پروتکل جدید در پرداخت سیار با استفاده از رمز-امضا و خم بیضوی

**آتنا لطفی،** دانشجوی کارشناسی‌ارشد مهندسی فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد

**محمدعلی دوستاری\*،** استادیار دانشکده فنی و مهندسی، دانشگاه شاهد

**چکیده-** با افزایش نفوذ تلفن همراه و توسعه تجارت سیار، استفاده از تلفن همراه به عنوان ابزار پرداخت روز به روز گسترش می­یابد. با توجه به اهمیت امنیت در تجارت و پرداخت و به دلیل ویژگی­های شبکه­های بی­سیم و محدودیت­های موجود در ابزار پرداخت، پروتکل­های پیشنهادی در حوزه پرداخت سیار می­بایستی علاوه بر تامین کارایی از امنیت مناسبی نیز برخوردار باشند. در این مقاله که در راستای اهداف فوق می­باشد، یک پروتکل پرداخت امن و کارا مبتنی بر سناریوی ارتباطی فروشنده محور ارائه می­شود. در پروتکل پیشنهادی با استفاده از طرح کلید عمومی خودگواهی[[1]](#footnote-1) مبتنی بر رمزنگاری خم بیضوی، امضای رقمی شانور[[2]](#footnote-2) و همچنین طرح رمز-امضا، راه حلی جهت رمزنگاری تصدیق اصالت شده ارائه می­گردد. بنابراین بکارگیری راه حل­ پیشنهادی در پروتکل، سبب کاهش بار محاسباتی و پیچیدگی زمانی در مقایسه با دیگر طرح­های رمزنگاری کلید عمومی می­شود. به­علاوه، پروتکل ارائه شده در برابر حملات امنیتی شناخته شده مقاوم می­باشد و همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می­آورد.

**کلید واژه-** **سیستم پرداخت سیار،پروتکل پرداخت، رمزنگاری خم بیضوی، کلید عمومی خودگواهی، امضای رقمی شانور**

**A New M-Payment protocol Using SignCryption & Elliptic Curve Cryptography**

**Atena Lotfi,** Faculty of Engineering, Shahed University

**Mohammad-Ali Doostari[[3]](#footnote-3)\*,** Faculty of Engineering, Shahed University

***Abstract****-* *As a result of increasing penetration of mobile phone and M-commerce development, usage of cell phone as a mean of payment is growing day by day. Considering the importance of security in commerce and payment, due to the characteristics of wireless networks and constraints of cell phones, proposed protocols in payment area require security in addition to efficiency. In this paper, in order to achieve the mentioned goals, a secure and efficient payment protocol based on vendor-centric communication scenario is proposed. In this proposal, we take advantage of self-certified public keys (SCPKs) based on elliptic curve, Schnorr digital signature and sign-encryption scheme in order to provide a solution for an authenticated encryption. Applying the proposed solutions in this protocol leads to reduction in computational load and time complexity* *comparing to other public-key encryption schemes. In addition, the offered protocol is resistant to known security attacks and also provides privacy and fair payment transaction for clients.*

**Keywords-** Mobile Payment System, Payment Protocol, Elliptic Curve Cryptography, Self-Certified Public Key, Schnorr Digital Signature

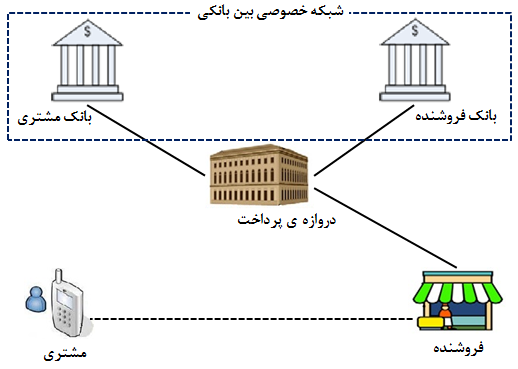
1. **مقدمه**

پرداخت سیار، یک پرداخت الکترونیکی در محیط بی­سیم می­باشد که در آن حداقل یکی از طرف­های شرکت کننده در تراکنش از ابزار پرداخت سیار استفاده می­کند [۱]. با توجه به اهمیت امنیت در تجارت و پرداخت، پروتکل­های پیشنهادی در حوزه پرداخت سیار می­بایستی با دید همه جانبه نسبت به مباحث امنیتی در زمینه­ی شبکه­های سیار و محدودیت­های موجود در ابزار پرداخت طراحی شوند [2]. بنابراین برای غلبه بر مشکلات مرتبط با پرداخت سیار، توجه به دو بحث امنیت و کارایی در طراحی پروتکل­های پرداخت سیار یک ضرورت محسوب می­شود.

تا کنون تلاش­های فراوانی در راستای ارائه­ی پروتکل­های پرداخت متناسب با نیازمندی­های موجود در تجارت سیار صورت گرفته است که در بسیاری از این پروتکل­ها جهت تامین نیازمندی­های امنیتی از سیستم­های رمز کلید عمومی استفاده می­شود. مسئله مهم در این سیستم­ها، نیاز به برقراری ارتباط بین کلید عمومی و هویت شخص - اصالت کلید عمومی- می­باشد. البته برای رفع این مسئله، راه حل­هایی ارائه گردید که یک راه حل، سیستم­های رمز کلید عمومی مبتنی بر گواهینامه می­باشد؛ اما استفاده از این سیستم­ها در حوزه­ی پرداخت سیار به دلیل نیاز به ساختار کلید عمومی، مدیریت و کنترل گواهینامه­ها نامناسب می­باشد. پروتکل­های SET [3]–[5] و iKP [6],[7] نمونه­هایی از پروتکل­های پرداخت ارائه شده مبتنی بر طرح کلید عمومی مبتنی بر گواهینامه می­باشند. جهت رفع مشکلات طرح کلید عمومی مبتنی بر گواهینامه، طرح کلید عمومی مبتنی بر هویت اولین بار توسط شامیر در 1984 [8] بیان گردید. اگرچه این طرح، مشکلات سیستم رمز کلید عمومی مبتنی بر گواهینامه را برطرف می­کند ولی عیب آن وابستگی تمامی کلیدهای خصوصی به کلید اصلی مرکز تولید کلید[[4]](#footnote-4) می­باشد.

سیستم­های رمز کلید عمومی خودگواهی برای مواجهه با مشکلات بیان شده در دو طرح فوق معرفی گردیدند. در سیستم رمز کلید عمومی خودگواهی، گواهینامه به طور ضمنی در خود کلید عمومی قرار می­گیرد که این امر، کاهش هزینه­ی ارتباطی و حافظه مصرفی را در مقایسه با طرح­های مبتنی بر گواهینامه سبب می­شود؛ بنابراین استفاده از سیستم­های رمز کلید عمومی خودگواهی در بحث پرداخت سیار سبب بهبود فرآیند پرداخت می­شود. البته در طراحی پروتکل­های پرداخت سیار استفاده از سیستم رمز متقارن اگر چه سبب کاهش بار محاسباتی تراکش پرداخت می­شود ولی مستلزم به اشتراک گذاری مقادیر محرمانه بین طرفین شرکت کننده در پروتکل می­باشد. در نتیجه استفاده از سیستم­های رمز متقارن در پروتکل پرداخت، محدودیت­هایی را در طراحی پروتکل به وجود می­آورد. از جمله پروتکل­های مهم در حوزه پرداخت سیار مبتنی بر رمزنگاری متقارن، می­توان به پروتکل­های KSL [9],[10] و Tellez [11]–[15] اشاره نمود. بنابراین در طراحی پروتکل پیشنهادی از سیستم رمز کلید عمومی خودگواهی جهت برقراری خواسته­های امنیتی استفاده می­شود.

در شکل1، یک سناریوی ارتباطی برای سیستم پرداخت سیار نشان داده شده است. در این سناریو، مشتری در زمان تراکنش پرداخت قادر به برقراری ارتباط مستقیم با بانک خود نمی­باشد که دلیل آن می­تواند عدم دسترسی مشتری به اینترنت یا هزینه­ی بالای پیاده سازی مکانیسم­های دیگر جهت برقراری این ارتباط باشد. در این سناریو، مشتری با فروشنده فقط از طریق یک کانال بی­سیم بردکوتاه (مانند: بلوتوث، NFC، Infrared یا Wi-Fi) در ارتباط می­باشد که این امر تسهیل فرآیند خرید را برای مشتریان (مانند: عابران و رانندگان) فراهم می­آورد [12],[14].



**شکل1-** **سناریوی پرداخت سیار**

پروتکل پیشنهادی ما در این مقاله، منطبق با این سناریوی ارتباطی است. در این پروتکل، طرحی جدید برای عملیات رمزنگاری کلید عمومی جهت استفاده در تراکنش پرداخت ارائه می­گردد که در این طرح پیشنهادی از سیستم رمز کلید عمومی خودگواهی، رمزنگاری خم بیضوی، طرح­ رمز-امضا، طرح تصدیق هویت و امضای رقمی شانور استفاده می­شود. در این طرح استفاده از سیستم رمز کلید عمومی خودگواهی سبب بهبود فرآیند پرداخت و کاهش هزینه­ی ارتباطی و حافظه مصرفی در مقایسه با طرح­های امضای مبتنی بر گواهینامه می­شود. از طرفی استفاده از خم بیضوی سبب کاهش طول کلید و حافظه مصرفی می­شود. همچنین طرح شانور نیز به دلیل توان محاسباتی پایین یک طرح مناسب جهت استفاده در دستگاه­هایی با منابع محدود می­­باشد. پروتکل پیشنهادی خواسته­های امنیتی محرمانگی، تصدیق اصالت، عدم انکار فرستنده و دست نخوردگی اطلاعات را برآورده می­نماید؛ همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می­آورد. این پروتکل در برابر حملات مردی در میان، تکرار، و ایفای نقش نیز مقاوم می­باشد.

این مقاله از بخش­های مختلفی تشکیل شده است. در بخش 2، مفاهیم و مقدماتی که برای ارائه­ی پروتکل پرداخت مورد نیاز است بیان می­شود. در بخش 3، موجودیت­ها و نمادهای استفاده شده در پروتکل پیشنهادی به همراه جزییات پروتکل توضیح داده می­شود. پروتکل ارائه شده در بخش 4 مورد تحلیل و بررسی قرار می­گیرد و در بخش پایانی نتیجه­ی کار انجام شده بیان می­گردد.

1. **پیش زمینه**

در این بخش، به معرفی طرح هایی که مبنای کار در ارائه­ی راه حل پیشنهادی قرارگرفته پرداخته می­شود.

**1.2 سیستم رمز خم بیضوی**

امنیت در این سیستم رمز، به سختی مسئله لگاریتم گسسته خم بیضوی بستگی دارد که از آن برای تولید زوج کلید عمومی/خصوصی در سیستم­های رمز کلید عمومی استفاده می­شود. از مزایای قابل توجه ECC، استفاده از تعداد بیت­های کمتر نسبت به دیگر روش­های رمزنگاری می­باشد. در واقع ECC، با طول کلید کوتاه­تر، امنیتی مشابه با دیگر سیستم‌های رمزنگاری کلید عمومی را فراهم می‌آورد که این امر سبب اجرای سریع­تر و صرفه جویی بیشتر در پهنای باند می­شود. بنابراین استفاده از سیستم­های رمز خم بیضوی مخصوصا برای برنامه­های دستگاه سیار با منابع محدود بسیار مناسب می­باشند [16]–[18].

**2.2 طرح رمز-امضا**

این طرح اولین بار در سال 1997 توسط زنگ [19] معرفی شد. این روش، نمونه­ای جدید در رمزنگاری کلید عمومی است که در آن عملیات امضا و رمز به طور همزمان و تنها در یک گام منطقی انجام می­گردد؛ یعنی این روش سبب کاهش زمان محاسبات و صرفه جویی در حجم پیام ها نسبت به روش «امضا-سپس-رمز» می­شود [20].

**3.2 طرح تصدیق هویت و امضای رقمی شانور**

طرح­های شانور، از پروتکل­های «صفر-دانش »[[5]](#footnote-5) می­باشند. طرح­های مبتنی بر صفر-دانش جز روش­های قوی برای بررسی صحت ادعای طرف مدعی است. به­علاوه طرح شانور به علت داشتن توان محاسباتی پایین و تعداد گذرهای آن جهت استفاده در دستگاه­هایی با توان محاسباتی پایین و حافظه محدود مناسب می­باشد. طرح تصدیق هویت شانور از سه مرحله تشکیل شده است که به ترتیب عبارتند از: «ادعای طرف مدعی»، «پرسش تصدیق­کننده» و «پاسخ مدعی» که با قرار دادن این سه مرحله در پروتکل پرداخت پیشنهادی می­توان عملیات پرداخت منصفانه­ای را برای مشتری طراحی نمود. همچنین طرح امضای رقمی شانور نیز از سه مرحله تشکیل شده است ولی به صورت غیرتعاملی انجام می­شود یعنی در آن هر سه مرحله را امضا کننده انجام می­دهد و نتیجه مرحله­ی دوم و سوم به عنوان امضای پیام برای تصدیق­کننده ارسال می­شود تا بررسی صحت امضا انجام گیرد [21],[22].

1. **پروتکل پرداخت پیشنهادی**

پروتکل پیشنهادی از پنج موجودیت، مشتری[[6]](#footnote-6)، فروشنده[[7]](#footnote-7)، بانک مشتری[[8]](#footnote-8)، بانک فروشنده[[9]](#footnote-9) و دروازه­ی پرداخت[[10]](#footnote-10) تشکیل شده است. دروازه­ی پرداخت به عنوان یک رابط بین بانک مشتری/فروشنده(شبکه خصوصی بین بانکی) و دو موجودیت دیگر مشتری و فروشنده، جهت انجام تسویه عمل می­کند؛ یعنی توسط این شبکه­ی خصوصی بین بانکی، انتقال واقعی پول انجام می­گیرد و پول توسط بانک مشتری از اعتبار مشتری کسر و به اعتبار فروشنده اضافه می­شود. به علاوه، یک موجودیت مورد اعتماد به نام SA در سیستم پرداخت پیشنهادی وجود دارد و موجودیت­های شرکت کننده در پروتکل به منظور تولید زوج کلید عمومی/خصوصی خود باید در آن ثبت نام نمایند.

**1.3 نمادها**

نمادها و علائم استفاده شده در پروتکل پیشنهادی در جدول 1 نشان داده می­شود.

**جدول1- نمادها**

|  |  |
| --- | --- |
| شرح | نماد |
| بیان کننده­ی نام­­های طرفین شرکت کننده در پروتکل می­باشند که به ترتیب عبارتند از: مشتری، فروشنده، دروازه­ی پرداخت، بانک مشتری و بانک فروشنده. | {C, M, PG, I, A} |
| مشخصه­ی هویتی موجودیت P |  |
| کلید عمومی موجودیت P |  |
| کلید خصوصی موجودیت P |  |
| بیان کننده­ی مقدار «شاهد»[[11]](#footnote-11) برای موجودیت P می­باشد که توسط SA تولید می­گردد و شرح آن در بخش 2.3 آمده است. |  |
| پیام m، رمزشده توسط کلید متقارن K |  |
| امضا توسط موجودیت P با استفاده از طرح امضای ارائه شده در بخش 1.3.3 |  |
| رمز-امضا روی پیام توسط فرستنده برای گیرنده­ی توسط طرح ارائه شده در بخش 2.3.3 |  |
| کلید جلسه بین دو طرف شرکت کننده­ی A و B |  |
| شناسه تراکنش که توسط فروشنده به هر تراکنش تخصیص می یابد. |  |
| تاریخ و زمان سفارش کالا یا خدمات |  |
| یک مقدار دلخواه |  |
| شرح سفارش که شامل اطلاعات: آدرس تحویل برای کالاهای فیزیکی و جزییات سفارش خرید است. |  |
| وضعیت کسر مبلغ از اعتبار مشتری و افزایش اعتبار به حساب فروشنده که توسط بانک مشتری و فروشنده اعلام می­گردد. |  |
| قیمت کل کالا و خدمات |  |
| درخواست مشخصه هویتی فروشنده که این در خواست را مشتری از فروشنده می­نماید. |  |
| تابع درهم سازی یکطرفه روی پیام m |  |
| مانده حساب مشتری که توسط بانک مشتری در به مشتری اعلام می­گردد. |  |
| قرارداد خرید که شامل قیمت و شرح سفارش، شناسه منحصر به فرد قرارداد فی مابین فروشنده و مشتری، شناسه مشتری و فروشنده می­باشد. |  |
| رسید مشتری به فروشنده جهت دریافت سفارش با شرایط ذکر شده در قرارداد |  |
| تبادل اطلاعات لازم برای شروع پروتکل پرداخت بین مشتری و فروشنده |  |
| مجوز پرداخت به بانک جهت کسر از اعتبار مشتری که توسط مشتری برای بانک او صادر می­شود و پاسخ مربوط به این درخواست توسط بانک مشتری برای مشتری برگردانده می­گردد. |  |
| درخواست خرید توسط مشتری برای فروشنده ارسال می­شود و پاسخ مربوط به این درخواست توسط فروشنده به مشتری برگردانده می­شود. |  |
| درخواست افزایش اعتبار فروشنده توسط فروشنده برای PG ارسال می­شود و پاسخ این درخواست توسط PG برای او بازگردانده می­شود. |  |

**2.3 مفروضات پروتکل**

1. موجودیت مورد اعتماد SA، مسئول تولید پارامترهای سیستم می­باشد. SA، کلید عمومی/خصوصی() خود را با استفاده از رمزنگاری خم بیضوی تولید می­کند و پارامترهای عمومی که این مرکز مورد اعتماد منتشر می­کند، شامل: کلید عمومی خود()، خم بیضوی() روی میدان و نقطه­ی پایه() است.
2. هر طرف شرکت کننده ، به صورت دلخواه مقدار را انتخاب و را محاسبه می­کند و سپس را برای SA می­فرستد. بعد از دریافت ، طرفSA، یک عدد دلخواه را انتخاب و را به عنوان شاهد و را به عنوان کلید خصوصی جزئی[[12]](#footnote-12) محاسبه می­نماید. سپس را برای ارسال می­کند و با استفاده از کلید خصوصی جزئی دریافتی، کلید خصوصی خود را به صورت محاسبه می­کند. هر شرکت کننده­ای با دریافت شاهد می­تواند کلید عمومی کاربر را به صورت محاسبه نماید. در پروتکل پیشنهادی، مشتری می­تواند از نام مستعار به جای هویت واقعی خود استفاده کند. در این صورت مشتری به ازای هر نام مستعار، دارای یک زوج کلید عمومی/خصوصی خواهد بود و ارتباط بین هویت واقعی مشتری و نام­های مستعار او فقط برای مشتری و بانک او شناخته شده خواهد بود که بدین شکل گمنامی مشتری حفظ می­گردد [16].
3. قبل از انجام پرداخت، مشتری می­بایست در بانکی حساب باز کند و شاهد مربوط به بانک را دریافت و در دستگاه سیار خود ذخیره نماید. فروشنده نیز، نیاز به ثبت نام در یک دروازه­ی پرداخت دارد و شاهد دروازه­ی پرداخت را بعد از ثبت نام دریافت می­کند.
4. ارتباط بین مشتری و فروشنده از طریق یک شبکه­ی بی­سیم برد کوتاه است و ارتباط بین فروشنده و دروازه­ی پرداخت از طریق اینترنت انجام می­شود.
5. در این پروتکل جهت برقراری کلید محرمانه بین دو طرف A و B، از یک طرح کلید عمومی خود گواهی مبتنی بر ECC استفاده می­شود. در این طرح، طرف A عدد دلخواه را انتخاب و کلید جلسه را محاسبه می­کند و سپس را برای طرف B ارسال می­کند. بعد از دریافت پیام فوق، B کلید جلسه را به صورت محاسبه می­کند [16]. اثبات درستی آن به شکل زیر می­باشد:

= = = = =

**3.3 روش­های ارائه شده جهت استفاده در پروتکل پیشنهادی**

ابتدا روشی جهت امضا رقمی بر اساس طرح امضای رقمی شانور پیشنهاد می­شود که از تلفیق امضای رقمی شانور با کلید عمومی خودگواهی مبتنی بر ECC، این طرح امضا ارائه می­شود. در ادامه طرحی برای امضا و رمز پیام به طور همزمان و در یک گام پیشنهاد شده است. این طرح از تلفیق امضای رقمی شانور، طرح رمز-امضا و رمزنگاری کلید عمومی خودگواهی مبتنی بر ECC حاصل می­شود.

**1.3.3** **جزییات طرح پیشنهادی امضای رقمی شانور مبتنی بر رمزنگاری کلید عمومی خودگواهی و خم بیضوی**

طرف A، می­خواهد پیام m را امضا نماید و برای B ارسال کند و B، تحیق صحت امضا را انجام می­دهد. برای این منظور طرف A، عدد دلخواه را انتخاب و سپس مقادیر ، و را به شکل زیر محاسبه می­کند. طرف ، را به عنوان امضای پیام برای B ارسال می­نماید و B بعد از دریافت امضای دریافتی، بررسی صحت آن را انجام می­دهد.

|  |  |
| --- | --- |
| **generation** | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **verification** | |
|  |  |
|  |  |

**2.3.3 جزییات طرح رمز- امضا مبتنی بر رمزنگاری کلید عمومی خودگواهی، خم بیضوی و طرح امضای رقمی شانور**

طرف A، پیام m را امضا و رمز و برای B ارسال می­کند. B، بعد از دریافت ، تحیق صحت امضا را انجام می­دهد و پیام m را بازیابی می­­نماید.

|  |  |
| --- | --- |
| **generation** | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **verification** | |
|  |  |
|  |  |
|  |  |
|  |  |

**4.3 جزییات پروتکل**

|  |  |  |
| --- | --- | --- |
| Step1) | | |
| Step1.1) |  |  |
|  |  |  |
| Step1.2) |  | = |
|  |  |  |
| step2) |  |  |
|  |  |  |
| step3) |  |  |
|  |  | |
| step4) | " با استفاده از شبکه­ی خصوصی بین بانکی" | |
|  | 1) | |
|  | 2) , | |
|  | 3) | |
|  | 4) | |
|  |  | |
| step5) |  |  |
|  |  |  |
| step6) |  |  |
|  |  | رسید دریافت کالا و خدمات |
| step7) |  |  |

در ادامه شرح گام های پروتکل بیان می­گردد:

**گام 1.** C و M، اطلاعات لازم برای شروع پروتکل پرداخت را مبادله می­کنند. این گام خود شامل دو مرحله می­باشد:

* C، ابتدا پیغامی را که شامل شاهد و شناسه منحصر به فرد خود می­باشد برای M ارسال می­کند و درخواست خرید از M را می­نماید. البته جهت حفظ گمنامی، مشتری می­تواند از نام مستعار به جای هویت واقعی خود استفاده نماید.
* M، بعد از دریافت پیغام از C و انتخاب عدد تصادفی ، کلید جلسه­ای را جهت برقراری ارتباط امن با مشتری تشکیل می­دهد و اطلاعات درخواستی مشتری را توسط این کلید جلسه، رمز و برای C ارسال می­کند. M، مقدار درهم سازی فیلدی به نام که شامل اطلاعاتی از جمله: قیمت، شرح سفارش و شناسه منحصر به فرد قرارداد فی مابین خود و مشتری است را در پیغام ارسالی به C قرار می­دهد.

**گام 2.** مشتری با دریافت پیغام و با استفاده از کلید خصوصی خود و مقدار دریافتی، کلید جلسه را محاسبه می­کند. سپس توسط آن، قسمت اول را رمزگشایی می­نماید. بعد از بررسی آن، اگر قیمت و دیگر موارد مورد قبولش باشد درخواست خرید را برای فروشنده تحت عنوان ارسال می­کند. در پیغام ، مجوز پرداخت مشتری به بانک خود با نام قرار گرفته است که مطابق با روش توضیح داده شده در بخش 2.3.3 توسط مشتری، رمز و امضا می­گردد. در پیغام ، مقدار تصادفی قرار گرفته که بانک مشتری در پاسخ به پیغام ، از آن به عنوان کلید متقارن استفاده خواهد نمود. در این پروتکل در انتهای تراکنش خرید، مشتری باید رسیدی را جهت دریافت موفقیت آمیز کالا یا خدمات به فروشنده تحویل دهد که برای این منظور از طرح تصدیق هویت شانور استفاده می­گردد. این طرح شامل سه مرحله می­باشد که مرحله اول این طرح، ادعای طرف C می­باشد که تحت عنوان و با استفاده از مقدار تصادفی تولید می­شود. یک مقدار تصادفی می­باشد که توضیح آن در گام 5 آمده است.

**گام 3.** M، بعد از رمزگشایی پیغام ، آن را چک می­کند و اگر قیمت و دیگر موارد مورد قبولش باشد درخواست افزایش اعتبار را تحت عنوان برای PG ارسال می­کند. این پیغام توسط M، امضا و برای PG رمز شده است. در این پیغام مقدار تصادفی ، در واقع مرحله دوم از طرح تصدیق هویت شانور می­باشد.

**گام 4.** مراحل موجود در گام 4، تحت شبکه­ی خصوصی بین بانکی انجام می­شود. بنابراین امنیت پیغام­های مبادله شده برای ما مهم نمی­باشد. در اولین مرحله PG، را به همراه برخی اطلاعات دیگر برای بانک مشتری ارسال می­کند. بانک مشتری بعد از بررسی این پیغام و اطمینان از صحت آن، اعتبار مشتری را چک می­نماید و نتیجه را به PG اعلام می­کند. در پایان، PG بعد از دریافت پاسخ از I و A، پیغام را تشکیل می­دهد.

**گام 5.** PG، را برای M ارسال می­کند. M با بررسی مقدار تابع در هم سازی موجود در پیغام می­تواند اطمینان حاصل نماید که PG پیغام را با توجه به پاسخ دریافتی از I تشکیل داده است. چون مقدار عدد تصادفی راطرف I می­داند ولی PG نمی­داند.

**گام 6.** M، سپس مقدار دلخواه e، ، و اطلاعات دیگر را توسط کلید جلسه بین خود و C رمز می­کند و در صورت افزایش اعتبار، مجوز استفاده از کالا و خدمات مورد درخواست مشتری را برای او ارسال می­کند.

**گام7.** C، بعد از دریافت موفقت آمیز کالا و خدمات، رسید را طبق مرحله سوم از طرح تصدیق هویت شانور تولید و برای M ارسال می­کند. M نیز بعد از دریافت رسید، آن را اعتبار سنجی می­نماید که برابری معادله زیر بیانگر دریافت یک رسید معتبر از مشتری می­باشد.

1. **تحلیل و بررسی پروتکل پیشنهادی**

**1.4 خواسته­های امنیتی**

در این زیر بخش پروتکل پرداخت ارائه شده از لحاظ ویژگی­های امنیتی مورد بررسی قرار گرفته و سپس در جدول 2، نتیجه­ی مقایسه پروتکل پیشنهادی با پروتکل­های دیگر از لحاظ خواسته­های امنیتی نشان داده شده است.

* **محرمانگی تراکنش:** در پروتکل پیشنهادی، کانال ارتباطی بین C، M و PG ناامن می­باشد؛ بنابراین می­بایست اطلاعات مهم مبادله شده بین طرفین در طول انتقال برای افراد غیرمجاز آشکار نگردد که برای دستیابی به این امر، می­بایست از رمزنگاری استفاده شود. بدین منظور در پروتکل ارائه شده، ارتباط بین C و M از طریق یک کلید جلسه­ی مشترک به نام ، رمز می­شود و از طرفی اطلاعاتی که C برای I از طریق M ارسال می­کند و نام دارد به وسیله­ی تکنیک توضیح داده شده در بخش 2.3.3 رمز می­گردد و همچنین پیغام مبادله شده بین M و PG نیز با استفاده از همین تکنیک رمز می­شود.
* **گمنامی:** به منظور محفاظت از هویت واقعی مشتری، او می­تواند از نام مستعار() به جای هویت واقعی خودش استفاده نماید؛ یعنی به جای استفاده از ، هر مشتری باید دارای چندین باشد و این ­ها فقط برای خود مشتری و بانک او شناخته شده باشند و فروشنده نتواند ارتباطی بین و هویت واقعی مشتری برقرار نماید. بدین شکل گمنامی مشتری برقرار می­شود.
* در ادامه سه ویژگی تصدیق اصالت موجودیت­ها، دست نخوردگی تراکنش و عدم انکار را در پروتکل پیشنهادی بررسی می­نماییم:
* در پروتکل پیشنهادی، مشتری و فروشنده لازم نیست که یکدیگر را تصدیق اصالت نمایند بلکه این وظیفه­ی PG و I می­باشد که این ادعاها را بررسی نمایند و از طرفی چون اطلاعات مبادله شده بین C و M توسط کلید جلسه رمز می­شود؛ بنابراین هر یک از این طرف­ها، بعد از رمزگشایی پیغام دریافتی از طرف دیگر، می­بایست معنادار بودن فیلدهای پیغام دریافتی را بررسی نماید. در صورت معناداربودن، می­تواند اطمینان داشته باشد که پیغام دریافتی در طول مسیر تغییر نیافته است.
* در پروتکل ارائه شده، اطلاعاتی که C برای I ارسال می­کند با استفاده از روش SignCrypt ارائه شده در بخش 2.3.3 رمز و امضا می­شود؛ بنابراین I می­تواند اطمینان داشته باشد که خود C مجوز درخواست کسر از اعتبار را صادر نموده است و از طرفی چون C نیز آن را امضا کرده است؛ بنابراین نمی­تواند ارسال این درخواست را انکار نماید. بعد از رمزگشایی پیغام دریافتی توسط I، در صورتی که فیلدهای این پیغام معنادار باشد؛ I می­تواند اطمینان داشته باشد که پیغام در طول انتقال تغییر نیافته است؛ بنابراین سه ویژگی فوق برآورده می­شود و همین طور برای پیغام درخواست افزایش اعتباری که M به PG ارسال می­کند نیز این سه ویژگی به دلیل استفاده از طرح بیان شده در بخش 2.3.3 برقرار است.
* در این پروتکل، پیغام پاسخ کاهش اعتبار، که I برای C از طریق M ارسال می­کند توسط کلید متقارن K که در پیغام وجود دارد رمز می­شود. از طرفی، چون پیغام ، فقط قابل رمزگشایی توسط I می­باشد، بنابراین C می­تواند اطمینان داشته باشد که پیغام حتما از طرف I ارسال شده است(تصدیق اصالت) و درصورت معناداربودن فیلدهای پیغام دریافتی، C می­تواند اطمینان داشته باشد که پیغام در مسیر انتقال تغییر نیافته است.
* پاسخ درخواست افزایش اعتبار فروشنده، توسط PG امضا می­شود. بنابراین M می­تواند اطمینان داشته باشد که این پیغام حتما از طرف PG فرستاده شده است و اطلاعات دست نخورده می­باشد واز طرفی، PG هم نمی­تواند ارسال آن را انکار نماید. وجود فیلد در پیغام، تضمین می­نماید که PG در راستای پیغام دریافتی از I، را تولید نموده است. چون مقدار تصادفی ، فقط در اختیار C می­باشد و او این مقدار را برای M در گام دوم ارسال می­کند و همچنین مقدار n در نیز قرار دارد. بنابراین M و I هر دو این مقدار را دارند ولی PG آن را ندارد.
* **ایستادگی در مقابل حمله­ مردی در میان:** یعنی فرد مهاجم خودش را بین دو طرف قانونی قرار دهد و بتواند یکی از این دو یا هر دو را فریب دهد. از آن جایی که پیام­های مهم، به صورت رمزشده­ی تصدیق اصالت شده می­باشند بنابراین دشمن و مهاجم نمی­تواند نقش هیچ کدام از طرف­های قانونی را ایفا کند پس در نتیجه پروتکل­ پیشنهادی در برابر این حمله مقاوم می­باشد.
* **مقاوم بودن در مقابل حمله­ تکرار:** ممکن است مهاجمی بخواهد با استراق سمع پیام­های مبادله شده بین طرفین شرکت کننده در یک تراکنش یک نشست جعلی تشکیل دهد. اما از آن جایی TID به ازای هر تراکنش مقدار منحصر به فردی دارد و همچنین به دلیل استفاده از مقدار دلخواه Nonce، بنابراین مهاجم قادر نخواهد بود اطلاعاتی که در تراکنش­های قبلی جمع آوری کرده است را در تشکیل یک تراکنش جدید به کار ببرد.
* **مقاوم بودن در مقابل حمله ایفای نقش:** ممکن است مهاجمی بخواهد از طرف مشتری، مجوز کسر از اعتبار را صادر نماید؛ ولی به دلیل این که در پروتکل­های پیشنهادی، مجوز کسر از اعتبار، توسط مشتری امضا و رمز می­شود و از طرفی درخواست افزایش اعتبار نیز توسط فروشنده امضا و رمز شده است؛ بنابراین این حمله امکان پذیر نمی­باشد.
* **تراکنش پرداخت منصفانه:** یکی از ویژگی­های مهم در پروتکل­های پرداخت، حفظ منافع شرکت کنندگان در پروتکل می­باشد. در پروتکل پیشنهادی، در طول اجرای تراکنش پرداخت مشتری قبل از دریافت کالا یا خدمات درخواستی، پول را پرداخت می­کند. بنابراین در این پروتکل ریسکی برای فروشنده وجود ندارد اما مشتری ممکن است کالا یا خدمات را دریافت نکند. برای منصفانه کردن عملیات پرداخت، از طرح تصدیق هویت شانور استفاده ­گردید.

**جدول2- مقایسه پروتکل­ها از لحاظ خواسته­های امنیتی**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| پروتکل  ویژگی | SET | 3KP |  |  |  |  |  |
| محرمانگی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| عدم انکار تراکنش | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| گمنامی مشتری | 🗶 | 🗶 | 🗶 | 🗶 | ✓ | ✓ | ✓ |
| مبادله منصفانه | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | ✓ |
| تصدیق اصالت موجودیت ها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| جامعیت و دست نخوردگی اطلاعات | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| مقاوم در برابر حمله تکرار | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| مقاوم در برابر حمله مردی در میان | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| مقاوم در برابر حمله ایفای نقش | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| عدم ثبت نام در فروشنده قبل از پرداخت | ✓ | ✓ | 🗶 | 🗶 | 🗶 | ✓ | ✓ |
| عدم ارسال گواهینامه و بررسی اعتبار آن | 🗶 | 🗶 | 🗶 | ✓ | ✓ | ✓ | ✓ |

**1.4 کارایی**

مقایسه پروتکل پیشنهادی با پروتکل­های دیگر از نظر تعداد عملیات مورد نیاز برای انجام تراکنش پرداخت در جدول 3 نشان داده شده است.

**جدول3- مقایسه پروتکل­ها از لحاظ تعداد عملیات مورد نیاز**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| پروتکل  عملیات | | SET | 3KP |  |  |  |  |  |
| رمزنگاری کلید عمومی | C | 1 | 1 | - | - | - | 2 | 1 |
| M | 1 | 1 | 1 | - | - | 3 | 1 |
| PG | 1 | - | 1 | - | - | 1 | - |
| رمزگشایی کلید عمومی | C | - | - | - | - | - | 2 | - |
| M | 1 | - | 1 | - | - | 2 | - |
| PG | 2 | 2 | 1 | - | - | 1 | 1 |
| تولید امضا | C | 1 | 1 | - | - | - | 2 | 1 |
| M | 3 | 1 | 1 | - | - | 3 | 1 |
| PG | 1 | 1 | 1 | - | - | 1 | 1 |
| بررسی صحت امضا | C | 2 | 2 | - | - | - | 2 | - |
| M | 2 | 2 | 1 | - | - | 2 | 1 |
| PG | 2 | 2 | 1 | - | - | 1 | 1 |
| رمزنگاری/رمزگشایی کلید متقارن | C | 2 | - | 4 | 4 | 5 | - | 4 |
| M | 1 | - | 3 | 5 | 6 | - | 3 |
| PG | 2 | - | - | 2 | 2 | - | - |
| توابع درهم سازی | C | 3 | 2 | 3 | 3 | 2 | 1 | 2 |
| M | 3 | 4 | 3 | 3 | 4 | 2 | 3 |
| PG | 2 | 1 | - | 1 | 1 | 1 | 2 |
| توابع درهم سازی کلید دار | C | - | - | 2 | 2 | 2 | - | - |
| M | - | 1 | 1 | 2 | 2 | - | - |
| PG | - | - | - | 1 | 1 | - | - |

(مبتنی بر رمزنگاری نامتقارن[2] ,[9] ,[10]) (مبتنی بر رمزنگاری متقارن[2] ,[9] ,[10])

(مبتنی بر رمزنگاری متقارن-فروشنده محور[11]) (مبتنی بر رمزنگاری نامتقارن-فروشنده[12]- [15])

(پروتکل پیشنهادی)

در ادامه پروتکل­ها را از نظر میزان بار محاسباتی و پیچیدگی زمانی مورد مقایسه قرار می­دهیم. برای این منظور برای هر یک از عملیات استفاده شده توسط موجودیت­های شرکت کننده در پروتکل یک زمانی تخصیص داده می­شود که نمادهای استفاده شده برای این امر به شکل فوق می­باشد[14],[16]:

: زمان برای ضرب بدون پیمانه N

: زمان برای ضرب با پیمانه N

: زمان برای تابع درهم سازی

: زمان برای تابع درهم سازی کلید­دار

: زمان برای توان رسانی پیمانه ای

: زمان برای ضرب خم بیضوی

: زمان برای انجام عملیات رمزنگاری و رمزگشایی متقارن

* از زمان جمع و تفریق صرف نظر می­شود؛ چون زمان آن در مقایسه با دیگر زمان­ها نسبتا کم می­باشد. بنابراین در تحلیل پیچیدگی زمانی از آن­ها صرف نظر می­گردد[14].
* رمزنگاری/رمزگشایی متقارن تقریبا صد برابر سریع­تر از رمزنگاری/رمزگشایی نامتقارن است[16].
* زمان مورد نیاز برای انجام عمل ضرب خم بیضوی کندتر از عمل ضرب و سریع تر از عمل توان رسانی می­باشد[16].

با توجه به نکات بیان شده در بالا، پیچیدگی زمانی پروتکل­ها مورد بررسی قرار می­گیرد. برای این منظور ابتدا زمان مورد نیاز برای انجام عملیات رمزنگاری، رمزگشایی، امضا و بررسی صحت امضا در پروتکل و پروتکل پیشنهادی در جدول 4 نشان داده می شود و سپس بر اساس آن کار تحلیل و مقایسه پروتکل ها انجام می­گیرد.

**جدول4- زمان انجام عملیات**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| زمان عملیات  پروتکل | رمز و امضا  () | رمزگشایی و بررسی صحت امضا () | تولید امضا  () | بررسی صحت امضا  () |
|  | 3+3+2+ 3 | 5++5+11 | \_ | \_ |
|  | 2+1+2 | 2+ 3 | 1++ | 1+2 |

**جدول5- مقایسه پروتکل­ها از لحاظ پیچیدگی زمانی**

|  |  |  |
| --- | --- | --- |
| *نام پروتکل* | *موجودیت شرکت کننده* | *زمان مورد نیاز* |
|  | C | 2 + 2 + 5 |
| M | 4 + 2 + 6 |
| PG | 1 + 1 + 2 |
|  | C | 3 + 2 + 4 |
| M | 3 + 2 + 5 |
| PG | 1 + 1 + 2 |
|  | C | 2 + 2 + 1 |
| M | 3 + 2 + 2 |
| PG | 1 + 1 + 1 |
|  | C | 1 + 4 + 2 |
| M | 1 + 1 + 3 + 3 |
| PG | 1 + 1 + 1 + 2 |

نتیجه­ای که از جدول 5 حاصل می­شود به صورت زیر می­باشد:

* از نظر پیچیدگی زمانی در سمت مشتری:
* از نظر پیچیدگی زمانی در سمت فروشنده:
* از نظر پیچیدگی زمانی در سمت دروازه­ی پرداخت:

دو پروتکل *و* مبتنی بر رمزنگاری متقارن می­باشند. که اگر چه سبب کاهش بار محاسباتی تراکش پرداخت می­شوند ولی نیاز به اشتراک گذاری مقادیر محرمانه بین طرفین شرکت کننده در پروتکل می­باشد.

1. **نتیجه گیری**

هدف در این مقاله، طراحی پروتکلی متناسب با نیازمندی­های حوزه­ی پرداخت سیار می­باشد. پروتکل ارائه شده در این مقاله، مبتنی بر سناریوی ارتباطی فروشنده محور می­باشد. در این پروتکل، طرحی جدید برای عملیات رمزنگاری کلید عمومی جهت استفاده در تراکنش پرداخت ارائه شد که در طرح پیشنهادی از سیستم رمز کلید عمومی خودگواهی، رمزنگاری خم بیضوی، طرح­ رمز-امضا، طرح تصدیق هویت و امضای رقمی شانور استفاده گردیده است.

پروتکل ارائه شده ویژگی­های محرمانگی، تصدیق اصالت، عدم انکار فرستنده و دست نخوردگی اطلاعات را برآورده می­نماید؛ همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می­آورد. به علاوه، این پروتکل در برابر حملات مردی در میان، تکرار، و ایفای نقش نیز مقاوم می­باشد. پروتکل پیشنهادی از لحاظ خواسته­های امنیتی نسبت به سایر پروتکل­های اشاره شده بهتر می­باشد ولی از نظر بار محاسباتی و پیچیدگی زمانی تراکنش پرداخت نسبت به پروتکل­های متقارن ضعیف­تر و نسبت به پروتکل­های نامتقارن قوی­تر می­باشد.

**مراجع**

1. M.V. alizadeh, R.A. Moghaddam, S. Momenebellah, “New mobile payment protocol: Mobile Pay Center Protocol (MPCP),” 3rd International Conference [Electronics Computer Technology (ICECT),](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5934630)  2011, pp.74–78.
2. S. Kungpisdan, “Modelling, Design, and Analysis of Secure Mobile Payment Systems,” Ph.D. Dissertation, Faculty of Information Technology, Monash University, 2005.
3. S.M. Shedid, M. El-Hennawy, M. Kouta, “Modified SET Protocol for Mobile Payment: An Empirical Analysis,” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010, pp. 289–295.
4. Xun-yi Ren, Li-li Wei, Jun-feng Zhang, X. Ma, “The Improvement of SET Protocol based on Security Mobile Payment,” Journal of Convergence Information Technology, Volume6, Number 7, July 2011, pp. 22–28.
5. S. Kungpisdan, B. Srinivasan, P.D. Le, “A PRACTICAL FRAMEWORK FOR MOBILE SET PAYMENT,” IADIS International Conference e-Society ,2003, pp. 321–328.
6. M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen, M. Waidner, “Design, Implementation, and Deployment of the iKP Secure Electronic Payment System,” IEEE Journal on selected areas in communications, vol. 18, NO. 4, 2000, pp. 611–626.
7. K. Ogata, K. Futatsugi, “Flaw and modification of the iKP electronic payment protocols,” Information Processing Letters 86 (2003) [Online], [www.elsevier.com/locate/ipl](http://www.elsevier.com/locate/ipl), pp. 57– 62.
8. A. Shamir, “Identity-Based Cryptosystem and Signature Scheme,” in Proceedings of CRYPTO, 1984, pp. 47 –53.
9. B.T.S. Toh, S. Kungpisdan, P.D. Le, “KSL Protocol: Design and Implementation,” Proc. IEEE, Conference on Cybernetics and Intelligent Systems, 2004, pp. 544–549.
10. S. Kungpisdan, B. Srinivasan, P.D. Le, “Accountability Logic for Mobile Payment Protocols,” Proc*.* IEEE, the International Conference on Information Technology: Coding and Computing (ITCC’04) , pp. 40–44.
11. J.T. Isaac, J.M. Sierra, A. Izquierdo, M. Carbonell, “A secure for a payment system based on a Kiosk centric case mobile scenario,” Ingenieria UC, Universidad de Carabobo, VeneZuela, 2006, pp. 25–36.
12. J.T. Isaac, J.S. Camara, A.I. Manzanares, J.T. Marquez, “Anonymous Payment in a Kiosk Centric Model using Digital signature scheme with message recovery and Low Computational Power Devices,” Journal of Theoretical and Applied Electronic Commerce Research, 2006, pp. 1–11.
13. J.T. Isaac, J.S. Camara, “A Secure Payment Protocol for Restricted Connectivity Scenarios in M-Commerce,” Proc. 8th International Conference on E-Commerce and Web Technologies, (EC-Web’07), 2007, pp. 1–10.
14. J.T. Isaac, J.S. Camara, S. Zeadally, J.T. Marquez, “A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks,” Computer Communications ,2008, pp. 2478–2484.
15. M.V. Astudillo, J.T. Isaac, D.S. Touceda, H.P. López, “Evaluation of a Client Centric Payment Protocol Using Digital Signature Scheme with Message Recovery Using Self-Certified Public Key,” ICCSA 2009, Part II, LNCS 5593, Springer-Verlag Berlin Heidelberg, pp. 155–163.
16. W. Li, Q. Wen, Q. Su, Z. Jin, “An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network,” Computer Communications , vol 35 , 2012, pp. 188–195.
17. A. Menezes, M. Qu, S. Vanstone, “Elliptic Curve Systems,” IEEE P1363 Part4 Standard, 1995.
18. A. Babel, “Elliptic Curve Cryptography,” F090740, Universiteit Utrecht, INFOB3CRP – Cryptography.
19. Y. Zheng, “Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost (En-cryption),” CRYPTO '97 Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, 2011, pp. 165–179.
20. L. Savu, “Combining Public Key Encryption with Schnorr Digital Signature,” Journal of Software Engineering and Applications,” 2012, pp.102–108.
21. A.J. Menezes, P.C.V. Oorschot, S.A. Vanstone, “Handbook of Applied Cryptography,” CRC-Press , 1996.
22. J. Pieprzyk, T. Hardjono, J. Seberry, “Fundamentals of Computer Security”, Springer, 2003.

1. Self-Certified [↑](#footnote-ref-1)
2. Schnorr [↑](#footnote-ref-2)
3. doostari@shahed.ac.ir [↑](#footnote-ref-3)
4. Key Generation Center(KGC) [↑](#footnote-ref-4)
5. Zero-Knowledge [↑](#footnote-ref-5)
6. client [↑](#footnote-ref-6)
7. merchant [↑](#footnote-ref-7)
8. issuer [↑](#footnote-ref-8)
9. acquirer [↑](#footnote-ref-9)
10. payment gateway [↑](#footnote-ref-10)
11. witness [↑](#footnote-ref-11)
12. partial [↑](#footnote-ref-12)