An Introduction to Lattice-Based Cryptography II

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

Announcements

- Homework 6 due on 5/8 at 11:59pm
- Same for scholarly paper extra credit
- Final review sheet up on Canvas/ELMS and course webpage
- Review session next class
- Practice exam and cheat sheet will be released by the end of the week

Post-quantum Cryptography

SIS

LWE

Digital Signatures

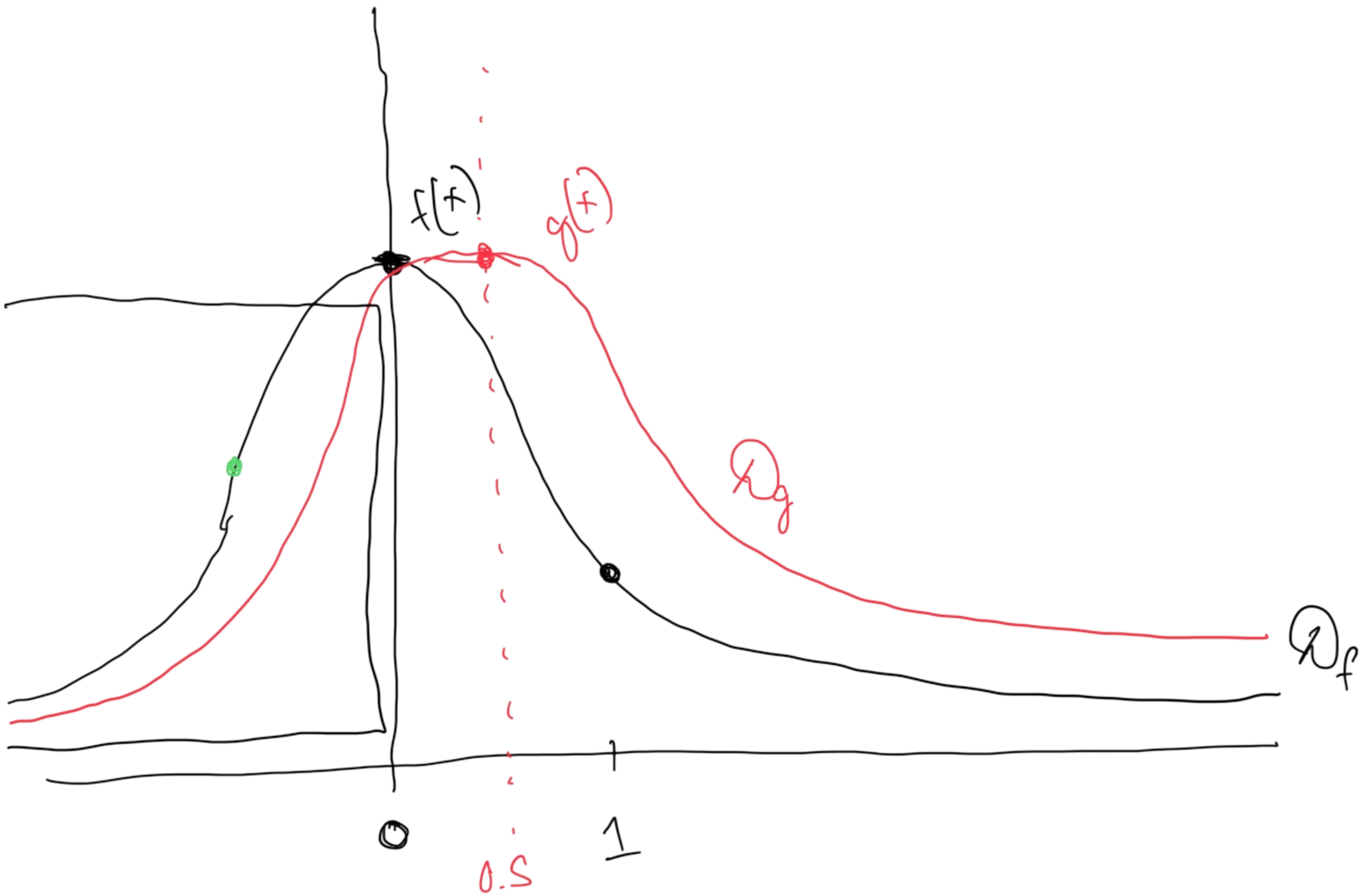
A

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

$$\underbrace{\overbrace{A}^{m}}_{\mathbb{Z}_p}{}_{\,n} \; z = \bar{0} \bmod p.$$

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 $\boxed{\frac{f(x)}{M \cdot g(x)}}$. between 0 and 1. $\frac{\cancel{g(x)} \cdot f(x)}{M \cdot \cancel{g(x)}}$
- If condition holds then $\forall\, x, \frac{f(x)}{M} \cdot g(x) \leq 1$
- Probability of outputting x is $\Pr[\mathit{sampling}\ x] \cdot \Pr[\mathit{sample\ is\ accepted}] = g(x) \cdot \frac{f(x)}{M \cdot g(x)} = \frac{f(x)}{M}$.
- Normalizing, we get the correct probability distribution
- Expected number of draws from $g(x)$ before a sample is accepted is $\boxed{M}$.

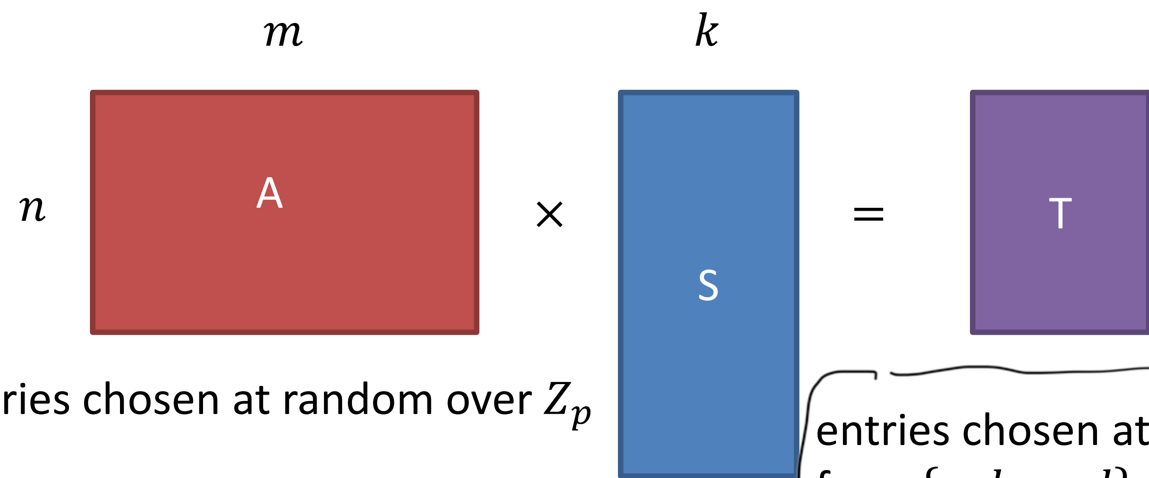


f(x)
g(x)
$\mathcal{D}_g$
$\mathcal{D}_f$
0
0.5
1

Lattice-Based Signatures
Lyubashevsky 2011

similar but simpler than the newly standardized post-quantum digital signature (Dilithium)

Key Generation (Schorr)



entries chosen at random over Z_p

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

Public Key:

$g^x = y$

Secret Key:

(x)

Sign—Attempt 1

Gaussian

$I = g^K$

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

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

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

r

Output (c,z)

$s = \boxed{rx + K}$

(3) $S \times c + y = z$

Verify

$g^{s} \cdot y^{-r}$

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

$$A \times \underbrace{\tilde{z}}_{Sc+y} - T \times \tilde{c} = \underbrace{\tilde{d}}_{Ay}$$

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

$$A(Sc+y) - Tc$$

$$\cancel{Tc} + Ay - \cancel{Tc}$$

correctness.

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:

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

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

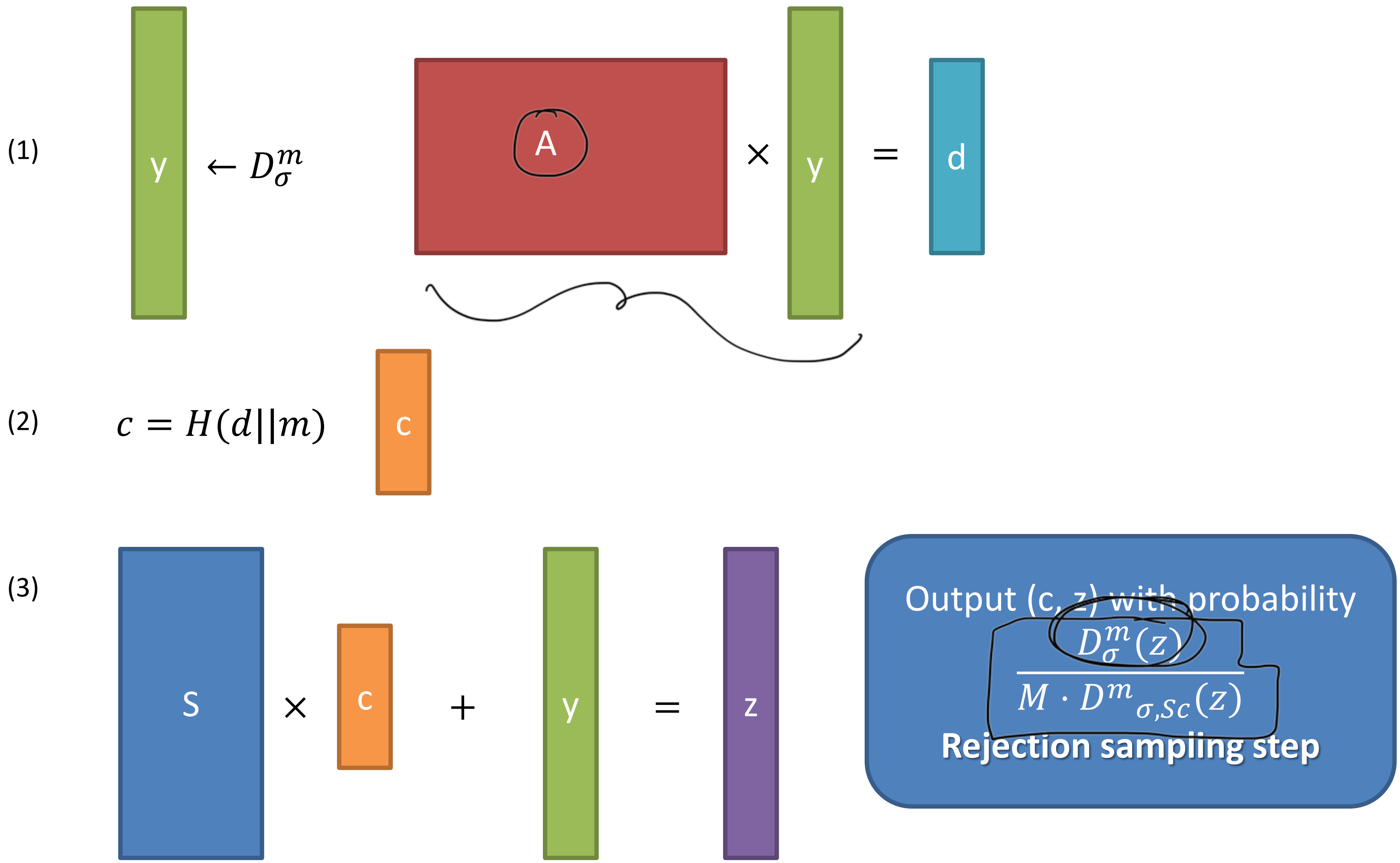
$Av = 0 \bmod p$

$v = \left(z_1 - z_2 - S(c_1 - c_2)\right)$

- 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?

identification protocol is not $\boxed{\text{zero knowledge}}$

Sign


(1)
y
$\leftarrow D_\sigma^m$
A
$\times$
y
$=$
d
(2)
$c = H(d||m)$
c
(3)
S
$\times$
c
$+$
y
$=$
z
Output (c, z) with probability
$$\frac{D_\sigma^m(z)}{M \cdot D^m{}_{\sigma,Sc}(z)}$$
Rejection sampling step