

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

NP ♀

BQP

- 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 and FHE assumptions [1], [7]
- Concrete hardness of post-quantum cryptosystems (with or without side information) [2], [3], [4], [5], [6], [8], [9]
- Concrete hardness of FHE (with or without side information) [10]

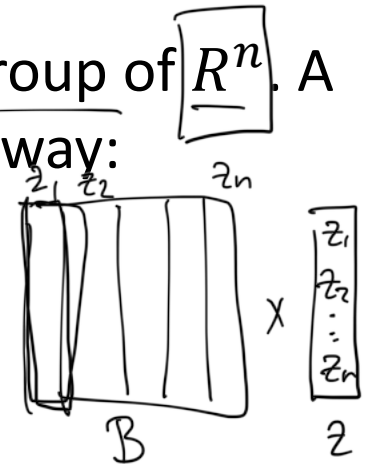
- [1] Constant-Round Group Key-Exchange from the Ring-LWE Assumption. D. Apon, D. Dachman-Soled, H. Gong, J. Katz. PQCrypto 2019.
- [2] LWE with Side Information: Attacks and Concrete Security Estimation. D. Dachman-Soled, L. Ducas, H. Gong, M. Rossi, CRYPTO 2020.
- [3] Security of NewHope under Partial Key Exposure. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. Research in Mathematics and Public Policy, 2020
- [4] (In)Security of Ring-LWE Under Partial Key Exposure. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. Journal of Mathematical Cryptology, 2020.
- [5] Towards a Ring Analogue of the Leftover Hash Lemma. D. Dachman-Soled, H. Gong, M. Kulkarni, A. Shahverdi. Journal of Mathematical Cryptology, 2020.
- [6] BKW Meets Fourier: New Algorithms for LPN with Sparse Parities. D. Dachman-Soled, H. Gong, H. Kippen, A. Shahverdi. TCC 2021
- [7] Compressed Oblivious Encoding for Homomorphically Encrypted Search. S. G. Choi, D. Dachman-Soled, D. Gordon, L. Liu, A. Yerukhimovich. CCS 2021
- [8] When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer. M. Fahr Jr., H. Kippen, A. Kwong, T. Dang, J. Lichtinger, D. Dachman-Soled, D. Genkin, A. Nelson, R. Perlner, A. Yerukhimovich, D. Apon. CCS 2022, RWC 2023
- [9] Refined Security Estimation for LWE with Hints via a Geometric Approach. D. Dachman-Soled, H. Gong, T. Hanson, H. Kippen, CRYPTO 2023.
- [10] On the Concrete Security of Approximate FHE with Noise-Flooding Countermeasures, Cryptology ePrint Archive.

Lattices

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

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

“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 .

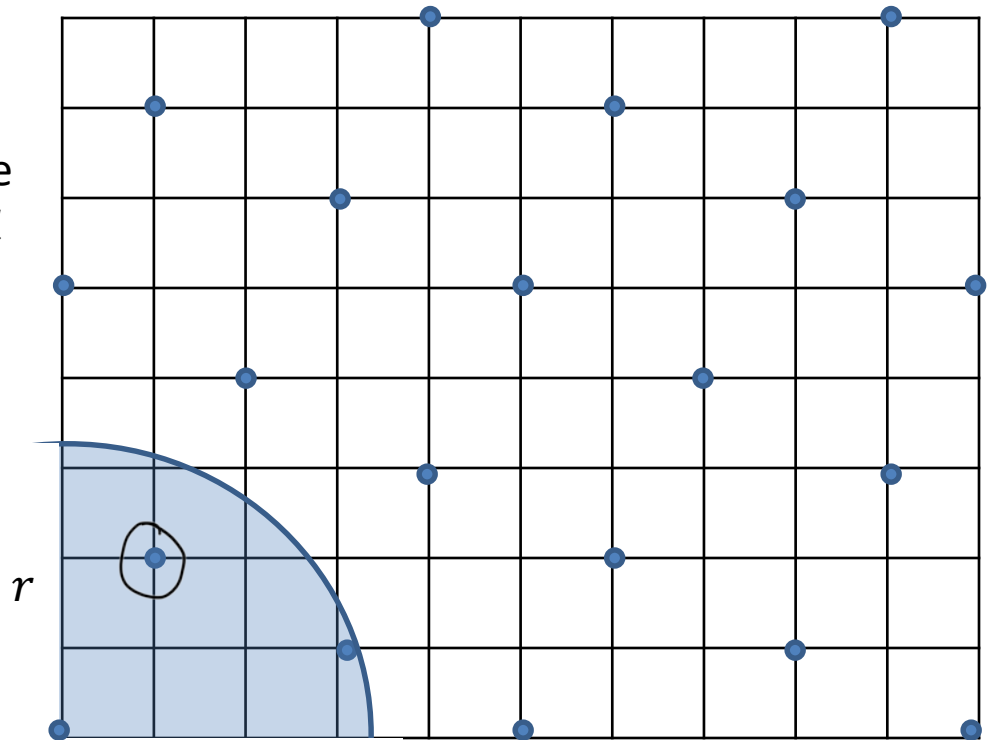
Shortest vector: $(1, 2)$

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

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!

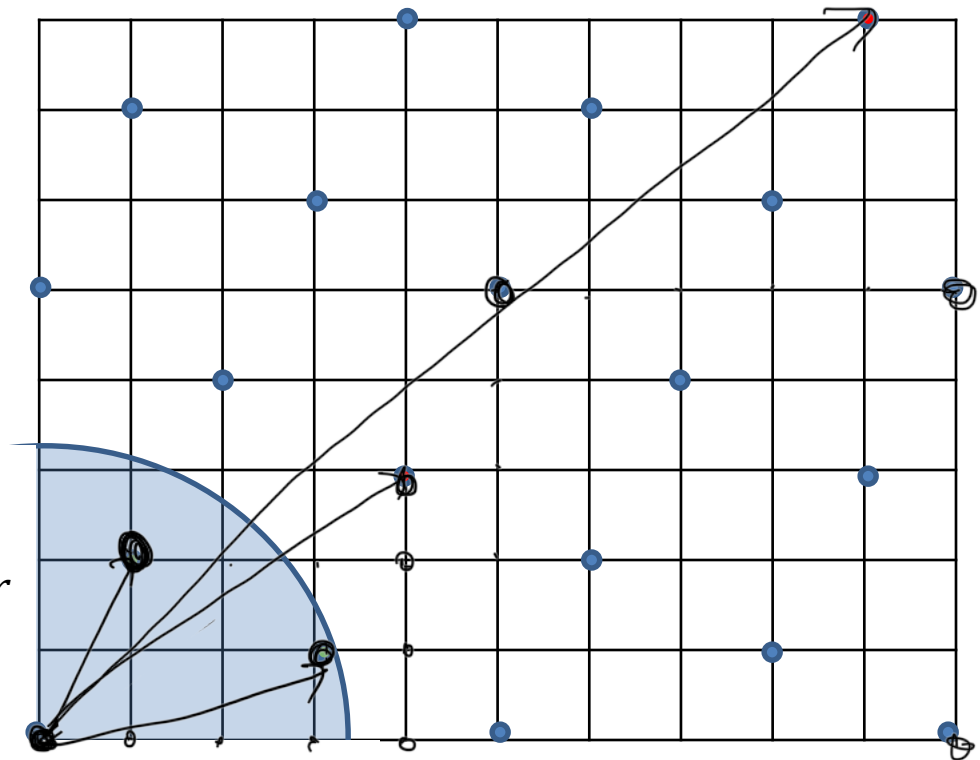
For the lattice to the right,

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

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

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

matrix integer + its inverse is integer



Hard Lattice Problems

- Are all parameterized by “approximation factor” $\gamma > 1$.
- **Shortest Vector Problem (SVP)**: Given a basis B , find a non-zero vector $v \in L(B)$ whose length is at most $\gamma \cdot \lambda_1(L(B))$. $\rightarrow (n^2)$
- **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 $\gamma \cdot \lambda_n(L(B))$.
- **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 $\lambda_1(L(B)) > \gamma \cdot r$.

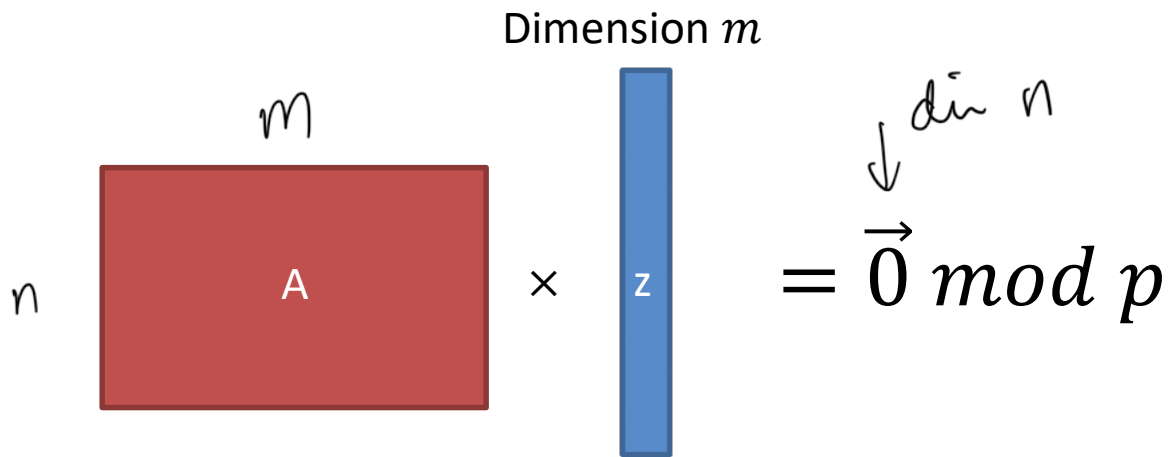
(Promise Problem)

Believed hard
even for a
quantum
computer!

Cryptographic Hard Problems

Shortest Integer Solution

The SIS Problem



Public $n \times m$ matrix A , with entries chosen at random over \mathbb{Z}_p

$n \ll m$

Dimension n

$\{-1, 0, 1\}^m$

$p \approx 10^4$

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

Relation to Lattices

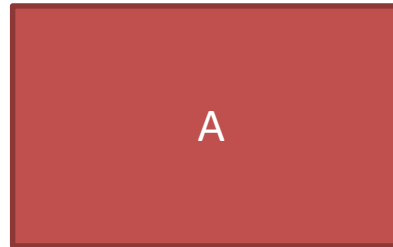
- Worst-Case to Average-Case Reduction:
Breaking the cryptosystem on average is as hard as breaking the hardest instance of the underlying lattice problem.
- SIS:
 - Worst-Case to Average-Case Reduction from SIVP.

find
shortest
basis

CRHF from Lattices

CRHF from Lattices

Public Matrix:



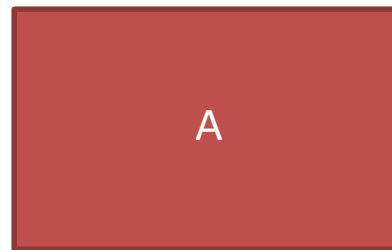
Input:



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

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

To evaluate the hash on z output:



\times



$=$



$$u \in Z_p^n$$

$$z_1, z_2 \in \{0,1\}^m$$

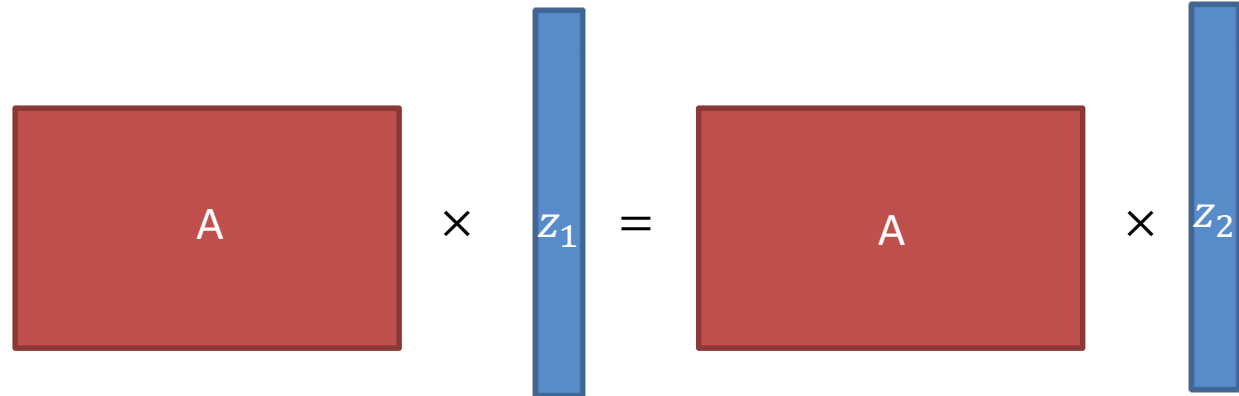
$$Az_1 = u \quad Az_2 = u$$

$$A \begin{bmatrix} z_1 \\ -z_2 \end{bmatrix} = 0 \pmod p$$

← SIS solution

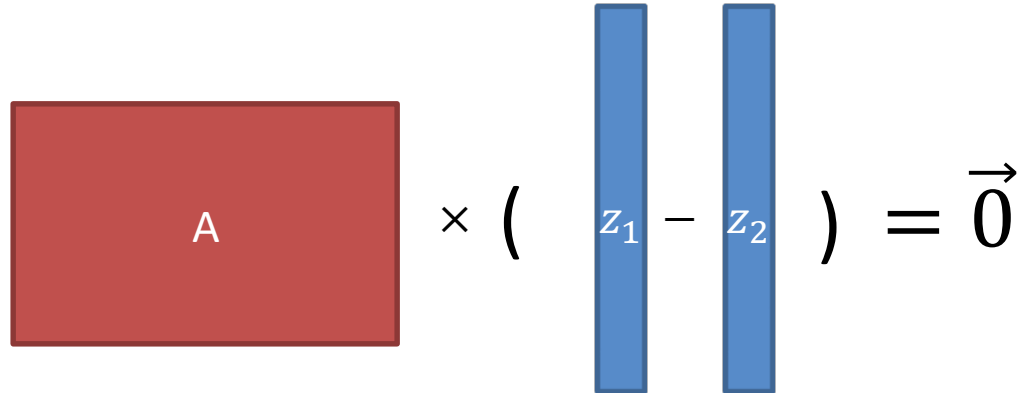
CRHF from Lattices

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 blocks, each labeled with the letter 'A'. The first 'A' block is on the left, followed by a multiplication symbol '×', a blue vertical bar labeled 'z₁', an equals sign '=', a second 'A' block, another multiplication symbol '×', and a second blue vertical bar labeled 'z₂'.

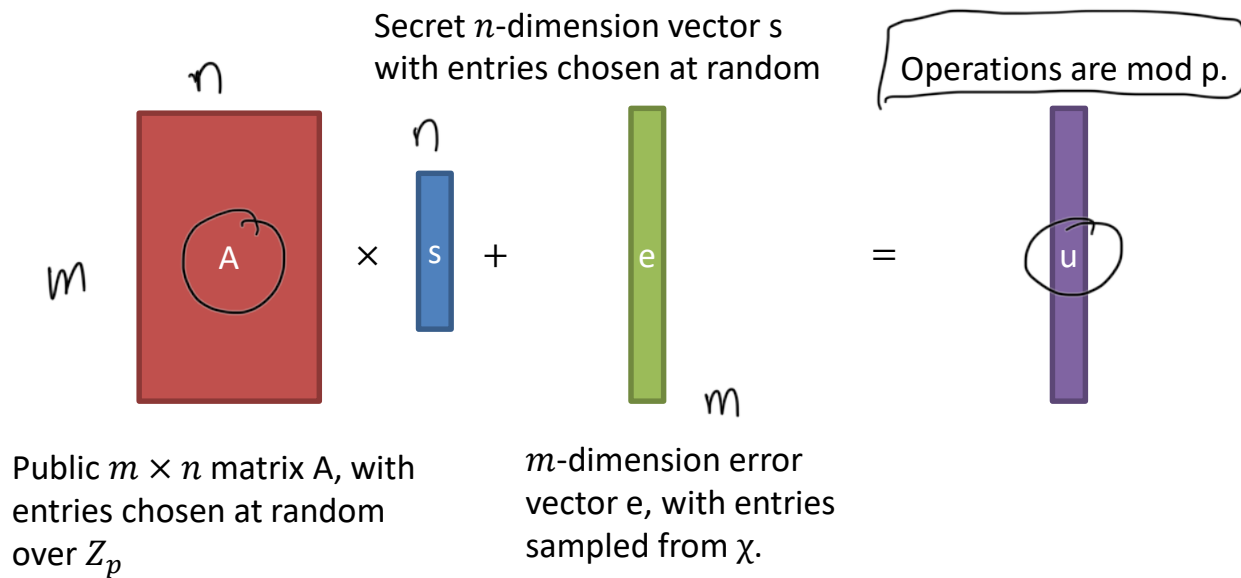
Obtain
 $(z_1 - z_2) \in$
 $\{-1,0,1\}^m$:



A diagram illustrating the equation $A \times (z_1 - z_2) = \vec{0}$. It features a red rectangular block labeled 'A' on the left, followed by a multiplication symbol '×', an opening parenthesis '(', two blue vertical bars labeled 'z₁' and 'z₂' with a minus sign '-' between them, a closing parenthesis ')', an equals sign '=', and a blue vector symbol '0' with a right-pointing arrow above it.

The LWE Problem (Search)

Learning with Errors

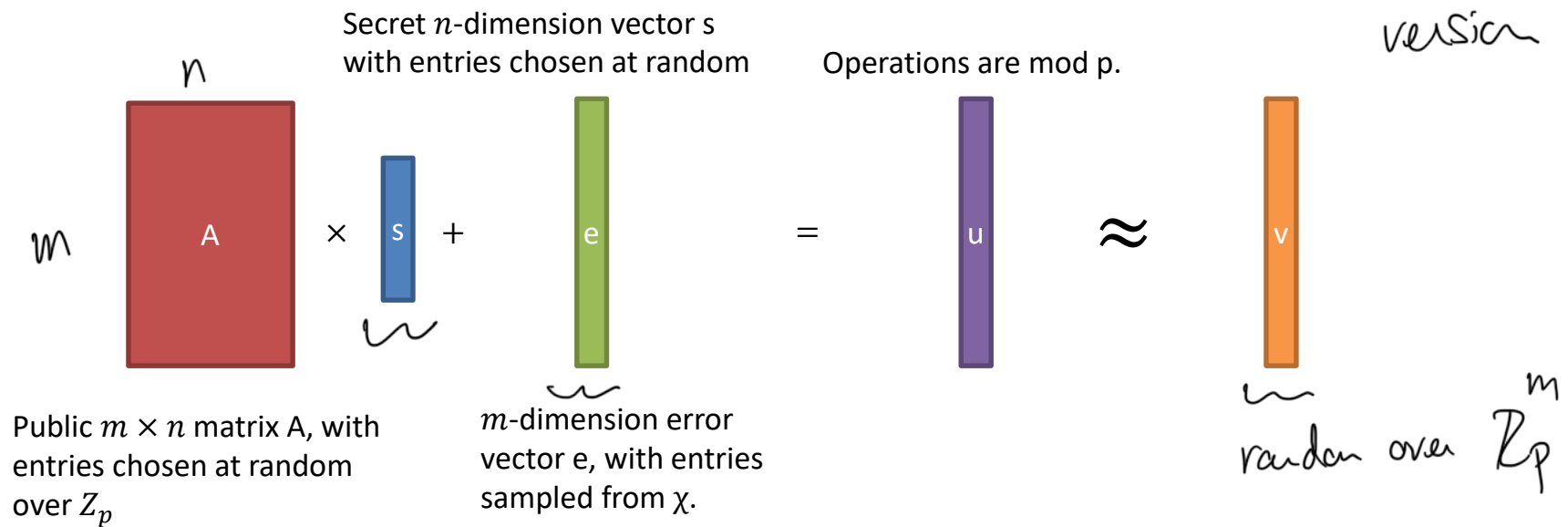


Problem: Given, A , $u = As + e$, find s .

noisy system of linear equations

The LWE Problem (Decision)

As hard as
search
version



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

Relation to Lattices

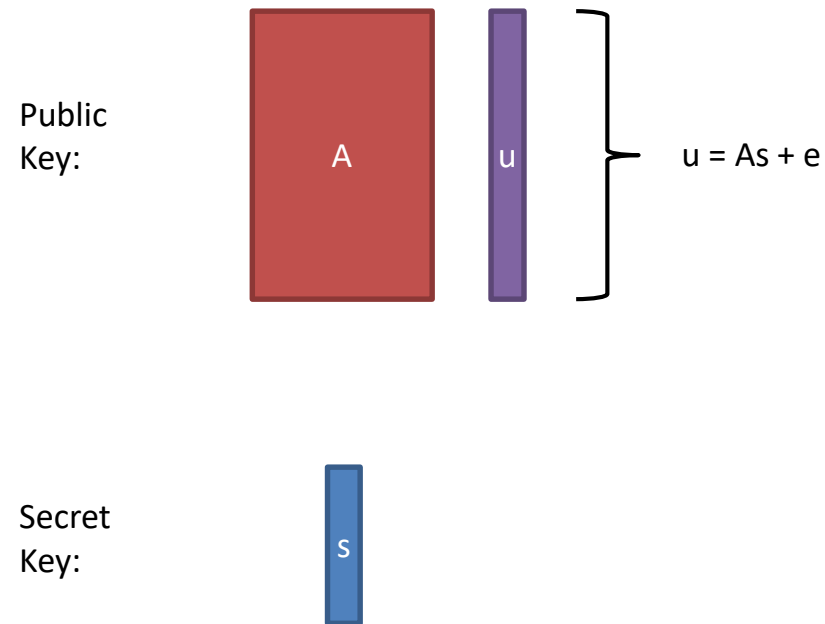
- Worst-Case to Average-Case Reduction:
Breaking the cryptosystem on average is as hard as breaking the hardest instance of the underlying lattice problem.
- LWE:
 - Worst-Case to Average-Case **Quantum** Reduction from SIVP.
 - Worst-Case to Average-Case **Classical** Reductions from GapSVP.

very hard

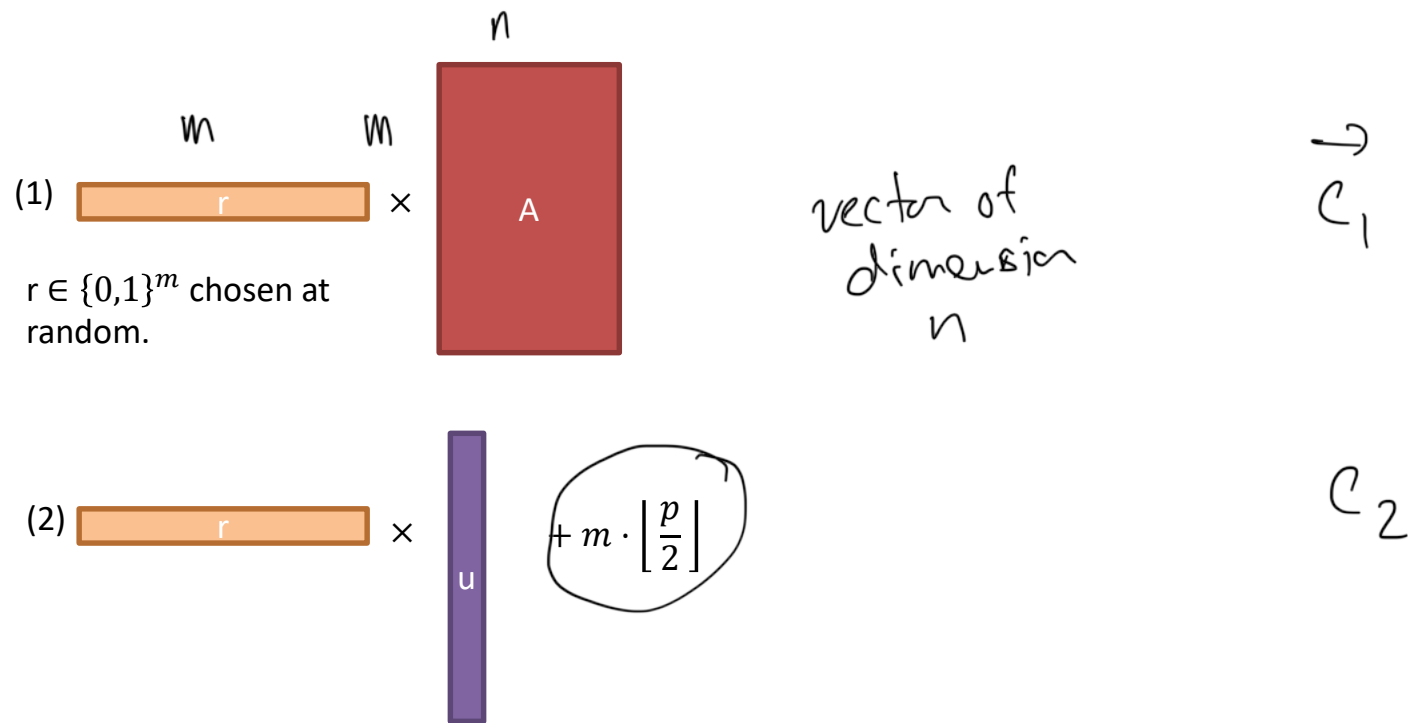
Lattice-Based Encryption

Regev's Cryptosystem [Regev '04]

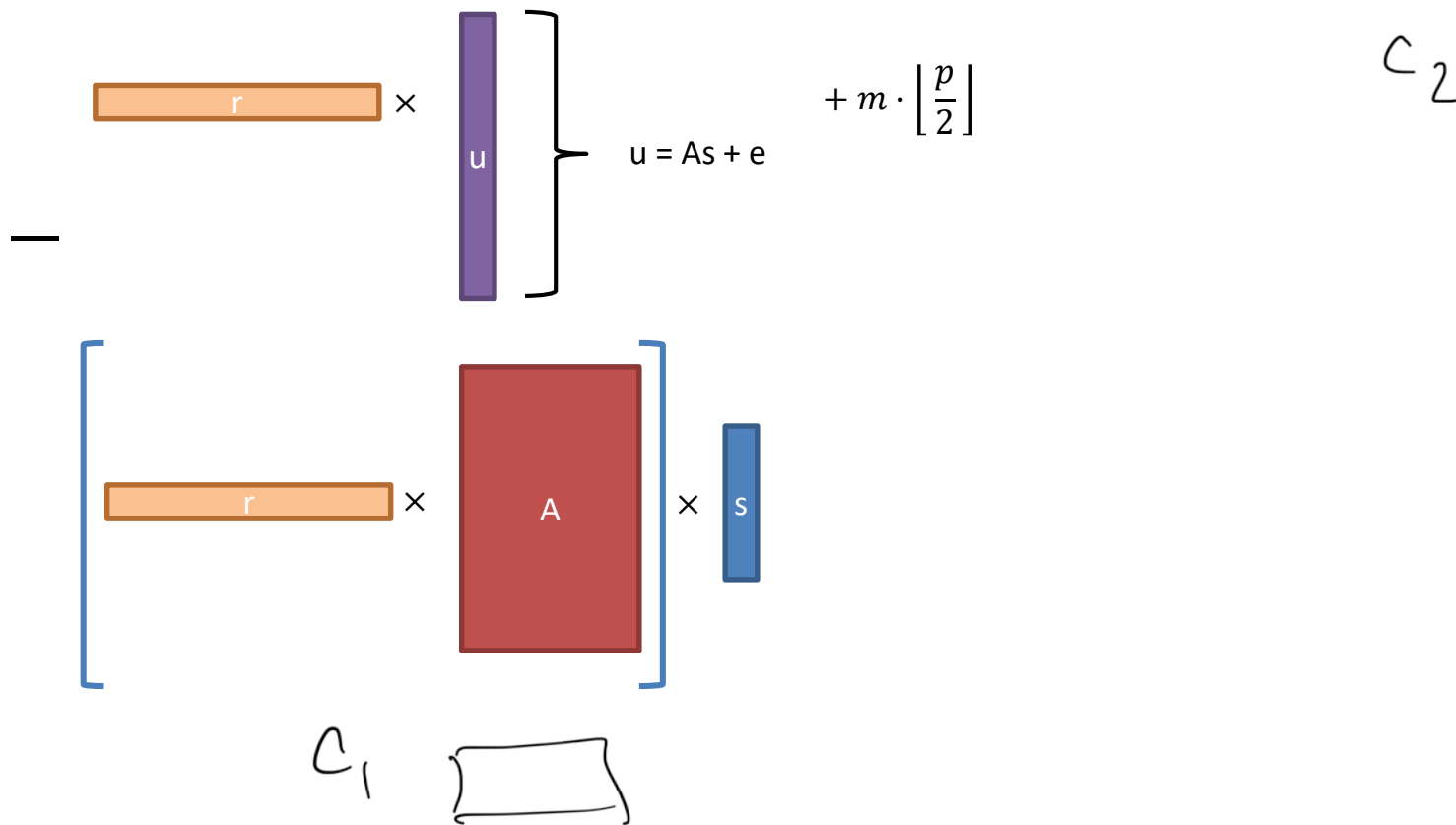
Public Key Encryption.



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



Regev's Cryptosystem—Decryption



Regev's Cryptosystem—Decryption

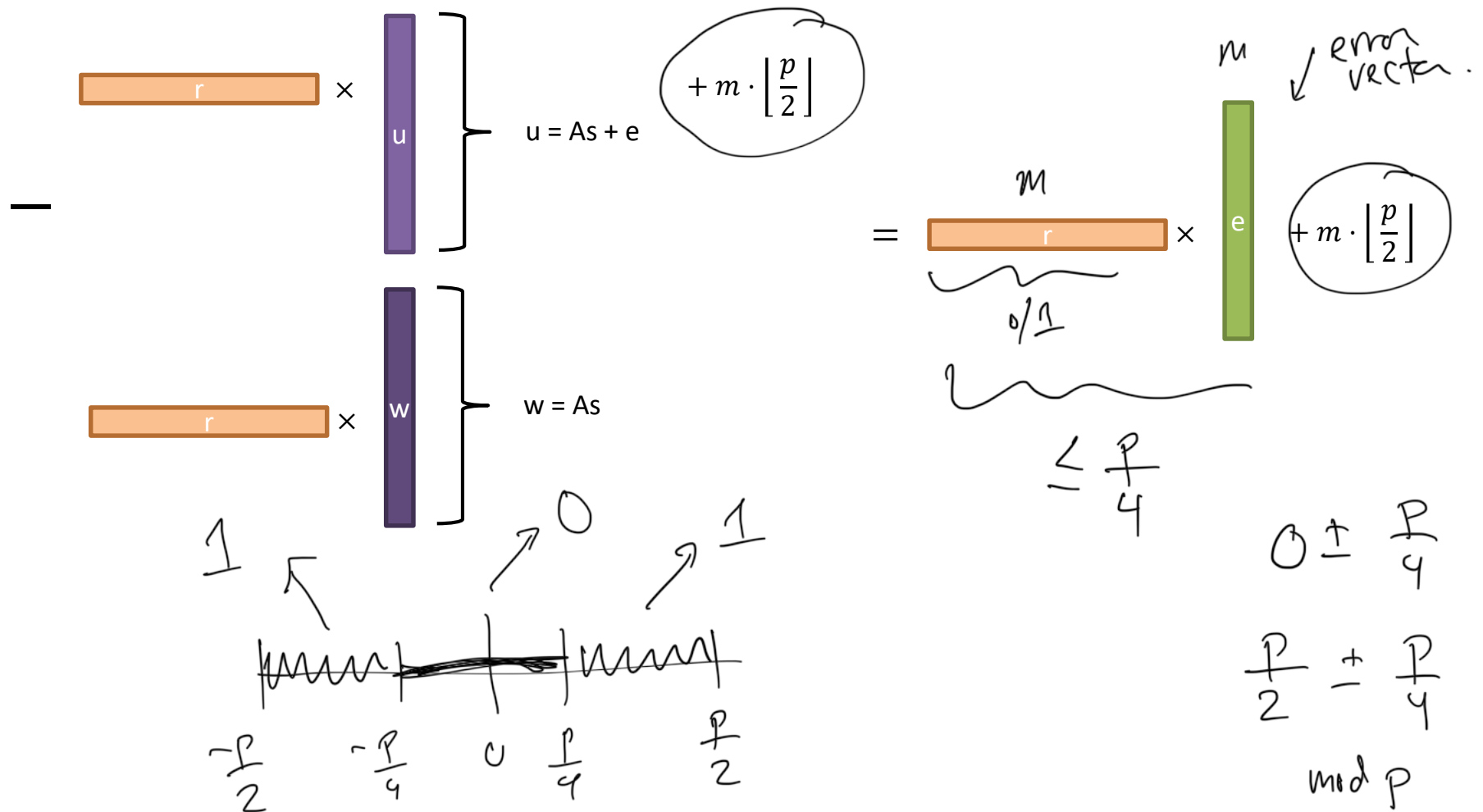
The diagram illustrates the decryption process in Regev's cryptosystem. It shows the ciphertext u (purple vertical bar) and the public key r (orange horizontal bar) being multiplied together. This product is then compared to the product of the public key r and the secret key s (blue vertical bar) multiplied by the matrix A (red square). The difference between these two products is the error term e , which is added to the message m scaled by $\frac{p}{2}$.

$$r \times u = r \times (As + e) + m \cdot \left\lfloor \frac{p}{2} \right\rfloor$$

The diagram uses the following visual representations:

- r : orange horizontal bar
- u : purple vertical bar
- A : red square
- s : blue vertical bar

Regev's Cryptosystem—Decryption



Regev's Cryptosystem—Decryption

$$\begin{array}{l}
 \text{—} \\
 \begin{array}{l}
 \boxed{r} \times \left. \begin{array}{c} \boxed{u} \\ \boxed{w} \end{array} \right\} \begin{array}{l} u = As + e \\ w = As \end{array} + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \\
 \\
 \boxed{r} \times \left. \begin{array}{c} \boxed{u} \\ \boxed{w} \end{array} \right\} \begin{array}{l} u = As + e \\ w = As \end{array} \\
 \\
 \approx 0 + m \cdot \left\lfloor \frac{p}{2} \right\rfloor
 \end{array}
 \end{array}$$

The diagram illustrates the decryption process in Regev's cryptosystem. It shows the subtraction of the product of a random vector r and a noise vector w from the ciphertext u . The ciphertext u is defined as $u = As + e$, where s is the secret message and e is the noise. The noise vector w is defined as $w = As$. The resulting difference is approximately zero, plus a term $m \cdot \lfloor \frac{p}{2} \rfloor$, which is the noise component of the ciphertext.

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.

algebraic number theory

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. *Kyber scheme*
- 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. $q = 1 \pmod{2n}$.
- 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 $p(x) \in Z_q[x]/x^n+1$
- 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

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