هفتمین کنفرانس بین المللی انجمن رمز ایران

24 و 25 شهریورماه 1389، دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

دانشگاه صنعتی خواجه نصیرالدین طوسی

بهبود عملکرد پروتکل پرداخت Payword

سمانه لایقیان جوان[1]، عباس قائمی بافقی[2] و یعقوب فرجامی[3]

دانشجوی کارشناسی ارشد IT دانشگاه قم [1]

samaneh.layeghian@gmail.com

استادیار دانشگاه فردوسی مشهد [2]

ghaemib@um.ac.ir

استادیار دانشگاه قم [3]

farjami@gmail.com

چکیده

پروتکل payword یک پروتکل پرداخت خُرد می‌باشد که توسط Ron Rivest ارائه شده و به منظور کاهش عملیات کلید عمومی، از زنجیره هایی از توابع درهم سازی برای خرید از فروشندگان استفاده می کند. هر زنجیره به عنوان مجموعه ای از سکه های الکترونیکی در نظر گرفته می شود. این پروتکل دارای برخی ضعفهای امنیتی و کاربردی از قبیل عدم امکان بکارگیری یک زنجیره از سکه ها جهت خرید از فروشندگان مختلف، عدم گمنامی مشتری نسبت به فروشنده و بانک، امکان رهگیری خریدهای مشتری و قابلیت انکار تراکنش توسط مشتری یا فروشنده می باشد. پیشنهادات مختلفی برای بهبود payword مطرح شده که هریک قسمتی از مشکلات موجود را رفع می کنند. در پروتکل پیشنهادی در این مقاله ضمن حفظ کارایی، تمام مشکلات فوق به جز مساله گمنامی مشتری نسبت به بانک حل شده است.

واژگان کلیدی

پرداخت الکترونیکی، payword، کارایی، گمنامی، رهگیری، زنجیره درهم سازی.

1- مقدمه

امروزه با رشد وتوسعه تجارت الکترونیکی، مساله پرداخت‌های الکترونیکی از اهمیت ویژه‌ای برخوردار شده است. سیستم‌های پرداخت الکترونیکی مختلفی تا کنون ارائه شده‌اند. به طور کلی از لحاظ حجم پرداخت این سیستم‌ها به دو دسته پرداخت‌های کلان و پرداخت‌های خرد تقسیم می‌شوند [1]. در پرداخت‌های کلان به دلیل حجم بالای مبادلات مالی، نیاز به تامین ویژگیهای امنیتی در حد بالا می‌باشد، به عنوان مثال ویژگی‌های محرمانگی پیامها، احراز هویت نقش‌های درگیر، جامعیت داده‌ها، حفظ حریم خصوصی مشتری، انکارناپذیری تراکنش توسط طرفین و گمنامی مشتری حتی المقدور باید تامین شود. به این منظور معمولا از محاسبات رمزنگاری سنگین و امن از قبیل رمزنگاری کلید نامتقارن و امضای دیجیتال استفاده می‌شود[2,3,4]. بانک‌ها نیز باید به صورت online در تراکنش‌ها دخیل باشند. این سربار بالای محاسباتی و ارتباطی باعث افزایش هزینه پرداخت‌ها می‌شود. سیستم‌های پرداخت خرد برای خرید کالاهای با ارزش پایین، از قبیل یک صفحه وب، مقاله، روزنامه و ... مورد استفاده قرار می‌گیرد. بنابراین سربار محاسباتی و ارتباطی و فضای ذخیره‌سازی آن باید پایین و متناسب با یک پرداخت خرد باشد، بنابراین در طراحی این سیستم‌ها سعی می‌شود از عملیات رمزنگاری سنگین از قبیل رمزنگاری نامتقارن و امضای دیجیتال کمتر استفاده شود و غالباً

توابع درهم سازی و عملیات رمزنگاری متقارن بکار می‌رود [5,6,7,8,9]. بنابراین این سیستم‌ها نسبت به پرداختهای کلان از سطح امنیتی پایین‌تری برخوردارند. با این حال طراحی آنها باید به گونه‌ای باشد که هزینه تقلب و دزدی در آنها، به نسبت مبلغی که فرد متقلب به دست خواهد آورد، مقرون به صرفه نباشد. به طور کلی نیازمندی‌های اصلی یک سیستم پرداخت خرد عبارتند از: حذف یا حداقل کردن محاسبات کلید عمومی، حذف نیاز به online بودن بانک‌ها، کاهش تبادل پیام‌ها، کاهش فضای ذخیره‌سازی ، جلوگیری از جعل سکه، جلوگیری از دو بار خرج کردن سکه یا تشخیص آن و ... .

تاکنون الگوهای پرداخت خرد متفاوتی ارائه شده است. دسته ای از این الگوها مبتنی بر استفاده از زنجیره‌ای از توابع درهم سازی می‌باشند. پروتکل اولیه برای استفاده از توابع درهم سازی، payword می‌باشد که یک پروتکل پرداخت خردِ offline و مبتنی بر اعتبار می‌باشد. مشتری برای خرید از هر فروشنده زنجیره‌ای از توابع درهم‌سازی را تولید و قراردادی امضا می‌کند. هر عضو از یک زنجیره به عنوان یک سکه در پرداخت استفاده می‌شود. payword دارای مشکلاتی است، از جمله اینکه مشتری برای هر فروشنده زنجیره جداگانه‌ای تولید می‌کند، احتمال خرج کردن بیش از اعتبارِ موجود در حساب مشتری وجود دارد، مشتری گمنام نیست و خریدهای وی قابل رهگیری می‌باشد، ویژگی عدم انکارپذیری نیز تامین نیست. برای رفع مشکلات payword پیشنهادات مختلفی مطرح شده که در ادامه مورد بررسی قرار خواهد گرفت [10,11,12,13]. هر یک از این پیشنهادات تعدادی از مشکلات موجود را برطرف نموده است.

پروتکل پیشنهادی در راستای گردآوری ویژگیهای امنیتی و کاربردی مورد نیاز به صورت یکجا مطرح شده است. در این پروتکل از یک زنجیره برای خرید از فروشندگان مختلف استفاده می‌شود. از آنجا که زنجیره پیش پرداخت می‌شود امکان خرج کردن بیش از اعتبار مشتری وجود ندارد. یک کلید مشترک مخفی بین مشتری و بانک، جهت حفظ جامعیت پیامهای مشتری و احراز هویت وی به بانک استفاده می‌شود. وجود شناسه مستعار برای مشتری، گمنامی وی نسبت به فروشنده را حفظ می‌کند. مشتری از باقیمانده امضا شده زنجیره توسط فروشنده به عنوان رسید پرداخت استفاده می‌کند، جهت کاهش سربار مشتری نیز یک زنجیره از توابع درهم‌سازی به عنوان رسید دریافت کالا به کار می‌رود و مشتری و فروشنده هیچیک قادر به انکار تراکنش نخواهند بود. در انتهای مقاله نشان داده می‌شود که پروتکل پیشنهادی نسبت به دیگر پروتکل‌های مبتنی بر توابع درهم‌سازی، ویژگی‌های بیشتری را تامین می‌کند، بدون اینکه از کارایی کمتری برخوردار باشد.

در ادامه این مقاله در بخش ۲ پروتکل پرداخت payword و تعدادی از پروتکل‌هایی که با توسعه payword ایجاد شده اند، مورد بررسی قرار گرفته‌اند. در بخش ۳ پروتکل پیشنهادی شرح داده شده است. در بخش ۴ پروتکل پیشنهادی از لحاظ معیارهای مختلف امنیتی و کاربردی مورد بررسی و مقایسه با برخی پروتکل‌های دیگر قرار گرفته است. بخش ۵ به تحلیل کارایی پروتکل پیشنهادی اختصاص یافته و نهایتا در بخش ۶ نتیجه حاصل از مقاله به اختصار بیان شده است.

۲- پروتکل‌های مبتنی بر توابع درهم سازی

پروتکل پایه برای استفاده از توابع درهم‌سازی، payword می‌باشد [3]. هدف این پروتکل که توسط Rivest ارائه شده، کاهش عملیات کلید عمومی با استفاده از زنجیره‌ای از توابع درهم‌سازی می‌باشد. در این پروتکل مشتری ابتدا گواهینامه امضا شده‌ای از بانک دریافت می‌کند که اطلاعات وی در آن قرار دارد. این گواهینامه به مشتری اجازه تولید زنجیره را می‌دهد و فروشنده را مطمئن می‌سازد که زنجیره دریافت شده، توسط بانک به وی پرداخت خواهد شد. مشتری برای خرید از یک فروشنده، طول زنجیره (n) و عدد تصادفی W_n را انتخاب نموده، سپس n بار تابع درهم سازی را بر روی آن اعمال می‌نماید، به طوریکه :

$$W_{n-1} = h(W_n), \ldots, W_{i-1} = h(W_i) \quad \{ i= 1, 2, \ldots, n\}$$

هر W_i بیانگر یک سکه با یک ارزش مالی خاص (به عنوان مثال ۱ سِنت) می باشد. مشتری آخرین مقدار (W_0) را در یک قرار داد الکترونیکی امضا نموده، به همراه گواهینامه خود برای فروشنده ارسال می‌کند که مشتری را متعهد به پرداخت سکه‌ها می‌نماید. مشتری برای پرداخت m سکه به فروشنده، مقادیر W_1 تا W_m را برای وی ارسال می‌کند. فروشنده برای تایید اعتبار سکه‌ها m بار تابع درهم‌سازی را روی W_m اعمال می‌کند تا W_0 را به دست آورد. از آنجا که توابع درهم‌سازی یکطرفه‌اند، کسی به جز مشتری قادر به تولید W_m با استفاده از W_0 نیست. در پایان روز فروشنده آخرین W_i دریافت شده را به همراه قرارداد امضا شده مشتری برای بانک ارسال می‌کند. بانک اعتبار سکه‌ها و امضا را بررسی نموده سپس مبلغ به اندازه i سکه را از حساب مشتری برداشت کرده و به حساب فروشنده می‌افزاید.

در پروتکل Payword مشکلاتی به چشم می‌خورد، از جمله:

- مشتری مجبور است برای خرید از هر فروشنده زنجیره جدیدی تولید و نگهداری نموده و به تعداد فروشندگان قرارداد الکترونیکی امضا نماید.
- مشتری در قبال سکه هایی که به فروشنده پرداخت

می‌کند رسیدی دریافت نمی نماید، بنابراین احتمال سوء استفاده فروشنده وجود دارد.

- فروشنده در قبال کالایی که به مشتری تحویل می دهد رسیدی دریافت نمی‌کند، بنابراین مشتری می تواند ادعا کند که کالا را دریافت ننموده است.

- مشتری گواهینامه خود را برای فروشندگان ارسال می‌کند، بنابراین گمنامی وی دراین سیستم حفظ نمی‌شود.

- از آنجا که مشتری شناسه واقعی خود را برای پرداخت بکار می‌برد، خریدهای مختلف وی توسط فروشنده قابل رهگیری است که این باعث نقض حریم خصوصی مشتری می‌شود.

- از آنجا که Payword یک سیستم offline و مبتنی بر اعتبار می‌باشد، بنابراین احتمال خرج کردن سکه‌ها بدون وجود اعتبار کافی در حساب مشتری وجود دارد. این مساله تا پایان روز که فروشنده سکه‌ها را به بانک ارائه کند قابل تشخیص نیست.

جهت رفع برخی از مشکلات مذکور پیشنهادات مختلفی ارائه شده است. به عنوان مثال جهت حل اختلاف بین طرفین و انکارناپذیری تراکنش، طرح‌های پیشنهادی غالبا از رسیدهای امضا شده به صورت دیجیتالی استفاده می‌کنند که باعث افزایش سربار محاسباتی برای انجام یک پرداخت خرد می‌شود [10].

Hwang در [11] پروتکلی پیشنهاد کرده که یک زنجیره از توابع درهم‌سازی را برای خرید از فروشندگان مختلف به کار می برد. از نوعی امضای چشم بسته شده (Blind Signature) مبتنی بر منحنی‌های بیضوی (Elliptic Curve) برای حفظ گمنامی کاربر استفاده می‌شود، بدین صورت که بانک زنجیره سکه‌ها را به صورت چشم بسته برای درخواست کننده امضا می‌کند، بنابراین متوجه نخواهد شد که چه زنجیره‌ای را برای کدام مشتری امضا نموده است. همچنین مشتری از یک شناسه گمنام هنگام خرید استفاده می‌کند، بنابراین گمنامی وی نسبت به فروشنده و بانک محفوظ می‌ماند و خریدهای وی قابل رهگیری نخواهد بود. اگر سکه‌ای دوبار خرج شده باشد، هنگام تسویه حساب فروشنده با بانک، این مساله مشخص شده و هویت وی فاش می‌شود. بزرگترین مشکل این طرح این است که بانک برای هر خرید باید online باشد. برای انجام هر خرید، مشتری درخواست خود را به بانک ارائه می‌نماید. بانک در پاسخ باید یک کلید جلسه را تولید نموده و آن را هم برای مشتری و هم فروشنده مورد نظر ارسال نماید. مراودات مشتری و فروشنده از طریق این کلید جلسه انجام می شود. عدم دریافت رسید در قبال پرداخت سکه‌ها یا تحویل کالا نیز از دیگر مشکلات این پیشنهاد می‌باشد.

پروتکل دیگری که در راستای عمومیت بخشیدن به یک زنجیره مطرح شد، NetPay [12] می‌باشد. این پروتکل از یک بخش شامل امضای بانک و یک ایندکس که توسط فروشندگان امضا شده و از فروشنده‌ای به فروشنده دیگر منتقل می‌شود، استفاده می‌کند. امضای بانک برای اعتبار بخشی به زنجیره توابع درهم سازی و ایندکس امضا شده برای جلوگیری از دو بار خرج کردن سکه‌ها توسط مشتری بکار می‌رود. در این پروتکل سکه‌ها پیش پرداخت می‌شوند، بنابراین مشتری بیشتر از اعتبار موجود در حساب خود، قادر به خرج کردن سکه‌ها نخواهد بود. مشکلی که در این طرح به چشم می‌خورد این است که برای هر خریدِ مشتری، فروشنده باید با فروشنده قبلی که مشتری از آن خرید نموده تماس برقرار کند. هر فروشنده باید شناسه مشتریان و آخرین ایندکس خرج شده توسط وی را نگهداری نماید. عدم دریافت رسید و عدم گمنامی کاربر نیز از مشکلات دیگر این پروتکل می‌باشد.

پروتکلِ offline دیگری نیز توسط wenbo ارائه شده است [13]. در این پروتکل نیز سکه‌ها پیش پرداخت می شوند. در الگوی wenbo قرارداد زنجیره شامل امضای بانک بر روی ریشه زنجیره و امضای فروشنده‌ها بر روی باقیمانده زنجیره می باشد. این امضاها امکان خرید از فروشندگان مختلف را میسر می‌سازد. اگر کل زنجیره توسط فقط یک فروشنده استفاده شود، در این حال تنها امضای بانک برای تایید اعتبار سکه‌ها مورد نیاز است. اما اگر مشتری قصد خرید از فروشنده دیگری را داشته باشد، فروشنده فعلی آخرین سکه پرداخت شده را امضای دیجیتالی می‌کند. بنابراین فروشنده بعدی متوجه می شود که چه تعداد از سکه ها تا کنون خرج شده است. از الگوی امضای Schnorr برای حفظ گمنامی مشتری نسبت به بانک استفاده می شود. در صورتی که یک مشتری سکه ای را دو بار خرج کند، با استفاده از الگوی Schnorr هویت وی برای بانک فاش خواهد شد. عدم دریافت رسید، گمنام نبودن مشتری نسبت به فروشندگان و قابلیت رهگیری خریدهای وی از مشکلات الگوی wenbo می باشد.

پروتکل پیشنهادی در راستای رفع مشکلات مذکور و گردآوری ویژگیهای امنیتی و کاربردی مورد نیاز به صورت یکجا مطرح شده که در ادامه مورد بحث قرار خواهد گرفت.

۳-پروتکل پیشنهادی

الگوی پیشنهادی را می‌توان به چهار فاز تقسیم کرد: فاز ثبت نام مشتری در بانک، فاز تولید سکه‌ها، فاز پرداخت سکه‌ها به فروشنده، فاز تسویه حساب فروشنده با بانک.

پیش از شرح پروتکل ابتدا توضیحاتی راجع به علائم اختصاری مورد استفاده ذکر می‌شود:

B, M, C: نمادهای مشخص کننده مشتری، فروشنده و

بانک.

W_0 ، R_0 : ریشه زنجیره های توابع درهم سازی مربوط به سکه ها و رسیدها.

n : طول زنجیره.

K_{CB}: کلید مخفی مشترک بین مشتری و بانک.

ID_{M_k}, CID: شناسه مشتری در بانک و شناسه فروشنده k ام.

ID_c: شناسه مستعار مشتری.

OI: لیست کالاهای خرید مشتری.

K: شمارنده بیانگرِ چندمین فروشنده.

۳-۱- ثبت نام مشتری در بانک

مطابق طرح، پیش از انجام عملیات پرداخت ، مشتری باید در بانک ثبت نام نموده، کلید مخفی مشترکی با بانک را به طریق امن از بانک دریافت کند (K_{CB}). از این کلید جهت رمز کردن درخواست اولیه مشتری و در طول تراکنش برای احراز هویت مشتری و اطمینان از جامعیت داده ها استفاده می شود. در این الگو فرض می شود که بانک مورد اعتماد بوده و اطلاعات مخفی مشتری را در اختیار فروشندگان قرار نخواهد داد.

۳-۲-تولید سکه‌ها

مرحله ۱: مشتری ابتدا یک مقدار تصادفی W_n را انتخاب نموده، سپس زنجیره‌ای از توابع درهم سازی به طول n را به شکل زیر ایجاد می‌نماید:

$$W_{n-1} = h(W_n), \dots , W_{i-1} = h(W_i) \dots \quad \{i= 1, 2, \dots, n\}$$

از هر عضو این زنجیره به عنوان یک سکه در پرداخت استفاده می شود. W_0 ریشه زنجیره می باشد.

سپس مشتری زنجیره دیگری با ریشه R_0 را همانند زنجیره W_0 به شکل زیر ایجاد می کند:

$$R_{n-1} = h(R_n), \dots , R_{i-1} = h(R_i) \dots \quad \{ i= 1, 2, \dots, n\}$$

از این زنجیره به عنوان رسیدی استفاده می‌شود که مشتری در قبال دریافت کالا به فروشنده ارائه خواهد نمود. مشتری R_k را فروشنده k اُم خواهد داد.

سپس مشتری ریشه این دو زنجیره (R_0, W_0) را به همراه طول زنجیره، با کلید متقارن مشترک خود با بانک (K_{CB}) رمزگذاری نموده و به همراه شناسه خود (CID)، برای بانک ارسال می‌کند.

$C \rightarrow B$:
$\{W_0, R_0, n\}K_{CB}$, CID

مرحله ۲: با دریافت درخواست مشتری، بانک با استفاده از شناسه مشتری (CID)، کلید مشترک با وی را استخراج نموده، درخواست را رمزگشایی می کند. در صورت معتبر بودن درخواست و وجود اعتبار کافی در حساب مشتری، مبلغ به اندازه n سکه از حساب مشتری برداشت می گردد. سپس بانک یک شناسه مستعار (ID_C) برای مشتری تولید می کند. این شناسه با هر بار درخواست زنجیره جدید، به روز می شود. سپس بانک شناسه مستعار مشتری را به همراه طول زنجیره (n)، ریشه زنجیره سکه ها (W_0) و ریشه زنجیره رسید (R_0) با کلید خصوصی خود امضا نموده و برای مشتری ارسال می کند. امضای این مقادیر توسط بانک، فروشندگان را مطمئن می سازد که زنجیره با طول مورد نظر، توسط بانک اعتباردهی شده است. جامعیت و عدم امکان تغییر این مقادیر نیز توسط این امضا تامین می شود.

$B \rightarrow C$:
Bank_Signature: $\{W_0, R_0, n, ID_c\}sign_B$

۳-۳-پرداخت سکه‌ها به فروشنده

مرحله ۱: فرض کنیم مشتری قصد پرداخت i سکه به اولین فروشنده را دارد. مشتری امضای بانک، شناسه مستعار خود (ID_C)، شناسه فروشنده (ID_M)، اولین سکه قابل پرداخت (W_1) ، آخرین سکه پرداخت شونده (W_i)، تعداد سکه‌های پرداخت شونده (i)، مهر زمانی (timestamp)، عدد ۱ که بیانگر اولین فروشنده می‌باشد، نتیجه اعمال تابع درهم سازی بر روی لیست کالاهای خرید (h(OI)) و عبارت زیر را برای اولین فروشنده ارسال می‌کند:

$$HMAC[1,W_i,W_1,i,timestamp,ID_{M_1},h(OI),K_{CB}]$$

HMAC تابعی یکطرفه می‌باشد. در ورودی تابع مذکور از کلید مخفی مشترک بانک و مشتری (K_{CB}) استفاده می‌شود، بنابراین فروشنده قادر به بازتولید و تحریف آن نخواهد بود. استفاده از تابع HMAC جامعیت داده‌های ارسالی مشتری را تضمین می‌نماید. مشتری از h(OI) در تولید این تابع استفاده می‌کند. فروشنده نیز مقدار h(OI) را برای بانک ارسال می‌کند. از این طریق بانک بدون اینکه قادر به استخراج لیست کالاهای خرید مشتری (OI) باشد، در صورتیکه مقدار HMAC به درستی بازتولید شود، مطمئن می‌شود طرفین بر روی لیست خرید توافق دارند. وجود مهر زمانی تازگی پیام را مشخص می‌کند.

فروشنده امضای بانک را تایید اعتبار نموده و مطمئن می‌شود سکه‌های با ریشه W_0، از طرف بانک اعتباردهی شده‌اند. سپس فروشنده i مرتبه تابع درهم سازی را بر روی W_i اعمال می‌کند، اگر نتیجه برابر با W_0 موجود در امضای بانک شد، فروشنده مطمئن می شودکه اولا سکه‌ها معتبرند، ثانیا اطمینان می یابد که سکه‌ها توسط خودِ مشتری تولید شده‌اند، زیرا از آنجا که

توابع درهم سازی یکطرفه می باشند، کسی به غیر از مشتری، با داشتن مقدار W_0 قادر به تولید W_i نخواهد بود.

درصورتیکه مشتری قصد پرداخت i سکه به k اُمین فروشنده را داشته باشد، باید پیام زیر را برای فروشنده ارسال نماید.

$C \rightarrow M_k$:
Bank_Signature, ID_C, ID_{M_k}, W_{j+i}, W_j, i, timestamp, OI, k,
HMAC[k,W_{j+i},W_j,i,timestamp, ID_{M_k} , h(OI), K_{CB}],
{W_j, i□, k-1, n-j, h(OI□), ID_C}$sign_{M_{k-1}}$, cert(M_{k-1})

در پیام مذکور، W_j آخرین سکه ای است که مشتری تا کنون خرج نموده است. W_{j+i} آخرین سکه‌ای است که مشتری قصد پرداخت آن به فروشنده k اُم را دارد. OI لیست کالاهای الکترونیکی مورد نظر مشتری می‌باشد. عبارت زیر:

{W_j, i□, k-1, n-j, h(OI□), ID_C}$sign_{M_{k-1}}$

بیانگر باقیمانده زنجیره سکه‌ها است که مشتری از فروشنده قبلی (k-1 اُمین فروشنده) دریافت کرده است. آخرین سکه خرج شده در فروشنده K-1 اُم (W_j) به همراه تعداد سکه‌های باقیمانده و شمارنده k، توسط کلید خصوصی این فروشنده امضا شده و برای مشتری ارسال شده است. فروشنده k اُم، امضای فروشنده قبلی را تایید اعتبار می‌نماید. این امضا فروشنده فعلی را مطمئن می‌سازد که W_j آخرین سکه خرج شده در فروشنده قبلی می‌باشد. فروشنده فعلی i بار تابع درهم‌سازی را بر روی W_{j+i} اعمال می‌کند، اگر نتیجه برابر W_j شد، سپس j مرتبه تابع درهم‌سازی را بر روی آن اعمال می‌کند، اگر W_0 به دست آمد، مطمئن می‌شود که سکه‌های درستی را دریافت نموده است.

مرحله ۲: فروشنده در پاسخ، آخرین سکه دریافت شده را به همراه تعداد سکه‌های خرج شده، مقدار k ، تعداد سکه‌های باقیمانده از زنجیره n تایی، نتیجه اعمال تابع درهم‌سازی بر روی لیست کالاهای مورد نظر (h(OI)) و شناسه مستعار مشتری (ID_C) با کلید خصوصی خود امضا نموده و همراه با گواهینامه دیجیتالی خود برای مشتری ارسال می‌کند.

$M_k \rightarrow C$:
{W_{j+i}, i, k, n-j-i, h(OI), ID_C}$sign_{M_k}$, cert(M_k)

مرحله ۳: فروشنده کالا یا سرویس درخواستی مشتری را در اختیار وی قرار می‌دهد.

$M_k \rightarrow C$: goods

مرحله ۴: مشتری در پاسخ R_k را به عنوان رسید دریافت کالا، برای فروشنده ارسال می‌نماید. فروشنده k مرتبه تابع درهم سازی را بر روی R_k اعمال می نماید. اگر نتیجه برابر R_0 موجود در امضای بانک شد، فروشنده مطمئن می‌شود که رسید معتبری را دریافت نموده است. از آنجا که توابع درهم‌سازی یکطرفه اند، کسی جز مشتری نمی تواند مقدار R_k را تولید نماید.

$C \rightarrow M_k$: R_k

۳-۴-تسویه حساب فروشنده با بانک

مرحله۱: در پایان روز، فروشنده برای واریز سکه‌ها به حساب خود اقدام می‌کند. فروشنده باید امضای بانک بر روی زنجیره، شناسه خود (ID_M)، شناسه مستعار مشتری (ID_C)، اولین سکه (W_j) و آخرین سکه ای (W_{j+i}) که دریافت نموده، تعداد سکه‌های دریافتی (i)، مهر زمانی (timestamp)، عدد k، h(OI) و عبارت[]HMAC فرستاده شده توسط مشتری را برای بانک ارسال نماید.

$M_k \rightarrow B$:
Bank_Signature, ID_C, ID_{M_k}, W_j, W_{j+i} , i, timestamp, k, h(OI),
HMAC[k,W_{j+i},W_j,i,timestamp, ID_{M_k} , h(OI), K_{CB}]

بانک امضای موجود را تایید اعتبار نموده، i مرتبه تابع درهم‌سازی را بر روی سکه W_{j+i} اعمال می‌کند. اگر نتیجه برابر W_j شد، بانک j مرتبه دیگر تابع درهم‌سازی را بر روی آن اعمال می‌نماید. اگر W_0 موجود در پیام امضا شده بانک به دست آمد، بانک مطمئن می‌شود که سکه‌ها معتبرند. سپس بانک با توجه به شناسه مشتری (ID_C)، کلید مشترک با وی (K_{CB}) را از بانک اطلاعاتی خود استخراج می‌کند. با در دست داشتن مقادیر K_{CB} وسایر اطلاعات ارسال شده توسط فروشنده، بانک مقدار تابع []HMAC را بازتولید می‌نماید. در صورت برابر بودن حاصل این محاسبه با مقدار []HMAC موجود در پیام ارسالی فروشنده، بانک مطمئن می شود که مشتری با شناسه ID_C، سکه‌های W_j تا W_{j+i} را به فروشنده با شناسه ID_{M_k}پرداخت نموده است، زیرا از آنجا فروشنده مقدار K_{CB} را ندارد، قادر به تولید این تابع []HMAC نخواهد بود. بانک برای سکه‌های W_j تا W_{j+i} شناسه فروشنده (ID_{M_k}) را ثبت می‌نماید، اما نیازی به نگهداری سایر اطلاعات ارسالی توسط فروشنده نمی‌باشد.

مرحله ۲: نهایتا بانک مبلغ مورد نظر را به حساب فروشنده واریز نموده، رسیدی برای وی ارسال می‌کند.

$B \rightarrow M_k$: Receipt

۴-تحلیل امنیتی

در این قسمت ویژگی‌های امنیتی مختلف مورد نیاز یک سیستم پرداخت خرد که توسط الگوی پیشنهادی فراهم شده، مورد بررسی قرار می‌گیرد.

جعل سکه: در این طرح از آنجا که امضای بانک بر روی

ریشه هر زنجیره پس از کسر وجه از حساب مشتری اعمال می‌شود، کسی قادر به جعل امضای بانک و در نتیجه جعل سکه‌ها نخواهد بود.

دزدی سکه: از آنجا که زنجیره سکه‌ها با اعمال توابع یکطرفه درهم‌سازی تولید می‌شود، هیچ فردی با در اختیار گرفتن یک W_i قادر به تولید سکه‌های دیگرِ آن زنجیره نخواهد بود. اگر شخصی به طریقی سکه‌های W_i تا W_j متعلق به یک مشتری را به دست آورد، برای پرداخت آن به یک فروشنده، باید باقیمانده امضا شده توسط فروشنده قبلی را نیز در دست داشته باشد. حتی در صورت در دست داشتن این مقدار، فقط سکه‌های W_i تا W_j زنجیره قابل استفاده خواهند بود که به دلیل ارزش پایین سکه‌ها ضرر زیادی متوجه فروشنده یا صاحب واقعی سکه‌ها نخواهد شد.

گمنامی: در طرح پیشنهادی، هویت واقعی مشتری برای فروشنده گمنام باقی می‌ماند. زیرا مشتری یک شناسه مستعار را در اختیار فروشنده قرار می‌دهد. اما از آنجا که پرداخت به صورت offline انجام می‌شود، احتمال دو بار خرج کردن سکه‌ها توسط مشتری وجود دارد. در این صورت فرد مجرم باید قابل شناسایی باشد، بنابراین هویت وی برای بانک گمنام نیست. می‌توان از روشهایی استفاده نمود که مادامی که مشتری سکه ای را دو بار خرج نکرده باشد هویت وی برای بانک فاش نگردد [14]. استفاده از این روش‌ها مستلزم انجام محاسبات خاصی توسط مشتری و فروشنده بر روی هر عضو زنجیره می‌باشد، بنابراین افزایش سربار محاسباتی را به همراه دارد و در پروتکل پیشنهادی استفاده نشده است.

حفظ حریم خصوصی: برای تامین این ویژگی لازم است که خریدهای مختلف مشتری توسط بانک یا فروشندگان قابل پیگیری نباشد و اطلاعات حساس مشتری نیز نباید در اختیار فروشندگان قرار گیرد. در طرح پیشنهادی اطلاعات خرید مشتری به بانک داده نمی‌شود، در عوض نتیجه تابع درهم سازی بر روی لیست خرید ($h(OI)$) در اختیار بانک قرار می گیرد. از آنجا که توابع درهم سازی یکطرفه هستند، لیست کالاها با داشتن این مقدار قابل استخراج نخواهد بود. همچنین از آنجا که بانک برای هر زنجیره، شناسه متفاوتی را برای مشتری تولید می‌کند، خریدهای مشتری در بازه های زمانی طولانی، توسط فروشندگان قابل رهگیری نخواهد بود. اطلاعات بانکی و سایر اطلاعات حساس مشتری نیز در اختیار فروشندگان قرار نمی‌گیرد، بنابراین حریم خصوصی مشتری حفظ می‌شود.

جامعیت داده: در طرح پیشنهادی، هنگام پرداخت سکه‌ها، شناسه مشتری و آخرین سکه استفاده شده در باقیمانده امضا شده فروشنده قبلی موجود است. از این طریق فروشنده مطمئن می شود که آخرین سکه خرج شده و شناسه مشتری در حین انتقال تغییر نکرده‌اند. اطلاعات سکه‌های مشتری، $h(OI)$، شناسه فروشنده فعلی و شمارنده k در پیام HMAC قرار گرفته‌اند. از آنجا که در تولید این مقدار از K_{CB}(که بین مشتری و بانک مخفی است) استفاده شده، فروشنده یا شخص ثالث دیگری قادر به تغییر داده‌های اصلی و بازتولید این تابع نخواهد بود، بنابراین جامعیت داده‌ها در طرح پیشنهادی تامین شده است.

تشخیص دوبار خرج کردن سکه: برای بررسی دوبار خرج شدن سکه‌ها، بانک برای هر سکه W_i باید شناسه فروشنده ارائه کننده سکه را نگهداری کند. اگر مشتری سکه W_i را در دو فروشنده مختلف خرج نموده باشد، بانک با دریافت دوباره این سکه متوجه می‌شود که فروشنده دیگری قبلا این سکه را ارائه نموده، بنابراین پی خواهد برد که مشتری سکه را دوبار خرج کرده است.

اگر فروشنده‌ای سکه W_i را دوبار به بانک ارائه نماید، بانک متوجه می‌شود که شناسه این فروشنده قبلا برای سکه W_i ثبت شده، بنابراین فروشنده اقدام به دوبار برداشت سکه نموده و مقصر است.

اگر مشتری بتواند سکه W_i را دو مرتبه به یک فروشنده پرداخت نماید، هنگام ارائه سکه‌ها به بانک به اشتباه تصور می‌شود که فروشنده قصد دوبار برداشت کردن سکه W_i را دارد. برای جلوگیری از این مشکل، فروشنده باید برای هر زنجیره با ریشه W_0 ، آخرین سکه خرج شده را نگهداری نماید. با دریافت هر سکه از مشتریان، فروشنده باید بررسی کند که آیا عضوی از این زنجیره را قبلا دریافت نموده یا خیر؟ در صورت وجود، اندیس سکه جدید باید از اندیس آخرین سکه خرج شده در این فروشنده بیشتر باشد.

رفع اختلاف بین مشتری و فروشنده : اگر فروشنده‌ای سکه‌ها را از مشتری دریافت نموده اما کالایی به وی ارائه ننماید، مشتری از باقیمانده امضا شده فروشنده برای اثبات پرداخت خود استفاده خواهد کرد. به این ترتیب که عبارتِ

$$\{W_{j+i}, i, k, n-j-i, h(OI), ID_C\}sign_{M_k}$$

را به همراه امضای بانک، برای بانک ارسال می‌کند. امضای بانک، سکه‌های متعلق به مشتری با شناسه ID_C را اعتباردهی می‌کند. امضای فروشنده نیز اثبات می‌کند که فروشنده سکه های W_j تا W_{j+i} از این زنجیره را از مشتری ID_C دریافت نموده است. اگر فروشنده رسید ارائه کالا را در اختیار نداشته باشد، مشخص می‌شود که کالا را به مشتری تحویل نداده است. بنابراین مشتری باید امضای فروشندگان را برای رفع اختلافات احتمالی نگهداری کند.

مشتری در صورت دریافت کالای مورد نظر باید رسیدی به فروشنده ارائه نماید. همانطور که ذکر شد هنگام تولید سکه‌ها، زنجیره R به طول n نیز توسط مشتری تولید شده و ریشه آن (R_0) به امضای بانک می‌رسد. مشتری در قبال دریافت کالا از فروشنده k اُم، مقدار R_k را به عنوان رسید به فروشنده ارائه می‌نماید. فروشنده k مرتبه تابع درهم‌سازی را بر روی R_k اعمال می‌کند، در صورتیکه R_0 به دست آید، فروشنده مطمئن می‌شود که رسید درستی دریافت نموده است.

چنانچه مشتری ادعا کند کالایی دریافت نکرده، فروشنده با ارائه R_k ادعای وی را رد خواهد نمود، زیرا این مقدار فقط در ازای تحویل کالا به فروشنده داده می‌شود و کسی جز مشتری نیز قادر به تولید آن نخواهد بود. بنابراین با استفاده از یک زنجیره و بدون نیاز به امضا نمودن رسید، مشتری قادر به انکار دریافت کالای مورد نظر نخواهد بود.

چنانچه فروشنده کالایی به غیر از کالای درخواستی مشتری را به وی ارائه نماید، مشتری با استفاده از باقیمانده امضا شده توسط فروشنده قادر به اثبات سفارش خود خواهد بود. زیرا فروشنده h(OI) را نیز به همراه باقیمانده زنجیره امضا نموده است.

۴-۱- مقایسه با پروتکل‌های دیگر

در جدول (۱) ویژگی‌های مختلف پروتکل پیشنهادی با پروتکل‌های مذکور مورد مقایسه قرار گرفته‌اند.

جدول (۱): مقایسه معیارهای امنیتی و کاربردی

پروتکل / ویژگی	Pay word	Hwang's et al	Wenbo's et al	Lee's et al	Net pay	پروتکل پیشنهادی
تشخیص دو بار خرج کردن	Y	Y	Y	Y	Y	Y
جلوگیری از جعل سکه	Y	Y	Y	Y	Y	Y
گمنامی نسبت به فروشنده	-	Y	-	-	Y	Y
گمنامی نسبت به بانک	-	Y	Y	-	-	-
عدم رهگیری سفارشات مشتری	-	Y	-	-	Y	Y
تحویل رسید در قبال دریافت سکه	-	-	-	Y	-	Y
تحویل رسید در قبال دریافت کالا	-	-	-	-	-	Y
خرید چندگانه	-	Y	Y	Y	Y	Y

با توجه به جدول(۱) مشاهده می‌شود که پروتکل پیشنهادی ویژگی‌های بیشتری را نسبت به پروتکل‌های مذکور تامین می‌کند.

۵- تحلیل کارایی

در پروتکل پیشنهادی مشتری مجبور نیست برای هر فروشنده زنجیره جدیدی تولید نموده و قرار داد الکترونیکی امضا کند. در نتیجه تعداد عملیات امضای دیجیتال توسط مشتری کاهش می‌یابد، اما در عوض هر فروشنده یک امضای دیجیتال بر روی باقیمانده زنجیره انجام می‌دهد. در جدول (۲) با فرض اینکه مشتری از k فروشنده مختلف خرید انجام دهد، تعداد عملیات انجام شده توسط نقشهای درگیر در پرداخت، در پروتکلهای مذکور مورد مقایسه قرار گرفته است.

مشاهده می‌شود در پروتکل پیشنهادی از رمزنگاری نامتقارن استفاده نشده است. تعداد عملیات تایید امضا نسبت به پروتکل‌های دیگر بهبود یافته، ولی تعداد عملیات امضای دیجیتال انجام شده توسط فروشنده نسبت به پروتکل Hwang's et al افزایش یافته، اما در عوض پروتکل پیشنهادی نیاز به online بودن بانک در هر تراکنش را حذف نموده است. محاسبات HMAC و رمزنگاری متقارن در پروتکل پیشنهادی نسبت به برخی دیگر از پروتکل‌های مذکور افزایش یافته که در مقایسه با عملیات امضا و تایید امضای دیجیتال و رمزنگاری نامتقارن از سربار بسیار کمتری برخوردار است. به طور کلی می‌توان گفت پروتکل پیشنهادی از کارایی بهتری نسبت به پروتکل‌های Netpay، Lee's et al و Wenbo's et al برخوردار است و نسبت به دو پروتکل PayWord و Hwang's et al کاهش کارایی نداشته است.

در جدول زیر n بیانگرطول زنجیره و عبارت ih نشان دهنده انجام i عمل درهم سازی به ازای دریافت سکه با اندیس i می باشد. C، M و B نیز مشخص کننده مشتری، فروشنده و بانک می‌باشند.

جدول (۲): مقایسه معیارهای کارایی،

پروتکل / عملیات		Pay Word	Hwang's et al	Wenbo's et al	Lee's et al	Netpay	پروتکل پیشنهادی
Digital signature	C	k	۰	k	0	0	۰
	M	۰	0	k	k	k	k
	B	1	۱	1	k+1	1	1
Signature verification	C	۰	0	1	1	1	1
	M	k * 2	k	3k	2k	2k	k
	B	k	k	3k	2k	2k	k
Public key operation	C	0	0	0	1+3k	k	0
	M	0	0	0	3k	0	0
	B	0	0	0	1	1	0
Symmetric operation	C	۰	2+3k	0	1	0	۱
	M	۰	3k	0	1	0	۰
	B	۰	6k	0	0	0	۱
Hash function	C	k * n	n+k	n+k	3+n	0	2n + k
	M	k * n	k+ih	k+ih	3+ih	ih	k+ ih
	B	k * n	k+n+ ih	ih	ih	n+ ih	k+ ih
HMAC	C	0	0	0	0	0	k
	M	0	0	0	0	0	0
	B	0	0	0	0	0	k
Offline bank		Yes	-	Yes	Yes	Yes	Yes

۶- نتیجه

در این مقاله دسته‌ای از سیستم‌های پرداخت خرد که مبتنی بر زنجیره‌ای از توابع درهم سازی می باشند، مورد بررسی قرار گرفته‌اند. ایده اولیه استفاده از زنجیره توابع درهم سازی در پروتکل payword بکار رفته است. این پروتکل دارای مشکلاتی در زمینه مسائل امنیتی و کاربردی است، از جمله: عدم گمنامی مشتری، امکان انکار تراکنش توسط مشتری یا فروشنده، امکان رهگیری سفارشات مشتری و وابستگی هر زنجیره به فروشنده خاص. تا کنون پیشنهادات مختلفی در راستای رفع این مشکلات مطرح شده است. هر یک از این پیشنهادات تعدادی از مشکلات را برطرف نموده‌اند. در این مقاله، با توسعه payword پروتکلی پیشنهاد شده که سعی در گردآوری ویژگیهای مورد نیاز یک سیستم پرداخت خرد به صورت یکجا دارد. نشان داده شده است که پروتکل پیشنهادی نسبت به دیگر پروتکل‌های مبتنی بر payword ، ویژگی‌های بیشتری را تامین می‌کند، بدون اینکه کاهش کارایی نسبت به بقیه پروتکل‌ها را به همراه داشته باشد.

مراجع

[1] O. M. Donal, P. Michael and T. Hitesh, ”Electronic Payment Systems for E-Commerce”, Second Edition, 2003.
[2] B. Mihir, “iKP.A Family of Secure Electronic Payment Protocols”, Proc. 1st USENIX Workshop on Electronic Commerce, New York, July 1995.
[3] “MasterCard and Visa Corporations, Secure Electronic Transaction (SET) Specification”, Book 1: Business Description Version 1.0, May 1997.
[4] D. Eastlake, CyberCash Credit Card Protocol Version 0.8, RFC 1898, February 1996.
[5] M. S. Manasee, “The Millicent Protocols for Electronic Commerce,” Proceeding of 1st USENIX workshop on Electronic Commerce, 1995.
[6] R. Ronald and S. Adi, “PayWord and MicroMint: Two Simple Micropayment Schemes”, Proceeding of Security Protocols Workshop, LNCS 1189, New York: Springer-Verlag, 1997.
[7] S. Marvin and T. J. Tyger, “NetBill: An Electronic Commerce System Optimized for Network Delivered Information and Services”, Proceeding of IEEE CompCon ’95, San Francisco, CA, USA, March 1995.
[8] A. Furche and G. Wrightson, ”SubScrip.An Efficient Protocol for Pay-Per-View Payments on the Internet”, Proc. 5th Int. Conference on Computer Communications and Networks (ICCCN .96), Rockville, October 1996.
[9] R. Hauser, M. Steiner and M. Waidner, “Micro-Payments Based on iKP”, Proc. 14th Worldwide Congress on Computer and Communications Security Protection, Paris, 1996.
[10] L. Manho and K. Kwangjo, “A Micro-payment System for Multiple-Shopping”, SCIS 2002 The 2002 Symposium on Cryptography and Information Security Shirahama,Japan, Feb 2002.
[11] H. Min-Shiang and S. Pei-Chen, “A Study of Micro-payment Based on One-Way Hash Chain”, International Journal of Network Security, Vol.2, No.2, Mar 2006.
[12] X. Dai and B. Lo, “NetPay – An Efficient Protocol for Micropayments on the WWW”. Fifth Australian World Wide Web Conference, Australia, 1999.
[13] W. Mao. “A Simple Cash Payment Technique for the Internet”, Proceedings of 1996 European Symposium Springer-Verlag, September 1996.

[14] C. jan and M. Ueli, “Digital Payment Systems with Passive Anonymity Revoking Trustees”, Lecture note in computer science, Springer verlage, 1996.