دسترسی در سایتِ http://jnrm.srbiau.ac.ir
سال دوم، شماره هشتم، زمستان ۱۳۹۵
شماره شاپا: ۱۶۸۲-۰۱۹۶

دانشگاه آزاد اسلامی، واحد علوم و تحقیقات

پژوهش‌های نوین در ریاضی

ارائه پروتکل جدید امضای دیجیتال کور مبتنی بر مسأله لگاریتم گسسته روی منحنی بیضوی

رضا شاهوردی *

دانشیار، دانشکده علوم ریاضی، دانشگاه آزاد اسلامی واحد قائمشهر، قائمشهر، ایران

تاریخ دریافت مقاله: ۹۵/۰۶/۱۶ تاریخ پذیرش مقاله: ۹۵/۱۰/۲۳

چکیده

در سال‌های اخیر سعی بر آن بوده است که با توجه به پیچیدگی محاسباتی کمتر و استحکام بیشتر مساله‌ی لگاریتم گسسته در منحنی بیضوی نسبت به سایر مسائل سخت، در کاربردهایی همچون امضای کور، روش رمزنگاری منحنی بیضوی جایگزین سایر روش‌ها همچون رمزنگاری DLP شود. در این مقاله، یک طرح امضای کور جدید مبتنی بر سیستم رمزنگاری منحنی بیضوی پیشنهاد شده است. طرح ارائه شده، به شیوه‌ای امن و کارآمد قادر است نیازهای یک سیستم امضای دیجیتال کور را برآورده کند. تحلیل و ارزیابی کارایی پروتکل ارائه شده در مقایسه با روش‌های که در گذشته مطرح شده است، برتری روش پیشنهادی را نشان می‌دهد.

واژه‌های کلیدی: امضای دیجیتال کور، لگاریتم گسسته، رمزنگاری منحنی بیضوی.

* .E-mail address: shahverdi_592003@yahoo.com

۱- مقدمه

همگام با رشد روز افزون شبکه‌های کامپیوتری و مخابرات دیجیتال، بکارگیری روش‌های مناسب برای برقراری ارتباطات امن در این سیستم‌ها امری حیاتی است. اتخاذ مکانیزم‌های بهینه برای این منظور بیش از پیش در کارایی چنین سیستم‌هایی تاثیرگذار می‌باشد. امروزه تحقیقات گسترده‌ای در این زمینه در حال انجام است. در این راستا، امضای کور با توجه به اساسی بودن نقش آنها در بسیاری از کاربردها، یکی از دغدغه‌های افرادی است که در حیطه‌ی رمزنگاری مشغول تحقیق و مطالعه هستند و در پی طرح ایده‌های جدیدتر، با کارایی مناسب‌تر و هزینه‌ی محاسباتی کمتر می‌باشند. طرح امضای‌کور یک طرح مهم رمزنگاری است و در پروتکل‌هایی که بی‌نام بودن مشترکین را تضمین می‌کند مفید است.

ایده طرح امضای کور در سال ۱۹۸۲، توسط دیوید چام مطرح شد[۸]. امضای کور دو موجودیت را شامل می‌شود: درخواست کننده‌ی امضا و امضا کننده. بر خلاف امضای دیجیتال که متقاضی امضا خودش امضا کننده‌ی پیام است، در یک طرح امضای کور، امضا کننده و متقاضی امضا دو نقش کاملاً متفاوت‌اند. در امضا دیجیتال در یک طرف امضا و در طرف دیگر تشخیص صحت امضا انجام می‌گردد. اما در یک طرح امضای کور، پروتکل امضا شامل مراحلی از قبیل کور کردن پیام توسط متقاضی امضا، امضای پیام کور توسط امضا کننده، بازگشائی کوری از امضا و بدست آوردن امضای معتبر توسط متقاضی امضا می باشد.

در امضای کور سه خصیصه بنیادی وجود دارد که بایستی برآورده شود: کور بودن پیام، غیر قابل ردیابی بودن و غیر قابل جعل پذیری.

کور بودن به این معنی است که متن پیام باید برای امضا کننده غیر قابل مشاهده باشد. غیر قابل جعل بودن نیز به این معناست که فقط امضا کننده می بایست قادر به تولید امضای معتبر باشد. غیر قابل ردیابی بودن نیز زمانی برآورده می‌شود که اگر امضای کور برای عموم آشکار شود، امضا کننده نتواند درخواست کننده امضا را شناسایی کند. امضای کور را می‌توان با یک مثال ساده توصیف کرد. فرض کنید پیامی را در داخل یک پاکت قرار دهیم و آن را برای امضا به سمت امضا کننده ارسال کنیم. امضا کننده بدون باز کردن پاکت، آن را امضا می‌کند. این پاکت قابلیت انتقال اثر امضا بر روی پیام دارد[۱۱]. با توجه به اساسی بودن نقش امضای کور در کاربردهایی همچون رای‌گیری الکترونیکی، پول الکترونیکی طراحی پروتکلی کارامد با امنیت بالا برای تولید امضای کور برای استفاده در این کاربردها یکی از اهداف انجام این بررسی است[۱۲،۲۱،۲۲].

اخیرا طرح‌های متعددی از امضای کور بر پایه مسئله لگاریتم گسسته ارائه و درباره آنها بحث شده است[۱۷،۱۸]. در سال ۱۹۹۵،کارمنیش و همکارانش یک طرح امضای کور بر پایه لگاریتم گسسته ارائه کردند[۱]. بلافاصله هارن طی مقاله‌ی به این موضوع اشاره کرد که طرح ارائه شده بوسیله‌ی کارمنیش از سوی امضا کننده قابل ردیابی است. به عبارتی اصل Untraceability در مورد روش مذکور برقرار نیست[۹]. سپس هارستر و دوستانش نشان دادند که تجزیه و تحلیل هارن صحیح نبوده است و غیر قابل ردیابی بودن روش را مورد تایید قرار دادند[۱۰]. با این وجود در ادامه لی، همکارانش[۴] ثابت کردند که مطالب هارستر درباره حمله هارن اشتباه بوده است و تاکید بر برآورده نشدن ویژگی غیرقابل ردیابی بودن روش کارمنیش داشته و همچنین یک طرح بهبود یافته امضا کور جدید، به منظور بالا بردن امنیت طرح کارمنیش برای مقاومت در برابر حمله مطرح شده توسط هارن ارائه کردند.

در این مقاله با هدف ایجاد بهبود در سیستم رمزنگاری مبتنی بر لگاریتم گسسته، یک طرح امضای کور جدید مبتنی بر مسأله لگاریتم گسسته روی منحنی بیضوی، پیشنهاد شده است، که به لحاظ توانایی امکان بیشتری در فراهم آوردن امکانات امنیتی مورد نیاز نسبت به طرح‌های ارائه شده بر پایه‌ی مسأله فاکتورگیری عدد صحیح و مسأله لگاریتم گسسته دارد. از دیگر ویژگی‌های این روش دارا بودن سایز کوچک کلید است که در نتیجه سرعت بیشتر، مصرف پهنای باند کمتر و کاهش سربار محاسباتی را خواهیم داشت[۱۴،۲۰].

سایر بخش‌های مقاله بدین‌صورت سازماندهی شده است:

در بخش ۲، برخی از مفاهیم مقدماتی طرح فوق مطرح می‌شود. در بخش ۳ طرح لی، هوانگ و حمله ارائه شده به این طرح از مرجع[۵] بیان می‌گردد. در ادامه در بخش ۴، پروتکل پیشنهادی معرفی می‌گردد و ویژگی‌های امنیتی طرح پیشنهادی در بخش ۵ بررسی می‌شود. در بخش۶ نیز عملکرد پروتکل ارائه شده را، با دیگر پروتکل‌ها مقایسه می‌کنیم و در نهایت در بخش ۷ نتیجه‌گیری و جمع بندی مطالب صورت می‌پذیرد.

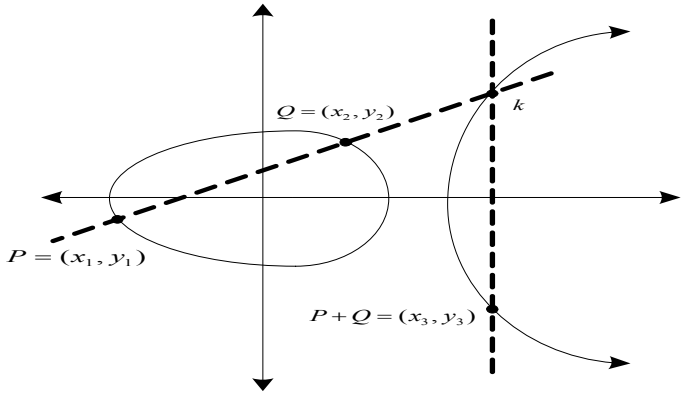
۲- مفاهیم اولیه

تحقیق و بررسی بر روی سیستم‌های رمز نگاری منحنی بیضوی اولین بار توسط میلر[۶] و کوبلیتز[۷] صورت گرفت. این بررسی آنها را به سمت معادلاتی با خواص ویژه هدایت کرد که از آنها می‌شد به راحتی در رمزنگاری استفاده کرد.

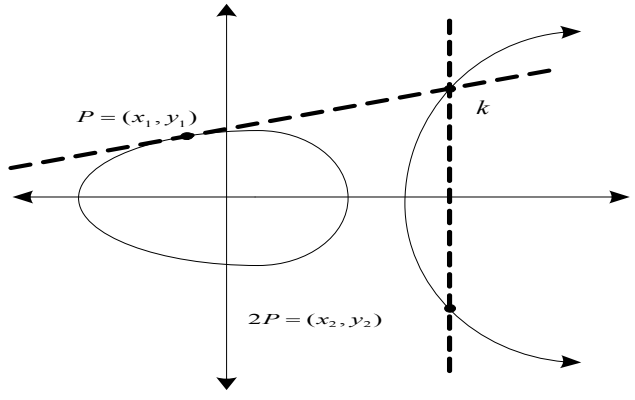
یک منحنی بیضوی روی $GF(2^m)$ عبارت است از نقطه‌ای در بی‌نهایت که به صورت O نمایش داده می‌شود، بعلاوه‌ی تمام نقاط به صورت (x,y) با این شرط که $(x, y)\in GF(2^m)$ باشند و در رابطه‌ی (۱) صدق کنند.

$$y^2 + xy = x^3 + ax^2 + b \qquad (۱)$$
$$a,b \in GF(2^m), b \neq 0$$

به‌طور کلی دو عملگر به نام‌های جمع نقطه‌ای و دو برابر کردن نقطه‌ای روی نقاط یک منحنی بیضوی تعریف می‌شود که به ترتیب در شکل ۱ و ۲ نمایش داده شده است.



شکل ۱. جمع نقطه‌ای در منحنی بیضوی



شکل ۲. دو برابر کردن نقطه‌ای در منحنی بیضوی

حال فرض کنید که منحنی بیضوی C روی میدان گالوای $GF(2^m)$ تعریف شده است، بنابراین روابط زیر برقرار هستند.

۱. $O + O = O$

۲. به ازای هر نقطه‌ای مثل P روی منحنی C داریم: $P+O=P$، بنابرین O عضو خنثی در جمع نقطه‌ای محسوب می‌شود.

۳. به ازای هر دو نقطه مثل P و Q روی منحنی C اگر داشته باشیم: $P+Q = O$، آنگاه معکوس نقطه‌ی P نقطه‌ی Q خواهد بود و برعکس. در این حالت اگر فرض کنیم p برابر (x, y) باشد ، آنگاه Q برابر خواهد بود با $(x, -x-y)$.

۴. فرض کنید که $P = (x_1, y_1)$ و $Q = (x_2, y_2)$ و همچنین حاصل جمع نقطه‌ای P و Q برابر نقطه‌ای مثل (x_3, y_3) باشد، آنگاه:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \qquad (۲)$$

که در آن λ از رابطه‌ی (۳) محاسبه می‌شود.

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1} \qquad (۳)$$

۵. فرض کنید که $P = (x_1, y_1)$ و همچنین حاصل دو برابر کردن نقطه‌ای P برابر نقطه‌ای مثل (x_2, y_2) باشد، آنگاه:

$$x_2 = \lambda^2 + \lambda + a$$
$$y_2 = \lambda(x_1 + x_3) + x_3 + y_1 \qquad (۴)$$

که در آن λ از رابطه‌ی (۵) محاسبه می‌شود.

$$\lambda = x_1 + \frac{x_1}{y_1} \qquad (۵)$$

اصلی‌ترین عملیات در رمزنگاری منحنی بیضوی عملیاتی موسوم به ضرب نردبانی است و همان طور که در (۶) نشان داده شده منظور این است که نقطه‌ای مثل P را k بار با خودش جمع نقطه‌ای کنیم و در نهایت به نقطه‌ای مثل Q برسیم.

$$Q = kp = \underbrace{p + p + \ldots + p}_{k} \qquad (۶)$$

برای هر نقطه‌ی P، به حداقل مقدار k که به ازای آن Q برابر نقطه‌ی بی‌نهایت (O) شود، مرتبه‌ی نقطه‌ی P می‌گویند.

اگر P و Q نقاط روی یک منحنی بیضوی باشند و داشته باشیم $Q = kP$ آنگاه با معلوم بودن دو نقطه‌ی P و Q، پیدا کردن مقدار k در عمل غیر ممکن است. این موضوع مسأله‌ی لگاریتم گسسته روی منحنی بیضوی نامیده می‌شود.

۳- تجزیه و تحلیل یک طرح امضای کور

در این بخش ابتدا پروتکل امضای کور [۴] توصیف می‌گردد و سپس در ادامه به شرح حمله وارد بر این طرح و چگونگی مقاوم سازی پروتکل در برابر حمله مطرحی می‌پردازیم.

۳-۱- طرح امضای کور لی هوانگ یانگ

در این بخش پروتکل پیشنهادی لی، هوانگ و یانگ بطور مختصر بیان می‌گردد. در این طرح امضا دو نوع شرکت کننده در نظر گرفته می‌شود: امضا کننده و گروهی از کاربران. یک کاربر از امضا کننده درخواست می‌کند با توجه به اعتبارش نزد امضا کننده متنی را برای او بدون این‌که بتواند محتوای آنرا ببیند، امضا نماید. امضا کننده نیز با توجه به اعتبار درخواست کننده امضا را تولید می‌کند. جزئیات مربوط به چگونگی این روند در ادامه شرح داده می‌شود.

امضا کننده ابتدا دو عدد اول (p,q) را به‌قسمی انتخاب می‌کند که $q|p-1$ گردد. او سپس یک عدد صحیح g را طوری انتخاب می‌کند که مولد با مرتبه q از Z_p^* باشد. همچنین یک عدد صحیح x را بعنوان کلید خصوصی اش انتخاب و $y \equiv g^x \bmod p$ را محاسبه می‌کند و آنگاه مقادیر (p, q, g, y) را به عنوان کلید عمومی منتشر می‌کند. امضا کننده سپس به‌طور تصادفی مقادیر $\bar{k}_1, \bar{k}_2, b_1, b_2$ را در Z_q انتخاب و $\bar{r}_2 \equiv g^{\bar{k}_2} \bmod p$ و $\bar{r}_1 \equiv g^{\bar{k}_1} \bmod p$ را بطوریکه روابط

$\gcd(\bar{r}_1, q), \gcd(\bar{r}_2, q) = 1$

برقرار باشند، محاسبه می‌کند. آنگاه امضا کننده مقادیر $\bar{r}_1, \bar{r}_2, b_1, b_2$ را برای متقاضی می‌فرستد.

متقاضی پس از دریافت مقادیر، پنج مقدار a, b, c, d, e به طور تصادفی انتخاب و آنها را بصورت خصوصی نزد خود نگه می‌دارد و سپس مقادیر $r_1 \equiv \bar{r}_1^{ab_1} g^c \bmod p$، $r_2 \equiv \bar{r}_2^{bb2} g^e \bmod p$ ، $r \equiv (r_1 r_2)^d \bmod p$ محاسبه کرده و با استفاده از آنها اقدام به کور کردن پیام m می‌کند.

$\bar{m}_1 \equiv m\bar{r}_1 \frac{r^{-1}}{2} ad (\bmod q)$ ، $\bar{m}_2 \equiv m\bar{r}_2 \frac{r^{-1}}{2} bd (\bmod q)$

در نهایت $(\bar{m}_1, \bar{m}_2)$ برای امضا کننده می‌فرستد.

امضا کننده نیز $\bar{s}_1 \equiv x\bar{r}_1 + \bar{k}_1 b_1 \bar{m}_1 \bmod q$،

$\bar{s}_2 \equiv x\bar{r}_2 + \bar{k}_2 b_2 \bar{m}_2 \bmod q$

محاسبه و برای متقاضی می‌فرستد. سرانجام متقاضی برای یافتن امضای معتبر، عمل بازگشایی کوری به‌وسیله محاسبه $s_1 \equiv \bar{s}_1 \bar{r}_1^{-1} \frac{r}{2} + cdm \pmod q$،

$s \equiv (s_1 + s_2) \bmod q$ ، $s_2 \equiv \bar{s}_2 \bar{r}_2^{-1} \frac{r}{2} + edm (\bmod q)$

انجام می‌دهد و امضا معتبر را بدست می‌آورد و سه تائی پیام و امضا را به صورت (m, r, s) برای یک تشخیص دهنده صحت امضا می‌فرستد. اعتبارسنج می‌تواند با بررسی تساوی $g^s \equiv y^r r^m \bmod p$، صحت و اعتبار امضا را تایید و یا رد کند.اگر تساوی برقرار باشد امضاء تایید می‌شود و در غیر اینصورت نقض می‌شود.

۳-۲- حمله به طرح امضای کور لی هوانگ یانگ

در پروتکل مطرح شده در بخش ۳-۱، اگر متقاضی درستکار نباشد، می‌تواند دو امضای معتبر برای دو پیام جداگانه، تنها با اجرای یکبار پروتکل با امضا کننده بدست می‌آورد[۵]. شرح این حمله در ادامه مطرح می‌گردد.

مرحله راه اندازی مانند قبل انجام می‌شود، با این تفاوت که متقاضی بجای محاسبه $r_1 \equiv \bar{r}_1^{ab_1} g^c \bmod p$ و $r_2 \equiv \bar{r}_2^{bb2} g^e \bmod p$ مقادیر $r_2 \equiv (\bar{r}_2^{bb2} g^e)^d \bmod p$، $r_1 \equiv (\bar{r}_1^{ab_1} g^c)^d \bmod p$ را محاسبه می‌کند. در این حمله نیازی به محاسبه r نیست. سپس متقاضی پیام را با محاسبه $(\bar{m}_1, \bar{m}_2)$ کور کرده و برای امضا کننده می‌فرستد.

$\bar{m}_1 \equiv m_\alpha \bar{r}_1 \bar{r}_1^{-1} ad (\bmod q)$ ، $\bar{m}_2 \equiv m_\beta \bar{r}_2 \bar{r}_2^{-1} bd (\bmod q)$

.

امضاء کننده نیز با محاسبه

$\bar{s}_1 \equiv x\bar{r}_1 + \bar{k}_1 b_1 \bar{m}_1 \bmod q$ ، $\bar{s}_2 \equiv x\bar{r}_2 + \bar{k}_2 b_2 \bar{m}_2 \bmod q$

امضا کور را تولید و سپس $(\bar{s}_1, \bar{s}_2)$ را برای متقاضی (حمله کننده) می‌فرستد. متقاضی مقادیر

$s_1 \equiv \bar{s}_1 \bar{r}_1^{-1} r_1 + cdm_\alpha \pmod q$ و

$s_2 \equiv \bar{s}_2 \bar{r}_2^{-1} r_2 + edm_\beta \pmod q$

محاسبه و (m_α, r_1, s_1)، (m_β, r_2, s_2) را منتشر می‌کند. اعتبارسنج می‌تواند با بررسی تساوی

$g^{s_1} \equiv y^{r_1} r^{m_\alpha} \pmod p$ ، $g^{s_2} \equiv y^{r_2} r^{m_\beta} \pmod p$

زیر صحت و اعتبار امضاء را تایید و یا رد کند.

این دو امضای معتبر برای دو پیام مجزا تنها با اجرای یکبار پروتکل بدست می‌آیند و می‌توان اثبات کرد که این دو امضا (s_1, s_2) برای دو پیام (m_α, m_β) معتبر است. جزئیات چگونگی اثبات صحت سنجی این طرح در[۵] بیان شده است.

۳-۳- مقاوم سازی در برابر حمله وارد شده بر طرح

برای بهبود طرح کافی است آنجایی‌که متقاضی پنج فاکتور را جهت کوری پیام انتخاب می‌کند، به این پنج فاکتور یک مقدار دیگر نیز بیفزایم و به صورت زیر عمل کنیم.

امضا کننده در فاز اولیه به‌طور تصادفی مقادیر $\bar{k}_1, \bar{k}_2, b_1, b_2$ را انتخاب کرده و در نهایت مقادیر $(\bar{r}_1, \bar{r}_2, b_1, b_2)$ را محاسبه و برای متقاضی می‌فرستد. سپس متقاضی شش مقدار (a, b, c, d, e) انتخاب و روابط $r_1 \equiv \bar{r}_1^{ab_1} g^c \bmod p$، $r_2 \equiv \bar{r}_2^{bb2} g^e \bmod p$ ، $r \equiv (r_1^d r_2^f) \bmod p$ محاسبه می‌کند. متقاضی پیام، با محاسبه $\bar{m}_1 \equiv m\bar{r}_1 2r^{-1} ad (\bmod q)$، $\bar{m}_2 \equiv m\bar{r}_2 2r^{-1} bf (\bmod q)$ متن را ناخوانا کرده و $(\bar{m}_1, \bar{m}_2)$ به امضا کننده می‌دهد. امضا کننده،

$\bar{s}_1 \equiv x\bar{r}_1 + \bar{k}_1 b_1 \bar{m}_1 \bmod q$ ، $\bar{s}_2 \equiv x\bar{r}_2 + \bar{k}_2 b_2 \bar{m}_2 \bmod q$

را محاسبه و $(\bar{s}_1, \bar{s}_2)$ برای متقاضی می‌فرستد. سرانجام متقاضی برای یافتن امضای معتبر، عمل بازگشایی کوری

با محاسبه

$s_2 \equiv \bar{s}_2 \bar{r}_2^{-1} \frac{r}{2} + efm \pmod q$ ، $s_1 \equiv \bar{s}_1 \bar{r}_1^{-1} \frac{r}{2} + cdm \pmod q$

$s \equiv (s_1 + s_2) \bmod q$ انجام و امضا معتبر بدست می‌آورد. سپس متقاضی سه تائی پیام، امضا به صورت (m, r, s)، برای تشخیص دهنده امضا می‌فرستد. صحت و اعتبار امضا با بررسی تساوی $g^s \equiv y^r r^m \bmod p$ تایید و یا رد می‌گردد.

۴- ارائه پروتکل پیشنهادی

در این بخش، پروتکل پیشنهادی خود را ارائه می‌کنیم. در طرح امضای کور پیشنهادی دو موجودیت و پنج فاز در نظر گرفته می‌شود. در مرحله‌ی اول امضا کننده اطلاعات لازم را منتشر می‌کند. در مرحله‌ی دوم به‌منظور دریافت امضا روی یک متن پوشیده شده، درخواست کننده یک نسخه‌ی پوشیده شده از پیام برای امضا کننده ارسال می‌کند. امضا کننده، پیام مخفی شده را امضا و آن را برای درخواست کننده ارسال می‌نماید. سپس درخواست کننده، امضای امضا کننده را از اطلاعات دریافتی استخراج می‌کند. در مرحله‌ی اعتبارسنجی نیز اعتبار امضای اعلام شده بررسی می‌شود. جزئیات مربوط به مراحل پروتکل را از طریق فرایندهای زیر توصیف می‌کنیم:

۴-۱- فاز آماده سازی پروتکل

امضا کننده یک میدان متناهی به عنوان پایه تعیین می‌کند. در این فاز سایز میدان و نوع میدان گالوا $GF(q)$ تعیین شده و همچنین نوع منحنی بیضوی نیز در این فاز تعیین می‌گردد. از آنجا که محاسبات روی میدان‌های گالوای باینری سریع انجام می‌شوند و نیز الگوریتم‌های سریع و کارآمدی برای پیاده سازی محاسبات روی $GF(2^m)$ ارائه شده است، معمولاً این میدان انتخاب می‌شود (m سایز میدان را مشخص می‌کند). نقطه‌ی اساسی $G \in E(F_q)$ برای منحنی بیضوی مورد نظر و مرتبه‌ی اساسی روی منحنی بیضوی (n) نیز در این فاز تعیین می‌شود.

امضا کننده عدد تصادفی d، از بازه $[1, n-1]$ به عنوان کلید خصوصی خود انتخاب و سپس با ضرب کردن نقطه‌ی آن در نقطه اساسی، نقطه $Q = dG$ را به عنوان کلید عمومی محاسبه می‌کند.

۴-۲- فاز درخواست امضا

به ازای هر درخواست از طرف کاربر، امضا کننده به منظور تولید امضا برای متن m مراحل زیر را انجام می‌دهد:

۱. انتخاب اعداد تصادفی $(\bar{k}_1, \bar{k}_2, b_1, b_2)$ از بازه‌ی $[1, n-1]$

۲. محاسبه نقاط $\bar{R}_1 = \bar{K}_1 G$ ، $\bar{R}_2 = \bar{K}_2 G$

۳. ارسال مقادیر $(\bar{R}_1, \bar{R}_2, b_1, b_2)$ برای درخواست کننده

در ادامه درخواست کننده به صورت تصادفی شش فاکتور تصادفی (a, b, c, d, e, f) از بازه‌ای $[1, n-1]$ به عنوان عوامل مخفی کننده انتخاب می‌کند و مقدار آنها را به صورت مخفی نزد خودش نگهداری می‌کند.در نهایت درخواست کننده نقطه‌ای R را مطابق رابطه‌ی (۷) محاسبه می‌کند. نقطه دارای مختصات (x_0, y_0) می‌باشد.

$$R_1 \equiv \bar{R}_1 (ab_1) + cG \qquad (۷)$$
$$R_2 \equiv \bar{R}_2 (bb_2) + eG$$
$$R \equiv R_1 d + R_2 f$$

اگر نقطه‌ی R برابر نقطه‌ی در بینهایت (عضو خنثی) باشد، درخواست کننده مجبور است مجددا مقادیر دیگری را برای فاکتورهای کوری، به صورت تصادفی تولید نماید و دوباره مقدار R را مطابق رابطه‌ی بالا محاسبه نماید. درخواست کننده در ادامه مقادیر پارامترهای $\bar{R}_{1x}, \bar{R}_{2x}, R_x$ را به صورت $r \equiv x_0 \bmod n$ محاسبه می‌کند.

سپس درخواست کننده متن پوشیده شده $\bar{m}_1, \bar{m}_2$ را با محاسبه رابطه‌ی (۸) بدست آورده و در نهایت آنها را برای امضا شدن به سوی امضا کننده ارسال می‌کند (R^{-1} عملگر معکوس روی Z_n است).

$$\bar{m}_1 \equiv m \bar{R}_{1x} (2 R_x^{-1}).ad \qquad (۸)$$
$$\bar{m}_2 \equiv m \bar{R}_{2x} (2 R_x^{-1}).bf$$

۴-۳- فاز تولید امضا

امضا کننده، بعد از دریافت مقادیر ارسالی از جانب متقاضی با استفاده از کلید خصوصی خود و محاسبه رابطه‌ی (۹)، امضا روی متن مخفی بدست آورده و مقادیر $\bar{s}_1, \bar{s}_2$ برای درخواست کننده ارسال می‌کند. امضا کننده در این مرحله مقادیر تصادفی که در مرحله راه‌اندازی انتخاب کرده بود را به پیام تزریق می‌نماید.

$$\bar{s}_1 \equiv d \bar{R}_{1x} + b_1 \bar{k}_1 \bar{m}_1 \qquad (۹)$$
$$\bar{s}_2 \equiv d \bar{R}_{2x} + b_2 \bar{k}_2 \bar{m}_2$$

۴-۴- فاز استخراج امضا

درخواست کننده بعد از دریافت $\overline{s}_1$, $\overline{s}_2$، مقدار S را با محاسبه هم‌نهشتی (۱۰) محاسبه می‌کند. در نهایت امضا کننده زوج (m, R, S) را به عنوان امضای متن m توسط امضا کننده در نظر می‌گیرد و مورد استفاده قرار می‌دهد.

$$s_1 \equiv \overline{S}_1 \left(\overline{R}_{1x}\right)^{-1} \left(R_x/2\right) + cdm \qquad (۱۰)$$
$$s_2 \equiv \overline{S}_2 \left(\overline{R}_{2x}\right)^{-1} \left(R_x/2\right) + efm$$
$$S \equiv S_1 + S_2$$

۴-۵- فاز اعتبارسنجی

بررسی تایید درستی امضا (R, S) برای متن m توسط ارزیابی مراحل زیر انجام می‌گیرد و در صورت تایید مورد استفاده قرار می‌گیرد.

(۱) محاسبه‌ی $v \equiv SG$

(۲) محاسبه‌ی $u \equiv \left(R_x Q + mR\right)$

(۳) تصدیق امضا اگر $u = v$

مراحل مختلف طرح پیشنهادی در شکل ۳ خلاصه شده است.

۵- آنالیز امنیت روش پیشنهادی

در این بخش به ارزیابی امنیت پروتکل پیشنهادی مشابه با روشی که در[۱۵،۱۶] استفاده شده است، می‌پردازیم و نشان می‌دهیم که روش پیشنهاد شده کلیه خواص امنیتی مورد نیاز یک طرح امضای کور را به‌درستی برآورده می‌سازد.

۵-۱- به لحاظ درستی و صحت سنجی

برای اثبات درستی امضا زمانی‌که متن و امضا دستکاری نشده‌اند، یک تشخیص دهنده امضا با دارا بودن مقادیر (R, S) و پیام و چک کردن روابط (۱۱) پی به صحت امضای تولید شده می‌برد.

$$v = SG \equiv \left(S_1 + S_2\right) G \qquad (۱۱)$$
$$\equiv \begin{bmatrix} \left(\overline{S}_1 \left(\overline{R}_{1x}\right)^{-1} \left(R_x/2\right) + cdm\right) \\ + \left(\overline{S}_2 \left(\overline{R}_{2x}\right)^{-1} \left(R_x/2\right) + efm\right) \end{bmatrix} G$$
$$\equiv \begin{pmatrix} \left[\left(d\overline{R}_{1x} + b_1 \overline{k}_1 \overline{m}_1\right)\overline{R}_{1x}^{-1} \left(R_x/2\right) + cdm\right] \\ + \left[\left(d\overline{R}_{2x} + b_2 \overline{k}_2 \overline{m}_2\right)\overline{R}_{2x}^{-1} \left(R_x/2\right) + efm\right] \end{pmatrix} G$$
$$\equiv \begin{pmatrix} \left[d\left(R_x/2\right) + b_1 \overline{k}_1 \left(m\overline{R}_{1x}\left(2R_x^{-1}\right)ad\right)\overline{R}_{1x}^{-1}\left(R_x/2\right) + cdm\right] \\ + \left[d\left(R_x/2\right) + b_2 \overline{k}_2 \left(m\overline{R}_{2x}\left(2R_x^{-1}\right)bf\right)\overline{R}_{2x}^{-1}\left(R_x/2\right) + efm\right] \end{pmatrix} G$$
$$\equiv \left[dR_x + m\left(b_1 \overline{k}_1 ad + cd + b_2 \overline{k}_2 bf + ef\right)\right] G$$
$$\equiv R_x G + mR = u$$

شکل ۳. مراحل پروتکل پیشنهاد شده برای تولید امضای کور

	User		Signer
Initialization	Waiting		Select his private key, d, randomly Declares $Q = dG$ as his public key Select $\overline{k}_1, \overline{k}_2, b_1, b_2$ randomaly and Computes $R_1 = \overline{k}_1 G, R_2 = \overline{k}_2 G$
		R_1, R_2, b_1, b_2 ←	
Requesting	Select (a, b, c, d, e, f) randomaly Computes $R_1 \equiv \overline{R}_1(ab_1) + cG$ $R_2 \equiv \overline{R}_2(bb_2) + eG$ $R \equiv R_1 d + R_2 f$ Computes $r \equiv x_0 \bmod n$ Computes $\overline{m}_1 \equiv m\overline{R}_{1x}\left(2R_x^{-1}\right).ad$ $\overline{m}_2 \equiv m\overline{R}_{2x}\left(2R_x^{-1}\right)bf$		Waiting
		$\overline{m}_1, \overline{m}_2$ →	
Singing	Waiting		Computes $\overline{s}_1 \equiv d\overline{R}_{1x} + b_1\overline{k}_1\overline{m}_1$ $\overline{s}_2 \equiv d\overline{R}_{2x} + b_2\overline{k}_2\overline{m}_2$
		$\overline{s}_1, \overline{s}_2$ ←	
Extraction (Unblinding)	Computes $s_1 \equiv \overline{S}_1\left(\overline{R}_{1x}\right)^{-1}\left(R_x/2\right) + cdm$ $s_2 \equiv \overline{S}_2\left(\overline{R}_{2x}\right)^{-1}\left(R_x/2\right) + efm$ $S \equiv S_1 + S_2$ Declares signature (R, S) as public		
Verification	If $SG \equiv R_x Q + mR$ Then validate the signature;		

۵-۲- به لحاظ غیر قابل جعل بودن

فرض کنید امضای جعلی برای پیامی دستکاری شده مثل m^* برابر با (S^*, R^*) بشود. در نتیجه حمله کننده به روشی باید قادر باشد مقادیر S^* و R^* را طوری پیدا کند که رابطه‌ی مربوط به اعتبارسنجی (۱۲) برقرار شود.

$$S^*G \equiv r^*Q + m^*R^* \qquad (۱۲)$$

ابتدا فرض می‌کنیم در بدترین حالت حمله کننده بتواند نقطه‌ی R^* در معادله‌ی بالا را به طریقی بدست آورد و سپس سعی در محاسبه‌ی مقدار S^* داشته باشد. از آنجایی که مقادیر Q, R^*, m^*, r^* همگی در اختیار جعل کننده قرار دارند در نتیجه جعل کننده مقدار نقطه‌ی (S^*G) را نیز دارد. با این وجود برای بدست آوردن S^*، جعل کننده باید مساله لگاریتم گسسته برای منحنی بیضوی را حل کند. بنابر آنچه که قبلا مطرح شد، حل این رابطه برای جعل کننده غیر ممکن خواهد بود. از طرف دیگر، با این فرض که جاعل مقدار S^* را بتواند به درستی در اختیار داشته باشد، قصد داریم نشان دهیم که پیدا کردن مقدار مناسب برای R^* به‌طوری که در معادله‌ی اعتبارسنجی (۱۳) صدق کند غیر ممکن خواهد بود.

$$m^*R^* \equiv S^*G - r^*Q \qquad (۱۳)$$

تا قبل از پیدا کردن R^*، مقدار r^* نیز مجهول است. بنابراین نقطه‌ی r^*Q برای جعل کننده نامعلوم است. در نتیجه سمت راست معادله و سمت چپ معادله دو مجهول وجود دارد که دانستن هر کدام منوط به پیدا کردن دیگری است. به نظر تنها راه باقی مانده پیدا کردن روشی در حذف پارامتر r^* از سمت راست است. برای این منظور جعل کننده باید این مقدار را برابر r^*dG قرار دهد. اما از آنجا که مقدار d نمی‌تواند داشته باشد، پس به هیچ عنوان قادر به حذف r^* و پیدا کردن مقداری برای R^* نیست.

۵-۳- به لحاظ غیر قابل ردیابی بودن

برای اثبات غیرقابل‌ردیابی بودن امضای پیشنهادی، در نظر بگیرید امضاکننده به ازای هر درخواست برای تولید امضا مجموعه مقادیر $\left(\left(\overline{K}, \overline{R}\right), \left(\overline{m}, \overline{S}\right)\right)$ را ثبت کند، زمانی‌که پیام m و امضای S, R به‌صورت عمومی اعلام شوند، امضا کننده به منظور ردیابی کردن امضای کور تولیدی، در میان مجموعه هایی که ثبت کرده، جستجو می‌کند و سعی در بررسی درستی معادله‌ی (۱۴) می‌نماید.

$$\begin{aligned} R &\equiv \left[\overline{R}_1(ab_1) + cG\right]d + \left[\overline{R}_2(bb_2) + eG\right]f \\ &\equiv \left[\left(\overline{K}_1 G\right)ab_1 + cG\right]d + \left[\left(\overline{K}_1 G\right)bb_2 + eG\right]f \\ &\equiv \left(\left[\overline{K}_1 ab_1 d + cd\right] + \left[\overline{K}_1 bb_2 f + ef\right]\right)G \end{aligned} \qquad (۱۴)$$

برای این منظور امضا کننده بجز مقدار نقاط **R,G** نیاز به در اختیار داشتن عوامل مخفی کننده نیز دارد. با این حال او تنها مقادیر

$$\left(S, R, m, Q, G, d, \overline{R}_{1,2}, \overline{k}_{1,2}, \overline{m}_{1,2}, \overline{S}_{1,2}, b_{1,2}\right)$$

را برای چک کردن رابطه بالا در اختیار دارد. بدیهی است، پیدا کردن متغیرهای کور کننده از مقادیر ثبت شده ، غیر ممکن است و از انجایی که تساوی **(R)** نیز به خاطر مشکل بودن حل مساله لگاریتم گسسته بر روی منحنی بیضوی اطلاعاتی در رابطه با فاکتورهای مخفی سازی آشکار نمی‌نماید، بنابراین هیچ راهی برای امضا کننده به منظور ردیابی امضا با چک کردن صحت معادله وجود ندارد و در نتیجه روش پیشنهاد شده غیر قابل ردیابی است. از طرفی ما از متغیرهای a, b, d, f برای مخفی کردن پیام در رابطه (۹) استفاده کرده‌ایم و چون امضا کننده هیچگاه قادر به پیدا کردن عوامل مخفی کننده نیست، در نتیجه خاصیت کور بودن پیام از دید امضا کننده نیز به خوبی برآورده می‌شود.

۶- ارزیابی کارایی روش پیشنهادی

در این قسمت روش پیشنهادی را با کارهای انجام شده قبلی مقایسه می‌کنیم. در جدول (۲) نمادهای استفاده شده برای انجام ارزیابی در روش پیشنهادی معرفی شده است. حال با توجه به جدول (۲)، پیچیدگی زمانی واحدهای عملیاتی مختلف بر حسب پیچیدگی زمانی ضرب پیمانه‌ای که از [۳] استخراج شده‌اند در جدول (۳) آورده شده است. به دلیل این‌که اساس و سرانجام روش پیشنهادی پیاده سازی سخت افزاری می‌باشد، در روش پیشنهادی میدان گالوای $GF(2^m)$ انتخاب شده است.

در این مقاله از جدول (۳) به عنوان مرجع برای انجام ارزیابی هزینه استفاده شده است. هدف ارزیابی، اثبات

کاهش هزینه در روش پیشنهادی است. هزینه روش پیشنهادی از لحاظ زمان لازم برای انجام ضرب پیمانه‌ای با روش [۱] و [۵] مقایسه شده است. همان‌گونه که در [۲] اشاره شده است، امضای کور پیشنهادی توسط کارمنیش و همکارانش در مقایسه با سایر روش‌هایی که مبتنی بر مساله لگاریتم گسسته هستند کارایی به مراتب بهتری دارد. در نتیجه ما در این بخش کارایی پروتکل ارائه شده در این مقاله، با روش مذکور مقایسه خواهیم کرد. نتایج این مقایسه در جدول (۱) مورد بررسی قرار گرفته است. همانطور که مشاهده می‌شود، هزینه روش پیشنهادی به مراتب پایین‌تر از دو روش دیگر بوده و دارای کارائی بالاتری نسبت به آن‌هاست.

نتیجه‌گیری

در این مقاله یک طرح امضای کور جدید مبتنی بر رمزنگاری منحنی بیضوی ارائه گردید. مساله سخت در روش پیشنهادی، مسئله لگاریتم گسسته روی منحنی بیضوی می‌باشد که در زمان معقول قابل حل نبوده و بعلاوه روش دارای خصوصیات کلید رمزنگاری کوچکتر، مصرف پهنای باند کمتر، نیاز به قدرت محاسباتی کمتر و سرعت بیشتر خواهد بود. با توجه به برتری‌های ذکر شده طراحی پروتکلی مناسب که بتواند با بکارگیری این سیستم رمزنگاری، امنیت لازم را در سیستم‌های مختلف ارتباطی، برقرار کند از اهداف انجام این مقاله است.

و در نهایت نشان دادیم که پروتکل پیشنهادی ضمن فراهم آوردن سطح امنیتی یکسان در مقایسه با سایر روش‌های مطرحی، پیچیدگی زمانی به مراتب کمتر و کارآیی بهتری برای اجرا دارد.

جدول ۱. مقایسه پیچیدگی زمانی بر حسب زمان مورد نیاز انجام ضرب پیمانه‌ای پیمانه

	پیچیدگی زمانی	برآورد تقریبی
طرح امضای کور[۱]	$2.T_{ADD}+10.T_{MUL}+7.T_{EXP}+2.T_{INV}$	$1696\ T_{MUL}$
طرح امضای کور[۵]	$5.T_{ADD}+29.T_{MUL}+11.T_{EXP}+3.T_{INV}$	$2669\ T_{MUL}$
طرح پیشنهادی	$5.T_{ADD}+12.T_{EC\text{-}MUL}+27.T_{MUL}+4.T_{EC\text{-}ADD}+3T_{INV}$	$375\ T_{MUL}$

جدول ۲. تعریف نمادهای استفاده شده در ارزیابی کارایی

علامت	تعریف نمادها
T_{MUL}	پیچیدگی زمانی برای اجرای یک ضرب پیمانه‌ای
T_{EXP}	پیچیدگی زمانی برای اجرای یک توان رسانی پیمانه‌ای
T_{ADD}	پیچیدگی زمانی برای اجرای یک جمع پیمانه‌ای
T_{EC_MUL}	پیچیدگی زمانی برای عمل ضرب نقطه‌ی روی منحنی بیضوی
T_{EC_ADD}	پیچیدگی زمانی برای عمل جمع نقطه‌ی روی منحنی بیضوی
T_{INV}	پیچیدگی زمانی برای اجرای یک وارون سازی در میدان

جدول ۳. تغییر واحدهای عملیاتی مختلف بر حسب T_{MUL}

پیچیدگی زمانی واحدهای عملیاتی	رابطه‌ی پیچیدگی زمانی بر حسب ضرب پیمانه‌ای
T_{EXP}	$240\ T_{MUL}$
T_{ADD}	قابل چشم پوشی
T_{EC_MUL}	$29\ T_{MUL}$
T_{EC_ADD}	$0.12\ T_{MUL}$
T_{INV}	$0.073\ T_{MUL}$

فهرست منابع

1. J.L. Camenisch, J.-M. Piveteau, and M.A. Stadler. Blind Signatures Based on the Discrete Logarithm Problem. Advances in Cryptology EUROCRYPT '94, Vol. 950, pp. 428-432. Springer-Verlag, 1994.

2. Wu, T., and Wang, J.R. Comment: A new blind signature based on the discrete logarithm problem for untraceability. Applied Mathematics and Computation Vol. 170, No. 21, pp. 999–1005. 2005.

3. Koblitz. N., Menezes. A.j, and Vanstone. S.A. The state of elliptic curve cryptography, Design, Code, Cryptography, Vol. 19, No. 2, pp. 173–193, 2000.

4. C.C. Lee, M.S. Hwang, 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.

5. C.I. Fan, D.J. Guan, C.I. Wang and D.R. Lin. Cryptanalysis of Lee-Hwang-Yang Blind Signature Scheme; Computer Standards & Interfaces, Vol. 31, No. 2, PP. 319-320, 2009.

6. V.S. Miller, Uses of elliptic curves in cryptography. In: Advances in Cryptology, CRYPTO-85, Lecture Notes in Computer Science, Vol. 218, pp. 417–426, 1985.

7. N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation Vol. 48, No. 177 PP. 203–209, 1987.

8. D.Chaum, Blind Signatures for Untraceable Payments. In Advances in Cryptology CRYPTO '82, pp. 199-203, New York: Plenum Press, 1983.

9. L. Harn, Cryptanalysis of the blind signatures based on the discrete logarithm problem; Electronics Letters Vol. 31 .pp. 1136–1137. 1995.

10. P. Horster, M. Michels, H. Petersen, Comment: cryptanalysis of the blind signatures based on the discrete logarithm problem; Electronics Letters Vol.31, No.21, (1995) 1827.

11. D.Chaum. Security without Identication Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, 28(10):10301044, ISSN 0001-0782. 1985.

12. D. Jena, S. Kumar Jena, and B. Majhi. A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in OnLine Digital Cash. In Proceedings of the 10th International Conference on Information Technology (ICIT'07), pp. 19, IEEE Computer Society. 2007.

13. S.A. Vanstone. Elliptic Curve Cryptosystem The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments. Information Security Technical Report, Vol. 2. pp.78-87, 1997.

14. W. Stallings. Cryptography and Network Security: Principles and Practice. Prentice Hall, 2006.

15. Zuowen Tan, Zhuojun Liu, and Chunming Tang. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP. MM Research Preprints, Vol. 21 No., pp.212-217, 2002.

Sciences Vol.176 No.3 pp. 263–284. 2006.

16. Yu-Fang Chung, Kuo-Hsuan Huang, Feipei Lai, and Tzer-Shyong Chen. ID-based Digital Signature Scheme on the Elliptic Curve Cryptosystem. Computer Standards & Interfaces, 29(6):pp. 601-604, 2007.

17. C. Fan, W.K. Chen, and Y.S. Yeh. Randomization enhanced Chaum's blind signature scheme; Computer Communications, vol. 23, pp. 1677–1680, 2000.

18. E. Mohammed, A. E. Emarah, and K. El-Shennawy. A blind signatures scheme based on ElGamal signature; in IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, pp. 51–53, 2000.

19. M. S. Hwang, C. Lee and Y. C. Lai. An untraceable blind signature scheme; IEICE Trans. Fundam Electron Commun. Comput. Sci. (Inst. Electron Inf. Commun. Eng), vol.E86-A, no.7, pp.1902-1906, 2003.

20. S. A. Vanstone, "Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments," Information Security Technical Report, vol. 2, no.2, pp. 78-87, 1997.

21. G.Z. Qadah, R. Taha, Electronic voting systems: requirements, design, and implementation, Computer Standards & Interfaces Vol. 29 No.3 pp. 376–386. 2007.

22. C.I. Fan, Ownership-attached unblinding of blind signatures for untraceable electronic cash, Information