DRS
Diagonal dominant Reduction for lattice-based Signature

Thomas PLANTARD, Arnaud SIPASSEUTH, Cedric DUMONDELLE, Willy SUSILO

Institute of Cybersecurity and Cryptology
University of Wollongong

http://www.uow.edu.au/~thomaspl
thomaspl@uow.edu.au

13 April 2018

Outline

General Description

Lattice based Digital Signature

- Work proposed in PKC 2008 **without** existing **attack**.
- Initially proposed to make GGHSign resistant to **parallelepiped** attacks.
- Modified to gain efficiency: avoid costly **Hermite Normal Form**.

General Description

Lattice based Digital Signature

- Work proposed in PKC 2008 **without** existing **attack**.
- Initially proposed to make GGHSign resistant to **parallelepiped** attacks.
- Modified to gain efficiency: avoid costly **Hermite Normal Form**.

Lattice based Digital Signature

- Secret key: **Diagonal Dominant** Basis $B = D - M$ of a lattice $\mathcal{L}$
- Public key: A basis P of the same lattice $P = UB$
- Signature of a message m: a vector s such that $(m - s) \in \mathcal{L}$ and $\|s\|_\infty < D$
- Signature security related to GDD_∞.

Secret Key

- A diagonal Dominant Basis with N_b $\pm b$ and N_1 ± 1.
- With a **cyclic** structure **but for the signs**.

Secret Key

- A diagonal Dominant Basis with N_b $\pm b$ and N_1 ± 1.
- With a **cyclic** structure **but for the signs**.

$$B = \begin{pmatrix} D & \pm1 & \pm1 & \pm b & 0 & \pm b & \pm1 & 0 & \pm1 & 0 \\ 0 & D & \pm1 & \pm1 & \pm b & 0 & \pm b & \pm1 & 0 & \pm1 \\ \pm1 & 0 & D & 1 & 1 & \pm b & 0 & \pm b & \pm1 & 0 \\ 0 & \pm1 & 0 & D & \pm1 & \pm1 & \pm b & 0 & \pm b & \pm1 \\ \pm1 & 0 & \pm1 & 0 & D & \pm1 & \pm1 & \pm b & 0 & \pm b \\ \pm b & \pm1 & 0 & \pm1 & 0 & D & \pm1 & \pm1 & \pm b & 0 \\ 0 & \pm b & \pm1 & 0 & \pm1 & 0 & D & \pm1 & \pm1 & \pm b \\ \pm b & 0 & \pm b & \pm1 & 0 & \pm1 & 0 & D & \pm1 & \pm1 \\ \pm1 & \pm b & 0 & \pm b & \pm1 & 0 & \pm1 & 0 & D & \pm1 \\ \pm1 & \pm1 & \pm b & 0 & \pm b & \pm1 & 0 & \pm1 & 0 & D \end{pmatrix}$$

Secret Key

- A diagonal Dominant Basis with N_b $\pm b$ and N_1 ± 1.
- With a **cyclic** structure **but for the signs**.

$$B = \begin{pmatrix} D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 \\ 0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 \\ \pm 1 & 0 & D & 1 & 1 & \pm b & 0 & \pm b & \pm 1 & 0 \\ 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 \\ \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b \\ \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 \\ 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b \\ \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 \\ \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 \\ \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D \end{pmatrix}$$

- Growing b creates a gap between Euclidean Norm and Manhattan Norm
- Cyclic structure to guarantee $\|M\|_\infty = \|M\|_1$

Public Key

- $P = UB$ with $U = P_{R+1} T_R P_R ... T_1 P_1$
- With P_i a random permutation matrix and

Public Key

- $P = UB$ with $U = P_{R+1} T_R P_R ... T_1 P_1$
- With P_i a random permutation matrix and

$$T_i = \begin{pmatrix} A^{\pm 1} & 0 & 0 & 0 \\ 0 & A^{\pm 1} & 0 & 0 \\ 0 & 0 & A^{\pm 1} & 0 \\ 0 & 0 & 0 & A^{\pm 1} \end{pmatrix}$$

with

$$A^{+1} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, A^{-1} = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}$$

Public Key

- $P = UB$ with $U = P_{R+1}T_RP_R...T_1P_1$
- With P_i a random permutation matrix and

$$T_i = \begin{pmatrix} A^{\pm 1} & 0 & 0 & 0 \\ 0 & A^{\pm 1} & 0 & 0 \\ 0 & 0 & A^{\pm 1} & 0 \\ 0 & 0 & 0 & A^{\pm 1} \end{pmatrix}$$

with

$$A^{+1} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, A^{-1} = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}$$

- U and U^{-} can been computed efficiently.
- U, U^{-1}, P coefficients are **growing regularly** during the R step.

Signing

- As $B = D - M$, we have $D \equiv M \pmod{\mathcal{L}}$
- $\|M\|_1 < D$ to guarantee **short number** of steps.

Signing

- As $B = D - M$, we have $D \equiv M \pmod{\mathcal{L}}$
- $\|M\|_1 < D$ to guarantee **short number** of steps.

Vector Reduction

1. $w \leftarrow Hash(m)$
2. until $\|w\|_\infty < D$
   1. Find q, r such $w = r + qD$
   2. Compute $w \leftarrow r + qM$

Signing

- As $B = D - M$, we have $D \equiv M \pmod{\mathcal{L}}$
- $\|M\|_1 < D$ to guarantee **short number** of steps.

Vector Reduction

1. $w \leftarrow Hash(m)$
2. until $\|w\|_\infty < D$
   1. Find q, r such $w = r + qD$
   2. Compute $w \leftarrow r + qM$

- Efficiency: No needs for **large arithmetic**.
- Security: Algorithm termination related to a public parameter D.

Signature Verfication

Alice Helps Bob

- Alice sends s such that $Hash(m) - s \in \mathcal{L}P$.
- Alice sends k such that $kP = Hash(m) - s$
- During signing, Alice extracts q such that $q(D - M) = Hash(m) - s$
- Alice compute $k = qU^{-1}$.

Signature Verfication

Alice Helps Bob

- Alice sends s such that $Hash(m) - s \in \mathcal{L}P$.
- Alice sends k such that $kP = Hash(m) - s$
- During signing, Alice extracts q such that $q(D - M) = Hash(m) - s$
- Alice compute $k = qU^{-1}$.

Bob checks that

- $\|s\|_\infty < D$,
- and $qP = Hash(m) - s$.

Best Known Attack

Find the Unique Shortest Vector of the lattice

$$\begin{pmatrix} v & 1 \\ P & 0 \end{pmatrix}$$

with $v = (D, 0, \ldots, 0)$ and a lattice gap

$$\gamma = \frac{\lambda_2}{\lambda_1} \lesssim \frac{\Gamma\left(\frac{n+3}{2}\right)^{\frac{1}{n+1}} \|D - M\|_2^{\frac{n}{n+1}}}{\|M\|_2} = \frac{\Gamma\left(\frac{n+3}{2}\right)^{\frac{1}{n+1}} \left(D^2 + N_b b^2 + N_1\right)^{\frac{n}{2(n+1)}}}{\sqrt{N_b b^2 + N_1}}$$

Best Known Attack

Find the Unique Shortest Vector of the lattice

$$\begin{pmatrix} v & 1 \\ P & 0 \end{pmatrix}$$

with $v = (D, 0, \ldots, 0)$ and a lattice gap

$$\gamma = \frac{\lambda_2}{\lambda_1} \lesssim \frac{\Gamma\left(\frac{n+3}{2}\right)^{\frac{1}{n+1}} \|D - M\|_2^{\frac{n}{n+1}}}{\|M\|_2} = \frac{\Gamma\left(\frac{n+3}{2}\right)^{\frac{1}{n+1}} \left(D^2 + N_b b^2 + N_1\right)^{\frac{n}{2(n+1)}}}{\sqrt{N_b b^2 + N_1}}$$

Conservator Choices

Dimension	N_b	b	N_1	Δ	R	γ	2^λ
912	16	28	432	32	24	$< \frac{1}{4}(1.006)^{d+1}$	2^{128}
1160	23	25	553	32	24	$< \frac{1}{4}(1.005)^{d+1}$	2^{192}
1518	33	23	727	32	24	$< \frac{1}{4}(1.004)^{d+1}$	2^{256}

Comments

Yang Yu and Leo Ducas Attack

- When b **is too big** compare to other value of M,
- **Machine learning** can extract position of b related to D.
- Sign of b could also sometime be extracted.

Consequence

BDD attack is simpler as the gap of new problem bigger.

Comments

Yang Yu and Leo Ducas Attack

- When b **is too big** compare to other value of M,
- **Machine learning** can extract position of b related to D.
- Sign of b could also sometime be extracted.

Consequence

BDD attack is simpler as the gap of new problem bigger.

Solutions

1. Find which sizes of b requires 2^{64} signatures: current attack 2^{17} for $b = 28$.
2. Uses b smaller: if b small, dimension increases by 20% to 30%.

Specificity

Specificity

- Digital Signature using **Hidden Structured** Lattice.
- **Diagonal Dominant** Basis.

Specificity

Specificity

- Digital Signature using **Hidden Structured** Lattice.
- **Diagonal Dominant** Basis.

Advantage

- **Generic** Lattice **without large integer** arithmethic.
- Use **Max Norm** to minimise leaking.

Specificity

Specificity

- Digital Signature using **Hidden Structured** Lattice.
- **Diagonal Dominant** Basis.

Advantage

- **Generic** Lattice **without large integer** arithmethic.
- Use **Max Norm** to minimise leaking.

Disadvantage

- **Quadratic structure** is memory costly.
- **Verfication still slower** than signing.