An Introduction to Lattice-Based Cryptography II

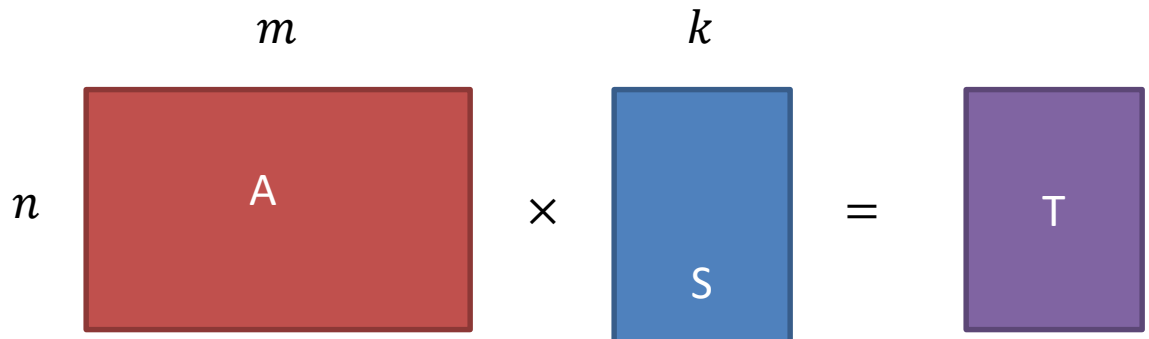
Dana Dachman-Soled
University of Maryland
danadach@umd.edu

Rejection Sampling

- Problem: Sample from a distribution D_f with probability density function $f(x)$ given draws from a distribution D_g with probability density function $g(x)$.
- Assuming $\forall\ x, f(x) \leq\ M \cdot\ g(x)$:
  - Sample from $x \leftarrow\ D_g$
  - Accept x with probability $\frac{f(x)}{M \cdot g(x)}$.
- If condition holds then $\forall\ x, \frac{f(x)}{M} \cdot\ g(x) \leq\ 1$
- Probability of outputting x is $\Pr[sampling\ x] \cdot \Pr[sample\ is\ accepted] =\ g(x) \cdot \frac{f(x)}{M \cdot\ g(x)} = \frac{f(x)}{M}$.
- Normalizing, we get the correct probability distribution
- Expected number of draws from $g(x)$ before a sample is accepted is M.

Lattice-Based Signatures Lyubashevsky 2011

Key Generation



entries chosen at random over Z_p

entries chosen at random from $\{-d, \ldots, d\}$

Public Key:

Secret Key:

Sign—Attempt 1

(1) $y \leftarrow D_\sigma^m$ A × y = d

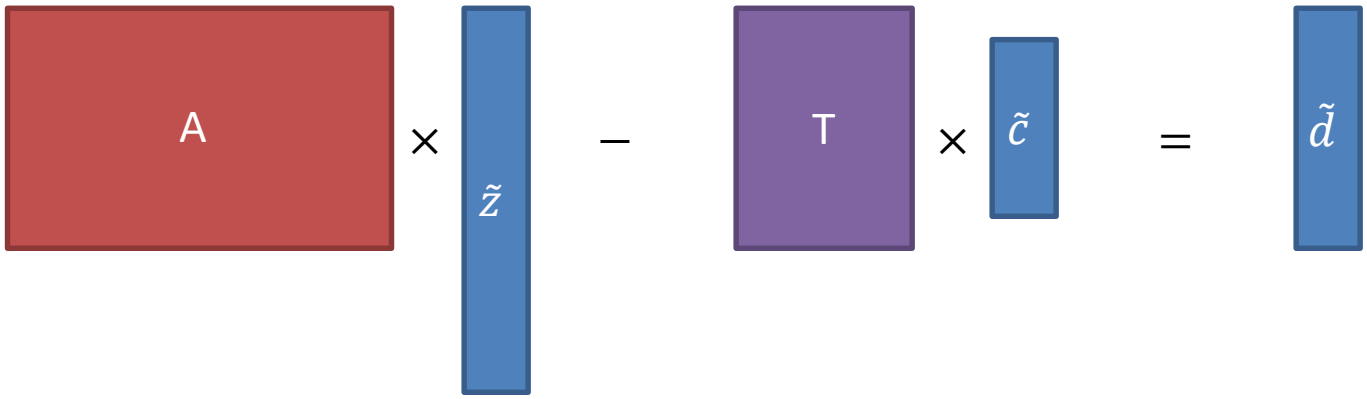
(2) $c = H(d||m)$ c

Output (c,z)

(3) S × c + y = z

Verify

Given public key (A, T), message m and signature $(\tilde{c}, \tilde{z})$:



Check that $\tilde{c} = H(\tilde{d}||m)$ and $\tilde{z}$ is short.

Security

- If adversary has not seen any signatures, can show (using RO methodology) that it is possible to extract the following from a forging adversary:
  - z_1 s.t. $Az_1 - Tc_1 = Ay$
  - z_2 s.t. $Az_2 - Tc_2 = Ay$
  - Subtracting and recalling that $T = AS$ we obtain:

$$A(z_1 - z_2) - T(c_1 - c_2) = 0$$

$$A(z_1 - z_2) - A\left(S\,(c_1 - c_2)\right) = 0$$

- Finding such z_1, z_2 was shown to be as hard as SIS.
- But what if adversary gets to see signatures? Is this still hard?

Sign

(1) $y \leftarrow D_\sigma^m$ A × y = d

(2) $c = H(d||m)$ c

(3) S × c + y = z

Output (c, z) with probability $\frac{D_\sigma^m(z)}{M \cdot D^m{}_{\sigma,Sc}(z)}$

Rejection sampling step