CS6846 – Quantum Algorithms and Cryptography

Finishing RSA. Fourier Transform

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output
2. Internal workings unknown and inscrutable

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output
2. Internal workings unknown and inscrutable
3. Box is consistent: same input, same output

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output
2. Internal workings unknown and inscrutable
3. Box is consistent: same input, same output
4. Anyone can interact (honest or adversary) by *querying* oracle

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output
2. Internal workings unknown and inscrutable
3. Box is consistent: same input, same output
4. Anyone can interact (honest or adversary) by *querying* oracle
5. *Random* oracle mimics random function

Random Oracle Model

1. Oracle is a box that takes some binary string as input and returns binary string as output
2. Internal workings unknown and inscrutable
3. Box is consistent: same input, same output
4. Anyone can interact (honest or adversary) by *querying* oracle
5. *Random* oracle mimics random function
6. Hard to invert by definition

RSA Encryption in ROM (Π):

$H : \{0,1\}^{2n} \to \{0,1\}^{\ell}$ (random oracle)

KeyGen: $\mathrm{GenRSA}(1^n) \to N, e, d$.

PK: (N, e) SK: (N, d).

Enc(m): Let $m \in \{0,1\}^{\ell}$.

Sample $r \leftarrow \mathbb{Z}_N^*$

Compute $r^e \bmod N$

$H(r) \oplus m$.

Dec(d, CT): Invert RSA & get r.

Compute $H(r)$ & get m.

Security

Theorem: If RSA is hard relative to GenRSA and H is modeled as a random oracle then the scheme Π is IND-CPA secure.

Proof: Let $\mathcal{A}$ be our adversary.

Consider the game $PubK_{\mathcal{A},\Pi}(n)$:

1. A random function H is chosen
2. GenRSA is run to get (N, e, d)

$\mathcal{A}$ is given $pk = (N, e)$ & may query $H(\cdot)$. $\mathcal{A}$ outputs 2 msgs $m_0, m_1 \in \{0,1\}^{\ell}$

3. $\mathcal{A}$ random bit b & $r \leftarrow \mathbb{Z}_N^*$ are chosen. $\mathcal{A}$ is given

$$r^e \bmod N, \quad \mathcal{H}(r) \oplus m_b.$$

$\mathcal{A}$ may continue to query $\mathcal{H}$.

4. $\mathcal{A}$ o/ps bit b'. The output of the expt is 1 if $b' = b$, 0 o.w.

Let us define $\varepsilon = \Pr\left(\mathrm{PubK}_{\mathcal{A},\Pi}(1^n) = 1\right)$

Let Query denote the event that $\mathcal{A}$ queried r to $\mathcal{H}$.

Let Succ be the event that $\mathrm{PubK}_{\mathcal{A},\Pi}(1^n) = 1$.

$$\Pr(\mathrm{Succ}) = \Pr(\mathrm{Succ} \wedge \overline{\mathrm{Query}}) + \Pr(\mathrm{Succ} \wedge \mathrm{Query}).$$

$$\leq \Pr(\mathrm{Succ} \wedge \overline{\mathrm{Query}}) + \Pr(\mathrm{Query}).$$

Claim: If H is a random oracle
$\Pr(\mathrm{Succ} \wedge \overline{\mathrm{Query}}) \leq \frac{1}{2}$.

Claim: If RSA is hard relative to GenRSA, H is modeled as RO, then $\Pr(\mathrm{Query})$ is negligible.

Pf Sketch: If Query occurs, then one of $\mathcal{A}$'s queries satisfies $r^e = c_1 \bmod N$.

$\therefore$ r is an answer to RSA.

Hence Pr(Query) is negligible as long as RSA is hard.

Boolean Fourier Analysis.

$\boxed{N = 2^n}$

Fourier Transform over $\mathbb{Z}_2^n$:

FT is a change of basis (essentially).

Consider a set of functions $\{\delta_y(x)\}_{y \in \{0,1\}^n}$

$$\delta_y(x) = 1 \text{ if } x = y$$
$$= 0 \text{ else.}$$

Let $g : \{0,1\}^n \to \mathbb{C}$, then

$$g(x) = \sum_{y \in \{0,1\}^n} g(y) \, \delta_y(x).$$

Called "standard" representation.

$$g = \left.\begin{bmatrix} g(0^n) \\ g(0^{n-1}1) \\ \vdots \\ g(1^n) \end{bmatrix}\right\} 2^n.$$

δ_y is a column vector with 0's everywhere except y^{th} position where we have a 1.

Fourier / Parity Basis :

Let $\sigma, x \in \mathbb{F}_2^n$, then

$$\sigma \cdot x = \sum_{i=1}^{n} \sigma_i x_i \pmod 2.$$

$$= \bigoplus_{i : \sigma_i = 1} x_i$$

$\pm$ version:

$$(-1)^{\sigma x} = \begin{cases} 1 & \text{if } \sigma\cdot x = 0 \\ -1 & \text{if } \sigma\cdot x = 1. \end{cases}$$

$\triangleq \chi_\sigma(x)$. Fourier characteristic.

Note:

$$\chi_0(x) = 1.$$

Define the Fourier Basis as $\{\chi_\sigma\}_{\sigma \in \{0,1\}^n}$

$$\chi_\sigma = \left.\begin{bmatrix} \chi_\sigma(0^n) \\ \chi_\sigma(0^{n-1}1) \\ \vdots \\ \chi_\sigma(1^n) \end{bmatrix}\right\} 2^n.$$

Prove:

1) 2^n in number ✓

2). Orthogonal.

We'll show:

$$\sum_{x \in \{0,1\}^n} \chi_\sigma(x)\,\chi_\gamma(x) = 0 \quad \text{if } \sigma \neq \gamma$$
$$= 2^n \quad \text{o.w.}$$

$$\underbrace{\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \chi_\sigma(x)\,\chi_\gamma(x)}_{} = 0 \quad \text{if } \sigma \neq \gamma$$
$$= 1 \quad \text{o.w.}$$

$$\mathbb{E}_{x \leftarrow \{0,1\}^n}\left(\underbrace{\chi_\sigma(x)\,\chi_\gamma(x)}_{\chi_{\sigma \oplus \gamma}(x)}\right) = 0 \quad \text{if } \sigma \neq \gamma$$
$$= 1 \quad \text{o.w.}$$

Consider

$$E_x\left[\chi_\sigma(x)\right]$$

Case 1: $\sigma \neq 0$

$$\begin{aligned}
E_x\left[\chi_\sigma(x)\right] &= E_x\left[(-1)^{\sigma x}\right] \\
&= E_x\left[\prod_{i:\sigma_i=1}(-1)^{x_i}\right] \\
&= \prod_{i:\sigma_i=1}\left[E_{x_i}\left((-1)^{x_i}\right)\right] \\
&= \prod_{i:\sigma_i=1}\left(\tfrac{1}{2}(-1)^1 + \tfrac{1}{2}(-1)^0\right) \\
&= 0.
\end{aligned}$$

Case 2: $\sigma = 0$

then $E_x\left[\chi_\sigma(x)\right] = 1.$

Hence

$$\underset{x \leftarrow \{0,1\}^n}{E_x}\left[\chi_\sigma(x)\right] = 1 \quad \text{if } \sigma = 0$$
$$= 0 \quad \text{otherwise}$$

Consider

$$E_x\left[\chi_\sigma(x)\chi_\gamma(x)\right] = E_x\left(\prod_{i:\sigma_i=1}(-1)^{x_i}\prod_{i:\gamma_i=1}(-1)^{x_i}\right)$$
$$= E_x\left(\prod_{\sigma_i\oplus\gamma_i=1}(-1)^{x_i}\right)$$
$$= E_x\left[\chi_{\sigma\oplus\gamma}(x)\right].$$
$$= 1 \text{ if } \sigma\oplus\gamma = 0, \text{ else } 0.$$

Change of Basis View:

$$g(x) = \sum_{\gamma \in \mathbb{F}_2^n} \hat{g}(\gamma)\, \chi_\gamma(x)$$

Claim: $\hat{g}(\sigma) = E_x\left[\chi_\sigma(x)\, g(x)\right]$

Proof: $E_x\left(\chi_\sigma(x)\, g(x)\right) = E_x\left(\sum_\gamma \hat{g}(\gamma)\chi_\gamma(x)\, \chi_\sigma(x)\right)$

$= \sum_\gamma \hat{g}(\gamma)\, E_x\left(\chi_\sigma(x)\chi_\gamma(x)\right)$

$= \hat{g}(\sigma).$

Special case $\hat{g}(0)$

$E_x\left(\chi_0(x)\, g(x)\right) = E_x\left(g(x)\right)$

Implementation of Basis Change:

$N = 2^n$

Claim: $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x g(x) |x\rangle$

Then $H^{\otimes n} |\psi\rangle = \sum_\gamma \hat{g}(\gamma) |\gamma\rangle$

Proof: $H^{\otimes n} |\psi\rangle = \frac{1}{\sqrt{N}} \sum_x g(x) \underbrace{H^{\otimes n} |x\rangle}_{\sum_\gamma \frac{1}{\sqrt{N}} (-1)^{\gamma x} |\gamma\rangle}$

$= \frac{1}{\sqrt{N}} \sum_x g(x) \sum_\gamma \frac{1}{\sqrt{N}} (-1)^{\gamma x} |\gamma\rangle$

$= \sum_\gamma \frac{1}{N} \sum_x g(x) (-1)^{\gamma \cdot x} |\gamma\rangle$

$= \sum_\gamma E_x\left(g(x) \chi_\gamma(x)\right) |\gamma\rangle = \sum_\gamma \hat{g}(\gamma) |\gamma\rangle.$

$$|\psi\rangle = H^{\otimes n} \sum_{\gamma} \hat{g}(\gamma)\, |\gamma\rangle.$$

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$$

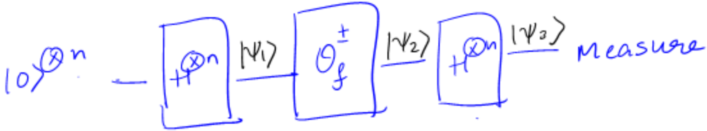
$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x} g(x)\, |x\rangle$$

$$|\psi_3\rangle = \sum_{\gamma} \hat{g}(\gamma)\, |\gamma\rangle.$$

Deutsch-Josza (Recall):

$f : \{0,1\}^n \to \{0,1\}$

Promise 1) f is 0 or 2) f is balanced.



Let $g(x) = (-1)^{f(x)}$.

$\hat{g}(0) = E_x(g(x)) = E_x((-1)^{f(x)})$

Tells which condition is true.

Convince yourselves that o/p of ckt is $\sum_{\gamma} \hat{g}(\gamma)|\gamma\rangle$