مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۳۱- ۲۵

ارائه یک طرح امضای وکالتی آستانه با قابلیت ابطال سریع جدید در چک الکترونیکی

گیلاندخت مفسر باقری[۱]، محمد بهشتی آتشگاه[۲]، رضا ابراهیمی آتانی[۳*]

۱ - کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه گیلان ۲- کارشناسی ارشد، دانشگاه صنعتی شریف

۳- استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان

(دریافت۹۱/۱۰/۲۵ پذیرش: ۹۲/۰۴/۰۹)

چکیده

مهم‌ترین فاکتور اعتبار بخشی به اسناد الکترونیکی به‌ویژه چک الکترونیکی که شامل بزرگ‌ترین ارقام تراکنشی در تجارت الکترونیکی می‌شود، بحث امضای روی آن جهت اعتبار بخشی به این سند الکترونیکی است. در میان انواع امضاهای دیجیتال، امضای وکالتی به‌عنوان نمونه‌ای از امضاهاست که در آن صاحب اصلی امضا قابلیت امضای خود را در اختیار فردی به نمایندگی خویش قرار می‌دهد تا فرد نماینده به وکالت از وی، قادر به تولید امضاء بر روی اسناد و مدارک باشد. یکی از چالش‌های پیش‌رو در این زمینه این است که صاحب اصلی امضاء قادر به جلوگیری از امضاهای ناخواسته باشد و هر لحظه امکان جلوگیری از تولید امضاء توسط نمایندگان سوءاستفاده‌گر را دارا باشد. در این مقاله، با افزودن قابلیت ابطال سریع به طرح امضای وکالتی آستانه چنین قابلیتی برای چک‌های الکترونیکی فراهم آورده شده است. طرح ارائه شده در مقابل جعل صاحب امضاء و همچنین جعل نماینده امن بوده و دیگر ملزومات امنیتی یعنی قابل تأیید بودن، غیرقابل انکار بودن، قابل شناسایی بودن و جلوگیری از سوء استفاده که برای یک طرح امضای وکالتی آستانه ضروری می‌باشند را برآورده می‌سازد.

واژه‌های کلیدی: امضاء دیجیتال، طرح امضاء وکالتی، امضای وکالتی آستانه، ابطال سریع وکالت، چک الکترونیکی.

۱. مقدمه

بانک‌ها که قلب تپنده جریان پولی و بدنه اقتصادی جامعه می‌باشند، همواره در چالش‌های فناوری‌های قدیم و تغییر به فناوری‌های جدید، درگیر هستند. وقتی سایر اجزاء یک جامعه با فناوری‌های جدید تغییر می‌کند، اگر بانک‌ها نتوانند خود را به‌روزرسانی کنند، اقتصاد ضعیف و سیستم بانکی ناکارآمد جلوه خواهد کرد. از جمله تغیرات نهادی امور مالی و اقتصادی که به‌واسطه رشد خیره کننده اینترنت اتفاق افتاده و به‌طور فزاینده‌ای در حال گسترش است، رواج بانکداری الکترونیکی و در نتیجه پیدایش بانک‌های مجازی و یا اینترنتی است.

مهم‌ترین ویژگی این بانک‌ها حذف معضل موقعیت فیزیکی بین بانک و مشتری است. یکی از چالش‌های بزرگ بانکداری الکترونیکی که تا به امروز در اجرایی شدن آن بسیاری از کشورها به مشکلات فراوان برخورد کرده‌اند، تبدیل خدمات چک سنتی به چک الکترونیکی و پیاده‌سازی و اجرایی‌کردن قوانین پیرامون آن می‌باشد.

چک الکترونیکی یک ابزار نوین پرداخت است که متشکل از امنیت و سرعت بوده و دارای بازدهی تمام تراکنش‌های الکترونیکی همگون و توأم با زیرساخت‌های قانونی گسترش یافته می‌باشد. چک الکترونیکی قابلیت جایگزینی با چک‌های کاغذی را در فرآیندهای تجاری دارد. یکی از چالش‌های به‌کارگیری چک الکترونیکی قابلیت جایگزینی با چک‌های کاغذی را در فرایندهای تجاری دارد. یکی از چالش‌های به‌کارگیری چک الکترونیکی، بحث تقویت امضاهای الکترونیکی به‌منظور به‌کار بردن الگوریتم‌های فعال پرداخت است. مفهوم چک الکترونیکی در طی پروسه‌ای پس از ابداع ecash توسط چوم[۱] در سال ۱۹۸۸ ارائه شد [۳-۱]. چک‌های الکترونیکی همچون چک‌های کاغذی دارای الزام قانونی برای پرداخت هستند و به‌جای امضاهای دست‌نویس، از امضاهای دیجیتالی در آنها استفاده می‌شود.

چک الکترونیکی، یک سند دیجیتالی امضاء شده به‌صورت الکترونیکی است که می‌تواند سایر اسناد و اطلاعات صورت‌حساب، اعلامیه‌ها، پشت‌نویسی و واگذاری را با خود به‌همراه داشته باشد. در مورد چک کاغذی، با وجود الزام قانونی پرداخت ازطرف صادرکننده، به‌دلیل مشکلاتی همچون موجود نبودن وجه کافی، قطعیت پرداخت

[1] chaum

* ایمیل نویسنده پاسخگو: rebrahimi@guilan.ac.ir

شدن آن نامعلوم و نسبت به سایر روش‌های سنتی کمتراست. اما با الکترونیکی شدن خود چک و مجاز شناسی بلادرنگ آن با بهره‌گیری از امضاها و گواهی‌های دیجیتالی و امکان بررسی وجود وجه کافی در حساب شخص صادرکننده، قطعیت پرداخت‌شدن آن معلوم و تضمین می‌شود، بدون آنکه همچون کارت‌های اعتباری ضرری متوجه مؤسسه اعتباری حامی یا دریافت‌کننده چک باشد و بدین طریق نسبت به نسخه فیزیکی خود، در جایگاه بالاتری قرارمی‌گیرد.

امضاهای وکالتی و وکالتی آستانه می‌توانند کاربردهای ویژه‌ای در مبحث بانکداری الکترونیک و به‌ویژه چک الکترونیکی داشته باشند. مفهوم امضای وکالتی اولین بار توسط مامبو[1] و همکارانش در سال ۱۹۹۶ میلادی مطرح شد [۴]. در یک طرح امضای وکالتی، صاحب امضاء وکالت خود (قابلیت امضای خود) را به یک نماینده اعطا می‌کند و پس از آن نماینده می‌تواند از طرف صاحب امضا پیام‌ها را امضا نماید.

در سال ۱۹۹۷، کیم[2] [۵] و همکارانش و زانگ[3] و همکارانش [۶] به‌ترتیب و به‌طور مستقل اولین طرح‌های امضای وکالتی آستانه را ارائه نمودند. امروزه طرح‌های امضای وکالتی آستانه بسیاری ارائه شده‌اند که برای نمونه می‌توان به [۹- ۷] اشاره نمود. در این امضاها، وکالت به جای یک نفر به یک گروه n نفره از نمایندگان داده می‌شود، به‌گونه‌ای که اگر حداقل t نفر از آنها توافق نمایند، می‌توانند پیام را امضاء کنند. با توجه به کاربرد این‌گونه از امضاها در بانکداری و چک‌های الکترونیکی، به‌طور طبیعی بحث اعطای وکالت و ابطال آن بسیار حائز اهمیت است.

در نظر بگیرید که یک چک الکترونیکی در وجه یک شخص صادر شده و قابل پرداخت باشد؛ اما فرض کنید که صاحب چک پشیمان شده و نمی‌خواهد وجه چک از حساب او پرداخت شود، در این حالت باید مکانیزمی وجود داشته باشد تا او بتواند به سرعت جلوی این کار را بگیرد. به‌همین دلیل است که در این مقاله از یک طرح امضای وکالتی آستانه جدید با امکان ابطال سریع وکالت استفاده شده است. طرح ارائه شده بر اساس مرجع [۱۰] بوده و در آن از تکنیک سئو[4] و همکارانش استفاده شده است [۱۱]. این طرح از لحاظ کارآیی بسیار بهتر از طرح می‌باشد [۱۰].

ادامه این مقاله بدین صورت سازماندهی شده است: در بخش بعد طرح پرداخت FTSC مرور شده، در بخش۳، طرح امضای وکالتی آستانه خود را ارائه نموده و از حیث کارآیی و امنیت بررسی می‌شود. در بخش۴، سناریوی پرداخت چک الکترونیک را ارائه نموده و در نهایت نتیجه‌گیری در بخش ۵ بیان می‌شود.

[1] Mambo
[1] Kim
[2] Zhang
[4] Seo

۲. طرح ابتکاری پرداخت FSTC

طرح ائتلافی سرویس‌های تکنولوژی‌های مالی FSTC[5] توسط گروهی از بانک‌های امریکایی و آژانس‌های تحقیقاتی و ارگان‌های دولتی در سال ۱۹۹۳ بنا نهاده شد [۱۲]. چک الکترونیکی FSTC اولین نمونه از اسناد مالی امضاء شده به‌صورت رمزنگاری است،که به‌دلیل ویژگی‌های قابل توجه آن در ارائه خدمات جدیدی از طرف بانک‌ها به مشتریان در راستای تسهیل و کاهش هزینه‌های بالاسری تراکنش‌های مالی در حرکت از ابزارها و اسناد مالی کاغذی به‌سمت گونه الکترونیکی دارای اهمیت است [۱۳].

در این روش جهت انجام عملیات پرداخت به‌وسیله چک الکترونیکی، پرداخت‌کننده چکی را صادر خواهد کرد که اطلاعاتی مشابه چک کاغذی را دارا است. کاربران توسط گواهی بانکی که از آن اجازه صادر کردن چک را دارند، تأیید می‌شوند. این گواهی توسط دریافت‌کننده وجه، برای بررسی امضای دیجیتال روی چک، استفاده می‌شود. بانک می‌تواند محدودیت‌هایی را روی حساب کاربری اعمال کند مثلاً نوع گواهی، حداکثر سقف مبلغ برای پرداخت، واحدهای ارزی مجاز و یا تأیید چند امضاء برای حساب‌های شرکت‌ها (امضای وکالتی). پیش‌بینی شده که بانک مرکزی و یا ارگان‌های دولتی به‌عنوان ریشه امضاء و صادرکننده گواهی‌ها[6] برای ارگان‌ها باشند. برای انجام یک پرداخت، کاربران حساب مورد نظر به‌صورت آنلاین بر روی وب‌سایت سیستم پرداخت، جایی که شناسه کاربری دریافت‌کننده وجه و مقدار وجه مورد نظر را برای پرداخت وارد می‌کنند، احراز هویت می‌شوند. مقدار وجه از حساب پرداخت‌کننده کم می‌شود و به حساب اعتباری فرد دریافت‌کننده وجه، افزوده می‌شود. اغلب امکاناتی وجود دارد که زمان و تاریخ انجام پرداخت را مشخص می‌کند. دسترسی به حساب‌های کاربری با استفاده از پروتکل امن SSL و امضای دیجیتال صورت می‌گیرد. به‌ویژه با پیشرفت امضاهای دیجیتال و بستر آن یعنی PKI روز به روز استفاده از آن در حساب‌های بانکی فزونی می‌یابد [۱۴].

در معماری FSTC همه افراد قادر به صادرکردن چک الکترونیکی خواهند بود که با یک زیرساخت سخت‌افزاری ممکن خواهد بود. عملکرد این ابزار با ایجاد ایمنی توسط کلید مخفی و اطلاعات گواهی (Certificate) تأمین خواهد شد. برای تعریف ساختار و محتوای چک الکترونیک زبان برنامه‌نویسی FSML[7] برای تعریف ساختار و محتوای چک الکترونیک ساخته شده که محتوای سندهای مالی امضاء شده را تعریف می‌کند [۱۵]. FSML با استفاده از تعمیم زبان استاندارد نشانه‌گذاری SGML[8] به‌وجود آمده است. SGML به‌عنوان زبان ویژه تشریحی به جای XML استفاده شده است [۱۶و۱۷].

[5] Financial Services Technology Consortium
[6] Certificate
[7] Financial Services Markup Language
[8] Standard Generalized Markup Language

۳. طرح امضای وکالتی آستانه ارائه شده

در این بخش یک طرح امضای آستانه‌ای جدید با قابلیت ابطال سریع وکالت ارائه می‌شود که در واقع بهبودی از طرح امضای وکالتی است که در [۱۰] ارائه شده است.

۳-۱. مقدمات طرح

در طرح ارائه شده، سیستم دارای سه نوع شرکت‌کننده می‌باشد: صاحب امضاء که با O نشان داده می‌شود، گروه نمایندگان امضاءکننده که شامل n امضاءکننده $PS = \{P_1, P_2, \cdots, P_n\}$ می‌شود و یک میانجی امنیتی به‌نام SEM[1] است. پارامترهای سیستم و همچنین نمادهایی که تعریف می‌شوند به‌صورت زیر است:

- O : صاحب امضاء.
- PS : گروه نمایندگان امضاءکننده که شامل n امضاءکننده است.
- SEM : یک میانجی امنیتی که به‌صورت یک سرور بر خط[2] مورد اعتماد عمل می‌کند.
- p, q : دو عدد اول بزرگ به‌طوری که $q|p-1$.
- g: یک مولد از گروه $\mathbb{Z}_p^*$ از مرتبه q.
- صاحب امضاء کلید خصوصی $x_o \in \mathbb{Z}_q^*$ و کلید عمومی متناظر آن یعنی $y_o = g^{x_o} \bmod p$ را دارد. هر نماینده همانند P_i که در گروه PS است کلید خصوصی $x_i \in \mathbb{Z}_q^*$ و کلید عمومی متناظر $y_i = g^{x_i} \bmod p$ را در اختیار دارد. به طور مشابهی $x_s \in \mathbb{Z}_q^*$ کلید خصوصی و $y_s = g^{x_s} \bmod p$ کلید عمومی SEM می‌باشد.
- h(·) : یک تابع چکیده‌ساز یک‌طرفه که در مقابل تصادم مقاوم می‌باشد.
- APSID: نشان‌دهنده شناسه امضاءکنندگان واقعی است.
- ω: یک گواهینامه که شامل اطلاعاتی چون شناسه صاحب امضاء، شناسه‌های نمایندگان، شناسه SEM، طول دوره اعتبار وکالت و غیره می‌باشد.

تمامی کلیدهای عمومی به‌وسیله یک مرکز صدور گواهی[3] (CA) گواهی می‌شود. البته این مرجع صدور گواهی یک CA با قابلیت تست اثبات دانش صفر[4] است و به‌همین دلیل از تأثیر حملات جانشانی کلید عمومی[5] جلوگیری می‌شود.

۳-۲. توصیف طرح ارائه‌شده

به‌طور کلی، طرح ارائه شده از سه فاز فاز تولید سهم وکالتی، فاز تولید امضای وکالتی و فاز تأیید امضای وکالتی تشکیل شده است.

فاز تولید سهم وکالتی: صاحب امضاء اعداد تصادفی $k_i, k_s \in \mathbb{Z}_q^*(1 \le i \le n)$ انتخاب کرده و قرار می‌دهد $k_o = \sum_{i=1}^{n} k_{P_i} + k_s$. همچنین صاحب امضاء پارامترهای $K_s = g^{k_s} \bmod p$، $K_{P_i} = g^{k_{P_i}} \bmod p$ و $K_o = g^{k_o} \bmod p$ را محاسبه نموده و اعلام می‌نماید، سپس صاحب امضاء سهم وکالتی هر نماینده P_i (که $1 \le i \le n$) است) و همچنین SEM را به‌صورت زیر محاسبه می‌کند:

$$\sigma_{P_i} = k_{P_i} K_{P_i} + x_o h(\omega, K_o) \bmod q \quad (۱)$$

$$\sigma_S = k_s K_s + x_o h(\omega, K_o) \bmod q \quad (۲)$$

صاحب امضاء عبارت $(\omega, K_o, \sigma_{P_i}, K_{P_i})$ را به هر نماینده P_i و $(\omega, K_o, \sigma_s, K_s)$ را به SEM ارسال می‌کند. برای تأیید سه‌تائی‌های دریافتی؛ هر P_i، $R_{P_i} = g^{\sigma_{P_i}} \pmod p$ را محاسبه کرده و عبارت (ω, R_{P_i}) را به SEM می‌فرستد. SEM نیز $R_S = g^{\sigma_S} \pmod p$ را محاسبه نموده و به P_i ارسال می‌نماید. در نهایت هر نماینده P_i از طریق کنترل رابطه $R_{P_i} \cdot R_S = K_{P_i}^{K_{P_i}} \cdot K_s^{K_s} \cdot y_o^{2h(\omega, K_o)} \bmod p$ صحت داده دریافتی را کنترل می‌کند. SEM نیز با روند مشابهی از صحت داده‌ها اطمینان حاصل می‌کند. سپس هر P_i و SEM سهم‌های وکالتی خود را به‌صورت زیر محاسبه می‌نمایند.

$$\begin{aligned} &P_i: \sigma^*_{P_i} = \sigma_{P_i} + x_i h(\omega, K_o) \bmod q \\ &SEM: \sigma_{P_S} = \sigma_S + x_S h(\omega, K_o) \bmod q \end{aligned} \quad (۳)$$

فاز تولید امضای وکالتی: بدون از دست دادن کلیت، فرض می‌شود که $\{P_1, P_2, \cdots, P_t\}$ است، چرا که قرار است تا t نماینده با همکاری یکدیگر امضای وکالتی را صورت دهند. در این فاز ابتدا O مقدار APSID را در تابع چکیده‌ساز σ_S گنجانده و سه‌تائی $(\sigma_S, g^{\sigma_S}, APSID)$ را برای SEM ارسال می‌کند تا SEM نیز با تأیید آن از هویت t نماینده امضاءکننده اطلاع حاصل نماید.

هر $P_i (1 \le i \le t)$ نیز عدد تصادفی $l_{P_i} \in_R \mathbb{Z}_q$ را انتخاب کرده و عبارت $L_{l_{P_i}} = g^{l_{P_i}} \pmod p$ را محاسبه کرده و سپس $(\omega, m, K_o, R_{P_i}, L_{P_i})$ را به SEM می‌فرستد. ابتدا SEM داده دریافتی را از حیث تطابق با $(\omega, K_{P_i}, K_o, \sigma_{P_i})$ که در مراحل قبل دریافت کرده بود، کنترل می‌کند. در ادامه SEM باید از حصول شرایط زیر اطمینان حاصل نماید:

a) دوره اعتبار وکالت مشخص شده در ω باید معتبر باشد.
b) K_o نباید در لیست ابطال قرار داشته باشد. اگر K_o در لیست ابطال قرار داشته باشد به این معنی است که دوره وکالت اعطائی به نمایندگان منقضی شده است.

اگر SEM از اعتبار وکالت تمام نمایندگان اطمینان حاصل کرد به طریق زیر توکن[6] صادر می‌کند:

۱) SEM عدد تصادفی $l_S \in_R \mathbb{Z}_q$ را انتخاب کرده و عبارات زیر را محاسبه می‌نماید.

[1] Security Mediator
[2] On-Line
[3] Certification Authority
[4] Zero-Knowledge Proof Test
[5] Public Key Substitute Attack
[6] Token

$$L_S = g^{l_S} (\mathrm{mod}\ p), L_o = g^{l_S}.g^{\sum_{i=1}^{n} k_{P_i}} (\mathrm{mod}\ p) \quad (۴)$$

۲) در نهایت، SEM امضای جزئی خود (توکن) را به فرم زیر بـرروی پیام m صادر می‌کند.

$$S_{SEM} = l_S + \sigma_{P_S} h(m, L_o) \mod p \quad (۵)$$

سپس SEM مقـادیر (L_o, S_{SEM}, L_S) را بـه نماینـدگان و همچنـین شخص تأییدکننده ارسال می‌کند. نمایندگان نیز از طریق معادله زیر از صحت داده فوق اطمینان حاصل می‌نمایند.

$$g^{S_{SEM}} = L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)} \mod p \quad (۶)$$

علاوه بر آن، هر P_i یک عدد تصادفی $k_i \in_R \mathbb{Z}_q^*$ را انتخاب و عبارت $r_i = g^{k_i} (\mathrm{mod}\ p)$ را محاسبه و اعـلام نمـوده و در نهایـت امضـای فردی خود را به‌صورت زیر تولید می‌کند. توجه کنیـد کـه در ادامـه برای راحتی کار از نماد $H = h(R, APSID, m)$ استفاده می‌شود.

$$R = \prod_{i=1}^{t} r_i \ (\mathrm{mod}\ p) \quad (۷)$$

$$\gamma_i = (k_i R + S_{SEM}) + \sigma_{P_i}^* H \ (\mathrm{mod}\ q) \quad (۸)$$

سپس تمـام نماینـدگان امضـاهای انفـرادی خـود γ_i را بـه‌همـراه پارامترهای r_i و K_{P_i} به یک منشی[1] تحویل می‌دهند. منشی می‌تواند فردی از میان خود نمایندگان و یا فرد دیگری خـارج از آنهـا باشـد. منشی از طریق بررسی رابطه زیر، اعتبار امضـاهای فـردی را کنتـرل می‌کند.

$$g^{\gamma_i} = r_i^R \left[L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)}\right] \times \left[K_{P_i}^{K_{P_i}}.(y_o.y_i)^{h(m,K_o)}\right]^H \mathrm{mod}\ p \quad (۹)$$

همچنین منشـی عبـارت $K = \prod_{i=1}^{t} K_{P_i}^{K_{P_i}}$ و کلیـد عمـومی گروهـی $y_t = \prod_{i=1}^{t} y_i$ را محاسبه و منتشر می‌نماید.

صحت رابطه فوق:

$$\begin{aligned} g^{\gamma_i} &= g^{(k_i R + S_{SEM}) + \sigma_{P_i}^* H} = g^{k_i R}.g^{S_{SEM}}.g^{\sigma_{P_i}^* H} \mathrm{mod}\ p \\ &= r_i^R \left[L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)}\right] \times \left[g^{\sigma_{P_i} + x_i h(\omega,K_o)}\right]^H \mathrm{mod}\ p \\ &= r_i^R \left[L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)}\right] \times \left[K_{P_i}^{K_{P_i}} y_o^{h(m,K_o)} y_i^{h(m,K_o)}\right]^H \mathrm{mod}\ p \\ &= r_i^R \left[L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)}\right] \times \left[K_{P_i}^{K_{P_i}}.(y_o.y_i)^{h(m,K_o)}\right]^H \mathrm{mod}\ p \end{aligned}$$

پـس از تأییـد تمـام امضـاهای انفـرادی، منشـی امضـای نهـائی را به‌صورت زیر تولید می‌نماید.

$$S = \sum_{i=1}^{t} \gamma_i \ (\mathrm{mod}\ q) \quad (۱۰)$$

در نهایت، $(\omega, S, K_o, R, APSID)$ یک امضای وکالتی معتبر روی متن m است.

فاز تأیید امضاء: شخص تأییدکننده می‌تواند اعتبار امضای وکالتی را از طریق معادله زیر کنترل نماید:

$$g^S = R^R.\left[L_S.\left(R_S.y_S^{h(\omega,K_o)}\right)^{h(m,L_o)}\right] \times \left[K.(y_o.y_t)^{h(\omega,K_o)}\right]^H \mathrm{mod}\ p. \quad (۱۱)$$

۳-۳. تحلیل امنیتی طرح ارائه‌شده

۱- صحت طرح ۲: تمامی روابط استفاده شده در طرح مثل امضاهای انفرادی، معادله تأیید و غیره بـه‌درسـتی نوشـته شـده‌انـد. بـا انجـام یکسری محاسبات سر راست می‌توان صحت روابط مذکور را بررسـی کرد.

۲- ابطال سریع: با قرار دادن یک میـانجی امنیتـی در طـرح ارائـه شده، مشکل ابطال سریع طرح امضای وکالتی آستانه از بین مـی‌رود چرا که در طی روند صدور هر امضاء توسط نمایندگان، SEM اعتبـار وکالت آنان را کنترل می‌کند و چنانچه صـاحب امضـاء وکالـت اعطـا شده را باطل نموده باشـد (یعنـی K_o را در لیسـت ابطـال قـرار داده باشد) SEM دیگر توکن را برای نمایندگان صادر ننموده و در نتیجه آنها نیز نخواهند توانست تا امضای وکالتی معتبری را صورت دهند.

۳- قابـل تأییـدبـودن[3]: در طـرح ارائـه شـده، امضـاء شـامل $(\omega, S, K_o, R, APSID)$ است و بنابراین هر تأییدکننده‌ای مـی‌توانـد از ω و APSID هویت صـاحب امضـاء، نماینـدگان و SEM را بشناسـد. چون کلید عمومی صاحب امضاء در قسمت تأیید مورد استفاده قـرار می‌گیرد، پس تأییدکننده می‌تواند از توافق صاحب امضاء روی مـتن امضاء شده اطمینان حاصل نماید.

۴- غیرقابل جعل‌بودن[4]: فرض کنید که صاحب امضاء قصـد جعـل امضاء را داشته باشد. او از کلید خصوصـی کـاربران اطلاعـی نـدارد و بنابراین از سهم $\sigma_{P_i}^*$ آگاهی نداشته و نمی‌تواند امضای وکالتی را جعل نماید. از طرفی چون در رابطه تأیید، عبـارات R, K_{P_i} بـه تـوان خـود رسیده‌اند، پس دست مهاجم بداندیش برای جعل امضاء عملاً بسته

[1] Clerk

[2] Correctness
[3] Verifiability
[4] Unforgeability

خواهد بود، چرا که او فقط حق انتخاب برای S, K_o دارد و این در حالی است که حل مسئله لگاریتم گسسته (DLP) دشوار است.

۵- قابل شناسایی بودن[1]: در طرح ارائه شده، اطلاعات هویتی نمایندگان به‌طور آشکار در امضای وکالتی معتبر، ω و APSID آمده است. همچنین کلید عمومی نمایندگان (y_i) در معادله تأیید به‌کار می‌رود. بنابراین هر شخصی می‌تواند هویت نمایندگان را از امضایی که توسط ایشان صادر شده تشخیص دهد و هویت آنها را از روی ω و APSID تأیید نماید.

۶- غیر قابل انکار بودن[2]: با فرض سخت بودن مسئله لگاریتم گسسته (DLP)، هیچ کسی از کلید خصوصی کاربران (x_i) اطلاعی ندارد و تنها هر نماینده کلید خصوصی خود را می‌داند. بنابراین نماینده‌ای که امضای وکالتی را صادرمی‌کند، می‌تواند آن را جعل کند چرا که در صدور امضای وکالتی، نمایندگان از کلید خصوصی خود استفاده می‌کنند.

۷- جلوگیری از سوء استفاده[3]: تنها نمایندگان مجاز می‌توانند با استفاده از کلیدهای خصوصیشان و با مشارکت یکدیگر یک امضای وکالتی معتبر صورت دهند، چرا که تنها هر نماینده‌ای از کلید خصوصیش اطلاع دارد. بنابراین چنان‌چه نماینده‌ای از زوج کلید وکالتی خود برای اهداف دیگری استفاده کند، او خود مسئولیت آن را بر عهده خواهد داشت. بنابراین سناریوی سوء استفاده منتفی است. علاوه بر آن راه سوء استفاده صاحب امضاء و مهاجم بداندیش نیز بسته است برای اینکه آنها نمی‌توانند یک زوج کلید وکالتی معتبر را محاسبه نمایند. طرحی که در این مقاله ارائه شده، بهبودی از طرحی است که در مرجع [۱۰] آمده است. در جدول ۱، این طرح از حیث پیچیدگی محاسباتی با طرح ارائه شده در این مقاله مقایسه شده است . در این مقایسه، واضح است که طرح ارائه شده در این مقاله از نظر کارایی بسیار بهتر از طرح [۱۰] است. لازم به ذکر است که در جدول **۱**، T_e زمان لازم برای محاسبه یک توان‌رسانی(به پیمانه)، T_m زمان لازم برای محاسبه یک ضرب پیمانه‌ای و T_h زمان لازم برای محاسبه یک چکیده‌سازی است.

جدول ۱: مقایسه پیچیدگی محاسباتی

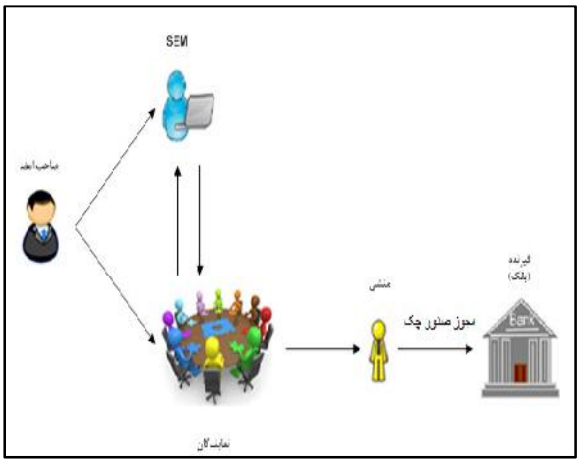
	طرح ارائه‌شده در مرجع [۱۰]	طرح Hwang و همکارانش [۱۹]	طرح Xie [۱۹]	طرح ارائه شده
تولید سهم مخفی	$(n^2t+n)T_e+(3n^2t-2nt-3n^2+4n-t+1)T_m$	$(n^2t)T_e+(3n^2t-2nt-3n^2+3n-t)T_m$	$(n^2t+2n)T_e+(3n^2t-2nt-3n^2+6n-t+1)T_m$	-
تولید سهم وکالتی	$(2n)T_e+(4n+3)T_m+T_h$	$(2t+1)T_e+(nt-n+2t)T_m+2T_h$	$(2t+1)T_e+(nt-n+2t+1)T_m+2T_h$	$(n+3)T_e+(3n+3)T_m+(2n+2)T_h$
تولید امضای وکالتی (شامل امضاهای انفرادی و نهایی)	$(2t+12)T_e+(3t+12)T_m+5T_h$	$(4t^2-t-1)T_e+(10t^2-13t+5)T_m+(t^2-t)T_h$	$(nt+5t^2-3t+3)T_e+(nt+5t^2-5t+12)T_m+3T_h$	$(6t+7)T_e+(3t+7)T_m+3T_h$
تأیید امضای وکالتی	$7T_e+(2t+3)T_m+3T_h$	$4T_e+(t+4)T_m+2T_h$	$(n+t+7)T_e+(n+t+5)T_m+2T_h$	$6T_e+(t+6)T_m+3T_h$
ابطال سریع وکالت	✓	×	×	✓

[1] Identifiability
[2] Undeniability
[3] Prevention of Misuse

۴. سناریوی پرداخت

چنانچه A یا امضاءکننده اصلی را به‌عنوان مدیر عامل یک شرکت و یا ریاست یک وزارت خانه در نظر بگیرید، در صورت صدور جواز وکالت از طرف وی، n نفر به‌عنوان نماینده قابلیت ایجاد امضای وکالتی را از طرف صاحب اصلی امضاء دارا خواهند بود. این n نفر در واقع معاونین مدیر عامل در بخش های مختلف هستند و هر کدام در یکی از بخش‌های مرتبط با پست خود حق ایجاد امضاء به نیابت از مدیر کل و یا حق برداشت از کل بودجه سازمانی را با موافقت ریاست کل دارا می‌باشند. در این میان به‌عنوان مثال، جهت تأسیس شعبه جدیدی از شرکت فرض شود معاونین مرتبط با بخش عمرانی و کارگزینی باید ساختمان جدید و کارمندان جدیدی را مهیا نمایند، این افراد در واقع همان t نفری خواهند بود که از میان n نفر توانایی ایجاد امضای نهایی را با توافق میان گروهی خود و با نظارت نهایی مدیر عامل، خواهند داشت. در تمامی این مراحل SEM نیز به‌عنوان میانجی امنیتی و ناظر بر کل امور انجام شده حضور خواهد داشت. برای ایجاد امضای وکالتی ابتدا مدیر عامل بخشی از وکالت خود را به SEM و بخش دیگر را به معاونین عمرانی و کارگزینی می‌دهد. در مرحله بعد معاونین و SEM یکدیگر را تأیید نموده و درصورتی‌که SEM از اعتبار وکالت معاونین مطمئن شود،برای آنها توکن (همان قطعه دیگر وکالت) را صادرمی‌کند. B به‌عنوان معاون مالی امضاءکننده نهایی لحاظ خواهد شد که در واقع یکی از معاونین بخش کارگزینی و یا بخش عمرانی است که بنا به صلاحدید SEM با توجه به انجام امور محوله توانایی دسترسی به امضاء بر روی چک را در غیاب مدیر عامل خواهد داشت

مطابق شکل ۱، امضای B جهت انجام مراحل تراکنش بانکی و عملیات پرداخت در سرورهای بانکی دارای اعتبار خواهد بود. باید توجه داشت که درتمامی مراحل، مدیر عامل قادر به باطل نمودن جواز نمایندگی است و می‌تواند از تولید هرگونه امضای ناخواسته جلوگیری نماید.



شکل ۱: سناریوی تولید امضای وکالتی تا صدور چک الکترونیکی

همچنین امضای وکالتی تولید شده همراه با اطلاعات درج شده در جدول ۲ در قالب FSML در بلوک مرتبط با امضای دیجتال درج می‌شود و پس از مرحله تأیید اعتبار، توسط بانک منجر به صدور چک الکترونیکی و اتمام پروسه تراکنش پرداخت الکترونیکی می‌شود.

جدول ۲: اطلاعات لازم جهت صدور چک الکترونیکی

نام بلوک	شرح
Account	شماره حساب، نام صاحب حساب، نوع حساب، نام بانک و ...
Check	تاریخ چک، شماره سریال چک، مبلغ، در وجه ...
Signature	بخش امضاها
Certificate	گواهیX.509 مربوط به امضای دیجیتال و کلید عمومی
Endorsement	بخش مربوط به پشت‌نویسی چک
Deposit	بخش مربوط به حساب دریافت‌کننده چک (به حساب گذاشتن)
Bank Stamp	بخش مربوط به عملیات بانکی
Invoice	بخش مربط به صورتحساب و لیست مربوط به چک
Attachment	بخش مربوط به ضمائم چک

۵. نتیجه‌گیری

همگام با ورود تکنولوژی ارتباطات الکترونیکی در تمامی عرصه‌های زندگی انسان معاصر، طبعاً عملیات پرداخت‌های بانکی نیز احتیاج به نگرشی دوباره خواهند داشت. انجام تراکنش‌های پرداخت‌های الکترونیکی فاقد امنیت و بدون اطمینان از هویت واقعی افراد هیچ ارزشی نخواهد داشت. به‌کارگیری از علم رمزنگاری و امضاهای دیجیتال راهگشای این چالش خواهد بود.

در این مقاله، طرح امضای جدیدی با افزودن امکان ابطال سریع به امضای وکالتی آستانه ارائه شده که به فرد امضاکننده اصلی این امکان را می‌دهد که علاوه بر بخشیدن حق امضای خود به معاونینش، در هر لحظه که سوءنیت آنان بر وی احراز گردید حق وکالت آنان را فسخ نماید و امضای افراد سوءاستفاده‌گر را از درجه اعتبار ساقط نماید. تمامی نیازهای امنیتی یک امضای وکالتی از جمله قابل تأیید بودن، غیرقابل انکار بودن، قابل شناسایی بودن و جلوگیری از سوءاستفاده در این طرح برآورده شده است.

۶. مراجع

[1] D. Chaum, "Privacy Protected Payments: Unconditional Payer and/or Payee Anonymity in Smart Card 2000"; North-Holland, pp. 69-92, 1989.

[2] http://www.chaum.com/articles/Online_Cash_Checks.htm

[3] B. den Boer, D. Chaum, E. van Heyst, S. Mjxlsnes, & A. Steenbeek, "Efficient Offline Electronic ChecksAdvances in Cryptology EUROCRYPT '89"; J.-J. Quisquater& J. Vandewalle (Eds.), Springer-Verlag, pp. 294-301,1989.

[4] M. Mambo, K. Usuda, E. Okamoto,"Proxy signature: Delegation of the power to sign messages"; IEICE Transactions on Fundamentals, Vol. 79–A (9), pp. 1338–1353, 1996.

[5] S. J. Kim, S. J. Park, D. H. Won, "Proxy Signatures, revisited. ICICS'97, LNCS 1334, Springer-Verlag, pp. 223–232, 1997.

[6] K. Zhang, "Threshold proxy Signature Schemes"; Information Security Workshop, Japan, pp. 191–197, 1997.

[7] J. Hu, J. Zhang. "Cryptanalysis & Improvement of a Threshold proxy Signature Scheme"; Computer Standards & Interfaces, pp. 169–173, 2009.

[8] J. Liu and Sh. Huang, "Identity-Based Threshold Proxy Signature from Bilinear Pairings"; INFORMATICA, Vol. 21, No. 1, Institute of Mathematics and Informatics, pp. 41-56, 2010.

[9] Z. Tan. "Improvement on C.-L Hsu et al's threshold proxy signature scheme with known signers"; international Conference on Convergence Information Technology, pp. 1463–1467, 2007.

[10] M. Beheshti-Atashgah, M. Gardeshi and M. Bayat, "A New Threshold Proxy Signature Scheme with Fast Revocation"; Int. J. of Computer and Electrical Eng. Vol. 4, No. 5, pp. 766- 770, 2012.

[11] S. H. Seo, K. A. Shim, S. H. Lee, "A Mediated Proxy Signature Scheme With Fast Revocation for Electronic Transactions"; Proceedings of the 2nd Int. Conference on Trust, Privacy and Security in Digital Business, Aug 22-26, 2005, Copenhagen, Denmark.LNCS 3592. Berlin, German: Springer-Verlag, 2005: 216–225.

[12] Financial Services Technology Consortium, 2001, http://www.fstc.org/.

[13] F. MofakhamNasiri, design and implementation of e in Cheque"; published by Jahad Collegiate, In Persia 1384.

[14] D. O. Mahony, M. Peirce, H. Tewari, "Electronic Payment Systemsfor E-Commerce 2nd edition"; Artech House INC, pp.139, 2001.

[15] J. Kravitz, (ed.), FSML.Financial Services Markup Language, Version 1.5, Financial Services Technology Consortium, Chicago, IL, July 1999.

[16] Standard Generalized Markup Language"; Int. Standards, Organization (ISO) 8879, 1986.

[17] Extensible Markup Language (XML) 1.0, 2nd ed., W3C Recommendation,October 2000, http://www.w3.org/.

[18] Q. Xie, "Improvement of Tzeng et al.'s Nonrepudiable Threshold proxy Signature Scheme with known signers"; Applied Mathematics and Computation, Vol. 168, pp. 776-782, 2005.

[19] M. S. Hwang, I. C. lin, E. j. Lu, "A Secure Nonrepudiable Threshold Proxy Signature Scheme with known Signer"; Informatica (LjUbljana) Vol. 11, No. 2, pp.137-144, 2009.