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

1. Description
2. Security Analysis
3. Implementation Details
4. Comments
5. Specificity

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

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

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

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

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 $\sum_{i=1}^{d} u_i$ 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 (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$_\alpha$ 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.

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

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**.