هشتمین کنفرانس بین المللی انجمن رمز ایران
دانشگاه فردوسی مشهد - ۲۳ و ۲۴ شهریور ۱۳۹۰

# FAPSWPP : یک پروتکل خرید امن کالای الکترونیکی مبتنی بر APSWPP

سمانه لایقیان جوان [۱]، عباس قائمی بافقی [۲]
[۱] کارشناس ارشد مهندسی فناوری اطلاعات
[۲] استادیارگروه مهندسی کامپیوتر دانشگاه فردوسی مشهد

## چکیده

**در این مقاله با توسعه پروتکل پرداخت الکترونیکی APSWPP ، یک پروتکل خرید امن کالای الکترونیکی به نام FAPSWPP پیشنهاد می شود که در آن با بکارگیری گواهینامه CEMBS و استفاده از روش تبادل خوشبینانه، مشتری از دریافت کالا در ازای پرداخت وجه و فروشنده نیز از دریافت وجه و رسید در قبال تحویل کالا مطمئن می باشند. پروتکل پیشنهادی از لحاظ معیارهای امنیتی و کارایی مورد ارزیابی و مقایسه با پروتکل‌های مرتبط قرار گرفته، نشان داده می شود که علاوه بر کارایی بهتر، کلیه ویژگی‌های امنیتی مورد نیاز یک سیستم خرید امن را فراهم می آورد.**

## کلمات کلیدی

**خرید الکترونیکی، امنیت، تبادل منصفانه، کارایی**

## ۱- مقدمه

تاکنون پروتکل‌های پرداخت الکترونیکی مختلفی از جمله پول الکترونیکی [۲, ۳]، چک الکترونیکی [۴, ۵]، پروتکل‌های پرداخت خرد [۶, ۷] و پروتکل‌های مبتنی بر کارت اعتباری [۸] توسعه یافته است. پرداخت از طریق شبکه‌ها به خصوص اینترنت امنیت بالایی می طلبد، زیرا ارسال داده‌ها و اطلاعات محرمانه مالی نگرانی‌های زیادی به دنبال می‌آورد. اصلی ترین نیازهای امنیتی یک پروتکل پرداخت امن عبارتند از محرمانگی[۱]، احراز هویت[۲]، انکارناپذیری[۳]، جامعیت داده‌ها[۴] ، مجوز دسترسی[۵]، حفظ حریم خصوصی افراد[۶] و گمنامی[۷].

در تراکنش‌های خرید کالاهای الکترونیکی از قبیل پروتکل NetBill [۹] و پروتکل پیشنهادی Lee [۱۰] ، نیاز امنیتی دیگری نیز به چشم می خورد. در تراکنش‌های غیر الکترونیک، از آنجا که معامله در یک مکان مشخص صورت می گیرد، هیچ یک از طرفین نمی تواند بدون انجام درست تعهدات خود تراکنش را به صورت نیمه تمام رها کند. اما در معاملات الکترونیکی افراد غالباً مکان فیزیکی قابل شناسایی و مشخصی ندارند. هر یک از طرفین می تواند بدون انجام کامل تعهدات خود ناپدید شود. برای جلوگیری از این مشکل، پروتکل‌های خرید الکترونیک باید به گونه ای طراحی شوند که امکان این گونه از تخلفات برای هیچ یک از طرفین وجود نداشته باشد. به چنین معامله ای، مبادله منصفانه[۸] می‌گویند.

تا کنون مطالعات زیادی در زمینه تبادل منصفانه انجام شده که به دو دسته کلی پروتکل‌های تبادل تدریجی و پروتکل‌های تبادل مبتنی بر شخص ثالث تقسیم می شوند. پروتکل‌های تبادل تدریجی به تدریج با چندین مرحله تبادل پیام، احتمال تبادل منصفانه را افزایش می دهند [۱۱]. پروتکل‌های مبتنی بر شخص ثالث از یک شخص ثالث مورد اعتماد به صورت برخط یا برون خط استفاده می کنند [۱۲, ۱۳]. پروتکل‌هایی که فقط هنگام بروز اختلاف به شخص ثالث رجوع می‌شود را پروتکل‌های تبادل خوشبینانه[۹] می نامند [۱۳, ۱۴].

در این مقاله با توسعه پروتکل پرداخت سیار APSWPP[۱۰] [۱]، یک پروتکل خرید امن کالای الکترونیکی پیشنهاد شده است. در این پروتکل توسعه یافته که FAPSWPP[۱۱] نامیده شده از روش تبادل خوشبینانه جهت برقراری مبادله منصفانه استفاده می شود. پروتکل پیشنهادی از لحاظ معیارهای امنیتی و کارایی ارزیابی و با سایر پروتکل‌های خرید الکترونیکی مقایسه شده و نشان داده می‌شود که علاوه بر تامین کلیه ویژگی‌های امنیتی مورد نیاز، از کارایی بهتری نسبت به آنها برخوردار است.

در ادامه مقاله در بخش ۲ ایده گواهینامه CEMBS[۱۲] و خلاصه ای از پروتکل APSWPP بیان می شود. در بخش ۳ پروتکل پرداخت پیشنهادی

FAPSWPP شرح داده می شود. بخش ۴ به تحلیل ویژگی‌های امنیتی پروتکل پیشنهادی اختصاص یافته است. در بخش ۵ ویژگی‌های امنیتی و کارایی پروتکل پیشنهادی مورد مقایسه با پروتکل‌های مرتبط قرار گرفته و نهایتا در بخش ۶ جمع بندی و نتیجه گیری انجام می شود.

## ۲- کارهای مرتبط

### ۲-۱- گواهینامه CEMBS

ایده گواهینامه CEMBS اثبات می کند که پیام رمز شده $C_T$ شامل امضای فرد A بر روی فایل عمومی M می باشد که توسط A رمزنگاری شده است، بدون اینکه این امضا از پیام رمز شده قابل استخراج باشد [۱۵]. این گواهینامه به شکل زیر توسط A ایجاد می گردد:

فرض کنیم p و q دو عدد اول باشند به طوریکه $p = 2q + 1$ باشد. اگر $G \in Z^*_p$ باشد آنگاه خواهیم داشت: $q = ord(G)$. مقدار g نیز یک مولد از $Z^*_q$ می باشد. پارامتر n برابر با مقدار pq انتخاب می شود $(n = pq)$.

اگر SK و PK کلیدهای خصوصی و عمومی جهت انجام امضای دیجیتال و تایید اعتبار آن باشند، v را به گونه ای انتخاب می کنیم که رابطه زیر برقرار باشد:

$$(SK)^v (PK) = 1 \bmod n$$

**ایجاد امضا:** A عدد $r \in Z_n$ را انتخاب نموده و مقادیر $T = r^v \bmod n$ و $d = h(M, T)$ و $D = r(Sk_A)^d \bmod n$ را محاسبه می کند. امضای A بر روی پیام M عبارتست از $sign_A = (d, D)$. برای تایید اعتبار امضا باید بررسی کرد که عبارت $d = h(M, D^v J^d)$ برابر True باشد.

**رمزنگاری:** A عدد $w \in_R Z^*_q \bmod n$ را انتخاب نموده، مقادیر $W = g^w \bmod n$ و $V_T = D(PK_T)^w \bmod n$ را محاسبه می کند. پیام رمز شده عبارتست از : $C_T = (W, V_T)$. توجه داشته باشید که در اینجا تنها D رمزنگاری شده و d به صورت عمومی باقی می ماند. این مساله محرمانگی D را از بین نخواهد برد.

**تولید CEMBS** : CEMBS_Cert برای اثبات سه معادله زیر، بدون آشکار کردن مقدار w استفاده می‌شود:

$$W = g^w \bmod n \quad (۱)$$

$$V_T = D(PK_T)^w \bmod n \quad (۲)$$

$$d = h(M, D^v J^d) \quad (۳)$$

فرض کنیم $V = D^v$ باشد. معادلات (۱)، (۲) و (۳) را به شکل زیر می توان بازنویسی کرد:

$$d = h(M, VJ^d) \quad (٤)$$

$$W = g^w \bmod n \quad (٥)$$

$$(V_T)^v / V = (PK_T^v)^w \bmod n \quad (٦)$$

CEMBS نیز عبارتست از :

$$Cert = (r, c, V, d)$$

به طوریکه $V = D^v$ در رابطه (۴) قرار می گیرد و (r, c) بدون فاش کردن مقدار w، اثبات می کند که روابط (۵) و (۶) برای w برقرار می باشد. روند ایجاد (r, c) به شکل زیر می باشد:

مقدار $u \in \{1, 2, \ldots, q-1\}$ را به طور تصادفی انتخاب کرده، مقادیر $a = g^u \bmod n$ و $A = (PK_T^v)^u \bmod n$ را محاسبه می نماییم. همچنین r و c را برابر عبارات زیر قرار می دهیم:

$$r = u - cw \bmod q$$

$$c = h(g, W, PK_T^v, (V_T)^v / V, a, A)$$

در عبارت فوق، h یک تابع درهم سازی یکطرفه با دامنه زیر می باشد:

$$h: \{0, 1\}^* \rightarrow \{0, 1\}^{|q|-1}$$

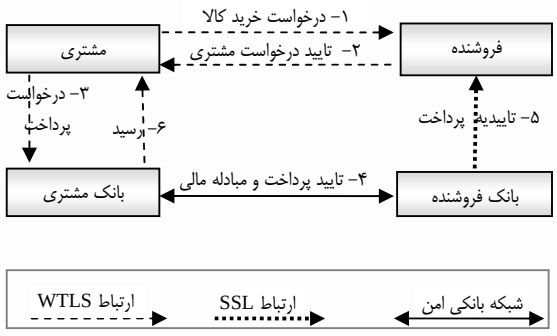
**تایید اعتبار CEMBS :** برای ارزیابی $Cert = (r, c, V, d)$ باید بررسی کنیم که آیا رابطه (۴) و عبارت زیر برقرار می باشند یا خیر؟

$$C = h(g, W, PK_T^v, (V_T)^v / V, g^r W^c, (PK_T^v)^r (V_T^v/V)^c)$$

معلوم بودن $Cert = (r, c, V, d)$ کمکی به افشای مقدار D نمی کند، زیرا D از رابطه $V = D^v \bmod n$ قابل استخراج نمی باشد.

### ۲-۲- پروتکل APSWPP

پروتکل APSWPP مبتنی بر SWPP[۱۳] بوده و جهت استفاده در محیط سیار پیشنهاد شده است [۱]. APSWPP علاوه بر تامین کارایی بهتر برخی ضعف‌های امنیتیِ SWPP از قبیل عدم گمنامی مشتری و عدم حفظ حریم خصوصی مشتری را نیز مرتفع می‌کند. در این پروتکل از یک گواهینامه دیجیتالی مستعارِ امضا شده به صورت چشم بسته[۱۴] و یک حساب بانکی گمنام، برای مخفی نگه داشتن هویت مشتری استفاده می شود [۱]. معماری، اجزاء اصلی و روند انجام این پروتکل در شکل (۱) به صورت سطح بالا نشان داده شده است.




**شکل (۱) : معماری پروتکل APSWPP**

در [۱] نشان داده شده که پروتکل APSWPP کلیه ویژگی‌های امنیتی مورد نیاز یک پرداخت الکترونیکی امن شامل محرمانگی، احراز هویت، انکارناپذیری، جامعیت داده‌ها، مجوز دسترسی حفظ حریم خصوصی افراد و گمنامی را فراهم می‌کند. اما در این پروتکل مسائل دیگر یک سیستم خرید الکترونیکی شامل ویژگی مبادله منصفانه مورد بررسی قرار نگرفته است.

## ۳- توسعه پروتکل APSWPP جهت ایجاد یک سیستم امن خرید کالای الکترونیکی

در این قسمت با توسعه پروتکل APSWPP قصد تامین ویژگی تبادل منصفانه را داریم. بدین معنی که مشتری باید مطمئن شود که در ازای پرداخت وجه حتما کالای مورد نظر خود را دریافت خواهد کرد. فروشنده نیز باید مطمئن شود که در قبال تحویل کالا وجه مورد نظر را دریافت می کند. همچنین هیچیک از طرفین نباید قادر به انکار دریافت عنصر مورد نظر خود باشند. به این منظور مشتری و فروشنده باید رسیدهای امضا شده ای مبنی بر پرداخت وجه یا تحویل کالا دریافت کند. این پروتکل توسعه یافته را FAPSWPP می‌نامیم.

پیش از ادامه مطالب ابتدا در جدول ۱ توضیحاتی راجع به علایم اختصاری مورد استفاده در پروتکل بیان می شود.

**جدول (۱) : علائم اختصاری**

| علامت | توصیف |
|---|---|
| I, A, C, M | فروشنده، مشتری، بانک فروشنده، بانک مشتری |
| T | شخص ثالث مورد اعتماد |
| PI | اطلاعات پرداخت |
| MBI | اطلاعات بانکی فروشنده |
| CBI | اطلاعات بانکی مشتری |
| HI | عددی تصادفی برای مخفی کردن اطلاعات کالاها از بانک |
| CID | شناسه ای یکبارمصرف که خریدار به فروشنده اعلام میکند، به طوریکه $CID = h(ID_C, R_C)$ |
| OI | سفارش خرید مشتری |
| t | مهر زمانی |
| Tid | شناسه تراکنش که تراکنش را به طور منحصر به فرد مشخص می کند. |
| $ID_X$ | شناسه منحصر به فرد عامل X |
| $Sign_X$ | امضای دیجیتالی انجام شده توسط عامل X |
| $PK_X$ | کلید عمومی عامل X |
| $Cert_X$ | گواهینامه دیجیتالی X |
| $ID_c$ | شناسه منحصر به فرد مشتریِ گمنام که در بانک ثبت شده است. |
| h() | تابع درهم سازی یکطرفه |
| $R_c$ | عددی تصادفی برای مخفی کردن شناسه اصلی مشتری از فروشنده |
| $k_A$ | رمز مخفی جهت دسترسی مشتری به حساب |
| Nonce | عددی تصادفی است برای مخفی کردن رمز مخفی $K_A$ |
| [x, k] | رمزگذاری پیام x توسط کلید k |
| m | کالایی که مشتری قصد خرید آن را دارد. |
| PID | شناسه مشخص کننده کالای m |
| $C_T$ | رسید دریافت کالا که مشتری امضا و با کلید عمومی شخص ثالث رمزگذاری می کند. |

در پروتکل FAPSWPP از یک شخص ثالث مورد اعتماد جهت تامین ویژگی تبادل منصفانه کمک گرفته می شود که در صورت بروز اختلاف به وی رجوع می شود. در ادامه پروتکل توسعه یافته پیشنهادی شرح داده می شود.

فرض می کنیم مراحل زیر قبل از انجام تراکنش انجام شده است:

فروشنده در یک شخص ثالث مورد اعتماد (TTP[۱۵]) ثبت نام کرده و کالای m را به وی ارائه می‌کند تا شخص ثالث آن را با کلید k رمزگذاری نموده و در یک مکان عمومی که ما آن را کاتالوگ می نامیم، به عنوان تبلیغ کالای m قرار دهد. زمانی که مشتری قصد خرید کالای m از فروشنده را دارد، باید کالای رمز شده [m, k] را از کاتالوگ دانلود کند. برای هر کالای m فروشنده باید کالا را به همراه توصیف آن و شناسه مشخص کننده کالا برای شخص ثالث ارسال نماید. شخص ثالث برای هر کالا یک کلید رمزنگاری k تولید کرده و آن را در اختیار فروشنده نیز قرار می دهد. در این روش شخص ثالث کالا را ارزیابی کرده و از تطابق آن با توصیفی که برای آن ارائه شده اطمینان می یابد. جهت خرید کالا، مشتری کالای رمز شده را از کاتالوگ شخص ثالث مورد اعتماد دانلود می کند، پس از تطابق کالای رمز شده با توصیف آن مطمئن باشد.

### ۳-۱- مراحل انجام تراکنش

این پروتکل از ۱۰ مرحله تشکیل می‌شود که در ادامه بیان شده و سپس به تحلیل مکانیزمهای امنیتی به کار رفته در پروتکل پرداخته می‌شود.

#### ۳-۱-۱- درخواست خرید کالا

مشتری ابتدا کالای رمز شده [m, k] را به همراه شناسه کالا (PID) از کاتالوگ شخص ثالث مورد اعتماد دانلود می کند، سپس یک کانال امن WTLS[۱۶] با فروشنده برقرار کرده و یک تراکنش را آغاز می نماید. مشتری در پیام آغازین شناسه خود ($ID_C$) را همراه با عدد تصادفی (HI) و سفارش خرید (OI) برای فروشنده ارسال می کند. از HI جهت مخفی کردن سفارش خرید از چشم بانک استفاده می شود. سفارش خرید (OI) شامل شناسه کالا (PID)، قیمت کالا (Price)، شناسه مشتری ($ID_C$) و شناسه فروشنده ($ID_M$) می باشد.

۱- Customer → Merchant:
{ $ID_C$, HI, TidRequest, OI}

#### ۳-۱-۲- تایید درخواست مشتری

فروشنده با دریافت درخواست مشتری شناسه Tid (شامل تاریخ و زمان فعلی) را برای مشخص کردن تراکنش ایجاد می کند. فروشنده در پاسخ شناسه تراکنش (Tid)، قیمت کالا (Price)، شناسه خود ($ID_M$) و شناسه بانک خود ($ID_A$) را به همراه کالای رمزنگاری شده با کلید k برای مشتری ارسال می نماید.

۲- Merchant → Customer:
{ Tid, Price, $ID_M$, $ID_A$ } , [m, k]

#### ۳-۱-۳- ایجاد و رمزگذاری رسید دریافت کالا

مشتری با دریافت کالای رمز شده از فروشنده، آن را با کالای رمز شده ای که از کاتالوگ شخص ثالث دانلود کرده مقایسه می کند تا از برابری آنها مطمئن شود. در صورت درستی کالا، مشتری رسید دریافت کالا را به شکل زیر ایجاد می‌کند:

Receipt : {Tid, $ID_M$, $ID_C$, Price, OI}

سپس رسید فوق را با کلید خصوصی خود مطابق روشی که در بخش ۲-۲ ذکر شد امضا می نماید.

Signed_Receipt : {Tid, $ID_M$, $ID_C$, Price, OI}$Sign_C$

پس از تولید رسید امضا شده، مشتری باید آن را با کلید عمومی شخص ثالث مورد اعتماد رمزگذاری کرده و پیام $C_T$ را به شکل زیر ایجاد کند:

$C_T = [(\{Tid, ID_M, ID_C, Price, OI\}Sign_C), PK_T]$

مشتری گواهینامه CEMBS را نیز باید ایجاد کند. به کمک این گواهینامه، فروشنده بدون امکان استخراج رسید امضا شده مشتری از $C_T$ ، می تواند ارزیابی کند که $C_T$ شامل رسید امضا شده مشتری می باشد که با کلید عمومی شخص ثالث ($PK_T$) رمزنگاری شده است. مشتری $C_T$ و گواهینامه CEMBS را به همراه گواهینامه دیجیتالی مستعار خود برای فروشنده ارسال می نماید.

۳- Customer → Merchant:

$C_T = [(\{Tid, ID_M, ID_C, Price, OI\}Sign_C), PK_T]$ ,
$CEMBS\_Cert, Cert_C$

### ۳-۱-۴- امضای قرارداد تراکنش توسط فروشنده

فروشنده محتوای رسید امضا شده مشتری را در اختیار دارد. با دریافت $C_T$ و CEMBS_Cert و نیز با دراختیار داشتن کلید عمومی شخص ثالث ($PK_T$)، فروشنده ابتدا باید مطمئن شود که $C_T$ شامل امضای مشتری بر روی اطلاعات رسید می باشد. به این منظور به کمک اطلاعات موجود محاسباتی را جهت ارزیابی این مساله انجام می دهد که با عبارت زیر نشان داده می شود:

$Verify (CEMBS\_Cert, C_T, Receipt, PK_T, PK_C) = Yes$

چنانچه ارزیابی رسید امضا و رمز شده درست بود، فروشنده پیامی شامل شناسه تراکنش (Tid)، شناسه خود ($ID_M$) و شناسه بانک خود ($ID_A$)، شناسه مشتری ($ID_C$)، قیمت کالا (Price) و نتیجه اعمال تابع درهم سازی بر روی سفارش خرید (OI) و عدد تصادفیِ HI ایجاد کرده، با کلید خصوصی خود امضا می نماید. امضای این اقلام اثبات می کند که فروشنده انجام تراکنش مزبور را پذیرفته است. فروشنده این پیام امضا شده را همراه با گواهینامه دیجیتالی خود برای مشتری ارسال می کند:

٤- Merchant → Customer :

$\{Tid, ID_M, ID_A, ID_C, Price, h(OI, HI)\}Sign_M , Cert_M$

### ۳-۱-۵- درخواست پرداخت

در این مرحله مشتری باید درخواست پرداخت وجه به فروشنده را تولید و امضا کرده و برای بانک خود ارسال نماید. این درخواست شامل شناسه تراکنش (Tid)، شناسه فروشنده ($ID_M$)، شناسه بانک فروشنده ($ID_A$)، شناسه مشتری ($ID_C$)، قیمت کالا (Price) ، مقدار h(OI,HI)، عدد تصادفی NONCE و نتیجه اعمال تابع درهم سازی بر روی رمز مخفی $K_A$ و NONCE ($h(Nonce, K_A)$) می‌باشد. مشتری این پیام را امضا نموده و به همراه قرارداد امضا شده توسط فروشنده و گواهینامه فروشنده برای بانک خود ارسال می کند.

٥- Customer → Customer's Bank :

$\{Tid, ID_M, ID_A, ID_C, Price, h(OI, HI)\}Sign_M , Cert_M,$
$\{Tid, ID_M, ID_A, ID_C, Price, h(OI, HI), NONCE,$
$h(Nonce, K_A)\}Sign_C$

### ۳-۱-۶- تایید پرداخت و مبادله مالی

بانک مشتری، امضای فروشنده را بوسیله کلید عمومی موجود در گواهینامه اش تایید اعتبار و فروشنده را احراز هویت می نماید. سپس مقدار h(OI, HI) که توسط فروشنده امضا شده و (OI, HI) که توسط مشتری امضا شده را با یکدیگر مقایسه می کند تا مطمئن شود این دو مقدار برابرند و مشتری و فروشنده روی لیست کالاهای خرید توافق دارند. از آنجا که مشتری دارای گواهینامه ای است که هویت واقعی او را نشان نمی دهد، برای تایید امضای مشتری با توجه به $ID_C$ موجود در پیام، بانک کلید عمومی مربوط به $ID_C$ مزبور را از بانک اطلاعاتی خود استخراج نموده و امضای $sign_C$ را تایید اعتبار می نماید. همچنین بانک، مقدار $h(Nonce, K_A)$ را محاسبه نموده و با مقدار $h(Nonce, K_A)$ که مشتری ارسال نموده مقایسه می کند تا مطمئن شود برابر هستند. از آنجا که فقط مشتری از رمز $K_A$ مطلع است، فرد دیگری جز او نمی توانسته $h(Nonce,K_A)$ را تولید کرده باشد. در صورت عدم وجود مشکل، بانک خریدار مبلغ کالاها را از حساب مشتری کم کرده و درخواست واریز به حساب فروشنده را به بانک فروشنده ارائه می نماید.

٦ - Customer's Bank → Merchant's Bank:
Notification of payment

### ۳-۱-۷- ارسال رسید پرداخت به مشتری

بانک خریدار رسید امضا شده ای برای خریدار ارسال می نماید.

۷ - Customer's Bank → Customer :
$\{Tid, ID_M, ID_C, Price, h(OI, HI)\}sign_I$

### ۳-۱-۸- ارسال تاییدیه پرداخت به فروشنده

بانک فروشنده، مبلغ را به حساب فروشنده واریز نموده و تاییدیه امضا شده را برای فروشنده می فرستد.

۸ - Merchant's Bank → Merchant
$\{Tid, ID_M , ID_C , Price, h(OI, HI)\}sign_A$

### ۳-۱-۹- تحویل کلید رمزگشایی کالا

فروشنده با دریافت تاییدیه دریافت وجه از بانک خود، باید کلید رمزگشایی کالا را برای مشتری ارسال نماید.

۹ - Merchant → Customer : k

### ۳-۱-۱۰- تحویل رسید دریافت کالا

مشتری با در اختیار گرفتن K، کالای رمز شده ارسالی توسط فروشنده را رمزگشایی نموده، کالای مورد نظر (m) را به دست می آورد. چنانچه فروشنده کلید درستی را ارسال نموده و مشتری کالای خود را به دست آورد، مشتری باید رسید امضا شده دریافت کالا را برای فروشنده ارسال نماید.

۱۰ - Customer → Merchant:
$\{Tid, ID_M, ID_C, Price, OI\}Sign_C$

## ۴- تحلیل ویژگی‌های امنیتی پروتکل FAPSWPP

در این قسمت ویژگی‌های امنیتی مختلف این پروتکل مورد بررسی قرار می گیرد، سپس نشان داده می شود که چنانچه یکی از طرفین تعهدات خود را به درستی انجام ندهد، چگونه پروتکل پیشنهادی مانع نقض حقوق طرف مقابل خواهد شد.

### ۴-۱- محرمانگی

محرمانگی اطلاعات و امنیت ابتدا به انتها با ترکیب TLS/SSL و WTLS فراهم می شود. با قرار دادن دروازه WAP[۱۷] در داخل شبکه خصوصی، مشکل WAP gap نیز حل می شود.

### ۴-۲- جامعیت داده‌های ارسالی

جامعیت داده‌های ارسالی توسط مکانیزم WTLS تامین می گردد. استفاده از امضای دیجیتال نیز جامعیت داده‌های امضا شده را تضمین می نماید.

### ۴-۳- احراز هویت

در پروتکل پیشنهادی مشتری به واسطه وجود گواهینامه دیجیتالی و با انجام امضای دیجیتالی به بانک خود احراز هویت می گردد، هرچند هویت واقعی وی به دلیل استفاده از نام مستعار در گواهینامه و حساب بانکی وی فاش نمی شود. مشتری گواهینامه با نام مستعار و گواهینامه CEMBS خود را برای فروشنده نیز ارسال می کند. فروشنده از طریق این گواهینامه اطمینان می یابد که با مشتری مزبور در حال انجام تراکنش می باشد، هرچند هویت واقعی وی را نمی تواند احراز نماید. احراز هویت فروشنده به مشتری نیز توسط مکانیزم WTLS انجام می‌شود.

### ۴-۴- حفظ حریم خصوصی

به منظور حفظ حریم خصوصی افراد، هر نقشی فقط در حد نیاز باید به اطلاعات دسترسی داشته باشد. به عنوان مثال فروشنده و مشتری نباید به اطلاعات بانکی یکدیگر دست یابند. لیست کالاهای خرید مشتری نیز نباید در اختیار بانک قرار گیرد. به این منظور در مرحله اول پروتکل، مشتری یک عدد تصادفی HI را تولید کرده و برای فروشنده ارسال می نماید که به منظور پنهان کردن لیست کالاهای خریداری شده مشتری از چشم بانک استفاده می شود. بانک نتیجه تابع درهم سازی h(OI,HI) را مشاهده می کند که به دلیل یکطرفه بودن توابع درهم سازی، قادر به استخراج OI نخواهد بود.

از آنجا که مشتری از طریق بانک خود اقدام به پرداخت می کند، نیازی نیست که اطلاعات بانکی خود را برای فروشنده ارسال نماید. فروشنده نیز اطلاعات بانکی خود را مبادله نمی کند، پس مشتری و فروشنده به اطلاعات بانکی یکدیگر دسترسی نداشته و حریم خصوصی آنها محفوظ می ماند.

### ۴-۵- انکارناپذیری قبول تراکنش توسط فروشنده

در مرحله چهارم فروشنده با ارزیابی $C_T$ دریافت شده از مشتری اطمینان می یابد که $C_T$ حاوی رسید امضا شده مشتری می باشد. سپس فروشنده شناسه تراکنش (Tid) را به همراه شناسه خود ($ID_M$)، شناسه بانک خود ($ID_A$)، شناسه مشتری ($ID_C$) ، قیمت کالا (Price) و نتیجه تابع درهم سازی بر روی مقادیر OI و HI با کلید خصوصی خود امضا کرده و برای مشتری ارسال می نماید. امضای این اقلام مانع از امکان تغییر داده‌ها شده و جامعیت پیام را تامین می کند. فروشنده نیز دیگر قادر به انکار پذیرفتن درخواست خرید مشتری نخواهد بود.

### ۴-۶- انکارناپذیری قبول پرداخت وجه توسط مشتری

در مرحله پنجم مشتری پس از دریافت پاسخ فروشنده، این پاسخ امضا شده و گواهینامه فروشنده را به همراه پیام امضا شده خود برای بانک خویش ارسال می‌نماید. در این مرحله مشتری باید شناسه تراکنش (Tid) را به همراه شناسه فروشنده ($ID_M$)، شناسه بانک فروشنده ($ID_A$)، شناسه مشتری ($ID_C$) ، قیمت کالا (Price) ، نتیجه تابع درهم سازی بر روی مقادیر OI و HI ، مقدار تصادفی NONCE و نتیجه تابع درهم سازی بر روی مقدار NONCE و رمز مخفی $k_A$ را با کلید خصوصی خود امضا نموده و برای بانک خود ارسال نماید. با این عمل امضا مشتری دیگر قادر به انکار سفارش پرداخت وجه به فروشنده نیست.

### ۴-۷- انکار ناپذیری دریافت وجه توسط فروشنده

در مراحل ۷ و ۸ رسیدهای امضا شده به فروشنده و مشتری از طریق بانک ارسال می گردد که انکارناپذیری پرداخت وجه توسط مشتری را فراهم می کند.

### ۴-۸- گمنامی مشتری

در این پروتکل هویت واقعی مشتری به دلیل استفاده از نام مستعار در گواهینامه و حساب بانکی وی فاش نمی گردد.

### ۴-۹- نقض تبادل منصفانه توسط فروشنده

در ۳ حالت فروشنده ممکن است خلافکار باشد:

- فروشنده در مرحله هشتم تاییدیه دریافت وجه را از بانک خود دریافت کند، اما کلید رمزگشایی نادرستی را برای مشتری ارسال نماید.
- فروشنده در مرحله هشتم تاییدیه دریافت وجه را از بانک خود دریافت کند اما بدون ارسال کلید رمزگشایی کالا برای مشتری تراکنش را خاتمه دهد.
- فروشنده ممکن است ادعا کند کلید رمزگشایی را به این دلیل ارسال ننموده که مشتری پرداخت را انجام نداده است.

چنانچه هریک از موارد فوق رخ دهد، مشتری باید دادخواست خود را به همراه قرارداد امضا شده فروشنده که در مرحله چهارم دریافت کرده بود، همچنین رسید پرداخت وجه که در مرحله هفتم از بانک خود دریافت کرده و نیز رسید امضا شده دریافت کالا (Signed_Receipt) به همراه مقادیر OI و HI برای شخص ثالث مورد اعتماد ارسال نماید. شخص ثالث از فروشنده رسید تحویل کالا را درخواست می کند. چنانچه فروشنده رسید امضا شده توسط مشتری را به شخص ثالث ارائه نماید، شخص ثالث مطمئن می شود که فروشنده کلید رمزگشایی درست را به مشتری تحویل داده و از وی رسید

تحویل کالا را دریافت کرده است. بنابراین دادخواست مشتری معتبر نبوده و رد خواهد شد. در غیر این صورت شخص ثالث امضای فروشنده بر روی قرارداد امضا شده را تایید اعتبار می کند، سپس با استفاده از OI و HI مقدار h(OI, HI) را بازتولید نموده و با مقدار h(OI, HI) موجود در قرارداد امضا شده فروشنده مقایسه می کند تا مطمئن شود فروشنده سفارش OI را پذیرفته است. شخص ثالث رسید پرداخت امضا شده توسط بانک را نیز تایید اعتبار می کند تا مطمئن شود مشتری وجه کالا را پرداخت کرده است. سپس کلید رمزگشایی کالای مزبور (k) را برای مشتری و رسید دریافت کالای امضا شده توسط مشتری را برای فروشنده ارسال می کند. بنابراین مشتری کلید رمزگشایی و فروشنده نیز رسید تحویل کالا را دریافت می کند.

## ۴-۱۰- نقض تبادل منصفانه توسط مشتری

مشتری ممکن است در مرحله نهم کلید رمزگشایی کالا را از فروشنده دریافت کند، اما در عوض رسید امضا شده دریافت کالا را به فروشنده ارائه ننماید. در این حالت فروشنده دادخواست خود را همراه با مقدار $C_T$ دریافت شده از مشتری و مقادیر OI و HI برای شخص ثالث ارسال می کند. شخص ثالث $C_T$ را با کلید خصوصی خود رمزگشایی کرده و رسید امضا شده مشتری را به دست می‌آورد. سپس باید مقدار h(OI, HI) را بازتولید کند تا مطمئن شود فروشنده و مشتری بر روی کالای واحدی توافق کرده اند. نهایتا شخص ثالث رسید امضا شده مشتری را برای فروشنده و کلید رمزگشایی کالای مزبور را نیز برای مشتری ارسال می نماید.

# ۵- مقایسه و جمع بندی

## ۵-۱- مقایسه ویژگی‌های امنیتی

از بین پروتکلهای خرید کالای الکترونیکی، دو پروتکل Lee's et al و NetBill ویژگیهای امنیتی بیشتر و کارایی مطلوب تری را فراهم کرده اند. در جدول (۲) پروتکل FAPSWPP از لحاظ ویژگی‌های امنیتی با این دو پروتکل مقایسه شده است. با توجه به جدول (۲) مشاهده می شود که پروتکل توسعه یافته FAPSWPP علاوه بر تامین کلیه ویژگی‌های امنیتی مورد نیاز یک سیستم پرداخت الکترونیکی، ویژگی تبادل منصفانه که مورد نیاز یک سیستم خرید امن کالای الکترونیکی می باشد را نیز فراهم آورده است.

**جدول (۲): مقایسه ویژگی‌های امنیتی پروتکل‌های خرید**

| پروتکل / ویژگی امنیتی | NetBill | Lee's | FAPSWPP |
|---|---|---|---|
| محرمانگی | بله | بله | بله |
| احراز هویت | بله | بله | بله |
| جامعیت داده | بله | بله | بله |
| انکارناپذیری قبول تراکنش توسط فروشنده | بله | - | بله |
| انکارناپذیری قبول پرداخت وجه توسط مشتری | بله | - | بله |
| انکار ناپذیری دریافت وجه توسط فروشنده | - | بله | بله |
| حفظ حریم خصوصی | - | بله | بله |
| گمنامی مشتری | - | - | بله |
| اطمینان مشتری از دریافت کالا در ازای پرداخت وجه | بله | - | بله |
| اطمینان فروشنده از دریافت وجه در ازای تحویل کالا | بله | بله | بله |
| اطمینان فروشنده از دریافت رسید تحویل کالا | - | - | بله |

## ۵-۲- مقایسه کارایی

معیارهایی که در کارایی یک پروتکل موثر است عبارتند از: تعداد پیام‌های مبادله شونده توسط هریک از نقش‌های درگیر، تعداد عملیات رمزنگاری انجام شده و پهنای باند مورد نیاز که به تعداد و اندازه پیام‌ها بستگی دارد.

در جدول (۳) ویژگی‌های کارایی پروتکل FAPSWPP با دو پروتکل خرید NetBill و Lee's et al مقایسه شده است. با توجه به این جدول مشاهده می‌شود که کلیه محاسبات انجام شده به جز تعداد عملیات درهمسازی در پروتکل پیشنهادی FAPSWPP نسبت به NetBill کاهش یافته که باعث می شود کارایی بسیار بهتری نسبت به NetBill داشته باشد. تعداد عملیات محاسباتی سنگین رمزنگاری کلید نامتقارن نیز در پروتکل FAPSWPP نسبت به پروتکل Lee's et al کاهش چشمگیری دارد که در مجموع باعث بهبود کارایی نسبت به پروتکل Lee's et al می شود.

**جدول (۳) مقایسه ویژگی‌های کارایی پروتکل‌های خرید**

| پروتکل / عملیات | NetBill | Lee's et al | FAPSWPP |
|---|---|---|---|
| رمزنگاری/ رمزگشایی نامتقارن | ۶ | ۸ | ۱ |
| امضا / تایید امضای دیجیتال | ۱۳ | ۹ | ۱۰ |
| رمزنگاری/ رمزگشایی متقارن | ۲۸ | ۲ | ۲ |
| عملیات تابع درهمسازی | ۲ | ۹ | ۴ |
| سربار ارتباطی (تعداد پیام‌های تبادلی) | ۱۵ | ۹ | ۱۰ |

# ۶- نتیجه گیری

در این مقاله پروتکل پرداخت امن APSWPP جهت تامین ویژگی تبادل منصفانه توسعه داده شد است. در پروتکل توسعه یافته که FAPSWPP نامیده شده، در هر تراکنش مشتری مطمئن است که در ازای پرداخت وجه حتما کالای مورد نظر خود را دریافت خواهد کرد. فروشنده نیز اطمینان دارد که در قبال تحویل کالا، وجه مورد نظر و رسید تحویل کالا را دریافت می کند. همچنین هیچیک از طرفین قادر به انکار دریافت عنصر مورد نظر خود نیستند. در این پروتکل از روش تبادل خوشبینانه استفاده شده است. گواهینامه CEMBS نیز جهت مبادله اطلاعات محرمانه و امضای روی آن به صورت منصفانه، به منظور اطمینان فروشنده از دریافت رسید تحویل کالا به کار رفته است.

پروتکل پیشنهای از لحاظ معیارهای امنیتی و کارایی مورد ارزیابی و مقایسه با دو پروتکل خرید NetBill و Lee's et al قرار گرفته و نشان داده شدکه در پروتکل FAPSWPP علاوه بر بهبود کارایی، ویژگی‌های امنیتی کاملا برآورده شده است.

# مراجع

[۱] لایقیان جوان، سمانه، قائمی بافقی، عباس، مینایی، بهروز، **یک پروتکل پرداخت گمنام و خصوصی مبتنی بر SWPP**، کنفرانس سالانه کامپیوتر، دوره پانزدهم، تهران، زمستان ۱۳۸۸.

[۲] Chaum, david, fiat, amos., *"untraceable electronic cash"*, Center for mathematics and computer science, (۲۰۰۰).

[۳] Financial Crimes Enforcment., *"A Survey of Electronic Cash"*, Electronic Banking and Internet Gaming, US Department of Treasury, (۲۰۰۰).

[٤] Pasupathinathan, Vijayakrishnan, Pieprzyk, Josef, Wang, Huaxiong., *"Privacy Enhanced Electronic Cheque System"*, Seventh IEEE International Conference on E-Commerce Technology, ۲۰۰۵.

[٥] Neuman, Clifford, Medvinsky, Gennady., *"Requirements for Network Payment: The NetChequeTM Perspective"*, Information Sciences Institute University of Southern California, ۲۰۰۴.

[٦] Puhrerfellner, Michael., *An implementation of the Millicent micro-payment protocol and its application in a pay-per-view business model*, Master's Thesis, university wien, December ۲۰۰۰.

[۷] Hwang, Min-Shiang, Pei-Chen, Sung., *"A Study of Micro-payment Based on One-Way Hash Chain"*, International Journal of Network Security, No.۲, Mar. (۲۰۰۶).

[۸] MasterCard and VISA Corporations, *Secure Electronic Transaction (SET) Specification.Book ۳: Formal Protocol Definition*, Version ۱.۰, May ۱۹۹۷.

[۹] Cox, Benjamin, Tygar, J, Sirbu, Marvin., *"NetBill Security and Transaction Protocol"*, In Proceedings Of The ۱st USENIX Workshop In Electronic Commerce, July ۱۹۹۵.

[۱۰] Lee, Manho, Kim, Kwangjo., *"A Micro-payment System for Multiple-Shopping"*, SCIS, ۲۰۰۲.

[۱۱] Bahreman, A, Tygar, I., *"Certified Electronic Mail"*, In Proceeding of the Internrt Society Symposion on Network and Distributed System Security, February ۱۹۹۴.

[۱۲] Franklin, Matthew, Reiter, Michael., *"Fair Exchange With A Semi-Trusted Third Party"*, Proceeding Of The ۴th ACM Conference On Computer And Communications Security, April ۱۹۹۷.

[۱۳] Bao, Feng; Deng, Robert, Mao, Wenbo., *"Efficient And Practical Fair Exchange Protocols With Offline TTP"*, In Proceeding Of The IEEE Symposium On Security And Privacy, Mat ۱۹۹۸.

[۱٤] Asokan, N, schunter, M, waidner, S., *"optimistic protocol for fair exchange"*, In t. Matsumoto Editor, Proceeding Of The ۴th ACM Conference On Computer And Communications Security, April ۱۹۹۷.

[۱٥] Mao, Wenbo., *"Verifiable escrowed signature"*, Springer-Verlag, ۱۹۹۷.

## زیرنویس‌ها

* confidentiality
۲ authentication
۳ Non Repudiation
٤ integrity
٥ authorization
٦ privacy
۷ anonymity
۸ Fair Exchange
۹ Optimistic Exchange Protocol
۱۰ Anonymous and Private Secure Wireless Payment Protocol
۱۱ Fair Anonymous and Private Secure Wireless Payment Protocol
۱۲ Certificate of Encrypted Message Being a Signature
۱۳ Secure Wireless Payment Protocol
۱٤ Blindly Signed Pseudo Digital Certificate
۱٥ Trusted Third Party
۱٦ Wireless Transport Layer Security
۱۷ Wireless Application Protocol