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**.

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

Secret Key

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

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

- 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 $U = P_{R+1} T_R P_R \ldots T_1 P_1$
- 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 $U = P_{R+1} T_R P_R ... T_1 P_1$
- 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

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

- 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.

Odd Manhattan

Thomas PLANTARD

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 Cryptosystem

- Using **Generic Lattice** generated form its **Dual**.
- Dual created from an **Odd** Vector of bounded **Manhattan** norm.

General Description

Lattice based Cryptosystem

- Using **Generic Lattice** generated form its **Dual**.
- Dual created from an **Odd** Vector of bounded **Manhattan** norm.

Lattice based Key Encryption Message

- Encrypt a message m in the **parity bit** of a vector close to the lattice.
- CCA achived using classic method i.e. Dent's.

Public Key Encryption

Setup

- Alice choose 3 public parameters
  1. d a lattice dimension,
  2. b an upper bound,
  3. p a prime number.
- Alice creates a secret random vector $w \in \mathcal{M}_{d,l}$ i.e.
  1. with w_i odd,
  2. with $\sum_{i=1}^{d} |w_i|$ bounded by $l = \lfloor \frac{p-1}{2b} \rfloor$
- Alice publish the Lattice $\mathcal{L}$ such that $w \in \mathcal{L}^*$.

Public Key Encryption

Setup

- Alice choose 3 public parameters
  1. d a lattice dimension,
  2. b an upper bound,
  3. p a prime number.
- Alice creates a secret random vector $w \in \mathcal{M}_{d,l}$ i.e.
  1. with w_i odd,
  2. with $\sum_{i=1}^{d} |w_i|$ bounded by $l = \lfloor \frac{p-1}{2b} \rfloor$
- Alice publish the Lattice $\mathcal{L}$ such that $w \in \mathcal{L}^*$.

Encryption/Decryption

- To encrypt $m \in \{0, 1\}$, Bob computes v such $\exists u$
  1. $(v - u) \in \mathcal{L}$
  2. $\|u\|_\infty \leq b$
  3. $\sum_{i=1}^{d} u_i \bmod 2 = m$
- To decrypt, Alice extract $m = (vw^t \bmod p) \bmod 2$.

Probability that a random lattice could be a public key

Theorem

Let $\mathcal{L}$ a full rank lattice of determinant $p > 2$ prime and dimension $d > 1$, and $l \in \mathbb{N}^*$, the probability that a Lattice does not have such vector in its dual $\mathcal{L}^* \cap \mathcal{M}_{d,l} = \varnothing$ is given by

$$\mathcal{P}_{p,d,l} = \left(1 - \frac{1}{p^{d-1}}\right)^{2^{d-1}\binom{\left\lfloor \frac{l+d}{2} \right\rfloor}{d}}$$

Probability that a random lattice could be a public key

Theorem

Let $\mathcal{L}$ a full rank lattice of determinant $p > 2$ prime and dimension $d > 1$, and $l \in \mathbb{N}^*$, the probability that a Lattice does not have such vector in its dual $\mathcal{L}^* \cap \mathcal{M}_{d,l} = \varnothing$ is given by

$$\mathcal{P}_{p,d,l} = \left(1 - \frac{1}{p^{d-1}}\right)^{2^{d-1}\binom{\left\lfloor \frac{l+d}{2} \right\rfloor}{d}}$$

Cryptosystem Parameters

By taking $p \approx 2^{d+1} b^d (d)!$, we insure that $\mathcal{P}_{p,d,\frac{p-1}{2b}} < \frac{1}{2}$ i.e.
the set of **all possible public key** represents more than **half** of the set of **all generic lattices** with equivalent dimension and determinant.

Computational Hardness for message security

Definition (α-Bounded Distance Parity Check (BDPCα))

Given a lattice $\mathcal{L}$ of dimension d and a vector v such that $\exists u, (v - u) \in \mathcal{L}, \|u\| < \alpha\lambda_1(\mathcal{L})$, find $\sum_{i=1}^{d} u_i$ mod 2.

Computational Hardness for message security

Definition (α-Bounded Distance Parity Check (BDPCα))

Given a lattice $\mathcal{L}$ of dimension d and a vector v such that $\exists u, (v - u) \in \mathcal{L}, \|u\| < \alpha\lambda_1(\mathcal{L})$, find $\sum_{i=1}^{d} u_i \bmod 2$.

Theorem ($BDD_{\frac{\alpha}{4}} \leq BDPC_\alpha$)

For any l_p−norm and any $\alpha \leq 1$ there is a polynomial time Cook-reduction from $BDD_{\frac{\alpha}{4}}$ to $BDPC_\alpha$.

Computational Hardness for message security

Definition (α-Bounded Distance Parity Check (BDPCα))

Given a lattice $\mathcal{L}$ of dimension d and a vector v such that $\exists u, (v-u) \in \mathcal{L}, \|u\| < \alpha\lambda_1(\mathcal{L})$, find $\sum_{i=1}^{d} u_i$ mod 2.

Theorem ($BDD_{\frac{\alpha}{4}} \leq BDPC_{\alpha}$)

For any l_p-norm and any $\alpha \leq 1$ there is a polynomial time Cook-reduction from $BDD_{\frac{\alpha}{4}}$ to $BDPC_{\alpha}$.

Extracting message is as hard as...

1. BDD_α with $\alpha = \frac{1}{o(d)}$ for $l_\infty-$norm,
2. USVP_γ with $\gamma = o(d)$ for $l_\infty-$norm,
3. GapSVP_γ with $\gamma = o(\frac{d^2}{\log d})$ for $l_\infty-$norm,
4. GapSVP_γ with $\gamma = o(\frac{d^2}{\log d})$ for l_2-norm.

Best Known Attack

Find the Unique Shortest Vector of the lattice

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

with a lattice gap

$$\gamma = \frac{\lambda_2}{\lambda_1} \simeq \frac{\Gamma\left(\frac{d+3}{2}\right)^{\frac{1}{d+1}} p^{\frac{n}{n+1}}}{\sqrt{\pi d^{\frac{(b+1)b}{2b+1}}}}$$

Best Known Attack

Find the Unique Shortest Vector of the lattice

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

with a lattice gap

$$\gamma = \frac{\lambda_2}{\lambda_1} \simeq \frac{\Gamma\left(\frac{d+3}{2}\right)^{\frac{1}{d+1}} p^{\frac{n}{n+1}}}{\sqrt{\pi d \frac{(b+1)b}{2b+1}}}$$

Conservator Choices

Dimension	Bound	Determinant	$\mathcal{P}_{p,d,\frac{p-1}{2b}}$	Gap	2^{λ}
1156	1	$2^{11258} - 4217$	$\lesssim 0.336$	$< \frac{1}{4}(1.006)^{d+1}$	2^{128}
1429	1	$2^{14353} - 15169$	$\lesssim 0.137$	$< \frac{1}{4}(1.005)^{d+1}$	2^{192}
1850	1	$2^{19268} - 7973$	$\lesssim 0.218$	$< \frac{1}{4}(1.004)^{d+1}$	2^{256}

Implementation

Side-Channel resistance

Constant time achieved by reorganising inner product computation.

Implementation

Side-Channel resistance

Constant time achieved by reorganising inner product computation.

Shared Computation

- Due to CCA, implementation encrypting λ message $m = 0, 1$.
- Optimisation to **share** some **common computation** while encrypting.

Implementation

Side-Channel resistance

Constant time achieved by reorganising inner product computation.

Shared Computation

- Due to CCA, implementation encrypting λ message $m = 0, 1$.
- Optimisation to **share** some **common computation** while encrypting.

Pseudo Mersenne

Using $p = 2^n - c$, to accelerate **modular reduction**.

Comment

Tancrede Lepoint

- **Implementation issue** regarding CCA security.
- Shared secret was not randomised when return decryption failure.

Specificity

Specificity

- Secret key is composed by only one **Odd** vector of bounded **Manhattan** Norm.
- Message is encrypted in the **parity bit** of a close vector.

Specificity

- Secret key is composed by only one **Odd** vector of bounded **Manhattan** Norm.
- Message is encrypted in the **parity bit** of a close vector.

Advantage

- Majority of all **generic lattices** are **potential public keys**.
- As Hard as **BDD** $_{\frac{1}{o(d)}}$ for $l_\infty -$norm i.e. **max norm**.
- No decryption error.
- Simplicity.

Specificity

Specificity

- Secret key is composed by only one **Odd** vector of bounded **Manhattan** Norm.
- Message is encrypted in the **parity bit** of a close vector.

Advantage

- Majority of all **generic lattices** are **potential public keys**.
- As Hard as **BDD** $_{\frac{1}{o(d)}}$ for $l_\infty-$norm i.e. **max norm**.
- No decryption error.
- Simplicity.

Disadvantage

- Keys and Ciphertext **size**.