به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۱ اسفند ۱۳۹۱

جلسه‌ی ۵: قضیه‌ی شانون و امنیت محاسباتی

مدرس: دکتر شهرام خزائی *نگارنده: سید مرتضی موسوی*

۱ امنیت کامل

تعریف ۱ *یک رمز دارای امنیت کامل است اگر برای هر زوج پیام $m_0, m_1 \in \mathcal{M}$ و هر $c \in \mathcal{C}$ داشته باشیم:*

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} = \Pr\{\mathbf{C} = c | \mathbf{M} = m_1\}$$

به عبارت دیگر اگر $\mathbf{K}$ متغییر تصادفی خروجی الگوریتم $\mathsf{Gen}()$ باشد و $\mathbf{C}_0$ و $\mathbf{C}_1$ بیانگر متغییرهای تصادفی $\mathsf{Enc}_{\mathbf{K}}(m_0)$ و $\mathsf{Enc}_{\mathbf{K}}(m_1)$ باشند، در این صورت $\mathbf{C}_0 \equiv \mathbf{C}_1$ (یعنی، $\mathbf{C}_0$ و $\mathbf{C}_1$ دارای توزیع یکسان هستند).

می‌توان امنیت کامل را با آزمایش زیر که با $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ نمایش داده می‌شود تعریف کرد. آزمایش، میزان موفقیت یک مهاجم $\mathcal{A}$ در حمله به یک سیستم رمز Π را مدل می‌کند و و مراحل انجام آن به ترتیب زیر است:

۱. $k \leftarrow \mathsf{Gen}()$

۲. $m_0, m_1 \leftarrow \mathcal{A}()$ که $m_0, m_1 \in \mathcal{M}$

۳. $b \leftarrow \{0, 1\}$

۴. $c \leftarrow \mathsf{Enc}_k(m_b)$

۵. $\hat{b} \leftarrow \mathcal{A}(c)$

در صورتی که حدس مهاجم صحیح باشد، یعنی $\hat{b} = b$، خروجی آزمایش که با $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ نشان داده می‌شود برابر یک خواهد شد و در غیر این صورت صفر. دقت کنید که خروجی آزمایش یک متغیر تصادفی است که به سکه‌های تصادفی که احیاناً در الگوریتم تولید کلید، الگوریتم رمزگذاری و الگوریتم مهاجم مورد استفاده قرار می‌گیرند، بستگی دارد. با استفاده از این آزمایش می‌توان تعریف معادل زیر را برای امنیت کامل ارائه کرد.

لم ۱ *یک سیستم رمز Π دارای امنیت کامل است اگر وفقط اگر برای هر مهاجم $\mathcal{A}$ که در آزمایش فوق شرکت می‌کند، داشته باشیم:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\} \leq \frac{1}{2}$$

۲ اثبات قضیه‌ی شانون

قضیه ۲ *فرض کنید $|\mathcal{K}|$ تعداد اعضای فضای کلید و $|\mathcal{M}|$ تعداد اعضای فضای متن باشد. برای امنیت کامل لازم است $|\mathcal{K}| \geq |\mathcal{M}|$.*

برهان. برهان خلف : فرض می‌کنیم $|\mathcal{K}| < |\mathcal{M}|$ باشد. برای یک $m_1 \in \mathcal{M}$ و $k \in \mathcal{K}$ دلخواه، متن رمزی c را طوری در نظر بگیرید که $c = \mathsf{Enc}_k(m_1)$. به وضوح داریم:

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_1\} \quad > \quad 0$$

مجموعه‌ی $\mathcal{S}$ را به صورت زیر تعریف می کنیم:

$$\mathcal{S} = \{m | \exists k \in \mathcal{K} : m = \mathsf{Dec}_k(c)\}$$

به وضوح داریم:

$$|\mathcal{S}| \leq |\mathcal{K}|$$

با استفاده از فرض خلف می‌دانیم $|\mathcal{K}| < |\mathcal{M}|$ پس خواهیم داشت $|\mathcal{S}| < |\mathcal{M}|$ و در نتیجه:

$$\exists m_0 \notin \mathcal{S}, m_0 \in \mathcal{M}$$
$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} = 0$$

پس اگر تعداد اعضای فضای کلید کمتر از تعداد اعضای فضای متن باشند، امنیت کامل نداریم. ■

۳ سیستم‌های عملی و امنیت محاسباتی

در عمل برای سیستم‌های رمزنگاری، مخفی نگه داشتن طول پیام از حمله‌کننده مقرون به صرفه نیست. بدین منظور فرض می‌کنیم که در سیستم‌های رمز عملی پیام‌های با طول یکسان به متن‌های رمزی با طول یکسان رمز می‌شوند و مرحله دوم آزمایش شنود تک پیامی را به صورت زیر تغییر می‌دهیم:

۲ $m_0, m_1 \leftarrow \mathcal{A}()$ که $m_1, m_0 \in \mathcal{M}$ و $|m_0| = |m_1|$

همچنین در سیستم‌های عملی هدف غیرعملی امنیت کامل را کنار گذاشته و خود را محدود به امنیت محاسباتی می‌کنیم که با توجه به فرض‌های زیر مدل می‌شود:

۱. مهاجم دارای توان محاسباتی محدود می‌باشد.

۲. مهاجم می‌تواند با احتمال ناچیز موفق شود.

تعریف ۲ *می‌گوییم $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$، (t, ε)-امن است اگر برای هر مهاجم $\mathcal{A}$ که در زمان t اجرا می‌شود داشته باشیم:*

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

مقدار ε نشان دهنده مزیت مهاجم نسبت به مهاجمی است که کاملاً تصادفی مقدار $\hat{b}$ را تولید می‌کند. در عمل اگر برای همه مقادیر t و ε که $t/\varepsilon \geq ۲^{۸۰}$، سیستم رمز (t, ε)-امن باشد، سطح مناسبی از امنیت داریم. در این صورت حمله‌کننده‌هایی که به ترتیب در زمان‌های $t = ۱$، $t = ۲^{۴۰}$ و $t = ۲^{۸۰}$ اجرا می‌شوند دارای حداکثر مزیت $\varepsilon = ۲^{-۸۰}$، $\varepsilon = ۲^{-۴۰}$ و $\varepsilon = ۱$ می‌باشند. یک سیستم رمز که طول کلید آن ۸۰ بیت است بالقوه می‌تواند چنین سطحی از امنیت برآورده کند. مهاجمی را در نظر بگیرید که دو پیام دلخواه متفاوت $m_۰$ و $m_۱$ خروجی می‌دهد. سپس مهاجم با دریافت متن رمزی چالش c که رمزشده $m_۰$ یا $m_۱$ است، به صورت زیر تصمیم می‌گیرد:

- مهاجم t کلید ۸۰ بیتی $k_۱, \cdots, k_t$ را به تصادف انتخاب می‌کند.
- به‌ازای هر کلید k_i، مهاجم متن رمزی چالش c را رمز گشایی می‌کند.
- اگر برای یکی از کلیدها $\mathsf{Dec}_{k_i}(c) = m_b$ باشد، مهاجم مقدار $\hat{b} = b$ را برمی‌گرداند.
- در غیر اینصورت مهاجم بیت تصادفی $\hat{b} \leftarrow \{۰, ۱\}$ را برمی‌گرداند.

فرض کنیم سیستم رمز و پیام‌های $m_۰$ و $m_۱$ و متن رمزی c به‌گونه‌ای هستند که هیچ کلید اشتباهی (هر کلیدی غیر از کلید انتخابی چالشگر) متن رمزی c را به $m_۰$ یا $m_۱$ رمزگشایی نکند. اگر طول پیام‌های $m_۰$ و $m_۱$ به اندازه کافی طولانی انتخاب شوند (مثلاً ۱۰۰ بیت)، چنین فرضی با احتمال خیلی زیاد صحیح است. پیشامد اینکه کلید انتخاب شده توسط چالشگر در بین t کلید انتخاب شده توسط مهاجم باشد را با E نشان دهید. در اینصورت مزیت مهاجم که در زمان t اجرا می‌شود برابر است با $\varepsilon = \frac{t}{۲^{۸۰}}$، زیرا:

$$\begin{aligned}
\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱\} &= \Pr\{\hat{b} = b\} \\
&= \Pr\{\hat{b} = b \mid E\} \times \Pr\{E\} + \Pr\{\hat{b} = b \mid \overline{E}\} \times \Pr\{\overline{E}\} \\
&= ۱ \times \tfrac{t}{۲^{۸۰}} + \tfrac{۱}{۲} \times (۱ - \tfrac{t}{۲^{۸۰}}) \\
&= \tfrac{۱}{۲}(۱ + \tfrac{t}{۲^{۸۰}})
\end{aligned}$$

بنابراین $t/\varepsilon = ۲^{۸۰}$.

۴ گسترش کلید

در رمزنگاری به روش رمز یکبار مصرف نیاز داریم طول کلید به اندازه‌ی طول متن اصلی باشد. اگر طول کلید کوتاه باشد لازم داریم طول کلید به اندازه‌ی متن اصلی گسترش یابد.
به عنوان مثال، سیستم رمز $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ روی فضای $\mathcal{M} = \{۰, ۱\}^{۲n}$ را در نظر بگیرید که در آن:

- $\mathsf{Gen}()$ یک رشته‌ی تصادفی k به طول n تولید می‌کند.
- $\mathsf{Enc}()$: الگوریتم رمزگذاری، پیام $m = m_۰||m_۱ \in \{۰, ۱\}^{۲n}$ و کلید $k \in \{۰, ۱\}^n$ را به متن رمزی $c = (m_۰ \oplus k)||(m_۱ \oplus k)$ تبدیل می کند که در آن $|m_۰| = |m_۱|$ است.
- $\mathsf{Dec}()$: الگوریتم رمزگشایی، متن رمزی $c = c_۰||c_۱ \in \{۰, ۱\}^{۲n}$ و کلید $k \in \{۰, ۱\}^n$ را به پیام $m = (c_۰ \oplus k)||(c_۱ \oplus k)$ تبدیل می کند که در آن $|c_۰| = |c_۱|$ است.

اما این روش بسیار ساده شکسته می‌شود. به طور مثال مهاجم $\mathcal{A}$ دو متن $m_0 = 0^{2n}$ و $m_1 = 1^n 0^n$ را به عنوان متن‌های آزمون می‌دهد. سپس دو نیمه‌ی متن رمز شده را با یک دیگر xor می‌کند. در صورتی که حاصل 0^n شد، نتیجه‌گیری می‌کند که متن اول رمز شده است (یعنی در مرحله ۵ آزمایش $\hat{b} = 1$ را به خروجی می‌دهد) و در صورتی که حاصل 1^n باشد، نتیجه‌گیری می‌کند که متن دوم رمز شده است (یعنی در مرحله ۵ آزمایش $\hat{b} = 0$ را به خروجی می‌دهد). این مهاجم دارای مزیت $\varepsilon = \frac{1}{2}$ است زیرا داریم:

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\} = 1$$

در جلسات بعد روش‌های مناسب‌تری برای گسترش کلید معرفی خواهد شد.