جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

پنجمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

Archive of SID

بهبود امنیت طرح امضای کور لی، هوانگ و یانگ

علی ناصری
دانشگاه امام حسین (ع)
a_naseri@ict.gov.ir

حمید مرادی موفق
دانشگاه امام حسین (ع)
h.m.movafagh@gmail.com

چکیده: در سال ۲۰۰۵، سه نفر به اسامی لی، هوانگ و یانگ یک طرح امضای کور بر پایه لگاریتم گسسته ارائه کردند. این امضا خصوصیات غیر قابل ردگیر بودن[1] و عدم ارتباط‌پذیر بودن[2] را برآورده می‌کند. در این مقاله یک حمله به این طرح طراحی می شود به طوریکه در این حمله متقاضی امضا، تنها با اجرای یک بار پروتکل امضا با امضا کننده، می‌تواند بیش از یک امضا معتبر بدست آورد و این یک خاصیت مهم امنیتی امضا کور را نقض می‌کند. بنابراین اثبات می گردد امضا ی مذکور نا امن است.در نهایت با ارائه یک راهکارمناسب امنیت امضای مذکوردر برابر حمله ارایه شده تامین می گردد.

واژه های کلیدی: لگاریتم گسسته، امضای کور، غیر قابل ردگیر بودن، عدم ارتباط‌پذیر بودن

۱- مقدمه

در سال ۱۹۸۲، D.Chuam یک ایده طرح امضای کور ارائه کرد که به صورت تئوری اطلاعاتی نظیر، بدست آوردن یک لینک بین امضا و مثلاً عمل امضا کردن _ که کوری را برای یک امضا تولید می‌کند _ را از امضا کننده سلب می‌کرد [1].این موضوع معمولاً به خاصیت عدم ارتباط‌پذیر بودن یا غیر قابل ردگیر بودن، ارجاع داده می‌شود.به علت خاصیت عدم لینک‌پذیری و عدم جعل‌پذیری امضاها، امضاهای کور در پروتکل‌های پرداخت –الکترونیکی غیر قابل ردگیری [2,1] و سیستمهای رأی‌گیری الکترونیکی بدون افشای هویت [4,3]، بطور وسیعی بکار برده می‌شوند. اخیراً طرحهای متعددی از امضای کور بر پایه مسئله لگاریتم گسسته ارائه و درباره آنها بحث شده است[5,6,7,8]. در سال ۱۹۹۴ Carmenish و همکارانش یک طرح امضای کور بر پایه لگاریتم گسسته ارائه کردند [5]. در سال ۱۹۹۵، Harn طی مقاله ای ادعا نمود که طرح Carmenish خاصیت غیر قابل ردگیر بودن را برآورده نمی کند[6]. ,و همانطور که در مرجع[7] آمده است Horster و همکارانش ادعا نمودند که تجزیه تحلیل Harn صحیح نبوده است. در نهایت در سال ۲۰۰۵ ، Lee و همکارانش در مقاله مرجع [8] نشان دادند که مقاله Horster درباره حمله Harn اشتباه بوده است و سپس آنها یک طرح

[1] untraceability
[2] unlinkability

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archive of SID

امضای کور بهبود یافته در مرجع [8] ارائه دادند تا امنیت طرح Carmenish را برای مقاومت در برابر حمله مطرح شده در مرجع[5] بالا ببرند.

در یک طرح امضای کور امن، این موضوع بیش از هر چیزی می‌بایستی ضمانت شود که هر متقاضی امضا در صورت انجام x (xعدد صحیح) بار پرتکل امضاء با امضا کننده، حداکثر x امضای معتبر بدست آورد [1,2,3]. این مقاله وجود نقص امنیتی در طرح مرجع [8] را نشان می‌دهد به طوریکه متقاضی با اجرای تنها یکبار پروتکل امضا با امضاکننده می‌تواند دو امضای موجود را برای دو پیام مجزا بدست آورد. در ادامه در بخش ۲ طرح لی، هوانگ و یانگ از مرجع [8] بیان می گردد. در بخش ۳حمله به این طرح ارائه می‌شود و در بخش ۴ بهبود و مقاوم‌سازی طرح مذکور در برابر حمله ارائه می گردد. در بخش ۵ به نتیجه گیری پرداخته می شود و در نهایت در بخش ۶ مراجع ذکر خواهد شد.

۲- طرح امضای کور لی هوانگ یانگ

در این بخش طرح لی، هوانگ و یانگ را از [8] بیان می گردد. دو نقش اصلی این طرح را امضاکننده و متقاضی امضا _ که از امضاکننده تقاضای امضا دارد _ برعهده دارند.

۲-۱- راه‌اندازی

امضاکننده دو عدد بزرگ اول p و q را انتخاب می‌کند به طوری که $q|p-1$ و g یک مولد با مرتبه p از Z^*p باشد. امضا کننده یک عدد صحیح x را بعنوان کلید خصوصی‌اش انتخاب می‌کند و $y \equiv g^x (\mathrm{mod}\ p)$ و (p,q,g,y) را به عنوان کلید عمومی منتشر می‌کند.

امضاکننده به صورت تصادفی $\tilde{k}_1, \tilde{k}_2, b_1, b_2$ را در Zq انتخاب می‌کند و مقادیر زیر را محاسبه می‌کند.

$$\tilde{r}_1 \equiv g^{\tilde{k}_1} (\mathrm{mod}\ p) \quad (۱)$$

$$\tilde{r}_2 \equiv g^{\tilde{k}_2} (\mathrm{mod}\ p) \quad (۲)$$

و باید $GCD(\tilde{r}_2, q)=1$ و $GCD(\tilde{r}_1, q)=1$ باشند آنگاه امضاکننده $(\tilde{r}_1, \tilde{r}_2, b_1, b_2)$ را برای متقاضی می‌فرستد.

۲-۲-کور کردن پیام

وقتی متقاضی $(\tilde{r}_1, \tilde{r}_2, b_1, b_2)$ را دریافت کرد متقاضی ۵ مقدار تصادفی (a,b,c,d,e) را انتخاب می‌کند و آنها را نزد خود نگه می‌دارد پس متقاضی مقادیر زیر را محاسبه می‌کند.

$$r_1 \equiv \tilde{r}_1^{\,ab_1} g^{\,c} (\mathrm{mod}\ p) \quad (۳)$$

$$r_2 \equiv \tilde{r}_2^{\,bb_2} g^{\,e} (\mathrm{mod}\ p) \quad (۴)$$

$$r \equiv (r_1 r_2)^d (\mathrm{mod}\ p) \quad (۵)$$

سپس متقاضی پیام m را با محاسبه:

$$\tilde{m}_1 \equiv m\tilde{r}_1 \frac{r}{2}^{-1} ad (\mathrm{mod}\ q) \quad (۶)$$

$$\tilde{m}_2 \equiv m\tilde{r}_2 \frac{r}{2}^{-1} bd (\mathrm{mod}\ q) \quad (۷)$$

کور می‌کند و $(\tilde{m}_1, \tilde{m}_2)$ را جهت امضا به امضاکننده تحویل می‌دهد.

۲-۳ امضا کردن

پس از رسیدن $(\tilde{m}_1, \tilde{m}_2)$ به امضاکننده، امضاکننده به صورت زیر امضا می‌کند.

$$\tilde{s}_1 \equiv x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1 (\mathrm{mod}\ q) \quad (۸)$$

$$\tilde{s}_2 \equiv x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2 (\mathrm{mod}\ q) \quad (۹)$$

و $(\tilde{s}_1, \tilde{s}_2)$ را به متقاضی تحویل می‌دهد.

۲-۴-بازگشایی کوری

سرانجام متقاضی برای یافتن امضای معتبر عمل بازگشایی کوری انجام می‌دهد و محاسبه می‌کند.

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} \frac{r}{2} + cdm (\mathrm{mod}\ q) \quad (۱۰)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} \frac{r}{2} + edm (\mathrm{mod}\ q) \quad (۱۱)$$

متقاضی سپس $s \equiv (s_1 + s_2) (\mathrm{mod}\ q)$ را محاسبه می‌کند و سه تایی (m, r, s) را منتشر می‌کند.

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

۲-۵- تصدیق کردن

تصدیق‌کننده با بررسی کردن تساوی زیر پی به معتبر بودن یا جعلی بودن امضا می‌برد.

(۱۲)

$$g^{s} \equiv y^{r} r^{m} (\mathrm{mod}\ \ p)$$

۳- حمله به طرح امضای کور لی، هوانگ و یانگ

در پروتکل که در بخش دوم توضیح داده شد اگر متقاضی درستکار نباشد می‌تواند دو امضای معتبر برای دو پیام جداگانه m_α و m_β به ترتیب، تنها با اجرای یکبار پروتکل با امضاکننده بدست آورد.

حمله ارائه شده در زیر شرح داده می‌شود.

۳-۱-راه‌اندازی

مرحله راه اندازی مانند قبل انجام می شود با این تفاوت که متقاضی بجای محاسبه

$r_1 \equiv \tilde{r}_1^{\,ab_1} g^{c} (\mathrm{mod}\ \ p)$ و

$r_2 \equiv \tilde{r}_2^{\,bb_2} g^{e} (\mathrm{mod}\ \ p)$ و

$$r \equiv (r_1 r_2)^{d} (\mathrm{mod}\ \ p)$$

مقادیر زیر را محاسبه می‌کند.

$$r_1 \equiv (\tilde{r}_1^{\,ab_1} g^{c})^{d} (\mathrm{mod}\ \ p) \qquad (۱۳)$$

و

$$r_2 \equiv (\tilde{r}_2^{\,bb_2} g^{e})^{d} (\mathrm{mod}\ \ p) \qquad (۱۴)$$

و در این حمله نیازی به محاسبه r نیست.

۳-۲-کور کردن پیام

متقاضی سپس $(\tilde{m}_1, \tilde{m}_2)$ را به صورت زیر تشکیل می‌دهد:

$$\tilde{m}_1 \equiv m_\alpha \tilde{r}_1 r_1^{-1} ab (\mathrm{mod}\ \ q) \qquad (۱۵)$$

و

$$\tilde{m}_2 \equiv m_\alpha \tilde{r}_2 r_2^{-1} ab (\mathrm{mod}\ \ q) \qquad (۱۶)$$

و $(\tilde{m}_1, \tilde{m}_2)$ را برای امضاکننده می‌فرستد.

۳-۳-امضا کردن

امضاکننده هم $(\tilde{s}_1, \tilde{s}_2)$ را به صورت قبل محاسبه می‌کند.

$$\tilde{s}_1 \equiv x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1 (\mathrm{mod}\ \ q) \qquad (۱۷)$$

$$\tilde{s}_2 \equiv x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2 (\mathrm{mod}\ \ q) \qquad (۱۸)$$

و $(\tilde{s}_1, \tilde{s}_2)$ را برای متقاضی (حمله کننده) می‌فرستد.

۳-۴-بازگشایی کوری

متقاضی(حمله کننده)

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} r_1 + cdm_\alpha (\mathrm{mod}\, q) \qquad (۱۹)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} r_2 + edm_\beta (\mathrm{mod}\, q) \qquad (۲۰)$$

را محاسبه می‌کند و مقادیر زیر را منتشر می‌کند.

(m_α, r_1, s_1) و (m_β, r_2, s_2)

۳-۵-تصدیق کردن

$$g^{s_1} \equiv y^{r_1} r^{m_\alpha} (\mathrm{mod}\ \ p) \qquad (۲۱)$$

$$g^{s_2} \equiv y^{r_2} r^{m_\beta} (\mathrm{mod}\ \ p) \qquad (۲۲)$$

این دو امضای معتبر برای دو پیام مجزا تنها با اجرای یکبار پروتکل بدست می آیند

حال ثابت می کنیم این دو امضا (s_1, s_2) برای دو پیام (m_α, m_β) معتبرند

اثبات:

$$\begin{aligned}
g^{s_1} &\equiv g^{\tilde{s}_1 \tilde{r}_1^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{(x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1)\tilde{r}_1^{-1} r + cdm\alpha} \\
&\equiv g^{x\tilde{r}_1\tilde{r}_1^{-1} r_1 + \tilde{k}_1 \tilde{m}_1 b_1 \tilde{r}_1^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{xr_1 + \tilde{k}_1 b_1 m_\alpha \tilde{r}_1 r_1^{-1} ad \tilde{r}_1^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{xr_1} g^{\tilde{k}_1 b_1 m_\alpha ad + cdm_\alpha} \\
&\equiv y^{r_1} g^{(\tilde{k}_1 ab_1 d + cd) m_\alpha} \\
&\equiv y^{r_1} r_1^{m_\alpha}
\end{aligned}$$

و بهمین ترتیب برای (m_β, r_2, s_2) نیز اثبات می‌شود.

۴- مقاوم‌سازی در برابر حمله و ارائه طرح بهبود یافته

ما برای بهبود این طرح بهتر است این طرح را ساده‌تر کنیم یعنی پیام را در یک مرحله کور کنیم یعنی به جای محاسبه $(\tilde{m}_1, \tilde{m}_2)$، تنها $(\tilde{m}_1)$ را محاسبه و با آن کار کنیم و یا اینکه آنجایی که متقاضی پنج مقدار (a,b,c,d,e) را جهت کوری پیام انتخاب می‌کند به این پنج فاکتور یک مقدار f دیگر بیفزاییم و به صورت زیر عمل کنیم.

۴-۱- راه‌اندازی

مرحله راه اندازی مانند قبل انجام میشود یعنی امضاکننده $\tilde{k}_1, \tilde{k}_2, b_1, b_2$ را در Zq انتخاب می‌کند و مقادیر زیر را محاسبه می‌کند.

$$\tilde{r}_1 \equiv g^{\tilde{k}_1} \pmod{p} \qquad (۲۳)$$

$$\tilde{r}_2 \equiv g^{\tilde{k}_2} \pmod{p} \qquad (۲۴)$$

به طوری که $GCD(\tilde{r}_1, q) = 1$ و $GCD(\tilde{r}_2, q) = 1$ باشند آنگاه $(\tilde{r}_1, \tilde{r}_2, b_1, b_2)$ را برای متقاضی می‌فرستد.

۴-۲- کور کردن پیام

متقاضی بعد از دریافت $(\tilde{r}_1, \tilde{r}_2, b_1, b_2)$ شش مقدار (a,b,c,d,e,f) را انتخاب می‌کند و خصوصی نزد خود نگه می‌دارد و مقادیر زیر را محاسبه می کند

$$r_1 \equiv \tilde{r}_1^{\,ab_1} g^{\,c} \pmod{p} \qquad (۲۵)$$

$$r_2 \equiv \tilde{r}_2^{\,bb_2} g^{\,e} \pmod{p} \qquad (۲۶)$$

$$r \equiv (r^{\,d}{}_1 r_2^{\,f}) \pmod{p} \qquad (۲۷)$$

سپس پیام m را به ترتیب زیر کور می‌کند.

$$\tilde{m}_1 \equiv m\tilde{r}_1 2r^{-1}ad \pmod{q} \qquad (۲۸)$$

$$\tilde{m}_2 \equiv m\tilde{r}_2 2r^{-1}bf \pmod{q} \qquad (۲۹)$$

و $(\tilde{m}_1, \tilde{m}_2)$ را به امضاکننده می‌دهد.

۴-۳- امضا کردن

امضاکننده پس از دریافت $(\tilde{m}_1, \tilde{m}_2)$ به صورت زیر عمل می‌کند.

$$\tilde{s}_1 \equiv x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1 \pmod{q} \qquad (۳۰)$$

$$\tilde{s}_2 \equiv x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2 \pmod{q} \qquad (۳۱)$$

و $(\tilde{s}_1, \tilde{s}_2)$ را برای متقاضی می‌فرستد.

۴-۴- بازگشایی کوری

پس از رسیدن $(\tilde{s}_1, \tilde{s}_2)$ به متقاضی، متقاضی امضای معتبر s را برای پیام m به صورت زیر بدست می‌آورد.

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} \frac{r}{2} + cdm \pmod{q} \qquad (۳۲)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} \frac{r}{2} + efm \pmod{q} \qquad (۳۳)$$

$$s \equiv (s_1 + s_2) \pmod{q} \qquad (۳۴)$$

سپس متقاضی (m, r, s) را منتشر می‌کند.

۴-۵- تصدیق کردن

تصدیق کننده بررسی می‌کند که:

$$g^{\,s} \equiv y^{r} r^{m} \pmod{p} \qquad (۳۵)$$

۴-۶- اثبات موجودیت امضا

با توجه به طرح بهبود ارائه شده این حمله دیگر کارساز نخواهد بود چون دیگر نمی توان فاکتور r را از معادلات حذف کرد.

$$g^{s} \equiv g^{s_1+s_2}$$

$$\equiv g^{(\tilde{s}_1\tilde{r}_1^{-1}\frac{r}{2}+cdm)+(\tilde{s}_2\tilde{r}_2^{-1}\frac{r}{2}+efm)}$$

$$\equiv g^{((x\tilde{r}_1+\tilde{k}_1b_1\tilde{m}_1)\tilde{r}_1^{-1}\frac{r}{2}+cdm)+((x\tilde{r}_2+\tilde{k}_2b_2\tilde{m}_2)\tilde{r}_2^{-1}\frac{r}{2}+efm)}$$

$$\equiv g^{((x\tilde{r}_1+\tilde{k}_1b_1(m\tilde{r}_1 2r^{-1}ad))\tilde{r}_1^{-1}\frac{r}{2}+cdm)+((x\tilde{r}_2+\tilde{k}_2b_2(m\tilde{r}_2 2r^{-1}bf))\tilde{r}_2^{-1}\frac{r}{2}+efm}$$

$$\equiv g^{xr} g^{((\tilde{k}_1b_1a+c)d+(\tilde{k}_2b_2b+e)f)m} \equiv y^{r} r^{m}$$

۵- نتیجه‌گیری

با حمله ای که روی طرح لی، هوانگ و یانگ انجام شد، امنیت آن نقض گردید زیرا با انجام یکبار پروتکل امضا بین متقاضی و امضا کننده دو امضای معتبر برای دو پیام مجزا بدست آمد. بنابراین اگر این طرح را برای یک سیستم پرداخت الکترونیکی غیر قابل ردگیری بکاررگیرند، یک مشتری (همان متقاضی امضا) پس از اجرای یک فرآیند برای گرفتن یک پول الکترونیکی با بانک ، می‌تواند دو پول الکترونیکی معتبر بدست آورد که این باعث ورشکستگی بانک می‌شود و یا اینکه به طور مشابهی اگر طرح لی، هوانگ و یانگ برای ساخت یک سیستم رأی‌گیری الکترونیکی بی‌هویت استفاده شود، یک رأی‌دهنده (متقاضی) می‌تواند دو رأی الکترونیکی معتبر را بدست آورد و در نتیجه دو رأی ثبت کند. لذا نتایج محاسبه رأی‌گیری نادرست خواهد بود، با بهبود صورت گرفته این مقاله ، مشکلات طرح مذکور از بین خواهد رفت و امنیت آن تضمین می گردد. ضعف الگوریتم ارائه شده از انجا ناشی می شود که الگوریتم کوری آسیب پذیراست؛ چون r را با توان رساندن (r_1, r_2) با یک توان یعنی $r \equiv (r_1 r_2)^d \pmod{p}$ محاسبه کرده و حمله کننده می تواند r را محاسبه نکند و هر کدام از (r_1, r_2) را جدا گانه با به توان d رساندن در معادلات جایگزین r کند و حمله را انجام دهد. اما در الگوریتم بهبود یافته جدید برای رفع این مشکل فاکتور f را وارد می کنیم و r را به صورت $r \equiv (r^d{}_1 r_2{}^f) \pmod{p}$ محاسبه می کنیم و مشکل برطرف می شود.

سپاسگزاری

از حمایت های مالی و علمی مرکز تحقیقات مخابرات تقدیر و تشکر می شود.

۴- مراجع

[1] D.Chaum, "Blind signatures for untraceable payments", Advances in Cryptology CRYPTO' 82,pp.199-203,1983.
[2] C.I.Fan ,"Ownership-attached unblinding of blind signatures for untraceable electronic cash" , Information Sciences,vol.176.no.3,pp.263-284,2006.
[3] C.I.Fanand C.L.Lei,"An unlinkably divisible and intention attachable ticket scheme for runoff elections" , Journal of Network and Computer Applications ,vol.25,no.2,pp.93-107,2002.
[4] P.Horster ,M.Michels and H.Petersen, "Comment: cryptanalysis of the blind signatures based on the discretel ogarithm problem" , Electronics Letters ,vol.31,no.21,pp.1827,1995.
[5] J.Carmenisch, J.Piveteau and M.Stadler ,"Blind signatures based on the discrete logarithm problem" ,Advances in Cryptology-EUROCRYPT'94,pp.428-432,1994.
[6] L.Harn, "Cryptanalysis of the blind signatures based on the discrete logarithm problem", Electronics Letters,vol.31,no.14,pp.1136-1137,1995.
[7] H.Nurmi ,A.SalomaaandL .Santean ,"Secret ballot elections in computer networks" , Computers&Security,vol.10,no.6,pp.553-560,1991.
[8] C.C.Lee ,M.S.Hwang and W.P.Yang," A new blind signature based on the discrete logarithm problem for untraceability" , Applied Mathematics and Computation,vol.164,no.3,pp.837-841,2005.

Archvie of SID