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

1 Description
2 Security Analysis
3 Comments
4 Specificity
### 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*.

**Secret key:** Diagonal Dominant Basis $B$ of a lattice $L$

**Public key:** A basis $P$ of the same lattice $P = UB$

**Signature of a message $m$:** a vector $s$ such that $(m - s) \in L$ and $\|s\|_\infty < D$

**Signature security related to $GDD_\infty$.**
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 $GDD_\infty$. 
A diagonal Dominant Basis with $N_b \pm b$ and $N_1 \pm 1$.

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

With a \textit{cyclic} structure \textbf{but for the signs}.

\[
B = \begin{pmatrix}
D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 \\
0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 \\
\pm 1 & 0 & D & 1 & 1 & \pm b & 0 & \pm b & \pm 1 & 0 \\
0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 \\
\pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 & \pm b \\
\pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b & 0 \\
0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 & \pm b \\
\pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 & \pm 1 \\
\pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D & \pm 1 \\
\pm 1 & \pm 1 & \pm b & 0 & \pm b & \pm 1 & 0 & \pm 1 & 0 & D
\end{pmatrix}
\]
A diagonal Dominant Basis with $N_b \pm b$ and $N_1 \pm 1$.

With a **cyclic** structure **but for the signs**.

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

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

\[
A^+ = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},
A^- = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}
\]
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
  \[
  A^{\pm 1} = \begin{pmatrix}
  1 & 2 \\
  1 & 1
  \end{pmatrix}, A^{-1} = \begin{pmatrix}
  -1 & 2 \\
  1 & -1
  \end{pmatrix}
  \]

- \( U \) and \( U^{-1} \) can be computed efficiently.
- \( U, U^{-1}, P \) coefficients are **growing regularly** during the \( R \) step.
As $B = D - M$, we have $D \equiv M \pmod{L}$

$\|M\|_1 < D$ to guarantee short number of steps.
Signing

As $B = D - M$, we have $D \equiv M \pmod{L}$

$\|M\|_1 < D$ to guarantee short number of steps.

Vector Reduction

1. $w \leftarrow \text{Hash}(m)$
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 $D$. 
As \( B = D - M \), we have \( D \equiv M \mod \mathcal{L} \)

\[ \| M \|_1 < D \] to guarantee short number of steps.

**Vector Reduction**

1. \( w \leftarrow \text{Hash}(m) \)
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 Verification

**Alice Helps Bob**

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

$\|s\|_{\infty} < D$, and $qP = \text{Hash}(m) - s$. 
Alice Helps Bob

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

Bob checks that

- $\|s\|_{\infty} < D$,
- and $qP = \text{Hash}(m) - s$. 
Best Known Attack

Find the Unique Shortest Vector of the lattice

\[
\begin{pmatrix}
  \nu \\
  \nu
\end{pmatrix}
\]

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

\[
\gamma = \frac{\lambda_2}{\lambda_1} \leq \frac{\Gamma\left(\frac{n+3}{2}\right) \frac{1}{n+1} \|D - M\|_2^{\frac{n}{n+1}}}{\|M\|_2} = \frac{\Gamma\left(\frac{n+3}{2}\right) \frac{1}{n+1} (D^2 + N_b b^2 + N_1) \frac{n}{2(n+1)}}{\sqrt{N_b b^2 + N_1}}
\]
Best Known Attack

Find the Unique Shortest Vector of the lattice

\[
\begin{pmatrix}
  v \\
  P
\end{pmatrix}
\]

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

\[
\gamma = \frac{\lambda_2}{\lambda_1} \leq \frac{\Gamma\left(\frac{n+3}{2}\right) \frac{1}{n+1} \|D - M\|_{2}^{\frac{n}{n+1}}}{\|M\|_{2}} = \frac{\Gamma\left(\frac{n+3}{2}\right) \frac{1}{n+1} (D^2 + N_b b^2 + N_1) \frac{n}{2(n+1)}}{\sqrt{N_b b^2 + N_1}}
\]

Conservator Choices

<table>
<thead>
<tr>
<th>Dimension</th>
<th>( N_b )</th>
<th>( b )</th>
<th>( N_1 )</th>
<th>( \Delta )</th>
<th>( R )</th>
<th>( \gamma )</th>
<th>( 2^\lambda )</th>
</tr>
</thead>
<tbody>
<tr>
<td>912</td>
<td>16</td>
<td>28</td>
<td>432</td>
<td>32</td>
<td>24</td>
<td>(&lt; \frac{1}{4}(1.006)^{d+1} )</td>
<td>( 2^{128} )</td>
</tr>
<tr>
<td>1160</td>
<td>23</td>
<td>25</td>
<td>553</td>
<td>32</td>
<td>24</td>
<td>(&lt; \frac{1}{4}(1.005)^{d+1} )</td>
<td>( 2^{192} )</td>
</tr>
<tr>
<td>1518</td>
<td>33</td>
<td>23</td>
<td>727</td>
<td>32</td>
<td>24</td>
<td>(&lt; \frac{1}{4}(1.004)^{d+1} )</td>
<td>( 2^{256} )</td>
</tr>
</tbody>
</table>
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.
Yang Yu and Leo Ducas Attack

- When \( b \) is too big compared to other values of \( M \),
- **Machine learning** can extract position of \( b \) related to \( D \).
- Sign of \( b \) could also sometimes 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

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

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

Advantage

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

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

Advantage

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

Disadvantage

- **Quadratic structure** is memory costly.
- **Verification 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
Lattice based Cryptosystem

- Using **Generic Lattice** generated from its **Dual**.
- Dual created from an **Odd Vector** of bounded **Manhattan** norm.
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 achieved using classic method i.e. Dent’s.
Public Key Encryption

Setup

- Alice chooses 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 $l = \left\lfloor \frac{p-1}{2b} \right\rfloor$
- Alice publishes the Lattice $\mathcal{L}$ such that $w \in \mathcal{L}^*$.
Public Key Encryption

**Setup**
- Alice chooses 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 publishes the Lattice $\mathcal{L}$ such that $w \in \mathcal{L}^*$.

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

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 $\mathcal{L}^* \cap \mathcal{M}_{d,l} = \emptyset$ is given by

$$P_{p,d,l} = \left(1 - \frac{1}{p^{d-1}}\right)^{2d-1} \left\lfloor \frac{l+d}{2d} \right\rfloor$$
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 $\mathcal{L}^* \cap \mathcal{M}_{d,l} = \emptyset$ is given by

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

**Cryptosystem Parameters**

By taking $p \approx 2^{d+1} b^d (d)!$, we insure that $P_{p,d,\frac{p-1}{2b}} < \frac{1}{2}$ 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 ($\alpha$-Bounded Distance Parity Check (BDPC$\alpha$))

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$\alpha$ $\leq$ BDPC$\alpha$)

For any $l_p$-norm and any $\alpha \leq 1$ there is a polynomial time Cook-reduction from BDD$\alpha$ to BDPC$\alpha$.

Extracting message is as hard as...

1. BDD$\alpha$ with $\alpha = o(d)$ for $l_\infty$-norm,
2. USVP$\gamma$ with $\gamma = o(d)$ for $l_\infty$-norm,
3. GapSVP$\gamma$ with $\gamma = o(d^2 \log d)$ for $l_\infty$-norm,
4. GapSVP$\gamma$ with $\gamma = o(d^2 \log d)$ for $l_2$-norm.
Definition ($\alpha$-Bounded Distance Parity Check (BDPC$\alpha$))

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 $BDPC_{\alpha}$.
Computational Hardness for message security

Definition ($\alpha$-Bounded Distance Parity Check (BDPC$\alpha$))

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 ($BDD_{\alpha\frac{\lambda_1(\mathcal{L})}{4}} \leq BDPC_\alpha$)

For any $l_p$-norm and any $\alpha \leq 1$ there is a polynomial time Cook-reduction from $BDD_{\alpha\frac{\lambda_1(\mathcal{L})}{4}}$ to $BDPC_\alpha$.

Extracting message is as hard as...

1. BDD$\alpha$ with $\alpha = \frac{1}{o(d)}$ for $l_{\infty}$-norm,
2. USVP$\gamma$ with $\gamma = o(d)$ for $l_{\infty}$-norm,
3. GapSVP$\gamma$ with $\gamma = o(\frac{d^2}{\log d})$ for $l_{\infty}$-norm,
4. GapSVP$\gamma$ with $\gamma = o(\frac{d^2}{\log d})$ for $l_2$-norm.
Find the Unique Shortest Vector of the lattice

\[
\begin{pmatrix}
  v \\
  P
\end{pmatrix}
\begin{pmatrix}
  1 \\
  0
\end{pmatrix}
\]

with a lattice gap

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

Find the Unique Shortest Vector of the lattice

\[
\begin{pmatrix}
\nu \\
\rho
\end{pmatrix}
\]

with a lattice gap

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

Conservator Choices

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Bound</th>
<th>Determinant</th>
<th>(\mathcal{P}_{p, d, \frac{p-1}{2b}})</th>
<th>Gap</th>
<th>(2^\lambda)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1156</td>
<td>1</td>
<td>2^{11258} - 4217</td>
<td>(\lesssim 0.336)</td>
<td>(&lt; \frac{1}{4} (1.006)^{d+1})</td>
<td>2^{128}</td>
</tr>
<tr>
<td>1429</td>
<td>1</td>
<td>2^{14353} - 15169</td>
<td>(\lesssim 0.137)</td>
<td>(&lt; \frac{1}{4} (1.005)^{d+1})</td>
<td>2^{192}</td>
</tr>
<tr>
<td>1850</td>
<td>1</td>
<td>2^{19268} - 7973</td>
<td>(\lesssim 0.218)</td>
<td>(&lt; \frac{1}{4} (1.004)^{d+1})</td>
<td>2^{256}</td>
</tr>
</tbody>
</table>
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 $\lambda$ 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 $\lambda$ message $m = 0, 1$.
- Optimisation to **share** some **common computation** while encrypting.

Pseudo Mersenne

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

- **Implementation issue** regarding CCA security.
- Shared secret was not randomised when return decryption failure.
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 $\text{BDD} \frac{1}{o(d)}$ for $l_\infty$—norm i.e. max norm.
- No decryption error.
- Simplicity.
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 $\text{BDD} \frac{1}{o(d)} \text{ for } l_\infty$—norm i.e. max norm.
- No decryption error.
- Simplicity.

Disadvantage

- Keys and Ciphertext size.