Walnut Digital Signature Algorithm (WalnutDSA)

NIST Post Quantum Standardization Conference

Derek Atkins,
Chief Technology Officer

SECURE RF
Securing the Internet of Things®

April 11, 2018

WalnutDSA Method Overview

- Group-theoretic digital signature method based on:
  - Infinite group theory
  - Matrices over small finite fields
  - Permutations
- Built on *E*-Multiplication, one-way function published in 2005
- Key generation and signature verification are very fast
- Key and signature size (and therefore signature validation time) scales linearly with security – counteracts Grover
- Non-cyclic and non-abelian; HSP does not apply – not subject to Shor
- All known attacks are exponential and blocked by parameter-only changes

SECURE RF
Securing the Internet of Things®

WalnutDSA Structure

- **Systemwide Data:**
  - Braid Group: N
  - Finite Field: q
  - Encoder function: $E()$ – converts a hash string to a braid
- **Private Key:**
  - Braid Pair: Priv(S), Priv(S')
- **Public Key:**
  - T-Values: $\{\tau_1 \cdots \tau_N\}$ (non-zero entries in F_q)
  - Pub(S): Matrix + Permutation: (1,1) $\star$ Priv(S)
  - Pub(S'): MatrixPart of (1,1) $\star$ Priv(S')
- **Signature over hashed message $\mathcal{M}$:**
  - Sig: $\mathcal{R}\left(v_3 \cdot \mathrm{Priv(S)}^{-1} \cdot v_1 \cdot E(\mathcal{M}) \cdot \mathrm{Priv(S')} \cdot v_2\right) \in B_N$, where $\mathcal{R}$ is a rewriting method and the v_i (cloaking elements) disappear under $\star$
- **Verification:**
  - Verify signature length (2^{14} generator limit)
  - Compute M_1 =MatrixPart$((\mathrm{Id}_N, \mathrm{Id}_{S_N}) \star E(\mathcal{M}))$ · Pub(S')
  - Compute $(M_2, \sigma_2) =$ Pub(S) $\star$ Sig
  - Compare M_1 and M_2 for equality

SECURE RF
Securing the Internet of Things®

Issues Found

Factoring Attack(s)

- **Oxford Attack (prior to NIST):** Hart *et al* found a way to factor public keys and generate extremely long forged signatures when the private braids are the same. The shortest forgery they created was 2^{35} Artin generators.
  REFUTED: Maximum allowed signature length is 2^{16} generators. Conjectured shortest forgery is still 2^{20} generators ($> 2^{16}$).
- **Modifications:** It was shown by W. Beullens how to extend the Oxford factoring attack even when the private braids are different. Resulting forgeries are double the Oxford length.
  REFUTED: Conjectured shortest forgery is still 2^{21}, which is much longer than the allowed maximum of 2^{16}. We propose to further reduce the maximum to 2^{14}.

Issues Found

Pollard-rho Attack

- **Pollard-rho Attack:** A Pollard-rho attack (found by S. Blackburn) showed that the parameters were too small resulting in an insufficient number of public keys. Specifically, N and q must satisfy the inequality $q^{N(N-3)-1} > 2^{2*\mathrm{SecurityLevel}}$.

  ANSWERED: Increasing parameter N from 8 to 10 (without modifying q) defeats this attack.

Issues Found

Encoder Issues

- **Non-Injective Encoder:** It was pointed out by W. Beullens that the encoder, as specified, was non-injective which reduced the space of possible signatures.
  ANSWERED: Use a two-bit encoder to create an injective map from hash output to braid word.
- **Encoder Dimension** It was pointed out by Beullens that the message encoder generated a vector space with a dimension that was too small. Specifically, vector dimension must satisfy the inequality $q^{\text{dimension}} > 2^{2*\text{SecurityLevel}}$.
  ANSWERED: Change encoding parameters to injectively leverage the full space; results in dimension 66 for $N = 10$ which is sufficiently large to defeat these attacks without modifying q.

SECURE RF
Securing the Internet of Things®

Issues Found

Exponential Factoring Attack

- **Exponential Attack** Beullens and Blackburn found another exponential factoring attack that leveraged $t_1 = t_2 = 1$ and was able to produce forged private keys resulting in signatures short enough to be considered valid. The attack runs in $q^{N-5/2}$ time, but they claim they can reduce that to $q^{N/2-1}$.

  ANSWERED: Assuming their worst-case can be verified, increasing parameters N and q to 11 and $2^{31} - 1$ (M31) achieves 128-bit security (and B11M61 achieves 256-bit).

  With q prime we can also tweak cloaking elements and no longer require $t_1 = t_2 = 1$, further complicating this type of attack, increasing work to $q^{(N-1)/2}\sqrt{60}$, allowing us to reduce to B10. Performance impact is minimal (e.g. 175,285 cycles to verify a signature – still #1).

Performance

- Small implementation of verification function (~3000 bytes of code)
- 7 of the 8 submitted WalnutDSA implementations were the FASTEST signature verifications as reported by NIST:

	Submission	Specific Implementation	KeyPair Med	Keypair Ave	Sign Median	Sign Average	Open Med	Open Ave	sk	pk	bytes
2	WalnutDSA	walnut128-bkl	1782814	2086564	126822981	137691863	92699	96962	136	83	1100
3	WalnutDSA	walnut128-stochasticrewrite	1905902	2271199	45760337	51244842	95682	101529	136	83	1200
4	WalnutDSA	walnut128-stochasticrewriten	1935044	2574824	43111043	48246052	133359	147948	136	83	2000
5	WalnutDSA	walnut128-ref	1135380	1225046	2039841350	2071390234	166520	175770	136	83	1100
6	WalnutDSA	walnut256-ref	1162870	1255020	2026491143	2084771866	168897	193637	291	128	1800
7	WalnutDSA	walnut256-stochasticrewrite	4164257	4519863	127413278	134509781	181122	194916	291	128	2100
8	WalnutDSA	walnut256-bkl	4149445	4456087	454977624	472468875	179665	197243	291	128	1800

- The proposed increases in parameters still keeps WalnutDSA #1 (175,285 cycles)

SECURE RF
Securing the Internet of Things®

Summary

- Small code implementation
- Fast runtime
- Lots of analysis since this process began
- All attacks identified have been exponential and handled with parameter-only changes, typically within hours or days of notification
- Analysis has identified notable improvements we will include in the next round
- We feel WalnutDSA is an innovative alternative to Lattice/Hash methods and should continue to be studied in this process

Thank You!

Any Questions?

Derek Atkins, CTO
Phone: +1 203.227.3151
Email: DAtkins@SecureRF.com

SECURE RF
Securing the Internet of Things®