


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۹ مهر ۱۳۹۱

جلسه‌ی ۵: تقویت سختی، استدلال کاهش در رمزنگاری، معرفی تابع یک‌طرفه جهانی f_{uni}

مدرس: شهرام خزائی *نگارنده: سحر مهرپور*

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

۲ تقویت سختی

قضیه ۱ (*قضیه تقویت سختی*[۵]) *برای هر تابع یک‌طرفه ضعیف f چندجمله‌ای $m(\cdot)$ وجود دارد به طوری که تابع g یک‌طرفه قوی است.*

$$g(x_1, \ldots, x_{m(n)}) = (f(x_1), \cdots, f(x_{m(n)}))$$

که $|x_1| = \ldots = |x_{m(n)}|$.

۳ استدلال کاهش در رمزنگاری

در نظریه پیچیدگی وقتی می‌گوییم مساله P به مساله Q کاهش می‌یابد، $P \leq_p Q$، یعنی حل کردن مساله P از حل کردن مساله Q سخت‌تر نیست. برای اثبات این‌که مساله P به مساله Q کاهش می‌یابد، کافی است نشان دهیم اگر الگوریتم A بتواند مساله Q را حل کند، می‌توان از آن برای ساخت الگوریتم A' برای حل مساله P، استفاده کرد.

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

استفاده از استدلال کاهش[۶] در رمزنگاری کمی متفاوت است. برای درک آن مثال زیر را بررسی می‌کنیم.

فرض کنیم f یک تابع یک‌طرفه قوی باشد. نشان می‌دهیم تابع g به صورت $g(x,y) = (f(x), f(y))$ یک‌طرفه قوی است.

شرط‌های تابع یک‌طرفه قوی را بررسی می‌کنیم:

- برقراری شرط اول بدیهی است، چون اگر محاسبه f آسان باشد، محاسبه g نیز آسان است.
- برای شرط دوم نقیض شرط را در نظر می‌گیریم و در اثبات آن از استدلال کاهش استفاده می‌کنیم:

فرض کنیم g یک‌طرفه ضعیف نباشد؛ پس یک حمله‌کننده کارا وجود دارد که احتمال موفقیت آن در معکوس کردن g قابل توجه باشد. نشان می‌دهیم که حمله‌کننده کارایی وجود دارد که f را با احتمال قابل توجهی معکوس می‌کند.

به طور دقیق‌تر فرض کنیم حمله‌کننده $\mathcal{A} \in \mathsf{nuPPT}$ و چندجمله‌ای $p(\cdot)$ وجود داشته باشدکه برای تعداد نامتناهی n داشته باشیم:

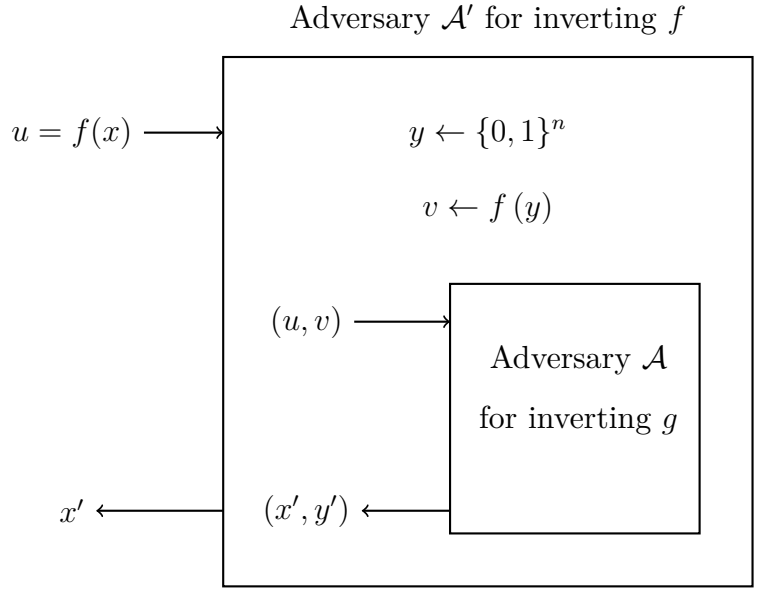
$$\Pr\{x,y \leftarrow \{0,1\}^n; (u,v) \leftarrow g(x,y); (x',y') \leftarrow \mathcal{A}\left(1^{2n}, \left(u,v\right)\right) : g(x',y') = (u,v)\} \geq \frac{1}{p(2n)}$$

با استفاده از $\mathcal{A}$، حمله‌کننده $\mathcal{A}' \in \mathsf{nuPPT}$ را به صورت زیر برای معکوس کردن f می‌سازیم.
حمله‌کننده $\mathcal{A}'$ ورودی $u = f(x)$ را دریافت می‌کند که x یک رشته تصادفی n بیتی است و هدف آن پیدا کردن یک نقش معکوس x' برای آن با احتمال موفقیت قابل توجه است.

اولین چیزی که به ذهن می‌رسد این است که ورودی (u,u) را به حمله‌کننده $\mathcal{A}$ بدهیم، اما این روش مناسبی نیست چون ممکن است حمله‌کننده $\mathcal{A}$ در پیداکردن نقش معکوس برای ورودی‌های به فرم $(f(x), f(x))$ که x یک رشته تصادفی n بیتی است دارای احتمال موفقیت ناچیز باشد. بنابراین ورودی حمله‌کننده $\mathcal{A}$، باید دارای توزیع مناسب باشد.

روش درست در شکل زیر دیده می‌شود. حمله‌کننده $\mathcal{A}'$ ابتدا $v = f(y)$ را برای یک رشته تصادفی n بیتی y محاسبه می‌کند و سپس ورودی (u,v) را به حمله‌کننده $\mathcal{A}$ می‌دهد. وقتی $\mathcal{A}$ خروجی (x',y') را برمی‌گرداند، $\mathcal{A}'$، x' را به عنوان خروجی برمی‌گرداند.

[۶] reduction argument



داریم:

$$\Pr\{x \leftarrow \{۰,۱\}^n; u \leftarrow f(x); x' \leftarrow \mathcal{A}'(۱^n, u) : f(x') = u\} \geq \frac{۱}{p(۲n)}$$

زیرا رویداد این‌که x' نقش معکوس $u = f(x)$ باشد (یعنی $\mathcal{A}'$ موفق باشد)، اجتماع دو رویداد زیر است:

- رویداد این‌که (x', y') نقش معکوس (u, v) باشد (یعنی $\mathcal{A}$ موفق باشد)،
- رویداد این‌که (x', y') نقش معکوس (u, v) نباشد (یعنی $\mathcal{A}$ موفق نباشد) ولی x' نقش معکوس u باشد.

پس اگر g یک‌طرفه نباشد، f نیز یک‌طرفه نیست.

۴ معرفی تابع یک‌طرفه جهانی f_{uni}

برای ساخت یک سامانه رمز[۷] به یک تابع یک‌طرفه قوی نیاز داریم. ولی فرض وجود تابع کافی نیست، بلکه باید آن را داشته باشیم. قضیه زیر، روشی برای ساخت یک تابع یک‌طرفه جهانی[۸]، به شرط وجود یک تابع یک‌طرفه بیان می‌کند. با داشتن این تابع یک‌طرفه ضعیف، می‌توانیم با استفاده از قضیه تقویت سختی تابع یک‌طرفه قوی را به دست آوریم.

قضیه ۲ *اگر تابع یک‌طرفه وجود داشته باشد، تابع f_{uni} که به روش زیر ساخته می‌شود یک‌طرفه ضعیف است.*

[۷] cryptosystem
[۸] universal one-way function

یک کدینگ استاندارد برای ماشین‌های تورینگ در نظر می‌گیریم و فرض کنیم که همه ماشین‌های به فرم M ۱ ۰ ... ۰ معادل باشند. تابع f_{uni} ابتدا رشته ورودی y را به دو رشته M و x تفکیک می‌کند که M به عنوان کد یک ماشین تورینگ و x به عنوان ورودی آن تفسیر می‌شود. سپس M روی x به تعداد $|y|^3$ گام اجرا می‌شود. اگر M خاتمه یافت $f_{\mathsf{uni}}(y) = (M, M(x))$ را به خروجی می‌دهد. در غیر این صورت $f_{\mathsf{uni}}(y) = (M, x)$ را به خروجی می‌دهد.

Algorithm ۱ $f_{\mathsf{uni}}(y)$

interpret y as $\langle M, x\rangle$ where $|M| = \log_2(|y|)$
run M on input x for $|y|^3$ steps
if M terminates **then**
  output $(M, M(x))$
else
  ouput (M, x)
end if

برهان. قبل از این‌که ثابت کنیم f_{uni} یک‌طرفه ضعیف است، لم زیر را ثابت می‌کنیم.

لم ۳ *اگر تابع یک‌طرفه (قوی) وجود داشته باشد، یک تابع یک‌طرفه (قوی) وجود دارد که در زمان $\mathcal{O}(n^2)$ قابل محاسبه است.*

برهان. فرض کنیم g تابع یک‌طرفه قوی باشد که در زمان $\mathcal{O}(n^c)$ قابل محاسبه باشد. اگر $c \leq 2$ لم بدیهی است. برای $c > 2$ یک تابع g' را که روی رشته‌های n^c بیتی عمل می‌کند، می‌سازیم و نشان می‌دهیم که یک‌طرفه قوی است و در زمان مربعی (برحسب طول ورودی) قابل محاسبه است.

تابع g' ورودی $m = n^c$ بیتی خود را به $\langle a, b\rangle$ تفکیک می‌کند که $|a| = n^c - n$ و $|b| = n$. برای این‌کار $n = \sqrt[c]{m}$ باید محاسبه شود. سپس $g'(\langle a, b\rangle)$ به صورت زیر محاسبه می‌شود:

$$g'(\langle a, b\rangle) = (a, g(b))$$

زمان محاسبه g' شامل $|a|$ مرحله برای کپی کردن a، $|b|^c$ مرحله برای محاسبه $g(b)$ و $\mathcal{O}(m^2)$ مرحله برای محاسبه $\sqrt[c]{m}$ و تفکیک کردن ورودی است.

$$\mathcal{O}(m^2) + |a| + |b|^c < \mathcal{O}(m^2)$$

اثبات یک‌طرفه بودن g' با استفاده از یک استدلال کاهش ساده صورت می‌پذیرد.

■

فرض کنید g تابع یک‌طرفه‌ای باشد که در زمان زمان مربعی قابل محاسبه است. اکنون نشان می‌دهیم f_{uni} یک‌طرفه ضعیف است. فرض می‌کنیم نباشد و می‌خواهیم به این تناقض برسیم که g یک‌طرفه قوی نیست.

$$\forall q \in \mathsf{Poly}\ \ \exists \mathcal{A} \in \mathsf{nuPPT}\ \ \exists \text{ infinitely many } n\text{'s}:$$

$$\Pr\{y \leftarrow \{0,1\}^n : f_{\mathsf{uni}}\left(\mathcal{A}\left(1^n, f_{\mathsf{uni}}\left(y\right)\right)\right) = f_{\mathsf{uni}}\left(y\right)\} > 1 - \frac{1}{q\left(n\right)}$$

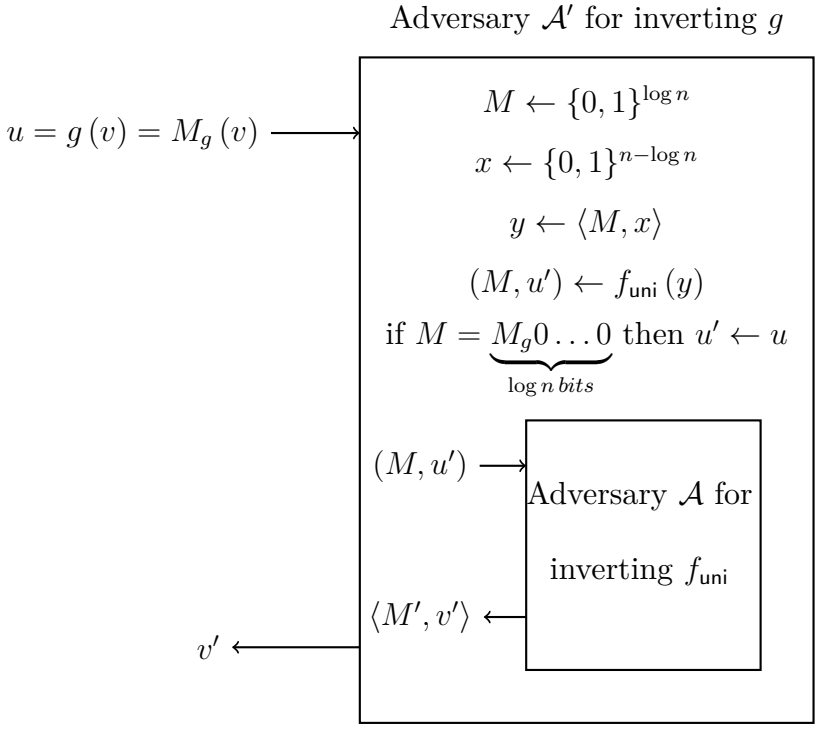
قرار دهید $q\left(n\right) = n^{۳}$.

$$\forall q \in \mathsf{Poly}\ \ \exists \mathcal{A} \in \mathsf{nuPPT}\ \ \exists \text{ infinitely many } n\text{'s}:$$
$$\Pr\{y \leftarrow \{0,1\}^n : \mathcal{A}\left(1^n, f_{\mathsf{uni}}\left(y\right)\right) \in f_{\mathsf{uni}}^{-1}\left(f_u\left(y\right)\right)\} > 1 - \frac{1}{n^3}$$

فرض کنیم M_g از نظر اندازه کوچکترین ماشین تورینگی باشد که g را محاسبه می‌کند (اندازه M_g ثابت است مثلا $|M_g| = ۱۰^{۵}$).
اگر $\log n > |M_g|$ باشد:

$$\Pr\{M \leftarrow \{0,1\}^{\log n} : M \text{ is equivalent to } M_g\} \geq$$
$$\Pr\{M \leftarrow \{0,1\}^{\log n} : M = \underbrace{M_g 0 \ldots 0}_{\log n\, bits}\} = 2^{-\log n} = \frac{1}{n}$$

پس برای nهای به اندازه کافی بزرگ، شانس خوبی (غیر قابل اغماض) داریم که یک رشته تصادفی $\log n$ بیتی توصیف یک ماشین تورینگ معادل M_g باشد.
اکنون یک حمله‌کننده به نام $\mathcal{A}'$ به صورت زیر برای معکوس کردن g می‌سازیم.



دقت کنید توزیع ورودی الگوریتم $\mathcal{A}'$، خروجی تابع g یا ماشین تورینگ M_g به ازای یک ورودی تصادفی $n-\log n$ بیتی است. بنابراین اگر $M = M_g \circ \ldots \circ$ باشد، (M,u) و (M,u') دارای توزیع یکسان می‌باشند. (شرط اجرا شدن g در زمان $\mathcal{O}\left(n^{۲}\right)$ اینجا استفاده می‌شود. اما اگر مثلاً g در زمان $\mathcal{O}\left(n^{c}\right)$ که $c > ۳$ است اجرا شود، برای nهای بزرگ، متغیرهای تصادفی u و u' توزیع یکسان نخواهند داشت؛ چون f_{uni} خاتمه نمی‌یابد.)

داریم:

$$\Pr\{v \leftarrow \{0,1\}^{n-\log n}; u = g(v) : \mathcal{A}' \text{ succeeds in inverting } u\} \geq$$
$$\Pr\{M = \underbrace{M_g 0 \ldots 0}_{\log n} \wedge \mathcal{A} \text{ succeeds in inverting } (M,u')\} \geq \frac{1}{n^3}$$

که بیانگر یک‌طرفه نبودن g است که تناقض است.

نامساوی اول واضح است، چون رویداد دوم زیرمجموعه رویداد اول است. برای نشان دادن نامساوی دوم، مکمل رویداد را درنظر می‌گیریم و از کران اجتماع[۹] استفاده می‌کنیم. داریم:

$$\Pr\{M \neq \underbrace{M_g 0 \ldots 0}_{\log n} \vee \mathcal{A} \text{ is not successful in inverting } (M,u')\} \leq$$
$$\Pr\{M \neq \underbrace{M_g 0 \ldots 0}_{\log n}\} + \Pr\{\mathcal{A} \text{ is not successful in inverting } u'\} \leq$$
$$1 - \frac{1}{n} + \frac{1}{n^3} < 1 - \frac{1}{n^3}$$

■

[۹] union bound