KU LEUVEN

Practical Attacks on the Walnut Signature Scheme

Ward Beullens   Simon R. Blackburn

KU Leuven
Royal Holloway

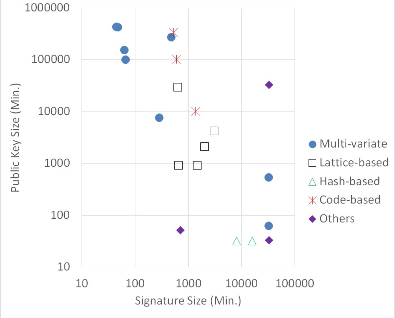
December 2, 2018

WalnutDSA is a Signature Scheme submitted to the NIST PQC project.

Small signatures and keys (best combined size of all submissions)

Very fast key generation and verification

Is used in the real world! ⚠



Size Comparison (Signature)

1. Preliminaries
   - Braid groups
   - WalnutDSA
2. Attacks
   - Collision search attack
   - Factorization attack
   - Inverting the group action attack
3. Conclusion

1. Preliminaries
   - Braid groups
   - WalnutDSA
2. Attacks
   - Collision search attack
   - Factorization attack
   - Inverting the group action attack
3. Conclusion

Figure: A braid

A braid of order N is a collection of strings connecting N upper points to N lower points.

Two braids are equivalent if one can be deformed continuously into the other.

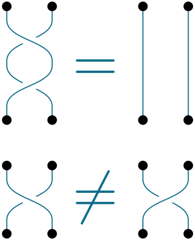


Figure: Equivalence of braids

We can compose braids and invert them. Equivalence classes of braids of order N form a group B_N.

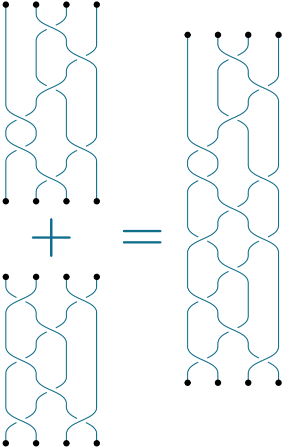


Figure: Composition of braids

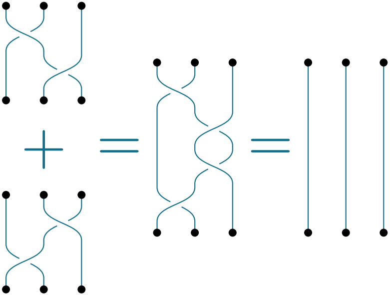


Figure: Inverse of a braid

Algebraic definition of braid groups

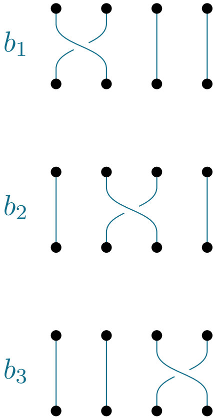


Figure: The three Artin generators b_1, b_2 and b_3 that generate B_4.

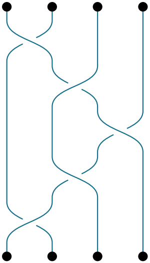


Figure: The braid $b_1 b_2^{-1} b_3 b_2 b_1^{-1}$

Braid group B_N is generated by a set of $N-1$ generators.

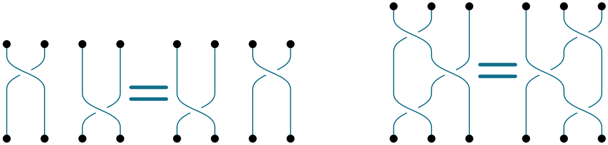


Figure: Relations $b_1 b_3 = b_3 b_1$ (left) and $b_1 b_2 b_1 = b_2 b_1 b_2$ (right).

Theorem (Artin and Bohnenblust, 1946)
These are the only relations between the generators. The braid groups have a purely algebraic definition.

$$B_N = \left\langle b_1, \cdots, b_{N-1} \;\middle|\; \begin{array}{cc} b_i b_j = b_j b_i & \text{for } 1 \leq i < j < N \text{ and } j - i \geq 2 \\ b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} & \text{for } 1 \leq i < N-1 \end{array} \right\rangle .$$

There is a natural homomorphism $\sigma : B_N \to S_N$ that assigns a permutation to each braid.

A braid that maps to the identity permutation is called *pure*.

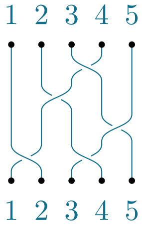


Figure: A braid with underlying permutation $(124)(35)$.

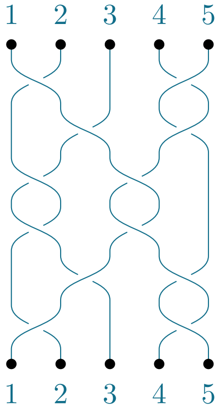


Figure: A pure braid.

WalnutDSA uses a new (right) group action
$\star : B_N \curvearrowright GL(\mathbb{Z}_p, N) \times S_N$, called E-multiplication.

$$(M, \pi) \star b := (M \cdot Mat(b, \pi), \pi\sigma(b))$$

We define $\mathcal{P} : B_N \to GL(\mathbb{Z}_p, N) \times S_N$ by acting on $(1_N, e)$

$$\mathcal{P}(b) := (1_N, e) \star b, .$$

When restricted to P_N, $\mathcal{P} : P_N \to GL(\mathbb{Z}_p, N)$ is a group morphism.

For all N, there is a braid groups B_N, which has a subgroup P_N.

We saw 3 objects:

1. σ, a group morphism that takes a braid and outputs a permutation
2. E-multiplication $(\star)$, a group action of B_N on $GL(\mathbb{Z}_p, N) \times S_N$.
3. $\mathcal{P}(s) := (1_N, e) \star s$ is a group morphism when restricted to pure braids.

Secret key

Two random secret braids s_1, s_2.

Public key

The result of acting on $(1_N, e)$ with s_1, s_2 i.e. $\mathcal{P}(s_1), \mathcal{P}(s_2)$

Signature

A signature for document d is a braid s such that

$$\mathcal{P}(s_1) \star s = \mathcal{P}(E(d)) \star s_2$$

where E is an encoding function that takes a document and outputs a pure braid.

Remark: This can be verified from public information.

1. Preliminaries
   - Braid groups
   - WalnutDSA
2. Attacks
   - Collision search attack
   - Factorization attack
   - Inverting the group action attack
3. Conclusion

A signature sig is valid for document d if

$$\mathcal{P}(s_1) \star \mathsf{sig} = \mathcal{P}(E(d)) \star s_2 \,.$$

The only dependence on d is through $\mathcal{P}(E(d))$. If we can find d_1, d_2 such that $\mathcal{P}(E(d_1)) = \mathcal{P}(E(d_2))$ we can break EUF-CMA security of the signature scheme.

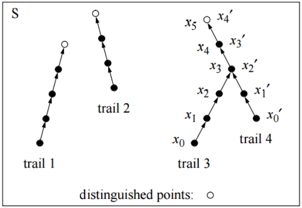
The first step in calculating E is a cryptographic hash function

$\downarrow$

Nothing better than a generic collision search.

Distinguished point method: (Van Oorschot , Wiener)

Collision search in a function $f : D \to D$ takes $|D|^{\frac{1}{2}}$ function evaluations.



$|\mathcal{P}(E(\{0,1\}^*))| \approx q^{13}$ $\Rightarrow$ Collision search in $q^{6.5}$ function evaluations

$2^{37.5}$ for SL1
2^{60} for SL5

Finding the following collision took 1 hour on a desktop PC.

$d_1 =$`"I would like to receive 915665927010966 7494 free samples of chocolate chip cookies."`

$d_2 =$`"I would like to receive 10213941738370235726 free samples of gluten-free raisin cookies."`

Adversaries can use this attack if they can hide ± 50 bits of entropy in plausible looking messages.

The designers of Walnut adopted 2 countermeasures:

1. Change the encoding mechanism E

   $\downarrow$

   $\dim(\mathcal{P}(E(0,1^*)))$ is now $(N-2)^2+1$ instead of 13.
2. Increase N from 8 to 10

this results in:
Key size +50%
Signature size +25%

The idea is to collect signatures $\mathsf{sig}_1, \cdots, \mathsf{sig}_k$ for some documents $d_1, \cdots, d_k$. Compute the matrices $M_i = \mathcal{P}(E(d_i))$.

To forge a signature for a document d, write $M = \mathcal{P}(E(d))$ as a product of the M_i, and use this factorization to combine the signatures sig_i into a signature sig for d.

We adapted an attack by Hart, Kim, Micheli, Perez, Petit and Quek (Oxford & Birmingham) on an earlier version of Walnut.

The attack works fast in practice, but the signatures are much longer than honest signatures (2^{32} vs 2^{12}) $\Rightarrow$ not useful in practice.

Simple countermeasure: Impose a length limit on signatures.

A signature sig is valid for document d if

$$\mathcal{P}(s_1) \star \mathsf{sig} = \mathcal{P}(E(d)) \star s_2\,.$$

Hard problem

Given (M_1, π_1) and (M_2, π_2) find a (short) braid s such that

$$(M_1, \pi_1) \star s = (M_2, \pi_2).$$

Solution

Step 1 : Reduce to the case $(M, \pi) \star s = (1_N, e)$
Step 2 : Solve the problem using the chain of subgroups.

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset P_N \subset B_N$$

$$(M, \pi) = \left(\begin{pmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \pi \right)$$

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset P_N \subset B_N$$

Step 0: Pick s' in B_N whose permutation is π^{-1}.

$$(M,\pi)\star s' = \left(\begin{pmatrix} * & * & * & * & * & {\color{red}*} \\ * & * & * & * & * & {\color{red}*} \\ * & * & * & * & * & {\color{red}*} \\ 0 & 0 & 0 & * & * & {\color{red}*} \\ 0 & 0 & 0 & 0 & {\color{red}*} & {\color{red}*} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, e\right)$$

We got three rows of zeros for free!

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset {\color{red}P_N} \subset B_N$$

Step 1: Find s_1 that kills the last column. $O(q^{N/2})$

Observation: A braid in P_i acts as multiplication by a matrix that only differs from the identity matrix in the upper left i-by-i matrix.

$$(M, \pi) \star s' \cdot s_1 = \left(\begin{pmatrix} * & * & * & * & * & 0 \\ * & * & * & * & * & 0 \\ * & * & * & * & * & 0 \\ 0 & 0 & 0 & * & * & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, e \right)$$

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset P_N \subset B_N$$

Step 2: Pick s_2 that kills the $(N-1)$-th column. $O\left(q^{\frac{N-1}{2}}\right)$

Observation: A braid in P_i acts as multiplication by a matrix that only differs from the identity matrix in the upper left i-by-i matrix.

$$(M,\pi) \star s' \cdot s_1 \cdot s_2 = \left(\begin{pmatrix} * & * & * & * & 0 & 0 \\ * & * & * & * & 0 & 0 \\ * & * & * & * & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, e \right)$$

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset P_N \subset B_N$$

Step i : Pick s_i that kills the $(N+1-i)$-th column. $O\left(q^{N-i/2}\right)$

Observation: A braid in P_i acts as multiplication by a matrix that only differs from the identity matrix in the upper left i-by-i matrix.

$$(M, \pi) \star s' \cdot s_1 \cdot \ldots \cdot s_N = \left(\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, e \right)$$

$$\{e\} = P_1 \subset P_2 \subset \cdots \subset P_{N-1} \subset P_N \subset B_N$$

Most expensive step is $O\left(q^{N-3/2}\right)$, but we can improve this to $O\left(q^{N/2-1}\right)$ at cost of slightly larger signatures (but still small enough).

forging signature for 128-bit secure parameters: $< 1s$
forging signature for 256-bit secure parameters: $39s$

Parameters	Original	New	Increase
N	8	10	
q	2^5	$2^{31} - 1$	
Public key length	83 Bytes	780 Bytes	$\times 9.4$
Signature length	713 Bytes	1308 Bytes	$+83\%$
Signing time	39.5 ms	59.2 ms	$+50\%$
Verification time	0.05 ms	0.09 ms	$+80\%$

1. Preliminaries
   - Braid groups
   - WalnutDSA
2. Attacks
   - Collision search attack
   - Factorization attack
   - Inverting the group action attack
3. Conclusion

- Original parameters are totally broken
- New sizes are comparable to lattice signature schemes.
- Latest iteration of Walnut seems broken by the Kotov, Menshov and Ushakov attack.
- Despite this Walnut is still being pushed into the wild ⚠

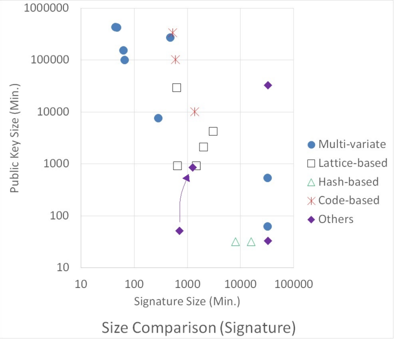


Figure: Updated key and signature sizes.