A New Lattice-based Threshold Verifiable Secret Sharing Scheme

Saba Karimani , Zahra Naghdabadi ,
Taraneh Eghlidos , Mohammad Reza Aref

saba_karimani , Naghdabadi_z@ee.sharif.edu
teghlidos , aref@sharif.edu

Electrical Engineering Department
Sharif University of Technology

May29,2018

A New Lattice-based Threshold Verifiable Secret Sharing Scheme

Saba Karimani , Zahra Naghdabadi ,

Taraneh Eghlidos , Mohammad Reza Aref

saba_karimani , Naghdabadi_z@ee.sharif.edu
teghlidos , aref@sharif.edu

Electrical Engineering Department
Sharif University of Technology

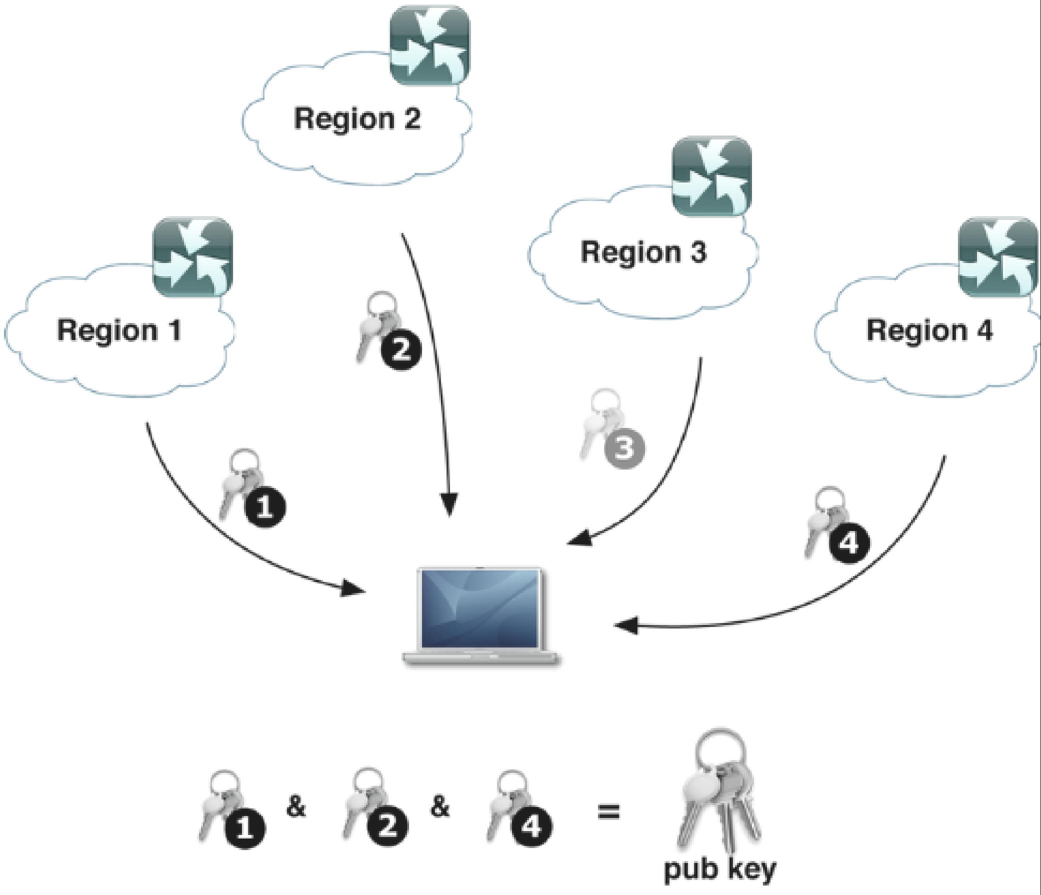
May29,2018

OUTLINE

- **Introduction:**
- What is secret sharing?
- History
- **Lattices**
- **Our proposed scheme**
- **Results**
- **Conclusion**

WHAT IS SECRET SHARING?

Secret sharing schemes make it possible to share a secret among a set P of participants in a way that only certain subsets of them can recover the secret.



WHY DO WE SHARE A SECRET?

AVOID CHEATING

Some body may sell out the secret

AVOID KEY LOSS

The person in charge may lose the key

KEY MANAGEMENT

Organize who gets access to the secret

SECRET SHARING STAGES

01

Shares Generation

The Dealer produces the shares

02

Shares Distribution

Shares are sent to participants through a secure channel

03

Shares Combination

t participants get together and recover the secret

DIFFERENT FEATURES

VERIFIABILITY

ACCESS STRUCTURE

MULTI-USE

HISTORY

1979

Secret Sharing problem was first solved independently by Shamir & Blakley

1994

Shor introduced quantum algorithms for solving factorization and discrete logarithm

2011

First lattice based (n, n) secret sharing scheme was proposed by Georgescu based on LWE problem

2015

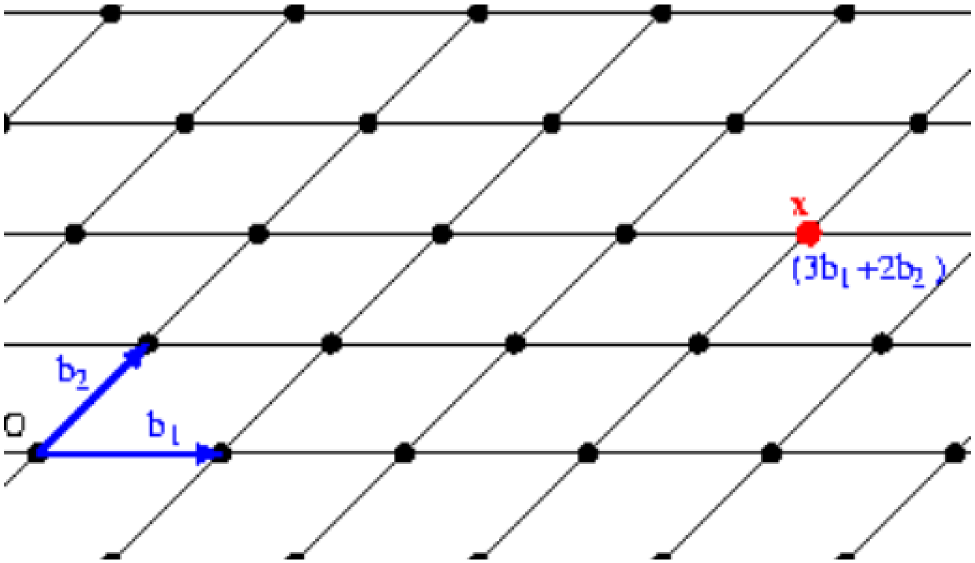
An efficient lattice based multi-stage secret sharing scheme was proposed by Pilaram & Eghlidos


Quantum computers can be
MILLION TIMES FASTER
than today computers

WHAT ARE LATTICES?

- An array of points in m-dimensional real vector space

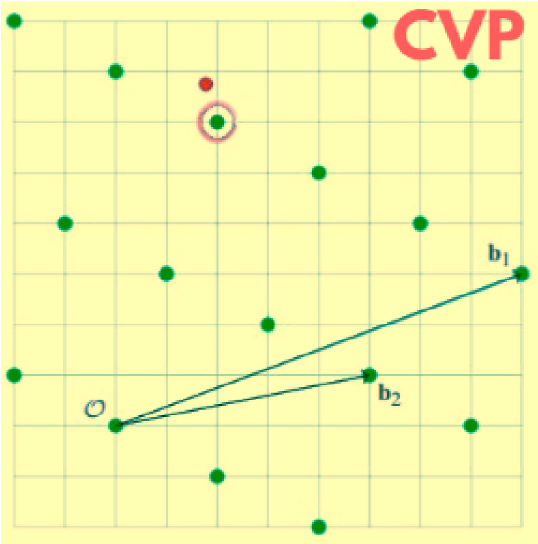
$$\Lambda = \mathcal{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z}\}$$

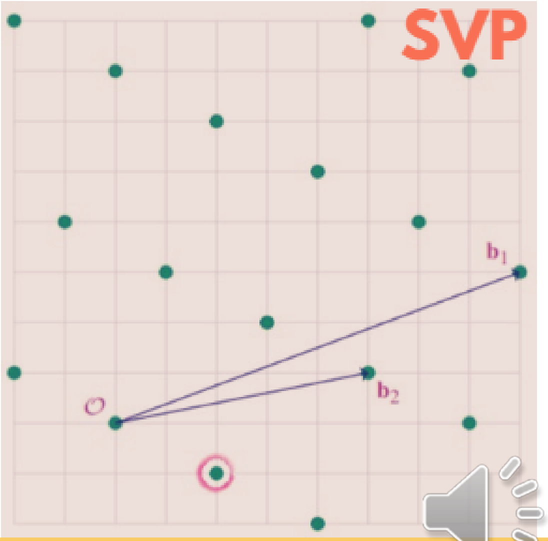


WHY LATTICES?

Most post-quantum schemes are lattice based.

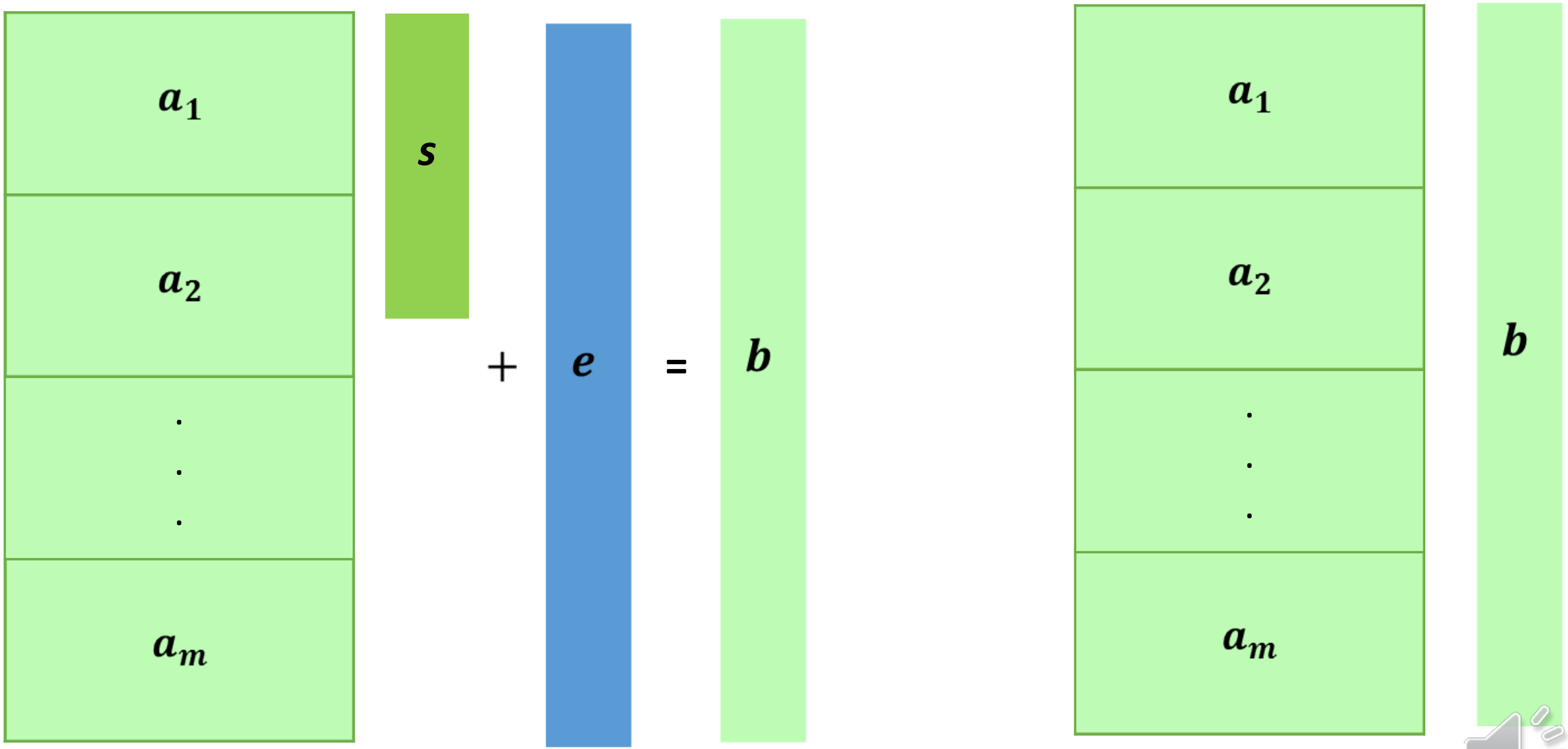
- provable security
- Linear and fast computations
- NP-hard problems





LEARNING WITH ERRORS (LWE) PROBLEM

There is a polynomial-time quantum reduction for solving certain lattice problems in the worst-case to solving LWE.(Regev O. [2])



AJTAI HASH FUNCTION

Coverting the function $f_A(x) = Ax\ modq$ for $n, m, q, d \in \mathbb{N}$,

$m > \frac{nlogq}{logd}$, $q = O(n^c)$, Random $x \in \{0,1, \dots , d-1\}^m$ and

uniformly random $A \in \mathbb{Z}_q^{n\times m}$ is equivalent to solving any

instance of approximate SVP which is still hard as there is no

classic /quantum algorithm to solve it.(Ajtai M. [1])

HOW TO SHARE A SECRET QUANTUM RESISTANTLY?

PRELIMINARIES

ALGORITHM 1

Outputs A, R.
R is a trapdoor for LWE problem

ALGORITHM 2

On inputs A, R and b for which b = As + e outputs s.

PE SECRET SHARING

Shares a matrix (m secrets) among participants.

ALGORITHMS

- **Algorithm (1) :** An efficient randomized algorithm which on inputs $t \geq 1, q \geq 2$ and $m = t(\lceil logq \rceil + 2)$, outputs a matrix $A \in \mathbb{Z}_q^{t \times m}$ and a trapdoor $R \in \mathbb{Z}^{2t \times t\lceil logq \rceil}$ such that A is computationally pseudorandom matrix under LWE assumption.

- **Algorithm (2) :** An efficient algorithm, with overwhelming probability over all random choices, for $\boldsymbol{s} \in \mathbb{Z}_q^m$ and $||\boldsymbol{e}|| < \frac{q}{O(\sqrt{tlogq})}$ or $\boldsymbol{e} \leftarrow D_{\mathbb{Z}^t, \alpha q}$ for $\frac{1}{\alpha} \geq \sqrt{tlogq}.\omega_t$, on inputs a pseudorandom matrix A, a trapdoor R and a vector $\boldsymbol{b}$ in the form of $\boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e}$, outputs **s**.

Micciancio D. and Peikert C. [3]

SHARES GENERATION

Generate and Send the share $(\widetilde{a}_i, \widetilde{b}_i, r_i, \widetilde{r}_i)$ to the participant P_i for $1 \leq i \leq n$ as follows:

Run Algorithm (1) with inputs $t \geq 1, q \geq 2, m = t[logq] + 2$ to get A, R.

$$A = \begin{pmatrix} a_1^T \\ \vdots \\ a_t^T \end{pmatrix} \qquad R = \begin{pmatrix} \widetilde{R_1} & \bar{R} \\ \widetilde{R_2} & \end{pmatrix}$$ and publish $\bar{R}$

Choose uniformly random integers $\alpha_j^i \in \mathbb{Z}_q$ for $+1 \leq i \leq n\,, 1 \leq j \leq t$.

Set $\widetilde{a}_i = a_i$ for $1 \leq i \leq t$

Set $\widetilde{a}_i = \sum_{j=1}^{t} \alpha_j^i a_j$ for $t + 1 \leq i \leq n$

Set $\widetilde{b}_i =< \widetilde{a}_i . s > +e_i$ for $1 \leq i \leq n$

Choose $\lambda_i \,, \widetilde{\lambda}_i \in \mathbb{Z}_q^t$ randomly with uniform distribution and publish them.

Set $r_i = \widetilde{R_1} \lambda_i \,, \widetilde{r}_i = \widetilde{R_2} \widetilde{\lambda}_i$

VERIFICATION

Choose $F \in \mathbb{Z}_q^{p\times m}$, $C \in \mathbb{Z}_q^{p\times t}$ randomly and publicly publish them. Set $f_s = Fs$, $\widetilde{f_{i_1}} = F\widetilde{a_i}$, $\widetilde{f_{i_2}} = Fb_i$ which b_i is the binary form of $\widetilde{b_i}$, $\widetilde{f_{i_3}} = Cr_i$, $\widetilde{f_{i_4}} = C\widetilde{r_i}$ for $1 \le i \le n$ and announce them as public values.

Compare $F\widetilde{a_i}$ with $\widetilde{f_{i_1}}$, Fb_i with $\widetilde{f_{i_2}}$, Cr_i with $\widetilde{f_{i_3}}$ and $C\widetilde{r_i}$ with $\widetilde{f_{i_4}}$

If shares are correctly verified, continue
Else, ask the dealer to resend the shares

SECRET RECOVERY

When participant $\{P_{i_1}, P_{i_2}, \dots, P_{i_t}\}$ get together:

Set $\widetilde{R_1} = \left[r_{i_1}, \dots, r_{i_t}\right]\left[\lambda_{i_1}, \dots, \lambda_{i_t}\right]^{-1}$

Set $\widetilde{R_2} = \left[\widetilde{r_{i_1}}, \dots, \widetilde{r_{i_t}}\right]\left[\widetilde{\lambda_{i_1}}, \dots, \widetilde{\lambda_{i_t}}\right]^{-1}$

Set $R = \begin{pmatrix} \widetilde{R_1} & \bar{R} \\ \widetilde{R_2} & \end{pmatrix}$

Set $\tilde{b} = \begin{pmatrix} \widetilde{b_{i_1}} \\ \vdots \\ \widetilde{b_{i_t}} \end{pmatrix}$ and $\tilde{A} = \begin{pmatrix} \widetilde{a_{i_1}}^T \\ \vdots \\ \widetilde{a_{i_t}}^T \end{pmatrix}$

Run Algorithm (2) with input $(\tilde{A}, R, \tilde{b})$ to obtain the secret s.
Compare Fs with f_s for verification.

SECURITY THEOREMS

Theorem 1: In the proposed scheme, any subset of participants of size less than t cannot recover the undisclosed trapdoor **R**.

Theorem 2: In the proposed scheme, any subset of participants of size less than t cannot recover the secret **s**.

RESULTS

scheme	Access structure	type	Verifiability
Shamir	(t, n)	Polynomials and Lagrange interpolation	No
Blakley	(t, n)	Hyperplanes intersection	No
Georgescu	(n, n)	Lattice-based (LWE-based)	Yes (not post-quantum)
Bansarkhani	(n, n)	Lattice-based (Ajtai-based)	Yes
Pilaram & Eghlidos	(t, n)	Lattice-based (Ajtai-based)	Yes
Our scheme	(t, n)	Lattice-based (LWE-based)	Yes

SUMMARY

- Secret Sharing
- Lattices
- A new scheme

Applications:

Electronic voting

Cloud computing

...

Features:

Verifiability

threshold access structure

LWE-based

REFERENCES

1. M. Ajtai, “Generating hard instances of lattice problems (extended abstract),” in Proc. 28th Annu. ACM Symp. Theory Comput., 1996.

2. Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography." Journal of the ACM (JACM) 56, no. 6 (2009).

3. Micciancio D. and Peikert C., "Trapdoors for lattices: Simpler, tighter, faster, smaller." In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2012.

4. Pilaram, H. and Eghlidos, T. “An efficient lattice based multi-stage secret sharing scheme”, Dependable and Secure Computing, IEEE Transactions on, PrePrint (2015).

THANK YOU

for your time!

AN EFFICIENT LATTICE BASED MULTI-STAGE SECRET SHARING SCHEME

01

02

03

Shares generation:

v: public vector , $S_i = B_i v$

$A_i C = B_i W$ for i=1,…,m

Shares distribution:

Participant P_j's Share: vector c_j

Public: matrices A_i, i=1,…,m and λ_j, j=1,…,n

Participant P_j 's Share: vector c_j

Shares combination:

Pilaram, H. and Eghlidos, T. [4], PE

SHARES COMBINATION

Participants $\{j_1, \dots, j_t\} \subseteq \{1, \dots, n\}$Desired secret $S_i, i \in \{1, \dots, n\}$
Send Vector $d^i_{j_l} = A_i c_{j_l},\ l = 1, \dots t$ to the combiner

$D_i = [d^i_{j_1}, \dots, d^i_{j_t}]$, $W = [\lambda_{j_1}, \dots, \lambda_{j_t}]$

$D_i W^{-1} = [d^i_{j_1}, \dots, d^i_{j_t}] W^{-1} = [A_i c_{j_1}, \dots, A_i c_{j_t}] W^{-1} =$
$[B_i \lambda_{j_1}, \dots, B_i \lambda_{j_t}] W^{-1} = B_i [\lambda_{j_1}, \dots, \lambda_{j_t}] W^{-1} = B_i W W^{-1} = B_i$

Combiner: $s_i = B_i v$