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

معرفی و تحلیل یک طرح جدید امضارمز

مهدی علاقه بند
پژوهشکده پردازش هوشمند علائم
دانشکده برق، کامپیوتر و فناوری اطلاعات
دانشگاه امام حسین (ع)
m.alaghband@gmail.com

مجید سلیمانی پور
کامپیوتر و فناوری اطلاعات
دانشکده برق
دانشگاه امام حسین (ع)
soleimanipour@ihu.ac.ir

محمدرضا عارف
آزمایشگاه تئوری اطلاعات و مخابرات امن
دانشکده برق
دانشگاه صنعتی شریف
aref@sharif.edu

چکیده :

در این مقاله یک طرح امضارمز جدید و امن مبتنی بر خم‌بیضوی پیشنهاد شده است. بواسطه الگوریتم‌های امضارمز توابع امضای دیجیتال و رمزنگاری با هم ترکیب شده و هزینه محاسبات و طول پیام ارسالی از وضعیت امضاء–سپس–رمز کمتر می‌شود. این طرح پیشنهادی علاوه بر داشتن خصوصیات محرمانگی پیام، اعتبار، یکپارچگی، غیر قابل جعل کردن و انکارناپذیری پارامترهای امنیت پیشرو و تأیید همگانی مستقیم را نیز دارا می‌باشد. در این طرح، قاضی بدون نیاز به کلید خصوصی فرستنده بطور مستقیم و تنها در یک مرحله قادر به تأیید امضای فرستنده است. از طرف دیگر در صورتی که کلید خصوصی فرستنده آشکار شود محرمانگی و اعتبار پیام‌های امضارمز شده قبلی همچنان پابرجا است. با توجه به کارآمد بودن این طرح از نظر هزینه محاسبات و داشتن کلیه پارامترهای امنیتی می‌توان از این طرح در سیستم‌هایی نظیر کارت‌های هوشمند و همینطور مخابرات سیار استفاده کرد.

واژه‌های کلیدی: رمزنگاری کلیدعمومی، امضا دیجیتال، امضارمز، خم بیضوی، امنیت پیشرو

۱– مقدمه

امنیت اطلاعات و احرازهویت فرستنده برای سیستم‌های مخابراتی علی الخصوص شبکه‌های گسترده‌ای مانند اینترنت یک موضوع مهم و اساسی است. جهت حفظ محرمانگی پیام و همینطور جلوگیری از جعل آن، باید فرستنده با استفاده از یک الگوریتم امضای دیجیتال و با کلید خصوصی خود پیام را امضا کرده و در مرحله بعد پیام و امضای دیجیتال با استفاده از یک الگوریتم رمزنگاری متقارن، رمز شود. فرستنده، جهت رمزکردن کلید الگوریتم متقارن از یک الگوریتم رمزنگاری کلید عمومی با کلید عمومی گیرنده استفاده می‌کند.

پس از دریافت چنین پیامی ابتدا گیرنده با استفاده از کلید خصوصی خود کلید متقارن را بازیابی کرده و از آن جهت استخراج متن اصلی و امضا استفاده می‌کند. در نهایت گیرنده می‌تواند امضا را نیز تأیید کند. به چنین عملکرد دو طرفه‌ای طرح امضا–سپس–رمز می‌گویند. (شکل ۱)

برای اولین بار آقای Zheng طرحی را پیشنهاد کرد که به واسطه آن دو تابع امضای دیجیتال و رمزنگاری کلید عمومی جهت

دستیابی به احراز هویت و محرمانگی با هم ترکیب شدند[1].

در امضارمز، فرستنده با استفاده از کلید عمومی گیرنده کلید رمزنگاری متقارن را بدست می‌آورد. گیرنده نیز با استفاده از کلید خصوصی خود به همان کلید متقارن دست پیدا می کند.(شکل ۲)

هر سیستم امضارمز شامل دو مرحله امضارمز و بازگشایی امضارمز[1] است که می‌بایست دارای ۳ خصوصیت زیر باشد :

۱. خروجی منحصربفرد[2]: پس از انجام عملیات بازگشایی امضارمز بر روی پیام امضارمز شده همان پیام اولیه بازیابی شود.

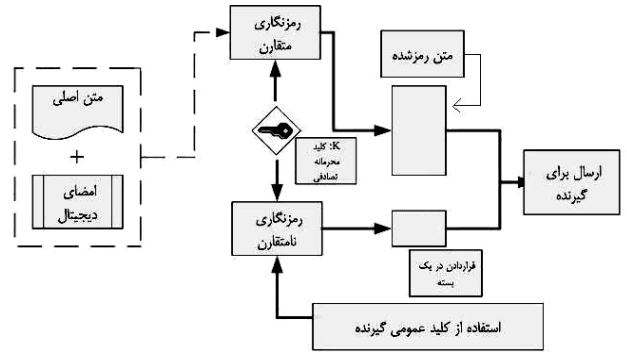
۲. کارآیی[3] : هزینه محاسبات که شامل زمان محاسبات در مراحل امضارمز و بازگشایی امضارمز و همچنین طول پیام ارسالی است کمتر از روش امضاء–سپس–رمز باشد.

۳. امنیت : هر الگوریتم امضارمز باید خصوصیات محرمانگی پیام[4]، انکارناپذیری[5]، یکپارچگی[6] و غیرقابل جعل شدن[7] را داشته باشد.

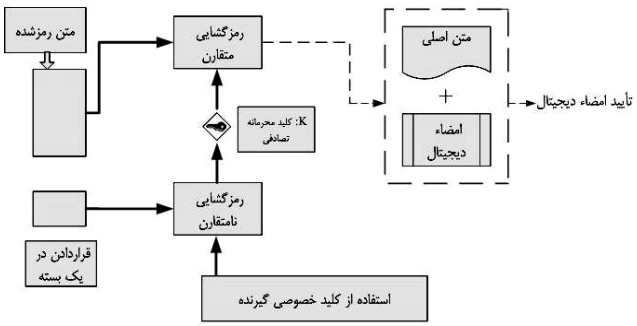
پس از آن Zheng [2]، طرح امضارمز دیگری را مبتنی بر خم بیضوی[8] پیشنهاد کرد که به واسطه آن حدود ۵۸٪ در هزینه محاسبات و ۴۰٪ در طول پیام ارسالی صرفه جویی می‌شود. Jung [3] نشان داد که طرح Zheng [1] وقتی که کلید خصوصی فرستنده لو برود، از خصوصیت امنیت پیشرو[9] پیام پشتیبانی نمی کند. و همچنین آنها یک طرح جدید امضارمز مبتنی بر مسئله لگاریتم گسسته (DLP[10]) با خصوصیت جانبی امنیت پیشرو پیشنهاد دادند. بواسطه خصوصیت امنیت پیشرو اگر کلید خصوصی فرستنده (d_A) آشکار شود، همچنان حمله کننده قادر به بازیابی پیام‌های امضارمز شده قبلی نیست و فاش شدن کلید خصوصی فرستنده اثری بر محرمانگی پیام‌های امضارمز شده قبلی ندارد. با توجه به این تعریف در طرح Jung دشمن حتی با مشاهده کلید خصوصی فرستنده نمی تواند متن اصلی متناظر با آن کلید را مشاهده کند.

در طرح‌های[1_3] به دلیل آنکه در مرحله تأیید امضا به کلید خصوصی گیرنده نیاز داریم، در صورتی که انکاری صورت - پذیرد (گیرنده منکر امضا از طرف خود شود) قاضی به طور مستقیم قادر به تأیید امضا نیست زیرا کلید خصوصی گیرنده را نمی‌داند.

Bao&Deng [4] برای اولین بار طرحی را پیشنهاد دادند که به واسطه آن قاضی (شخص ثالث معتبر) بدون استفاده از کلید خصوصی گیرنده قادر به تأیید امضا می‌باشد. در طرح‌های امضارمز [4,6,7] و حتی در وضعیت امضا–سپس–رمز جهت تأیید امضا توسط هر شخص ثالث در مرحله اول نیازمند همکاری گیرنده در رمزگشایی متن اصلی هستیم.



الف) طرح امضا– سپس – رمز در فرستنده



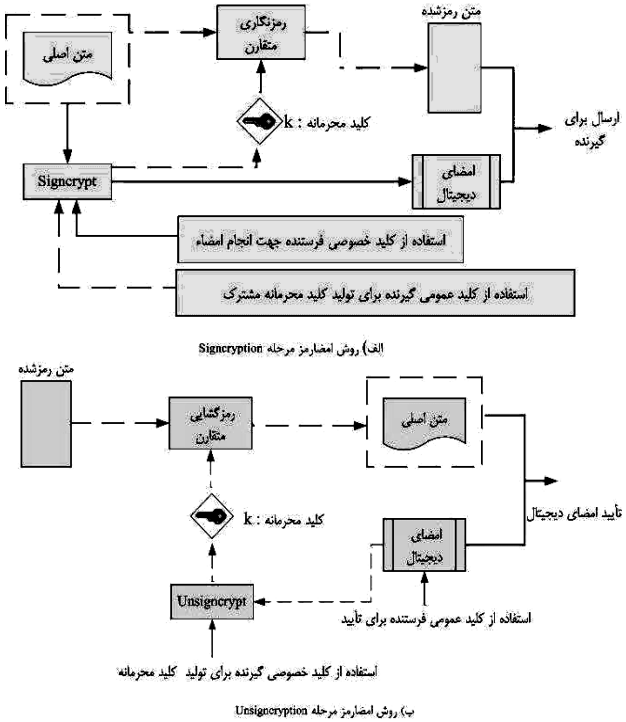
ب)طرح امضا– سپس – رمز در گیرنده

شکل ۱: روش امضا–سپس–رمز[4]

به عبارت دیگر ابتدا گیرنده با استفاده از کلید خصوصی خود متن رمز شده را بازگشایی کرده و سپس متن اصلی و امضای مربوط به آن از جانب فرستنده را جهت بررسی اعتبار در اختیار شخص ثالث قرار می‌دهد. این در حالی است که در چنین

[1] Unsigncryption
[2] Unique Unsigncryption
[3] Efficiency
[4] Confidentiality
[5] Non-repudiation
[6] Integrity
[7] Unforgeability
[8] Elliptic Curve
[9] Forward Secrecy
[10] Discrete Logarithm Problem

وضعیتی گیرنده متن امضارمز شده توانایی هرگونه تغییر و یا جعل بر روی امضای فرستنده را ندارد. در اصطلاح طرح های امضارمز با چنین وضعیتی دارای خصوصیت تأیید همگانی غیرمستقیم[1] هستند.



شکل ۲ : روش امضارمز [7]

Gamage [5] نیز طوری طرح Bao&Deng [4] را بهینه سازی کرده است که هرکس به طور مستقیم می‌تواند امضای متن اصلی را تأیید کند. به عبارت دیگر طرح Gamage دارای خصوصیت تأیید همگانی مستقیم است.

بنابراین تفاوت طرح Bao&Deng وGamage در این است که در طرح Bao&Deng جهت تأیید توسط قاضی ابتدا باید گیرنده متن رمز شده را بازگشایی کرده و سپس قاضی با استفاده از آن و امضای مربوطه درباره اعتبار مین امضارمز تصمیم گیری کند. جهت انجام این کار، نه تنها به مشارکت گیرنده نیاز است بلکه باید از یک پروتکل دو مرحله‌ای نیز استفاده کنیم. ولی در طرح Gamage هر فردی بدون نیاز به مشارکت گیرنده و تنها در یک مرحله امضا را تأیید می کند.

Han,Yang & Hu [6] یک طرح امضارمز دیگر مبتنی بر خم بیضوی مطرح کردند. در این طرح به جای الگوریتم رمز متقارن از یک XOR ساده استفاده شده است. ولی در مقابل هیچکدام از خصوصیات امنیت پیشرو و تأیید همگانی مستقیم را دارا نبوده و در ثانی بدلیل تعدد محاسبه معکوس، بار محاسباتی آن کمی از طرح‌های دیگر بیشتر است.

درطرح[7]، Hwang یک روش امضارمز مبتنی برخم بیضوی پیشنهاد کرده است. این طرح مدعی است که علاوه بر محرمانگی ، اعتبار[2]، یکپارچگی[3] ، انکارناپذیری و غیر قابل جعل کردن ،خصوصیات امنیت پیشرو و تأیید همگانی غیرمستقیم را نیز دارا است. ولی برخلاف این ادعا در صورت داشتن خصوصیت امنیت پیشرو در الگوریتم مذکور محرمانگی از بین می‌رود. از طرف دیگر با توجه به اینکه مشخصات اساسی امنیتی هر طرح امضارمزی محرمانگی پیام، اعتبار، یکپارچگی، غیرقابل جعل کردن و انکارناپذیری[8] است، طرح Hwang با مشکل جدی مواجه می‌شود.

در طرح پیشنهادی، علاوه بر اینکه مشکل طرح Hwang برطرف شده و طرح دارای خصوصیت امنیت پیشرو است، الگوریتم دارای خصوصیت تأییدهمگانی مستقیم نیز می‌باشد. این درحالی است که هیچ گونه بار محاسباتی فوق العاده‌ای به سیستم تحمیل نشده است.

۲- نقطه ضعف طرح Hwang :

در طرح Hwang ادعا شده است که الگوریتم امضارمز مطرح شده دارای خصوصیت امنیت پیشرو است. اما با کمی دقت در این طرح می‌توان دریافت که این خصوصیت با مشکل مواجه است. امنیت پیشرو به این معنی است که اگر کلید خصوصی فرستنده آشکار شود، محرمانگی و اعتبار پیام‌های قبلی امضاء شده همچنان باقی بماند.

بر خلاف ادعای فوق در مواقعی که کلید خصوصی فرستنده به دست گیرنده برسد و یا شخص ثالثی که کلید خصوصی فرستنده را دارد با گیرنده تبانی کند (حمله تبانی) خصوصیت امنیت پیشرو با مشکل مواجه می‌شود. زیرا در صورتیکه کلید خصوصی فرستنده برای افراد یک شبکه آشکار شود، بطور طبیعی گیرنده نیز از کلید خصوصی فرستنده (d_A) مطلع می‌گردد. بنابراین در دو وضعیت فوق کلید خصوصی فرستنده به دست گیرنده می‌رسد. در این طرح و در مرحله امضارمز از رابطه $s = d_A - h.r \bmod n$ جهت تأمین اعتبار فرستنده استفاده می‌شود. با توجه به تعریف

[1] Indirect Public Verification

[2] Authenticity
[3] Integrity

امنیت پیشرو، اگر در طرح Hwang کلید خصوصی فرستنده (d_A) آشکار شود با توجه به رابطه مذکور و این نکته که فقط گیرنده قابلیت محاسبه h را دارد گیرنده می‌تواند $r = h^{-1}.(d_A - s)$ را محاسبه کند. (زیرا $h = H(m\|r_1)$ و r_1 یک عددتصادفی است که توسط فرستنده انتخاب می‌شود) اما تضمینی بر عدم ارسال r برای دشمن از جانب گیرنده وجود ندارد. زیرا در سیستم‌های کلید عمومی هیچ گونه فرضی مبنی بر قابل اطمینان بودن گیرنده موجود نیست. دسترسی دشمن به r نیز موجب از بین رفتن محرمانگی پیام و بازیابی متن اصلی می‌گردد. زیرا دشمن با داشتن r می‌تواند متن اصلی را محاسبه کند. .به عبارت دیگر مدل Hwang در برابر یک نوع حمله تبانی ضعیف است و از اینرو خصوصیت امنیت پیشرو را دارا نمی‌باشد زیرا در این صورت محرمانگی پیام و عملاً اصل رمزنگاری زیر سؤال می‌رود. در قسمت بعد در طرح پیشنهادی خواهیم دید که حتی اگر کلید خصوصی فرستنده به دست گیرنده هم بیفتد، گیرنده قابلیت تبانی را نداشته و خصوصیت امنیت پیشرو همچنان برقرار است.

۳- طرح پیشنهادی :

این طرح پیشنهادی دارای چهار مرحله برقراری[1] ، امضارمز[2]، بازگشایی امضارمز[3] و تأییدامضا[4] است. درمرحله نخستین پارامترهای سیستم منتشر می‌شود. در مرحله امضارمز، فرستنده (A) پیام امضارمز شده را برای گیرنده (B) می‌فرستد. در مرحله بازگشایی امضارمز نیز گیرنده با استخراج کلید متقارن، متن اصلی را بازیابی کرده و امضا را نیز تأیید می‌کند. نهایتاً در مرحله تأیید هر شخص ثالثی بطور مستقیم و بدون نیاز به گیرنده می‌تواند تصمیم بگیرد که آیا پیام مذکور از طرف A ارسال شده است یا نه.

۳-۱- مرحله برقراری :

پارامترهای زیر به عنوان مقادیر مشترک بین فرستنده، گیرنده و دیگر افراد شبکه بصورت عمومی پخش می شود.

q : یک عدد اول بزرگ که $q > 2^{160}$

a,b : دوعدد صحیح کوچکتر از q که در رابطه $4a^3 + 27b^2 \neq 0$ صدق کند.

F : یک خم بیضوی روی میدان متناهی GF(q) با معادله

$$y^2 = x^3 + ax + b \mod q$$

G : نقطه پایه (مولد) خم بیضوی F با مرتبه n

O : نقطه در بینهایت روی F

n : مرتبه نقطه G ($n \times G = O$) – سمبل "×" اشاره به ضرب نقاط خم بیضوی دارد–

H : تابع یکطرفه درهم‌ساز[5] که بصورت $H : \{0,1\}^* \rightarrow Z_n$ تعریف می‌شود.

$E_k(.)/D_k(.)$: الگوریتم رمزنگاری و رمزگشایی متقارن با کلید خصوصی k

فرستنده بطور تصادفی d_A را به عنوان کلید خصوصی خود انتخاب کرده و از روی آن کلیدعمومی $U_A = d_A \times G$ را محاسبه می‌نماید. گیرنده نیز به همین ترتیب از روی d_B ، U_B را محاسبه می کند.

۳-۲-مرحله امضارمز :

فرض کنید A می‌خواهد پیام m را امضارمز کرده و برای B بفرستد.

۱. تأیید کلید عمومی B (U_B) از روی گواهی آن

۲. انتخاب تصادفی r ($r<n$)

۳. محاسبه $R = r \times G = (r_1, r_2)$

۴. محاسبه $K = r \times U_B = (k, l)$

۵. استفاده از الگوریتم رمزنگاری متقارن جهت تولید متن رمزشده $C = E_k(m)$

۶. استفاده از تابع یکطرفه درهم‌ساز جهت تولید $h = H(C\|r_1)$

۷. محاسبه $P = H(h.r) \times G$

۸. محاسبه $s' = d_A - H(h.r) \bmod n$

۹. محاسبه $s = s' + h$

۱۰. ارسال (C,R,s,P) برای B

۳-۳- مرحله بازگشایی امضارمز :

B پس از دریافت (C,R,s,P) جهت دستیابی به متن اصلی و بررسی امضا مراحل زیر را انجام می دهد :

۱. تأیید کلید عمومی A (U_A) از روی گواهی آن

۲. محاسبه $K = d_B \times R = (k, l)$

[1] Initialization
[2] Signcryption
[3] Unsigncryption
[4] Verification
[5] Hash function

۳. استفاده از الگوریتم رمزگشایی متقارن جهت استخراج متن اصلی $m = D_k(C)$

۴. استفاده از تابع یکطرفه درهم‌ساز جهتتولید $h = H(C \| r_1)$

- r1 مؤلفه x نقطه R می باشد-

۵. محاسبه $s' = s - h$

۶. بررسی رابطه $s' \times G + P \stackrel{?}{=} U_A$. در صورتی که این رابطه درست باشد (C,R,s,P) از طرف A ارسال شده است.

۴- بررسی مشخصات امنیتی طرح پیشنهادی :

کلیه مشخصات امنیتی این طرح مبتنی بر دو مسئله سخت لگاریتم گسسته مبتنی بر خم بیضوی[9] (ECDLP[1]) و مسئله دیفی-هلمن مبتنی بر خم بیضوی [10] (ECDHP[2]) است. هر دوی این مسائل از مسئله‌های سخت محسوب می‌شوند. در این قسمت با توجه به سخت بودن مسائل فوق مشخصات امنیتی طرح پیشنهادی فوق بررسی می‌گردد.

۱) محرمانگی :

در این طرح پیشنهادی اگر دشمن بخواهد متن اصلی را پیدا کند، باید کلید متقارن k را بدست بیاورد. محاسبه k نیز منوط به حل مسئله لگاریتم گسسته است. دشمن می‌تواند از یکی از معادلات زیر به k دست پیدا کند.

(1) $K = r \times U_B$, $R = r \times G$

(2) $K = r.d_B \times G$

(3) $K = d_B \times R$

جهت محاسبه معادله (۱)، حمله کننده باید ابتدا r را محاسبه کرده و سپس با استفاده از U_B، K را محاسبه کند. که این کار منوط به حل ECDLP است. اگر دشمن بخواهد K را از روی معادله (۲) بدست بیاورد باید ECDHP را حل کند.زیرا $r \times G$ و $r \times U_B$ را داشته و باید $r.d_B \times U_B$ را حل کند.در معادله (۳) نیز محاسبه کلید خصوصی B مستلزم حل مسئله لگاریتم گسسته است.

۲) اعتبار :

در طرح پیشنهادی هرکسی توانایی بررسی رابطه تأیید امضا $s' \times G + P \stackrel{?}{=} U_A$ را دارد. در صورتی که رابطه مذکور برقرار باشد اعتبار فرستنده نیز برای تأیید کننده محرز می‌گردد.

۳) یکپارچگی :

گیرنده می‌تواند بررسی کند که آیا پیام دریافتی همان پیام اصلی اولیه ایست که فرستنده ارسال کرده یا نه. فرستنده با استفاده از قسمت های۶ و۸ و۹ مرحله امضارمز، s را محاسبه و برای گیرنده ارسال می‌کند. اگر دشمن C را به C' تغییردهد، m نیز به m' تغییر پیدا می‌کند و $h = H(C \| r_1)$ به $h' = H(C' \| r_1)$ تبدیل می‌شود. به همین ترتیب مقدار s' به $s'' = d_A - H(h'.r) \bmod n$ تبدیل می‌شود. اما با توجه به اینکه دشمن r و d_A را ندارد قادر به محاسبه s'' و در نتیجه زیر سؤال بردن یکپارچگی پیام نیست.

۴) غیر قابل جعل کردن :

در این طرح دشمن بدون در اختیار داشتن کلیدخصوصی فرستنده قابلیت هیچ گونه جعل معتبری را ندارد.به عبارت دیگر حمله کننده بدون اطلاع از کلید خصوصی فرستنده قادر به جعل(m,R,s) نیست. زیرا جهت جعل به عدد تصادفی r نیاز دارد.

۵) انکارناپذیری :

در صورتی که فرستنده منکر پیام ارسالی خود شود، قاضی با استفاده از مرحله تأییدامضاء ،می‌تواند به حقیقت پی ببرد. زیرا فقط فرستنده قادر به تولید پارامترهایی است که در رابطه تأیید امضاء صدق کند.

۶) امنیت پیشرو :

امنیت پیشرو به این معنا است که اگر کلید خصوصی فرستنده (d_A) لو برود، همچنان حمله کننده قادر به بازیابی پیام‌های امضارمز شده قبلی نباشد. در این طرح پیشنهادی ، اگر حمله کننده بخواهد m را بدست بیاورد باید به کلید متقارن K دست پیدا کرده و از آن برای رمزگشایی C استفاده کند. که حتی با اطلاع از d_A نیز این کار مقدور نیست. زیرا ناگزیر به محاسبه معکوس دو تابع درهم سازهستیم و هیچ کسی حتی گیرنده قادر به محاسبه $H(hr)$ نیست.

$$K = r \times U_B = [h^{-1}.(H^{-1}.(d_A - s))] \times U_B \quad , \quad h = H(m \| r_1)$$

۶) تأیید همگانی مستقیم[3] :

این طرح نیز مانند طرح Gamage [5] خاصیت تأیید همگانی مستقیم را دارا می باشد. زیرا هرکسی با داشتن (C,R,s,P) و

[1] Elliptic Curve Discrete Logarithm Problem
[2] Elliptic Curve Diffie-Hellman Problem
[3] Direct Public Verification

کلید عمومی فرستنده قادر به بررسی اعتبار امضاء می‌باشد. مزیت دیگر تأیید همگانی مستقیم در این است که در فرآیند تأیید امضا نیز همچنان محرمانگی پیام باقی می‌ماند و نیازی به آشکار شدن متن اصلی حتی برای تأییدکننده نیز نیست. این در حالی است که در وضعیت امضاء–سپس–رمز نیز چنین مزیتی وجود ندارد.

جدول ۱: مقایسه مشخصات امنیتی طرح های امضارمز با طرح پیشنهادی

	محرمانگی	صحت	جعل ناپذیری	انکارناپذیری	امنیت پیشرو	تأیید همگانی مستقیم
Zheng [1]	✓	✓	✓	با پروتکل جانبی	×	×
Zheng [2]	✓	✓	✓	با پروتکل جانبی	×	×
Bao & Deng [4]	✓	✓	✓	بطور مستقیم	×	×
Gamage et al.[5]	✓	✓	✓	بطور مستقیم	×	✓
Jung et al. [3]	✓	✓	✓	با پروتکل جانبی	✓	×
Hwang et al. [7]	✓	✓	✓	بطور مستقیم	×	×
Han & Yang [6]	✓	✓	✓	بطور مستقیم	×	×
طرح پیشنهادی	✓	✓	✓	بطور مستقیم	✓	✓

جدول ۲: مقایسه هزینه محاسبات طرح های امضارمز با طرح پیشنهادی

	ضرب مبتنی بر خم بیضوی	جمع مبتنی بر خم بیضوی	عملیات توان رسانی	محاسبه معکوس در پیمانه	جمع	تابع درهم ساز
Zheng [1]	—	—	۳	۱	۱	۴
Zheng [2]	۳	۱	—	۱	۱	۴
Bao & Deng [4]	—	—	۵	۱	۱	۶
Gamage et al.[5]	—	—	۵	۱	۱	۴
Jung et al. [3]	—	—	۵	۱	۱	۴
Hwang et al. [7]	۵	۱	—	—	۱	۲
Han & Yang [6]	۵	۱	—	۳	۱	۴
طرح پیشنهادی	۵	۱	—	—	۳	۴

۵- مقایسه مشخصات امنیتی و هزینه محاسباتی طرح پیشنهادی با سایر طرح ها :

با توجه به قسمت‌های قبلی و مطالب گفته شده، این طرح تنها طرحی است که کلیه مشخصات امنیتی مذکور را یکجا در برداشته و بار محاسباتی آن همچنان از وضعیت امضاء–سپس–رمز کمتر و مشابه طرح های قبلی است.

با توجه به نقطه ضعف بیان شده بر روی الگوریتم Hwang [7]، طرح پیشنهادی و طرح Jung[3] طرح‌هایی هستند که خاصیت امنیت پیشرو را دارا هستند. از طرف دیگر این طرح پیشنهادی به همراه روش Gamage [5] تنها طرح‌هایی هستند که از خصوصیت تأیید همگانی مستقیم پشتیبانی می‌کنند. از دیگر مزایای طرح پیشنهادی انکارناپذیری مستقیم آن است. در طرحهای [3_1] جهت دستیابی به خاصیت انکارناپذیری نیاز به

یک پروتکل جانبی "اثبات دانایی صفر"[1] داریم. خلاصه موارد فوق در جدول ۱ لیست شده است.

در جدول ۲، مقایسه‌ای میان طرح‌های مختلف از لحاظ هزینه محاسبات انجام گرفته‌است. مزیت محاسباتی طرح پیشنهادی در این است که بر خلاف اکثریت طرح‌های امضارمز نیازی به محاسبه معکوس یک پارامتر در الگوریتم نیست. اهمیت این موضوع از آن جهت است که بعد از عملیات توان رسانی (یا ضرب مبتنی بر خم بیضوی) زمانبرترین عملیات محاسبه معکوس یک عدد در گروه متناظر آن است.

از طرف دیگر در یک سطح امنیتی مشابه محاسبه ضرب دو نقطه درخم بیضوی سریعتر از عملیات توان‌رسانی در میدان-های متناهی است[11]. این موضوع یک مزیت محاسباتی برای کلیه سیستم های مبتنی بر خم بیضوی محسوب می شود.

۶- نتیجه‌گیری :

در این مقاله یک طرح امضارمز جدید مبتنی بر خم بیضوی با خصوصیات امنیت پیشرو و تأیید همگانی مستقیم معرفی گردید. بواسطه امنیت پیشرو در صورتیکه کلید خصوصی فرستنده آشکار شود محرمانگی پیام های از قبل ارسال شده همچنان باقی خواهد ماند. بواسطه تأیید همگانی مستقیم نیز هر فردی بطور مستقیم و بدون از بین رفتن محرمانگی قابلیت تأیید امضاء را دارد. این طرح پیشنهادی کلیه شرایط لازم جهت در اختیار داشتن یک الگوریتم امضارمز قابل اطمینان را بانضمام امنیت پیشرو و تأیید همگانی مستقیم در بردارد. از نظر بار محاسباتی نیز همچنان از روش امضا-سپس-رمز بهتر عمل می‌کند. به عبارت دیگر طرح امضارمز پیشنهادی در مجموع، از نقطه نظر خصوصیات امنیتی و بارمحاسباتی نسبت به طرح های امضارمز دیگر بهتر عمل می‌کند.

۷. مرجع :

[1]- Y. Zheng," Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)", Advances in Cryptology - Crypto'97, Lecture Notes in Computer Science, Vol 1294, pp. 165-179, Springer-Verlag, 1997

[2]- Y. Zheng and H. Imai," How to Construct Efficient Signcryption Schemes on Elliptic Curves",Information Processing Letters, 68(5), pp. 227-233, IEE Press, 1998

[3]- H.Y. Jung, K.S. Chang, D.H. Lee, J.I. Lim "Signcryption schemes with forward secrecy", Proceeding of WISA 2 (2001) 403–475

[4]- F. Bao and R. H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key", Public Key Cryptography (PKC'98), LNCS 1431, pp. 55-59. Springer-Verlag, 1998.

[5]- Chandana Gamage, Jussipekka Leiwo and Yuliang Zheng,"Encrypted Message Authentication by Firewalls", Proceedings of 1999 International Workshop on Practice and Theory in Public Key Cryptography (PKC'99), 1-3 March, 1999, Kamakura, Japan, LNCS, Vol.1560, pp.69-81, Springer-Verlag, 1999

[6]- Yiliang Han, Xiaoyuan Yang and Yupu Hu, "Signcryption Based on Elliptic Curve and Its Multi-Party Schemes", Proceedings of the 3rd international conference on Information security InfoSecu'04, pp.216-217, ACM Press, 2004

[7]- Ren-Junn Hwang, Chih-Hua Lai and Feng-Fu Su, "An Efficient Signcryption Scheme With Forward Secrecy Based on Elliptic Curve", Applied Mathematics and Computation, pp.870-881, V.167, No.2,Elsevier Inc., New Yor, 2005

[8]- J. Baek, R. Steinfeld and Y. Zheng," Formal Proofs for the Security of Signcryption", Public Key Cryptography (PKC 2002), LNCS 2274, pp. 80-98, Springer-Verlag, 2002.

[9]- D. Johnson, A. Menezes, S. Vanstone," The elliptic curve digital signature algorithm (ECDSA)",International Journal of Information Security 1 (1) (2001) 36–63

[10]- Certicom Research, Standards for efficient cryptography,SEC 1:"elliptic curve cryptography", Standards for efficient cryptography group (SECG), September 20, 2000.

[11]- L. Batina, S.B. O¨ rs, B. Preneel, J. Vandewalle, "Hardware architectures for public key cryptography", Integration the VLSI Journal 34 (1–2) (2003) 1–64.

[1] - Zero Knowledge