ارائهٔ یک طرح امضای وکالتی هویت‌گرا با استفاده از زوج‌نگارهای دوخطی

حمید ملا، محمد دخیل‌علیان و مهدی برنجکوب

دانشگاه صنعتی اصفهان

E-mail: hamidmala@gmail.com , mdalian@cc.iut.ac.ir , brnjkb@cc.iut.ac.ir

چکیده – در امضای وکالتی امضاکنندهٔ وکیل پیامهایی را از سوی موکل خود با کلید وکالت بگونه‌ای امضا می‌کند که وارسی‌کننده بتواند هویت امضا کنندهٔاصلی و صحت امضا را مشخص نماید.سیستمهای رمزنگاری کلید عمومی هویت‌گرا را می‌توان به عنوان جایگزین مناسبی برای سیستمهای رمز کلید عمومی گواهی‌گرا به ویژه هنگامی که مدیریت کلید کارامد و سطح امنیت متوسط لازم باشد، تلقی نمود. در این مقاله یک روش جدید برای امضای وکالتی هویت‌گرا با استفاده از زوج‌نگارهای دوخطی ارائه شده و امنیت وکارامدی روش مورد تحلیل قرار می‌گیرد.

کلید واژه- امضای دیجیتال، امضای وکالتی هویت‌گرا، زوج‌نگار دوخطی، سیستم رمز هویت‌گرا

۱- مقدمه

در یک سیستم کلید عمومی گواهی‌گرا، لازم است پیش از استفاده از کلید عمومی یک کاربر، گواهی وی وارسی شود. در نتیجه به زمان محاسبه و ذخیره‌سازی زیادی برای وارسی گواهی‌ها و ذخیرهٔ کلیدهای عمومی نیاز است. شامیر در سال ۱۹۸۴ برای نخستین بار مفهوم رمزنگاری هویت‌گرا[۱] را بمنظور ساده‌سازی فرآیند مدیریت کلید در رمزنگاری کلید عمومی گواهی‌گرا مطرح ساخت[۱]. ایدهٔ اصلی سیستمهای رمز هویت‌گرا این است که بتوان از اطلاعات شناسایی هر کاربر به عنوان کلید عمومی وی استفاده نمود. به عبارت دیگر در این سیستمها کلید عمومی هر موجودیت به جای اینکه از یک گواهی که توسط CA صادر شده است استخراج گردد، مستقیماً از نام، آدرس پست الکترونیکی، آدرس IP و... کاربر اقتباس می‌گردد. کلید خصوصی متناظر نیز توسط یک طرف سوم مورداعتماد که در اینجا مرکز تولید کلید[۲] ، KGC، خوانده می‌شود، ساخته و از طریق کانال امن دراختیار کاربر قرار داده می‌شود. شامیر در همان زمان یک الگوریتم امضای هویت‌گرا ارائه داد اما ابداع یک روش رمزنگاری هویت‌گرا تا سال ۲۰۰۱ به صورت یک مسئلهٔ حل‌نشده باقی ماند. در این سال Boneh و Franklin موفق به ابداع یک الگوریتم رمزگذاری هویت‌گرا با استفاده از زوج‌نگارهای دوخطی[۳] که از خم بیضوی استفاده می‌کنند شدند[۲]. زوج‌نگارهای دوخطی، شامل زوج‌نگارِ ویل[۴] و زوج‌نگارِ تیت[۵] اخیراً کاربردهای فراوانی در رمزنگاری یافته‌اند که مهمترین آنها ساختن روشهای رمزنگاری

[1] ID-based

[2] Key Generation Center
[3] Bilinear Pairings
[4] Weil Pairing
[5] Tate Pairing

هویت‌گراست[۲-۵].

مفهوم امضای وکالتی[1] نخستین بار در سال ۱۹۹۶ توسط Mambo ، Usuda و Okamoto ارائه گردید[۶]. در هر روش امضای وکالتی سه موجودیت شرکت دارند: امضاکنندهٔ اصلی یا موکل، امضاکنندهٔ وکیل و وارسی کننده. در این امضا، امضاکنندهٔ اصلی حق امضای خود را بنا به دلایلی همچون غیبت موقت، نداشتن وقت یا قدرت محاسباتی کافی و ... به امضاکنندهٔ وکیل واگذار می‌کند. امضای وکالتی کاربردهای فراوانی در سیستمهای توزیع‌شده، محاسبات شبکه‌ای و... یافته است. در چنین روشی امضاکنندهٔ اصلی با استفاده از کلید خصوصی خود اطلاعاتی را که بیانگر تفویض حق امضای خود است، امضا نموده و در اختیار وکیل قرار می‌دهد. این داده که آن را حکم[2] می‌نامیم متضمن شرایط وکالت مثلاً مدت وکالت و ... نیز خواهد بود که از سوی موکل تعیین می‌شود. وکیل نیز با استفاده از این اطلاعات و ترکیب آن با کلید خصوصی خود کلیدی به نام کلید وکالت می‌سازد و از آن برای امضا از طرف موکل خود استفاده می‌کند. این کلید بایستی با کلید خصوصی وکیل که از آن برای امضای پیامهای خود استفاده می‌کند تفاوت داشته باشد. امضای وکالتی نیز باید بگونه‌ای باشد که وارسی کننده با استفاده از یک معادلهٔ وارسی تغییر یافته و متفاوت از روش وارسیِ امضایِ معمول سیستم متقاعد شود که امضا توسط وکیل مجاز امضاکنندهٔ اصلی تولید شده است[۷].

بسته به اینکه امضاکنندهٔ اصلی نیز همچون امضاکنندگان وکیل قادر به تولید امضای وکالتی باشد یا نه، دو نوع امضای وکالتی وجود دارد: (۱)امضا بدون حمایت از وکیل، که در آن امضا کنندهٔ اصلی نیز می‌تواند امضای وکالتی تولید نماید و (۲) امضا با حمایت از وکیل که در آن هیچ کس به جز وکیل حتی امضا کنندهٔ اصلی نیز قادر به تولید امضای وکالتی نخواهد بود.

تولید کلید وکالت در حقیقت همان فرآیند تفویض امضاست. در مرجع [۶] از سه نوع تفویض امضا نام برده شده است: تفویض کامل، تفویض جزئی و تفویض با حکم و ضمانت‌نامه. در تفویض کامل، موکل کلید خصوصی خود را به وکیل واگذار می‌کند. در تفویض جزئی موکل با استفاده از کلید خصوصی خود، کلیدی به نام کلید امضای وکالتی ساخته و در اختیار وکیل قرار می‌دهد. این کلید باید بگونه‌ای باشد که وکیل نتواند از روی آن کلید خصوصی موکل را بدست آورد. در تفویض سوم، موکل وکالت‌نامه‌ای که در بردارندهٔ نام وکیل و موکل و شرایط وکالت است ترتیب داده و آن را با کلید خصوصی خود امضا می‌نماید و وکالت‌نامه و امضا شدهٔ آن را به وکیل خود می‌دهد. در این حالت وکیل خود اقدام به تولید کلید وکالت می‌نماید. ما در ادامه توجه خود را به امضای وکالتی با تفویض با حکم و ضمانت‌نامه معطوف می‌کنیم.

ویژگیهای یک امضای وکالتی امن به قرار زیر است[۸].

تمایزپذیری[3]:امضاهای وکالتی باید از امضاهای معمولی توسط هرکس قابل تمایز باشند.

وارسی‌پذیری : با داشتن امضای وکالتی، وارسی‌کننده باید بتواند از موافقت امضاکنندهٔ اصلی با پیام امضاشده اطمینان حاصل نماید.

جعل ناپذیری اکید[4]: وکیل تعیین شده می‌تواند برای امضاکنندهٔ اصلی امضای وکالتی تولید نماید اما امضاکنندهٔ اصلی و سایر موجودیتها که به وکالت گمارده‌نشده‌اند، نمی‌توانند امضای وکالتی تولید نمایند.

شناسایی پذیری اکید : باید هرکس قادر باشد هویت وکیل را از روی امضای وکالتی تعیین نماید.

انکار ناپذیری اکید[5] : هنگامی که یک وکیل یک امضای وکالتی معتبر از طرف موکل خود تولید می‌نماید، نباید

[1] Proxy Signature
[2] Warrant
[3] Distinguishability
[4] Strong non-forgeability
[5] Strong non-deniability

بتواند آن را چه نزد موکل وچه نزد طرف سوم انکار کند.

جلوگیری از سوءاستفاده : وکیل نمی‌تواند کلید امضا را برای مقاصدی غیر از تولید امضای وکالتی معتبر بکار برد. یعنی وی نمی‌تواند پیامهایی را که از سوی موکل، مجاز به امضای آنها نیست امضا نماید.

نخستین امضای وکالتی هویت‌گرابا امنیت قابل اثبات در سال ۲۰۰۴ توسط Xu، Zhang و Feng ارائه شده است. در این مقاله یک روش امضای وکالتی هویت‌گرا با هزینهٔ محاسباتی بسیار کمتر از روش آنها پیشنهاد می‌شود. در ادامه نخست زوج‌نگارهای دوخطی را معرفی می‌کنیم. سپس به تعریف دقیق امضای وکالتی هویت‌گرا می‌پردازیم و روش Xu و همکارانش را بیان می‌کنیم. آنگاه روش جدیدی برای امضای وکالتی هویت‌گرا پیشنهاد می‌کنیم. در پایان نیز ضمن ارائهٔ تحلیلی از امنیت و کارامدی پروتکل پیشنهادی، مقایسه‌ای با پروتکل Xu و همکاران انجام می‌شود.

۲- زوج‌نگارهای دوخطی

فرض کنید G_1 یک گروه دوریِ جمعی با مرتبهٔ اول q و G_2 نیز یک گروه دوریِ ضربی با همان مرتبه باشد. نیز فرض کنید P مولدی از گروه G_1 باشد. یک زوج‌نگار دوخطی نگاشتی به صورتِ $e: G_1 \times G_1 \longrightarrow G_2$ می‌باشد که دارای ویژگیهای زیر است:

۱- دوخطی بودن : برای هر دو عنصر $a,b \in Z_q^*$ داریم:

$$e(aP,bQ) = e(P,abQ) = e(bP,aQ)e(P,Q)^{ab} \quad (۱)$$

به عنوان یک نتیجه از این خاصیت به راحتی می‌توان نشان داد که برای هر $Q_1,Q_2 \in G_1$ داریم :

$$e(P,Q_1)e(P,Q_2) = e(P,Q_1+Q_2) \quad (۲)$$

۲- زوال‌ناپذیری[1]: وجود دارد $P,Q \in G_1$ بگونه‌ایکه $e(P,Q) \neq 1$.

۳- محاسبه‌پذیری: الگوریتم کارآمدی برای محاسبهٔ $e(P,Q)$ برای همهٔ $P,Q \in G_1$ وجود دارد.

در تعاریف زیر منظور از نمادِ $a \in_R A$ انتخاب یک عنصر از مجموعهٔ A به تصادف می‌باشد.

الف- مسئلهٔ معکوس زوج‌نگار دوخطی (BPIP[2]) : با داشتنِ $P \in G_1$ و $e(P,Q) \in G_2$ بدست آوردنِ Q مسئله‌ای سخت می‌باشد[۸]

ب- مسئلهٔ دیفی- هلمن محاسباتی (CDH[3]) در G_1 : با داشتن (P,aP,bP) به ازایِ $a,b \in_R Z_q^*$، محاسبهٔ abP یک مسئلهٔ سخت است؛ یعنی با هر الگوریتم احتمالاتیِ زمان- چندجمله‌ای، احتمال بدست آوردن آن بسیار ناچیز می‌باشد[۲].

ج- مسئلهٔ دیفی- هلمن تصمیمی (DDH[4]) در G_1 : با داشتن (P,aP,bP,cP) به ازایِ $a,b,c \in_R Z_q^*$، بررسی تساویِ $c = ab \bmod q$ مسئله‌ای ساده می‌باشد. زیرا تنها کافیست تساویِ $e(aP,bP) \stackrel{?}{=} e(P,cP)$ بررسی شود.

تعریف گروهِ گپ دیفی-هلمن (GDH[5]) : گروه مرتبه اولِ G_1 یک گروهِ GDH نامیده می‌شود اگر یک الگوریتم زمان-چندجمله‌ایِ کارآمد برای حل مسئلهٔ DDH در G_1 وجود داشته باشد و هیچ الگوریتم احتمالاتی زمان-چندجمله‌ای برای حل مسئلهٔ CDH با احتمال غیرقابل صرفنظر وجود نداشته باشد. دامنهٔ نگاشتهای دوخطی مورد استفاده در رمزنگاری باید نمونه‌هایی از گروههای GDH باشند. چنین گروههایی را می‌توان بر روی خمهای بیضوی فوق‌تکین[6] تعریف نمود. نگاشت e نیز برابر با یکی از دو نگاشتِ "تیت" یا "ویل" تعریف می‌شود. برای مطالعهٔ

[1] Non-degeneracy

[2] Bilinear Pairing Inversion Problem
[3] Computational Diffie-Hellman
[4] Decisional Diffie-Hellman
[5] Gap Diffie-Hellman
[6] Supersingular Elliptic Curve

دقیقتر می‌توانید به [۲] مراجعه کنید.

۳- امضای وکالتی هویت‌گرا

یک روش امضای وکالتی هویت‌گرا عبارتست از مجموعه الگوریتمِ $PS = (\mathcal{G}, \mathcal{K}, \mathcal{S}, \mathcal{V}, (\mathcal{D}, \mathcal{P}), \mathcal{PS}, \mathcal{PV})$ که هر کدام به صورت زیر مشخص می‌شوند[۹].

الگوریتم $\mathcal{G}$: مرکز، عدد تصادفیِ $s \in Z_q^*$ را به عنوان کلید خصوصی خود انتخاب و $P_{pub} = sP$ را محاسبه و پارامترهای عمومی سیستم را به صورت $params = \{G_1, G_2, e, q, P, P_{pub}, H\}$ اعلام و s را بعنوان کلید اصلی پنهان نگه می‌دارد. H تابع درهمی است به صورتِ $H : \{0,1\}^* \longrightarrow G_1$.

الگوریتم $\mathcal{K}$:هر کاربر اطلاعات شناسایی خود یعنی ID را به مرکز اعلام و خود را برای وی احراز اصالت می‌نماید. مرکز کلید خصوصی کاربر را به صورت $d_{ID} = sQ_{ID} = sH(ID)$ محاسبه و از طریق کانال امن در اختیار وی قرار می‌دهد.

الگوریتم $\mathcal{S}$: الگوریتم امضای معمول سیستم است که کلید امضای موکل یعنی d_d و پیام m_w را اخذ کرده و امضای w که آن را حکم می‌نامیم برمی‌گرداند. پیام m_w شامل هویت وکیل (ID_p)، و شرایطی که وکیل تحت آن مجاز به صدور امضاست می‌باشد.

الگوریتم $\mathcal{V}$: الگوریتم وارسی امضای معمول سیستم است که با اخذ هویت موکل، پیام m_w و حکم w امضای موکل را وارسی می‌کند.

الگوریتمهای $(\mathcal{D}, \mathcal{P})$: الگوریتمهای تخصیص وکیل‌اند. اگر هویت موکل و هویت وکیل را به ترتیب با ID_d و ID_p نمایش دهیم، الگوریتم $\mathcal{D}$ ورودیهای ID_d و ID_p و کلید خصوصی موکل (d_d)، و پیام m_w و حکم w را اخذ می‌کند. $\mathcal{P}$ نیز علاوه بر ID_d و ID_p کلید خصوصی وکیل (d_p)را نیز اخذ می‌کند. نتیجهٔ تعامل این دو الگوریتم کلید وکالت یا skp می‌باشد که کاربر ID_p از آن برای امضا از طرف ID_d استفاده خواهد کرد. این کلید تنها در اختیار ID_p باقی خواهد ماند.

الگوریتم $\mathcal{PS}$: الگوریتم امضای وکالتی است که با اخذ skp و پیام m و حکم w، امضای وکالتی $psig$ را برمی‌گرداند.

الگوریتم $\mathcal{PV}$: الگوریتم وارسی امضای وکالتی است که با اخذ هویت موکل، پیام m، حکم w و امضای وکالتی $psig$ اعتبار امضای وکالتی را بررسی می‌کند.

۴- امضای‌وکالتیXu، Zhang و Feng

در این روش که در سال ۲۰۰۴ ارائه شده است برای امضای معمول سیستم از روش SOK-IBS[1] استفاده می‌شود[۱۰]. مجموعه الگوریتمهای PS در این روش به صورت زیر تعریف می‌شود.

الگوریتم $\mathcal{G}$: فرض کنید k پارامتر امنیتی سیستم و G_1 یک گروه GDH با مرتبهٔ اول $q \geq 2^k$ با مولد P باشد. $e : G_1 \times G_1 \longrightarrow G_2$ نیز یک نگاشت دوخطی است. کلید اصلی مرکز برابر با $s \in Z_q^*$ انتخاب و کلید عمومی وی برابر با $P_{pub} = sP$ اعلام می‌شود. توابع درهمساز $H_1, H_2, H_3 : \{0,1\}^* \longrightarrow G_1$ و نیز تابع درهمِ $H_4 : \{0,1\}^* \longrightarrow Z_q^*$ بطور عمومی اعلام می‌شوند.

الگوریتم $\mathcal{K}$: کلید خصوصی کاربری با هویت ID برابر با $d_{ID} = sH_1(ID) = sQ_{ID} \in G_1$ از طریق کانال امن به وی ابلاغ می‌شود.

سایر مراحل طبق شکل ۱ خلاصه شده است. منظور از $r \in_R Z_q^*$ انتخاب عنصری از مجموعهٔ Z_q^* به تصادف می‌باشد. اگر هویت امضاکنندهٔ اصلی را با ID_d و زوج کلید عمومی/خصوصی وی را با d_d / Q_d و به همین ترتیب هویت وکیل و کلیدهای او را با ID_pو d_p / Q_p نمایش دهیم روند مراحل طبق شکل ۱ خواهد بود. با بررسی بیشتر

[1] Sakai-Ogishi-Kasahara Identity Based Signature

original signer

$r_d \in_R Z_q^*$

$U_d = r_d P$

$H_d = H_2(ID_d, m_w, U_d)$

$V_d = d_d + r_d H_d$

$\xrightarrow{m_w, w = (U_d, V_d)}$ **proxy signer**

$H_d = H_2(ID_d, m_w, U_d)$

$e(P, V_d) \stackrel{?}{=} e(P_{pub}, Q_d) e(U_d, H_d)$

$skp = H_4(ID_d, ID_p, m_w, U_d) d_p + V_d$

$r_p \in_R Z_q^*$

$U_p = r_p P$

$H_p = H_2(ID_p, m, U_p)$

$V_p = skp + r_p H_p$

verifier $\xleftarrow{m, psig = \{m_w, ID_p, U_d, U_p, V_p\}}$

$$\begin{cases} H_d = H_2(ID_d, m_w, U_d) \\ H_p = H_2(ID_p, m, U_p) \end{cases}$$

verification : $e(P, V_p) \stackrel{?}{=} e(P_{pub}, Q_p)^{H_4(ID_d, ID_p, m_w, U_d)} e(P_{pub}, Q_d) e(U_p, H_p) e(U_d, H_d)$

شکل ۱: روش امضای وکالتی هویت‌گرای Xu، Zhang و Feng

این روش می‌توان دریافت که این شیوه نیازمندیهای شش‌گانهٔ امضای وکالتی امن را برآورده می‌سازد اما از حیث کارآمدی تفاوت چندانی با بدیهی‌ترین روش امضای وکالتی که در سناریوی زیر بیان می‌شود ندارد: موکل وکالت‌نامه‌ای که در حقیقت همان m_w است، برای وکیل خود با درج نام وی و شرایط وکالت تنظیم و آن را با کلید خصوصی خود امضامی‌کند. نتیجهٔ این عمل، تولید حکمِ w می‌باشد. وکیل نیز هر زمان که خواست از طرف موکل خود پیامی همچون m را امضانماید، وکالت‌نامهٔ خود را نیز همراه پیام امضاشده ارسال می‌کند. وارسی کننده نیز ابتدا امضای وکالت‌نامه را وارسی می‌کند و سپس در صورت تأیید با استفاده از هویت وکیل که در وکالت‌نامه ذکرشده‌است، امضای پیام m را نیز وارسی می‌نماید. با این سناریو و استفاده از روش امضای SOK که وارسی آن به محاسبهٔ یک تابع درهم و سه زوج‌نگار نیاز دارد، جمعاً به محاسبهٔ دو تابع درهم و شش زوج‌نگار نیازخواهیم داشت. وارسی در روش مذکور منوط به محاسبهٔ دو مقدار درهم و پنج زوج‌نگار شده‌است یعنی تنها یک زوج‌نگار کم شده است. اما مزیت اصلی این روش نسبت به سناریوی فوق ، تفاوت کلید امضای وکالت و کلید خصوصی وکیل می‌باشد.

۵- امضای وکالتی جدید

اکنون با استفاده از روش امضای هویت‌گرای Hess، به عنوان امضای معمول سیستم یک روش امضای وکالتی هویت‌گرا با کارآمدی بسیار بهتر نسبت به روش Xu و همکاران پیشنهاد می‌کنیم. اما پیش از آن لازم است که روش امضای Hess معرفی گردد.

۵-۱- امضای هویت‌گرای Hess

در این روش نحوهٔ تعیین کلیدهای مرکز و کاربران همچون قبل است [۱۲]. برای امضا کردن پیام m، امضاکننده عدد k را به تصادف از مجموعهٔ Z_q^* انتخاب و r_A و c_A را به

original signer

$k \in_R Z_q^*$

$r_d = e(P,P)^k$

$c_d = H(m_w, r_d)$

$U_d = c_d.d_d + k.P$

$\xrightarrow{m_w, w = (c_d, U_d)}$ proxy signer

$r_d = e(U_d, P)e(Q_d, P_{pub})^{-c_d}$

$c_d \overset{?}{=} H(m_w, r_d)$

$skp = c_d.d_p$

$k_p \in_R Z_q^*$

$r_p = e(P,P)^{k_p}$

$c_p = H(m, r_p r_d)$

$U_p = c_p.skp + k_p.P$

verifier $\xleftarrow{m, psig = \{m_w, U_d, U_p, c_p, r_d\}}$

$c_d = H(m_w, r_d)$

$r_p.r_d = e(Up + U_d, P)e(Q_d + c_p Q_p, P_{pub})^{-c_d}$

$c_p \overset{?}{=} H(m, r_p.r_d)$

شکل ۲ : روش امضای وکالتی پیشنهادی

صورت $r_A = e(P,P)^k$ و سپس $c_A = H(m, r_A)$ و $U_A = c_A d_A + kP$ را محاسبه می‌نماید. آنگاه $m, (c_A, U_A)$ را به عنوان پیام و امضای آن برای وارسی کننده ارسال می‌کند. وارسی کننده نیز پس از محاسبهٔ $e(U_A, P)e(Q_A, P_{pub})^{-c_A} = r_A'$ که انتظار داریم در صورت صحت امضا برابر با r_A باشد، تساوی $c_A \overset{?}{=} H(m, r_A')$ را بررسی می‌کند. در صورت برقراری تساوی، امضا قبول و درغیراینصورت رد می‌شود، زیرا با استفاده از خاصیت دوخطی بودن زوج‌نگارِ e و رابطهٔ (۲) داریم:

$$\begin{aligned} r_A' &= e(U_A, P)e(Q_A, P_{pub})^{-c_A} \\ &= e(c_A d_A + kP, P)e(-c_A sQ_A, P) \\ &= e(c_A d_A + kP - c_A d_A, P) \\ &= e(kP, P) = e(P,P)^k = r_A \end{aligned}$$

۲-۵ تشریح روش امضای پیشنهادی

روش پیشنهادی در شکل ۲ نشان داده شده‌است.نامگذاری پارامترها همچون روش Xu انتخاب شده است. در این روش نخست موکل، وکالت‌نامهٔ m_w را با کلید خصوصی خود و طبق روش Hess امضا می‌کند و حکم w را تولید می‌نماید و هر دو را برای وکیل خود ارسال می‌کند. وکیل نیز طبق همان روش عمل وارسی را انجام می‌دهد. پس از اطمینان از صحت امضای موکل، کلید وکالت را برابربا

$$skp = c_d.d_p \qquad (۳)$$

محاسبه می‌کند که در آن c_d قسمتی از حکم صادره از سوی موکل است و d_p کلید خصوصی وکیل است. بنابراین کلید وکالت تنها در تملک وکیل قرارمی‌گیرد. پس از ساختن کلید وکالت نوبت به انجام امضای وکالتی از طرف موکل بر روی پیام m می‌رسد. در این مرحله با جایگزینی

$r_p r_d$ به جای r_p در محاسبهٔ c_p و نیز استفاده از کلید وکالت به جای d_p در محاسبهٔ U_p، امضای وکالتی به صورتِ

$$psig =< m_m, U_p, U_d, c_p, r_d > \quad (۴)$$

به وارسی‌کننده اعلام می‌شود. وی نخست $c_d = H(m_w, r_d)$ را محاسبه می‌کند و سپس با محاسبهٔ دو زوج‌نگار به صورت زیر، $r_p r_d$ را محاسبه می‌نماید:

$$r_p.r_d = e(Up + U_d, P)e(Q_d + c_p Q_p, P_{pub})^{-c_d} \quad (۵)$$

سپس عمل وارسی نهایی به صورتِ

$$c_p \overset{?}{=} H(m, r_p.r_d) \quad (۶)$$

انجام می‌شود. در صورت تساوی، امضای مورد نظر به عنوان یک امضای وکالتی معتبر توسط ID_p، از طرف ID_d شناخته و درغیر اینصورت رد می‌شود. زیرا با استفاده از خاصیت دوخطی بودن زوج‌نگار e داریم :

$$\begin{aligned} & e(U_p + U_d, P)e(Q_d + c_p Q_p, P_{pub})^{-c_d} \\ &= e(c_p.skp + k_p P + c_d d_d + kP, P) \\ &\times e(d_d + c_p d_p, P)^{-c_d} \\ &= e(c_p.c_d d_p + k_p P + c_d d_d + kP, P) \\ &\times e(-c_d d_d - c_d c_p d_p, P) \\ &= e(k_p P + kP, P)e(0, P) \end{aligned}$$

۳-۵- تحلیل امنیت و کارآمدی روش پیشنهادی

کارآمدی روش پیشنهادی از روش Xu به خصوص در مراحل وارسی بسیار بهتر است. اگر پروتکل را به چهار قسمت "امضای وکالت‌نامه و صدور حکم"، "وارسی حکم و تولید کلید وکالت"، "تولید امضای وکالتی"و "وارسی نهایی" تقسیم کنیم، جدول ۱ مقایسهٔ دقیقی از تحلیل هزینه و کارآمدی دو روش بدست می‌دهد. در این جدول M_{G_1} بیانگر ضرب اسکالر در میدان G_1 است. H نشاندهندهٔ تابع درهمسازی است که یک رشتهٔ باینری با طول دلخواه را به نقطه‌ای از خم بیضوی می‌نگارد. A_{G_1}

جدول(۱): مقایسهٔ کارآمدی روش پیشنهادی و روش

مرحله/روش	Xu و...	پیشنهادی
امضای وکالتنامه	$2M_{G_1} + H + A_{G_1}$	$3M_{G_1} + H + A_{G_1} + e$
وارسی وکالتنامه و تولید کلید وکالت	$3P + M_{G_1} + 2H + A_{G_1}$	$2P + 2M_{G_1} + H + e$
تولید امضای وکالتی	$2M_{G_1} + H + A_{G_1}$	$3M_{G_1} + H + A_{G_1} + e$
وارسی نهایی	$5P + M_{G_1} + 2H + e$	$2P + 2M_{G_1} + 2H + 2A_{G_1} + e$

جمع در میدان G_1 و P نیز نمایانگر زوج‌نگار و e نشاندهندهٔ نمارسانی پیمانه‌ای می‌باشد. از سایر محاسبات که هزینهٔ کمتری دارند صرف‌نظر شده است. در این میان پرهزینه ترین عملیات، محاسبه زوج‌نگار و ساده‌ترین عملیات نمارسانی می‌باشد[۲]. توجه نمایید که در این پروتکل لازم نیست برای محاسبهٔ r_d یا r_p هر بار یک زوج‌نگار محاسبه گردد زیرا کافیست که تنها یک بار $e(P,P)$ محاسبه شود و سپس با یک نمارسانی ساده در G_2 حاصل r_d یا r_p بدست می آید.

اگرچه Xu و همکارانش اثباتی برای امنیت روش خود ارائه داده‌اند[۱۱] اما اثبات امنیت آنها طبق مدل پیشگویی تصادفی[1] صورت گرفته است. اثبات امنیت در این مدل یعنی فرض اینکه توابع درهم مورد استفاده در پروتکل از دید دشمن، جعبه سیاه به نظر برسند، به هیچ وجه تضمین کنندهٔ امنیت یک پروتکل نیست[۱۳].

[1] Random Oracle Model

به راحتی می توان مشاهده نمود که وجود حکم در روش پیشنهادی متضمن نیازمندیهای امنیتیِ تمایزپذیزی، وارسی‌پذیری ، اکیداًقابل شناسایی بودن و عدم سوءاستفادهٔ وکیل می‌باشد. روش پیشنهادی، ویژگیِ ، اکیداًغیرقابل انکار بودن را نیز از روش امضایِ Hess به ارث می‌برد. ما در ادامه مهمترین ویژگی امضای وکالتی یعنی "اکیداًغیر قابل جعل بودن" را با تفصیل بیشتر مورد بررسی قرار می‌دهیم.

۵-۳-۱- حصول ویژگی اکیداًغیر قابل جعل بودن

واضح است که خودِ موکل نسبت به سایر کاربران سیستم از امکانات بیشتری برای جعل یک امضای وکالتی از سویِ وکیل خود برخوردار است. نشان می‌دهیم که حتی موکل نیز قادر به جعل امضای وکالتیِ وکیل نیست. فرض کنید موکل بخواهد یک امضای وکالتی جعلی از طرف موکل بر روی پیام m انجام دهد. تنها چیزی که وی به آن دسترسی ندارد کلید خصوصی وکیل (d_p)و کلید وکالتِ skp است. وی عدد تصادفیِ k_p را انتخاب کرده و به تبع آن r_p و c_p را محاسبه می‌کند. اکنون وی باید U_p را چنان بیابد که با قرار گرفتن در رابطهٔ (۵) ، $r_p.r_d$ صحیح را بدست دهد و بنابراین برای یافتن U_p باید معادلهٔ

$$e(U_p, P) = a \qquad (۷)$$

که یک مسئلهٔ BPIP است، حل شود. واضح است که در معادلهٔ فوق a برابر است با :

$$a = e(U_d, P)^{-1} e(Q_d + c_p Q_p, P_{pub})^{c_d} . r_p r_d$$

و بنابراین برای جعل امضای وکالتی لازم است که مسئله سختِ BPIP حل شود. به طریق مشابه می‌توان نشان داد که وکیل نیز قادر به جعل وکالت‌نامه نیست.

۵-۳-نتیجه‌گیری

در این مقاله یک پروتکل امضای وکالتی در محیط هویت‌گرا با استفاده از زوج‌نگارهای دوخطی پیشنهاد شد. هزینهٔ محاسباتی روش پیشنهادی به ویژه در مرحلهٔ وارسی که تعداد زوج‌نگارهای کمتری نیاز دارد از روش Xu و همکاران که در سال ۲۰۰۴ ارائه شده بسیار بهتر است. همچنین نشان داده شد که با فرض سخت بودن "مسئلهٔ محاسبهٔ معکوس زوج‌نگار دوخطی"، امضای وکالتی پیشنهادی حتی بوسیلهٔ موکل نیز غیرقابل جعل می‌باشد.

مراجع

[1] A. Shamir, *Identity-based Cryptosystems and Signature Schemes*, Proceedings of CRYPTO'84, LNCS 196, pages 47-53, Springer-Verlag,1984.

[2] D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Proceedings of CRYPTO 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[3] D. Boneh, B. Lynn, and H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology - Proceedings of ASIACRYPT 2001, LNCS 2248, pages 566-582, Springer-Verlag, 2001.

[4] A. Joux, *One Round Protocol for Tripartite Diffie-Hellman*, Algorithmic Number Theory Symposium { Proceedings of ANTS 2002, LNCS 1838, pages 385{394, Springer-Verlag, 2000.

[5] D. Boneh and X. Boyen, *Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles*, Advances in Cryptology - Proceedings of EUROCRYPT 2004, LNCS 3027, pages 223-238, Springer-Verlag, 2004.

[6] M. Mambo, K. Usuda and E. Okamoto, *Proxy signatures for delegating signing operation*, Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, pp.48-57, 1996.

[7] F. Zhang, R. Safavi-Naini and C. Lin , *New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings*, Cryptology ePrint Archive, Report 2003/104.

[8] C. Lin and T. Wu , *An Identity-based Ring Signature Scheme from Bilinear Pairings*, Proc. of ACISP2001, LNCS 2119, pp.474-486, Springer Verlag, 2001.

[9] B. Lee, H. Kim and K. Kim, *Secure mobile agent using strong non-designated proxy signature*, Proc. of ACISP2001, LNCS 2119, pp.474-486, Springer Verlag, 2001.

[10] J. Xu, Z. Zhang, D. Feng. *ID-Based Proxy Signature Using Bilinear Pairings*, available at http://eprint.iacr.org/2004/206/

[11] R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, Proc. of SCIS'00, Okinawa, Japan, Jan. pp. 26-28, 2001.

[12] F. Hess, *Efficient Identity Based Signature Schemes Based on Pairings*, Selected Areas in Cryptography, Proceedings of SAC 2002, LNCS 2595, pages 310-324, Springer-Verlag, 2002.

[13] R. Canetti, O. Goldreich and S. Halevi, *The Random Oracle Methodology, Revisited* , Proceedings of 30th Annual ACM Symposium on the Theory of Computing, pages 209-218, May 1998, ACM