Cryptography

Lecture 25

Announcements

- HW9 due on Wed 5/8 **extended**
- Final Review Sheet up on course webpage
- Upcoming:
  - HW10 will be due on Wed 5/15 “optional”
  - Scholarly paper EC due on 5/13
  - Final Review Sheet solutions and Cheat Sheet will be posted on Canvas by the end of the week

Agenda

- Post-Quantum Crypto

Traditional Crypto Assumptions

- Factoring: Given $N = pq$, find p, q
  - RSA Given $N = pq$, e, $x^e \ mod \ N$, find x.
- Discrete Log: Given $g^x \ mod \ p$, 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

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.

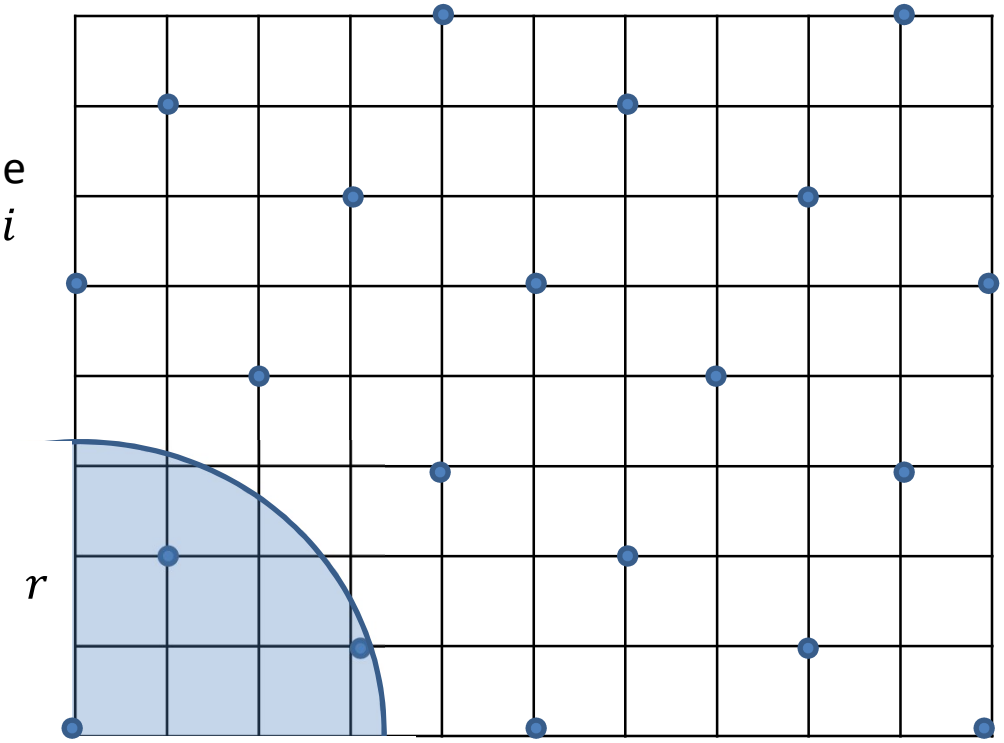
Lattices

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

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

"integer linear combinations of the basis vectors"

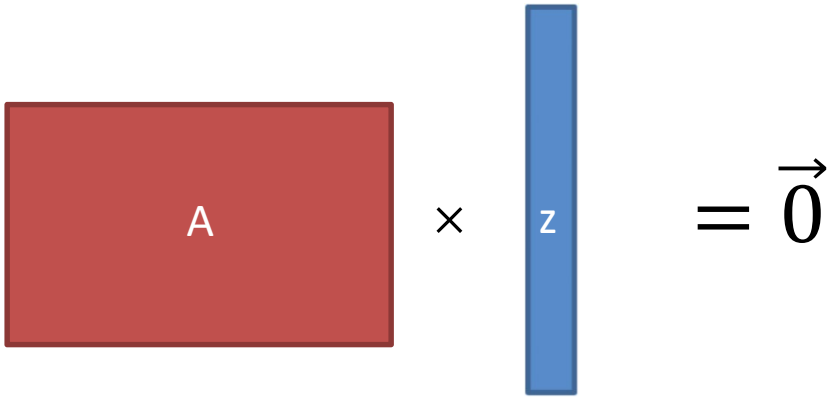
i-th successive minima $\lambda_i(L(B))$: The smallest radius r such that there are i linearly independent vectors $\{v_1, \ldots, v_i\}$ of length at most r.



Hard Lattice Problems

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

The SIS Problem



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

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

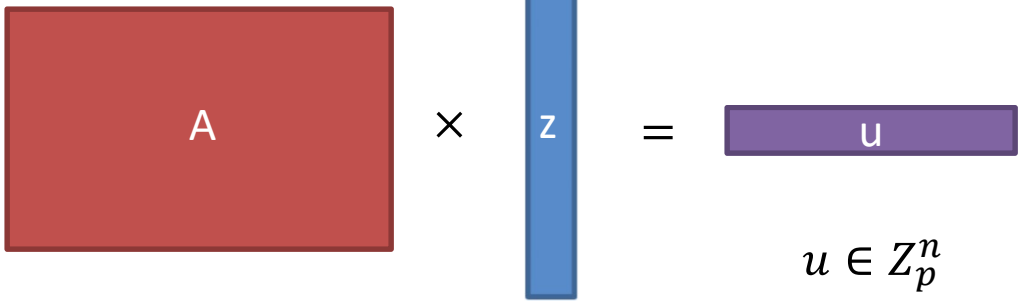
Public Matrix:

Input:

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

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

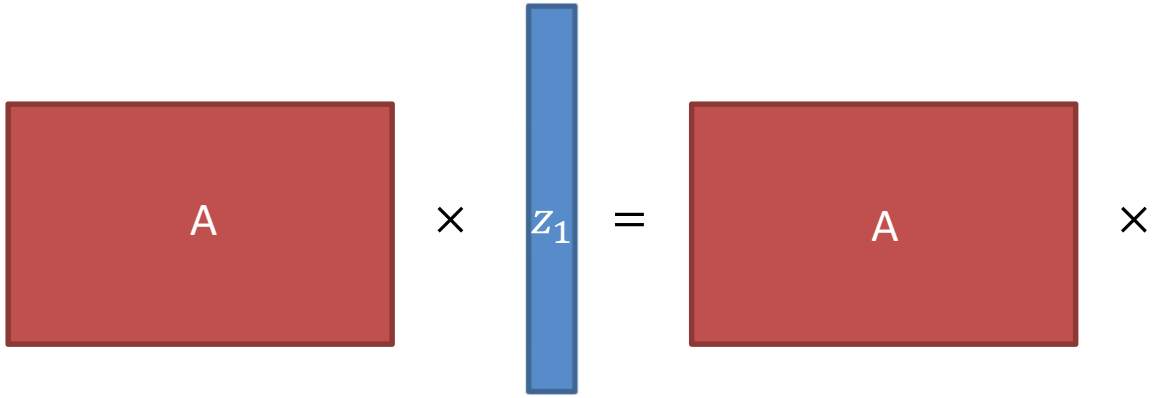
To evaluate the hash on z output:



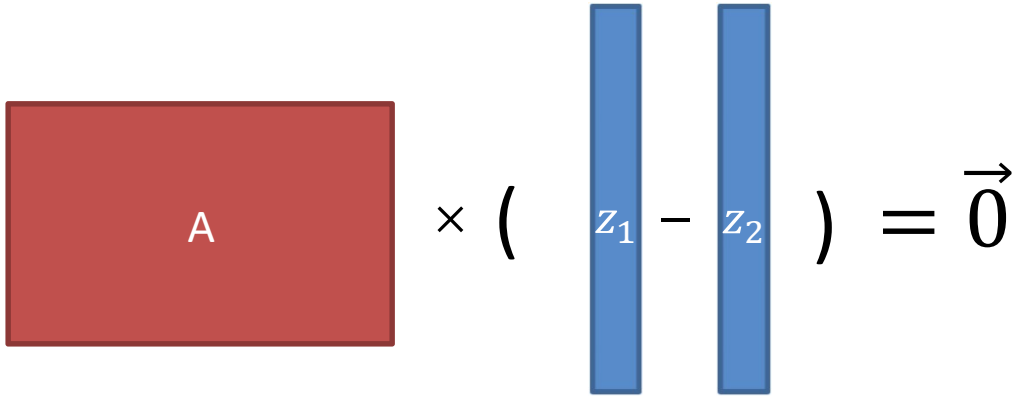
$u \in Z_p^n$

CRHF from Lattices

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



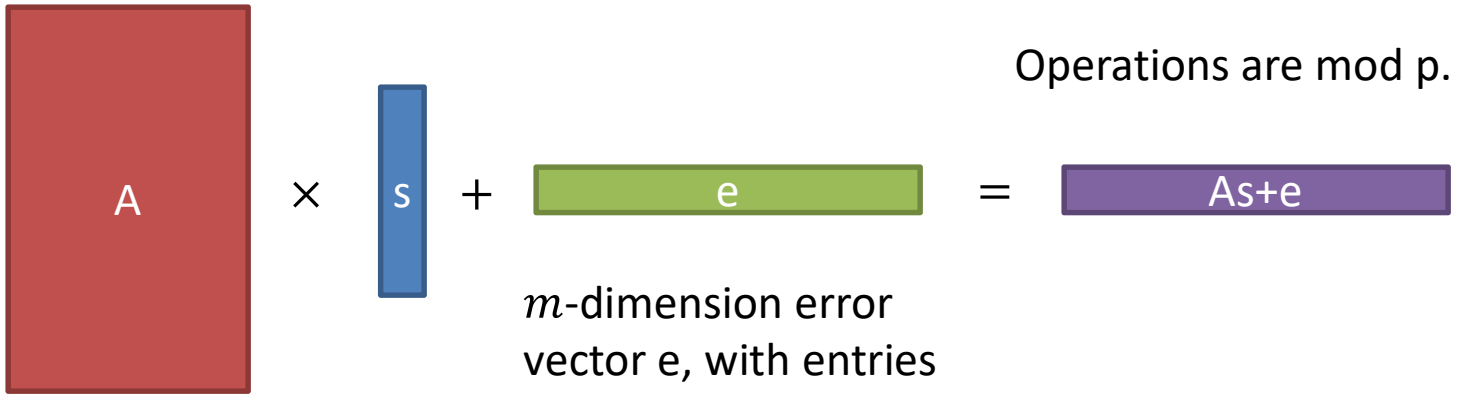
Obtain $(z_1 - z_2) \in \{-1,0,1\}^m$:



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.
Distribution χ depends on dimension of A and the modulus.

Problem: Given, A, As+e, find s.