



بهبود امنیت طرح امضای کور لی، هوانگ و یانگ

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

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

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^۱ و عدم ارتباطپذیر بودن^۲ را برآورده می‌کند. در این مقاله یک حمله به این طرح طراحی می‌شود به طوری که 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 می‌گردد امضای مذکور نا امن است. در نهایت با ارائه یک راهکار مناسب امنیت امضای مذکور در برابر حمله ارائه شده تامین می‌گردد.

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

۱- مقدمه

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 نمی‌کند [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

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 لینک پذیری و عدم جعل پذیری امضاها، امضاها کور در پروتکل های پرداخت - الکترونیکی غیر قابل ردگیری [1,2] و سیستمهای رأی گیری الکترونیکی بدون افشای هویت [3,4].

¹ untraceability
² unlinkability

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.

$$r_1 \equiv \tilde{r}_1^{ab} g^c \pmod{p} \quad (۳)$$

$$r_2 \equiv \tilde{r}_2^{bb} g^e \pmod{p} \quad (۴)$$

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

سپس متقاضی پیام m را با محاسبه:

$$\tilde{m}_1 \equiv m \tilde{r}_1^{-1} \pmod{q} \quad (۶)$$

$$\tilde{m}_2 \equiv m \tilde{r}_2^{-1} \pmod{q} \quad (۷)$$

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

۳-۲ امضا کردن

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

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

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

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

۴-۲ بازگشایی کوری

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

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} \pmod{q} \quad (۱۰)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} \pmod{q} \quad (۱۱)$$

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

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 (عدد صحیح) بار پرتکل امضاء با امضاکننده، حداکثر X امضای معتبر بدست آورد [1,2,3]. این مقاله وجود نقص امنیتی در طرح مرجع [8] را نشان می‌دهد به طوری که متقاضی با اجرای تنها یکبار پرتکل 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 می‌گردد. در بخش ۳ حمله به این طرح ارائه می‌شود و در بخش ۴ بهبود و مقاوم‌سازی طرح مذکور در برابر حمله ارائه می‌گردد. در بخش ۵ به نتیجه گیری پرداخته می‌شود 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 می‌گردد. 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. امضاکننده یک عدد صحیح x را بعنوان کلید خصوصی اش انتخاب می‌کند و $y \equiv g^x \pmod{p}$ و (p, q, g, y) را به عنوان کلید عمومی منتشر می‌کند.

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

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

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

و باید $GCD(\tilde{r}_1, q) = 1$ و $GCD(\tilde{r}_2, q) = 1$ باشند آنگاه

امضاکننده $(\tilde{r}_1, \tilde{r}_2, b_1, b_2)$ را برای متقاضی می‌فرستد.

۳-۳- امضا کردن

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

$$\tilde{s}_1 \equiv x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1 \pmod{q} \quad (17)$$

$$\tilde{s}_2 \equiv x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2 \pmod{q} \quad (18)$$

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

۳-۴- بازگشایی کوری

متقاضی (حمله کننده)

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} r_1 + cdm_\alpha \pmod{q} \quad (19)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} r_2 + edm_\beta \pmod{q} \quad (20)$$

را محاسبه می کند و مقادیر زیر را منتشر می کند.

$$(m_\beta, r_2, s_2) \quad \text{و} \quad (m_\alpha, r_1, s_1)$$

۳-۵- تصدیق کردن

$$g^{s_1} \equiv y^{r_1} r^{m_\alpha} \pmod{p} \quad (21)$$

$$g^{s_2} \equiv y^{r_2} r^{m_\beta} \pmod{p} \quad (22)$$

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:

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

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

۳-۵- تصدیق کردن

تصدیق کننده با بررسی کردن تساوی زیر پی به معتبر بودن یا جعلی بودن امضا می برد.

$$(12)$$

$$g^s \equiv y^r r^m \pmod{p}$$

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

در پروتکل که در بخش دوم توضیح داده شد اگر متقاضی درستکار نباشد می تواند 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 می شود.

۳-۱- راه اندازی

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

$$r_1 \equiv \tilde{r}_1^{ab_1} g^c \pmod{p} \quad \text{و}$$

$$r_2 \equiv \tilde{r}_2^{bb_2} g^e \pmod{p}$$

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

مقادیر زیر را محاسبه می کند.

$$r_1 \equiv (\tilde{r}_1^{ab_1} g^c)^d \pmod{p} \quad (13)$$

و

$$r_2 \equiv (\tilde{r}_2^{bb_2} g^e)^d \pmod{p} \quad (14)$$

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 می دهد:

$$\tilde{m}_1 \equiv m_\alpha \tilde{r}_1 r_1^{-1} ab \pmod{q} \quad (15)$$

و

$$\tilde{m}_2 \equiv m_\alpha \tilde{r}_2 r_2^{-1} ab \pmod{q} \quad (16)$$

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

۴-۳- امضا کردن

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

$$\tilde{s}_1 \equiv x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1 \pmod{q} \quad (30)$$

$$\tilde{s}_2 \equiv x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2 \pmod{q} \quad (31)$$

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

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 می آورد.

$$s_1 \equiv \tilde{s}_1 \tilde{r}_1^{-1} \frac{r}{2} + cdm \pmod{q} \quad (32)$$

$$s_2 \equiv \tilde{s}_2 \tilde{r}_2^{-1} \frac{r}{2} + efm \pmod{q} \quad (33)$$

$$s \equiv (s_1 + s_2) \pmod{q} \quad (34)$$

سپس متقاضی (m, r, s) را منتشر می کند.

۴-۵- تصدیق کردن

تصدیق کننده بررسی می کند که:

$$g^s \equiv y^r r^m \pmod{p} \quad (35)$$

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.

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

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

$$\equiv g^{((x\tilde{r}_1 + \tilde{k}_1 b_1 \tilde{m}_1) \tilde{r}_1^{-1} \frac{r}{2} + cdm) + ((x\tilde{r}_2 + \tilde{k}_2 b_2 \tilde{m}_2) \tilde{r}_2^{-1} \frac{r}{2} + efm)}$$

$$\equiv g^{((x\tilde{r}_1 + \tilde{k}_1 b_1 (m\tilde{r}_1^{-1} ad)) \tilde{r}_1^{-1} \frac{r}{2} + cdm) + ((x\tilde{r}_2 + \tilde{k}_2 b_2 (m\tilde{r}_2^{-1} bf)) \tilde{r}_2^{-1} \frac{r}{2} + efm)}$$

$$\equiv g^{x^r g^{((\tilde{k}_1 b_1 a + c)d + (\tilde{k}_2 b_2 b + e)f)m}} \equiv y^r r^m$$

۴-۴- مقاوم سازی در برابر حمله و ارائه طرح بهبود یافته

ما برای بهبود این طرح بهتر است این طرح را ساده تر 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 می کند به این پنج فاکتور یک مقدار f دیگر بیفزاییم و به صورت زیر عمل کنیم.

۴-۱- راه اندازی

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

$$\tilde{r}_1 \equiv g^{\tilde{k}_1} \pmod{p} \quad (23)$$

$$\tilde{r}_2 \equiv g^{\tilde{k}_2} \pmod{p} \quad (24)$$

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 می فرستد.

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 می کند و خصوصی نزد خود نگه می دارد و مقادیر زیر را محاسبه می کند

$$r_1 \equiv \tilde{r}_1^{ab_1} g^c \pmod{p} \quad (25)$$

$$r_2 \equiv \tilde{r}_2^{bb_2} g^e \pmod{p} \quad (26)$$

$$r \equiv (r_1^d r_2^f) \pmod{p} \quad (27)$$

سپس پیام m را به ترتیب زیر کور می کند.

$$\tilde{m}_1 \equiv m\tilde{r}_1^{-1} ad \pmod{q} \quad (28)$$

$$\tilde{m}_2 \equiv m\tilde{r}_2^{-1} bf \pmod{q} \quad (29)$$

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



- 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.SalomaandL .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.

۵- نتیجه گیری

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 بکارگیرند، یک مشتری (همان متقاضی امضا) پس از اجرای یک فرآیند برای گرفتن یک پول الکترونیکی با بانک، می تواند دو پول الکترونیکی معتبر بدست آورد که این باعث ورشکستگی بانک می شود و یا اینکه به طور مشابهی اگر طرح لی، هوانگ و یانگ برای ساخت یک سیستم رأی گیری الکترونیکی بی هویت استفاده شود، یک رأی دهنده (متقاضی) می تواند دو رأی الکترونیکی معتبر را بدست آورد و در نتیجه دو رأی ثبت کند. لذا نتایج محاسبه رأی گیری 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 پذیر است؛ 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 $r \equiv (r^d r_2^f) \pmod{p}$ 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

