مقدمه‌ای پیشرفته بر رمزنگاری ۷ آبان ۱۳۹۱

جلسه‌ی ۱۳: امنیت و آزمایش در رمزنگاری

مدرس: شهرام خزائی *نگارنده: آرش احدی*

پیش از آغاز، مروری بر نمادهای یک سیستم رمز داریم. همان‌گونه که پیش‌تر دیده‌ایم از نمادهای زیر برای سیستم‌های رمز بهره می‌بریم.
$\mathcal{M}$: فضای متن اصلی
N : متغییر تصادفی متن اصلی
$\mathcal{K}$: فضای کلید
C : متغییر تصادفی متن رمزشده
$\mathcal{C}$: فضای متن رمزشده

۱ تعریف شانون از امنیت

اکنون یک سیستم رمز به‌طور کامل امن (در حضور شنودگر) را معرفی می‌کنیم.

تعریف ۱ *یک سیستم رمز*[۱] $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *را روی فضای متن* $\mathcal{M}$ *به طور کامل امن*[۲] *در حضور شنودگر*[۳] *گوییم هرگاه برای هر* $m \in \mathcal{M}$ *و هر متن رمز شده* $c \in \mathcal{C}$ *که* $\Pr[C = c] > 0$، *رابطه زیر برقرار باشد:*

$$\Pr[M = m|C = c] = \Pr[M = m].$$

دو لم زیر شرط‌های معادلی را برای به‌طور کامل بودن یک ساختار رمز ارائه می‌کند:

لم ۱ $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای متن* $\mathcal{M}$ *به‌طور کامل امن است؛ اگرو تنهااگر برای هر توزیع احتمال روی* $\mathcal{M}$ *و هر متن* $m \in \mathcal{M}$ *و هر متن رمزی*[۴] $c \in \mathcal{C}$ *داشته باشیم*

$$\Pr[C = c|M = m] = \Pr[C = c].$$

لم ۲ $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای متن* $\mathcal{M}$ *دارای امنیت کامل است؛ اگرو تنهااگر برای هر توزیع احتمال روی* $\mathcal{M}$ *و هر* $m_0, m_1 \in \mathcal{M}$ *و هر* $c \in C$ *رابطه زیر برقرار باشد*

$$\Pr[C = c|M = m_0] = \Pr[C = c|M = m_1].$$

اثبات دو لم بالا ساده است.

---
[۱] encryption scheme
[۲] perfectly secret
[۳] eavesdrpper
[۴] ciphertext

۲ تعریف امنیت با استفاده از آزمایش

اکنون یک آزمایش را برای سنجش به طورکامل امن بودن $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ارائه می‌کنیم:
آزمایش تشخیص‌ناپذیری هجومی $\mathsf{PrivK}^{\mathbf{eav}}_{\mathcal{A},\Pi}$ [۵]

- دشمن دو متن $m_۰, m_۱ \in \mathcal{M}$ را انتخاب می‌کند.
- Gen یک کلید تصادفی k را تولید می‌کند. هم‌چنین یک بیت تصادفی $b \in \{۰, ۱\}$ به طور تصادفی یکنواخت توسط یک موجود که در آزمایش تعریف شده‌است، انتخاب می‌شود. سپس متن رمزشده $c \leftarrow \mathsf{Enc}_k(m_b)$ به $\mathcal{A}$ داده می‌شود.
- یک کلید تصادفی k توسط Gen تولید می‌شود.
- یک بیت تصادفی $b \in \{۰, ۱\}$ تولید می‌شود.
- متن رمز $c \leftarrow \mathsf{Enc}_k(m)$ محاسبه و به $\mathcal{A}$ داده می‌شود.
- $\mathcal{A}$ یک بیت $b' \in \{۰, ۱\}$ را ارائه می‌کند.

نتیجه آزمایش ۱ اعلام می‌شود هرگاه $b' = b$ و در غیر این صورت ۰ اعلام می‌شود. می‌گوییم $\mathcal{A}$ موفق بوده هرگاه نتیجه آزمایش ۱ باشد و در این‌صورت می‌نویسیم $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱$.
قضیه زیر اهمیت آزمایش بالا را نشان می‌دهد.

قضیه ۳ *$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ روی فضای متن $\mathcal{M}$ دارای امنیت کامل است هرگاه برای هر دشمن $\mathcal{A}$ داشته باشیم*

$$\Pr\left[\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱\right] = \frac{۱}{۲}.$$

تعریف معادل دیگری از امنیت با تعریف دو آزمایش جداگانه می‌توان ارائه کرد.
آزمایش تشخیص‌ناپذیری هجومی $\mathsf{PrivK}^{\mathbf{eav}-\mathrm{b}}_{\mathcal{A},\Pi}$ **(که** $b \in \{۰, ۱\}$**):**

- دشمن دو متن $m_۰, m_۱ \in \mathcal{M}$ را انتخاب می‌کند.
- Gen یک کلید تصادفی k را تولید می‌کند. سپس متن رمزشده $c \leftarrow \mathsf{Enc}_k(m_b)$ به $\mathcal{A}$ داده می‌شود.
- یک کلید تصادفی k توسط Gen تولید می‌شود.
- متن رمز $c \leftarrow \mathsf{Enc}_k(m_b)$ محاسبه و به $\mathcal{A}$ داده می‌شود.
- $\mathcal{A}$ یک بیت $b' \in \{۰, ۱\}$ را ارائه می‌کند.

قضیه ۴ *$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ روی فضای متن $\mathcal{M}$ دارای امنیت کامل است هرگاه برای هر دشمن $\mathcal{A}$ داشته باشیم*

$$\Pr\left[\mathsf{PrivK}^{\mathrm{eav}-0}_{\mathcal{A},\Pi} = ۱\right] = \Pr\left[\mathsf{PrivK}^{\mathrm{eav}-1}_{\mathcal{A},\Pi} = ۱\right].$$

[۵] adversarial indistingushability expriment

۳ قضیه شانون و امنیت محاسباتی

قضیه زیر شرط لازمی را برای ساختارهای رمز به‌طور کامل امن ارائه می‌کند.

قضیه ۵ *اگر* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *یک ساختار رمز دارای امنیت کامل روی فضای متن و* $\mathcal{M}$ *فضای کلید* $\mathcal{K}$ *باشد،* $|\mathcal{K}| \geq |\mathcal{M}|$.

به دلیل محدودیت فوق، در عمل در پی ساخت رمزهای به طور کامل و استفاده از آن‌ها نیستیم، خود را به حمله کننده ایی که دارای محدودیت محاسباتی هستند و از طرفی در صورت موفقیت دارای احتمال موفقیت کمی هستند قانع می‌کنیم. تحلیل چنین حمله کننده‌های به یکی از دو روش زیر می‌تواند انجام گیرد:
تحلیل دقیق[۶]**:** یک رمز را (t, ϵ)-امن گوییم هرگاه هر الگوریتم حمله‌کننده‌در زمان حداکثر t، با احتمال حداکثر ϵ بتواند رمز را بشکند.
تحلیل مجانبی[۷]**:** می‌گوییم یک گردایه از رمزها که با یک کمیت رمز اندیس‌گذاری شده‌اند، امن است هرگاه احتمال شکسته شدن آن توسط هر ماشین تورینگ احتمالاتی چندجمله‌ای غیر یکنواخت، ناچیزباشد.
در ادامه مفهوم جامع‌تری از سیستم رمز با کلید خصوصی را مطالعه می‌کنیم:

۴ سیستم رمز خصوصی

تعریف ۲ *یک رمز خصوصی، یک سه‌تایی* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *از الگوریتم‌های احتمالاتی با زمان چندجمله‌ای است که*

- Gen*: یک مقدار* n *را به عنوان ورودی دریافت می‌کند و یک کلید* k *را به عنوان خروجی ارائه می‌کند.*
- Enc*: الگوریتم رمزنگاری است که کلید* k *و متن اصلی* $m \in \{۰, ۱\}^*$ *را دریافت می‌کند و متن رمز شده* c *را ارائه می‌نماید.*
- Dec*: الگوریتم رمزگشایی لست که کلید* k *و متن رمزی* c *را دریافت و متن اصلی* m *راارائه می‌کند.*
- *برای هر* n *و هر خروجی* Gen *مثل* k *و هر* $m \in \{۰, ۱\}^*$ *رابطه* $\Pr[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] = ۱$

برقرار است.

سیستم رمز خصوصی با طول ثابت:

تعریف ۳ *سیستم رمز خصوصی با طول ثابت، سیستمی است که فضای پیام آن* $\{۰, ۱\}^{l(n)}$ *است به جای* $\{۰, ۱\}^*$ *به ازای یک تابع چند جمله ای* $l : N \to N$

تولید رمز امن به دلیل آن‌که طول کلید باید حداقل برابر با طول متن باشد، کارا نیست. لذا در عمل دو تضعیف برای امنیت در نظر گرفته می‌شود در نظرگرفتن فقط الگوریتم‌های احتمالاتی با زمان چندجمله‌ای (PPT) به عنوان الگوریتم‌های حمله‌کننده (دشمن) تغییر احتمال $\frac{۱}{۲}$ در تعریف بالا با $\frac{۱}{۲} + \epsilon(n)$ که در آن ϵ یک تابع ناچیز است. بدین‌گونه دو روش مطرح می‌شود.

[۶] concrete
[۷] asymptotical

۱.۴ امنیت تک‌پیامی

آزمایش متن منفرد $\mathsf{PrivK}^{\mathbf{eav}}_{\mathcal{A},\Pi}(n)$:

- $k \leftarrow \mathsf{Gen}(1^n)$
- $(m_0, m_1) \leftarrow \mathcal{A}(1^n)$ که در آن $|m_0| = |m_1|$.
- $b \leftarrow \{0, 1\}$
- $c \leftarrow \mathsf{Enc}_k(m_b)$
- $\hat{b} \in \{0, 1\} \leftarrow \mathcal{A}(c)$
- $\hat{b}$ را به عنوان خروجی ارائه می‌شود.

نتیجه این آزمایش، $\widehat{b}$ است. نتیجه آزمایش بالا را ۱ گوییم هرگاه $\hat{b} = b$ و در غیر این صورت ۰ می‌گوییم. می‌گوییم $\mathcal{A}$ موفق بوده هرگاه نتیجه آزمایش ۱ باشد. آزمایش دیگری وجود دارد که در آن b ورودی نیست و تصادفی می باشد. چنین آزمایشی را موفقیت آمیز گوییم هرگاه $\widehat{b} = b$.
با استفاده از آزمایش متن منفرد مفهوم تشخیص ناپذیری زیر را داریم:
تشخیص‌ناپذیری متن منفرد:

تعریف ۴ *ساختار رمز* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *را دارای امنیت تک پیامی در حضور شنودگر گوییم هرگاه برای هر ماشین تورینگ احتمالاتی غیر یکنواخت با زمان چندجمله‌ای*[۸] *رابطه زیر برقرار باشد:*

$$\Pr\left[\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \epsilon(n)$$

که در آن $\epsilon(n)$ *یک تابع ناچیز است.*

به طور مشابه می‌توان دو آزمایش $\mathsf{PrivK}^{\mathrm{eav-b}}_{\mathcal{A},\Pi}(n)$ را برای $b \in \{0, 1\}$ تعریف کرد. لم زیر تعریف معادلی را برای مفهوم بالا ارائه می‌کند.

لم ۶ *ساختار رمز* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *متن دارای امنیت تک پیامی است اگر برای هر غیر یکنواخت تابع ناچیز* ϵ *جود داشته باشد که*

$$\left|\Pr\left[\mathsf{PrivK}^{\mathrm{eav-0}}_{\mathcal{A},\Pi}(n) = 1\right] - \Pr\left[\mathsf{PrivK}^{\mathrm{eav-1}}_{\mathcal{A},\Pi}(n) = 1\right]\right| \leq \epsilon(n).$$

در آزمایش زیر دشمن حمله کننده می تواند از چندین پیام استفاده کند.

[۸] non-uniform PPT

۲.۴ امنیت چندپیامی

آزمایش چند متنی $\mathsf{PrivK}^{\mathbf{mult}}_{\mathcal{A},\Pi}(n)$:

- $k \leftarrow \mathsf{Gen}(1^n)$
- $(m_0^1, \ldots, m_0^\ell, m_1^1, \ldots, m_1^\ell) \leftarrow \mathcal{A}(1^n)$ که در آن برای هر i $|m_0^i| = |m_1^i|$.
- $b \leftarrow \{0, 1\}$
- $c_i \leftarrow \mathsf{Enc}_k(m_b^i)$
- $\hat{b} \leftarrow \mathcal{A}(c_1, \ldots, c_\ell)$

خروجی این آزمایش $\hat{b}$ است که آن را با $\mathsf{PrivK}^{\mathrm{mult}}_{\mathcal{A},\Pi}(n)$ نمایش می‌دهیم. نتیجه آزمایش و موفقیت آن نیز مشابه آزمایش‌های قبل تعریف می‌شود.

تعریف ۵ *$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ را امن تحت چندین متن گوییم هرگاه برای هر حمله کننده PPT غیر یکنواخت $\mathcal{A}$ تابع ناچیز ϵ وجود داشته باشد که*

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

۳.۴ امنیت معنایی

تعریف ۶ *$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ را دارای امنیت معنایی[۹] امن گوییم هرگاه برای هر حمله‌کننده PPT غیریکنواخت $\mathcal{A}$، شبیه‌ساز PPT غیریکنواخت $\mathcal{S}$ وجود داشته باشد به‌گونه‌ای که برای هر تابع توزیع احتمال قابل پیاده‌سازی در زمان چندجمله‌ای $\{\chi_n\}_{n\in\mathbb{N}}$ و هر دو تابع محاسبه‌پذیر با PPT ها مثل f و h تابع ناچیز ϵ وجود داشته باشد که*

$$|\Pr[\mathcal{A}(1^n, \mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{S}(1^n, h(m)) = f(m)]| \leq \epsilon(n).$$

که در آن، احتمال روی متن m با تابع توزیع $\{\chi_n\}_{n\in\mathbb{N}}$ و نیز کلید $k \leftarrow \mathsf{Gen}(1^n)$ و بیت‌های تصادفی مورد استفاده $\mathcal{A}$ و $\mathcal{S}$ گرفته شده است.

لم ۷ *یک سیستم رمز خصوصی دارای امنیت تک پیامی در حضور یک شنودگر است اگر و تنها اگر به طور معنایی چنین باشد.*

[۹] semanticaly secure