RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: CRYP-T10

CRYPTANALYSIS OF COMPACT-LWE

Jonathan Bootle, Mehdi Tibouchi, Keita Xagawa

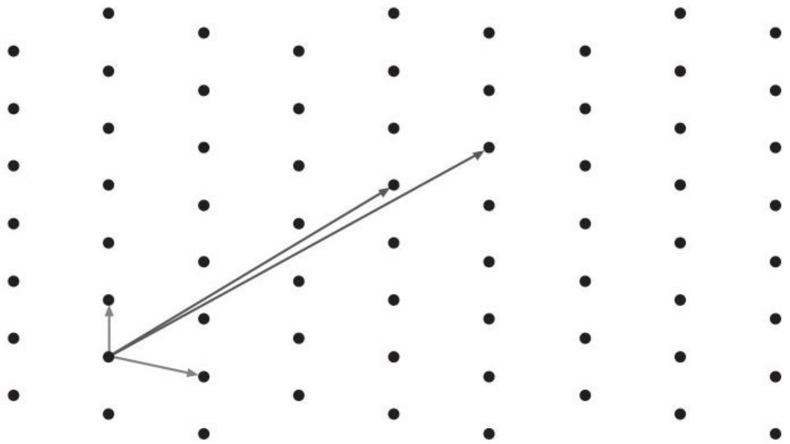
UCL

erc
uropean Research Council
stablished by the European Commission

NTT

Background Information

- Lattice-based cryptographic assumption



Based on the learning-with-errors (LWE) assumption

Compact-LWE

Hoped to achieve security for smaller parameters

Background Information

- Proposed by Liu, Li, Kim, and Nepal at ACISP'17 invited talk

Josef Pieprzyk
Suriadi Suriadi (Eds.)

LNCS 10343

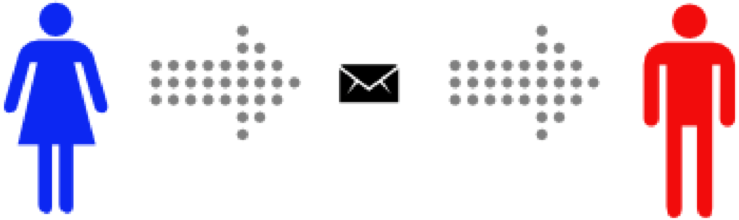
Information Security and Privacy

22nd Australasian Conference, ACISP 2017
Auckland, New Zealand, July 3–5, 2017
Proceedings, Part II

2 Part II

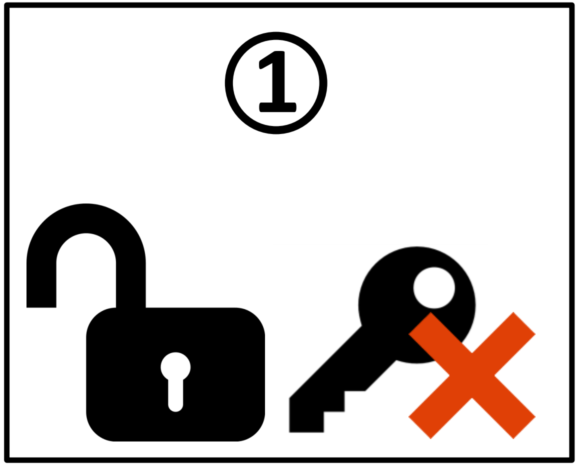
Springer

- Gives lightweight encryption scheme for constrained devices

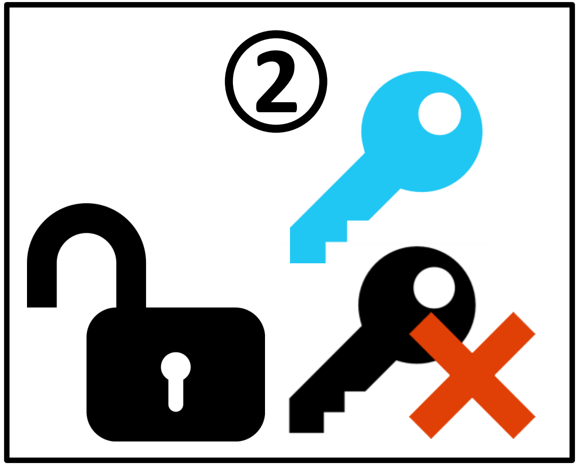


Background Information

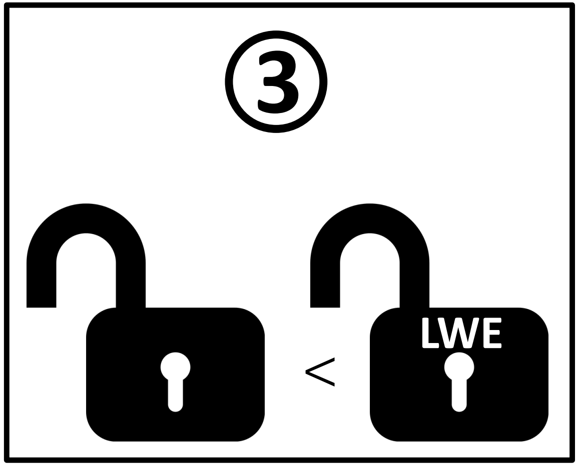
Basic Decryption Attack



Equivalent Secret Keys

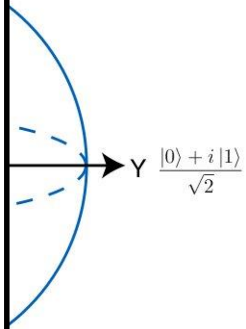


Parameter Choice



Honest Decryption:	500 ciphertexts per second
Our Decryption:	18,000 ciphertexts per second

Background Information



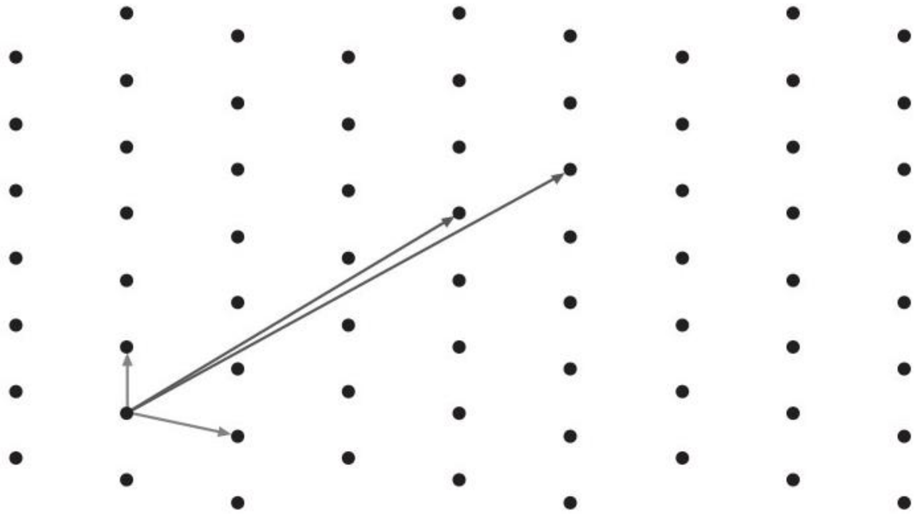
Cryptanalysed by us and others

BACKGROUND

Lattices

An n-dimensional lattice $\mathcal{L}$ is

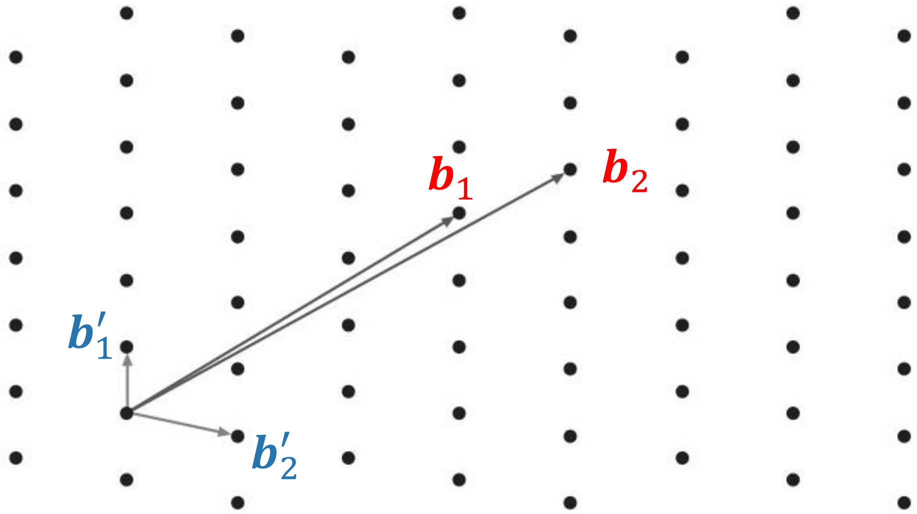
- A discrete additive subgroup of $\mathbb{R}^n$
- Generated by a basis $\mathcal{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
- $\mathcal{L} = \sum_{i=1}^{n}(\mathbb{Z} \cdot \boldsymbol{b}_i)$



Lattices

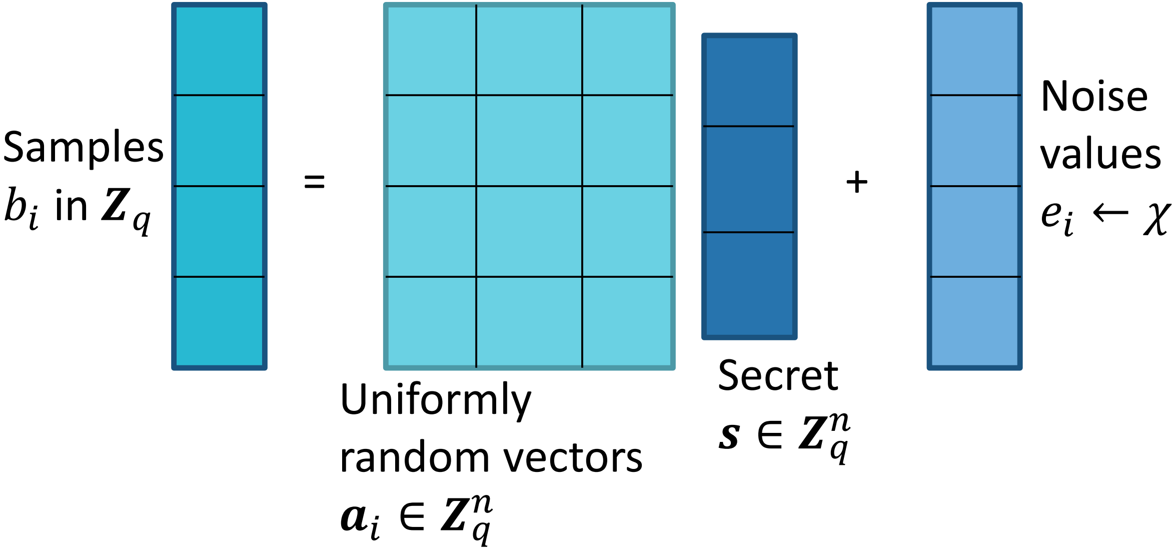
- Solve lattice problems by finding short vectors
- Example reduction algorithms are LLL and BKZ
- Add and subtract rows
- Find short basis vectors

$$\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix} \rightarrow \begin{pmatrix} \boldsymbol{b}'_1 \\ \boldsymbol{b}'_2 \end{pmatrix}$$



Learning with Errors

$$b_i = \langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + e_i$$
$$\boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e}$$



Samples b_i in $\boldsymbol{Z}_q$

=

Uniformly random vectors $\boldsymbol{a}_i \in \boldsymbol{Z}_q^n$

Secret $\boldsymbol{s} \in \boldsymbol{Z}_q^n$

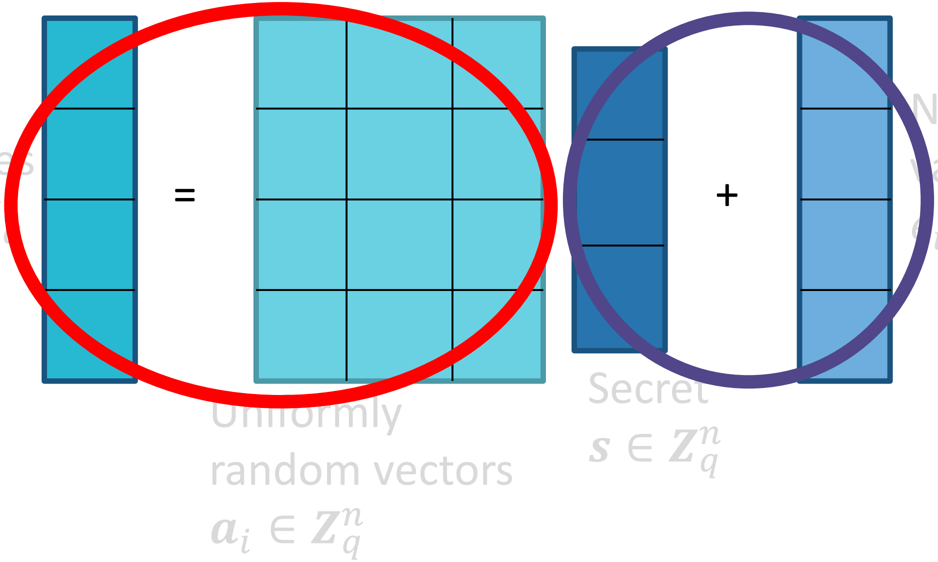
+

Noise values $e_i \leftarrow \chi$

Learning with Errors

Decision: does $(\boldsymbol{b}, A)$ look random?
Search: given $(\boldsymbol{b}, A)$, find $\boldsymbol{s}$

$\boldsymbol{b}$ and A
are public

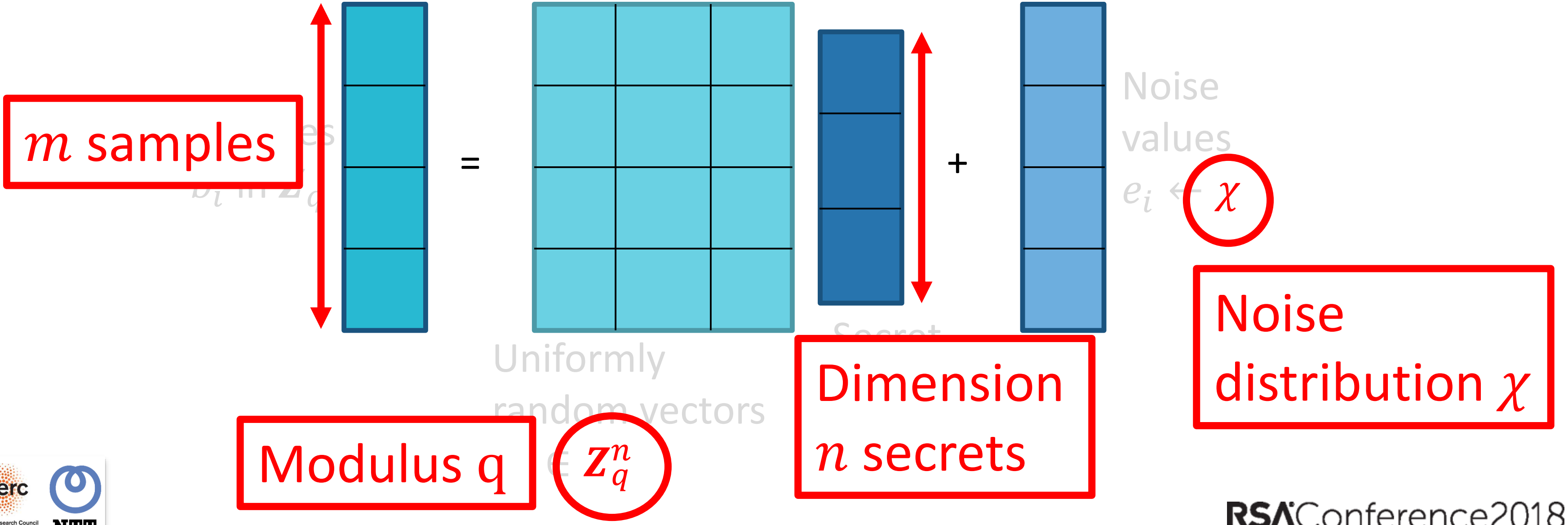

=
+
Uniformly
random vectors
$\boldsymbol{a}_i \in \boldsymbol{Z}_q^n$
Secret
$\boldsymbol{s} \in \boldsymbol{Z}_q^n$

$\boldsymbol{s}$ and $\boldsymbol{e}$
are private

Learning with Errors

Decision: does $(\boldsymbol{b}, A)$ look random?

Search: given $(\boldsymbol{b}, A)$, find $\boldsymbol{s}$



m samples

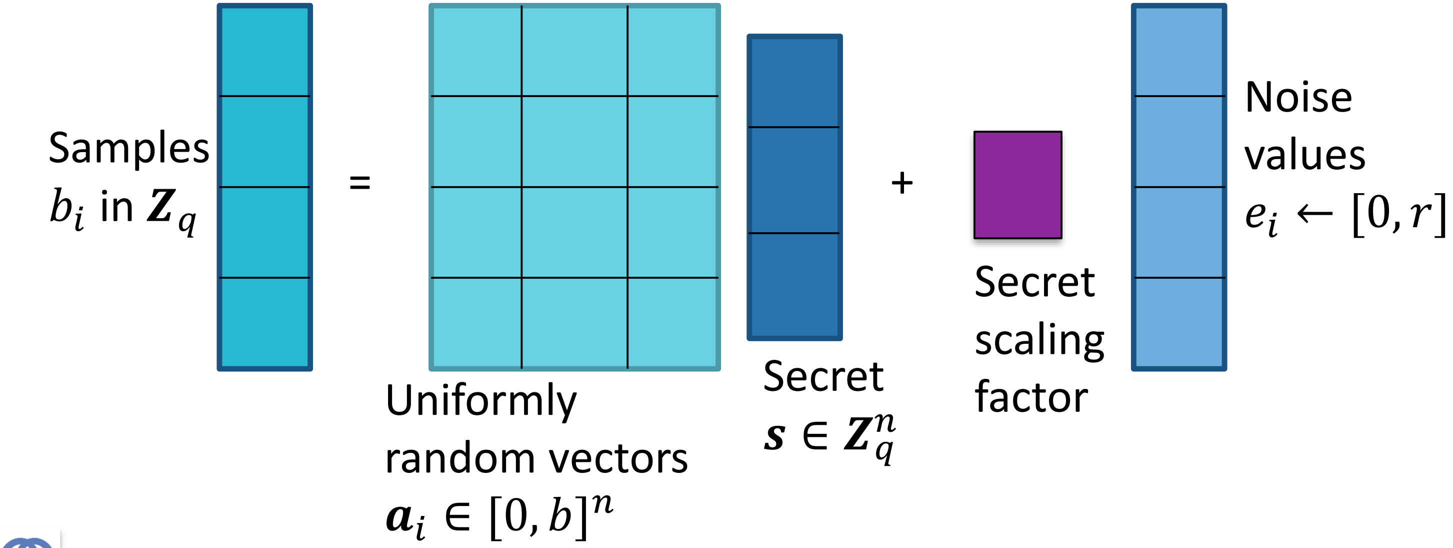
Modulus q

Dimension
n secrets

Noise
distribution χ

Compact-LWE

$$b_i = \langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + sk_q^{-1} \cdot p \cdot e_i$$



Samples b_i in $\boldsymbol{Z}_q$

=

Uniformly random vectors $\boldsymbol{a}_i \in [0, b]^n$

Secret $\boldsymbol{s} \in \boldsymbol{Z}_q^n$

+

Secret scaling factor

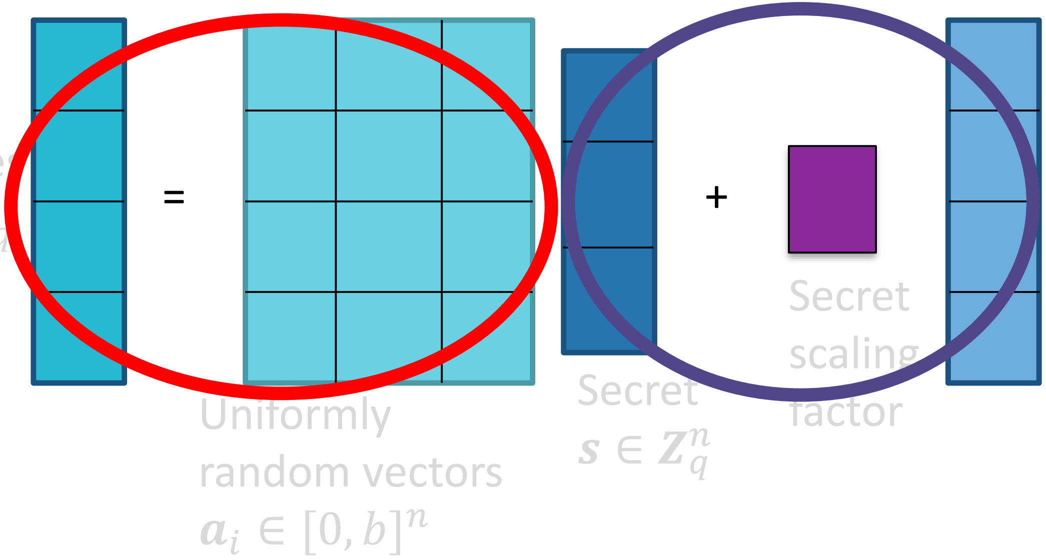
Noise values $e_i \leftarrow [0, r]$

Compact-LWE

Decision: does $(\boldsymbol{b}, A)$ look random?

Search: given $(\boldsymbol{b}, A)$, find $\boldsymbol{s}$

$\boldsymbol{b}$ and A are public

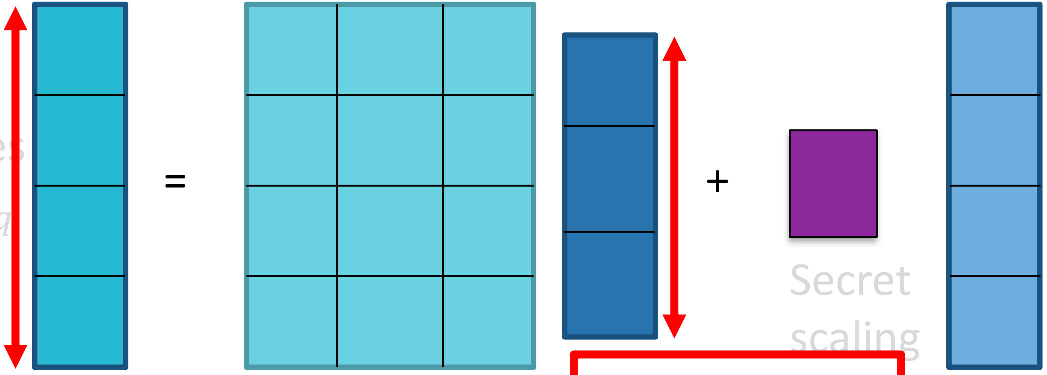

=
+
Uniformly random vectors $\boldsymbol{a}_i \in [0, b]^n$
Secret $\boldsymbol{s} \in \boldsymbol{Z}_q^n$
Secret scaling factor

$\boldsymbol{s}, \boldsymbol{e}$ and the scaling factor are private

Compact-LWE

$$b_i = \langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + sk_q^{-1} \cdot p$$

Scaling factor ingredients



m samples

maximum size of A elements

b

Dimension n secrets modulo q

Noise bound r

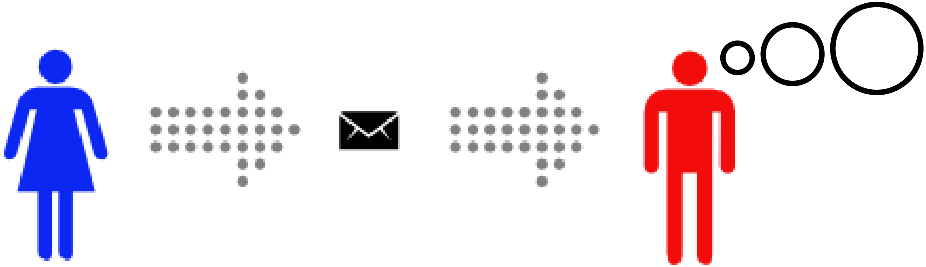
Parameters

Public Parameters

- $pp = (q, n, m, t, w, b)$
- t, maximum plaintext size
- w, knapsack weight for encryption
- $\boldsymbol{PK} = (A, \boldsymbol{b})$

Secret Parameters

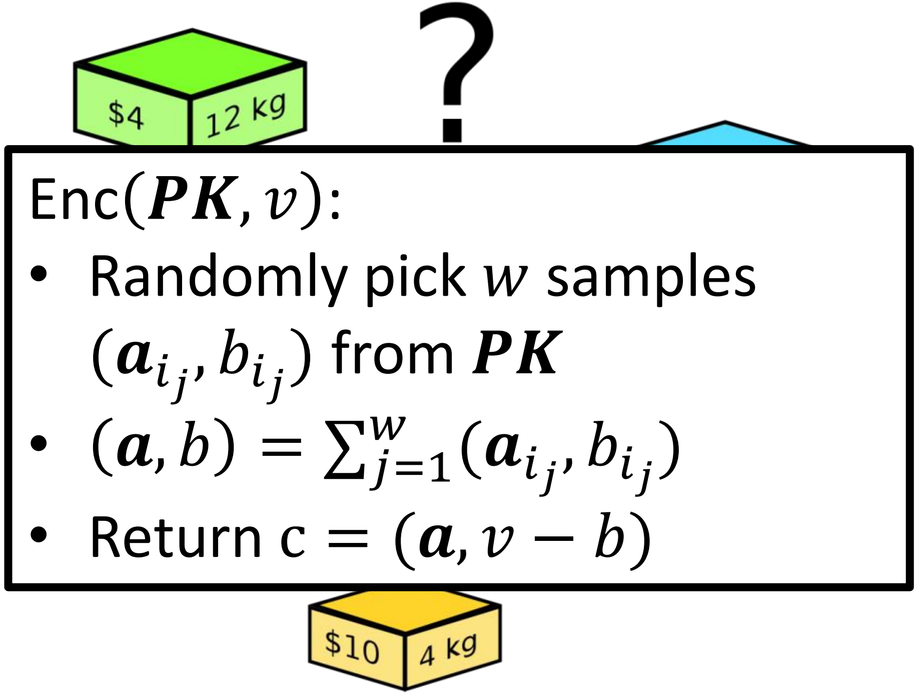
- $\boldsymbol{K} = (\boldsymbol{s}, sk, r, p)$



$$n + 1 < m < n^2$$
$$2b(b\,log_2 b + 1) < q$$
$$2log_2 b < n$$
$$t \leq p$$
$$sk \cdot (t - 1) + wrp < q$$
$$b < r$$

Encryption Idea

- $\boldsymbol{PK}$ contains random-looking samples $(\boldsymbol{a}_i, b_i)$ from $(A, \boldsymbol{b})$
- Add knapsack of b_i to hide message
- Include same knapsack of $\boldsymbol{a}_i$ to allow decryption



Enc$(\boldsymbol{PK}, v)$:

- Randomly pick w samples $(\boldsymbol{a}_{i_j}, b_{i_j})$ from $\boldsymbol{PK}$
- $(\boldsymbol{a}, b) = \sum_{j=1}^{w} (\boldsymbol{a}_{i_j}, b_{i_j})$
- Return c $= (\boldsymbol{a}, v - b)$

Comparison of Parameters

Compact-LWE Parameters

- Claims 138-bit security
- $q = 2^{32}$
- $n = 13$
- $m = 74$
- $t = 2^{16}, w = 86, b = 16$

Lizard, Classical Parameters, 2016

- Claims 128-bit security
- $q \approx 2^{10}$
- $n = 544$
- $m = 840$

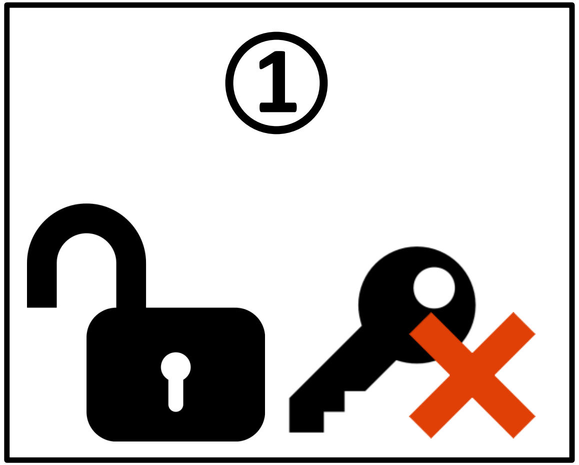
Implementation Results

- Implemented on MTM-CM5000-MSP device
- Contiki OS
- 50 encryptions per second
- 500 decryptions per second

Contiki

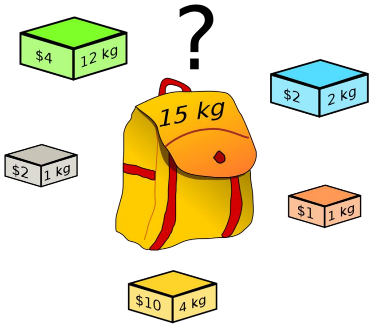
The Open Source OS for the Internet of Things

BASIC DECRYPTION ATTACK



Attack Strategy

- $c = (\boldsymbol{a}, v - b) = (\boldsymbol{a}, b')$
- $(\boldsymbol{a}, b) = \sum_{j=1}^{w} (\boldsymbol{a}_{i_j}, b_{i_j})$
- Create lattice encoding knapsack
- Find a short vector with lattice reduction



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

$$\begin{pmatrix} 1 & \mathbf{0} & \kappa \boldsymbol{a} & b' \\ \mathbf{0} & tI_m & -\kappa A & \boldsymbol{b} \\ 0 & \mathbf{0} & \mathbf{0} & q \end{pmatrix}$$

Solves knapsack

Recovers plaintext

Experimental Results

- Correctly decrypted 9998/10,000 random ciphertexts
- Roughly 16 decryptions per second
- 3.4 GHz Core i7-3770 desktop
- Sagemath, LLL in fplll

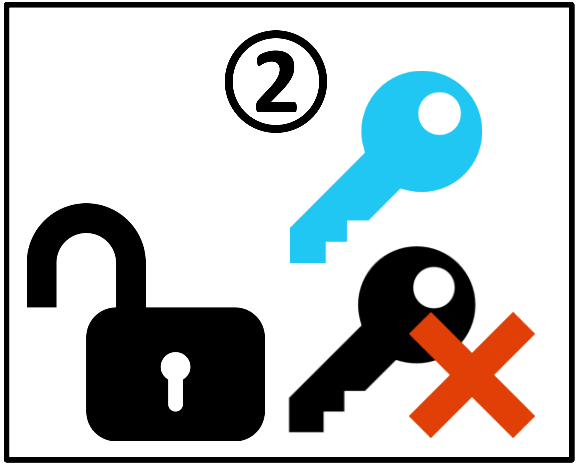
- One lattice reduction per ciphertext
- Relies on low dimension n = 13

🤔

- Honest decryption: 500 decryptions per second, constrained device

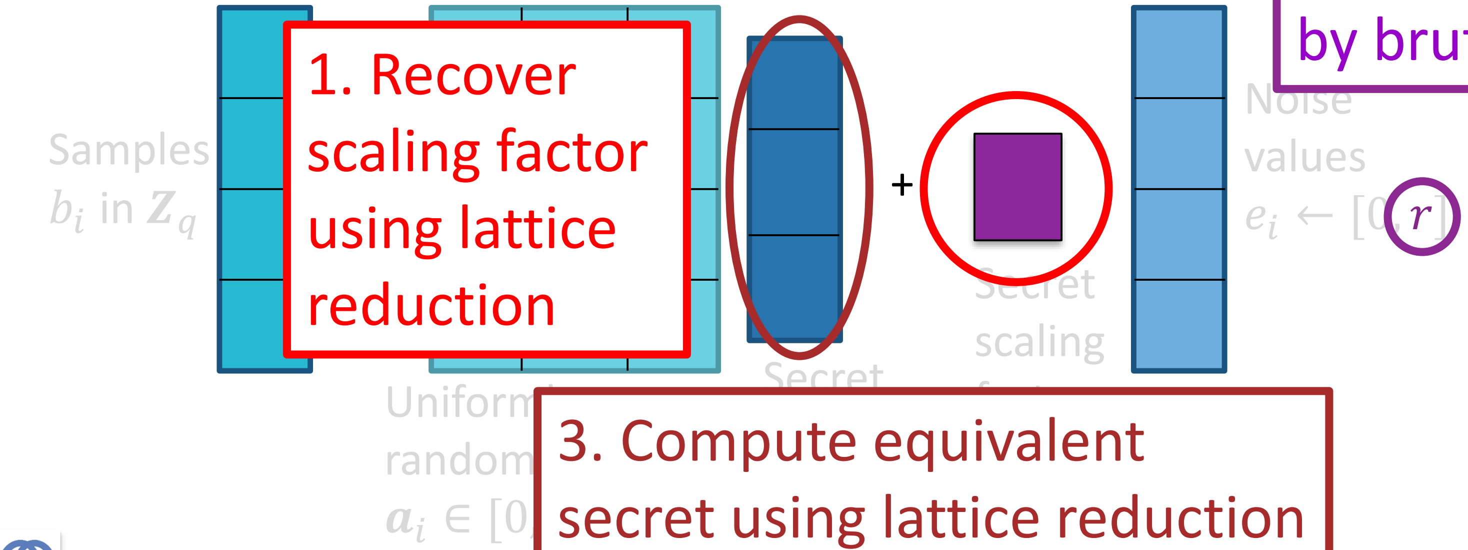
SECRET KEY RECOVERY

*equivalent secret key



Attack Strategy

$$b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + sk_q^{-1} \cdot p \cdot e_i$$



1. Recover scaling factor using lattice reduction

2. Find other secret values by brute force

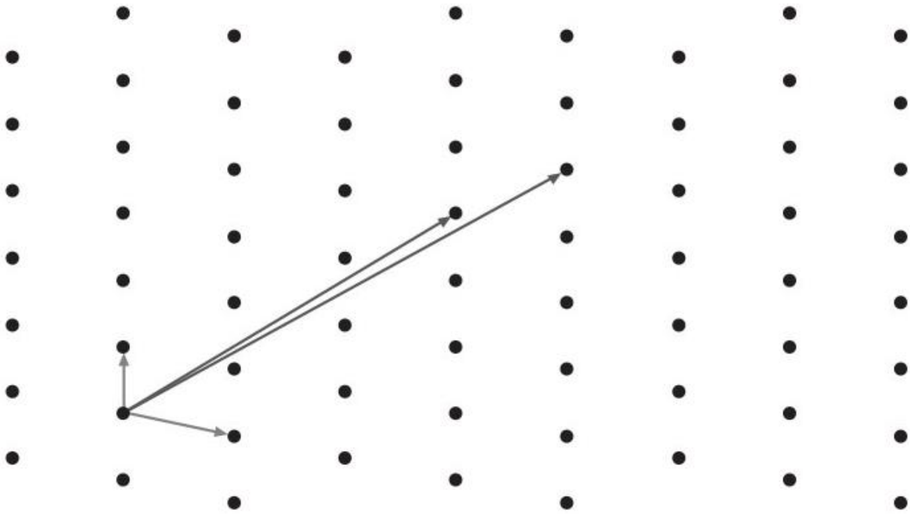
3. Compute equivalent secret using lattice reduction

Step 1: Scale-factor Recovery

- $\boldsymbol{b} = A\boldsymbol{s} + k\boldsymbol{e}$
- Compute short U such that $U^T A = 0 \; mod \; q$
- $U\boldsymbol{b} = k \; U\boldsymbol{e} \, mod \; q$

Public

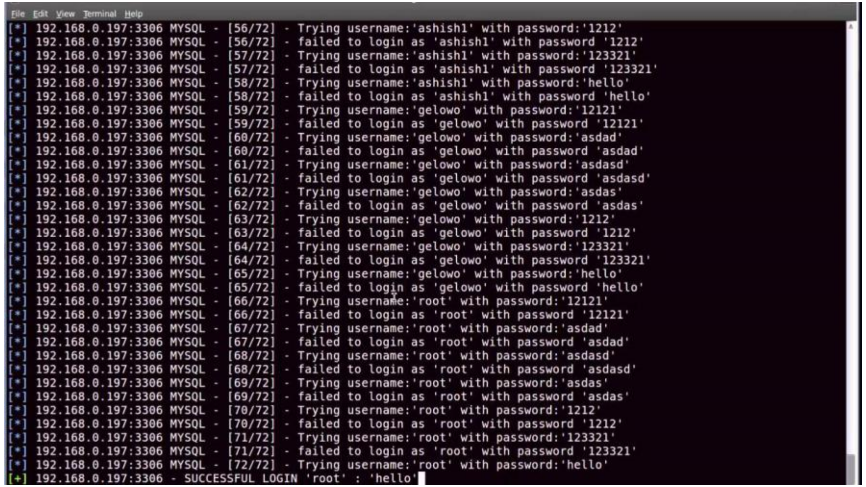
Short vector in $\begin{pmatrix} (U\boldsymbol{b})^T \\ qI \end{pmatrix}$



Step 2: Recovering Secret Key Parameters

- Secret scale-factor is $k = sk_q^{-1} \cdot p$
- Brute force search for sk and p
- Use the values which maximise r

$$sk \cdot (t - 1) + wrp < q$$



```
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[+] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

Step 3: Find an Equivalent Secret

- Secret is a short lattice vector
- Use with modified decryption algorithm

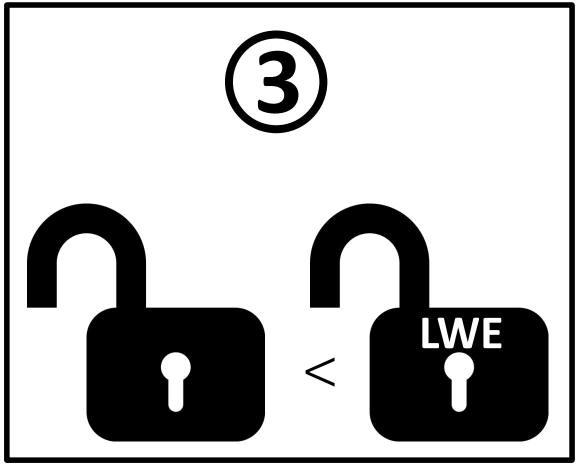
$$\begin{pmatrix} A^T & 0 \\ qI_m & 0 \\ k^{-1} & t \end{pmatrix}$$

Experimental Results

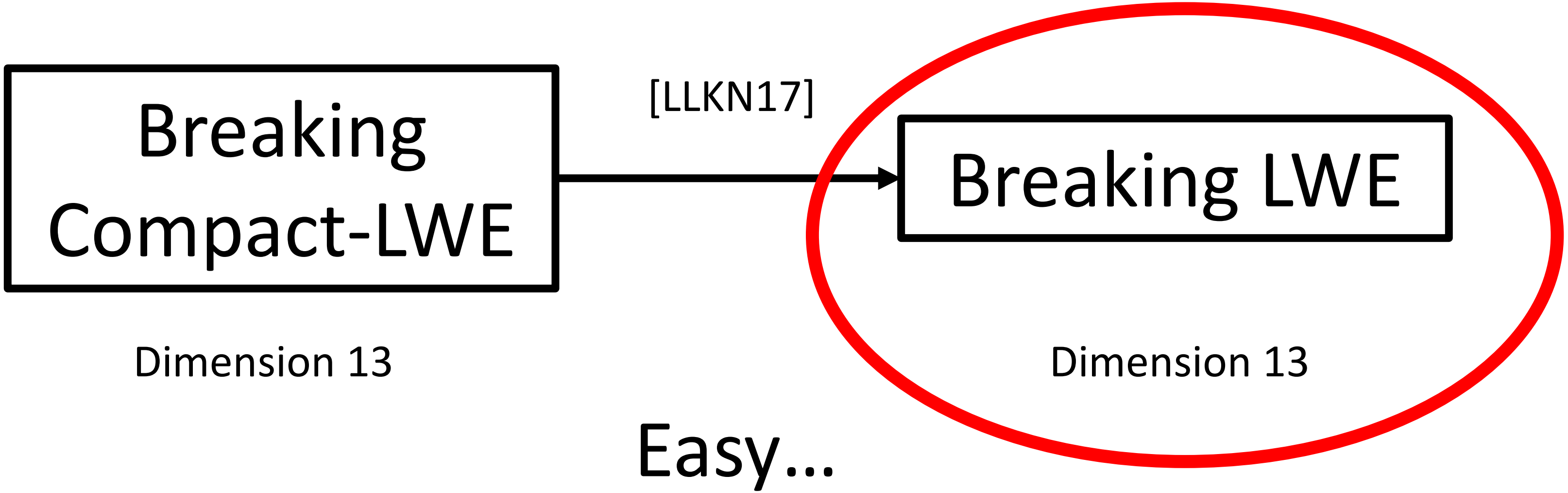
- Correctly decrypted 10,000/10,000 random ciphertexts
- 1.28 seconds to get a key
- 53 microseconds per ciphertext
- Over 18,000 decryptions per second

sage

PARAMETER CHOICE



Hardness Reductions



Breaking Compact-LWE

[LLKN17]

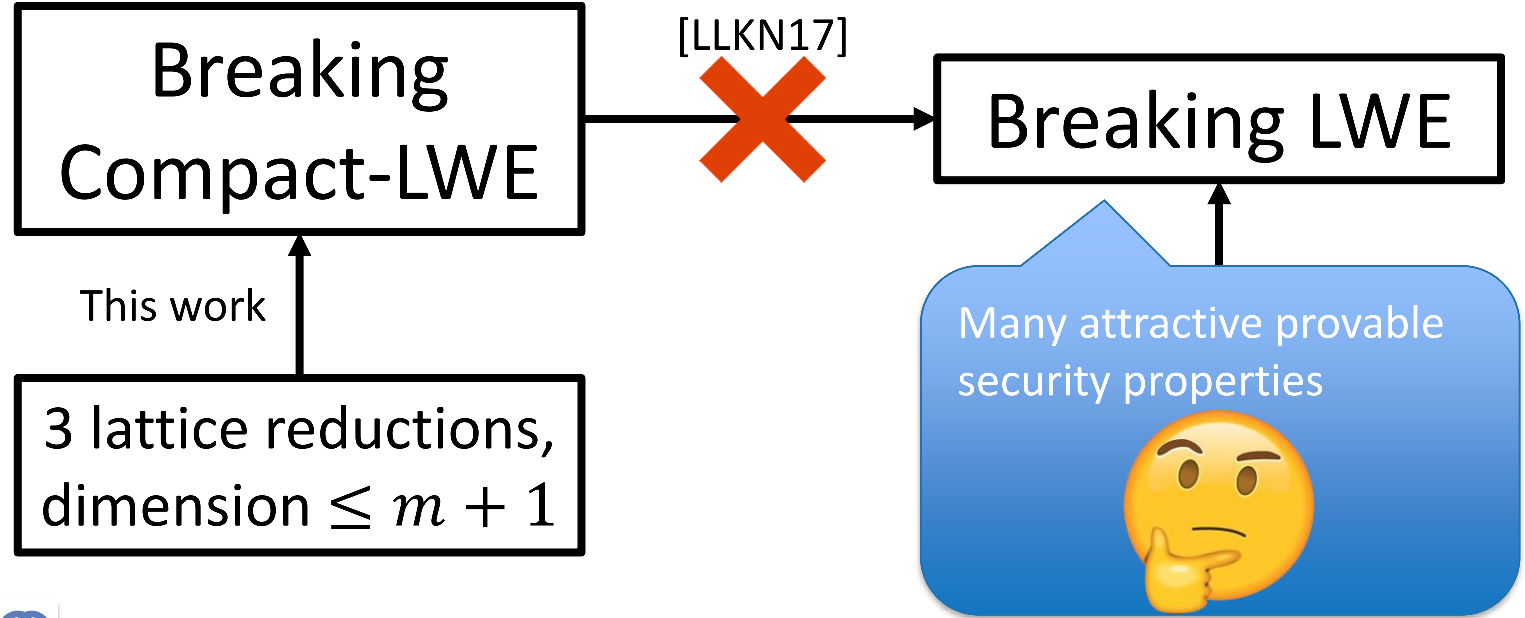
Breaking LWE

Dimension 13

Dimension 13

Easy…

Hardness Reductions



Breaking Compact-LWE

[LLKN17]

Breaking LWE

This work

3 lattice reductions, dimension $\leq m + 1$

Many attractive provable security properties 🤔

THANKS!

NIST Version Attack Paper: https://eprint.iacr.org/2018/020.pdf

NIST Version Attack Code: https://goo.gl/2Vo3T7