پروتکلی کارامد مبتنی بر رمزنگاری منحنی بیضوی برای ارتباط امن کاربران با خدمات‌دهنده

مهدی نیکوقدم[۱]
دانشکده مهندسی، دانشگاه فردوسی مشهد
مشهد، ایران
mahdi.nikooghadam@um.ac.ir
شماره تلفن: ۰۵۱۳۸۸۰۵۴۳۶

هاله امین طوسی[۲]
[۲]دانشکده مهندسی، دانشگاه فردوسی مشهد
مشهد، ایران
amintoosi@um.ac.ir
شماره تلفن: ۰۵۱۳۸۸۰۵۴۳۶

چکیده — در حال حاضر استفاده گسترده از فضای اینترنت و ارتباطات کاربر/خدمات‌دهنده، بستر خوبی برای حمله مهاجمین و شنود و دزدیدن اطلاعات حیاتی ایجاد کرده است. در پروتکل‌های برقراری نشست، کاربر درخواستی را برای خدمات‌دهنده ارسال کرده و خدمات‌دهنده به آن پیام پاسخ خواهد داد. پس از انجام احراز هویت دو طرفه، کلید نشست امن بین آن‌ها ایجاد خواهد شد و از این پس، ارتباط آن‌ها از طریق همین کلید نشست انجام خواهد گردید. نیکوقدم و همکاران در سال ۲۰۱۶ پروتکلی ارائه کرده‌اند و ادعا نموده اند که پروتکل پیشنهادی آنها در مقابل انواع مختلف حملات مقاوم است. در این مقاله، نشان خواهیم داد که روش نیکوقدم و همکاران نیاز امنیتی محرمانگی رو به جلو را تامین نخواهد کرد و امکان حدس رمزعبور کاربر وجود دارد. همچنین در این مقاله، یک پروتکل قوی و کارآمد برای احرازهویت و توافق کلید برای ارتباط امن کاربران با خدمات دهنده ارائه خواهیم داد. صحت پروتکل ارائه شده توسط ابزار Scyther به اثبات رسیده است. تحلیل امنیتی انجام شده برروی پروتکل نیز نشان میدهد که پروتکل ارائه شده در مقابل بسیاری از حملات مقاوم بوده و نیاز امنیتی محرمانگی رو به جلو را نیز تامین می نماید.

کلید واژه — احراز هویت دو طرفه، پروتکل برقراری نشست، کلید نشست، محرمانگی رو به جلو.

۱. مقدمه

در حال حاضر، با رشد چشم‌گیر فناوری اطلاعات و رفتن به سوی هوشمند سازی شهرها و خانه‌های هوشمند یکی از نگرانی‌های عمده به خصوص در حوزه اینترنت اشیاء، بحث پروتکل‌های احراز هویت و امنیت اطلاعات ارسال شده بین خدمات‌دهنده و کاربران است. در حوزه پروتکل‌های برقراری نشست، پژوهش‌های زیادی بر پایه تبادل کارت هوشمند بین خدمات دهنده و کاربر مطرح شده است. در سال ۲۰۱۲ هسیه و لی[۱] یک پروتکل احراز هویت پیشنهاد دادند با این حال وانگ و همکاران [۲] نشان دادند که پروتکل هسیه و لی در برابر حمله حدس رمز عبور کاربر مقاوم نیست و سپس آن‌ها یک پروتکل بهبودیافته ارائه دادند و ادعا کردند که می‌تواند در برابر حملات مختلف مقاوم باشد. سپس چانگ و همکاران[۳] ادعا کردند که در [۲] حریم خصوصی کاربران حفظ نمی‌شود، زیرا کاربر از همان شناسه اولیه برای تمامی نشست‌ها استفاده می‌کند. همچنین یک پروتکل بهبود یافته ارائه دادند و ادعا کردند که از حملات مختلف جلوگیری می‌کند و همچنین حریم خصوصی کاربر حفظ می‌شود. با این حال کوماری و همکاران[۴] نشان دادند که طرح پیشنهاد شده در[۳] امکان حدس رمزعبور کاربر و همچنین حمله جعل هویت را برای مهاجم فراهم می‌کند، همچنین یک پروتکل احراز هویت پیشنهاد دادند و ادعا کردند که سطح قابل قبولی از امنیت را فراهم می‌کند. سپس داس و گواسوامی [۵] طرح احراز هویت کاربر مبتنی بر بیومتریک که ویژگی گمنامی کاربر و نیز ویژگی‌های قوی دیگری نیز برای تایید اعتبار کاربر نهایی داشت را پیشنهاد دادند. بعد از مدتی، میشرا و همکاران [۶] طرحی برای احراز هویت دوطرفه بر پایه بیومتریک ارائه دادند که دارای فاز تغییر رمزعبور بود. همچنین در سال ۲۰۱۶ نیکوقدم و ارشد [۷] پروتکلی برای احرازهویت و توافق کلید با هدف تامین گمنامی کاربر ارائه کرده‌اند. در این مقاله اثبات خواهیم کرد که مقاله نیکوقدم و همکاران [۷] برخی نیازهای امنیتی همانند محرمانگی رو به جلو را تامین نمی‌کند و درمقابل حمله حدس زدن رمز عبور نیز آسیب پذیر می‌باشد. در ادامه نیز، پروتکلی قوی و کارآمد برای ارتباط امن کاربر با خدمات‌دهنده ارائه خواهیم داد.

ادامه ساختار مقاله به شرح زیر است. بخش ۲ به بررسی روش نیکوقدم و همکاران می پردازد و آسیب های آن را شرح میدهد. در بخش ۳، پروتکل پیشنهادی به تفضیل شرح داده خواهد شد. بخش ۴ اختصاص به تحلیل امنیتی پروتکل ارائه شده دارد و صحت پروتکل را از طریق ابزار Scyther [۸] نیز نشان میدهد. در بخش ۵، جمع بندی مقاله ارائه خواهد شد.

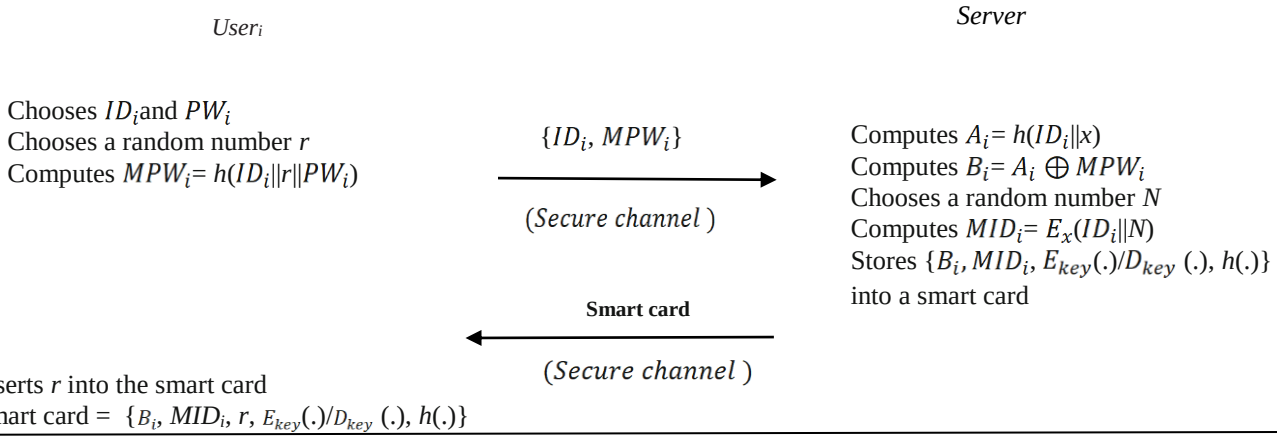
۲. بررسی روش نیکوقدم و همکاران

در این بخش، روش ارائه شده توسط نیکوقدم و همکاران [۷] بطور خلاصه ارائه شده و ضعف های امنیتی آن بیان می گردد.

جدول ۱: نمادهای بکار رفته در روش نیکوقدم و همکاران [۷]

تعریف	نماد
کاربر i	$\boldsymbol{U_i}$
خدمات‌دهنده	$\boldsymbol{S}$
شناسه‌ی کاربر i	$\boldsymbol{ID_i}$
رمز عبور کاربر i	$\boldsymbol{PW_i}$
کلید مخفی خدمات دهنده	$\boldsymbol{X}$
کلید جلسه	$\boldsymbol{SK}$
رمزنگاری و رمزگشایی متقارن با کلید مخفی k	$\boldsymbol{E_k(0)/D_k(0)}$
XOR	$\oplus$
عملیات الحاق	$\|$
تابع درهم‌ساز	$\boldsymbol{h(0)}$

جدول ۱ نمادهای بکاررفته در پروتکل ارائه شده در [۷] را نشان میدهد. شکل ۱ نیز مرحله ثبت نام در پروتکل ارائه شده در [۷] نشان میدهند.

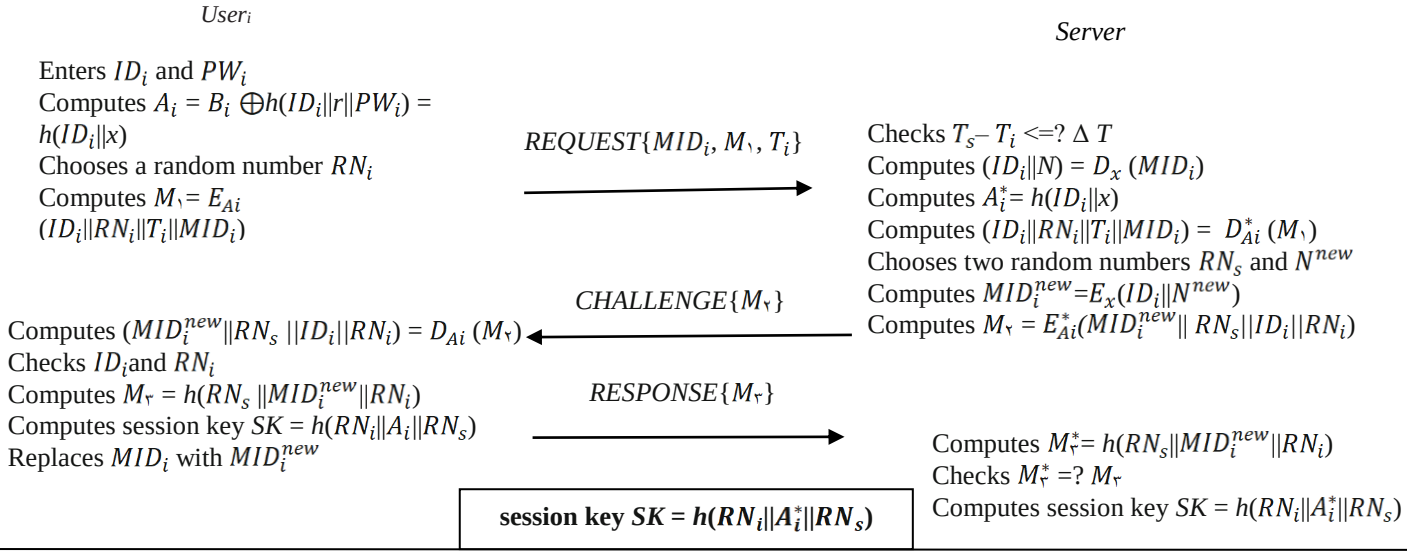


شکل۱: مرحله ثبت نام پروتکل پیشنهادی نیکوقدم و همکاران [۷]

در مرحله ثبت‌نام کاربر یک شناسه و یک رمزعبور و همچنین یک عدد تصادفی برای خود انتخاب کرده و $MPW_i = h(ID_i||r||PW_i)$را می‌سازد و پارامترهای $\{ID_i, MPW_i\}$ را از طریق کانال امن برای خدمات‌دهنده ارسال خواهد کرد. خدمات دهنده پارامترهایی که در زیر مشاهده می‌کنید را به دست می‌آورد.

Computes $A_i = h(ID_i||x)$
Computes $B_i = A_i \oplus MPW_i$
Chooses a random number N
Computes $MID_i = E_x(ID_i||N)$
Stores $\{B_i, MID_i, E_{key}(.)/D_{key}(.), h(.)\}$
into a smart card

در انتها، پارامترهای $\{B_i, MID_i, E_{key}(.)/D_{key}(.), h(.)\}$ را درون کارت هوشمند ذخیره کرده و کارت هوشمند را از طریق کانال امن برای کاربر ارسال می‌کند. کاربر نیز مقدار $\boldsymbol{r}$ را به کارت هوشمند اضافه می‌کند. در نهایت مقادیری که در کارت هوشمند ذخیره شده است عبارتند از $\{B_i, MID_i, r, E_{key}(.)/D_{key}(.), h(.)\}$



شکل۲: مرحله احراز هویت پروتکل نیکوقدم و همکاران [۷]

شکل ۲ مرحله احراز هویت در پروتکل ارائه شده در [۷] را نشان میدهد. در مرحله احراز هویت، ابتدا کاربر کارت هوشمند خود را درون کارت‌خوان وارد کرده و رمزعبور و شناسه انتخابی خود را وارد میکند. پس از بدست آوردن مقادیر زیر، کاربر پیغام $REQUEST\{MID_i, M_1, T_i\}$را برای خدمات دهنده ارسال می‌کند.

Enters ID_i and PW_i
Computes $A_i = B_i \oplus h(ID_i||r||PW_i) = h(ID_i||x)$
Chooses a random number RN_i
Computes $M_1 = E_{Ai}\ (ID_i||RN_i||T_i||MID_i)$

خدمات دهنده به محض دریافت پیغام $REQUEST\{MID_i, M_1, T_i\}$ابتدا از نظر زمانی آن را چک می‌کند که پیغام تازه باشد و سپس به علت اینکه MID_i با کلید مخفی خودش رمز شده آن را رمزگشایی‌می‌کند و پارامتر$A_i^* = h(ID_i||x)$ را به دست می‌آورد و حال چون A_i^* را دارد، پارامتر M_1 را رمزگشایی می‌کند. اگر رمزگشایی به درستی انجام شود در واقع با این کار، کاربر نیز احراز هویت شده است. بعد از به دست آوردن پارامترهایی که در ادامه مشاهده میشود، در نهایت پیغام $CHALLENGE\{M_2\}$ را برای کاربر ارسال خواهد کرد.

Checks $T_s - T_i <=? \Delta T$
Computes $(ID_i||N) = D_x\ (MID_i)$
Computes $A_i^* = h(ID_i||x)$
Computes $(ID_i||RN_i||T_i||MID_i) = D_{Ai}^*\ (M_1)$
Chooses two random numbers RN_s and N^{new}
Computes $MID_i^{new} = E_x(ID_i||N^{new})$
Computes $M_2 = E_{Ai}^*(MID_i^{new}||\ RN_s||ID_i||RN_i)$

حال کاربر چون مقدار A_i را دارد میتواند M_2 را رمزگشایی کند و با پارامترهای به دست آمده از رمزگشایی M_2 از طریق ID_i وRN_i خدمات دهنده را احراز هویت خواهد کرد و M_3 و کلید نشست را خواهد ساخت. در ادامه، چگونگی ساخت این پارامترها مشخص شده است. در نهایت پیغام $RESPONSE\{M_3\}$را برای خدمات دهنده ارسال می‌کند.

Computes $(MID_i^{new}||RN_s\ ||ID_i||RN_i) = D_{Ai}\ (M_2)$
Checks $ID_i$and RN_i
Computes $M_3 = h(RN_s\ ||MID_i^{new}||RN_i)$
Computes session key $SK = h(RN_i||A_i||RN_s)$

خدمات دهنده هم بعد از احراز هویت کاربر از طریق M_3 کلید نشست را می‌سازد و در نهایت کلید نشست نهایی بین طرفین ارتباط یعنی خدمات‌دهنده و کاربر قطعی می‌شود.

Computes $M_3^* = h(RN_s||MID_i^{new}||RN_i)$
Checks $M_3^* =? M_3$
Computes session key $SK = h(RN_i||A_i^*||RN_s)$

در ادامه، ضعف های امنیتی موجود در پروتکل نیکوقدم و همکاران [۷] شرح داده میشود.

عدم تامین محرمانگی رو به جلو: نیاز امنیتی محرمانگی روبه جلو بیان می‌کند که حتی اگر کلید مخفی خدمات‌دهنده به هر دلیلی به دست متخاصم بیفتد، متخاصم نباید بتواند به کلید نشست دست یابد. در پروتکل ارائه شده در [۷]، اگر فرض کنیم که x که کلید مخفی خدمات دهنده است به دست مهاجم بیفتد، از آنجایی که در قسمت احراز هویت تمامی پیام‌ها بر روی کانال عمومی رد و بدل می‌شود مهاجم میتواند MID_i را از کانال عمومی بردارد و با داشتن x و با رمزگشایی کردن MID_i دررابطه $MID_i= E_x(ID_i||N)$ مقادیر ID_i و N را بدست آورد. از طرفی چون هم x و هم ID_i را دارد، با استفاده از رابطه $A_i^* = \mathrm{h}(ID_i \,||\, \mathrm{x})$ مقدار A_i^* که برابر با همان A_i را بدست خواهد آورد. حال با داشتن A_i و با رمزگشایی $M_۲$ در رابطه $M_۲= E_{Ai}^*(MID_i^{new}||\ RN_s||ID_i||RN_i)$ می‌تواند مقادیر RN_i و RN_s را بدست آورد و به این شکل می‌تواند به کلید نشست دست پیدا کند.

آسیب پذیری درمقابل حمله حدس رمزعبور کاربر: در حمله فوق مشخص شد که اگر کلید محرمانه خدمات دهنده لو برود، مهاجم میتواند مقادیر ID_i و در نتیجه A_i را بدست آورد. از طرفی اگر مهاجم به کارت هوشمند به هر طریقی مثل گم شدن کارت هوشمند یا حمله فیزیکی دست پیدا کند میتواند به مقادیر حساسی که درون آن است یعنی B_i ،$MIDi,\ r$ دسترسی داشته باشد. حال چون xor برگشت پذیر است پس از رابطه $B_i = A_i \oplus MPW_i$ میتواند مقدار MPW_i را بدست آورد و از طرفی چون از رابطه $MPW_i = h(ID_i||r||PW_i)$ تمامی مقادیر به جز رمزعبور را دارد و به علت اینکه معمولا رمزعبور تعداد بیت زیادی ندارد میتواند با آزمون و خطا و حمله دیکشنری، رمزعبور کاربر را بدست آورد.

در ادامه، به منظور رفع آسیب پذیریهای فوق، پروتکل پیشنهادی در این مقاله به تفضیل، معرفی می گردد.

۳. پروتکل پیشنهادی با استفاده از رمزنگاری منحنی بیضوی

پروتکل پیشنهادی ارائه شده در این مقاله، شامل سه مرحله ثبت نام، احراز هویت و تغییر رمز عبور است که هر یک در ادامه به طور کامل شرح داده خواهد شد. در ابتدا، در جدول ۲، نمادهای بکاررفته در الگوریتم پیشنهادی معرفی می گردد. سپس، مراحل سه گانه الگوریتم پیشنهادی بیان خواهند شد.

جدول ۲: نمادهای بکار رفته در پروتکل پیشنهادی

تعریف	نماد
کاربر i	U_i
خدمات‌دهنده	S
شناسه‌ی کاربر i	ID_i
رمز عبور کاربر i	PW_i
کلید محرمانه خدمات دهنده	d_s
کلید عمومی خدمات دهنده	D_s=d_s.P
نقطه‌ی اساسی روی منحنی بیضوی E	P
اعداد تصادفی	r, b_i, a_i, t, c_i
کلید نشست	SK
رمزنگاری و رمزگشایی متقارن با کلید مخفی k	$E_k(\cdot)/\ D_k(\cdot)$
XOR	$\oplus$
عملیات الحاق	$\|\|$
مهر زمانی خدمات‌دهنده و کاربر	T_s, T_e
تابع درهم‌ساز	$h(\cdot)$

A. مرحله‌ی ثبت‌نام

همانگونه که در شکل ۳ نشان داده شده است، کاربر و خدمات‌دهنده در یک ملاقات حضوری گام‌های زیر را انجام داده و در پایان این مرحله، خدمات‌دهنده کارت هوشمند را به کاربر ارائه می‌دهد.

گام اول: در ابتدا کاربر برای خود یک شناسه و رمز عبور و دو عدد تصادفی b_i و a_i را انتخاب نموده و با توجه به این پارامترها، مقادیر PW_u و AB_i و W_i را با توجه به روابط زیر محاسبه می‌کند.

$$PW_u = \mathrm{h}(PW_i||a_i||ID_i) \oplus PW_i$$
$$W_i = h(ID_i||\ PW_u||a_i)$$
$$AB_i = a_i \oplus b_i$$

سپس کاربر از طریق کانال امن، پارامترهای $\{ID_i,\ W_i,\ AB_i, a_i, PW_u\}$ را برای خدمات‌دهنده ارسال می‌کند.

گام دوم: خدمات دهنده پس از دریافت پارامترهای $ID_i,\ W_i,\ AB_i, a_i, PW_u$، پارامتر HID_i را محاسبه کرده، عدد تصادفی c_i را انتخاب میکند و سپس به کمک آن‌ها، روابط زیر را محاسبه می‌کند.

$$HID_i = \mathrm{h}(ID_i||\ AB_i) \oplus ID_i$$
Choose random number c_i
$$HID_i = \mathrm{h}(ID_i||\ AB_i) \oplus ID_i$$
Choose random number c_i
$$M_i = h(d_s||c_i)$$
$$C_i = M_i \oplus PW_u$$
$$W_i^{new} = (HID_i||\ PW_u||\ a_i)$$
$$MID_i = E_{ds}\,(HID_i, W_i^{new},\ AB_i, M_i)$$
Store in smart card
$$\{D_s,\ W_i^{new}, MID_i,\ HID_i, C_i, E_{key}(.)/\ D_{key}(.), h(.)\}$$

سپس خدمات دهنده پارامترهای زیر را درون کارت هوشمند قرار داده و از طریق کانال امن برای کاربر می‌فرستد.

$$D_s,\ W_i^{new}, MID_i,\ HID_i, C_i, E_{key}(.)/\ D_{key}(.), h(.)$$

گام سوم: با دریافت کارت هوشمند توسط کاربر پارامتر D_s و HID_i را حذف نموده و پارامترهای a_i را در کارت ذخیره می‌کند. در نهایت کارت هوشمند شامل مقادیر

$$D_s,\ W_i^{new},\ a_i, MID_i,\ HID_i, C_i, E_{key}(.)/\ D_{key}(.), h(.)$$

می‌باشد.

B. *مرحله ی احراز هویت*

شکل ۴ ، مراحل احراز هویت در پروتکل پیشنهادی را نشان میدهد. گامهای این پروتکل به شرح زیر هستند.

گام اول: در ابتدا کاربر کارت هوشمند خود را وارد دستگاه کارت‌خوان کرده و سپس شناسه و رمز عبور خود را وارد می‌کند. سپس محاسبات زیر توسط کارت هوشمند انجام می‌شود.

Inserts smart card

Enters HID_i and pw_i

$$PW_u^* = h(PW_i^* || a_i || HID_i^*) \oplus PW_i^*$$

$$W_i^{new*} = h(HID_i^* || PW_u^* || a_i)$$

$$W_i^{new} =? W_i^{new*}$$

Choose time stamp T_s

Choose $r \epsilon Zn$ $R=r.p$

$$key_1 = r.D_s$$

$$MP = E_{key_1}(MID_i || HID_i || W_i^{new} || a_i)$$

و سپس پیغام $\{MP,\ MID_i, R,\ T_s\}$ REQUEST را از طریق کانال عمومی برای خدمات‌دهنده ارسال می‌نماید.

گام دوم: به محض دریافت پیام REQUEST $\{MP,\ MID_i, R,\ T_s\}$ توسط خدمات‌دهنده، تازگی پیام با بررسی تساوی $|T_e - T_s| \le \Delta T$ مورد بررسی قرار می‌گیرد. در صورت تازگی پیام ارسالی، خدمات‌دهنده پارامتر $key_1' = d_s.R$ را با کلید مخفی خود یعنی d_s میسازد و از آنجایی که $key_1' = key_1$ میتواند مقدار MP را بااستفاده از آن رمزگشایی کند و پارامترهای a_i^*وW_i^{new*}وHID_i^*وMID_i^* را بدست آورد. حال با مقایسه $\boldsymbol{T_s^*} =? \boldsymbol{T_s}$ و همچنین مقایسه $W_i^{new*} = ?W_i^{new**}$ هویت کاربر را بررسی میکند، اگر هویت تایید شد پارامترهای زیر را به دست می‌آورد. در نهایت پیام CHALLENGE $\{T, F\}$ ارسال می‌گردد.

$$b_i = AB_i \oplus a_i$$

Choose $t \epsilon Zn$ $T=t.p$

$$key_2' = t.R$$

$$SK=h(b_i || M_i || W_i^{new} || key_2 || key_1')$$

$$F = E_{key_2}(b_i || W_i^{new} || HID_i)$$

گام سوم: بعد از دریافت پیام CHALLENGE توسط کاربر، ابتدا کاربر مقدار key_2' را با استفاده از رابطه $key_2' = r.T$ می‌سازد و از آنجایی که $key_2' = key_2$ برابر است F را رمزگشایی می‌کند و پارامتر W_i^{new*} را به دست می‌آورد و به وسیله $W_i^{new} = ?W_i^{new*}$ و $HID_i^* = ?HID_i$ احراز هویت را انجام می‌دهد. درصورت تایید هویت خدمات دهنده، ابتدا M_i را از طریق رابطه زیر بدست می‌آورد و سپس کلید جلسه را می‌سازد.

$$M_i = C_i \oplus PW_u$$

$$SK=h(b_i || M_i || W_i^{new} || key_2' || key_1)$$

C. *مرحله‌ی تغییر رمز عبور*

ابتدا کاربر کارت هوشمند خود را وارد دستگاه میکند و شناسه و رمزعبور قدیمی خود یعنی HID_i^*و pw_i^* را وارد میکند. و سپس تقاضای تغییر رمز عبور به همراه رمز عبور جدیدش را ارسال می‌کند.

$$PW_u^* = h(PW_i^* || a_i || HID_i^*) \oplus PW_i^*$$

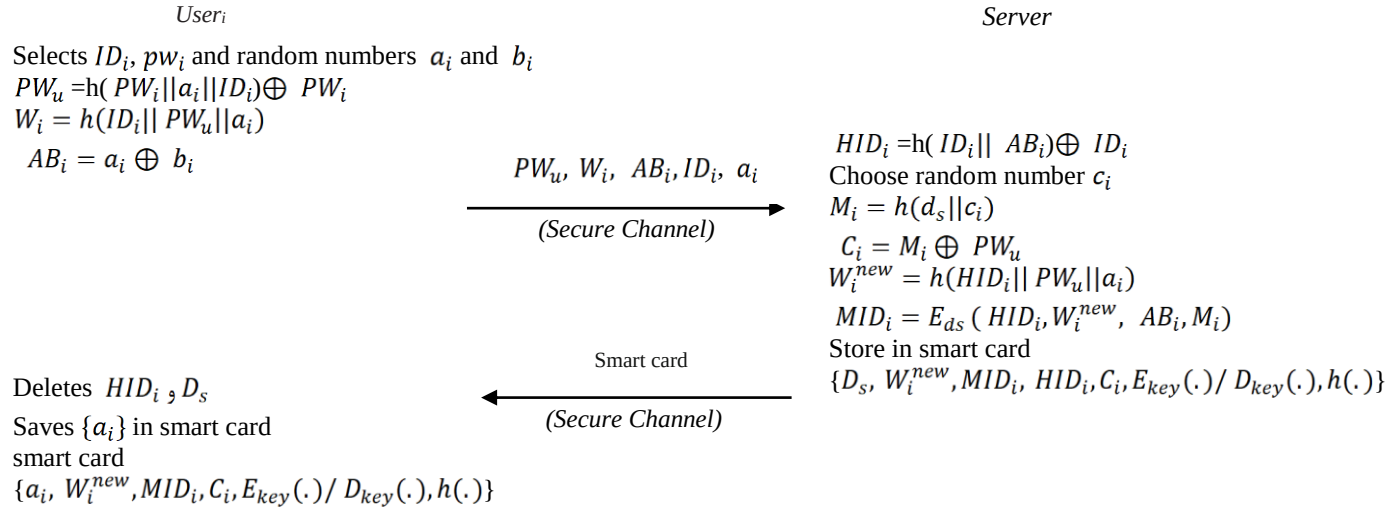
$$W_i^{new*} = h(HID_i^* || PW_u^* || a_i)$$

$$W_i^{new} =? W_i^{new*}$$

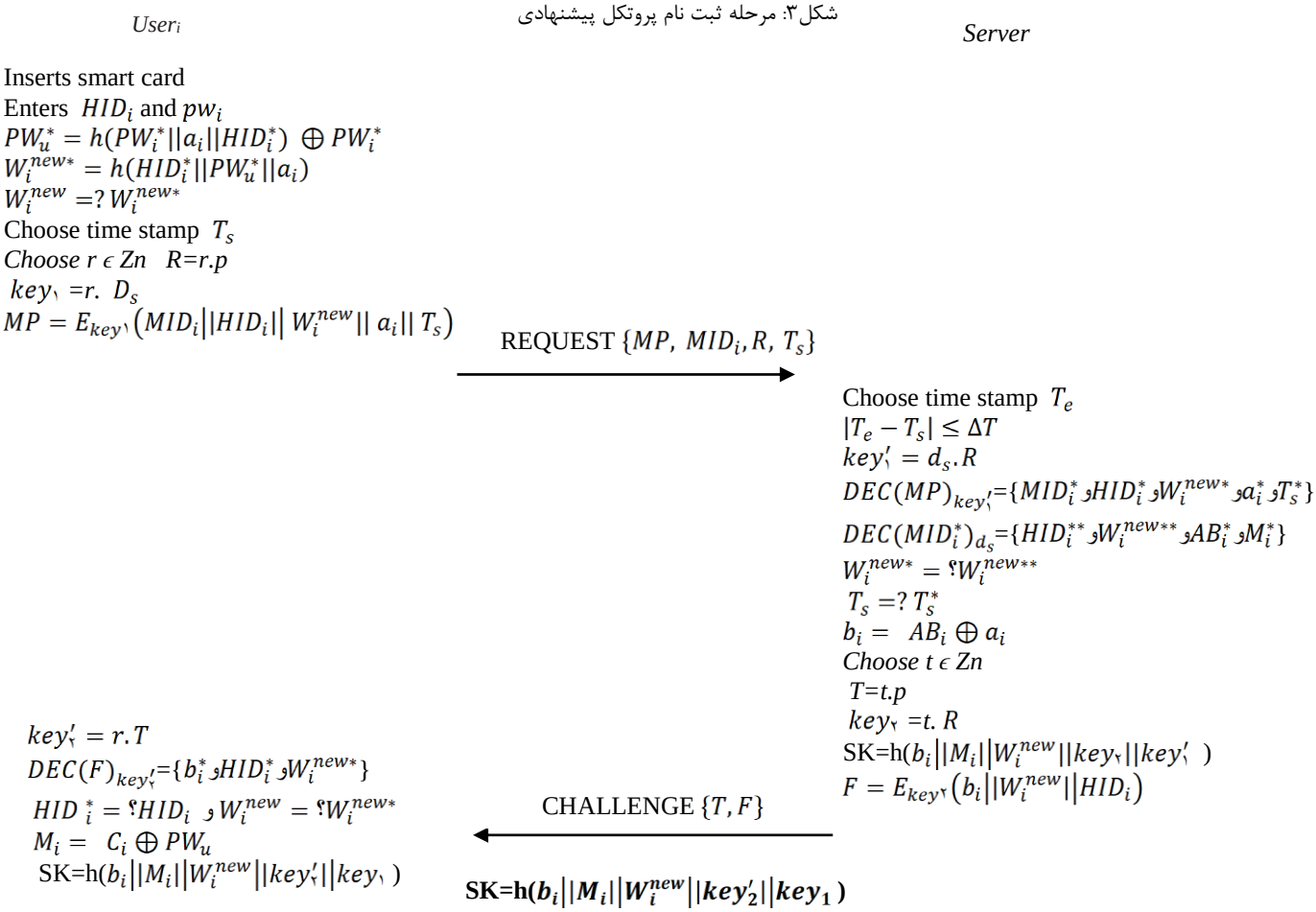
اگر تساوی بالا برقرار شود مشخص میشود که شخص مورد نظر کارت هوشمند خود را در در دست دارد و کارت هوشمند سرقتی نمی‌باشد. حال اگر رمز جدید را $\boldsymbol{PW_i^{**}}$ فرض کنیم، پارامترهای زیر دوباره با رمز عبور جدید محاسبه میشود و در انتها $\boldsymbol{W_i^{new**}}$ جایگزین $\boldsymbol{W_i^{new*}}$ در کارت هوشمند می‌شود.

$$PW_u^* = h(PW_i^* || a_i || HID_i^*) \oplus PW_i^*$$

$$W_i^{new**} = h(HID_i^* || PW_u^{**} || a_i)$$



شکل۳: مرحله ثبت نام پروتکل پیشنهادی



شکل۴: مرحله احرازهویت پروتکل پیشنهادی

۴. تحلیل امنیتی پروتکل پیشنهادی

در این بخش، مقاومت پروتکل پیشنهادی در مقابل تعدادی از حملات معروف مورد بررسی قرار میگیرد. در ادامه نیز، نتایج بررسی صحت پروتکل پیشنهادی توسط ابزار **Scyther** ارائه می گردد.

تامین گمنامی کاربر

اگرمهاجم پیام‌های REQUEST، CHALLENGE را شنود کند و همچنین اگر مهاجم کارت هوشمند را حتی به *سرقت برد* یا پیدا کند و اطلاعات آن را استخراج کند، نباید بتواند به شناسه اصلی کاربر دست پیدا کند. از آنجایی که در این پروتکل، ابتدا کاربر شناسه اصلی خود را به خدمات دهنده می‌دهد و خدمات دهنده یک شناسه موقت جدید یعنی HID_i =h(ID_i|| AB_i)⊕ ID_i را در اختیار کاربر قرار میدهد، مهاجم حتی اگر اگر بتواند به مقادیر HID_i وAB_i هم دست پیدا کند به هیچ عنوان نخواهد توانست به شناسه اصلی دست پیدا کند.

Known-key secrecy: پارامترهای تصادفی r و t توسط طرفین جلسه انتخاب می‌شود و در هر جلسه متمایز هستند و به پارامترهای r و tگذشته مرتبط نمی‌باشند در نتیجه با افشای کلید جلسه گذشته، امکان رسیدن به کلید جلسه‌ی جدید توسط مهاجم وجود ندارد.

محرمانگی روبه جلو: اگر PW_i کاربر یا کلید مخفی خدمات‌دهنده یعنی d_s افشا شوند مهاجم نباید قادر به دستیابی کلید جلسه باشد. در این پروتکل، مهاجم حتی با فاش شدن کلید مخفی خدمات‌دهنده یعنی d_s قادر به دستیابی به کلید نشست درست نمی‌باشد زیرا تنها دو موجودیت کاربر و خدمات‌دهنده، امکان دانستن key_1وkey_2 را دارند.

افشای پارامترهای موقتی یک جلسه: در صورت افشای پارامترهای تصادفی یعنی r, b_i, a_i, t, c_i مهاجم نباید توانایی رسیدن به کلید جلسه درست را داشته باشد. با توجه به عدم دانستن کلید محرمانه خدمات دهنده یعنی d_s و همچنین PW_u توسط مهاجم، وی امکان دستیابی به کلید جلسه‌ی درست را ندارد.

دزدیده شدن تاییدکننده‌ها: با توجه به اینکه پارامتری در پایگاه داده طرفین ذخیره نمی‌شود. مهاجم حتی با دستیابی به پایگاه داده‌ی طرفین هم توانایی رسیدن به کلید نشست را ندارد. همچنین در صورت مفقود شدن یا دزدیده شدن کارت هوشمند و استخراج اطلاعات درون آن توسط مهاجم، به دلیل وجود اعداد تصادفی یعنی t و r که کاربر و خدمات‌دهنده می‌دانند و دخیل بودن این پارامترها در ساخت کلید نشست، مهاجم با وجود دارا بودن اطلاعات کارت هوشمند قادر به یافتن کلید جلسه نمی‌باشد.

حمله‌ی حدس رمز عبور برون‌خط: اگر مهاجم پیام‌های REQUEST ، CHALLENGE را به‌دست آورد، قادر به حدس رمز عبور کاربر نمی‌باشد زیرا حتی اگر مهاجم کارت هوشمند را هم به دست آورد و حتی HID_i وa_i را هم به دست آورد باز هم قادر به بدست آوردن پسورد اصلی خدمات دهنده به علت نوع رابطه زیر نخواهد بود.

PW_u =h($PW_i||a_i||HID_i)\oplus$ PW_i

حمله‌ی تکرار: فرض می‌شود مهاجم قصد ارسال پیام تکراری REQUEST$\{MP, MID_i, R, T_s\}$ را برای خدمات‌دهنده دارد. با توجه به بررسی معادله‌ی $|T_e - T_s| \leq \Delta T$ درسمت خدمات‌دهنده، در صورت تکراری بودن پیام ارسالی، جلسه خاتمه می‌یابد. اگر مهاجم بخواهد مهر زمانی T_2 را به T_2^* تغییر دهد و پیام $\{EA_i, RID_i, T_S^*\}$ را برای خدمات‌دهنده ارسال نماید، خدمات‌دهنده با مقایسه‌ی مهر زمانی به‌دست آمده از رمزگشایی MP با پارامتر ارسالی T_S^* در کانال عمومی متوجه تغییر مهر زمانی می‌گردد. در نتیجه مهاجم قادر به ارسال پیام های تکراری و یا تغییر مهر زمانی نمی‌باشد.

حمله‌ی Denning-sacco: مهاجم با دستیابی به کلیدهای جلسه‌ی گذشته، قادر به رسیدن به پارامترهای کلید مخفی خدمات‌دهنده یا رمز عبور کاربر نمی‌باشد. در این پروتکل با توجه کلید جلسه یعنی SK=h($b_i||M_i||W_i^{new}||key_2'||key_1$) و حضور key_2' وkey_1 که خود از اعداد تصادفی بدست آمده و همچنین مسئله لگاریتم گسسته منحنی بیضوی (ECDLP) امکان به دست آوردن کلید جلسه را ندارد.

حمله جعل هویت:

الف) جعل هویت کاربر

برای جعل هویت کاربر توسط مهاجم، مهاجم باید پیام REQUEST را به خدمات‌دهنده ارسال نماید. در نتیجه مهاجم نیازمند محاسبه‌ی مقادیر W_i^{new*} و T_S^* است. برای محاسبه‌ی مقدار معتبر W_i^{new*}، مهاجم باید کلید محرمانه خدمات دهنده یعنیd_s و همچنین عدد تصادفی r را بداند. اما این مقادیر توسط کاربر و خدمات دهنده محرمانه نگهداری می‌شود.

ب) جعل هویت خدمات‌دهنده

برای جعل هویت خدمات‌دهنده، مهاجم باید بتواند پیام $\{T, F\}$ CHALLENGE معتبر را بسازد و برای کاربر ارسال نماید. برای به‌دست آوردن W_i^{new*}، مهاجم نیاز به دانستن عدد تصادفی تولیدی

کاربر یعنی r و یا عدد تصادفی تولید شده توسط خدمات دهنده یعنی t را دارد. اما مهاجم به علت مسئله لگاریتم گسسته منحنی بیضوی (ECDLP) قادر به به دست آوردن این اعداد تصادفی نیست.

اثبات درستی پروتکل پیشنهادی با استفاده از ابزار Scyther

یک ابزار قدرتمند و مؤثر به‌منظور تجزیه‌وتحلیل، شناسایی حمله‌های احتمالی و آسیب‌پذیری‌های پروتکل‌های امنیتی است. Scyther مبتنی بر الگوریتم مدل توسعه است که نمایش نامحدود از ردیابی‌ها را فراهم می‌نماید و پروتکل را به طور خودکار تحلیل نموده و رفتار آن را درمقابل اکثر حمله‌های ممکن مورد بررسی دقیق قرار می‌دهد.

شکل ۵، خروجی بررسی پروتکل پیشنهادی توسط scyther را نمایش میدهد. ویژگی Niagree تضمین میکند که طرفین ارتباط موافقت می‌کنند که پیام‌ها به طور امن و با ترتیبی درست بین آن‌ها رد و بدل شده است. ویژگی Nisynch تضمین می‌کند که پیام‌های رد و بدل شده بین طرفین قابل رمزگشایی و ارسال دوباره نباشد.

ویژگی Alive تضمین می‌کند که ترتیب مراحل پروتکل به وسیله طرفین ارتباط، تایید شده است.

ویژگی Weakagree تضمین می‌کند که در پروتکل، امکان جعل هویت وجود نداشته باشد. ویژگی secret نیز تضمین خواهد کرد که پارامتر مربوطه امن خواهد ماند. همانگونه که در شکل ۵ نشان داده شده است پروتکل احراز هویت معرفی شده در مقاله، قادر است تمامی ویژگی های فوق را تامین نماید.

Scyther results : verify

Claim				Status		Comments
MAHDI	U	MAHDI,U1	Secret XOR(pwi,H1(pwi,ai,hidi))	Ok		No attacks within bounds.
		MAHDI,U2	Secret H1(bi,XOR(ci,XOR(pwi,H1(pwi,ai,hidi))),H1(h...	Ok	Verified	No attacks.
		MAHDI,U3	Secret idi	Ok	Verified	No attacks.
		MAHDI,U4	Alive	Ok		No attacks within bounds.
		MAHDI,U5	Nisynch	Ok		No attacks within bounds.
		MAHDI,U6	Niagree	Ok		No attacks within bounds.
		MAHDI,U7	Weakagree	Ok		No attacks within bounds.
	S	MAHDI,S1	Secret XOR(pwi,H1(pwi,ai,hidi))	Ok	Verified	No attacks.
		MAHDI,S2	Secret H1(XOR(ABi,ai),XOR(ci,XOR(pwi,H1(pwi,ai,hid...	Ok	Verified	No attacks.
		MAHDI,S3	Secret idi	Ok	Verified	No attacks.
		MAHDI,S4	Alive	Ok	Verified	No attacks.
		MAHDI,S5	Nisynch	Ok	Verified	No attacks.
		MAHDI,S6	Niagree	Ok	Verified	No attacks.
		MAHDI,S7	Weakagree	Ok	Verified	No attacks.

Done.

شکل۵: خروجی بررسی پروتکل پیشنهادی توسط ابزار scyther

۵. نتیجه‌گیری:

در این مقاله پروتکلی کارامد بر پایه رمزنگاری منحنی بیضوی برای ارتباط امن کاربران با خدمات دهنده ارائه شد. تحلیل امنیتی پروتکل نشان داد که این پروتکل قادر است محرمانگی روبه جلو را تامین نموده و کاربر را درمقابل حملات مختلفی چون جعل هویت و تکرار محافظت نماید. صحت پروتکل باکمک ابزار scyther نیز بررسی و تایید گردید.

منابع:

[۱] Hsieh, W., and Leu, J., Exploiting hash functions to intensify the remote user authentication scheme. *Comput Secur* ۳۱(٦):۷۹۱–۷۹۸, ۲۰۱۲.

[۲] Wang, D., Ma, C., Wang, P., and Chen, Z., Robust smart card based password authentication scheme against smart card security breach. IACR Cryptology ePrint Archive. Retrieved from eprint.iacr.org/۲۰۱۲/٤۳۹.eps, ۲۰۱۲.

[۳] Chang, Y., Tai, W., and Chang H, Untraceable dynamic-identitybased remote user authentication scheme with verifiable password update. *Int J Commun Syst*, ۲۰۱۳.

[٤] Kumari, S., Gupta, M. K., Khan, M. K., and Li, X., An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement. *Secur Commun Netw* ۷(۱۱):۱۹۲۱–۱۹۳۲, ۲۰۱٤.

[٥] Das AK, Goswami A. An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J Med Syst*.۳۸(٦):۲۷, ۲۰۱٤.

[٦] Mishra D, et.al., Cryptanalysis and improvement of Yen et al.'s biometric-basedauthentication scheme for telecare medicine information systems. *J Med Syst*. ۳۸(٦):۲٤, ۲۰۱٤.

[۷] Nikooghadam M, Jahantigh R, Arshad H, A lightweight authentication and key agreement protocol preserving user anonymity.Multimedia Tools and Applications:۱–۲۳, ۲۰۱٦.

[۸] Cremers, C, Scyther - Semantics and Verification of Security Protocols. Ph.D. dissertation, Eindhoven University of Technology, ۲۰۰٦.