


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۱۱ مهر ۱۳۹۱

جلسه‌ی ۶: تجزیه‌پذیری، لگاریتم گسسته و خانواده توابع یک‌طرفه

مدرس: شهرام خزائی *نگارنده: حلیمه خوجملی*

۱ نمادگذاری

PPT: مجموعه الگوریتم‌های تصادفی چندجمله‌ای[۱]
nuPPT: مجموعه حمله‌کننده[۲]های تصادفی چندجمله‌ای غیریکنواخت[۳]
NEG: مجموعه توابع ناچیز[۴]
Poly: مجموعه توابع چندجمله‌ای
$\mathsf{INVERT}_{\mathcal{A}}^{f}(n)$: پیشامدی است که در آن، حمله‌کننده $\mathcal{A}$ در معکوس کردن $f(x)$ که x یک رشته تصادفی به طول n است، موفق باشد. یعنی:

$$\Pr\{\mathsf{INVERT}_{\mathcal{A}}^{f}(n)\} = \Pr\{x \leftarrow \{0,1\}^n; y \leftarrow f(x) : f(\mathcal{A}(1^n, y)) = y\}$$

۲ یادآوری شرط یک‌طرفه قوی

تابع یک‌طرفه قوی دارای شرط زیر است:

$$\forall \mathcal{A} \in \mathsf{nuPPT}\ \exists \varepsilon(n) \in \mathsf{NEG}\ \forall n : \Pr\{\mathsf{INVERT}_{\mathcal{A}}^{f}(n)\} \leq \varepsilon(n)$$

شرط معادل:

$$\forall \mathcal{A} \in \mathsf{nuPPT}\ \forall p(n) \in \mathsf{Poly}\ \exists n_0\ \forall n \geq n_0 : \Pr\{\mathsf{INVERT}_{\mathcal{A}}^{f}(n)\} \leq \frac{1}{p(n)}$$

یعنی احتمال موفقیت حمله‌کننده‌های کارا در معکوس کردن f، به طور مجانبی از معکوس هر چند جمله‌ای کوچکتر است.
تابع یک‌طرفه قوی نباشد یعنی:

---

[۱] probabilistic polynomial time
[۲] adversary
[۳] non-uniform
[۴] negligible

$$\exists \mathcal{A} \in \mathsf{nuPPT}\ \exists p(n) \in \mathsf{Poly}\ \exists \text{ infintely many } n\text{'s} : \Pr\{\mathsf{INVERT}^f_{\mathcal{A}}(n)\} \ > \ \frac{1}{p(n)}$$

تابع یک‌طرفه ضعیف:

$$\exists q(n) \in \mathsf{Poly}\ \forall \mathcal{A} \in \mathsf{nuPPT}\ \exists n_0\ \forall n \geq n_0 : \Pr\{\mathsf{INVERT}^f_{\mathcal{A}}(n)\} \leq 1 - \frac{1}{q(n)}$$

تابع یک‌طرفه ضعیف نیست:

$$\forall q(n) \in \mathsf{Poly}\ \exists \mathcal{A} \in \mathsf{nuPPT}\ \exists \text{ infintely many } n\text{'s} : \Pr\{\mathsf{INVERT}^f_{\mathcal{A}}(n)\} \ > \ 1 - \frac{1}{q(n)}$$

۳ فرض تجزیه‌پذیری

تعریف ۱ *فرض تجزیه‌پذیری*[۵] *به صورت زیر تعریف می‌شود:*

$$\forall \mathcal{A} \in \mathsf{nuPPT}\ \exists \varepsilon(n) \in \mathsf{NEG}\ \forall n : \Pr\{p, q \leftarrow \Pi_n; N = pq : \mathcal{A}(N) \in \{p, q\}\} \leq \varepsilon(n)$$

که:

$$\Pi_n = \{q \mid q < 2^n, q \textit{ is a prime}\}\ .$$

یعنی احتمال موفقیت حمله‌کننده‌های کارا در پیدا کردن یکی از عوامل عدد N که حاصل‌ضرب دو عدد اول تصادفی n بیتی به اندازه کافی بزرگ است، ناچیز است.

سؤال: چرا فرض اینکه هیچ حمله‌کننده nuPPT نمی‌توان یافت که احتمال موفقیت غیرقابل اغماضی در تجزیه کردن اعداد مرکب بزرگ داشته باشد معقول است؟
مسئله تجزیه اعداد جزوه مسائل بسیار مهم می‌باشد و افراد زیادی سعی کردند تا آن را حل کنند، یکی از سخت‌ترین حالت‌های تجزیه اعداد این است که عدد مورد نظر حاصل‌ضرب دو عدد اول تصادفی n بیتی باشد. الگوریتم‌هایی برای تجزیه اعداد وجود دارد که پیچیدگی آن‌ها به صورت دقیق محاسبه می‌شود و از $\mathbf{۲}^{\mathcal{O}(\sqrt{n \log n})}$ است. البته الگوریتم‌های دیگری وجود دارد که پیچیدگی آن‌ها را به صورت فرا ابتکارانه[۶] تقریب می‌زنند و دارای پیچیدگی $\mathbf{۲}^{\mathcal{O}(\sqrt[۳]{n \log^۲ n})}$ است.
در عمل ماجول ۱۰۲۴-بیتی یا ۲۰۴۸-بیتی استفاده می شود که در حال حاضر غیر قابل شکستن است و بزرگترین عدد شکسته شده ۷۶۸-بیتی است که برای تجزیه آن پردازشی معادل ۱۵۰۰ سال کارکرد یک کامپیوتر معمولی استفاده شد.
به مثال تابع ضرب[۷] که قبلا بیان کردیم برمی‌گردیم، f_{mult} را به صورت زیر بیان می‌کنیم:

$$f_{\text{mult}}(x, y) = xy \qquad |x| = |y|$$

قبلاً بیان کردیم که f_{mult} به خودی خود یک‌طرفه قوی نیست ولی تحت تجزیه‌پذیری، یک‌طرفه‌ی ضعیف است.

[۵] factoring assumption
[۶] heuristic
[۷] multiplication

قضیه ۱ f_{mult} *با شرط تجزیه‌پذیری یک تابع یک‌طرفه ضعیف است.*
اثبات شهودی: از قضیه اعداد اول داریم

$$|\{q \mid q < x, q \text{ is a prime}\}| \sim \frac{x}{\ln x}$$

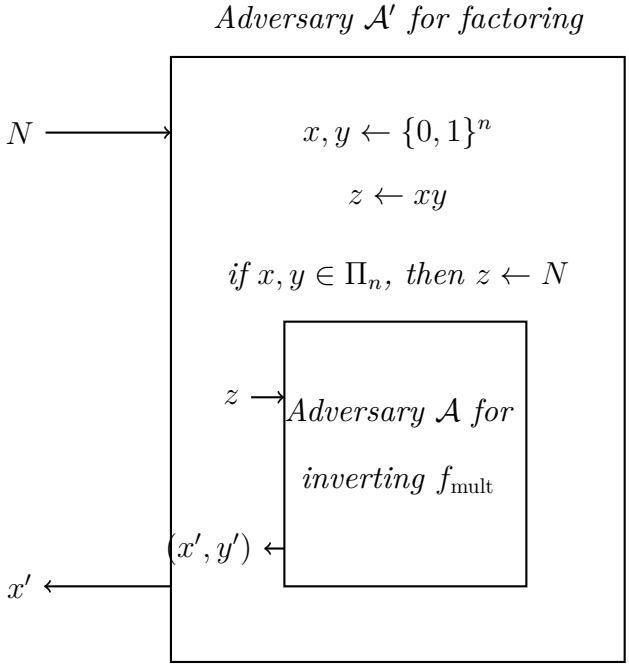
ولی از قضیه چبیشف [۸] *نیز داریم:*

$$\{q \mid q < x, q \text{ is a prime}\}| \geq \frac{x}{2\log_2 x}$$

احتمال اینکه یک عدد تصادفی n بیتی، عدد اول باشد حداقل $\frac{۱}{۲n}$ است، که احتمال قابل توجهی است. بنابراین برای تولید اعداد اول ابتدا اعداد تصادفی تولید کرده و به صورت احتمالاتی یا قطعی اول بودنشان را چک می‌کنیم. به عنوان مثال اگر برای یک ماجول ۲۰۴۸-بیتی RSA بخواهیم اعداد اول ۱۰۲۴ تولید کنیم، کافی است اول بودن حدود ۴۰۰۰ عدد تصادفی ۱۰۲۴-بیتی را امتحان کنیم، زیرا از هر ۲۰۰۰ عدد تصادفی به طور متوسط یکی از آن‌ها اول است. امّا احتمال اینکه یک عدد تصادفی $۲n$ بیتی حاصل‌ضرب دو عدد اول n بیتی باشد حدود $(\frac{۱}{۲n})^۲ = \frac{۱}{۴n^۲}$ است. به عبارت دیگر کسر قابل توجهی از اعداد به این فرم هستند که طبق فرض تجزیه‌پذیری، پیدا کردن عوامل اول آن‌ها کار دشواری است، که نشان دهنده یک‌طرفه ضعیف بودن تابع f_{mult} است.

برهان. *فرض می‌کنیم f_{mult} یک‌طرفه ضعیف نباشد، پس به ازای هر $q(n)$ از جمله $q(n) = ۸n^۲$ یک حمله‌کننده $\mathcal{A} \in \mathsf{nuPPT}$ وجود دارد که $f_{\text{mult}}(x)$ را برای x های تصادفی n بیتی با احتمال حداقل $\frac{۱}{q(n)}$ برای تعداد نامتناهی n معکوس می‌کند. حال با استفاده از این $\mathcal{A}$ یک $\mathcal{A}' \in \mathsf{nuPPT}$ برای فرض تجزیه‌پذیری می‌سازیم. ورودی $\mathcal{A}$ باید حاصل‌ضرب دو عدد تصادفی n بیتی باشد ولی N حاصل‌ضرب دو عدد اول تصادفی n بیتی است، بنابراین عدد N را که ورودی $\mathcal{A}'$ است نمی‌توان مستقیم به عنوان ورودی به $\mathcal{A}$ داد. برای حل مشکل، مشابه ایده جلسه قبل، حمله‌کننده کارای $\mathcal{A}'$ را به صورت زیر می‌سازیم:*
حمله‌کننده $\mathcal{A}'$ ابتدا دو عدد تصادفی n بیتی x و y را تولید می‌کند و $z = xy$ را محاسبه می‌کند. عدد z دارای توزیع مناسب به عنوان ورودی $\mathcal{A}$ است. اگر x و y هر دو عدد اول باشند، $\mathcal{A}'$ به جای z، عدد N را که دریافت کرده است به $\mathcal{A}$ می‌دهد. در این صورت توزیع ورودی $\mathcal{A}$ باز هم مناسب است. در نهایت $\mathcal{A}'$ یکی از خروجی‌های $\mathcal{A}$ را به عنوان خروجی $\mathcal{A}'$ برمی‌گرداند.

[۸] Chebyshev



پیشامد $\mathsf{FACT}_{\mathcal{A}'}(n)$ *را پیشامدی بگیرید که در آن، حمله‌کننده* $\mathcal{A}'$ *در پیدا کردن یکی از عوامل عدد* N *که حاصل‌ضرب دو عدد اول تصادفی* n *بیتی است، موفق باشد. داریم:*

$$\Pr\{\mathsf{FACT}_{\mathcal{A}'}(n)\} \geq \Pr\{x, y \in \Pi_n \wedge \mathsf{INVERT}_{\mathcal{A}}^{f_{\text{mult}}}(n)\}$$

با استفاده از کران اجتماع[۹] *داریم:*

$$\begin{aligned}
\Pr\{\overline{x, y \in \Pi_n} \vee \overline{\mathsf{INVERT}_{\mathcal{A}}^{f_{\text{mult}}}(n)}\} &\leq \Pr\{\overline{x, y \in \Pi_n}\} + \Pr\{\overline{\mathsf{INVERT}_{\mathcal{A}}^{f_{\text{mult}}}(n)}\} \\
&\leq \underbrace{1 - \frac{1}{4n^2}}_{\text{Chebyshev}} + \frac{1}{8n^2} \\
&= 1 - \tfrac{1}{8n^2}
\end{aligned}$$

بنابراین:

$$\Pr\{\mathsf{FACT}_{\mathcal{A}'}(n)\} \geq 1 - (1 - \frac{1}{8n^2}) = \frac{1}{8n^2}$$

پس تابع ناچیز $\varepsilon(n)$ *وجود ندارد که احتمال موفقیت* $\mathcal{A}'$ *را از بالا محدود کند؛ یعنی آنچه که در فرض تجزیه‌پذیری آمده است برقرار نیست. بنابراین نشان دادیم که اگر* f_{mult} *یک‌طرفه ضعیف نباشد، فرض تجزیه پذیری درست نیست.*

■■

[۹] union bound

۴ خانواده توابع یک‌طرفه

برای ساختن سامانه‌های رمز[۱۰] به خانواده توابع یک‌طرفه[۱۱] نیاز داریم.

تعریف ۲ *مجموعه $\mathcal{F}$ که به صورت زیر بیان شده*

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

خانواده‌ای از توابع یک‌طرفه است اگر شرط‌های زیر را داشته باشد:

- *(قابلیت تولید کارای توابع) الگوریتم* $\mathsf{Gen} \in \mathsf{PPT}$ *وجود داشته باشد به طوری که* $i \leftarrow \mathsf{Gen}(1^n)$ *یک عضو* $i \in \mathcal{I}$ *تولید کند.*
- *(قابلیت نمونه برداری کارای اعضای دامنه) الگوریتم PPTای وجود داشته باشد که از روی $i \in \mathcal{I}$ یک عضو $\mathcal{D}_i$ را به صورت یکنواخت تولید کند.*
- *(قابلیت محاسبه کارای توابع روی مقادیر دامنه) الگوریتم PPTای وجود داشته باشد که به ازای هر $i \in \mathcal{I}$ و $x \in \mathcal{D}_i$ بتواند $f_i(x)$ را محاسبه کند.*
- *(سخت بودن محاسبه نقش معکوس برای حمله‌کننده‌های کارا)*

$$\forall \mathcal{A} \in \mathsf{nuPPT}\ \exists \varepsilon(n) \in \mathsf{NEG}\ \forall n :$$

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

قضیه ۲ *تابع یک‌طرفه قوی داریم اگر و تنها اگر خانواده‌ای از توابع یک‌طرفه داشته باشیم.*

برهان. روش ساخت به صورت زیر است. اگر تابع یک‌طرفه قوی $f : \{۰,۱\}^* \longrightarrow \{۰,۱\}^*$ وجود داشته باشد یک خانواده از توابع یک‌طرفه را به صورت زیر می‌سازیم.

$$\mathcal{F} = \{f_i : \mathcal{D}_i \longrightarrow \mathcal{R}_i\}_{i \in I}$$
$$\mathcal{I} = \{0\}$$
$$\mathcal{D}_0 = \{0,1\}^*, \mathcal{R}_0 = \{0,1\}^*$$
$$f_0 = f$$

برعکس: اگر خانواده‌ای از توابع یک‌طرفه $\mathcal{F}$ داشته باشیم تابع یک طرفه قوی را به صورت زیر می‌سازیم.

$$g(r_1, r_2) = (i, f_i(x)) \qquad r_1, r_2 \in \{0,1\}^{p(n)}$$

[۱۰] cryptosystem
[۱۱] collection of one-way functions

که r_1 مقدار تصادفی است که Gen استفاده می‌کند، r_1 مقدار تصادفی است که الگوریتم نمونه‌برداری اعضای دامنه استفاده می‌کند، و $p(n)$ کران بالای زمان اجرای الگوریتم Gen و الگوریتم نمونه‌برداری اعضای دامنه می‌باشد. اثبات یک‌طرفه بودن ساده است.

■■

۵ خانواده توابع یک‌طرفه مبتنی بر فرض تجزیه‌پذیری

قضیه ۳ *اگر فرض تجزیه‌پذیری درست باشد، آنگاه $\mathcal{F}$ یک خانواده توابع یک‌طرفه است.*

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

$$\mathcal{I} = 2\mathbb{N}$$

$$\mathcal{D}_i = \{(p,q) \mid p,q \text{ are prime and },\ |p| = |q| = \frac{i}{2}\}$$

$$f_i(p,q) = pq$$

اثبات قضیه آسان است.

۶ خانواده توابع یک‌طرفه مبتنی بر سختی لگاریتمی گسسته

می‌دانیم برای p های اول $\mathbb{Z}_p^* = \{0, 1, \ldots, p-1\}$ به همراه ضرب پیمانه‌ای به هنگ p یک گروه متناهی با مرتبه[۱۲] $p-1$ است و اگر g یک مولد این گروه باشد $\mathbb{Z}_p^* = \langle g \rangle = \{g^0, g^1, \ldots, g^{p-2}\}$.
اگر تجزیه مرتبه گروه را بدانیم آنگاه الگوریتم کارایی وجود دارد که یک مولد برای گروه بدهد و همچنین الگوریتم کارایی وجود دارد که g و p را باهم و با توزیع یکنواخت تولید می‌کند.
اگر $\mathbb{G}$ یک گروه متناهی باشد، آنگاه:

$$\mathbb{G} = \{g^i : i = 1, \ldots, |\mathbb{G}|\}$$

اگر $x \in \mathbb{Z}_{|\mathbb{G}|}$ ، با توجه به رابطه بازگشتی $g^{2^{i+1}} = (g^{2^i})^2$ و با در نظر گرفتن نمایش باینری x، می‌توان g^x را به صورت کارا محاسبه کرد.

$$g^x = g^{\sum x_i 2^i} = \prod (g^{2^i})^{x_i}$$

ولی لزوماً از روی $y = g^x$ نمی‌توانیم x را به طور کارا محاسبه کرد (x را لگاریتم گسسته y می‌نامیم). سختی محاسبه لگاریتم گسسته در حالت کلی به اندازه بزرگترین عامل اول مرتبه گروه بستگی دارد. به همین دلیل در رمزنگاری از گروه‌هایی که مرتبه آن ها اول باشد استفاده می‌کنیم.
به عنوان مثال استفاده از زیرگروه $\mathbb{Z}^*_{2q+1}$ که دارای مرتبه q است، بسیار کاربرد دارد. در این حالت اگر g مولد $\mathbb{Z}^*_{2q+1}$ باشد، g^2 مولد $\mathbb{G}$ است.

[۱۲] order

$$\mathbb{Z}^*_{2q+1} = \langle g \rangle \implies \mathbb{G} = \langle g^2 \rangle$$

تعریف ۳ *فرض کنید الگوریتم کارای* $(\mathbb{G}, g, q) \leftarrow \mathsf{GroupGen}(1^n)$ *برای تولید یک گروه و یک مولد آن که* $|\mathbb{G}| = q$ *یک عدد اول* n *بیتی است، وجود داشته باشد. می‌گوییم مسئله لگاریتم گسسته برای خانواده گروه‌های* GroupGen *مشکل است اگر:*

$$\forall \mathcal{A} \in \mathsf{nuPPT}\ \exists \varepsilon(n) \in \mathsf{NEG}\ \exists n_0 \forall n \geq n_0 :$$

$$\Pr\{(\mathbb{G}, g, q) \leftarrow \mathsf{GroupGen}(1^n); x \leftarrow \mathbb{Z}_q; y = g^x : \mathcal{A}(y) = x\} \leq \varepsilon(n)$$

قضیه ۴ *اگر مسئله لگاریتم گسسته برای خانواده گروه‌های* GroupGen *مشکل باشد، خانواده توابع نمایی که به صورت زیر تعریف می‌شوند، یک‌طرفه است:*

$$\mathcal{F} = \{f_i : \mathcal{D}_i \leftarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$$
$$\mathcal{I} = \{(\mathbb{G}, g, q) \mid (\mathbb{G}, g, q) \leftarrow \mathsf{GroupGen}(1^n; r), r \in \{0,1\}^{p(n)}\}$$
$$\mathcal{D}_i = \{x \mid x \in \mathbb{Z}_q\},\ \mathcal{R}_i = \mathbb{G}$$
$$f_i(x) = g^x$$

که $p(n)$ *زمان اجرای الگوریتم* $\mathsf{GroupGen}(1^n; r)$ *می‌باشد و* r *مقدار تصادفی است که استفاده می‌کند.*