دانشکده علوم ریاضی و آمار

مدرس: دکتر مجتبی رفیعی نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۱۹: طرح‌های رمزنگاری کلید عمومی

۱۵ خرداد ۱۴۰۱

فهرست مطالب

۱ فرضیات رمزنگاری

در آغاز این جلسه به کمک چند فرض ذیل که در جلسات گذشته بدان‌ها پرداخته شد، به طراحی چند سیستم رمز کلید عمومی می‌پردازیم:

۱. **فرض تجزیه:** اگر p و q دو عدد اول تصادفی n بیتی باشند، آن‌گاه محاسبه p یا q از روی حاصل‌ضرب $N = pq$ سخت است.

۲. **فرض RSA:** محاسبه x از روی N $x^e \mod N$ که N حاصلضرب دو عدد اول تصادفی n بیتی است و e به تصادف از $\mathbb{Z}^*_{\phi(N)}$ انتخاب می‌شود، سخت است.

۳. **فرض لگاریتم گسسته**[1]: در گروه G با مولد g محاسبه $\log_g h$ از روی عنصر تصادفی $h \in G$ سخت است.

[1] Discrete Logarithm Assumption

۴. **فرض دیفی-هلمن محاسباتی (CDH[2])**: در گروه G با مولد g و مرتبه q، وقتی x و y به تصادف از $\mathbb{Z}_q$ انتخاب شوند، محاسبه‌ی g^{xy} از روی g^x و g^y سخت است.

۵. **فرض دیفی-هلمن تصمیمی (DDH[3])**: در گروه G با مولد g و مرتبه q، دو توزیع (g^x, g^y, g^{xy}) و (g^x, g^y, g^r) وقتی که x, y, r به تصادف از $\mathbb{Z}_q$ تولید شود، تمایزناپذیرند.

فرضیات فوق به صورت غیر رسمی ارائه شده اند، اما همه آنها را می‌توان به صورت رسمی بیان کرد. به عنوان مثال برای رسمی کردن فرض تجزیه می‌توان آزمایش زیر را تعریف کرد:

تعریف ۱ *آزمایش تجزیه $\mathsf{Factor}_{\mathcal{A}}(n)$ به صورت زیر است:*

۱. *اعداد اول تصادفی n-بیتی p و q تولید می‌شوند و $N = pq$ محاسبه می‌شود.*

۲. $p' \leftarrow \mathcal{A}(N)$

خروجی این آزمایش، که با $\mathsf{Factor}_{\mathcal{A}}(n)$ نشان داده می‌شود برابر است با ۱، اگر $p' \in \{p, q\}$ و در غیر این صورت، خروجی آزمایش ۰ است.

تعریف ۲ *(فرض تجزیه) برای هر مهاجم چندجمله‌ای تصادفی $\mathcal{A}$، تابع ناچیز $\varepsilon(n)$ وجود دارد که:*

$$\Pr\{\mathsf{Factor}_{\mathcal{A}}(n) = 1\} \leq \varepsilon(n)$$

لم ۱ *اگر فرض RSA برقرار باشد، فرض تجزیه نیز برقرار است.*

نکته ۱ *ممکن است مسئله تجزیه سخت باشد ولی RSA آسان باشد؛ درواقع نمی‌دانیم که مسئله تجزیه و RSA معادل هم هستند یا نه.*

لم ۲ *اگر فرض DDH برقرار باشد، فرض CDH نیز برقرار است.*

برهان. اگر بتوانیم مسئله دیفی-هلمن محاسباتی را حل کنیم (یعنی از روی g^x و g^y بتوانیم g^{xy} را بدست آوریم)، یقینا می‌توانیم دو توزیع $(g,\, g^x,\, g^y,\, g^{xy})$ و $(g,\, g^x,\, g^y,\, g^r)$ را تمایز دهیم و در نتیجه می‌توانیم مسئله DDH را حل کنیم. ■

۲ سیستم رمز RSA

برای سادگی نمایش الگوریتم GenRSA را که ماژول‌های RSA را تولید می‌کند به صورت زیر تعریف می‌کنیم. **الگوریتم GenRSA**: با ورودی 1^n، ابتدا دو عدد اول n بیتی تصادفی p و q تولید و $N = pq$ را محاسبه می‌کند. سپس عدد تصادفی e را تولید می‌کند که $\gcd(e,\, \phi(N)) = 1$ باشد. در نهایت $d = e^{-1} \mod \phi(N)$ را محاسبه می‌کند. خروجی الگوریتم (N, e, d) است.

اولین ایده‌ای که برای ساخت سیستم رمز نامتقارن به ذهن می‌رسد به صورت زیر است که به سیستم رمز RSA ساده[4] معروف است:

۱. $(pk,\, sk) \leftarrow \mathsf{Gen}(1^n)$
الگوریتم تولید کلید Gen با ورودی 1^n، ابتدا $(N,\, e,\, d) \leftarrow \mathsf{GenRSA}(1^n)$ را اجرا می‌کند و سپس کلیدهای عمومی و خصوصی را به صورت $pk = (N,\, e)$ و $sk = (N,\, d)$ محاسبه می‌کند.

۲. $c \leftarrow \mathsf{Enc}_{pk}(m)$
الگوریتم رمزنگاری تحت کلید عمومی $pk = (N, e)$ پیام $m \in \mathbb{Z}_N^*$ را به متن رمزی $c = m^e \mod N$ می‌نگارد.

۳. $m \leftarrow \mathsf{Dec}_{sk}(c)$
الگوریتم رمزگشایی تحت کلید خصوصی $sk = (N, d)$ متن رمزی $c \in \mathbb{Z}_N^*$ را به پیام $m = c^d \mod N$ می‌نگارد.

گفتیم این سیستم رمز امنیت CPA ندارد، چون الگوریتم رمزنگاری تصادفی نیست.

[2] Computational Diffie-Hellman Assumption
[3] Decisional Diffie-Hellman Assumption
[4] Plain RSA

۱.۲ سیستم رمز RSA با تابع درهم‌سازی

یک روش برای ساخت طرح رمزنگاری نامتقارن، به‌کارگیری فرض RSA، استفاده از تابع درهم‌سازی[5] و سیستم رمز متقارن است. در ادامه به شرح چنین سیستمی می‌پردازیم که با پیش‌فرض درستی فرض RSA دارای امنیت CCA است.
فرض کنید $\Pi = (\mathsf{G}, \mathsf{E}, \mathsf{D})$ یک سیستم رمز متقارن با فضای کلید یکنواخت $\mathcal{K}$ و $H_N : \mathbb{Z}_N^* \to \mathcal{K}$ خانواده‌ای از توابع درهم‌سازی باشد.
همانند قبل مولد $\mathsf{GenRSA}(1^n)$ ماژول‌های RSA را تولید می‌کند.

۱. $(N,\, e,\, d) \leftarrow \mathsf{GenRSA}(1^n)$
$pk = (N,\, e)$
$sk = (N,\, d)$

۲. $\langle y, \mathsf{E}_k(m)\rangle \leftarrow \mathsf{Enc}_{pk}(m)$ که y و k به صورت زیر محاسبه می‌شوند:
$r \leftarrow \mathbb{Z}_N^*$ (r به تصادف از $\mathbb{Z}_N^*$ انتخاب می‌شود.)
$k = H_N(r)$
$y = r^e \mod N$

۳. $\mathsf{D}_k(c_2) \leftarrow \mathsf{Dec}_{sk}\langle c_1,\, c_2\rangle$ که k به صورت زیر محاسبه می‌شود:
$r = c_1^d \mod N$
$k = H_N(r)$

این استانداردی است به نام ISO که در عمل خیلی از آن استفاده نمی‌شود.می‌توان ثابت کرد که اگر سیستم رمز متقارن استفاده شده دارای امنیت اصالت‌سنجی[6] بوده و تابع درهم‌سازی نیز اوراکل تصادفی باشد، سیستم رمز عمومی تولیدشده دارای امنیت CCA خواهد بود. در این‌جا فرض بر ایده‌آل بودن تابع درهم‌سازی است که مصداقی ندارد؛ درنتیجه برای حل این مشکل از توابع درهم‌سازی معروف استفاده می‌شود که نمی‌توان امنیتش را اثبات کرد، اما تابه‌حال نیز شکسته نشده است.

۳ سیستم رمز الگمال

در این بخش می‌خواهیم بر مبنای فرض DDH و بدون استفاده از تابع درهم‌سازی، یك سیستم رمز بسازیم که امنیت متن اصلی منتخب داشته باشد. سیستم رمزی که در ادامه معرفی می‌کنیم سیستم رمز الگمال است:

۱. $(G, q, g) \leftarrow \mathsf{GroupGen}(1^n)$ (یك گروه دوری G با مرتبه q و مولد g تولید می‌کند.)
$x \leftarrow \mathbb{Z}_q$ (به تصادف x را از $\mathbb{Z}_q$ انتخاب می‌کند.)
$h = g^x$
$pk = (G, q, g, h)$
$sk = (G, q, g, x)$

۲. $\langle g^r, m \cdot h^r\rangle \leftarrow \mathsf{Enc}_{pk}(m)$ که r به تصادف از $\mathbb{Z}_q$ انتخاب می‌شود.

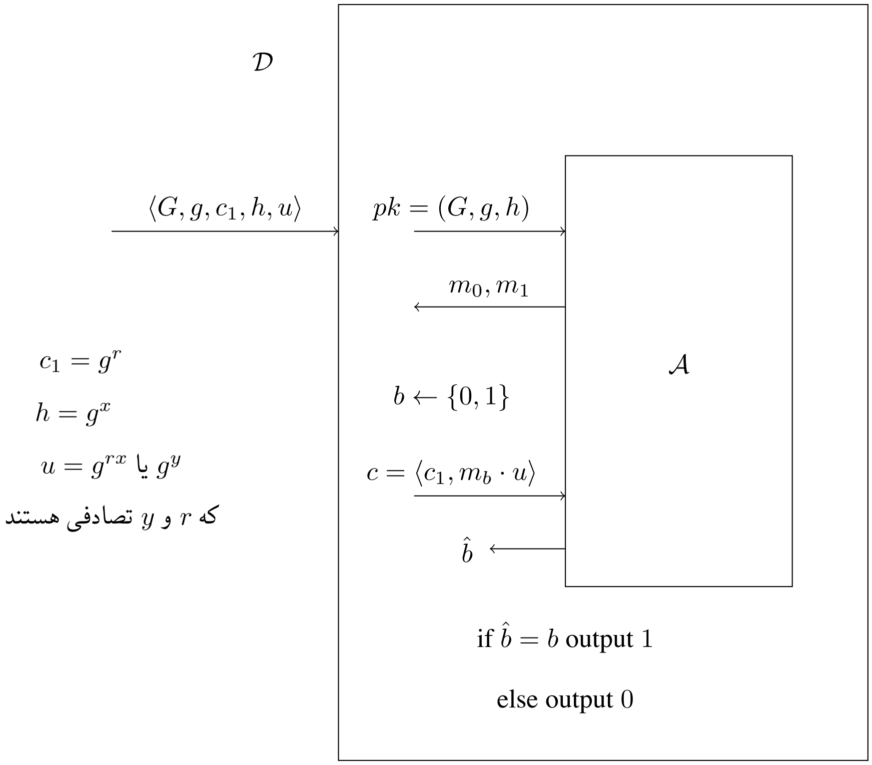
۳. $\frac{c_1}{c_2^x} \leftarrow \mathsf{Dec}_{sk}(\langle c_1, c_2\rangle)$

لم ۳ *سیستم رمز الگمال تحت فرض DDH، امنیت متن اصلی منتخب دارد.*

برهان. این لم را با استفاده از کاهش اثبات می‌کنیم:
فرض کنید سیستم رمز الگمال تحت فرض DDH، امنیت CPA ندارد. در این صورت یك مهاجم چندجمله‌ای $\mathcal{A}$ برای حمله به این سیستم وجود دارد که با احتمال غیرناچیز $\mu(n)$ در آزمایش تمایز موفق می‌شود. تمایزگر $\mathcal{D}$ را به صورت زیر از روی مهاجم $\mathcal{A}$ می‌سازیم:

[5] Hash Function

[6] مشابه امنیت CCA است، اما مهاجم نمی‌تواند هیچ پیام رمزشده‌ی معتبری تولید کند



تمایزگر $\mathcal{D}$ توزیع‌های $DH = \langle G, g, g^r, g^x, g^{rx}\rangle$ و $R = \langle G, g, g^r, g^x, g^y\rangle$ را با احتمال غیرناچیز $\mu(n)$ تشخیص می‌دهد، زیرا:

$$\begin{gathered}\Pr\{\mathcal{D} = 1|DH\} = \Pr\{\hat{b} = b\} \geq 1/2 + \mu(n) \\ \Pr\{\mathcal{D} = 1|R\} = 1/2 \\ \Rightarrow |\Pr\{\mathcal{D} = 1|DH\} - \Pr\{\mathcal{D} = 1|R\}| \geq \mu(n)\end{gathered}$$

با فرض DDH به تناقض رسیدیم. پس فرض خلف باطل و حکم برقرار است. ■

نکته ۲ *این سیستم تحت فرض DDH، امنیت متن رمزشده منتخب ندارد. یکی از دلایل آن این است که این سیستم دارای خاصیت هومومورفیک است.*

تعریف ۳ *می‌گوییم یک سیستم رمز دارای خاصیت هومومورفیک است، اگر برای هر پیام m_1 و m_2 در فضای پیام با متن‌های رمزشده c_1 و c_2، رابطه $c_1 \cdot c_2 = \mathsf{Enc}_k(m_1 \cdot m_2)$ برقرار باشد.*

قضیه ۴ *اگر یک سیستم رمز کلید عمومی دارای ویژگی هومومورفیک باشد، دارای امنیت CCA نیست.*

از این ویژگی در ساخت پروتکل‌ها استفاده می‌شود.
یکی از کاربردهای این ویژگی این است که اگر متن رمزشده یک پیام را داشته باشیم، می‌توانیم یک متن رمزشده جدید برای همان پیام تولید کنیم، بدون اینکه بدانیم پیام اصلی یا کلید خصوصی چیست. فرض کنید $c = \mathsf{Enc}_{pk}(m)$ را داریم. کافیست c را در یک متن رمزشده از ۱ ضرب کنیم، تا به یک متن رمزشده جدید برای m برسیم.
این موضوع کاربردهای زیادی دارد؛ مثلا در رای‌گیری الکترونیکی چنین کاری انجام می‌شود.