


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۲۱ آبان ۱۳۹۱

جلسه‌ی ۱۶: رمزنگاری با کلید عمومی

مدرس: شهرام خزائی *نگارنده: امیرحسین نودهی ثابت*

۱ رمزنگاری با کلید عمومی

در سیستم رمزنگاری با کلید عمومی، می‌خواهیم کاری کنیم که نیازی به اشتراک‌گزاری یک کلید و مخفی نگه داشتن آن بین دو طرف نباشد. در این سیستم ما کلید را به دو قسمت تقسیم می‌کنیم، یک کلید مخفی برای رمزگشایی (sk) و یک کلید عمومی برای رمز کردن (pk).

تعریف ۱ *(سیستم رمزنگاری با کلید عمومی[۱]) یک سه‌تایی مرتب به صورت* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *از الگوریتم‌های* PPT[۲]*، یک سیستم رمزنگاری با کلید عمومی است که در آن:*

- Gen*: الگوریتم تولید کلید است که با ورودی* 1^n *زوج کلید* (pk, sk) *را تولید می‌کند.*

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

- Enc*: الگوریتم رمزنگاری است که کلید عمومی* pk *و متن اصلی* $m \in \{0,1\}^n$ *را می‌گیرد و متن رمزی* c *را تولید می کند.*

$$c \leftarrow \mathsf{Enc}_{pk}(m)$$

- Dec*: الگوریتم رمزگشایی است یک الگوریتم قطعی[۳] است و کلید خصوصی* pk *و متن رمزی* c *را می‌گیرد و پیام* $m \in \{0,1\}^n \cup \{\perp\}$ *را تولید می‌کند:* $m \leftarrow \mathsf{Dec}_{sk}(c)$

که اگر پیام رمزگشایی شده $\perp$ *باشد به معنی نامعتبر بودن متن رمزی است.*

- *برای همه* $n \in \mathbb{N}$*،* $m \in \{0,1\}^n$

$$\Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n) : \mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$

همچنین باید یک الگوریتم با زمان چندجمله ای وجود داشته باشد که با ورودی $(1^n, i)$*،* i *امین پیام* n *بیتی را بر اساس یک ترتیبی تولید کند.*

---

[۱] pblic-key cryptosystem
[۲] probabilistic polynomial time
[۳] deterministic

تعریف ۲ (*رمزنگاری با کلید عمومی امن*[۴]) *به سیستم رمزنگاری با کلید عمومی، امن گوییم اگر برای همه تمایزگرهای* nuPPT *مانند* $\mathcal{D}$*، یک تابع ناچیز* $\varepsilon(\cdot)$ *وجود داشته باشد که برای همه مقادیر* $n \in \mathbb{N}$ *و* $m_0, m_1 \in \{0,1\}^n$ *تمایزگر* $\mathcal{D}$ *بین توزیع‌های زیر با احتمال حداکثر* $\varepsilon(n)$ *تمایز قائل شود:*

- $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(m_0))\}_n$
- $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(m_1))\}_n$

امنیت کامل[۵]**:** امنیت کامل امکان ندارد، زیرا یک حمله کننده با منابع نامحدود[۶] می تواند به راحتی پیام‌های m_0 و m_1 را با مقادیر تصادفی که الگوریتمEnc استفاده می‌کند رمز کرده و با مقایسه با متن رمزی، پیام مورد نظر را بدست آورد.

الگوریتم رمزکردن قطعی: اینکه یک الگوریتم رمزکردن قطعی داشته باشیم هم غیر ممکن است، چون در غیر این صورت حمله کننده میتواند به راحتی پیام m_0 و m_1 را رمز کرده و با مقایسه با متن رمزی، بین این دو تمایز قائل شود.

مثل رمزنگاری با کلید خصوصی، ما می توانیم تعاریف را به امنیت چندپیامی[۷] گسترش دهیم. خوشبختانه در رمزنگاری با کلید عمومی، امنیت چند پیامی با تک پیامی [۸] معادل است.

۲ ساخت یک سیستم رمزنگاری عمومی

به نظر می‌رسد که جایگشت دریچه‌دار[۹] ، مناسب سیستم رمز با کلید عمومی باشد. می‌توانیم اندیس i از تابع را کلید عمومی و دریچه t را کلید خصوصی قرار دهیم. در نتیجه:

$$\mathsf{Enc}_i(m) = f_i(m)$$

و

$$\mathsf{Dec}_{i,t}(c) = {f_i}^{-1}(c)$$

به هر حال بر اساس تعریف ما، این امنیت ندارد، زیرا قطعی است و می‌تواند مورد حمله قرار گیرد. سیستم بهتر برای پیام های تک بیتی این است که قرار دهیم:

$$\mathsf{Enc}_i(x) = \{r \leftarrow \{0,1\}^n : \langle f_i(r), b(r) \oplus m \rangle\}$$

به طوری که b بیت هاردکور برای f است.
الگوریتم: امنیت تک بیتی با سیستم کلید عمومی

---

[۴] secure
[۵] perfect secrecy
[۶] unbounded adversary
[۷] multi-message security
[۸] single-message security
[۹] trapdor permutation

- $\mathsf{Gen}(1^n) : (f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. $\text{Output}(pk, sk) \leftarrow ((f_i, b_i), f_i^{-1})$.
- $\mathsf{Enc}_{pk}(m) : \text{Pick } r \leftarrow \{0,1\}^n$. $\text{Output}(f_i(r), b_i(r) \oplus m)$.
- $\mathsf{Dec}_{sk}(c_1, c_2) :$ Compute $r \leftarrow f_i^{-1}(c_1)$ and output$b_i(r) \oplus c_2$.

اینجا، $(f_i, f_i^{-1})_{i \in I}$ خانواده‌ای از جایگشت‌های دریچه‌دار یک‌طرفه هستند و b_i بیت هاردکور متناظر با f_i است. Gen_T الگوریتم PPT برای نمونه گیری از اندیس جایگشت دریچه‌ای از I است.

قضیه ۱ *اگر جایگشت دریچه‌دار وجود داشته باشد، سیستم رمزی که در بالا ساختیم یک سیستم رمزنگاری کلید عمومی با امنیت تک‌بیتی است.*
اثبات: *به عنوان فرض خلف در نظر بگیرید که وجود دارد یک $\mathcal{D} \in \mathsf{nuPPT}$ و چندجمله‌ای p به طوری که $\mathcal{D}$ با احتمال $\frac{1}{p(n)}$ بین دو توزیع زیر تمایز قایل می شود:*

- $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(0))\}$
- $\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : (pk, \mathsf{Enc}_{pk}(1))\}$

با استفاده از لم پیش‌بینی[۱۰]، ماشین $\mathcal{A}$ وجود دارد به طوری که:

$$\Pr[m \leftarrow \{0,1\}; (pk, sk) \leftarrow \mathsf{Gen}(1^n) : \mathcal{A}(pk, \mathsf{Enc}_{pk}(m)) = m] > \frac{1}{2} + \frac{1}{2p(n)}$$

حال می توانیم از $\mathcal{A}$ برای ساخت ماشین $\mathcal{A}'$ استفاده کنیم که هاردکور b را پیش‌بینی می‌کند:
$\mathcal{A}'$ بر روی ورودی (pk, y)، ابتدا c را از $\{۰, ۱\}$ انتخاب کرده، m را برابر $\mathcal{A}(pk, (y, c))$ قرار داده و $c \oplus m$ را به خروجی می دهد.
توجه کنید که:

$$\begin{aligned}
&\Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n); r \leftarrow \{0,1\}^n : \mathcal{A}'(pk, f_{pk}(r)) = b(r)] \\
&= \Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n); r \leftarrow \{0,1\}^n; c \leftarrow \{0,1\} : \mathcal{A}(pk, f_{pk}(r), c)) \oplus c = b(r)] \\
&= \Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n); r \leftarrow \{0,1\}^n; m \leftarrow \{0,1\} : \mathcal{A}(pk, f_{pk}(r), m)) \oplus b(r) = m] \\
&= \Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n); m \leftarrow \{0,1\} : \mathcal{A}(pk, f_{pk}(r), m)) = m] \\
&\geq \frac{1}{2} + \frac{1}{2p(n)}
\end{aligned}$$

۳ سیستم رمزنگاری با کلید عمومی الجمال

سیستم رمزنگاری الجمال خیلی ساده و رایج و کارا است. برای ساخت آن ابتدا یک فرض جدید را بیان می کنیم.
فرض دیفی–هلمن تصمیمی (DDH[۱۱]). فرض DDH اظهار می‌کند که دو توزیع زیر از لحاظ محاسباتی غیر قابل تمایزند:

- $\{p \leftarrow \tilde{\Pi}_n; y \leftarrow \mathsf{Gen}_q; a, b \leftarrow \mathbb{Z}_q : (p, y, y^a, y^b, y^{ab})\}_n$

[۱۰] prediction
[۱۱] Decisional Diffie-Hellman

- $\{p \leftarrow \tilde{\Pi}_n; y \leftarrow \mathsf{Gen}_q; a, b \leftarrow \mathbb{Z}_q : (p, y, y^a, y^b, y^z)\}_n$

به طوری که:

$$\tilde{\Pi}_n = \{p | p \in \Pi_n \ and \ p = ۲q + ۱, q \in \Pi_{n-۱}\}$$

q متناظر را عدد اول Sophie–Germain گوییم. ما از گروه ضربی $G = \mathbb{Z}_p$ استفاده می‌کنیم، زیرا ساختار ویژه‌ای دارد که استفاده از آن آسان است. اولا G دارای زیرگروه G_q از مرتبه q است و چون q اول است، G_q گروه دوری خواهد بود. در نتیجه انتخاب یک مولد از گروه G_q آسان است (هر عضوی مولد است). وقتی $p = ۲q + ۱$ ، زیرگروه G_q شامل همه توان ۲ها به پیمانه p است. بنابر این انتخاب مولد این گونه است که ابتدا به آسانی به طور تصادفی یک $a \in G$ انتخاب می کنیم و بعد $a^۲$ را محاسبه میکنیم.
در فرض DDH ، مساله مهم این است که گروهی که با آن کار می‌کنیم یک گروه مرتبه اول[۱۲] است. در گروه مرتبه اول، همه اعضا به جز عضو همانی از مرتبه یکسانی هستند. به عبارت دیگر، در گروهی مانند G، اعضایی وجود دارند که از مرتبه ۲، q و $۲q$ هستند و تمایز قائل شدن بین این موارد آسان است. به عنوان مثال، اگر در $T = (p, y, g, h, f)$ متوجه شویم که g و h از مرتبه q و f از مرتبه $۲q$ است، در نتیجه بلافاصله می‌فهمیم که T یک DDH-tuple نیست.
توجه کنید که فرض DDH ، فرض لگاریتم گسسته را ایجاب می‌کند، چون بعد از حل کردن لگاریتم گسسته بر روی دو مولفه اول، تشخیص دادن این که مولفه سوم y^{ab} است یا نه، آسان است.
حالا یک سیستم رمزنگاری با کلید عمومی بر اساس فرض DDH می سازیم.

الگوریتم: رمزنگاری کلید عمومی الجمال امن

- $\mathsf{Gen}(۱^n)$: یک عدد اول مناسب $p = ۲q + ۱$ با طول n بیت انتخاب کنید. یک $g \in \mathbb{Z}_p$ به طور تصادفی انتخاب کنید و $h \leftarrow g^۲ \mod p$ را محاسبه کنید. یک $a \leftarrow \mathbb{Z}_q$ انتخاب کنید. $pk \leftarrow (p, h, h^a \mod p)$ و $sk \leftarrow (p, h, a)$ را به خروجی بدهید.
- $\mathsf{Enc}_{pk}(m)$: یک $b \leftarrow \mathbb{Z}_q$ را انتخاب کنید. $(h^b, h^{ab} \cdot m \mod p)$ را به خروجی بدهید.
- $\mathsf{Dec}_{sk}(c = c(c_۱, c_۲))$: $(c_۲ / c_۱^a \mod p)$ را به خروجی بدهید.

[۱۲] prime-order