Advanced Cryptography

NP (Non-deterministic Polynomial time)
= set of languages such that membership can be proved in polynomial time.

Interactive Proofs

We allow interaction between the prover and the verifier.

Randomization

There is a very small probability that the verifier may accept false proofs.

What about Non-interactive proofs where the verifier V is randomized. Suppose we have 2 $n \times n$ matrices A and B, over a finite field. And we want to verify $C = AB$. We can do this by using the best known matrix multiplication algorithm of $O(n^{2.36})$. But, we can do the verification more efficiently using randomization.

Assume the finite field $|\mathbb{F}| > n$.

We choose $r \in \mathbb{F}$.

Let $X = [1, r, \ldots, r^{n-1}]$.

We will check if $\underbrace{CX}_{O(n^2)}{}^{T} = (AB)X^{T}$.

$$\begin{bmatrix} c_{10} & \cdots & c_{1(n-1)} \end{bmatrix} \begin{bmatrix} 1 \\ r \\ \vdots \\ r^{n-1} \end{bmatrix} = \begin{bmatrix} \sum_{i=0}^{n-1} c_{1i}\, r^{i} \end{bmatrix}$$

$$\begin{bmatrix} AB_{10} & \cdots & AB_{1(n-1)} \end{bmatrix} \begin{bmatrix} 1 \\ r \\ \vdots \\ r^{n-1} \end{bmatrix} = \begin{bmatrix} \sum_{i=0}^{n-1} AB_{1i}\, r^{i} \end{bmatrix}$$

Suppose $\{AB_{1i}\} \neq \{C_{1i}\}$ but $\sum_{i=0}^{n-1} AB_{1i}\, r^i = \sum_{i=0}^{n-1} C_{1i}\, r^i$.

Then V will be accepting a false proof. But the probability of happening this is $\frac{n-1}{|\mathbb{F}|}$. So we need to have a big $|\mathbb{F}| \gg (n-1)$.

$$MA \equiv \underset{\text{prover}}{\text{Merlin}(M)} \rightleftarrows \underset{\text{verifier}}{\text{Arthur}(A)}$$

An Interactive Proof (IP) is a protocol between an all powerful prover P and a polynomial time verifier V such that for some language L, there should be

① Completeness - $\forall x \in L$, if

$t = (P, V(r))(x)$ — secret randomness of V.

Interaction transcript

then the probability that

V accepts the proof is large.

$$\boxed{Pr\left[V(t, r, x) = 1\right] \geq c}$$

c is called the completeness.

(2) Soundness – $\forall x \notin L$ and false prover P^*, $\boxed{Pr\left[V(t, r, x) = 1\right] \leq s.}$

We will repeat the interaction n times ($n >> 1$).

Sum check Protocol

Given a polynomial $f: \mathbb{F}^m \to \mathbb{F}$ of degree d in each variable. Fix any $H \subseteq \mathbb{F}$. You need to prove that $\sum_{h_1, \ldots, h_m \in H} f(h_1, \ldots, h_m) = \beta$.

P $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ V

(1) $\quad g_1(x) = \sum_{h_2, \ldots, h_m} f(x, h_2, \ldots, h_m)$

$$\xrightarrow{\qquad\qquad\qquad\qquad\qquad\qquad}$$

V checks that $g_1(x)$ is a univariate polynomial of degree $\leq d$.

Also $\sum_{h_1 \in H} g_1(h_1) = \beta$.

If these two steps pass, then, V chases $t_1 \in \mathbb{F}$ $(t_1 \leftarrow \mathbb{F})$ and sends it back to P.

$$\xleftarrow{\quad t_1 \leftarrow \mathbb{F}. \quad}$$

The goal of V is to catch the false prover P^* cheat. P^* will give a wrong $g_1(x)$. Suppose that wrong $g_1(x)$ passes the above checks. Now, the problem is reduced to

$$\sum_{h_2, \ldots, h_m \in H} f(t_1, h_2, \ldots, h_m) = g_1(t_1).$$

This holds true only for at most d elements. So the probability that this check passes for $P^* = \dfrac{d}{|\mathbb{F}|}$.

(2) $$g_2(x) = \sum f(t_1, x, \ldots, h_m)$$

$h_3, \dots, h_m \in H$

$$\longrightarrow$$

V will check that degree $\{g_2(x)\} \leq d$.

And $\sum_{h_2 \in H} g_2(t_1, h_2, \dots, h_m) = g_1(t_1)$.

If these checks pass, then, V $t_2 \leftarrow \mathbb{F}$.

$$\longleftarrow$$

$$\sum_{h_3, \dots, h_m \in H} f(t_1, t_2, h_3, \dots, h_m)$$

(m) During the mth interaction, the problem is reduced to $\sum_{h_m \in H} f(t_1, t_2, \dots, t_{m-1}, h_m)$

$= g_{m-1}(t_{m-1})$

$$g_m(x) = f(t_1, t_2, \dots, t_{m-1}, x)$$

$$\longrightarrow$$

V will check that $\deg\{g_m(x)\} \leq d$.

And then it $t_m \leftarrow \mathbb{F}$ and checks that

$g_m(t_m) = f(t_1, \dots, t_m)$

Here, V will have polynomial time of $O\left(m, d, |H|, \ln(|\mathbb{F}|)\right)$. And we will assume that basic arithmetic operations are of $O(1)$.

The number of interactions (m) is called the round complexity.

Communication complexity $= O\left(d\,m \cdot \ln(|\mathbb{F}|)\right)$

V runtime $= O\left(m\,(d \cdot |H|) \cdot \ln(|\mathbb{F}|)\right)$.

P runtime $= O\left(m \cdot \left(|H|^m \cdot T_f\right) \cdot \ln(|\mathbb{F}|)\right)$

T_f is the time required to compute f.

Completeness $\boxed{c = 1}$

What about the soundness. Suppose the claim is false.

$$\sum_{h_1, \ldots, h_m \in H} f(h_1, \ldots, h_m) \neq \beta.$$

In the first round, $g_1(x) \neq \sum_{h_2, \ldots, h_m \in H} f(x, h_2, \ldots)$.

To cheat there must exist a round i

such that

$$g_i \neq \sum f(t_1, t_2, \ldots, x, h_{i+1}, \ldots, h_m)$$

but $g_{i+1} = \sum f(t_1, \ldots, t_i, x, h_{i+2}, \ldots)$

Let that event be B_i. The probability that B_i happens

$$\Pr_{t_i \leftarrow \mathbb{F}}[B_i] \le \frac{d}{|\mathbb{F}|}$$

$$\boxed{\sum_{h \in H} g_{i+1}(h) = g_i(t_i)}$$

The probability that the wrong $g_i^*(t_i)$ and right $g_i(t_i)$ have the same value is $\frac{d}{|\mathbb{F}|}$

Considering m rounds, $\boxed{\text{soundness} = \frac{md}{|\mathbb{F}|}}$

and we want

$$\boxed{md \ll |\mathbb{F}|}$$