CS5500: Lecture 11

Recap

- Trapdoor Permutations: one-way function w/ additional properties...
  - some trapdoor which when known makes the function easy to convert
- RSA: based on DLP
- Goldwasser-Micali: Quad residue

GM Encryption

Gen: 2 large primes p, q $\quad N = p \cdot q$

↳ $PK = (N, y)$ and $SK = (p, q)$

Enc: (PK, b) — b is message bit

1. generate random $r \in \mathbb{Z}_N^*$
2. Give... (quad. res.)

$c = r^2 \pmod N$ if $b = 0$ and $r^2 y \pmod N$ if $b = 1$ (non-quad. residue)

Dec(SK, c): Check if $c \in \mathbb{Z}_N^*$ is a quad. residue using p and q.

↳ if c is quad res. mod N → quad res. mod p and q

* IND-security follows from the quadratic residuosity assumption
  - given N, no PPT can distinguish b/w Jac_+ that is QR_N vs NQR_N

GM is homomorphic encryption

- given a GM-ciphertext of b and of b', I can compute GM-ciphertext $(b + b') \pmod 2$
  - computation done on ciphertexts gives same output as if it was done on plaintexts

Want $(b + b')$ from ciphertexts (say c, c') → do $c * c'$

* $Enc(pk, b) \cdot Enc(pk, b')$ is an encryption of $b \oplus b = b + b' \pmod 2$.

Post-Quantum Security + Lattice-based Crypto

Why lattices?

↳ best algorithms run in 2^n time vs factoring + DLP can be solved $\sim 2^{\sqrt[3]{n}}$ subexp

↳ so far it's quantum resistant

↳ worst-case hardness is strongly connected to avg-hardness

↳ simple + efficient

↳ enabler of other capabilities
↳ Fully Homomorphic Encryption

1994: Shor gives quantum construction for factoring + DLP
↳ capacity still not available yet, but coming

Post Quantum Cryptography: schemes that **should** be quantum resistant

How it works

- matrix A, secret s

Try 1: Find s given $(A)s$

Try 2: Find s given $(A)s \bmod q$

] Gaussian Elim. makes this easy

Try 3: Find s given $(A)s + e$ ← noise

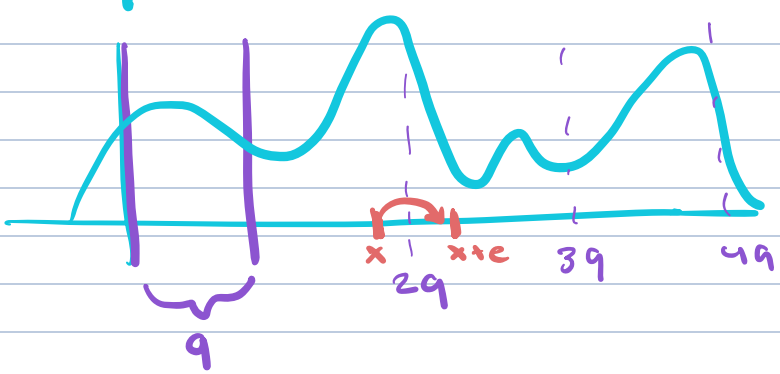
$(A)s$ ← Linear reg

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} s + e = \langle a_i, s \rangle + e_i$$

← Solvable

Try 4: Find s given $[(A)s + e] \pmod q$

↳ very hard to find s



- error can just bump you over to a new dist area in non-mod
- mod condenses and dist into just $0 \to q-1$

Solving Noisy, mod lin eqns

Given: A $(m \times n)$ and $[A \cdot \vec{s} + \vec{e}] \bmod q$ ($\vec{s}$: $n \times 1$, $\vec{e}$: $m \times 1$)

Parameters: dimensions m, n, mod q, error dist χ → uniform in interval $[-B, \ldots, B]$

↳ A: chosen at rand from $\mathbb{Z}_q^{m \times n}$, s from $\mathbb{Z}_q^n$, e from χ^m

Learning With Errors (LWE)

↳ decoding random linear codes (error correcting code w/ error)

↳ learning noisy linear functions

↳ worst-case hard lattice problems

Attack 1: Linearization

- given $A, [As+e]$, find s

try 1: each lin eqn is exact poly. eqn

ex. $b = \langle a, s \rangle + e = \sum_{i=1}^{n} a_i s_i + e$ → error bound $B=1$, $e \in [-1, 0, 1]$

↳ have eqn $(b - \sum a_i s_i - 1)(b - \sum a_i s_i)(b - \sum a_i s_i + 1) = 0$

* one of these is 0 so all will be 0

↳ even just solving deg. 2 polynomial equation is NP-hard

try 2: easy to solve given sufficiently many eqns

↳ using "linearization"

$$\sum a_i a_j a_k \, s_i s_j s_k + \sum a_{ij} s_i s_j + \sum a_i s_i + (b-1)b(b+1) = 0$$

replace w/ indep. var t_{ijk}

- created noiseless linear equation in t_{ijk}

* fewer eqn: more candidates → more eqns: less candidates

↳ when # eqns = # vars $\approx O(n^3)$

Generalized Linearization: (Attack 1)

- breakable when $m >> n^{2B+1}$
- set $B = n^{\Omega(1)}$ → ensure linearization doesn't get enough eqns to break it

What is the lattice?

- discrete, additive sub group of $\mathbb{R}^m$
- A is pts on lattice
- e does not have to be on lattice

Lattice Reduction (Attack 2)

LLL Alg.

- say $q/B = 2^{n^{\varepsilon}}$ for constant $\varepsilon > 0$

- LLL solves LWE in time $2^{\tilde{O}(n^{1-\varepsilon})} \cdot \text{poly}(n, \log q)$
  - ↳ poly in n and $\log q$ when $\frac{q}{B} = 2^{o(n)}$ ← more reasoning for why noise bounds can't be too small

Safe Parameters

- n = sec. parameter
- m : arbitrary poly in n (A is $n \times m$)
- B : small poly in n say $\sqrt{n}$
- q : poly in n, larger than B, could be as large as $2^{n^{0.99}}$ (say ↓ sub-exp)

↳ from quantum side: no known alg to break well-constructed LWE

Decisional LWE

- can you dist b/w $A, (As+e)$ and A, b
  - ($A, (As+e)$: correlated; A, b: completely independent)
  - ($A, (As+e)$ and A, b: can't see the dependence on A vs independence)
  - for arbitrary s
  - ↳ same hardness as LWE

Info-computation gap

- if m (columns in A) is much smaller than n, it is information-theoretically hard to find s
- $\frac{n}{\left(1 - \frac{\log 2B+1}{\log q}\right)} \leq m \leq \frac{n}{2^{\log\left(\frac{q}{2B+1}\right)}}$: s is uniquely determined given $(A, As+e)$ but it is computationally hard to recover

OWF + PRGs

$g_A(s, e) = As + e$

- ↳ one-way (by LWE)
- ↳ PRG (decisional LWE)
- ↳ can be trapdoor

Using LWE in ~~one~~ Secret-Key Encryption

Gen: sk = vector $s \in \mathbb{Z}_q^n$

Enc$_s(\mu)$ // $\mu \in \{0,1\}$ ← message

1. sample $a \in \mathbb{Z}_q^n$, small noise $e \in \mathbb{Z}$ ← decoder won't know e
2. $c = (a, b = \langle a, s \rangle + e + \mu \lfloor q/2 \rfloor)$

↳ decoder recovers this = noisy message

★ need significant large $\frac{\text{Signal}}{\text{noise}}$ ratio

$Dec_{SK}(c)$: output $round_{q/2}(b - \langle a, s \rangle \bmod q)$

↳ correctness as long as $|e| < q/4$