

معرفی و تحلیل یک طرح جدید امضارمز

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

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

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

چکیده :

در این مقاله یک طرح امضارمز جدید و امن مبتنی بر خم بیضوی 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 کلید عمومی، امضا دیجیتال، امضارمز، خم بیضوی، امنیت پیشرو

۱- مقدمه

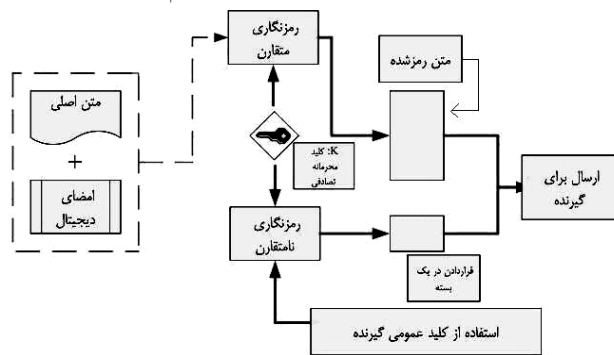
رمز کردن کلید الگوریتم متقارن از یک الگوریتم رمزنگاری کلید عمومی با کلید عمومی گیرنده استفاده می‌کند. پس از دریافت چنین پیامی ابتدا گیرنده با استفاده از کلید خصوصی خود کلید متقارن را بازیابی کرده و از آن جهت استخراج متن اصلی و امضا استفاده می‌کند. در نهایت گیرنده می‌تواند امضا را نیز تأیید کند. به چنین 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

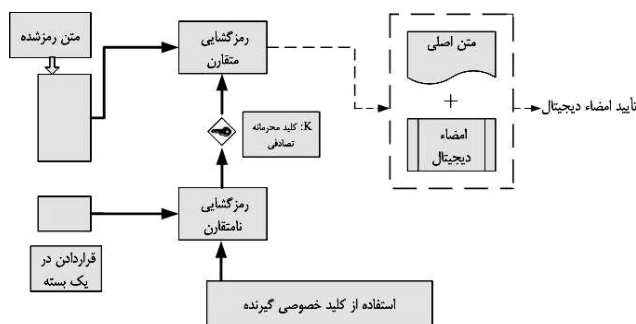
امنیت اطلاعات و احراز هویت فرستنده برای سیستم‌های مخابراتی علی‌الخصوص شبکه‌های گسترده‌ای مانند اینترنت یک موضوع مهم و اساسی است. جهت حفظ محرمانگی پیام و همینطور جلوگیری از جعل آن، باید فرستنده با استفاده از یک الگوریتم امضای دیجیتال و با کلید خصوصی خود پیام را امضا کرده و در مرحله بعد پیام و امضای دیجیتال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

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

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 می‌کند. (شکل ۲)

هر سیستم امضارمز شامل دو مرحله امضارمز و بازگشایی امضارمز^۱ است که می‌بایست دارای ۳ خصوصیت زیر باشد: ۱. خروجی منحصرنبرد^۲: پس از انجام عملیات بازگشایی امضارمز بر روی پیام امضارمز شده همان پیام اولیه بازیابی شود.

۲. کارایی^۳: 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^۴، انکارناپذیری^۵، یکپارچگی^۶ و غیرقابل جعل شدن^۷ را داشته باشد.

پس از آن [2] Zheng طرح امضارمز دیگری را مبتنی بر خم بیضوی^۸ 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 [1] Zheng وقتی که کلید خصوصی فرستنده لو برود، از خصوصیت امنیت پیشرو^۹ پیام پشتیبانی نمی‌کند. و همچنین آنها یک طرح جدید امضارمز مبتنی بر مسئله لگاریتم گسسته (DLP^{۱۰}) 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

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

a, b : دو عدد 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

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

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 درهم ساز^۵ که بصورت $H: \{0,1\}^* \rightarrow Z_n$ تعریف می شود.

$E_k(\cdot)/D_k(\cdot)$: 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 کلید عمومی $U_A = d_A \times G$ را محاسبه می نماید. گیرنده نیز به همین ترتیب از روی d_B ، U_B را محاسبه می کند.

۳-۲- مرحله امضارمز:

فرض کنید A می خواهد 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 رمز شده $C = E_k(m)$

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

۷. محاسبه $P = H(h.r) \times G$

۸. محاسبه $s' = d_A - H(h.r) \pmod n$

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 $K = d_B \times R = (k, l)$

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 می تواند $r = h^{-1} \cdot (d_A - s)$ را محاسبه کند. (زیرا $h = H(m || r_1)$ و r_1 یک عدد تصادفی است که توسط فرستنده انتخاب می شود) اما تضمینی بر عدم ارسال r برای دشمن از جانب گیرنده وجود ندارد. زیرا در سیستم های 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 می گردد. زیرا دشمن با داشتن r می تواند 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 نمی باشد زیرا در این صورت محرمانگی پیام و عملاً اصل رمزنگاری زیر سؤال می رود. 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^۱، امضارمز^۲، بازگشایی امضارمز^۳ و تأیید امضا^۴ است. در مرحله نخستین پارامترهای سیستم منتشر می شود. در مرحله امضارمز، فرستنده (A) پیام امضارمز شده را برای گیرنده (B) می فرستد. در مرحله بازگشایی امضارمز نیز گیرنده با استخراج کلید متقارن، متن اصلی را بازیابی کرده و امضا را نیز تأیید می کند. نهایتاً در مرحله تأیید هر شخص ثالثی بطور مستقیم و بدون نیاز به گیرنده می تواند 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 $q > 2^{160}$

¹ Initialization
² Signcryption
³ Unsigncryption
⁴ Verification

⁵ Hash function

۳. استفاده از الگوریتم رمزگشایی متقارن جهت استخراج متن

$$m = D_k(C) \text{ اصلی}$$

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

r_1 - مؤلفه x نقطه R می باشد -

$$s' = s - h$$

۶. بررسی رابطه $s' \times G + P = U_A$. 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.

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

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

$$(3) \quad K = d_B \times R$$

جهت محاسبه معادله (۱)، حمله کننده باید ابتدا r را محاسبه

کرده و سپس با استفاده از K, U_B 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

$r \times U_B$ و $r \times G$ 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

$s' \times G + P = U_A$ 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 های ۶ و ۸ و ۹ مرحله امضارمز، s را محاسبه و برای

گیرنده ارسال می‌کند. اگر دشمن C را به C' تغییر دهد، 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 کلید خصوصی

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 ساز هستیم و هیچ کسی حتی گیرنده قادر

به محاسبه $H(hr)$ نیست.

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

(۶) تأیید همگانی مستقیم^۳ :

این طرح نیز مانند طرح [5] Gamage خاصیت تأیید همگانی

مستقیم را دارا می‌باشد. زیرا هرکسی با داشتن (C, R, S, P) و

³ Direct Public Verification

¹ Elliptic Curve Discrete Logarithm Problem www.SID.ir

² Elliptic Curve Diffie-Hellman Problem

حالی است که در وضعیت امضاء-سپس-رمز نیز چنین مزیتی وجود ندارد.

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

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 جانی	✗	✗
Zheng [2]	✓	✓	✓	با پروتکل جانی	✗	✗
Bao & Deng [4]	✓	✓	✓	بطور مستقیم	✗	✗
Gamage et al.[5]	✓	✓	✓	بطور مستقیم	✗	✓
Jung et al. [3]	✓	✓	✓	با پروتکل جانی	✓	✗
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

با توجه به نقطه ضعف بیان شده بر روی الگوریتم [7] Hwang، طرح پیشنهادی و طرح Jung[3] طرح‌هایی هستند که خاصیت امنیت پیشرو را دارا هستند. از طرف دیگر این طرح پیشنهادی به همراه روش [5] Gamage تنها طرح‌هایی هستند که از خصوصیت تأیید همگانی مستقیم پشتیبانی می‌کنند. از دیگر مزایای طرح پیشنهادی انکارناپذیری مستقیم آن است. در طرح‌های [1_3] جهت دستیابی به خاصیت انکارناپذیری نیاز به

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.

- [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.

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

در جدول ۲، مقایسه‌ای میان طرح‌های مختلف از لحاظ هزینه محاسبات انجام گرفته است. مزیت محاسباتی طرح پیشنهادی در این است که برخلاف 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 در خم بیضوی سریعتر از عملیات توان‌رسانی در میدان-های متناهی است [11]. این موضوع یک مزیت محاسباتی برای کلیه سیستم‌های مبتنی بر خم بیضوی محسوب می‌شود.

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 پیام‌های 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 بار محاسباتی نسبت به طرح‌های امضارمز دیگر بهتر عمل می‌کند.

۷. مرجع :

- [1]- Y. Zheng, "Digital Signcryption or How to Achieve $\text{Cost}(\text{Signature} \ \& \ \text{Encryption}) \ll \text{Cost}(\text{Signature}) + \text{Cost}(\text{Encryption})$ ", 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

¹ - Zero Knowledge