CS598 DK
Cryptography (Advanced)

ANNOUNCEMENTS.

* Piazza
* Office Hours
* Syllabus
* Grading
* Participation

PUBLIC KEY ENCRYPTION.

Alice $\qquad\qquad\qquad\qquad\qquad\qquad$ Bob

pk_{Bob}

$m \qquad ct = Enc_{pk_{Bob}}(m) \longrightarrow$

Eve : pk_{Bob} , ct

* List all possible secret keys
* Check if any keys in the list are the "right" sk for Bob.
* If "right" sk was found, use it to decrypt & recover m.

$P \neq NP$.

∃ problems that are worst-case hard

Question: Suppose $P \neq NP$.

Then, can we base all cryptography on this assumption?

Assume something more than $P \neq NP$.

$\boxed{\text{ONE-WAY FUNCTION}}$ avg-case hardness for cryptography

f : easy to compute but hard to invert

$x \longrightarrow y = f(x)$ is "easy"

$y \longrightarrow x = f^{-1}(y)$ is "hard".

$\boxed{\text{TURING MACHINES}}$

Def. $\boxed{\text{Probabilistic}}$ Polynomial-Time Turing Machine

$\downarrow$

T.M. has a randomness tape

A T.M. $\mathcal{A}$ is (polynomial time) if $\exists c \in \mathbb{N}$ s.t. $\forall x$, $\underline{\mathcal{A}(x)}$ halts in $|x|^c$ steps.

Def. <u>non-uniform PPT Turing Machine</u>

Collection of PPT T.M.s, $(\underline{\mathcal{A}_1}, \underline{\mathcal{A}_2} \ldots)$ s.t. $\exists c \in \mathbb{N}$ s.t. $\forall x$,

$\mathcal{A}_{|x|}(x)$ halts in $|x|^c$ steps.

Negligible Function

__Def.__ A function $\nu(\cdot)$ is negligible if $\forall\, c \geq 0$, $c \in \mathbb{N}$, $\exists\, k_0\, (\in \mathbb{N})$ s.t. $\forall\, k\, (\in \mathbb{N}) \geq k_0$,

$$|\nu(k)| < \frac{1}{k^c}$$

Denoted by $\text{negl}(k)$.

__A function__ is negligible if it approaches 0 faster than the inverse of any polynomial.

__Examples.__ $\nu(k) = \frac{1}{2^k}$ is a negligible function.

$\nu(k) = \frac{1}{2^{(\log^2 k)}}$ is also a negl. function

NOT negl : $\frac{1}{k^{10}}$ is not a negl. function

Properties : If $\nu_1(k) = negl(k)$
and $\nu_2(k) = negl(k)$
then $\nu_1(k) + \nu_2(k) = negl(k)$
$\nu_1(k) \cdot \nu_2(k) = negl(k)$

$poly(k) \cdot negl(k) = negl(k)$

$\boxed{\text{ONE-WAY FUNCTION.}}$

Definition. $f : \{0,1\}^* \to \{0,1\}^*$ is one-way if :

* $\boxed{\text{EASY to compute}}$

$\exists$ PT M that computes $f(x)$ for all $x \in \{0,1\}^*$

* $\boxed{\text{DIFFICULT to invert}}$

$\forall$ PPT $\mathcal{A}$, $\exists$ ngl $\nu(\cdot)$ s.t. $\forall$ $k \in \mathbb{N}$,

$$\Pr_{x \leftarrow \{0,1\}^*}\left[\mathcal{A}(f(x)) \in f^{-1}(f(x)) \right] \leq \nu(k)$$

<u>Candidate</u> from factoring:

f is Defined As:

On input x, use x to sample $\underline{p, q}$.

$\downarrow$

N.

$f(x) = N$.

Candidate based on <u>LATTICES</u>:

$\boxed{\text{Lattice}}$ (n-dimensional lattice)

is a subset of $\mathbb{R}^n$ that is :

(a) <u>An additive subgroup.</u>

$0 \in L$, $\forall\, x, y \in L$

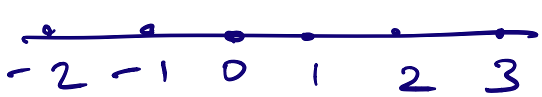
$-x,\ x+y$ are also $\in L$.

(b) <u>Discrete.</u>

$\forall\, x \in L$, there is a "neighborhood" of $x \in \mathbb{R}^n$ in which x is the only point in L.

<u>Eg.</u> $\{0\}$ is a lattice.

$\{\ldots\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\ldots\}$



1 - dim lattice

Consider a set of linearly independent basis vectors $\vec{b_1}, \ldots, \vec{b_n}$.

Lattice: All possible integer comb. of basis vectors.

$$\mathcal{L}(\vec{b_1} \ldots \vec{b_n}) = \left\{ \sum_{i \in [n]} c_i \vec{b_i} \;\middle|\; c_i \in \mathbb{Z} \right\}$$

Min. dist of a lattice:

Length of the shortest nonzero vector.

$$\lambda_1(\mathcal{L}) = \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|.$$

$\boxed{\text{HARD PROBLEMS}}$ (Oded Regev)

SVP Given an arbitrary basis $b_1 \ldots b_k$ of some lattice $\mathcal{L} = \mathcal{L}(b_1 \ldots b_k)$ find $x \in \mathcal{L}$ s.t. $\|x\| = \lambda_1(\mathcal{L})$

γ-Approx. SVP modify the above problem s.t. $\|x\| \leq \gamma(k) \cdot \lambda_1(\mathcal{L})$

γ-GAP SVP Given basis $B = b_1, \dots, b_k$ s.t. $\mathcal{L} = \mathcal{L}(B)$ has either $\lambda_1(\mathcal{L}) < 1$ or $\lambda_1(L) > \gamma(k)$, determine which is the case.

$\boxed{\text{OTHER HARD PROBLEMS.}}$

(implied by the hardness of γ-GAP SVP)

* SIS (Short Integer Solution)

  HSIS, ISIS

* LWE (Learning With Errors)

  LWE $\Rightarrow$ SIS

Hardness of solving systems of linear equations (modulo a prime)

$$14s_1 + 15s_2 + 5s_3 + 2s_4 = 8 \pmod{17}$$
$$13s_1 + 14s_2 + 14s_3 + 6s_4 = 16 \quad (\text{"})$$
$$6s_1 + 10s_2 + 13s_3 + 15s_4 = 3 \quad (\text{"})$$
$$8s_1 + 7s_2 + 16s_3 + 25s_4 \cdots s_{10} = 2 \quad (\text{"})$$

$n = 4$.

Gaussian elimination makes this easy even for large n.

Q: What if we had n equations in $m \gg n$ variables?
Finding a solution is still EASY.

Q: n EQNs in $m \gg n$ variables $s_1 \ldots s_m$
Find a solution where $s_1 \ldots s_m$ are all in $\{0, 1, 2\}$ $\longrightarrow$ THIS is hard!

In other words, set

$$A \in \mathbb{Z}_q^{n \times m}, \qquad b \in \mathbb{Z}_q^n$$

$\mathbb{Z}_q \longrightarrow$ set of all int. mod q.

Given $A_{n \times m}\, b_{n \times 1}$, finding "short" $\vec{s}_{m \times 1}$ s.t. $A\vec{s} = \vec{b}$ is hard

SIS Hardness Assumption (Formally)

Sample a prime q
Sample $A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, $\vec{b} \xleftarrow{\$} \mathbb{Z}_q^n$
and set B s.t. $(2B+1)^m \gg q^n$, and $m \gg n$

Then $\forall$ nu PPT T.M. M

$$\Pr_{\substack{A \xleftarrow{\$} \mathbb{Z}_q^{n \times m},\\ b \xleftarrow{\$} \mathbb{Z}_q^n}}\left[M(A, \vec{b}) \text{ outputs } \vec{s}_{m \times 1} \text{ s.t. } ①\ A\vec{s} = \vec{b} \text{ and } ②\ s \in [-B, \ldots B]^m \right] = \text{negl}(n)$$