به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۲۸ اردیبهشت ۱۳۹۳

جلسه‌ی ۲۳: سیستم رمز الجمال و امضای دیجیتال

مدرس: دکتر شهرام خزائی *نگارنده: سجاد صادقی*

در این جلسه ابتدا سیستم رمزی را مبتنی بر فرض دیفی-هلمن تصمیمی طراحی می کنیم که cpa امن است (امنیت متن انتخاب شده) و سپس به سراغ بحث امضای دیجیتال می‌رویم.

۱ سیستم رمز الجمال

تعریف ۱ *فرض دیفی-هلمن تصمیمی اگر G یک گروه با مولد g باشد آنگاه توزیع های زیر در زمان چندجمله ای از هم تمایزناپذیرند:*

$$(G, g, g^x, g^y, g^r) \approx (G, g, g^x, g^y, g^{xy})$$

که در این جا r یک عدد تصادفی است. یا به عبارتی دیگر می‌گوییم DDH نسبت به G سخت است اگر به ازای هر الگوریتم تصادفی A که در زمان چندجمله ای اجرا می‌شود داشته باشیم:

$$\Pr[A(G, g, g^x, g^y, g^r) = ۱] - \Pr[A(G, g, g^x, g^y, g^{xy}) = ۱] < \varepsilon(n)$$

که در آن $\varepsilon(.)$ یک تابع ناچیز است.

۱.۱ نحوه ی ساخت

باید یک الگوریتم تولید کلید، یک الگوریتم رمز کردن و یک الگوریتم رمز گشایی ارائه دهیم:

الگوریتم تولید کلید روی ورودی ۱^n :

- $(G, q, g) \leftarrow GroupGen(۱^n)$ (یک گروه دوری G با مرتبه ی q و مولد g تولید می‌کند)
- $x \leftarrow Z_q$ (x را به تصادف از Z_q انتخاب می‌کند)
- $h = g^x$
- $pk = (G, q, g, h)$

- $sk = (G, q, g, x)$

الگوریتم رمزنگاری روی ورودی کلید عمومی $pk = (G, q, g, h)$ و پیام $m \in G$:

- $r \leftarrow Z_q$ (r را به تصادف از Z_q انتخاب می کند)
- $\langle g^r, h^r \cdot m \rangle$ را به عنوان خروجی بده

الگوریتم رمز گشایی روی ورودی کلید خصوصی $sk = (G, q, g, x)$ و متن رمز شده $\langle c_1, c_2 \rangle$:

- $m = c_2 / {c_1}^x$

واضح است که الگوریتم رمزنگاری تصادفی است و هر بار که رمز می‌کنیم یک متن تصادفی می‌دهد. ب یاد دارید که اگر الگوریتم رمزنگاری تصادفی نباشد cpa امن نیست.
برای این که بررسی کنیم که الگوریتم رمزگشایی درست کار می‌کند فرض کنید:
$\langle c_1, c_2 \rangle = \langle g^r, h^r \cdot m \rangle$ ، $h = g^x$.
آنگاه خواهیم داشت:

$$\langle \frac{c_2}{c_1} \rangle = \frac{h^r \cdot m}{(g^r)^x} = \frac{(g^x)^r \cdot m}{g^{xr}} = \frac{g^{xr} \cdot m}{g^{xr}} = m$$

قضیه ۱ *اگر مسئله ی دیفی- هلمن محاسباتی نسبت به G سخت باشد آنگاه سیستم رمز الجمال در مقابل حمله ی متن انتخاب شده، امن است.*

برهان. فرض کنیم Π یک طرح سیستم الجمال باشد. ثابت می‌کنیم که Π در حضور یک حمله کننده ی غیرفعال (شنونده) دارای امنیت cpa می‌باشد.
فرض کنید $\mathcal{A}$ یک حمله کننده ی چندجمله ای تصادفی باشد و تعریف کنید:

$$\epsilon(n) = \Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1].$$

حال سیستم رمز تغییر یافته ی Π' را در نظر می‌گیریم که الگوریتم تولید کلید آن (Gen) همان الگوریتم تولید کلید Π است ولی الگوریتم رمز کردن آن روی پیام m و کلید عمومی $pk = (G, q, g, h)$ به این صورت است:

- $r \leftarrow Z_q$ (r را به تصادف از Z_q انتخاب می کند)
- $z \leftarrow Z_q$ (z را به تصادف از Z_q انتخاب می کند)
- $\langle g^r, g^z \cdot m \rangle$ را به عنوان خروجی بده

اگر چه Π' در واقع یک طرح رمز نیست (چون راهی برای رمز گشایی وجود ندارد) ولی آزمایش $PubK^{eav}_{\mathcal{A},\Pi'}(n)$ هنوز معتبر است چون فقط به الگوریتم تولید کلید و رمز کردن مربوط است. قسمت دوم متن رمز شده در Π' به صورت یکنواخت توزیع شده است و به پیام m وابسته نیست (چون z به طور تصادفی انتخاب شده و g^z یک عنصر تصادفی از $\mathcal{G}$ است).قسمت اول متن رمز شده هم به وضوح به پیام m ربطی ندارد بنابراین کل متن رمز شده ربطی به m ندارد:

$$.\Pr[PubK^{eav}_{\mathcal{A},\Pi'}(n) = ۱/۲]$$

حال الگوریتم چندجمله ای احتمالی D زیر را در نظر بگیرید که تلاش می‌کند تا مسئله ی دیفی-هلمن تصمیمی را نسبت به $\mathcal{G}$ حل کند:
می‌دانیم که D به عنوان ورودی $(G, q, g, g_۱, g_۲, g_۳)$ را دریافت می کند که $g_۱ = g^x$ و $g_۲ = g^r$ و $g_۳$ برابر با g^{xr} یا g^z می‌باشد(برای x, r, z تصادفی):

الگوریتم D :
روی ورودی $(G, q, g, g_۱, g_۲, g_۳)$:

- قرار بده $pk = (G, q, g, g_۱, g_۲, g_۳)$ و $\mathcal{A}(pk)$ را اجرا کن تا دو پیام $m_۱, m_۲$ را به دست بیاورد.
- یک بیت تصادفی b انتخاب کن و قرار بده $c_۱ := g_۲$ و $c_۲ := g_۳ \cdot m_b$
- متن رمز شده ی $\langle c_۱, c_۲ \rangle$ را به $\mathcal{A}$ بده و از آن بیت b' را بگیر
- اگر $b = b'$ بود یک به خروجی بده وگرنه صفر را به خروجی بده

حال رفتار D را بررسی می‌کنیم دو حالت ممکن است به وجود بیاید:

حالتtextbf اول: فرض کنیم ورودی $(G, q, g, g_۱, g_۲, g_۳)$ به D داده شده باشد که $g_۱ = g^x$ و $g_۲ = g^r$ و $g_۳$ برابر با g^z باشد، آنگاه D ، $\mathcal{A}$ را روی کلید عمومی $pk = (G, q, g, g^x)$ اجرا می‌کند و متن رمز شده ی $\langle c_۱, c_۲ \rangle = \langle g^r, g^z \cdot m_b \rangle$ را به دست می‌آورد. در این جا اگر خروجی b' مربوط به $\mathcal{A}$ برابر با b بود D یک را به خروجی می‌دهد و بنا براین داریم:

$$.\Pr[D(G, q, g, g^x, g^r, g^z) = ۱] = \Pr[PubK^{eav}_{\mathcal{A},\Pi'}(n) = ۱] = \frac{۱}{۲}$$

حالتtextbf دوم: فرض کنیم ورودی $(G, q, g, g_۱, g_۲, g_۳)$ به D داده شده باشد که $g_۱ = g^x$ و $g_۲ = g^r$ و $g_۳$ برابر با g^{xr} باشد، آنگاه D ، $\mathcal{A}$ را روی کلید عمومی $pk = (G, q, g, g^x)$ اجرا می‌کند و متن رمز شده ی $\langle c_۱, c_۲ \rangle = \langle g^r, g^{xr} \cdot m_b \rangle$ را به دست می‌آورد. در این جا اگر خروجی b' مربوط به $\mathcal{A}$ برابر با b بود D یک را به خروجی می‌دهد و بنا براین داریم:

$$.\Pr[D(G, q, g, g^x, g^r, g^{xr}) = ۱] = \Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = ۱] = \epsilon(n)$$

چون مسئله ی دیفی-هلمن تصمیمی سخت است پس باید داشته باشیم:

$$.negl(n) \geq \Pr[D(G, q, g, g^x, g^y, g^{xy}) = ۱] - \Pr[D(G, q, g, g^x, g^y, g^z) = ۱] = |\frac{۱}{۲} - \epsilon(n)|$$

و بنا براین داریم $\epsilon(n) \leq \frac{۱}{۲} + negl(n)$ و به این ترتیب اثبات کامل می‌شود. ■

۲.۱ مقاومت در برابر حمله ی متن رمزی انتخابی

حال این سوال پیش می‌آید که آیا الجمال تحت حمله ی cca امن است یا نه؟

برای بررسی آن ابتدا یک تعریف می‌آوریم:

تعریف ۲ *خاصیت هomomورفیک یک سیستم رمز با کلید عمومی دارای خاصیت هomomورفیک است اگر برای هر n و برای هر (sk, pk) که به وسیله ی الگوریتم تولید کلید به عنوان خروجی داده می‌شوند، بتوان گروه های $\mathcal{M}$ و $\mathcal{C}$ را تعریف کرد که:*

- *فضای پیام $\mathcal{M}$ است و همه ی متن های رمزی که به عنوان خروجی الگوریتم Enc_{pk} داده می‌شوند عضو $\mathcal{C}$ باشند.*
- *برای هر $m_1, m_2 \in \mathcal{M}$ و $c_1, c_2 \in \mathcal{C}$ که $m_1 = \mathsf{Dec}_{sk}(c_1)$ و $m_2 = \mathsf{Dec}_{sk}(c_2)$ داشته باشیم:*

$$Dec_{sk}(c_1 \cdot c_2) = m_1.m_2 .$$

سیستم رمز الجمال نیز دارای خاصیت هomomورفیک است:
اگر متن رمز شده ی پیام های m_1 و m_2 برابر با C_1 و C_2 باشند آنگاه:

$$C_1 = \mathsf{Enc}_{sk}(m_1) = \langle g^r, h^r \cdot m \rangle \ , \ C_2 = \mathsf{Enc}_{sk}(m_2) = \langle g^s, h^s \cdot m \rangle \ \Rightarrow$$
$$C_3 = \mathsf{Enc}_{sk}(m_3) = \mathsf{Enc}_{sk}(m_1 \cdot m_2) = \langle g^{r+s}, h^{r+s} \cdot m_1 \cdot m_2 \rangle$$

هم چنین این سیستم دارای خاصیت رمزگذاری مجدد هم هست:

تعریف ۳ *رمزگذاری مجدد اگر یک متن رمز شده داشته باشیم که رمز شده ی یک پیام باشد، می‌توان از روی آن دوباره متن را رمز کرد و متن رمزی جدیدی بدست آورد.*

در سیستم رمز الجمال داریم:

$$C = \mathsf{Enc}_{sk}(m) = \langle g^r, h^r \cdot m \rangle \ \Rightarrow \ C' = \langle g^r g^s, h^r h^s \cdot m \rangle$$

به عبارتی دیگر متن رمز شده ی C را در $Enc_{sk}(1)$ ضرب می‌کنیم و متن رمز شده ی جدیدی بدست می‌آید.

بنابراین به وضوح سیستم رمز الجمال cca امن نیست .(حمله کننده دو پیام مورد چالش m_1, m_2 را به چالشگر می‌دهد و چالشگر یک متن رمز شده ی c برمی‌گرداند که حمله کننده باید بگوید متن رمز شده ی کدام پیام است. حمله کننده متن m_3 را به چالشگر می‌دهد و متن رمزی c_3 را دریافت می‌کند و سپس متن رمز شده ی $c.c_3$ را به چالشگر می‌دهد و چالشگر به حمله کننده $m_3.m_b$ را برمی‌گرداند و حمله کننده با استفاده از این b می‌تواند به راحتی بفهمد که c متن رمز شده ی کدام پیام بوده است)

سیستم الجمال با استفاده از تابع درهم سازی و رمز متقارن می‌تواند امنیت cca را برای ما فراهم کند و دو نوع رمز RSA ی درهم سازی شده و الگوی درهم سازی- بعد- امضا در عمل این نوع امنیت را برای ما فراهم می‌کنند.

۲ امضای دیجیتال

در این قسمت امضای دیجیتال [۱] را توضیح می‌دهیم که دارای ویژگی های زیر است:

- باید برای ما جامعیت [۲] فراهم کند
- انکار ناپذیر باشد [۳] : اگر فردی پیامی را امضا کرد نتواند آن را انکار کند

ویژگی هایی که امضای دیجیتال را از کد اصالت سنجی پیام متمایز می‌کند:

- به طور عمومی قابل اثبات است [۴]:لازم نیست حتما یک کلید خصوصی داشته باشیم تا بتوانیم آن را اثبات کنیم.
- قابل انتقال است [۵]:اگر یک پیام به ما بدهند می‌توان آن را به نزدشخص دیگر برد و نشان داد که مثلا امضای کسی است.

تعریف ۴ *یک طرح امضا یک سه تایی از سه الگوریتم چندجمله ای احتمالی* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *است که دارای شرایط زیر است:*

۱. *الگوریتم تولید کلید* (Gen) *به عنوان ورودی پارامتر امنیت* 1^n *را می‌گیرید و دو کلید* (pk, sk) *با طول* n *را به خروجی می‌دهد که* pk *کلید عمومی و* sk *کلید خصوصی است.*

۲. *الگوریتم امضا* (Sign) *به عنوان ورودی کلید خصوصی* sk *و پیام* m *را می‌گیرد و به عنوان خروجی امضای* σ *را بیرون می‌دهد که با* $\sigma \leftarrow Sign_{sk}(m)$ *نمایش می‌دهیم*

۳. *الگوریتم معین تصدیق* (Vrfy) *به عنوان ورودی کلید عمومی* pk *و پیام* m *و امضای* σ *را می‌گیرد و خروجی آن یک بیت* b *است اگر* $b = 1$ *باشد یعنی امضا معتبر است و اگر* $b = 0$ *باشد امضا نامعتبر است. این را با* $b = \mathsf{Vrfy}_{pk}(m, \sigma)$ *نمایش می‌دهیم.*

یک شرط همواره باید برقرار باشد:

$$\mathsf{Vrfy}_{pk}(m, \mathsf{Sign}_{sk}(m)) = 1.$$

حال امنیت را برای این سیستم تعریف می‌کنیم. برای این کار ابتدا یک آزمایش طراحی می‌کنیم:

$\mathsf{Signforge}_{\mathcal{A},\Pi}(n)$:

- $(sk, pk) \leftarrow \mathsf{Gen}(1^n)$ به وسیله ی الگوریتم Gen دو کلید sk, pk را تولید کن

[۱] Digital Signature
[۲] Integrity
[۳] Non-repudation
[۴] Publicly verifiable
[۵] Transferable

- $(m, \sigma) \leftarrow \mathcal{A}^{Sign_{sk}}(pk)$ ، Q=مجموعه ی همه ی پیام هایی که امضای آن ها به وسیله ی $\mathcal{A}$ در طول اجرا درخواست شده اند
- خروجی ۱ را بده اگر و تنها اگر $\mathsf{Vrfy}_{pk}(m, \sigma) = ۱$ و $m \notin Q$

ابتدا الگوریتم تولید کلید ، کلید عمومی و خصوصی را تولید می‌کند . سپس به حمله کننده دسترسی اوراکلی به الگوریتم امضا می‌دهیم یعنی هر پیامی را که بخواهد برایش رمز می‌کنیم و در نهایت حمله کننده یک پیام را که قبلا امضای آن را از ما نپرسیده است به همراه امضایش به ما(چالشگر) می‌دهد و اگر امضای معتبری برای پیام باشد حمله کننده پیروز می‌شود.

تعریف ۵ *امنیت جعل ناپذیری امضا: می‌گوییم سیستم امضای دیجیتال Π دارای امنیت جعل ناپذیری است اگر برای هر مهاجم چندجمله ای احتمالی ، تابع ناچیز $\epsilon()$ وجود داشته باشد که :*

$$\Pr\{\mathsf{Signforge}_{\Pi,\mathcal{A}}(n) = ۱\} \leq \epsilon(n).$$

حال با سوال بعد رو به رو می‌شویم: چطور یک سیستم امضای دیجیتال امن طراحی کنیم؟

۱.۲ استفاده از RSA برای امضای دیجیتال

ابتدا به سراغ استفاده از RSA (کتابی) برای امضای دیجیتال می‌رویم[۶]:

برای طراحی سیستم باید یک الگوریتم تولید کلید ، یک الگوریتم امضا و یک الگوریتم تصدیق امضا را ارائه بدهیم:

- Gen : روی ورودی ۱^n الگوریتم $\mathsf{GenRSA}(۱^n)$ را اجرا کن تا (N, e, d) را بدست آوری. کلید عمومی برابر با $\langle N, e\rangle$ است و کلید خصوصی برابر با $\langle N, d\rangle$ می‌باشد.
- Sign : روی ورودی کلید خصوصی $sk = \langle N, d\rangle$ و پیام $\mathcal{Z}_N^*$ امضا را محاسبه کن:

$$\sigma = [m^d \ mod \ N].$$

- Vrfy : روی ورودی کلید عمومی $pk = \langle N, e\rangle$ و پیام $m \in \mathcal{Z}_N^*$ و امضای $\sigma \in \mathcal{Z}_N^*$ خروجی ۱ را بده اگر و تنها اگر :

$$m = [\sigma^e \ mod \ N]$$

این سیستم دارای امنیت جعل ناپذیری نیست چون خاصیت هومومورفیک دارد.
برای امن کردن این سیستم از تابع درهم سازی استفاده می‌کنیم که دو ویژگی مهم دارد:

- امنیت جعل ناپذیری را برای ما فراهم می‌کند
- اگر طول پیام خیلی بزرگ باشد خود امضا هم خیلی بزرگ می‌شود ولی با استفاده از تابع درهم سازی می‌توانیم طول امضا را کاهش دهیم.

[۶] Textbook RSA digital signature

۲.۲ امضای دیجیتال با RSA و تابع درهم سازی

حال از تابع درهم سازی در الگوریتم RSA استفاده می‌کنیم:

- Gen : روی ورودی 1^n الگوریتم $GenRSA(1^n)$ را اجرا کن تا (N, e, d) را بدست آوری. کلید عمومی برابر با $\langle N, e\rangle$ است و کلید خصوصی برابر با $\langle N, d\rangle$ می‌باشد.
- Sign : روی ورودی کلید خصوصی $sk = \langle N, d\rangle$ و پیام $\mathcal{Z}_N^*$ امضا را محاسبه کن:

$$\sigma = [H(m)^d \ mod \ N].$$

- Vrfy : روی ورودی کلید عمومی $pk = \langle N, e\rangle$ و پیام $m \in \mathcal{Z}_N^*$ و امضای $\sigma \in \mathcal{Z}_N^*$ خروجی ۱ را بده اگر و تنها اگر :

$$H(m) = [\sigma^e \ mod \ N]$$

در این مدل تابع درهم سازی باید کاملا تصادفی باشد که در مدل اوراکل تصادفی محقق می‌شود.
سیستم دیگری که استاندارد است و در عمل مورد استفاده قرار می‌گیرد سیستم امضای دیجیتال استاندارد می‌باشد[۷]:

۳.۲ سیستم امضای دیجیتال استاندارد (DSS)

سیستم امضای دیجیتال استاندارد (DSS) یا الگوریتم امضای دیجیتال (DSA) را NIST در سال ۱۹۹۱ طراحی کرد که مبتنی بر لگاریتم گسسته است و امنیت آن تا به حال اثبات یا رد نشده است.
اگر $\mathcal{G}$ یک الگوریتم چند جمله ای احتمالی باشد که روی ورودی 1^n خروجی (p, q, g) را می دهد که به جز با احتمال ناچیز:(۱) p و q نسبت به هم اول هستند و $||q|| = n$ ؛ (۲) $q|(p-1)$ ولی $q^2 \nmid (p-1)$ ؛ و (۳) g یک مولد از زیرگروه $\mathcal{Z}_p^*$ با درجه ی q باشد ؛

- Gen : روی ورودی 1^n الگوریتم $\mathcal{G}$ را اجرا کن تا (p, q, g) را بدست آوری. فرض کنیم $H : \{0,1\}^* \to \mathcal{Z}_q$ یک تابع باشد. یک $x \leftarrow \mathcal{Z}_q$ به طور یکنواخت و تصادفی انتخاب کن و قرار بده $y = [g^x \ mod \ p]$. کلید عمومی برابر است با $\langle H, p, q, g, y\rangle$ و کلید خصوصی برابر است با $\langle H, p, q, g, x\rangle$.
- Sign : روی ورودی کلید خصوصی $\langle H, p, q, g, x\rangle$ و پیام $m \in \{0,1\}^*$ ، $k \leftarrow \mathcal{Z}_q^*$ را به طور یکنواخت و تصادفی انتخاب کن و قرار بده $r = [[g^k \ mod \ p] \ mod \ q]$. $s = [(H(m) + xr).k^{-1} \ mod \ q]$ را محاسبه کن و امضای (r, s) را به عنوان خروجی بده.
- Vrfy : روی ورودی کلید عمومی $\langle H, p, q, g, y\rangle$ و پیام $m \in \{0,1\}^*$ و امضای (r, s) که $r \in \mathcal{Z}_q$ و $s \in \mathcal{Z}_q^*$ است ، مقادیر $u_1 = [H(m).s^{-1} \ mod \ q]$ و $u_2 = [r.s^{-1} \ mod \ q]$ را محاسبه کن. خروجی ۱ بده اگر و تنها اگر :

$$r = [[g^{u_1} y^{u_2} \ mod \ p] \ mod \ q]$$

[۷] Digital Signature Standard