


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۱۶ مهر ۱۳۹۱

جلسه‌ی ۷: خانواده توابع RSAو رابین، تابع هاردکور

مدرس: شهرام خزائی *نگارنده: مهنام السادات میرمخلصونی*

۱ خانواده RSA

فرض کنید سه‌تایی تصادفی (N, e, y) داده شده که $N = pq$، $p, q \in \Pi_n$ و $\gcd(e, \varphi(N)) = ۱$. فرض RSAادعا می‌کند که احتمال موفقیت هر حمله‌کننده‌ی کارایی که بتواند از روی (N, e, y) مقدار x را طوری به دست بیاورد که $y = x^e \bmod N$ باشد، ناچیز است. به عبارت دقیق‌تر فرض RSAبه صورت زیر است.

فرض RSA. برای هر مهاجم $\mathcal{A} \in \mathsf{nuPPT}$ یک تابع ناچیز $\varepsilon(n) \in \mathsf{NEG}$ وجود دارد به طوری که:

$$\Pr\{p, q \leftarrow \Pi_n, N = pq; e \leftarrow \mathbb{Z}^*_{\varphi(N)}; y \leftarrow \mathbb{Z}^*_n; x \leftarrow \mathcal{A}(N, e, y) : x^e = y \bmod N\} \leq \varepsilon(n)$$

تعریف ۱ *خانواده RSA به صورت زیر تعریف می‌شود:*

$$\mathcal{F} = \{f_i : \mathcal{D}_i \longrightarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$$

که در آن

$$\mathcal{I} = \{(N, e) : N = pq \ ; \ p, q \in \Pi_n \ ; \ e \in \ \mathbb{Z}^*_{\varphi(N)}\}$$
$$f_{N,e}(x) = x^e \bmod N \text{ و } \mathcal{R}_i = \mathcal{D}_i = \mathbb{Z}^*_N$$

قضیه ۱ *اگر فرض RSA درست باشد، RSA خانواده توابع یک‌طرفه می‌شود.*

قضیه ۲ *تابع $f_{N,e}(x) = x^e \bmod N$ یک جایگشت از $\mathbb{Z}^*_N$ است که در آن $e \in \ \mathbb{Z}^*_{\varphi(N)}$.*
برهان. *چون e یک عنصر $\mathbb{Z}^*_{\varphi(N)}$ است پس $(N, e) = ۱$ (طبق قضیه اویلر) و بنابراین d ای وجود دارد که:*

$$ed = ۱ \bmod N$$

حال نشان می‌دهیم تابع $g_{N,e}(x) = x^d$ تابع معکوس f است.

$$g_{N,e}(f_{N,e}(x)) = g_{N,e}(x^e) = (x^e)^d = x^{ed} = x$$

پس خانواده RSA ، خانواده ای از جایگشت‌هاست.(جایگشت یک تابع یک به یک و پوشاست).

■

تعریف ۲ *خانواده‌ی $\mathcal{F} = \{f_i : \mathcal{D}_i \longrightarrow \mathcal{R}_i\}_{i\in\mathcal{I}}$، یک خانواده از جایگشت‌های یک‌طرفه است اگر $\mathcal{F}$ یک خانواده از توابع یک‌طرفه باشد و برای هر $i \in \mathcal{I}$ تابع f_i یک جایگشت باشد.*

مثال ۳ *خانواده RSA یک خانواده از جایگشت‌های یک‌طرفه است.*

تعریف ۴ *یک خانواده از جایگشت‌های دریچه‌دار یک خانواده به صورت*

$$\mathcal{F} = \{f_i : \mathcal{D}_i \longrightarrow \mathcal{R}_i\}_{i\in\mathcal{I}}$$

است که شرایط زیر را داراست:

- *برای هر $i \in \mathcal{I}$، تابع f_i یک جایگشت است.*
- *یک الگوریتم PPT وجود دارد به طوری که برای هر $i \in \mathcal{I}$، (i,t) را محاسبه می‌کند (t دریچه اطلاعات است.).*
- *یک ماشین PPT وجود داشته باشد که برای $i \in \mathcal{I}$، $\mathcal{D}_i$ را محاسبه کند.*
- *یک ماشین PPT وجود داشته باشد که با داشتن $i \in \mathcal{I}$ و $x \in \mathcal{D}_i$، $f_i(x)$ را محاسبه کند.*
- *برای هر حمله‌کننده $\mathcal{A}$، تابع ناچیز $\varepsilon(n)$ وجود دارد که*

$$\Pr\{(i,t) \leftarrow \mathsf{Gen}(1^n), N = pq; x \leftarrow \mathcal{D}_i; y \leftarrow f_i(x); z \leftarrow \mathcal{A}(1^n, i, y) : f_i(z) = y\} \leq \varepsilon(n)$$

- *یک ماشین PPT وجود داشته باشد که با داشتن (i,t) و $y \in \mathcal{R}_i$ بتواند $f_i^{-1}(y)$ را محاسبه کند.*

درواقع جایگشت های یک طرفه دریچه دار، یک مجموعه از جایگشت های یک طرفه است که با به دست آوردن اطلاعات دریچه می توان معکوس جایگشت ها رایافت.

قضیه ۳ *اگر خانواده توابع یک طرفه RSA با*

$$ed = 1 \bmod N,\ e \in \mathbb{Z}^*_{\varphi(N)}, N = pq$$

دارای الگوریتم PPT Gen باشد به طوری که

$$[(N,e),d] \leftarrow \mathsf{Gen}(1^n)$$

$$f^{-1}_{N,d}(y) = y^d \bmod N$$

خانواده ای از جایگشت های دریچه دار است.

۲ فرض رابین

محاسبه ریشه‌ی eام به پیمانه N که N حاصلضرب دو عدد اول بزرگ باشد سخت است.حال می‌توان فرض مشابه زیر را درنظرگرفت: محاسبه ریشه دوم به پیمانه N بدون داشتن عامل‌های N سخت است. دقت کنید که این حالتی از RSAنیست، چون $1 \neq (2, \varphi(n))$). با این فرض می‌توانیم خانواده‌ی توابع دریچه‌دار رابین [1] را تعریف کنیم.

[1] Rabin

ابتدا مقدماتی را بیان می‌کنیم بعد توابع رابین را تعریف می‌کنیم.

تعریف ۵ *به مجموعه*

$$QR_p = \{x^۲ \bmod p \mid x \in \mathbb{Z}_p^*\}$$

مجموعه مانده‌های مربعی p می‌گویند و یک زیرگروه از $\mathbb{Z}_p^*$ است.

لم ۴ *اگر $p > ۲$ اول باشد، آن‌گاه QR_p یک گروه از اندازه $\frac{p-۱}{۲}$ است.*
برهان. *اگر $x^۲ = y^۲ \bmod p$ باشد آن‌گاه $(x+y)(x-y) = ۰$ درنتیجه $x = y$ یا $x = p-y \bmod p$ به عبارت دیگر اگر هر عنصر $\mathbb{Z}_p^*$ را به توان ۲ برسانیم هر کدام دقیقا به ۲ عنصر از $\mathbb{Z}_p^*$ می‌رود پس $|QR_p| = (\frac{p-۱}{۲})$.*
■

قضیه ۵ *اگر $p = ۴k+۳$ باشد و $y \in QR_p$، آن گاه $(y^{k+۱})^۲ = y$.*
برهان. *چون $y \in QR_p$ می‌توان فرض کرد $y = a^۲ \bmod p$. حال داریم:*

$$(y^{k+۱})^۲ = a^{۲(k+۱)^۲} = a^{۴k+۴} = a^{p+۱} = a^۲ = y$$

(قضیه اویلر $a^{p-۱} = ۱ \bmod p$) ■

قضیه ۶ *(باقی مانده چینی)*
$p_k, p_{k-۱}.....p_۱,$ دو به دو نسبت به هم اولند ($\gcd(p_i, p_j) = ۱$). فرض کنید $N = p_k p_{k-۱}...p_۱$ آن‌گاه نگاشت

$$c_N : \mathbb{Z}_n \to \mathbb{Z}_{p_۱}\mathbb{Z}_{p_۲}...\mathbb{Z}_{p_k}$$

$$c_N(y) = (y \bmod p_۱, ..., y \bmod p_k)$$

یک به یک و پوشاست.

قضیه ۷ *فرض کنید $N = pq$ و برای هر $x \in \mathbb{Z}_N^*$ داریم $c_N(x) = (y, z)$ آن گاه $x \in QR_N$ اگر و فقط اگر $z \in QR_p$ و $y \in QR_p$.*

قضیه ۸ *نگاشت $f : x \to x^۲ \bmod N$، ۴ به ۱ است که $N = pq$.*
برهان. *فرض کنید $c = x^۲ = f(x)$ آن‌گاه چون c مربع است y و z وجود دارد که*

$$yz = c = x^۲ \ , \ z = a^۲ \bmod q \ , \ y = b^۲ \bmod p$$

.
در واقع می‌توان y و z را به روش زیر به‌دست آورد

$$c \bmod p = x^۲ \bmod p = (x \bmod p)^۲ = y$$
$$c \bmod q = x^۲ \bmod q = (x \bmod q)^۲ = z$$

حال

$$f(ab) = f((p-a)b) = f(a(q-b))$$

$$= f((p-a)(q-b)) = (ab)^۲ = a^۲b^۲ = yz = x^۲ = c$$

■

نتیجه ۶ *اگر* $N = pq$ *آنگاه* $|QR_N| = \frac{|\mathbb{Z}_N^*|}{۴}$.

بنابراین فرض رابین را می‌توان به صورت زیر ارائه کرد.

فرض رابین. برای هر مهاجم $\mathcal{A} \in \mathsf{nuPPT}$ یک تابع ناچیز $\varepsilon(n) \in \mathsf{NEG}$ وجود دارد به طوری که:

$$\Pr\{p, q \leftarrow \Pi_n, N = pq; y \leftarrow QR_N; x \leftarrow \mathcal{A}(N, y) : x^۲ = y \bmod N\} \leq \varepsilon(n)$$

۳ خانواده توابع رابین

تعریف ۷ *خانواده توابع رابین به شکل زیر تعریف می‌شود*

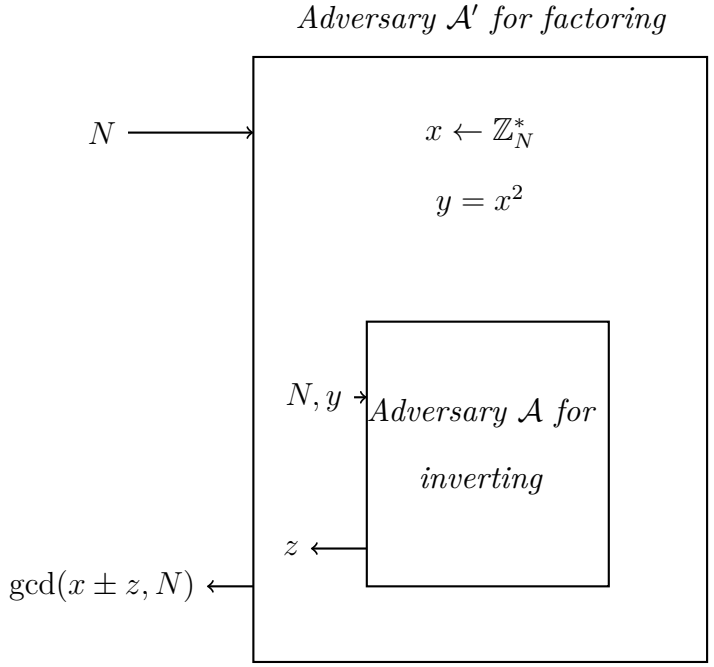
$$R = \{f_i : \mathcal{D}_i \longrightarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$$

$$I = \{N \mid N = pq, q, p \in \Pi_n\} .$$

$$D_i = \mathbb{Z}_N^*, R_i = QR_N, f_N(x) = x^۲ \bmod N$$

خانواده توابع رابین یک‌طرفه هستند.

قضیه ۹ *فرض رابین و فرض تجزیه‌پذیری معادلند.*
برهان. *ثابت می‌کنیم اگر فرض تجزیه‌پذیری برقرار باشد فرض رابین برقرار است.*
برهان خلف
فرض خلف: توابع رابین معکوس‌پذیرند. پس حمله‌کننده $\mathcal{A}$ *وجود دارد که توابع رابین را معکوس می‌کند، حال حمله‌کننده* $\mathcal{A}'$ *را به صورت زیر در نظر می‌گیریم*



حمله‌کننده $\mathcal{A}'$ عوامل N را به دست می‌دهد زیرا
$z^2 = x^2 \bmod N$ *درنتیجه* $x^2 - z^2 = 0 \bmod N$ *که می‌توان به صورت* $(x-z)(x+z) = 0 \bmod pq$ *نوشت درنتیجه* $(x-z)$ ، $(x+z)$ *شامل عامل‌های* N *هستند.*
حال ثابت می‌کنیم اگر فرض رابین برقرار باشد فرض تجزیه‌پذیری برقرار است.
برهان خلف
فرض خلف: فرض کنید N *تجزیه‌پذیر باشد پس* p *و* q *به دست می‌آیند.*

$$N = pq \Longrightarrow \varphi(N) = (p-1)(q-1)$$

حال با قضیه باقی‌مانده چینی به راحتی ریشه دوم قابل محاسبه است.

■

اگر در تعریف توابع رابین D_i را به QR_N تحدید کنیم، این مجموعه، مجموعه جایگشت‌های دریچه‌دار رابین می‌شوند.

۴ تابع هاردکور

تعریف ۸ *تابع* $h : \{0,1\}^* \longrightarrow \{0,1\}$ *را هارکور*[۲] *برای تابع یک‌طرفه* f *می نامیم اگر یک الگوریتم* $p.p.t$ *برای محاسبه* $h(x)$ *وجود داشته باشد و*

$$\forall \mathcal{A}\ \exists \varepsilon(n)\ \Pr\{x \leftarrow \{0,1\}^k : \mathcal{A}(1^n, f(x)) = h(x)\} \leq \varepsilon(n)$$

[۲] hardcore

مثال‌هایی که هاردکور نیست:

- تابع $f_p(x) = g^x$ (که g مولد گروه است) را در نظر بگیرید تابع h را به صورت زیر در نظر می‌گیریم

$$h(x) = \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square resigue} \\ -1 & \text{if } n \textit{ isn't a square resigue} \end{cases}$$

حال چون

$$\left(\frac{y}{p}\right) = \left(\frac{g^x}{p}\right) = \left(\frac{g}{p}\right)^x$$

اگر y مانده‌ی مربعی نباشد آن‌گاه x زوج نیست، پس h هاردکور نیست.

- فرض کنید e فرد است و $f_N(x) = x^e$ ، $N = \Pi p_i^{\alpha_i}$ و $\gcd(e, \varphi(N)) = ۱$ باشد.
تابع h را به همان صورت بالا تعریف می‌کنیم.

حال چون e فرد است $\left(\frac{x}{N}\right)^e = \left(\frac{x}{N}\right)$ پس $\left(\frac{f(x)}{N}\right) = \left(\frac{y}{N}\right)$ درنتیجه h برای f_N هاردکور نیست.

مثال‌هایی که هاردکور هست:

- تابع $\text{half}_N(x)$ که برای $۰ \leq x \leq \frac{N}{۲}$ برابر با یک است، تابع هاردکور برای RSAاست.
- تابع $\text{half}_{p-۱}(x)$ یک هاردکور برای تابع $f_{p,g}(x) = g^x \bmod p$ است.

دقت کنید اگر h برای تابع یک طرفه f هاردکور باشد، برای $g(x) = (f(x), h(x))$، هاردکور نیست.

۱.۴ یک تابع هاردکور برای هر تابع یک طرفه

فرض کنید $\langle x, r\rangle$، ضرب داخلی x و r باشد یعنی

$$\langle x, r\rangle = \sum x_i r_i \bmod ۲$$

فرض کنید f یک OWF(OWP) باشد و تابع g را به صورت زیر تعریف می‌کنیم:

$$g(x, r) = (f(x), r)$$

که $|x| = |r|$.
آن‌گاه g یک OWF(OWP) و $h(x, r) = \langle x, r\rangle$ یک هاردکور است.