Petit agree) that by adding sufficient cloaking elements into the message encoding within the signature, the Garside form is aduquately modified that no traces can be found and that forgeries can no longer be made. With this small addition, WalnutDSA signatures become completely immune to this attack.

1. Introduction

The digital signature algorithm known as WalnutDSA$^{\text{TM}}$ 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, Merz and Petit [6] proposed a practical forgery attack on WalnutDSA$^{\text{TM}}$. They found that using the Garside Normal Form of the signature allowed them to find commonalities with the Garside form of the encoded message, and using those commonalities they could create a forgery. As pointed out by the authors, the attack can be defeated by adding cloaking elements into the encoded message. Specifically, they conjecture that each additional cloaking element effectively mutates approximately five (5) permutation braids in the Garside Normal Form, but, when mutated, their attack no longer succeeds.

In this paper we show that with a sufficient number of cloaking elements their attack fails to create forgeries.

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

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$^{\text{TM}}$ 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 [7]. 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 $f(t_1, \ldots, t_N)$ 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 $f \mapsto {}^{\sigma}f$:

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

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

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

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 $\mathbb{F}_q$, $\{\tau_1, \ldots, \tau_N\}$, 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$^{\mathrm{TM}}$ signatures have length in the range $[L, 2L]$.

6. The Merz–Petit Attack

Before describing the Garside based approach proposed by Merz–Petit [6] we review some of the basic components Garside introduced to the field which date back to 1965. Recalling that the Artin presentation of the N strand braid group has generators $\{b_1, b_2, \ldots, b_{N-1}\}$, subject to the following relations:

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}, \qquad (i = 1, \ldots, N-2),$$
$$b_i b_j = b_j b_i, \qquad (|i-j| \geq 2).$$

A brief summary of Garside's approach [5] proceeds as follows. The fundamental braid Δ_N, which is defined to be

$$\Delta_N = (b_1 \cdots b_{N-1})(b_1 \cdots b_{N-2}) \cdots (b_1 b_2)\, b_1,$$

satisfies the properties: for $i = 1, \ldots, N-1$,

$$b_i \Delta = \Delta b_{N-i} \quad b_i^{-1} = x_i \Delta^{-1},$$

where x_i is a positive word in the generators (i.e., a word without negative exponents). Focussing on positive words in the braid generators, denoted B_N^+ enabled Garside to introduce an ordering of positive words: given two positive words $a, b \in B_N^+$ then $a \leq b$ if there exists a $c \in B_N^+$ such that $ac = b$. Further, given said $a, b \in B_N^+$ we can look for the smallest positive braid d such that $d \leq a$ and $d \leq b$. Garside proved such a smallest d exists and is unique (it is often denoted $a \wedge b$). Garside's seminal theorem states that every braid β can be uniquely expressed in the form

$$\Delta^r \, A_1 \cdots A_k,$$

where $r \in \mathbb{Z}$, $1 < A_i < \Delta$, and $A_i \, A_{i+1} \wedge \Delta = A_i$.

The underlying mathematical structure supporting the WalnutDSA protocol is the action of the braid group on a direct product of a large finite matrix group and a symmetric group. The action is inherently algorithmically difficult to reverse, and finding stabilizers (termed cloaking elements) is likewise a difficult problem. However, specialized classes of cloaking elements can be explicitly generated and it is, hence, possible to use them as a means of obscuring a braid: by inserting sufficiently many cloaking elements the structure of the original braid cannot be recovered in a tractable way.

The Merz and Petit universal forgery attack is a heuristic method that, using knowledge of a valid signature of a message M, aims to generate a signature of a second message M' that will be validated by a receiver. The decomposition algorithm introduced in their paper (which uses the Garside canonical for as its basis) can be applied because a Walnut signature has the form

$$W_1 E(H(M)) W_2$$

and, critically, the braid element $E(H(M))$ is known to everyone. Knowledge of $E(H(M))$ allows the algorithm to try to derive braids W_1', W_2' which satisfy the conditions $W_i \equiv W_i'$ (Mod Δ^2), and $W_1 \cdot W_2 \; = \; W_1' \cdot W_2'$. Once a forger has said elements in place, the braid $W_1' \cdot E\big(H(M')\big) \cdot W_2'$ will verify as a signature of a message M'.

In fact, knowledge of the entire $E(H(M))$ is not actually requisite. Were one to insert a single concealed cloaking element into the encoding $E(H(M))$ it is still possible that the A_i's in the Garside normal form (see above) of said encoding still appear in the Garside normal form for the signature. While the forgery in this case would be longer than the average signature, it might be within the acceptable length range. Thus, in order to completely thwart the heuristic attack, the signer must insert sufficiently many concealed cloaking elements into the braid $E(H(M))$ to completely alter the Garside normal form. We have done significant testing and have concluded that inserting cloaking elements every 10-15 generators will suffice. It should be noted that the approaches to removing cloaking elements required the attacker to be able to reduce the problem to a conjugacy search problem, Finding concealed cloaking elements in the encoded message does not fit into that effort.

7. Conclusion

WalnutDSA is a quantum-resistant, group-theoretic, public-key method. Merz and Petit proposed a practical forgery attack using the Garside Normal Form of the signature that allowed them to find commonalities with the Garside form of the encoded message, and using those commonalities they could create a forgery. We have shown that by inserting a modest number of cloaking elements in the encoded message we can change the resulting Garside form, rendering WalnutDSA completely secure against this attack.

References

[1] Anshel, I., Atkins, D., Goldfeld, D., Gunnells, P.E.:WalnutDSA$^{\mathrm{TM}}$: 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] Garside, F.A., The braid group and other groups. The Quarterly Journal of Mathematics bf 20(1), 235–254 (1969).

[6] Merz S.P., Petit C. (2018) *Factoring Products of Braids via Garside Normal Form,* https://eprint.iacr.org/2018/1142.

[7] 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