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

روشی برای بهبود امنیت چند طرح امضای وکالتی آستانه

حمید رضا کاکائی مطلق
موسسه تحقیقاتی داده سنجی پیشرفته
دانشگاه امام حسین(ع)
hkakaei@yahoo.com

حمید رضا میمنی
دانشگاه تهران
maimani@ipm.ir

محمد باقری
دانشکده ریاضیات و رمز
دانشگاه امام حسین(ع)

چکیده: در یک طرح (t,n) امضای وکالتی آستانه، شخص صاحب امضا، گروهی n نفری از اشخاص معین را نماینده خود قرار می‌دهد به نحوی که در صورت توافق حداقل t نفر از اعضای گروه، به نمایندگی از صاحب امضا قادر باشند تا یک پیام را تحت عنوان صاحب امضا، امضا نمایند. طرح‌های مختلفی برای این نوع از امضا ارائه گردیده است؛ اما بخاطر ضعف امنیتی در طراحی این طرح‌ها، حملاتی برای آنها پیشنهاد گردیده است. ما در این مقاله راهکاری را ارائه نمودیم که بوسیله آن بتوان امنیت این طرح‌ها را بهبود بخشید. همچنین اثبات نموده‌ایم که امنیت طرح‌های بهبود یافته بر مبنای حل مساله لگاریتم گسسته می‌باشد.

واژه‌های کلیدی: امضای دیجیتال، امضای وکالتی، امضای آستانه‌ای، امضای وکالتی آستانه

۱- مقدمه

در یک امضای وکالتی صاحب امضا قابلیت امضا خود را به یک نماینده، وکالت می‌دهد و از این رو نماینده می‌تواند با عنوان صاحب امضا اقدام به امضای پیام‌ها نماید. گیرنده یک امضای وکالتی، هنگام تایید امضا، خود امضا و وکالت نماینده را بررسی می‌کند. اساس امضای وکالتی به این گونه است که صاحب امضا بر روی اطلاعات مربوط به واگذاری نمایندگی (هر گونه حکم نمایندگی) امضائی انجام می‌دهد و آن را برای نماینده ارسال می‌نماید، سپس نماینده از آن به عنوان کلید نمایندگی خود استفاده می‌کند یا اینکه از آن برای تولید کلید نمایندگی استفاده می‌کند. با توجه به اینکه کلید نمایندگی توسط امضای صاحب امضا بر روی «وکالت نامه»[1] نمایندگی ساخته می‌شود، تایید کننده امضای وکالتی می تواند موافقت صاحب امضا را از روی امضای وکالتی بررسی نماید.

با ترکیب دو حوزه رمزنگاری آستانه و امضای وکالتی، حوزه جدیدی با عنوان «امضای وکالتی آستانه»[2] مطرح گردیده است. یک طرح (t,n) امضای وکالتی آستانه به این معناست که در آن یک صاحب امضا قابلیت امضای خود را در اختیار یک گروه n نفره از نمایندگان امضا قرار می‌دهد تا در صورت موافقت حداقل t نفر از نمایندگان، این امکان ایجاد گردد که بتوانند از جانب صاحب امضا اقدام به تولید یک امضای وکالتی نمایند.

[1] Warrant
[2] Threshold proxy signature

اولین بار طرح امضای وکالتی آستانه توسط کیم [1] و زانگ [2] به طور همزمان و مستقل از هم ارائه گردید. طرح کیم ویژگی انکار ناپذیری را تامین می‌کند، اما طرح زانگ این ویژگی را برآورده نمی‌نماید. این ویژگی به این معنی است که گروه نمایندگان، امضا تولید شده توسط آن گروه نمایندگی را نمی‌توانند منکر شوند. با توجه به ویژگی انکار ناپذیری طرح کیم، این طرح بیشتر مورد توجه قرار گرفته است و طرح‌های بسیاری بر مبنای آن می‌باشد. پس از آن سان [3] طرح امضای وکالتی آستانه‌ای را معرفی نمود که در آن هویت نمایندگان امضا کننده نیز مشخص می‌باشد و آنرا یک طرح امضای وکالتی آستانه با امضا کننده شناخته شده نامید. هسو و همکارانش در [4] نشان دادند که در طرح سان اگر t نفر یا بیشتر از نمایندگان همدست شوند قادر خواهند بود تا کلید خصوصی سایر نمایندگان را بدست آورند. آنها طرحی پیشنهاد نمودند که این ضعف را نداشت. پس از آن یانگ و همکارانش در [5] روش پیشنهادی هسو را بهبود بخشیدند و طرحی پیشنهاد دادند که از نظر حجم محاسباتی و میزان تبادل اطلاعات نسبت به طرح هسو بسیار کمتر می‌باشد. با ارزیابی‌های امنیتی که توسط سایر محققان بر روی طرح‌های امضای وکالتی انجام گرفت؛ حملاتی برای جعل این گروه از امضاها پیشنهاد گردید[6-8].

ما در این مقاله ابتدا در بخش ۲ تعاریف اولیه بکار رفته در این مقاله را معرفی نموده‌ایم. پس از آن در بخش ۳ هر کدام از سه طرح مورد نظر و حمله انجام شده به آن را شرح نموده‌ایم. سپس در بخش ۴ ایده‌ای برای بهبود امنیت آن‌ها پیشنهاد نموده‌ایم. در بخش ۵ ایده مطرح شده را برای بهبود امنیت طرح‌های مذکور بکار برده و اثبات می‌کنیم که امنیت طرح‌های بهبود یافته به حل مساله لگاریتم گسسته وابسته می‌باشد. نتیجه‌گیری این مطالب نیز در بخش۶ آمده است.

۲- تعاریف اولیه

نمادهایی که مورد استفاده قرار خواهند گرفت:

p, q : دو عدد اول بزرگ که به صورت $p \mid q-1$ می‌باشند.

g : یک عضو از Z_p^*، که از مرتبه q می‌باشد.

p_i : نماینده i ام امضا است، که $i = 1,...,n$.

(x_0, y_0): زوج کلید خصوصی و عمومی صاحب امضا که در آن $y_o = g^{x_o} \bmod p$.

(x_i, y_i): زوج کلید خصوصی و عمومی نماینده امضا p_i که در آن $y_i = g^{x_i} \bmod p$.

$ASID$: شناسه افرادی که در تولید امضا مشارکت نموده‌اند.

$h()$: تابع درهم ساز یک سویه، مقاوم در برابر حمله تصادم.

CA : مرکز مورد اعتمادی است که وظیفه آن تایید کلیدهای عمومی افراد می‌باشد.

m_w : وکالت نامه نمایندگی که توسط صاحب امضا صادر می‌گردد و شامل اطلاعاتی مربوط به مشخصات صاحب امضا، شناسه نمایندگان، نوع نمایندگی و محدودیت‌های آنان، سطح آستانه، مدت همکاری و اطلاعاتی از این قبیل می‌باشد.

۲-۱- روش تولید کلید مشترک پدرسن

این روش توسط پدرسن در [9] ارائه گردید. در این روش برای گروه کلید خصوصی D و کلید عمومی g^D در نظر گرفته شده است. کلید خصوصی کاربران a_{i0} و کلید عمومی $g^{a_{i0}}$ می‌باشد و سهم آنها از کلید گروهی به صورت v_i است. اگر n نفر قصد داشته باشند تا کلید مشترک با آستانه t را بین خودشان تولید کنند، به صورت زیر رفتار می‌کنند:

۱- کاربر i به صورت تصادفی چندجمله‌ای از مرتبه $t-1$، $f_i(x) = a_{i,0} + a_{i,1}x + ... + a_{i,t-1}x^{t-1}$ را انتخاب می‌کند. سپس مقادیر $g^{a_{i,0}}, g^{a_{i,1}}, ..., g^{a_{i,t-1}}$ را محاسبه کرده و برای تمام کاربران ارسال می‌نماید. حال برای هر کاربر j مقدار $f_i(j) \bmod q$ را محاسبه و به طور محرمانه ارسال می‌نماید. این عملیات توسط تمام اعضاء گروه انجام می‌گردد.

۲- هر کاربر j می‌تواند پیام‌های ارسال شده از کاربر i را بررسی کرده و از صحت آن مطمئن گردد.

$$g^{f_i(j)} = g^{a_{i,0}} (g^{a_{i,1}})^{j} ... (g^{a_{i,t-1}})^{j^{t-1}} \bmod p \qquad (۱)$$

به این ترتیب هر کاربر می‌تواند صحت $f_i(j)$ های دریافت شده را بررسی نماید. در صورت صحیح بودن آنها، سهم کلید خود را به صورت زیر محاسبه می‌نماید.

$$v_j = \sum_{i=1}^{n} f_i(j) \bmod q \qquad (۲)$$

۳- اگر تابع $F(x)$ را به صورت زیر تعریف کنیم:

$$F(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod q \qquad (۳)$$

که در آن $a_k=\sum_{i=1}^{n}a_{i,k} \bmod q, 0\le k\le t-1$ باشد. آنگاه $F(j)=v_j$ و کلید خصوصی گروه نیز برابر $F(0)$ می‌باشد.

برای بازسازی کلید خصوصی گروه باید حداقل t نفر از اعضای گروه، سهم کلید خود را به اشتراک بگذارند. در این حالت با کمک درونیابی لاگرانژ کلید خصوصی گروه محاسبه می‌گردد.

$$D=\sum_{i=1}^{t}F(i)\lambda_{i0} \bmod q, \lambda_{i0}=\prod_{j=1,j\neq i}^{t}\frac{-j}{i-j} \bmod q \qquad (۴)$$

در این روش می‌توان مقدار کلید محاسبه شده را بصورت $g^D=\prod_{i=1}^{n}g^{a_{i0}} \bmod p$ مورد تصدیق قرار داد.

۳- چند طرح امضای وکالتی آستانه

در این قسمت چند طرح امضای وکالتی آستانه را معرفی می‌نماییم. مراحل انجام این طرح‌ها را می‌توان به سه مرحله کلی تقسیم نمود. مرحله اول تولید کلید نمایندگی، که در آن کلید نمایندگی برای اعضاء گروه تولید می‌گردد. مرحله دوم تولید امضای وکالتی و مرحله سوم نیز تایید امضای وکالتی می‌باشد. همچنین در این بخش برای هر کدام از طرح‌ها یکی از حملات پیشنهاد شده را معرفی می‌نماییم.

۳-۱- طرح (t,n) امضای وکالتی آستانه سان

۳-۱-۱- تولید کلید نمایندگی

۱- تولید کلید گروه: با کمک روش تسهیم کلید پدرسن کلید عمومی گروه را تولید کرده و بین خود به اشتراک می‌گذارند. در این طرح هر نماینده p_i چند جمله‌ای مربوط به خود را به صورت زیر ایجاد می‌نماید.

$$f_i(x)=x_i+a_{i,1}x+\ldots+a_{i,t-1}x^{t-1} \bmod q \qquad (۵)$$

سهم کلید کاربر i به صورت $s_i=f(i)$ محاسبه شده و به طور محرمانه برای وی ارسال می‌گردد. پس از اینکه این کار توسط تمام اعضای گروه انجام شد. مقادیر $A_j=g^{a_j} \bmod p$ برای $j=1,\ldots,t-1$ به عنوان ضرایب چند جمله‌ای نهایی به طور عمومی منتشر می‌گردد. از این رو کلید عمومی گروه $y_G=g^{a_0} \bmod p$ است که در آن $a_0=\sum_{i=1}^{n}x_i \bmod q$ می‌باشد و $y_G=\prod_{i=1}^{n}y_i \bmod p$ خواهد بود.

۲- تولید نمایندگی: صاحب امضا با انتخاب $k\in Z_q$ مقدار $K=g^k \bmod p$ را محاسبه می‌کند و با الحاق m_w و K مقدار $e=h(m_w,K)$ را بدست می‌آورد. سپس صاحب امضا، کلید نمایندگی را با انجام یک امضای اسنور[10] بر روی وکالت نامه صورت $\sigma=ex_0+k \bmod q$ محاسبه می‌نماید.

۳- تسهیم نمایندگی: برای تقسیم نمودن کلید نمایندگی σ در یک طرح با آستانه t، صاحب امضا مقادیر تصادفی $b_j, j=1,\ldots,t-1$ را انتخاب می‌کند و مقادیر $B_j=g^{b_j} \bmod p$ ها را به طور عمومی اعلام می‌نماید. سپس مقادیر $\sigma_i=f'(i)=\sigma+b_1i+\ldots+b_{t-1}i^{t-1}$ را برای $i=1,\ldots,n$ محاسبه نموده و برای هر کاربر، σ_i مربوطه را به طور محرمانه ارسال می‌نماید. ضمناً مقادیر (m_w,K) را به طور عمومی اعلام می‌دارد.

۴- تولید سهم نمایندگی: هر نماینده امضای p_i صحت (σ_i,m_w,K) را، با بررسی معادله زیر تائید می‌کند.

$$g^{\sigma_i}=y_0^{h(m_w,K)}K\prod_{j=1}^{t-1}B_j^{i^j} \bmod p \qquad (۶)$$

در صورتی که این معادله برقرار باشد، هر کاربر سهم کلید نمایندگی خود را به صورت زیر محاسبه می‌نماید.

$$\sigma_i'=\sigma_i+s_i\,h(m_w,K) \bmod q \qquad (۷)$$

۳-۱-۲- تولید امضای وکالتی

اگر زیرگروه t عضوی از گروه نمایندگان قصد تولید یک امضای وکالتی را داشته باشند با اجرای مراحل زیر می‌توانند یک امضای وکالتی تولید نمایند. فرض می‌کنیم که اعضای زیر گروه امضا کننده $p_i, i=1,\ldots,t$ باشند.

۱- زیرگروه امضا کننده، ابتدا به روش پدرسن کلیدی را بین خودشان به اشتراک می‌گذارند. هر نماینده p_i چندجمله‌ای خود را به صورت زیر تولید می‌نماید.

$$f_i''(x)=(x_i+c_{i,0})+c_{i,1}x+\ldots+c_{i,t-1}x^{t-1} \bmod q \qquad (۸)$$

با توجه به روش تولید کلید پدرسن اگر $c_0=\sum_{i=1}^{t}c_{i,0}$ و $C_j=g^{c_j} \bmod p$ باشد. کلید عمومی زیرگروه $y=g^{c_0}$ می‌باشد، و سهم هر عضو p_i از کلید خصوصی زیرگروه به صورت $s_i'=f''(i)$ و طبق رابطه زیر می‌باشد.

$$s_i'=\sum_{i=1}^{t}x_i+c_0+c_1i+\ldots+c_{t-1}i^{t-1} \bmod q \qquad (۹)$$

۲- هر نماینده این زیرگروه، امضای خود را بر روی متن m به صورت زیر محاسبه می‌نماید و به طور محرمانه برای سایر نمایندگان ارسال می‌نماید.

$$\gamma_i = s_i' y + \sigma_i' h(ASID, m) \bmod q \qquad (۱۰)$$

۳- هر عضو این زیرگروه صحت اطلاعات منتشر شده را با بررسی معادله زیر تایید می‌نماید.

$$g^{\gamma_j} = [(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i}) \times (y_G \prod_{i=1}^{t-1} A_i^{j^i})^{h(m_w,K)}]^{h(ASID,m)} \times [y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t} y_i)]^y \bmod p \qquad (۱۱)$$

۴- هرعضو زیرگروه، مقدار s را که در معادله زیر صدق کند، محاسبه می‌نماید.

$$s = f''(0) y + [f(0) + f'(0)] h(m, ASID) \qquad (۱۲)$$

محاسبه این مقدار با کمک درونیابی لاگرانژ برای γ_iها صورت می‌پذیرد. با انجام این کار امضای وکالتی آستانه‌ای به صورت $(m, s, y, K, m_w, ASID)$ تولید می‌گردد.

۳-۱-۳- تایید صحت امضای وکالتی

مراحل تایید صحت امضای وکالتی برای هر شخصی که یک $(m, s, y, K, m_w, ASID)$ امضای وکالتی را دریافت نماید.

۱- تایید کننده با توجه به موارد موجود در وکالت نامه m_w، صاحب امضا و افراد گروه نمایندگان را شناسایی می‌کند. سپس کلید عمومی نمایندگان را از CA دریافت می‌نماید.

۲- با توجه به $ASID$، تایید کننده، نمایندگان امضا کننده را خواهد شناخت که در اینجا همان $p_1, ..., p_t$ می‌باشند.

۳- تایید کننده، صحت امضای وکالتی را با بررسی معادله زیر انجام می‌دهد.

$$g^s = [y_0^{h(m_w,K)} K \prod_{i=1}^{n} y_i]^{h(ASID,m)} (y \prod_{i=1}^{t} y_i)^y \bmod p \qquad (۱۳)$$

۳-۱-۴- حمله به طرح امضای وکالتی آستانه سان

طرح امضا سان [3] در مقابل جعل امضا توسط صاحب امضای بداندیش ناامن می‌باشد. در این طرح یک صاحب امضای بداندیش قادر به تولید یک امضای وکالتی جعلی بر روی متن دلخواه m می‌باشد، به نحوی که بتواند ادعا نماید که نمایندگان گروه نمایندگی آن را تولید نموده‌اند. برای این منظور فرض می‌کنیم شناسه نمایندگانی که امضا جعلی از جانب آنها تولید می‌گردد $ASID = (p_1, p_2, ..., p_t)$. صاحب امضا ابتدا مقادیر تصادفی $\alpha, \beta \in Z_q^*$ را انتخاب می‌نماید و سپس مقادیر $K = (\prod_{i=1}^{n} y_i)^{-1} g^{\alpha}$ و $y = (\prod_{i=1}^{t} y_i)^{-1} g^{\beta}$ را محاسبه می‌نماید. در نهایت امضا جعلی به صورت زیر خواهد بود.

$$s = (\alpha + x_0 h(m_w, K)) h(ASID, m) + \beta y \qquad (۱۴)$$

هر دریافت کننده چندتایی $(m, s, y, K, m_w, ASID)$ با توجه به معادله تایید صحت امضا در طرح سان، آن را به عنوان یک امضای معتبر خواهد پذیرفت.

$$g^s = [g^{\alpha} g^{x_0 h(m_w,K)}]^{h(ASID,m)} (g^{\beta})^y \bmod p = [y_0^{h(m_w,K)} K \prod_{i=1}^{n} y_i]^{h(ASID,m)} (y \prod_{i=1}^{t} y_i)^y \bmod p \qquad (۱۵)$$

۳-۲- طرح (t,n) امضای وکالتی آستانه هسو

هسو در طرح امضای خود [4] این نکته را مطرح نمود که در سیستم‌های امضا همواره مرکزی وجود دارد که مورد اعتماد سیستم است و وظیفه مقدار دهی اولیه سیستم از قبیل تعیین مقادیر h, g, q, p را بر عهده دارد. در طرحی که توسط هسو و همکارانش ارائه گردیده است برای تولید کلید گروهی از این مرکز مورد اعتماد که آن را SA[1] می‌نامیم، کمک گرفته شده است.

۳-۲-۱- تولید کلید نمایندگی

۱- تولید کلید گروه: SA کلید خصوصی گروه X_G را انتخاب و کلید عمومی $Y_G = g^{X_G} \bmod p$ را محاسبه می‌نماید. سپس چندجمله‌ای $f(x) = X_G + a_1 x + ... + a_{t-1} x^{t-1} \bmod q$ را انتخاب می‌نماید که ضرایب آن به طور تصادفی تولید می‌گردد. سپس برای هر کاربر p_i سهم کلید را به صورت $\gamma_i = f(i)$ محاسبه کرده و به طور محرمانه ارسال می‌نماید. مقدار $\tau_i = g^{\gamma_i} \bmod p$ نیز به طور عمومی اعلام می‌گردد.

۲- تولید نمایندگی: صاحب امضا با انتخاب $k \in Z_q$ مقدار $K = g^k \bmod p$ را محاسبه می‌کند. سپس با الحاق m_w و K

[1] System Authority

مقدار $e=h(m_w,K)$ را بدست می‌آورد و سپس مقدار $\sigma=k+x_0h(m_w,K) \bmod q$ را محاسبه می‌کند.

۳- تقسیم نمایندگی: برای تقسیم نمودن کلید نمایندگی σ، در یک طرح با آستانه t، صاحب امضا مقادیر تصادفی $b_j, j=1,...,t-1$ را انتخاب می‌کند و مقدار $B_j=g^{b_j} \bmod p$ ها را به طور عمومی اعلام می‌نماید. سپس $\sigma_i=f'(i)=\sigma+b_1i+...+b_{t-1}i^{t-1}$ $i=1,...,n$ ها را برای محاسبه نموده و برای هر کاربر، σ_i مربوطه را به طور محرمانه ارسال می‌نماید. ضمناً مقادیر (m_w,K) به طور عمومی اعلام می‌گردد.

۴- تولید سهم نمایندگی: هر نماینده امضای p_i صحت (σ_i,m_w,K) را، با بررسی معادله زیر تایید می‌کند.

$$g^{\sigma_i}=y_0^{h(m_w,K)}K(\prod_{j=1}^{t-1}B_j^{i^j}) \bmod p \qquad (۱۶)$$

در صورتی که این معادله برقرار باشد، هر کاربر سهم کلید نمایندگی خود را به صورت زیر محاسبه می‌نماید.

$$\sigma_i'=\sigma_i+\gamma_i\,h(m_w,K) \bmod q \qquad (۱۷)$$

۳-۲-۲- تولید امضای وکالتی

اگر زیرگروه t عضوی از گروه نمایندگان قصد تولید یک امضای وکالتی را داشته باشند با اجرای مراحل زیر می‌توانند یک امضای وکالتی تولید نمایند. فرض می‌کنیم که زیر گروه امضا کننده $p_i, i=1,...,t$ می‌باشند.

۱- ابتدا هر نماینده p_i که قصد امضا متن را دارد عدد تصادفی $k_i \in Z_q^*$ را انتخاب و مقدار $r_i=g^{k_i} \bmod p$ را محاسبه نموده و منتشر می‌نماید.

۲- پس از انجام مرحله قبل توسط همه امضا کنندگان، هر عضو این زیرگروه امضای انفرادی خود را بر روی متن m به صورت زیر محاسبه می‌نماید.

$$s_i=k_iR+(L_i\sigma_i'+x_i)h(R,ASID,m) \bmod q \qquad (۱۸)$$

$$R=\prod_{i=1}^{t}r_i \bmod p \,،\, L_i=\prod_{j=1,j\neq i}^{t}(-j)(i-j)^{-1}$$

s_iها به طور محرمانه برای منشی گروه ارسال می‌گردد. منشی گروه یکی از اعضای زیرگروه امضا کننده است که وظیفه جمع آوری امضای انفرادی نمایندگان و تایید آن ها را بر عهده دارد.

۳- منشی گروه صحت اطلاعات منتشر شده را با بررسی معادله زیر تایید می‌نماید.

$$g^{s_i}=r_i^R(((y_0\tau_i)^{h(m_w,K)}\times (\prod_{j=1}^{t-1}B_j^{i^j})K)^{L_i}y_i)^{h(R,ASID,m)} \bmod p \qquad (۱۹)$$

۴- در صورتی که امضای انفرادی t عضو شرکت کننده در امضا تایید گردید، منشی گروه امضای وکالتی آستانه را به صورت $S=\sum_{i=1}^{t}s_i \bmod q$ محاسبه می‌نماید. در نتیجه امضای وکالتی آستانه‌ای $(m,R,S,K,m_w,ASID)$ تولید می‌گردد.

۳-۲-۳- تایید صحت امضای وکالتی

مراحل تایید صحت امضای وکالتی برای هر شخصی که یک $(m,R,S,K,m_w,ASID)$ امضای وکالتی را دریافت نماید.

۱- تایید کننده با توجه به موارد موجود در وکالت نامه m_w، صاحب امضا و افراد گروه نمایندگان را می‌شناسد. سپس کلید عمومی نمایندگان را از CA دریافت می‌نماید.

۲- با توجه به $ASID$ تایید کننده، امضا کنندگان را خواهد شناخت که بنا بر فرض امضا کنندگان $p_1,...,p_t$ هستند.

۳- تایید کننده، صحت امضای وکالتی دریافت شده را با بررسی معادله زیر انجام می‌دهد.

$$g^s=R^R[K(y_0Y_G)^{h(m_w,K)}\prod_{i=1}^{t}y_i]^{h(R,ASID,m)} \bmod p \qquad (۲۰)$$

۳-۲-۴- حمله به طرح امضای وکالتی آستانه هسو

این طرح امضا در مقابل همدستی صاحب امضا و SA، برای جعل امضا ناامن می‌باشد. در صورتی که صاحب امضا و SA با هم قصد جعل امضای وکالتی آستانه طرح هسو را داشته باشند قادر خواهند بود تا یک امضای وکالتی آستانه جعلی بر روی متن پیام m تولید نمایند، به نحوی که بتوانند ادعا نمایند، نمایندگان گروه نمایندگی آن را تولید نموده‌اند. برای تولید چنین امضائی اگر فرض کنیم $ASID=(p_1,...,p_t)$ شناسه نمایندگان گروه باشد و $\alpha,\beta \in Z_q^*$ به طور تصادفی انتخاب گردند، آنگاه مقادیر $K=(\prod_{i=1}^{t}y_i)^{-1}g^{\alpha}$ و $R=g^{\beta}$ محاسبه می‌گردند. با کمک SA مقدار X_G را بدست آورده و مقدار امضای جعلی را به صورت زیر محاسبه می‌نماید.

$$s=[\alpha+(x_0+x_G)h(m_w,K)]h(R,ASID,m)+\beta R \quad (۲۱)$$

هر دریافت کننده چندتایی $(m,R,S,K,m_w,ASID)$ با توجه به معادله تایید صحت امضا در طرح هسو، آن را به عنوان یک امضا معتبر خواهد پذیرفت.

$$\begin{aligned} g^s &= (g^\beta)^R[g^\alpha(y_0Y_G)^{h(m_w,K)}]^{h(R,ASID,m)} \bmod p \\ &= R^R[K(y_0Y_G)^{h(m_w,K)}\prod_{i=1}^{t}y_i]^{h(R,ASID,m)} \bmod p \end{aligned} \quad (۲۲)$$

۳-۳- طرح (t,n) امضای وکالتی آستانه یانگ

یانگ و همکارانش [5] با اعمال تغییراتی در طرح هسو [3]، طرح جدیدی پیشنهاد نموده‌اند که از نظر پیچیدگی محاسبات و حجم انتقال اطلاعات بهتر از آن است و در آن، مرحله تولید کلید گروه حذف شده است.

۳-۳-۱- تولید کلید نمایندگی

۱- تولید نمایندگی: صاحب امضا با انتخاب $k\in Z_q$ مقدار $K=g^k \bmod p$ را محاسبه می‌کند. سپس با الحاق m_w و K مقدار $e=h(m_w,K)$ را محاسبه می‌کند. سپس مقدار $\sigma=k+x_0h(m_w,K) \bmod q$ را بدست می‌آورد و مقادیر (σ,m_w,K) را اعلام می‌دارد.

۲- تولید سهم نمایندگی: هر نماینده امضا p_i صحت (σ,m_w,K) را، با بررسی معادله زیر تائید می‌کند.

$$g^\sigma = Ky_0^{h(m_w,K)} \bmod p \quad (۲۳)$$

در صورتی که این معادله برقرار باشد، هر کاربر از σ به عنوان کلید نمایندگی خود استفاده می‌نماید.

۳-۳-۲- تولید امضای وکالتی

اگر زیرگروه t عضوی از گروه نمایندگان قصد تولید یک امضای وکالتی را داشته باشند با اجرای مراحل زیر می‌توانند یک امضای وکالتی تولید نمایند. فرض می‌کنیم که زیر گروه امضا کننده $p_i, i=1,\ldots,t$ می‌باشند.

۱- ابتدا هر نماینده که قصد مشارکت در امضا را دارد عدد تصادفی $k_i\in Z_q^*$ را انتخاب و مقدار $r_i=g^{k_i} \bmod p$ را منتشر می‌نماید.

۲- پس از انجام مرحله قبل توسط همه امضا کنندگان، هر عضو زیرگروه امضای انفرادی خود را بر روی متن m به صورت زیر محاسبه می‌نماید

$$s_i=k_iR+(t^{-1}\sigma+x_i)h(R,ASID,m) \bmod q \quad (۲۴)$$

که در آن $R=\prod_{i=1}^{t}r_i \bmod p$ و t همان سطح آستانه امضا می‌باشد. s_iها به طور محرمانه برای منشی ارسال می‌گردد.

۳- منشی گروه، صحت اطلاعات دریافت شده را با بررسی معادله زیر تایید می‌نماید.

$$g^{s_i}=r_i^R((Ky_0^{h(m_w,K)})^{t^{-1}}y_i)^{h(R,ASID,m)} \bmod p \quad (۲۵)$$

در صورتی که معادله بالا برای تمام s_iها، صدق کند؛ منشی، امضای وکالتی را به صورت $S=\sum_{i=1}^{t}s_i \bmod q$ محاسبه می‌نماید. با انجام این کار امضای وکالتی آستانه‌ای $(m,R,S,K,m_w,ASID)$ تولید می‌گردد.

۳-۳-۳- تایید صحت امضای وکالتی

مراحل تایید صحت امضای وکالتی برای هر شخصی که یک $(m,R,S,K,m_w,ASID)$ امضای وکالتی را دریافت نماید، با انجام مراحل زیر ممکن است.

۱- تایید کننده با توجه به موارد موجود در وکالت نامه m_w، صاحب امضا و افراد گروه نمایندگان را می‌شناسد. سپس کلید عمومی نمایندگان را از CA دریافت می‌نماید.

۲- با توجه به $ASID$ تایید کننده، نمایندگان مشارکت کننده در امضا را خواهد شناخت.

۳- تایید کننده، صحت امضای وکالتی تولید شده را با بررسی معادله زیر انجام می‌دهد.

$$g^s=R^R[Ky_0^{h(m_w,K)}\prod_{i=1}^{t}y_i]^{h(R,ASID,m)} \bmod p \quad (۲۶)$$

در صورتی که معادله بالا برقرار باشد، امضا تایید خواهد شد.

۳-۳-۴- حمله به طرح امضای وکالتی آستانه یانگ

طرح امضای یانگ [5] در مقابل جعل امضا توسط صاحب امضای بداندیش ناامن است. در این طرح یک صاحب امضای بداندیش قادر به تولید امضای وکالتی جعلی بر روی متن دلخواه m می‌باشد، به نحوی که بتواند ادعا نماید که نمایندگان گروه نمایندگی آن را تولید نموده‌اند. برای این منظور فرض

می‌کنیم $ASID=(p_1,...,p_t)$ نمایندگانی باشند که قرار است امضای جعلی از جانب آنها تولید گردد. صاحب امضا ابتدا مقادیر تصادفی $\alpha,\beta\in Z_q^*$ را انتخاب و مقادیر $R=g^{\beta}$ و $K=(\prod_{i=1}^{t}y_i)^{-1}g^{\alpha}$ را محاسبه می‌نماید.

در نهایت امضای جعلی به صورت زیر محاسبه می‌گردد.

$$s=[\alpha+x_0h(m_w,K)]h(R,ASID,m)+\beta R \bmod q \qquad (۲۷)$$

هر دریافت کننده چندتایی $(m,R,S,K,m_w,ASID)$ با توجه به معادله تایید صحت امضا در طرح یانگ، آن را به عنوان یک امضا معتبر خواهد پذیرفت.

$$\begin{aligned} g^s &= g^{\beta R}(g^{\alpha}g^{x_0h(m_w,K)})^{h(R,ASID,m)} \bmod p \\ &= R^R[Ky_0^{h(m_w,K)}\prod_{i=1}^{t}y_i]^{h(R,ASID,m)} \bmod p \end{aligned} \qquad (۲۸)$$

۴- ایده پیشنهادی

برای بهبود امنیت طرح‌های بررسی شده از قضیه‌ای کمک گرفته می‌شود که ابتدا آن را معرفی و سپس اثبات می‌نماییم.

قضیه: فرض می‌کنیم شخصی توانایی محاسبه $K\in Z_p^*$ و $\beta\in Z_q$ را داشته باشد به نحوی که $KY_G^K=g^{\beta} \bmod p$ باشد. در این صورت این شخص توانایی محاسبه لگاریتم گسسته $Y_G=g^{x_G}$ را خواهد داشت.

برهان: چون $K\in Z_p^*$، لذا r وجود دارد به طوری که $K=g^r \bmod p$. بنابراین رابطه زیر برقرار است.

$$\begin{aligned} &Y_G^K K=g^{\beta} \Rightarrow g^{x_GK}g^r=g^{\beta} \bmod p \Rightarrow \\ &r+x_GK=\beta \bmod q \Rightarrow x_G=g^{-r}(\beta-r) \bmod q \end{aligned} \qquad (۲۹)$$

۵- بهبود امنیت طرح‌های امضای وکالتی آستانه

با استفاده از این قضیه می‌توان تغییراتی در طرح‌های مورد بررسی ایجاد نمود و امنیت آنها را به حل مساله لگاریتم گسسته وابسته نمود.

۵-۱- بهبود طرح امضای سان

چنانچه هر نماینده در مرحله تولید کلید نمایندگی، مقدار کلید نمایندگی خود را به صورت $\sigma_i'=\sigma_i+s_iK \bmod q$ تولید نماید و سایر مراحل تولید امضا بدون تغییر بماند، آنگاه هر نماینده گروه، امضای انفرادی سایر نمایندگان را با کمک رابطه زیر تایید می‌نماید.

$$\begin{aligned} g^{\gamma_i} &=[(y_0^{h(m_w,K)}K\prod_{j=1}^{t-1}B_j^{ij})(Y_G\prod_{j=1}^{t-1}A_j^{ij})^K]^{h(ASID,m)} \\ &\times[y(\prod_{j=1}^{t-1}C_j^{ij})(\prod_{j=1}^{t}y_j)]^y \bmod p \end{aligned} \qquad (۳۰)$$

در نتیجه امضای وکالتی به صورت زیر محاسبه خواهد شد.

$$s=f''(0)y+[f(0)K+f'(0)]h(m,ASID) \qquad (۳۱)$$

در مرحله تایید امضا نیز هر شخص تایید کننده قادر است تا امضا تولید شده را با کمک رابطه زیر تایید نماید.

$$g^s=[y_0^{h(m_w,K)}KY_G^K]^{h(ASID,m)}(y\prod_{i=1}^{t}y_i)^y \bmod p \qquad (۳۲)$$

در این صورت حمله کننده برای موفقیت در جعل امضا، ابتدا باید مقادیر تصادفی $\alpha,\beta\in Z_q^*$ را انتخاب نماید و سپس مقادیر $y=(\prod_{i=1}^{t}y_i)^{-1}g^{\beta}$ و $K=Y_G^{-K}g^{\alpha}$ را محاسبه نماید تا امضای جعلی به صورت زیر محاسبه گردد.

$$s=(\alpha+x_0h(m_w,K))h(ASID,m)+\beta y \qquad (۳۳)$$

اما همانطور که اثبات شد، محاسبه $K=Y_G^{-K}g^{\alpha}$ به معنی حل مساله لگاریتم گسسته است.

۵-۲- بهبود طرح امضای هسو

چنانچه هر نماینده در مرحله تولید امضای انفرادی، مقدار زیر را به عنوان امضای انفرادی خود محاسبه و معرفی نماید.

$$\gamma_i=k_iR+(L_i\sigma_i'+x_iK)h(R,ASID,m) \bmod q \qquad (۳۴)$$

آنگاه منشی گروه، امضای انفرادی شرکت کنندگان در امضا را با کمک رابطه زیر تایید می‌نماید.

$$\begin{aligned} g^{\gamma_i} &= r_i^R(((y_0S_i)^{h(m_w,K)}(\prod_{j=1}^{t-1}B_j^{ij}) \\ &\times K)^{L_i}y_i^K)^{h(R,ASID,m)} \bmod p \end{aligned} \qquad (۳۵)$$

سپس مقدار امضای وکالتی را همانند قبل به صورت $s=\sum_{i=1}^{t}\gamma_i \bmod q$ محاسبه نماید. در مرحله تایید امضا نیز هر شخص تایید کننده قادر خواهد بود تا امضای تولید شده را با کمک رابطه زیر تایید نماید.

$$\begin{aligned} g^s &= R^R[K(y_0Y_G)^{h(m_w,K)}\times \\ &(\prod_{i=1}^{t}y_i)^K]^{h(R,ASID,m)} \bmod p \end{aligned} \qquad (۳۶)$$

در این صورت حمله کننده برای موفقیت در جعل امضا باید $\alpha,\beta\in Z_q^*$ را به طور تصادفی انتخاب نماید و مقادیر

$R=g^{\beta}$ و $K=(\prod_{i=1}^{t} y_i)^{-K} g^{\alpha}$ را محاسبه کند. با کمک SA مقدار X_G را بدست آورد تا مقدار امضای جعلی را به صورت زیر محاسبه نماید.

$$s=[\alpha+(x_0+x_G)h(m_w,K)]h(R,ASID,m)+\beta R \quad (۳۷)$$

آنگاه هر دریافت کننده، چندتایی $(m,R,S,K,m_w,ASID)$ را به عنوان یک امضای معتبر خواهد پذیرفت. اما طبق آنچه بیان شد، محاسبه مقدار $K=(\prod_{i=1}^{t} y_i)^{-K} g^{\alpha}$ به معنی حل مساله لگاریتم گسسته می‌باشد.

۵-۳- بهبود طرح امضای یانگ

چنانچه هر نماینده در مرحله تولید امضای انفرادی، مقدار زیر را به عنوان امضای انفرادی خود محاسبه نموده و معرفی نماید.

$$\gamma_i=k_i R+(t^{-1}\sigma+x_i K)h(R,ASID,m) \bmod q \quad (۳۸)$$

آنگاه منشی گروه، امضای انفرادی اعضای شرکت کننده در امضا را با کمک رابطه زیر تایید می‌نماید.

$$g^{\gamma_i}=r_i^R((Ky_0^{h(m_w,K)})^{t^{-1}} y_i^K)^{h(R,ASID,m)} \bmod p \quad (۳۹)$$

سپس مقدار امضای وکالتی را همانند قبل به صورت $s=\sum_{i=1}^{t}\gamma_i \bmod q$ محاسبه نماید. در مرحله تایید امضا نیز هر شخص تایید کننده قادر خواهد بود تا امضای تولید شده را با کمک رابطه زیر تایید نماید.

$$g^s=R^R[Ky_0^{h(m_w,K)}(\prod_{i=1}^{t} y_i)^K]^{h(R,ASID,m)} \bmod p \quad (۴۰)$$

در این صورت صاحب امضا برای موفقیت در جعل امضا باید ابتدا مقادیر تصادفی $\alpha,\beta\in Z_q^*$ را انتخاب نماید و سپس مقادیر $K=(\prod_{i=1}^{t} y_i)^{-K} g^{\alpha}$ و $R=g^{\beta}$ را محاسبه نماید. تا امضای جعلی به صورت زیر محاسبه گردد.

$$s=[\alpha+x_0 h(m_w,K)]h(R,ASID,m)+\beta R \bmod q \quad (۴۱)$$

آنگاه هر دریافت کننده، چندتایی $(m,R,S,K,m_w,ASID)$ را به عنوان یک امضای معتبر خواهد پذیرفت. اما طبق آنچه در قبل بیان شد، محاسبه مقدار $K=(\prod_{i=1}^{t} y_i)^{-K} g^{\alpha}$ به معنی حل مساله لگاریتم گسسته می‌باشد.

۶- نتیجه گیری

با توجه به آنچه بیان گردید، روش‌های مطرح شده برای امضای وکالتی آستانه، در مقابل بعضی از حملات مطرح شده آسیب پذیر بودند. در این مقاله راهکاری را ارائه نمودیم که با اعمال آن پارامترهای امضا به نحوی به هم وابسته شدند که امکان جعل امضا ممکن نمی‌باشد و به این صورت طرح‌های مذکور را در مقابل این قبیل حملات ایمن نمودیم. ضمناً اثبات کردیم که امنیت این طرح‌ها در مقابل آن حملات وابسته به حل مساله لگاریتم گسسته می‌باشد.

۷- تشکر و قدردانی

در اینجا لازم می‌دانم از راهنمایی‌ها و ایده‌های مرحوم دکتر محمد باقری تشکر کنم.

۸- مراجع

[1] S. J. Kim, S. J. Park, D. H. Won, *Proxy Signatures, revisited*. ICICS'97, Lecture Notes in Computer Science, Vol. 1334. Springer-Verlag, Berlin Heidelberg New York 1997.

[2]. K. Zhang, *Threshold proxy signature schemes*, Information Security Workshop, Japan, 1997.

[3] H. M. Sun, *An efficient nonrepudiable threshold proxy signatures with known signers*, Computer Communications 22(8),1999.

[4] C.-L. Hsu, T.-S. Wu, and T.-C. Wu, *New nonrepudiable threshold proxy signature scheme with known signers*, The Journal of Systems and Software 58(2001), 2001.

[5]. C.-Y. Yang, S.-F. Tzeng and M.-S. Hwang, *On the efficiency of nonrepudiable threshold proxy signatures with known signers*, The Journal of Systems and Software 22(9),2003.

[6] Zuowen Tan, Zhuojun Liu, Mingsheng Wang, *On the Security of Some Nonrepudiable Threshold Proxy Signature Schemes*, Lecture Notes in Computer Science, Volume 3439, Jan 2005.

[7] Yang F-Y., Jan J-K., Jeng W-J., "Cryptanalysis of a threshold proxy signature with known signers", http://eprint.iacr.org/2004/313.

[8] Tan Z-W., and Liu Z-J., "Cryptanalysis of Threshold Proxy Signature Schemes", MM Research Preprints, MMRC, AMSS, Academia Sinica No. 23, 2004

[9] T. P. Pedersen. *A Threshold Cryptosystem without a Trusted Party*, Proc. Eurocrypt1991, Lecture Notes in Computer Science, Vol. 547. Springer-Verlag, Berlin Heidelberg New York 1991.

[10] Schnorr C.P., "Efficient identification and signatures for smart cards", Advances in Cryptology:Crypto_89, LNCS, 435, Springer-Verlag, 1990.