مقدّمه‌ای بر رمزنگاری ـ کوئیز امتیازی

امیرحسین افشارراد

۱۵ اردیبهشت ۱۳۹۹

۱ تعاریف امنیت

تعریف ۱. آزمایش $\mathrm{CPA}(\mathcal{A}, \Pi, n, b)$ را برای مهاجم $\mathcal{A}$ و سیستم رمز متقارن Π به صورت زیر تعریف می‌کنیم:

1. $k \leftarrow \mathrm{Gen}(1^n)$
2. $(m_0, m_1) \leftarrow \mathcal{A}^{\mathrm{Enc}_k(.)}(1^n) \quad \text{with } |m_0| = |m_1|$
3. $c \leftarrow \mathrm{Enc}_k(m_b)$
4. $\hat{b} \leftarrow \mathcal{A}^{\mathrm{Enc}_k(.)}(1^n)$

خروجی این آزمایش، بیت $\hat{b}$ خواهد بود.

تعریف ۲. سیستم رمز متقارن Π را دارای امنیت متن اصلی انتخابی (یا CPA–امن) گوییم، هرگاه برای هر مهاجم چندجمله‌ای تصادفی غیریکنواخت $\mathcal{A}$، دو توزیع زیر تمایزناپذیر محاسباتی باشند:

$$\mathrm{CPA}(\mathcal{A}, \Pi, n, 0) \overset{c}{\simeq} \mathrm{CPA}(\mathcal{A}, \Pi, n, 1) \tag{۱}$$

یا به طور معادل، داشته باشیم:

$$\Big| \mathbb{P}[\mathrm{CPA}(\mathcal{A}, \Pi, n, 0) = 1] - \mathbb{P}[\mathrm{CPA}(\mathcal{A}, \Pi, n, 1) = 1] \Big| \leq \epsilon(n) \tag{۲}$$

که $\epsilon(n)$ تابعی ناچیز از n است.

تعریف ۳. آزمایش امنیت چپ–راست، $\mathrm{LR}(\mathcal{A}, \Pi, n, b)$ را برای مهاجم $\mathcal{A}$ و سیستم رمز متقارن Π به صورت زیر تعریف می‌کنیم:

1. $k \leftarrow \mathrm{Gen}(1^n)$
2. $\hat{b} \leftarrow \mathcal{A}^{\mathcal{O}(k,b,.,.)}(1^n)$

خروجی این آزمایش، بیت $\hat{b}$ خواهد بود. همچنین $\mathcal{O}(k, b, ., .)$ در تعریف فوق نیز به صورت زیر تعریف می‌شود:

$$\mathcal{O}(k, b, m_0, m_1) := \begin{cases} \mathrm{Enc}_k(m_b) & |m_0| = |m_1| \\ \perp & \text{otherwise} \end{cases} \tag{۳}$$

تعریف ۴. سیستم رمز متقارن Π را دارای امنیت چپ–راست[1] گوییم، هرگاه برای هر مهاجم چندجمله‌ای تصادفی غیریکنواخت $\mathcal{A}$، دو توزیع زیر تمایزناپذیر محاسباتی باشند:

$$\mathrm{LR}(\mathcal{A}, \Pi, n, 0) \overset{c}{\simeq} \mathrm{LR}(\mathcal{A}, \Pi, n, 1) \tag{۴}$$

یا به طور معادل، داشته باشیم:

$$\Big| \mathbb{P}[\mathrm{LR}(\mathcal{A}, \Pi, n, 0) = 1] - \mathbb{P}[\mathrm{LR}(\mathcal{A}, \Pi, n, 1) = 1] \Big| \leq \epsilon(n) \tag{۵}$$

که $\epsilon(n)$ تابعی ناچیز از n است.

[1] LR–secure

۲ سؤال اوّل

مسأله. با استفاده از برهان خلف، نشان دهید امنیت CPA امنیت LR را نتیجه می‌دهد. برای این منظور با استفاده از یک مهاجم مثل $\mathcal{A}$ برای آزمایش امنیت LR، مهاجمی مانند $\mathcal{B}$ برای آزمایش امنیت CPA بسازید و مزیت آن را محاسبه کنید. فرض کنید $\mathcal{A}$ تعداد $q(n)$ پرسمان از اوراکل خود انجام می‌دهد که $q(n)$ تابعی چندجمله‌ای از n است.

حل. برای اثبات آن که امنیت CPA امنیت LR را نتیجه می‌دهد؛ فرض می‌کنیم مهاجم $\mathcal{A}$ برای آزمایش امنیت LR با مزیت غیرناچیز موجود باشد. همچنین بدون از دست دادن کلیت مسأله فرض می‌کنیم مهاجم $\mathcal{A}$ همواره زوج پیام‌های با طول برابر به اوراکل $\mathcal{O}$ ارسال می‌کند؛ چون در غیر این صورت $\perp$ دریافت می‌کند که کمکی به او نمی‌کند. در این صورت مهاجم $\mathcal{B}$ برای آزمایش امنیت CPA را به صورت زیر می‌سازیم:

ابتدا عدد i را با توزیع یکنواخت از مجموعه‌ی $\{1, 2, \dots, q\}$ انتخاب می‌کنیم که q تعداد پرسمان‌های مهاجم $\mathcal{A}$ بوده و تابعی چندجمله‌ای از n است. در ادامه $\mathcal{B}$ مهاجم $\mathcal{A}$ را اجرا می‌کند و در نقش چالش‌گر آن عمل می‌کند و q پرسمان آن را پاسخ می‌دهد. اگر پرسمان jام مهاجم $\mathcal{A}$ به صورت زوج پیام (m_0^j, m_1^j) باشد، $\mathcal{B}$ برای پاسخ به این پرسمان به صورت زیر عمل می‌کند:

- اگر $j < i$ باشد، $\mathcal{B}$ مقدار $c_j = \mathrm{Enc}_k(m_0^j)$ را (با مراجعه به اوراکل خود) به عنوان خروجی برمی‌گرداند.
- اگر $j = i$ باشد، $\mathcal{B}$ زوج (m_0^j, m_1^j) را به عنوان ورودی خود به چالشگر آزمایش امنیت CPA می‌دهد و خروجی آن، c_j را به عنوان خروجی به $\mathcal{A}$ می‌دهد.
- اگر $j > i$ باشد، $\mathcal{B}$ مقدار $c_j = \mathrm{Enc}_k(m_1^j)$ را (با مراجعه به اوراکل خود) به عنوان خروجی برمی‌گرداند.

نهایتاً $\mathcal{B}$ بیت $\hat{b}$ را به عنوان خروجی از $\mathcal{A}$ دریافت می‌کند و همان را به عنوان خروجی آزمایش امنیت CPA ارائه می‌کند.

در ادامه نشان می‌دهیم $\mathcal{B}$ با عملکرد توصیف‌شده از مزیت غیرناچیزی در آزمایش امنیت CPA برخوردار است. برای این امر، ابتدا نمادگذاری $\mathrm{LR}_\ell(\mathcal{A}, \Pi, n)$ را خروجی آزمایش امنیت LR برای مهاجم $\mathcal{A}$ تعریف می‌کنیم، هرگاه این آزمایش به گونه‌ای تغییر یابد که اوراکل $\mathcal{O}$ برای ℓ پرسمان اوّل پیام با اندیس صفر، و برای $q - \ell$ پرسمان بعدی، پیام با اندیس یک را رمز کند. در این صورت به وضوح طبق تعریف داریم:

$$\begin{cases} \mathrm{LR}_q(\mathcal{A}, \Pi, n) = \mathrm{LR}(\mathcal{A}, \Pi, n, 0) \\ \mathrm{LR}_0(\mathcal{A}, \Pi, n) = \mathrm{LR}(\mathcal{A}, \Pi, n, 1) \end{cases} \tag{۶}$$

حال با توجّه به توضیحاتی که در مورد عملکرد $\mathcal{B}$ داده شد، چنان‌چه $\mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0)]$ را بر حسب مقدار i شرطی کنیم، خواهیم داشت:

$$\begin{aligned} \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0) = 1] &= \sum_{\ell=1}^{q} \mathbb{P}[i = \ell]\, \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0) = 1 | i = \ell] \\ &= \sum_{\ell=1}^{q} \frac{1}{q}\, \mathbb{P}[\mathrm{LR}_\ell(\mathcal{A}, \Pi, n) = 1] \end{aligned} \tag{۷}$$

همچنین با شرطی‌سازی احتمال $\mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1)]$ بر حسب مقدار i نیز خواهیم داشت:

$$\begin{aligned} \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1) = 1] &= \sum_{\ell=1}^{q} \mathbb{P}[i = \ell]\, \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1) = 1 | i = \ell] \\ &= \sum_{\ell=1}^{q} \frac{1}{q}\, \mathbb{P}[\mathrm{LR}_{\ell-1}(\mathcal{A}, \Pi, n) = 1] \\ &= \sum_{\ell=0}^{q-1} \frac{1}{q}\, \mathbb{P}[\mathrm{LR}_\ell(\mathcal{A}, \Pi, n) = 1] \end{aligned} \tag{۸}$$

حال با توجّه به فرض خلف مبنی بر غیرناچیز بودن مزیت مهاجم $\mathcal{A}$ در آزمایش امنیت LR، خواهیم داشت:

$$\mu_{\mathcal{A}}^{\mathrm{LR}}(n) = |\,\mathbb{P}[\mathrm{LR}(\mathcal{A}, \Pi, n, 0) = 1] - \mathbb{P}[\mathrm{LR}(\mathcal{A}, \Pi, n, 1) = 1]| \tag{۹}$$

که در آن، $\mu_{\mathcal{A}}^{\mathrm{LR}}(n)$ تابعی غیرناچیز بر حسب n است. حال با جایگزین کردن تساوی‌های عبارت ۶ در نامساوی ۹ خواهیم داشت:

$$|\,\mathbb{P}[\mathrm{LR}_q(\mathcal{A}, \Pi, n) = 1] - \mathbb{P}[\mathrm{LR}_0(\mathcal{A}, \Pi, n) = 1]| = \mu_{\mathcal{A}}^{\mathrm{LR}}(n) \tag{۱۰}$$

از طرفی اگر قدر مطلق تفاضل طرفین دو تساوی ۷ و ۸ را محاسبه کنیم، خواهیم داشت:

$$\begin{aligned}
&|\,\mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0) = 1] - \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1) = 1]| \\
&= \left|\sum_{l=1}^{q} \frac{1}{q}\,\mathbb{P}[\mathrm{LR}_\ell(\mathcal{A}, \Pi, n) = 1] - \sum_{l=0}^{q-1} \frac{1}{q}\,\mathbb{P}[\mathrm{LR}_\ell(\mathcal{A}, \Pi, n) = 1]\right| \\
&= \frac{1}{q}\,|\mathbb{P}[\mathrm{LR}_q(\mathcal{A}, \Pi, n) = 1] - \mathbb{P}[\mathrm{LR}_0(\mathcal{A}, \Pi, n) = 1]| \\
&= \frac{\mu_{\mathcal{A}}^{\mathrm{LR}}(n)}{q(n)}
\end{aligned} \tag{۱۱}$$

که نامساوی آخر از رابطه‌ی ۱۰ نتیجه شده است. ضمناً حاصل تقسیم دو تابع غیرناچیز بر حسب n نیز تابعی غیرناچیز (مثل $\mu_{\mathcal{B}}^{\mathrm{CPA}}(n)$) خواهد بود، به این ترتیب از رابطه‌ی ۱۱ به نتیجه‌ی زیر می‌رسیم:

$$\mu_{\mathcal{B}}^{\mathrm{CPA}}(n) = |\,\mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0) = 1] - \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1) = 1]| = \frac{\mu_{\mathcal{A}}^{\mathrm{LR}}(n)}{q(n)} \tag{۱۲}$$

که معادله‌ی ۱۲، طبق تعریف به معنی آن است که مهاجم $\mathcal{B}$ می‌تواند با مزیت غیرناچیز در آزمایش امنیت CPA موفّق شود و این تناقض است؛ چرا که فرض کرده بودیم این سیستم رمز از امنیت CPA برخوردار است. به این ترتیب فرض خلف باطل است و با فرض وجود امنیت CPA، سیستم دارای امنیت LR نیز خواهد بود.

همچنین در معادلات ۱۱ و ۱۲ مزیت مهاجم $\mathcal{B}$ نیز محاسبه شده است و مقدار آن، $\frac{\mu_{\mathcal{A}}^{\mathrm{LR}}(n)}{q(n)}$ به دست آمده است که $\mu_{\mathcal{A}}^{\mathrm{LR}}(n)$ و $q(n)$ به ترتیب مزیت $\mathcal{A}$ در آزمایش امنیت LR و تعداد پرسمان‌های آن در این آزمایش می‌باشند.

۳ سؤال دوم

مسأله. نشان دهید در مسأله‌ی قبل، نیازی نیست مهاجم $\mathcal{A}$ *دقیقاً* $q(n)$ پرسمان مطرح کند. به عبارت دیگر، مسأله‌ی قبل را برای حالتی که تعداد پرسمان‌های $\mathcal{A}$ یک متغیّر تصادفی با کران بالای $q(n)$ باشد حل کنید.

حل. تا به این‌جا فرض بر این بود که تعداد پرسمان‌های مهاجم $\mathcal{A}$ دقیقاً برابر با $q(n)$ است. در این قسمت فرض می‌کنیم q یک کران بالا برای تعداد پرسمان‌ها باشد و تعداد پرسمان‌ها را با متغیّر تصادفی $\mathbf{R}$ نشان می‌دهیم که $0 \leq \mathbf{R} \leq q(n)$. از نحوه‌ی عملکرد مهاجم $\mathcal{B}$ دیدیم که متغیّر i به صورت تصادفی انتخاب می‌شود و پرسمان iام از مهاجم $\mathcal{A}$، یعنی (m_0^i, m_1^i) به عنوان ورودی به چالشگر آزمایش امنیت CPA داده می‌شود. در حالتی که تعداد پرسمان‌ها تصادفی است، اگر داشته باشیم $\mathbf{R} < i$، دستور مذکور به مشکل می‌خورد و امکان ارائه‌ی ورودی به چالشگر آزمایش امنیت CPA وجود نخواهد داشت. برای رفع این مشکل، عملکرد مهاجم $\mathcal{B}$ را به این صورت گسترش می‌دهیم که اگر $\mathbf{R} < i$ (یعنی تعداد پرسمان‌های $\mathcal{A}$ کم‌تر از i باشد)، بلافاصله پس از اتمام پرسمان‌های $\mathcal{A}$ زوج $(0^n, 0^n)$ به عنوان ورودی به چالشگر آزمایش امنیت CPA داده شود. در این حالت خروجی نهایی $\mathcal{B}$ در آزمایش امنیت CPA به صورت تصادفی انتخاب می‌شود.

نکته‌ی قابل توجّه آن است که در حالت $\mathbf{R} < i$، خواهیم داشت:

$$\mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 0) = 1 | \, \mathbf{R} < i] = \mathbb{P}[\mathrm{CPA}(\mathcal{B}, \Pi, n, 1) = 1 | \, \mathbf{R} < i] = \frac{1}{2} \qquad (۱۳)$$

زیرا طبق توضیحات فوق در مورد نحوه‌ی عملکرد مهاجم $\mathcal{B}$، در این حالت خروجی مهاجم مستقل از ورودی‌های مسأله و به صورت تصادفی انتخاب می‌شود.

در ادامه مزیت مهاجم $\mathcal{B}$ را در آزمایش امنیت CPA محاسبه خواهیم کرد. برای این منظور، ابتدا یک لم ساده را معرّفی و اثبات می‌کنیم:

لم. اگر مهاجم $\mathcal{A}$ بتواند دو توزیع X_0 و X_1 را مشروط بر پیشامدهای A و B با مزیت‌های μ_A و μ_B از هم تمایز دهد؛ چنان‌چه A و B افرازی از فضای احتمال تشکیل دهند، مزیت مهاجم $\mathcal{A}$ در تمایز توزیع‌های X_0 و X_1 از رابطه‌ی زیر به دست خواهد آمد:

$$\mu_{\mathcal{A}} = \mathbb{P}[A]\mu_A + \mathbb{P}[B]\mu_B \qquad (۱۴)$$

اثبات. مطابق با رابطه‌ی ۱۵، خروجی $\mathcal{A}(X_0, X_1)$ را برابر با یک تعریف کنیم، هرگاه $\mathcal{A}$ بتواند با دریافت نمونه‌ای که به تصادف از یکی از این دو متغیّر تصادفی تولید شده، متغیّر تصادفی مولّد آن نمونه را به درستی تشخیص دهد:

$$\mathbb{P}[b \leftarrow \{0,1\}; x \leftarrow X_b : \mathcal{A}(x) = b] = \mathbb{P}[\mathcal{A}(X_0, X_1) = 1] = \frac{1}{2}(1 + \mu_{\mathcal{A}}) \qquad (۱۵)$$

در این صورت با شرطی‌سازی فضای احتمال بر روی پیشامدهای A و B می‌توان نوشت:

$$\begin{aligned}
\mathbb{P}[\mathcal{A}(X_0, X_1) = 1] &= \mathbb{P}[A]\,\mathbb{P}[\mathcal{A}(X_0, X_1) = 1|A] + \mathbb{P}[B]\,\mathbb{P}[\mathcal{A}(X_0, X_1) = 1|B] \\
&= \frac{1}{2}(1 + \mu_A)\,\mathbb{P}[A] + \frac{1}{2}(1 + \mu_B)\,\mathbb{P}[B] \\
&= \frac{1}{2}(\mathbb{P}[A] + \mathbb{P}[B]) + \frac{1}{2}(\mathbb{P}[A]\mu_A + \mathbb{P}[B]\mu_B) \\
&= \frac{1}{2} + \frac{1}{2}(\mathbb{P}[A]\mu_A + \mathbb{P}[B]\mu_B) \\
&= \frac{1}{2}\,(1 + \mathbb{P}[A]\mu_A + \mathbb{P}[B]\mu_B) \\
\Rightarrow \mu_{\mathcal{A}} &= \mathbb{P}[A]\mu_A + \mathbb{P}[B]\mu_B
\end{aligned} \qquad (۱۶)$$

حال با استفاده از این لم، می‌توانیم مزیت مهاجم $\mathcal{B}$ را زمانی که تعداد پرسمان‌ها به صورت متغیّر تصادفی $\mathbf{R}$ داده شده نیز محاسبه کنیم. کافی است دو پیشامد موجود در لم فوق را به صورت $\mathbf{R} \geq i$ و $\mathbf{R} < i$ تعریف کنیم. به وضوح این دو

پیشامد فضای احتمال را افراز می‌کنند. حال کافی است مشروط بر وقوع هر یک از این دو پیشامد، مزیت $\mathcal{B}$ در آزمایش امنیت CPA را محاسبه کنیم. (واضح است که می‌توان آزمون امنیت را به صورت یک آزمون تمایز دو متغیّر تصادفی بیان کرد؛ لذا می‌توان به صورت مستقیم از نتیجه‌ی لم فوق بهره برد.)

در صورتی که $i \le \mathbf{R}$ باشد، شرایط آزمایش دقیقاً مشابه با قسمت‌های قبلی (مشخّص بودن تعداد پرسمان‌ها) است و همان اثبات‌ها دقیقاً معتبر خواهند بود؛ بنابراین مهاجم در این حالت دارای مزیت محاسبه‌شده در رابطه‌ی ۱۲ می‌باشد. از طرفی اگر $i > \mathbf{R}$ باشد، با توجّه به توضیحات فوق و رابطه‌ی ۱۳، خروجی اعلام‌شده توسّط مهاجم تصادفی است، و مزیت آن در آزمایش امنیت برابر با صفر خواهد بود. به این ترتیب با جایگذاری این حقایق در نتیجه‌ی لم فوق خواهیم داشت:

$$\begin{aligned} \mu_{\mathcal{B}}^{\mathrm{CPA}}(n) &= \mathbb{P}[i \le \mathbf{R}]\mu_{\mathcal{B},\, i\le\mathbf{R}}^{\mathrm{CPA}}(n) + \mathbb{P}[i > \mathbf{R}]\mu_{\mathcal{B},\, i>\mathbf{R}}^{\mathrm{CPA}}(n) \\ &= \mathbb{P}[i \le \mathbf{R}]\frac{\mu_{\mathcal{A}}^{\mathrm{LR}}(n)}{q(n)} \end{aligned} \tag{۱۷}$$

به این ترتیب مزیت $\mathcal{B}$ در آزمایش امنیت CPA برابر با مقدار $\mathbb{P}[i \le \mathbf{R}]\dfrac{\mu_{\mathcal{A}}^{\mathrm{LR}}(n)}{q(n)}$ می‌باشد که اگر $\mu_{\mathcal{A}}^{\mathrm{LR}}(n)$ (مزیت $\mathcal{A}$ در آزمایش امنیت CPA) تابعی غیرناچیز و $q(n)$ تابعی چندجمله‌ای بر حسب n باشند، مقدار مزیت مهاجم $\mathcal{B}$ نیز غیرناچیز خواهد بود.

همچنین چون $\mathbb{P}[i \le \mathbf{R}] \ge \dfrac{1}{q}$، می‌توان کران پایینی برای مزیت مهاجم $\mathcal{B}$ نیز به صورت زیر معرّفی نمود:

$$\mu_{\mathcal{B}}^{\mathrm{CPA}} \ge \frac{1}{q^2}\mu_{\mathcal{A}}^{\mathrm{LR}} \tag{۱۸}$$