پیشنهاد یک روش امضای دیجیتال هویت‌گرای غیر قابل انکار

حمید مَلا و محمد دخیل‌علیان

دانشگاه صنعتی اصفهان، دانشکدهٔ برق و کامپوتر

E-mail: hamid_mala@ec.iut.ac.ir, mdalian@cc.iut.ac.ir

چکیده – سیستمهای رمزنگاری کلید عمومی هویت‌گرا را می‌توان به عنوان جایگزینی برای سیستمهای رمز کلید عمومی گواهی‌گرا به ویژه هنگامی که مدیریت کلید کارامد و سطح امنیت متوسط مورد نیاز باشد، تلقی نمود. در روشهای امضایی که تا کنون در این سیستمها پیشنهاد شده، گریزی از دسترسی مرکز تولید کلید خصوصی به کلید خصوصی موجودیتها نیست و علیرغم فرض اعتماد به این مرکز همواره امکان جعل امضای موجودیتها از سوی وی وجود دارد. در کاربردهای بسیار حساس لازم است که کلید خصوصی فرد که به منظور امضا به کار می‌رود صرفاً در اختیار خود وی باشد. با این دید در این مقاله یک روش امضای دیجیتال هویت‌گرا که حتی توسط مرکز نیز قابل جعل نباشد پیشنهاد می‌شود. در این روش نیز همچون اغلب روشهای رمزنگاری هویت‌گرا از زوج‌نگارهای دوخطی که روی خمهای بیضوی تعریف می‌شوند بهره گرفته شده است.

کلید واژه- امضای دیجیتال هویت‌گرا، انکارناپذیری، مرکز تولید کلید، زوج‌نگارهای دوخطی

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[1] را به منظور ساده‌سازی فرآیند مدیریت کلید در رمزنگاری کلید عمومی 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 مورد اعتماد که در اینجا مرکز تولید کلید[2] ، KGC، خوانده می‌شود، ساخته شده و از طریق کانال امن در اختیار 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[3] که از خم بیضوی استفاده می‌کنند شدند[۲]. زوج‌نگارهای دوخطی، شامل زوج‌نگارِ ویل[4] و

[1] ID-based

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

زوج‌نگارِ تیت[1] اخیراً کاربردهای فراوانی در رمزنگاری یافته‌اند که مهمترین آنها کمک به تحقق روشهای رمزنگاری هویت‌گراست[۲-۶].

اکثریت قریب به اتفاق روشها و ابزارهای رمزنگاری هویت‌گرا شامل انواع امضا، روشهای امن مبادلهٔ کلید، روشهای شناسایی امن و... متأثر از روش بونه-فرانکلین هستند و کم و بیش از پیکربندی[2] و پارامترهای این سیستم استفاده می‌کنند. یکی از ویژگیهای سیستم بونه-فرانکلین امکان دستیابی قانونی به کلید[3] خصوصی کاربران است. اگرچه این ویژگی در بسیاری موارد همچون زمانی که از کلید به منظور انجام رمزگذاری استفاده می‌شود، مطلوب است اما در کاربردی نظیر امضا که اساسی‌ترین نیازمندی آن انکارناپذیری[4] است، نامطلوب تلقی می‌گردد. به بیان دیگر همواره امکان جعل امضای کاربران از سوی مرکز تولید کلید وجود دارد. این در حالی است که در سیستمهای گواهی‌گرا این امکان وجود دارد که کاربر تعیین نماید که زوج کلید وی توسط CA تولید شود و یا اینکه خودش زوج کلید را تولید نموده و پس از اثبات در اختیار داشتن کلید خصوصی از مرکز بخواهد که کلید عمومی متناظر با آن را گواهی نماید. در این مقاله برای رفع این مشکل با تغییر نحوهٔ صدور کلید در روش امضای هویت‌گرای Chau-Cheon از تسلط مرکز بر کلید خصوصی کاربر جلوگیری نموده و یک روش امضای دیجیتال هویت‌گرا با ویژگی عدم انکار معرفی می‌کنیم.

در ادامه نخست زوج‌نگارهای دوخطی را معرفی می‌کنیم. سپس به مرور روش امضای هویت‌گرای Chau-Cheon که از نحوهٔ صدور کلید بونه-فرانکلین تبعیت می‌کند، می‌پردازیم. آنگاه با اصلاح این روش یک روش امضای هویت‌گرا با ویژگی عدم امکان جعل از سوی مرکز پیشنهاد می‌کنیم. در پایان نیز تحلیلی از امنیت و کارامدی روش پیشنهادی 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[5]: 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 دیفی- هلمن محاسباتی (CDH[6]) 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].

ب- مسئلهٔ دیفی- هلمن تصمیمی (DDH[7]) 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.

[1] Tate Pairing
[2] Setting
[3] Key escrow
[4] Nonrepudiation
[5] Non-degeneracy
[6] Computational Diffie-Hellman
[7] Decisional Diffie-Hellman

تعریف گروهِ گپ دیفی-هلمن (GDH[1]) : 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[2] تعریف نمود. نگاشت e نیز برابر با یکی از دو نگاشتِ "تیت" یا "ویل" تعریف می‌شود. برای مطالعهٔ دقیقتر می‌توانید به [۲] مراجعه کنید.

۳- روش امضای هویت‌گرای Chau-Cheon

این روش که در سال ۲۰۰۳ پیشنهاد شده از الگوریتمِ برپایی و استخراج کلید[3] مشابه با روش استاندارد بونه-فرانکلین استفاده می‌کند. در این‌جا این روش امضا را طی چهار الگوریتمِ برپایی سیستم هویت‌گرا، الگوریتم استخراج کلید کاربران، الگوریتم امضا و الگوریتم وارسیِ امضا بیان می‌کنیم[۷].

الگوریتم برپایی سیستم : در گام نخست، مرکز عدد اول q را انتخاب نموده و گروه جمعیِ G_1 با مولدِ P و گروه ضربیِ G_2 ، هر دو با مرتبهٔ q را تشکیل می‌دهد و یک نگاشت دوخطی به صورت $e:G_1\times G_1\to G_2$ تولید می‌نماید. در گام دوم عدد تصادفیِ $s\in Z_q^*$ را به عنوان کلید خصوصی خود انتخاب نموده و کلید عمومی خود را برابر با $P_{pub}=sP$ محاسبه می‌کند. در گام سوم پارامترهای عمومی سیستم را به صورت $params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2\}$ اعلام و s را بعنوان کلید اصلی پنهان نگه می‌دارد. توابع درهم مورد استفاده به صورتِ $H_1:\{0,1\}^*\times G_2\to Z_q^*$ و $H_2:\{0,1\}^*\to G_1^*$ تعریف می‌شوند.

الگوریتم استخراج کلید : :هر کاربر اطلاعات شناسایی خود یعنی $ID\in\{0,1\}^*$ را به مرکز اعلام و خود را برای وی احراز اصالت می‌نماید. مرکز، کلید خصوصی کاربر را به صورت $S_{ID}=sQ_{ID}=sH_2(ID)$ محاسبه و از طریق کانال امن در اختیار وی قرار می‌دهد. در حقیقت $Q_{ID}=H_2(ID)$ کلید عمومی کاربری با اطلاعات شناساییِ ID می‌باشد.

الگوریتم امضا : امضا کنندهٔ با هویتِ ID برای امضای پیام M، عدد تصادفی $r\in_R Z_q^*$ را انتخاب و امضا را به صورت زوجِ $\sigma=(U,V)$ اعلام می‌کند که در آن U و V از رابطهٔ (۳) محاسبه می‌شوند.

$$V=(r+h).S_{ID}\ ,\ h=H_1(M,U)\ ,\ U=r.Q_{ID} \qquad (۳)$$

الگوریتم وارسی امضا : برای وارسی امضای $\sigma=(U,V)$ که ادعا می‌شود امضای پیام M از سوی موجودیتی با هویت ID باشد، نخست $h=H_1(M,U)$ محاسبه و سپس بررسی می‌شود که آیا چهارتاییِ $(P,P_{pub},U+h.Q_{ID},V)$ در رابطهٔ (۴) صدق می‌کند یا نه.

$$e(P_{pub},U+h.Q_{ID})\overset{?}{=}e(P,V) \qquad (۴)$$

سازگاری روش به سادگی با استفاده از ویژگی دوخطی بودن نگاشت e به صورت زیر اثبات می‌شود. اگر $\sigma=(U,V)$ یک امضای معتبر پیام M از سوی موجودیتی با هویت ID باشد، آنگاه $U=r.Q_{ID}$ و $V=(r+h).S_{ID}$ به ازای $r\in_R Z_q^*$ و $h=H_1(M,U)$ می‌باشد، بنابراین :

$$\begin{aligned} e(P_{pub},U+h.Q_{ID}) &= e(s.P,(r+h).Q_{ID}) \\ &= e(P,(r+h).D_{ID}) \\ &= e(P,V) \end{aligned} \qquad (۵)$$

در مرجع [۷] در مورد امنیت این روش امضا، اثبات شده که که با فرض سخت بودن مسئلهٔ CDHP, روش امضای Chau-Cheon در مقابل حمله ID و پیام انتخابی وفقی[4]، امن می‌باشد.

[1] Gap Diffie-Hellman
[2] Supersingular Elliptic Curve
[3] Key Extraction
[4] Adaptive Chosen Message and ID Attack

۴- روش پیشنهادی

همانگونه که از روش امضای بیان شده در بخش (۳) برمی‌آید، به علت آگاهی KGC از کلید خصوصی کاربران در سیستم‌های هویت‌گرایی که از پیکربندی و نحوهٔ استخراج کلید بونه-فرانکلین استفاده می‌کنند، امضاهای مذکور قابل انکارند. زیرا مرکز به راحتی می‌تواند امضای کاربران را جعل نماید. در ادامه با فرض عدم اعتماد به KGC و تغییر روش امضای Chau-Cheon، یک روش امضا با ویژگی عدم انکار پیشنهاد می‌کنیم.

الگوریتم برپایی سیستم : دقیقاً همانند روش برپایی بیان شده در بخش (۳) است و پارامترهای سیستم به صورتِ $params = \{q, G_1, G_2, e, P, P_{pub}, H_1, H_2\}$ تعریف و اعلام می‌شوند. اما نحوهٔ تعیین کلید خصوصی کاربر به صورت زیر تغییر خواهد نمود.

الگوریتم استخراج کلیدهای کاربران : در گام اول، کاربرِ با هویت ID عدد تصادفی $r \in_R Z_q^*$ را به عنوان کلید خصوصی خود انتخاب و کور شدهٔ آن یعنی rP را به عنوان قسمتی از کلید عمومی خود برای مرکز ارسال می‌کند. در گام دوم مرکز، کلید خصوصی کاربر را طبق رابطهٔ (۶) محاسبه و از طریق کانال امن در اختیار وی قرار می‌دهد.

$$S_{ID} = sQ_{ID} = sH_1(ID, rP) \qquad (۶)$$

بنابراین می‌توان گفت که در این شیوهٔ جدید استخراج کلید، کاربر با هویتِ ID دارای یک جفت کلید عمومی به صورتِ

$$rP\ ,\ Q_{ID} = H_1(ID, rP) \qquad (۷)$$

و یک جفت کلید خصوصی به صورت رابطهٔ (۸) می‌باشد.

$$r\ ,\ S_{ID} = sQ_{ID} = sH_1(ID, rP) \qquad (۸)$$

الگوریتم امضا : کاربر با هویت ID و دارای کلیدهای چهارگانهٔ فوق، پیام M را به صورت زیر امضا می‌کند:

گام اول : با داشتن M و rP حاصل $H = H_2(ID, M, rP) \in G_1$ را محاسبه می‌کند.

گام دوم : با استفاده از هر دو کلید خصوصی خود حاصل $V = S_{ID} + rH \in G_1$ را نیز محاسبه می‌کند.

امضای پیام M به صورت زوج $< rP, V >$ از طرف کابر با هویت ID و دارای کلیدهای عمومی rP و Q_{ID} برای وارسی کنندهٔ امضا ارسال می‌شود.

الگوریتم وارسی امضا : وارسی کننده پس از دریافت پیام M و امضای آن، نخست نیمهٔ دیگر کلید عمومی کاربر را از رابطهٔ $Q_{ID} = H_1(ID, rP)$ محاسبه می‌کند. سپس H را از رابطهٔ $H = H_2(ID, M, rP) \in G_1$ محاسبه می‌نماید. آنگاه امضا را می‌پذیرد اگر و تنها اگر تساویِ (۹) برقرار باشد.

$$e(P, V) = e(P_{pub}, Q_{ID}).e(rP, H) \qquad (۹)$$

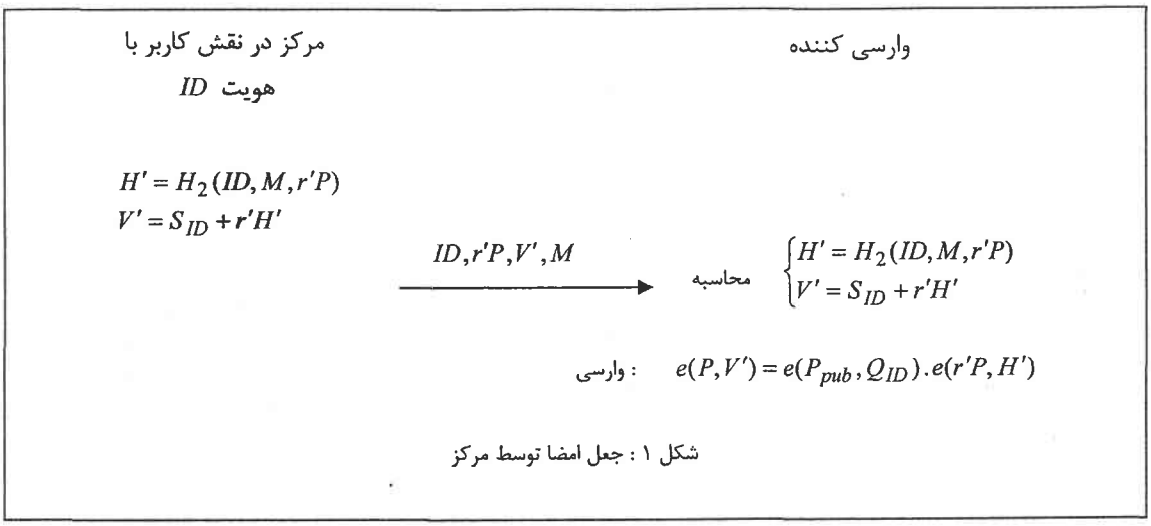
سازگاری عملیات امضا و وارسی آن به سادگی با استفاده از دوخطی بودن نگاشت e به صورت زیر قابل پیگیری است.

$$\begin{aligned} e(P, V) &= e(P, S_{ID} + rH) \\ &= e(P, S_{ID}).e(P, rP) \\ &= e(sP, Q_{ID}).e(rP, H) \\ &= e(P_{pub}, Q_{ID}).e(rP, H) \end{aligned} \qquad (۱۰)$$

از حیث برآورد هزینهٔ پیاده‌سازی می‌توان گفت که در روش Chau-Cheon در عملیات امضا بایستی دو ضرب اسکالر و یک تابع درهم و در عملیات وارسیِ امضا، یک تابع درهم و یک جمع در گروهِ G_1 و دو زوج‌نگار دوخطی محاسبه شود. در روش پیشنهادی برای عملیات امضا لازم است یک ضرب اسکالر و یک جمع در گروهِ G_1 و یک تابع درهم محاسبه شود و برای انجام وارسی یک تابع درهم و سه زوج‌نگار دوخطی باید محاسبه گردد. در اینجا منظور از ضرب اسکالر محاسبهٔ حاصلضرب عنصری از گروه G_2 در عنصری از گروه G_1 است که زمان محاسبهٔ آن از جمع در گروهِ G_1 بسیار بیشتر است. زمان محاسبهٔ یک زوج‌نگار دوخطی از هر دوی این عملگرها بیشتر است [۲]. بنابراین می‌توان گفت که هزینهٔ روش پیشنهادی در مرحلهٔ امضا اندکی کمتر از روش Chau-Cheon و در مرحلهٔ وارسی اندکی بیش از آن شده است. در عوض روش پیشنهادی از حیث امنیتی دارای ویژگی جدیدی نسبت به روش Chau-Cheon می‌باشد که در بخش بعد به آن می‌پردازیم.

۵- تحلیل امنیت، حصول ویژگی جعل ناپذیری و تکمیل روش

روش امضای پیشنهادی تمامی ویژگیهای امضای Chau-Cheon را به ارث می‌برد که به علت اثبات امنیت در مرجع



شکل ۱ : جعل امضا توسط مرکز

[۷] از پرداختن دوباره به آن صرفنظر می‌کنیم. اما همانگونه که قبلاً بیان گردید هدف اصلی از ارائهٔ این امضا دستیابی به ویژگی عدم انکار و جلوگیری از امکان جعل امضای کاربران سیستم هویت‌گرا توسط KGC است. ادعا می‌شود که چنانچه مرکز اقدام به جعل امضای کاربر نماید، کاربر قادر است اثباتی دال بر گناهکار بودنِ KGC ارائه نماید. مرکز از S_{ID} آگاه است و تنها r را در اختیار ندارد. وی با انتخاب $r' \in_R Z_q^*$ طبق شکل (۱) اقدام به جعل امضا می‌نماید. واضح است که امضای جعلیِ $< r'P, V' >$ در رابطهٔ وارسی صدق می‌کند و وارسی کننده امضای جعلی را تأیید می‌نماید. اما کاربری که هویت وی جعل شده است اثبات می‌کند که $r'P$ جعلی است ومرکز را رسوا می‌نماید. وی با ارائهٔ نیمهٔ اول کلید عمومی خود یعنی rP به دادگاه، اثبات می‌کند که کلید خصوصی متناظر با آن یعنی $S_{ID} = sQ_{ID} = sH_1(ID, rP)$ را در اختیار دارد. توجه کنید که ضرب شدنِ s در Q_{ID} به مثابهٔ این است که مرکز، Q_{ID} را با کلید خصوصی خودش امضا نموده است؛ بنابراین اثبات می‌شود که مرکز برای یک نفر دو کلید خصوصی صادر نموده است و به عنوان متخلف شناخته می‌شود. در حقیقت در صدور کلید به این روش، rP مانند گواهی خامی است که برای کاربر با هویت ID ترتیب داده شده است و مرکز نیز آن را به صورت $sH_1(ID, rP)$ امضا نموده است.

در پایان توجه به یک نکته ضروری است و آن اینکه چون کلید کاربران هر چند وقت یکبار باید تعویض شود، ممکن است گفته شود که صدور دو کلید برای یک کاربر امری طبیعی است و به منزلهٔ تخلف مرکز نخواهد بود. اما در پاسخ می‌توان گفت که با ذکر تاریخ صدور و انقضای کلید در Q_{ID} این مشکل به راحتی برطرف می‌شود. بنابراین باید Q_{ID} را به صورت رابطهٔ (۱۱) محاسبه نمود.

$$Q_{ID} = H_1(ID \| T, rP) \qquad (11)$$

که در آن T دربردارندهٔ زمان تولید و انقضای کلید عمومی rP می‌باشد.

۶- نتیجه‌گیری

در این مقاله به منظور حذف دسترسی مرکز تولید کلید به کلید خصوصی کاربران در سیستمهای رمز هویت‌گرا و امکانِ داشتن امضای غیر قابل انکار، یک روش امضای هویت‌گرا با ویژگی عدم انکار پیشنهاد شد. ویژگی عدم انکار بدست آمده صریح نیست به این مفهوم که مرکز قادر به جعل امضای کاربر هست اما کاربر می‌تواند جعلی بودن امضا را اثبات نماید. هزینهٔ پیاده سازی روش پیشنهادی در مقایسه با روش امضای هویت‌گرایِ Chau-Cheon تفاوت چندانی ندارد.

مراجع

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

[2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proceedings of CRYPTO 2001, LNCS 2139, pp. 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, pp. 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, pp. 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, pp. 223-238, Springer-Verlag, 2004.
[6] H. Mala, M. Dakhil-alian and M. Brenjkoub, "A New Identity-based Proxy Signature Scheme from Bilinear Pairings," Proceedings of IEEE International Conference on Information & Communication Technologies:from Theory to Applications(ICTTA'2006), Syria, 2006.
[7] J.C. Cha and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," Public Key Cryptography – PKC 2003, volume 2567 of Lecture Notes in Computer cience, pp. 18–30. Springer-Verlag, 2002.