

An Introduction to Lattice-Based Cryptography

Dana Dachman-Soled
University of Maryland
danadach@umd.edu

Traditional Crypto Assumptions

- Factoring: Given $N = pq$, find p, q
 - RSA Given $N = pq, e, x^e \bmod N$, find x .
- Discrete Log: Given $g^x \bmod p$, find x .
 - Diffie-Hellman Assumptions (g^x, g^y, g^{xy}) ,
 (g^x, g^y, g^z)

Are They Secure?

- Algorithmic Advances:
 - Factoring: Best algorithm time $2^{\tilde{O}(n^{\frac{1}{3}})}$ to factor n -bit number.
 - Discrete log: Best algorithm $2^{\tilde{O}(n^{\frac{1}{3}})}$ for groups Z_p^* , where p is n bits.
 - [Adrian et al. 2015] With preprocessing could possibly be feasible for nation-states and $n = 1024$.
 - Quasipolynomial time algorithms for small characteristic fields. Not known to apply in practice.
- Quantum Computers:
 - Shor's algorithm solves both factoring and discrete log in quantum polynomial time ($\tilde{O}(n^2)$).

Are They Secure?

“For those partners and vendors that have not yet made the transition to Suite B algorithms (ECC), we recommend not making a significant expenditure to do so at this point but instead to **prepare for the upcoming quantum resistant algorithm transition**.... Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy. ”—NSA Statement, August 2015

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

Google Dabbles in Post-Quantum Cryptography

By Richard Adhikari
Jul 12, 2016 2:06 PM PT

 Print
 Email

Post-Quantum Approach

- New set of assumptions based on finding short vectors in lattices.
- Believed to be hard for quantum computers.
- Evidence of hardness “worst case to average case reduction”.
- Versatile: Can essentially construct all cryptosystems out of these assumptions.

My Research

- New efficient cryptosystems from post-quantum assumptions
 - Constant Round Group Key Exchange [1]
- Understanding the concrete hardness of NIST candidate cryptosystems [2], [3]
- Understanding the hardness of post-quantum cryptosystems under side-channel leakage [2], [4], [5]

[1] Constant-Round Group Key-Exchange from the Ring-LWE Assumption. D. Apon, D. Dachman-Soled, H. Gong, J. Katz. PQCrypto 2019.

[2] LWE with Side Information: Attacks and Concrete Security Estimation. D. Dachman-Soled, L. Ducas, H. Gong, M. Rossi. IACR ePrint Cryptology archive.

[3] Partial Key Exposure in Ring-LWE-Based Cryptosystems: Attacks and Resilience. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. . IACR ePrint Cryptology archive.

[4] (In)Security of Ring-LWE Under Partial Key Exposure. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. Mathcrypt 2019. Journal of Mathematical Cryptology, to appear.

[5] Towards a Ring Analogue of the Leftover Hash Lemma. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. Mathcrypt 2019. Journal of Mathematical Cryptology, to appear.

Math Prelim

Matrix Multiplication

$$\begin{array}{cccc}
 m_{1,1} & m_{1,2} & m_{1,3} & v_{1,j} \\
 m_{2,1} & m_{2,2} & m_{2,3} & v_{2,j} \\
 m_{3,1} & m_{3,2} & m_{3,3} & v_{3,j}
 \end{array} \times \begin{array}{c} v_{1,j} \\ v_{2,j} \\ v_{3,j} \end{array} = \sum_{i=1}^3 v_{i,j} \cdot \begin{array}{c} m_{1,i} \\ m_{2,i} \\ m_{3,i} \end{array}$$

$$\begin{array}{cccccc}
 m_{1,1} & m_{1,2} & m_{1,3} & v_{1,1} & v_{1,2} & v_{1,3} \\
 m_{2,1} & m_{2,2} & m_{2,3} & v_{2,1} & v_{2,2} & v_{2,3} \\
 m_{3,1} & m_{3,2} & m_{3,3} & v_{3,1} & v_{3,2} & v_{3,3}
 \end{array} \times \begin{array}{c} v_{2,1} \\ v_{2,2} \\ v_{2,3} \end{array} :$$

For $j \in \{1,2,3\}$, j -th column of the output is computed as :

$$\sum_{i=1}^3 v_{i,j} \cdot \begin{array}{c} m_{1,i} \\ m_{2,i} \\ m_{3,i} \end{array}$$

Lattices

An n -dimensional lattice L is an additive discrete subgroup of R^n . A basis $\mathbf{B} \in R^{n \times n}$ defines a lattice $L(\mathbf{B})$ in the following way:

$$L(\mathbf{B}) = \{\mathbf{v} \in R^n \text{ s.t. } \mathbf{v} = \mathbf{B}\mathbf{z} \text{ for some } \mathbf{z} \in Z^n\}.$$

“integer linear combinations of the basis vectors”

i -th successive minima $\lambda_i(L(\mathbf{B}))$: The smallest radius r such that there are i linearly independent vectors $\{v_1, \dots, v_i\}$ of length at most r .

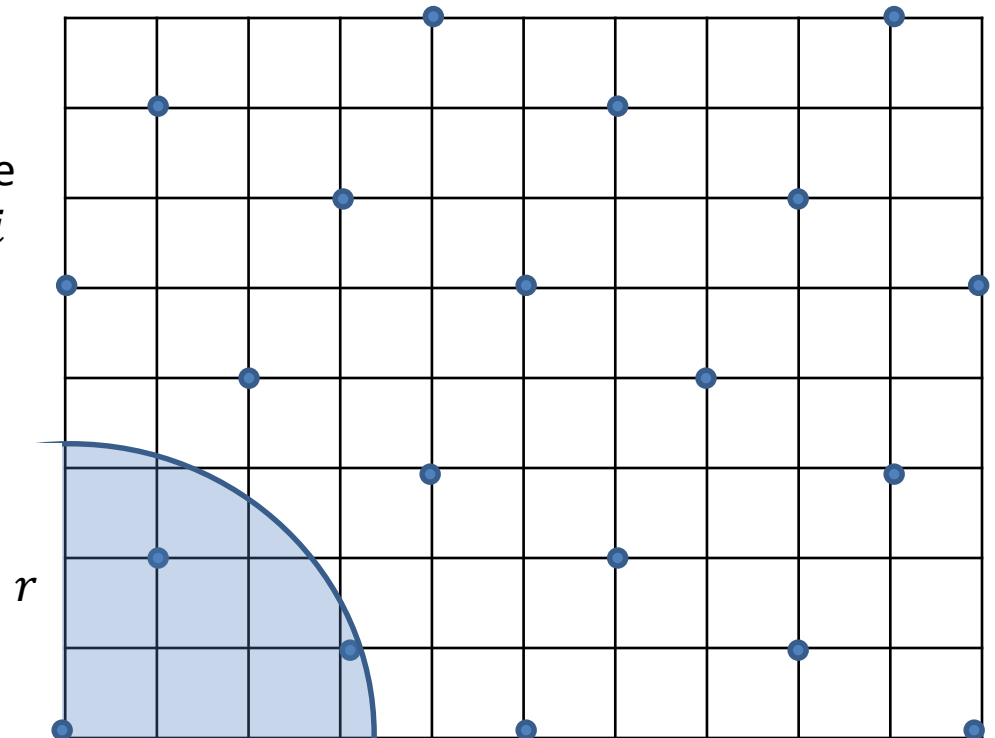
Shortest vector: $(1,2)$

$$\lambda_1 = \sqrt{5}$$

Shortest basis:

$$\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$$

$$\lambda_2 = \sqrt{10}$$



Lattices

An n -dimensional lattice L is an additive discrete subgroup of R^n . A basis $\mathbf{B} \in R^{n \times n}$ defines a lattice $L(\mathbf{B})$ in the following way:

$$L(\mathbf{B}) = \{\mathbf{v} \in R^n \text{ s.t. } \mathbf{v} = \mathbf{B}\mathbf{z} \text{ for some } \mathbf{z} \in Z^n\}.$$

“integer linear combinations of the basis vectors”

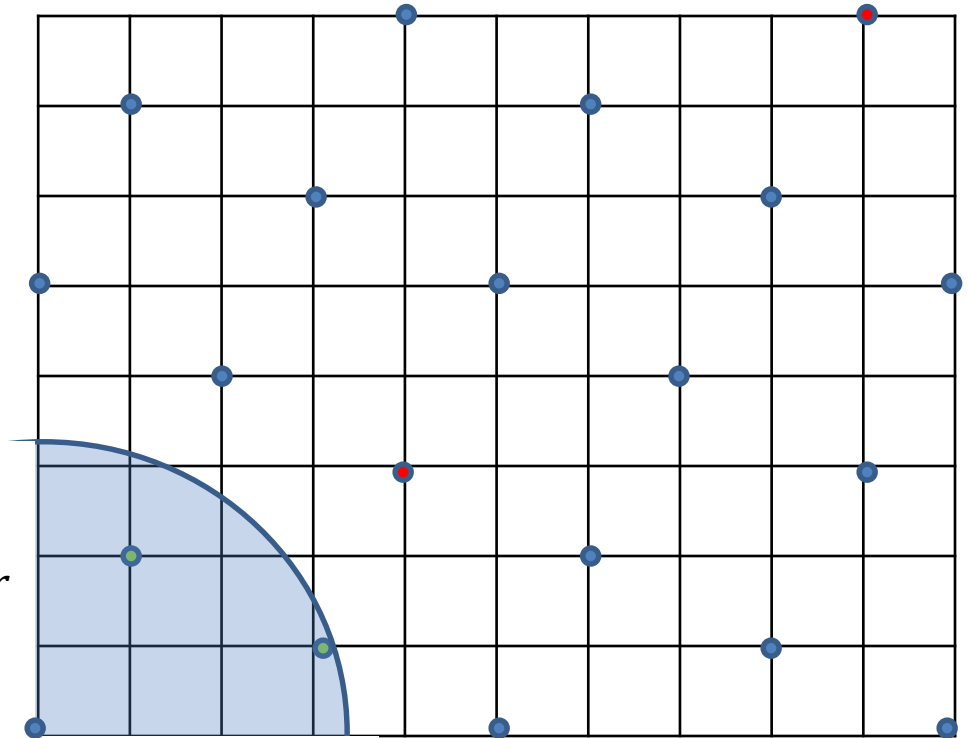
Basis is not unique!

For the lattice to the right,

$\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$ form a basis

$\begin{pmatrix} 4 & 9 \\ 3 & 8 \end{pmatrix}$ also form a basis

Given two bases B, B' , they define the same lattice iff $B' = BU$, where U is a r unimodular matrix (determinant ± 1).



Hard Lattice Problems

- Are all parameterized by “approximation factor” $\gamma > 1$.
- **Shortest Vector Problem (SVP)**: Given a basis B , find a non-zero vector $\mathbf{v} \in L(\mathbf{B})$ whose length is at most $\gamma \cdot \lambda_1(L(\mathbf{B}))$.
- **Shortest Independent Vector Problem (SIVP)**: Given a basis B , find a linearly independent set $\{v_1, \dots, v_n\}$ such that all vectors have length at most $\gamma \cdot \lambda_n(L(\mathbf{B}))$.
- **Gap Shortest vector problem (GapSVP)**: Given a basis B , and a radius $r > 0$
 - Return YES if $\lambda_1(L(B)) \leq r$
 - Return NO if $\lambda_1(L(B)) > \gamma \cdot r$.

Believed hard
even for a
quantum
computer!

Cryptographic Hard Problems

The SIS Problem

Dimension m

$A \times z = \vec{0} \pmod{p}$

Dimension n

Public $n \times m$ matrix A , with entries chosen at random over Z_p

$n \ll m$

Problem: Given A , find $z \in \{0,1\}^m$
(or sufficiently “short” z)

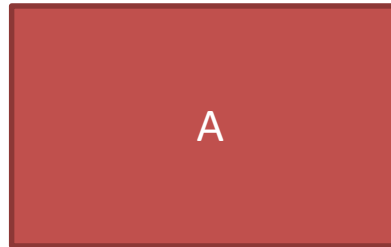
Relation to Lattices

- Worst-Case to Average-Case Reduction:
Breaking the cryptosystem on average is as hard as breaking the hardest instance of the underlying lattice problem.
- SIS:
 - Worst-Case to Average-Case Reduction from SIVP.

CRHF from Lattices

CRHF from Lattices

Public
Matrix:



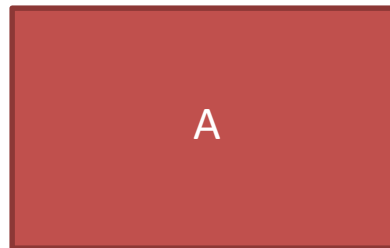
Input:



$$z \in \{0,1\}^m$$

Public $n \times m$ matrix A , with
entries chosen at random
over Z_p

To evaluate the
hash on z
output:



\times



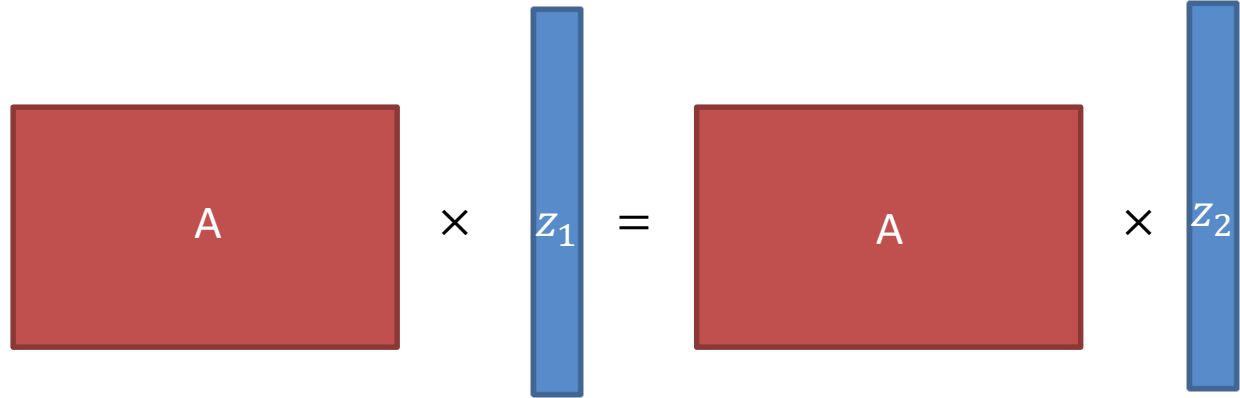
$=$



$$u \in Z_p^n$$

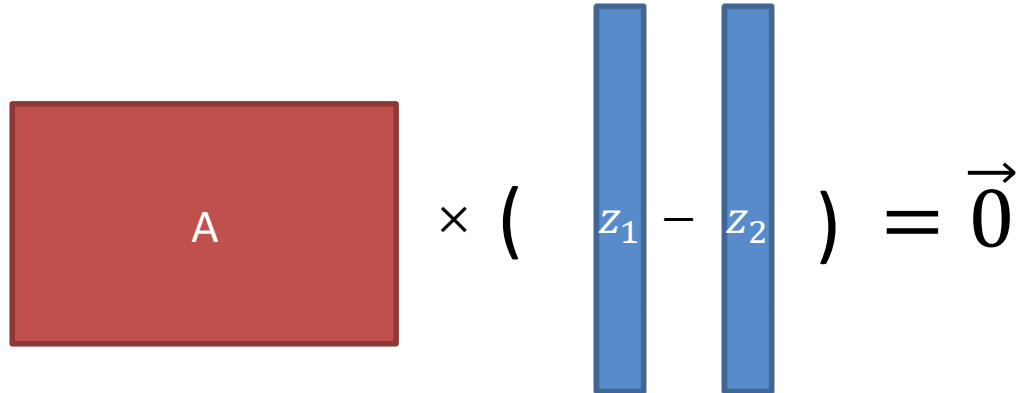
CRHF from Lattices

Given a collision
 $z_1, z_2 \in \{0,1\}^m$:



A diagram illustrating the equation $A \times z_1 = A \times z_2$. It features two red rectangular boxes, each containing the letter 'A'. To the right of the first 'A' box is a blue vertical bar containing the text z_1 . To the right of the second 'A' box is a blue vertical bar containing the text z_2 . Multiplication symbols (\times) are placed between the 'A' boxes and their respective z bars, and an equals sign (=) is placed between the two z bars.

Obtain
 $(z_1 - z_2) \in$
 $\{-1,0,1\}^m$:

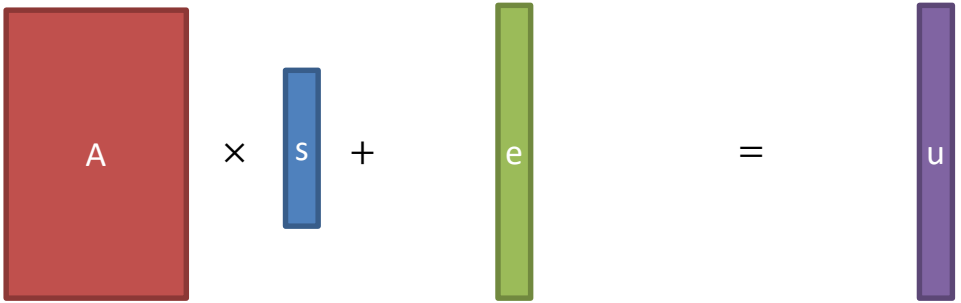


A diagram illustrating the equation $A \times (z_1 - z_2) = \vec{0}$. It features a red rectangular box containing the letter 'A'. To its right is a blue vertical bar containing z_1 , followed by a minus sign ($-$), another blue vertical bar containing z_2 , and a closing parenthesis $)$. To the right of the parenthesis is an equals sign (=) followed by a bolded zero with a vector arrow above it ($\vec{0}$). Multiplication symbols (\times) are placed between the 'A' box and the parenthesis, and between the parenthesis and the zero.

The LWE Problem (Search)

Secret n -dimension vector s
with entries chosen at random

Operations are mod p .



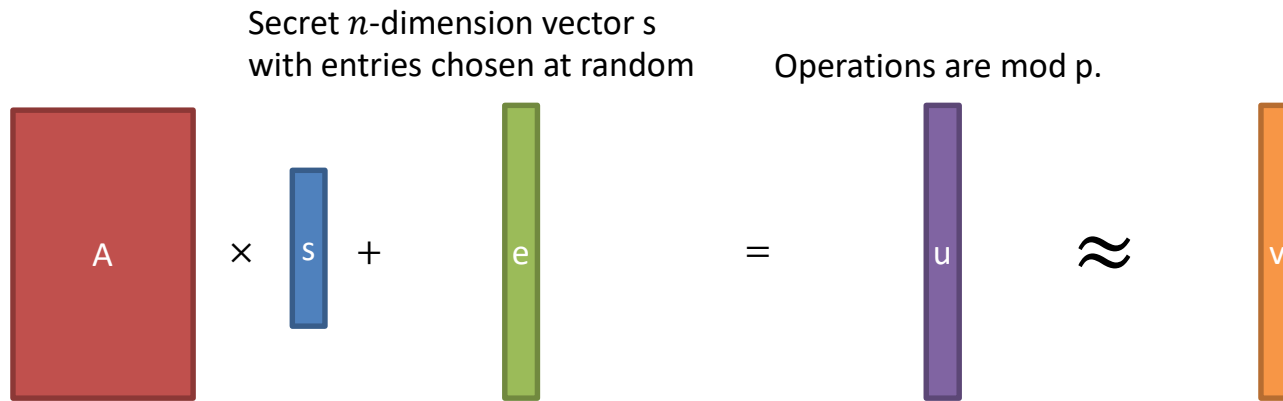
Public $m \times n$ matrix A , with
entries chosen at random
over Z_p

m -dimension error
vector e , with entries
sampled from χ .

$$A \times s + e = u$$

Problem: Given, A , $u = As+e$, find s .

The LWE Problem (Decision)



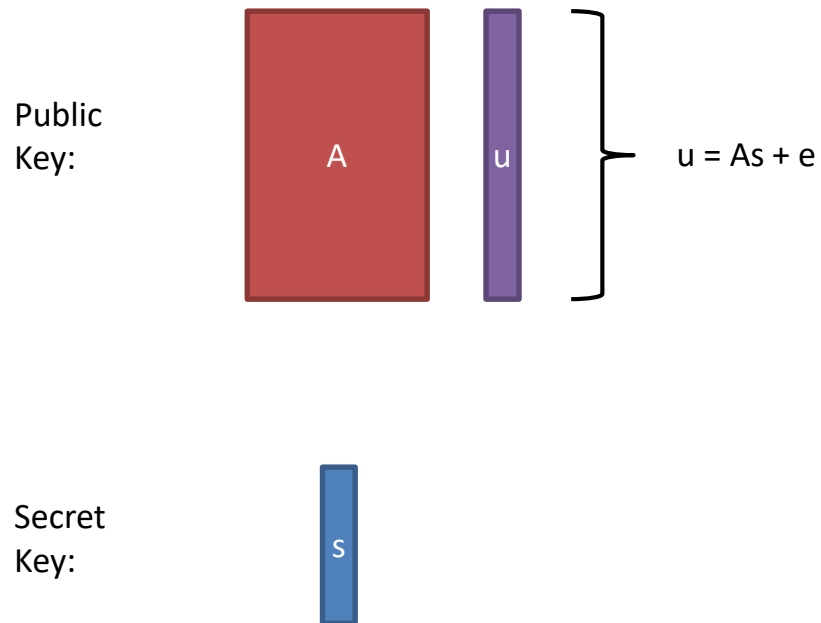
Problem: Distinguish (A, u) from (A, v)

Relation to Lattices

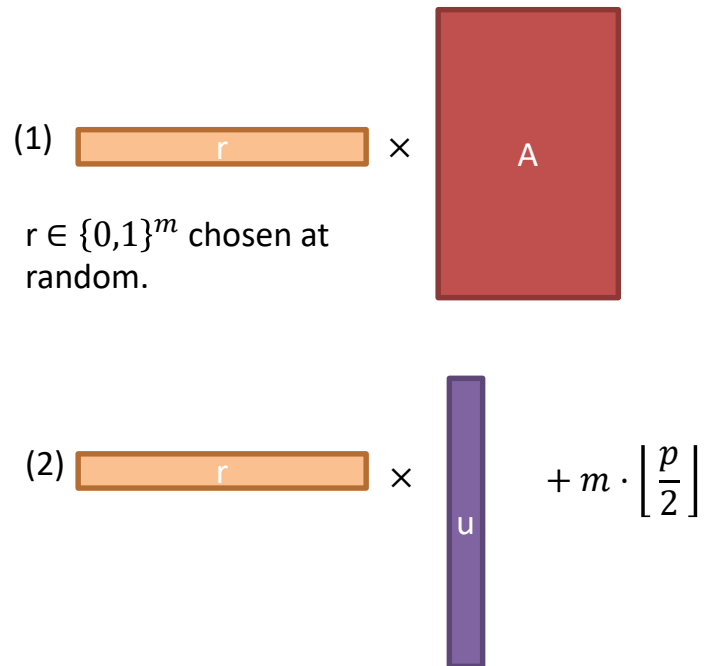
- Worst-Case to Average-Case Reduction:
Breaking the cryptosystem on average is as hard as breaking the hardest instance of the underlying lattice problem.
- LWE:
 - Worst-Case to Average-Case **Quantum** Reduction from SIVP.
 - Worst-Case to Average-Case **Classical** Reductions from GapSVP.

Lattice-Based Encryption

Regev's Cryptosystem [Regev '04]



Regev's Cryptosystem—Encryption of $m \in \{0,1\}$



Regev's Cryptosystem—Decryption

The diagram illustrates the decryption process in Regev's cryptosystem. It shows the relationship between the ciphertext u , the public key matrix A , the secret key vector s , and the error vector e . The equation $u = As + e$ is shown, where u is a purple vertical vector, A is a red square matrix, and s is a blue vertical vector. The error vector e is represented by the term $+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor$. A horizontal orange vector r is shown to the left of u , and another horizontal orange vector r is shown to the left of A . A blue bracket groups A and s together, with a multiplication sign \times between them. A horizontal line is drawn below the r and u components.

$$r \times u = u = As + e + m \cdot \left\lfloor \frac{p}{2} \right\rfloor$$
$$\left[r \times A \right] \times s$$

Regev's Cryptosystem—Decryption

The diagram illustrates the decryption process in Regev's cryptosystem. It shows the relationship between the ciphertext u , the public key r , the matrix A , and the secret key s .

The ciphertext u is represented by a purple vertical bar. The public key r is represented by an orange horizontal bar. The matrix A is represented by a red square, and the secret key s is represented by a blue vertical bar.

The equation $u = As + e$ is shown, where e is the error term. The error term is defined as $e = m \cdot \left\lfloor \frac{p}{2} \right\rfloor$.

The diagram shows the ciphertext u is equal to the product of the public key r and the matrix A multiplied by the secret key s , plus the error term e .

$$u = r \times \left[A \times s \right] + m \cdot \left\lfloor \frac{p}{2} \right\rfloor$$

Regev's Cryptosystem—Decryption

$$\begin{array}{l} \text{—} \\ r \times u \\ r \times w \end{array} \left. \vphantom{\begin{array}{l} r \times u \\ r \times w \end{array}} \right\} \begin{array}{l} u = As + e \\ w = As \end{array} + m \cdot \left\lfloor \frac{p}{2} \right\rfloor = r \times e + m \cdot \left\lfloor \frac{p}{2} \right\rfloor$$

The diagram illustrates the decryption process in Regev's cryptosystem. It shows two rows of vectors. The top row consists of a horizontal orange box labeled 'r' followed by a vertical purple box labeled 'u'. A bracket to the right of 'u' is labeled 'u = As + e'. The bottom row consists of a horizontal orange box labeled 'r' followed by a vertical purple box labeled 'w'. A bracket to the right of 'w' is labeled 'w = As'. To the right of these two rows is the expression '+ m · ⌊ p/2 ⌋'. An equals sign follows, leading to a horizontal orange box labeled 'r' followed by a vertical green box labeled 'e', and another '+ m · ⌊ p/2 ⌋' to the right. A horizontal line is drawn above the top row.

Regev's Cryptosystem—Decryption

$$\begin{aligned} & \text{—} \\ & \begin{array}{l} \text{orange } r \times \text{purple } u \\ \text{orange } r \times \text{dark blue } w \end{array} \left. \vphantom{\begin{array}{l} \text{orange } r \times \text{purple } u \\ \text{orange } r \times \text{dark blue } w \end{array}} \right\} \begin{array}{l} u = As + e \\ w = As \end{array} + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \\ & = \text{orange } r \times \text{green } e + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \\ & \approx 0 + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \end{aligned}$$

Properties of LWE

- Equivalence of Search/Decision LWE
- Equivalence of LWE with random secret/secret drawn from error distribution

Efficiency

- Efficiency is a main concern in lattice-based cryptosystems.
- In both SIS and LWE-based cryptosystems, the public key consists of a random matrix of size $m \times n$ ($m \geq n \log p$), requiring space $O(n^2 \log^2 p)$.
 - RSA and discrete-log based cryptosystems: public key size is linear in the security parameter.
- To reduce the public key size, consider lattices with structure.
- This is the Ring-LWE setting.

Ring-LWE Setting

- Highly efficient key exchange protocols are possible in the Ring-LWE setting.
 - Similar to Diffie-Hellman Key Exchange
- It is likely that at least one such scheme will be standardized by NIST.
- Details in the slides, but will skip in the lecture.

Summary

- Lattice-based cryptography is a promising approach for efficient, post-quantum cryptography.
- All the basic public key primitives can be constructed from these assumptions:
 - Public key encryption, Key Exchange, Digital Signatures
- For more information on research projects, please contact me at: danadach@umd.edu

Thank you!

The Ring Setting

- Quotient ring $\mathbb{Z}_q[x]/\Phi_m(x)$, where Φ_m is the m -th cyclotomic polynomial of degree $\varphi(m)$
 - e.g., $\Phi_{2n} = x^n + 1, n = 2, q = 13$.
 - $x^2 = -1 \pmod{x^2 + 1}$
 - $12x^3 + 15x^2 + 9x + 25 \rightarrow 12x^3 + 2x^2 + 9x + 12 \rightarrow x - 2 + 9x + 12 \rightarrow (10, 10)$.
- Lattice is defined as an ideal $I \subseteq \mathbb{Z}[x]/\Phi_m(x)$.
- Ring-LWE and ring-SIS problems are defined by substituting the matrix A with polynomials from the quotient ring and substituting polynomial multiplication for matrix-vector multiplication.
- The public key is now a polynomial in $\mathbb{Z}_q[x]/\Phi_m(x)$, and so can be described using $O(n \log q)$ bits.

NTT Transform

Consider Φ_m , where m is a power of 2. Then degree is equal to n , power of 2, $m = 2n$. $\Phi_{2n} = x^n + 1$

- Consider prime q s.t. $q \equiv 1 \pmod{2n}$.
- Then we have n $2n$ -th primitive roots modulo q
 - Why? Z_q^* is cyclic with order $q - 1$. $2n \mid (q - 1)$.
 - Let g be a generator of Z_q^* . g is a $(q - 1)$ -th primitive root.
 - $g^{a \cdot 2n} = g^{q-1}$, since $2n \mid (q - 1)$. g^a is a $2n$ -th primitive root. Also $(g^a)^i$, where i is relatively prime to $2n$.
 - Note that $(g^a)^n = -1 \pmod{q}$. Modulo $x^n + 1$ means $x^n = -1$.
 - Let $\gamma_1, \dots, \gamma_n$ be the n number of $2n$ -th primitive roots
- For a polynomial $p(x) \in Z_q[x]/x^n+1$
- For every γ_i , $p(\gamma_i) \pmod{p}$ is equal to taking $p(x)$ modulo $x^n + 1$ and modulo q and then evaluating the reduced polynomial at γ_i .

NTT Transform

- For a polynomial $p(x) \in \mathbb{Z}_q[x]/x^n+1$
- Evaluate $p(x)$ on all n number of $2n$ -th primitive roots. Obtain a vector $p(\gamma_1) \dots p(\gamma_n)$.
- Can now do both addition and multiplication coordinate-wise.

Key Exchange from Ring-LWE

Simple Key Exchange

P_1

P_2

$$(a, u_1 = a \cdot s_1 + e_1)$$

s_1

s_2

$$(a, u_2 = a \cdot s_2 + e_2)$$

$$u_2 \cdot s_1 \approx a \cdot s_2 \cdot s_1$$

RECONCILIATION

$$u_1 \cdot s_2 \approx a \cdot s_1 \cdot s_2$$