به نام خدا

دانشکده‌ی علوم ریاضی

مقدّمه‌ای بر رمزنگاری ۱۲ آبان ۱۳۹۲

جلسه‌ی ۱۱: تمایزناپذیری محاسباتی و تحلیل مجانبی

مدرس: دکتر شهرام خزائی *نگارنده: نوید علامتی*

۱ یادآوری

تعریف ۱ *سه‌تایی* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *یک سیستم رمز متقارن روی فضای* $\mathcal{M}$ *است که:*

- $k \leftarrow \mathsf{Gen}()$
- $\forall k \in \mathcal{K}, \forall m \in \mathcal{M} \quad c \leftarrow \mathsf{Enc}_k(m)$
- $\forall k \in \mathcal{K}, \forall c \in \mathcal{C} \quad m \leftarrow \mathsf{Dec}_k(c)$

و شرط نهایی زیر را دارد:

$$\Pr\{k \leftarrow \mathsf{Gen}() : \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m\} = ۱$$

برای سیستم رمز Π روی فضای پیام $\mathcal{M} \subset \{۰,۱\}^*$ آزمایش $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ را به صورت زیر در نظر بگیرید:

- $k \leftarrow \mathsf{Gen}()$
- $(m_۰, m_۱) \leftarrow \mathcal{A}()$ که $m_۰, m_۱ \in \mathcal{M}$ و $|m_۰| = |m_۱|$.
- $b \leftarrow \{۰,۱\}$
- $c \leftarrow \mathsf{Enc}_k(m_b)$
- $\hat{b} \in \{۰,۱\} \quad \hat{b} \leftarrow \mathcal{A}(c)$

در صورتی که b و $\hat{b}$ برابر باشند، خروجی آزمایش که با متغیر تصادفی $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ نشان داده می‌شود برابر یک و در غیر این صورت صفر تعریف می‌شود.

تعریف ۲ *می‌گوئیم سیستم رمز* Π، (t,ϵ)*-امن است اگر برای هر مهاجم* $\mathcal{A}$ *که در زمان* t *اجرا می‌شود، داشته باشیم:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱\} \leq \frac{۱}{۲}(۱ + \varepsilon)$$

۲ رویکردهای تحلیل سیستم‌های رمزنگاری

سیستم‌های رمزنگاری را می‌توان دو نوع تحلیل کرد:

- **رویکرد واقعی**[۱]: در این رویکرد می‌گوئیم یک سیستم (t,ε)-امن است، در صورتی که هیچ مهاجم با حدّاکثر زمان اجرای t نتواند با مزیت بیشتر از ε سیستم را بشکند.
- **رویکرد مجانبی**[۲]: در این رویکرد می‌گوئیم یک خانواده از سیستم‌های رمز امن است، هرگاه هیچ مهاجم *کارایی* نتواند با مزیت غیر *ناچیز* (قابل توجه) سیستم را بشکند.

تاکنون ما امنیت سیستم‌ها را به رویکرد واقعی (دقیق، عینی یا تحقیقی هم می‌توان گفت) مطرح کردیم. اما در ادامه از رویکرد مجانبی استفاده می‌کنیم که بی‌نیاز از t و ε و به دنبال کشیدن این مقادیر در تعاریف و اثبات‌های امنیتی است. اما باید مفاهیمی که در تعریف رویکرد مجانبی استفاده شده دقیقاً تعریف شوند.

خانواده‌ای از سیستم‌ها. در رویکرد واقعی، صرفا امنیت یک سیستم مطرح است در حالیکه در رویکرد مجانبی امنیت خانواده‌ای از سیستم‌ها مطرح است. اعضای خانواده توسّط یک پارامتر امنیّتی، که با n نشان داده می‌شود، شاخص می‌شوند.

مهاجم کارا. در رویکرد مجانبی زمان اجرای مهاجم برحسب پارامتر امنیّتی، n، سنجیده می‌شود و برای مدل کردن محدودیت قدرت محاسباتی مهاجم فرض می‌شود که مهاجم در زمان چندجمله‌ای برحسب پارامتر امنیّتی اجرا می‌شود. همچنین برای منظور کردن قدرت مهاجم در استفاده از سکه‌های تصادفی فرض می‌شود که مهاجم تصادفی است. بنابراین مهاجم کارا را می‌توان، در یک نگاه ساده، الگوریتم‌های تصادفی چندجمله‌ای[۳] در نظر گرفت. دقت کنید مهاجم PPT یک الگوریتم ثابت برای حمله به همه‌ی اعضای خانواده سیستم رمز دارد. اگر بخواهیم به مهاجم قدرت بیشتری در انتخاب الگوریتم خود برای حمله به سیستم بدهیم می‌توان مهاجم را به صورت دنباله‌ای از مهاجم‌ها در نظر گرفت که برای حمله به سیستم رمز با پارامتر امنیّتی n از nامین الگوریتم خود استفاده می‌کند. چنین مهاجم‌هایی غیر یکنواخت[۴] نامیده می‌شوند. لذا قوی‌ترین مدلی که برای حمله‌کننده کارا در رمزنگاری تصور می‌شود مهاجم چندجمله‌ای احتمالاتی غیریکنواخت[۵] است که به صورت $\mathcal{A}(1^n,\cdot)$ نشان داده می‌شود که علامت نقطه بیانگر ورودی‌های دیگر الگوریتم است.

مزیت. در رویکرد واقعی احتمال موفقیت (مزیت) مهاجم یک عدد ثابت است که استراتژی حمله‌کننده آنرا تعیین می‌کنند. در رویکرد مجانبی مزیت مهاجم تابعی از پارامتر امنیّتی، n، است که باز هم استراتژی حمله‌کننده آنرا تعیین می‌کنند. منظور از یک تابع ناچیز تابعی است که از معکوس هر چندجمله‌ای، برای nهای به اندازه کافی بزرگ، کوچکتر باشد.

شکستن سیستم. مفهوم دقیق شکستن در رویکرد واقعی توسط یک آزمایش تعریف می‌شود. در رویکرد مجانبی خانواده‌ای از آزمایش‌ها مطرح است که توسط پارامتر امنیّتی شاخص می‌شوند.

انتخاب پارامتر امنیّتی. در عمل برای استفاده از سیستم باید از سیستم به ازای یک پارامتر امنیّتی ثابت استفاده کرد. رویکرد مجانبی، امنیت سیستم را در صورتی که پارامتر امنیّتی به اندازه کافی بزرگ انتخاب شده‌باشد، تضمین می‌کند. پارامتر امنیّتی n لزوماً نشان‌دهنده‌ی سطح امنیت 2^n بیتی نیست.

---

[۱] Concrete analysis
[۲] Asymptotical analysis
[۳] Probablilistic Polynomial Time (PPT)
[۴] non-uniform
[۵] Non-uniform probablilistic polynomial time (nuPPT)

۳ تحلیل مجانبی

۱.۳ تابع ناچیز

تعریف ۳ (تابع ناچیز) *تابع نامنفی $\varepsilon : \mathbb{N} \to \mathbb{R}$ را ناچیز می‌گویند هرگاه به ازای هر $c > ۰$، یک $n_۰ \in \mathbb{N}$ وجود داشته باشد که برای $n > n_۰$ داشته باشیم $\varepsilon(n) < \frac{۱}{n^c}$.*

مثال ۴ *توابع $\frac{۱}{۲^n}$، $\frac{۱}{۲^{\sqrt{n}}}$ و $\frac{۱}{n^{\log n}}$ ناچیز هستند. توابع $\frac{۱}{n}$، $\frac{۱}{n^۲}$، $\frac{۱}{\sqrt{n}}$ و $\frac{۱}{n^{۱۰۰}}$ غیرناچیز (قابل‌توجه) هستند.*

قضیه ۱ *اگر $p(\cdot)$ یک چندجمله‌ای باشد و $\varepsilon_۱, \cdots, \varepsilon_{p(n)}$ توابع ناچیز باشند، آنگاه $\sum_{i=۱}^{p(n)} \varepsilon_i(n)$ ناچیز است.*

۲.۳ خانواده سیستم‌های رمز متقارن

تعریف ۵ (سیستم رمز متقارن) *سه‌تایی $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ از الگوریتم‌های چندجمله‌ای احتمالاتی (PPT) را یک خانواده از سیستم‌های رمز متقارن (به طور خلاصه یک سیستم رمز متقارن) روی فضای پیام $\mathcal{M}$ می‌نامیم هرگاه:*

- $k \leftarrow \mathsf{Gen}(۱^n)$
- $\forall k \in \mathcal{K}, \forall m \in \mathcal{M} \quad c \leftarrow \mathsf{Enc}_k(m)$
- $\forall k \in \mathcal{K}, \forall c \in \mathcal{C} \quad m \leftarrow \mathsf{Dec}_k(c)$

و شرط نهایی زیر را برای هر پیام $m \in \mathcal{M}$ داشته باشد:

$$\Pr\{k \leftarrow \mathsf{Gen}(۱^n) : \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m\} = ۱$$

۳.۳ امنیّت تک‌پیامی

آزمایش $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$ را به صورت زیر در نظر بگیرید.

- $k \leftarrow \mathsf{Gen}(۱^n)$
- $(m_۰, m_۱) \leftarrow \mathcal{A}(۱^n)$ که $m_۰, m_۱ \in \mathcal{M}$ و $|m_۰| = |m_۱|$
- $b \leftarrow \{۰, ۱\}$
- $c \leftarrow \mathsf{Enc}_k(m_b)$
- $\hat{b} \in \{۰, ۱\} \quad \hat{b} \leftarrow \mathcal{A}(c)$

در صورتی که b و $\hat{b}$ برابر باشند، خروجی آزمایش که با متغیر تصادفی $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$ نشان داده می‌شود برابر یک و در غیر این صورت صفر تعریف می‌شود.

تعریف ۶ (امنیّت تک‌پیامی) *می‌گوئیم سیستم Π دارای امنیّت تک‌پیامی است اگر برای هر مهاجمِ چندجمله‌ایِ احتمالاتیِ غیریکنواختِ $\mathcal{A}$، تابع ناچیز $\varepsilon(\cdot)$ وجود داشته باشد که:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = ۱\} \leq \frac{۱}{۲} + \varepsilon(n)$$

۴.۳ امنیّت چندپیامی

آزمایش $\mathsf{PrivK}^{\mathrm{mult}}_{A,\Pi}(n)$ را به صورت زیر در نظر بگیرید.

- $k \leftarrow \mathsf{Gen}(1^n)$
- $(m_0^1, \cdots, m_0^{p(n)}, m_1^1, \cdots, m_1^{p(n)}) \leftarrow \mathcal{A}(1^n)$
- $b \leftarrow \{0, 1\}$
- $i = 1, \cdots, p(n)$ برای $c_i \leftarrow \mathsf{Enc}_k(m_b^i)$
- $\hat{b} \leftarrow \mathcal{A}(c_1, \cdots, c_{p(n)})$

در صورتی که b و $\hat{b}$ برابر باشند، خروجی آزمایش که با متغیر تصادفی $\mathsf{PrivK}^{\mathrm{mult}}_{A,\Pi}(n)$ نشان داده می‌شود برابر یک و در غیر این صورت صفر تعریف می‌شود.

تعریف ۷ (امنیّت چندپیامی) *می‌گوئیم سیستم Π دارای امنیّت چندپیامی است اگر برای هر مهاجمِ چندجمله‌ایِ احتمالاتیِ غیریکنواختِ $\mathcal{A}$، تابع ناچیز $\varepsilon(\cdot)$ وجود داشته باشد که:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{mult}}_{\mathcal{A},\Pi}(n) = 1\} \leq \frac{1}{2} + \varepsilon(n)$$

۴ تمایزناپذیری محاسباتی مجانبی و مولد شبه‌تصادفی

تعریف ۸ (خانواده توزیع‌ها) *یک دنباله از توزیع‌های احتمال $X_1, X_2, \cdots$ را یک خانواده از توزیع‌ها گویند و با $\{X_n\}_{n\in\mathbb{N}}$ یا به اختصار $\{X_n\}$ نمایش می‌دهند.*

تعریف ۹ (تمایزناپذیری محاسباتی) *دو خانواده‌ی $X = \{X_n\}_{n\in\mathbb{N}}$ و $Y = \{Y_n\}_{n\in\mathbb{N}}$ را تمایزناپذیر محاسباتی می‌نامیم و می‌نویسیم $X \simeq Y$، اگر برای هر تمایزگر nuPPT مانند $\mathcal{D}$ یک تابع ناچیز مانند $\varepsilon(\cdot)$ وجود داشته باشد که:*

$$|\Pr\{\mathcal{D}(1^n, X_n) = 1\} - \Pr\{\mathcal{D}(1^n, Y_n) = 1\}| \leq \varepsilon(n)$$

تعریف ۱۰ (توزیع شبه‌تصادفی) *خانواده‌ی توزیع‌های $\{X_n\}$ که در آن X_n یک توزیع بر روی $\{0,1\}^{l(n)}$ به ازای یک چندجمله‌ای $l(\cdot)$ است شبه‌تصادفی نامیده می‌شود هرگاه $\{X_n\} \simeq \{U_{l(n)}\}$.*

تعریف ۱۱ (مولّد شبه‌تصادفی) *فرض کنید $l(\cdot)$ یک چندجمله‌ای و $G : \{0,1\}^* \to \{0,1\}^*$ یک الگوریتم قطعی باشد که هر ورودی n-بیتی s را به یک رشته $l(n)$-بیتی $G(s)$ تبدیل می‌کند. الگوریتم G یک مولّد شبه‌تصادفی است اگر*

- **(کارایی)** *الگوریتم G چندجمله‌ای باشد*
- **(گسترش)** $l(n) > n$
- **(شبه‌تصادفی)** $\{G(U_n)\} \simeq \{U_{l(n)}\}$.

مثال ۱۲ *فرض کنید مولّد شبه‌تصادفی $G(\cdot)$ با چندجمله‌ای گسترش $l(\cdot)$ در اختیار داریم. سیستم رمز متقارن Π روی فضای پیام $\mathcal{M} = \{0,1\}^{l(n)}$ را به صورت زیر در نظر بگیرید:*

- $k \leftarrow \mathsf{Gen}(1^n)$

- $\mathsf{Enc}_k(m) = m \oplus G(k)$
- $\mathsf{Dec}_k(c) = c \oplus G(k)$

سیستم فوق دارای امنیّت تک‌پیامی است امّا امنیّت چندپیامی ندارد. برای حمله به سیستم فوق، حمله‌کننده متنِ رمزیِ یکی از دو دسته پیام زیر را درخواست و (c_1, c_2) را دریافت می‌کند:

$$(m_0^1, m_0^2) = (0^{l(n)}, 0^{l(n)}) \quad (m_1^1, m_1^2) = (0^{l(n)}, 1^{l(n)})$$

حمله‌کننده در صورتی که c_1 و c_2 باهم برابر باشند، $\hat{b} = 0$ و در غیر این صورت $\hat{b} = 1$ قرار می‌دهد. حمله‌کننده‌ی توصیف‌شده، دارای مزیّت غیرناچیز و قابل توجّه است چرا که احتمال موفقیّت وی یک می‌باشد. لذا سیستم Π دارای امنیّت چندپیامی نیست.