پروتکل توافق کلید امن احراز اصالت شده برای کاربرد در گواهی (تصدیق) دیجیتال

امیرحسین رحیمی [۱]

[۱] کارشناس ارشد رمز و مربی دانشگاه آزاد اسلامی، واحد قم، گروه ریاضی، قم
amir.rahimi361@gmail.com

چکیده

پروتکل توافق کلید احراز اصالت شده یک مؤلّفه اساسی در برقراری کلید جلسه به منظور ایجاد کانال امن برای ارتباطات شبکه‌ای در محیط‌های باز و توزیع‌شده می‌باشد. تاکنون پروتکل‌های زیادی بر اساس تعیین هویّت اشخاص برای فراهم کردن احراز اصالت متقابل قوی و برقراری کلید جلسه عمومی در محیط‌های باز و دوگانه برای ارتباطات امن پیشنهاد شده‌اند. امّا اکثر پروتکل‌های موجود توافق کلید احراز اصالت شده فقط امنیت پیشرو جزئی و نسبی را فراهم می‌کنند. بنابراین چنین پروتکل‌هایی برای کاربردهای تکنولوژی روبه رشد جهان واقعی که امنیت پیشرو کامل را نیاز دارند مناسب نیستند. در این مقاله یک پروتکل توافق کلید احراز اصالت شده براساس شناسه‌ی هویّت امن دو بخشی ارائه می‌شود که اکثر مشخصه‌های امن مطلوب شامل: امنیت کلید معلوم، امنیت پیشرو کامل، امنیت پیشرو PKG، قابلیّت ارتجاع در برابر جعل هویّت کلید کشف رمز شده، قابلیّت ارتجاع در برابر تسهیم کلید نامعلوم، کنترل نکردن کلید، شناسایی نکردن امنیت اطلاعات کلید جلسه ثابت- موقتی را با بازدهی بالا به انجام می‌رساند و همچنین الگوریتم پیشنهادی زمان اجرای کوتاه‌تر، هزینه‌ی محاسباتی و ارتباطی کمتر و روش ذخیره‌سازی مؤثّر نسبت به سایر الگوریتم‌های پیشنهادی مشابه دارد و گذشته از این اخلال‌گر به آسانی نمی‌تواند در روند تبادل داده، کلید جلسه توافقی را کشف رمز کند.

کلمات کلیدی: توافق کلید، احراز اصالت کاربر، مولّد کلید خصوصی(PKG)، گواهی دیجیتال، تابع درهم‌ساز، لگاریتم گسسته، کلید جلسه محرمانه.

۱ مقدمه

اصولاً پروتکل توافق کلید برای فراهم کردن ارتباطات امن در محیط‌های باز و توزیع شده بکار می‌رود و برقراری کلید شیوه‌ای است که بوسیلهٔ آن دو (یا بیشتر) هویّت‌ها می‌توانند یک کلید محرمانهٔ تسهیم شده (کلید جلسه) را بعد از فعل و انفعالات پیام بین خودشان برقرار کنند؛ از این‌رو دو شیوهٔ مختلف برای برقراری

جدول ۱: نمادگذاری‌ها

نماد	تعریف	نماد	تعریف
ID	شناسه‌ی هویّت کاربر	$\oplus$	عملگر XOR
r_{ID}	عدد تصادفی	E	نگاشت خطی
p و q	دو عدد اول بزرگ به‌طوری‌که $p = ۲q + ۱$	$H(\cdot)$	تابع درهم‌ساز امن
G	گروه جمعی دوری	Z_P^*	گروه ضربی p
$G_۱, G_۲$	گروه ضربی دوری	$\|\|$	عملیات الحاق
F_P	میدان متناهی عدد اوّل p	$X(\mathrm{mod} p)$	باقیمانده X تقسیم بر p
AK	کلید احراز اصالت شده	SK	کلید جلسه
P_{pub}	کلید عمومی	ECC	رمزنگاری خم بیضوی
DLP	مسئله‌ی لگاریتم گسسته	CDH	فرض دفی-هلمن

کلید بین دوهویّت وجود دارد؛ در یکی ازروش‌ها هویّتی یک کلید جلسه ایجاد کرده و به طور امن آن‌را به هویّت دیگری برای هم‌پوشانی انتقال می‌دهد؛ ضمناً به منظور تأمین احراز اصالت پروتکل توافق کلید، تصدیق کلید عمومی اغلب در محیط کلید عمومی سنتی با تصدیق گواهی‌نامه بکاربرده می‌شود. Adi Shamir [۴] در ۱۹۸۴ رمزنگاری براساس شناسه هویّت را معرفی کرد. ایدهٔ او به تمامی بخش‌ها اجازه می‌داد شناسه‌های هویّت‌شان را به عنوان کلید عمومی بکار گرفته و به کمک مولّد کلید خصوصی (PKG)، کاربرها کلیدهای خصوصی‌شان را تولید کرده و براساس پروتکل‌های رمزنگاری اجرا شوند. احراز اصالت بدون تصدیق کلید عمومی مزیّت اصلی رمزنگاری براساس شناسهٔ هویّت است. پروتکل توافق کلید احرازاصالت شدهٔ دو بخشی (AK) علاوه براین‌که به بخش‌ها اجازه می‌دهد کلید جلسه‌ای که فقط به آن‌ها شناخته شده را محاسبه کنند بلکه اعتبار قسمت‌ها را نیز تضمین کنند. همچنین کلید جلسهٔ محرمانه می‌تواند یکپارچگی و استقلال داده را در طول جلسات متوالی فراهم کند. پروتکل توافق کلیدی که احراز اصالت متقابل کلید ضمنی (از باب به آلیس) را فراهم می‌کند؛ پروتکل توافق کلید احرازاصالت شدهٔ AK نامیده می‌شود دراین پروتکل توافق کلید، زمانی تصدیق کلید (از باب به آلیس) فراهم می‌شود که آلیس مطمئن شده باشد فقط باب کلید محرمانه را در تصرف دارد. پروتکلی که احراز اصالت کلید متقابل و همچنین تأییدیهٔ کلید متقابل را فراهم می‌کند تحت عنوان یک توافق کلید احراز اصالت شده با پروتکل تصدیق کلید (یا یک پروتکل AKC) نامیده می‌شود.

دراین مقاله، یک پروتکل توافق کلید احراز اصالت شدهٔ امن و مؤثّر (AK) بر اساس یک روش تابع درهم‌ساز امن و مسئلهٔ لگاریتم گسسته پیشنهاد می‌شود. همچنین دربخش بعدی با مقایسهٔ الگوریتم پیشنهادی نسبت به الگوریتم‌های مرتبط دیگر به این نتیجه می‌رسیم که الگوریتم پیشنهادی ما در مدّت زمان کمتری اجرا شده و علاوه بر این در هزینهٔ محاسباتی، ارتباطی و نحوهٔ ذخیره‌سازی مؤثّر ظاهرمی‌شود و همچنین بررسی خواهیم کرد که توابع درهم‌ساز از بُعد محاسباتی با عملگر معکوس اجراء نشدنی بوده و لذا الگوریتم پیشنهادی با پیروی از این ویژگی در برابر بیشتر حمله‌های شناخته شده پایداری خواهد کرد.

۲ تحلیل مؤلّفه‌های سیستم رمزنگاری طرح پیشنهادی

۱.۲ مفاهیم اساسی

طرح پیشنهادی از برخی سیستم‌های رمزنگاری، از قبیل: تابع درهم‌ساز (SHA-512)، MD5، مسئلهٔ لگاریتم گسسته، و پروتکل توافق کلید دفی هلمن و الگوریتم خم بیضوی بهره می‌گیرد. در الگوریتم SHA-1، مانند MD5 طول چکیده پیام آن ۱۶۰ بیت (معادل ۲۰ بایت) می‌باشد. هر چند طول چکیده پیام SHA-2 بیش از ۱۶۰ بیت است. امّا اغلب در سیستم‌های رمزنگاری از SHA-256 و SHA-512 استفاده می‌شود.

بنابراین برای هر پروتکل توافق کلید احرازاصالت شده شامل‌کردن مشخصه‌های امن زیر لازم می‌باشد:

۱. امنیت کلید معلوم: افشای یک کلید جلسهٔ محرمانه نباید باعث کشف رمز کلیدهای جلسهٔ دیگر شود. بنابراین توافق کلید می‌تواند از کشف رمزکلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار و حملهٔ خودی جلوگیری کند.

۲. امنیت پیشرو: اگرطول کلید خصوصی یک هویّت یا چند هویّت کشف رمز شود؛ آن‌گاه نباید امنیت کلیدهای جلسه مرتبط دیگر تحت تأثیر قرار گیرند. سیستمی امنیت پیشرو جزئی خواهد داشت که اگر طول کلید یک هویّت کشف رمز شود آن‌گاه امنیت سیستم بدون کشف رمزکردن کلیدهای جلسه قبلی تحریف خواهد شد. پس به منظور پایداری در برابر حملهٔ جستجوی جامع برای بازیابی عددتصادفی محرمانه، اگر اندازهٔ عدد تصادفی بزرگتر از کلید جلسه محرمانه باشد بهتر است. لذا برای نگهداری اطلاعات محرمانه (کلید جلسه) به عدد تصادفی نیاز است؛ چون اگر کلید محرمانه فاش شود آن‌گاه کلیدهای جلسه خطر کشف رمز دارند.

۳. محرمانگی پیشرو PKG: کلید اصلی PKG ممکن است بدون خطر کشف رمزکردن کلیدهای جلسه برقرار شدهٔ امن قبلی توسط هرکاربر تحریف شود.

۴. خطرکشف رمزکلید قابلیّت ارتجاع برای جعل هویّت: برای هر هویّتی مانند آلیس، خطرکشف رمزکردن طول کلید خصوصی آلیس، اخلال‌گر را به جعل هویّت آلیس قادر خواهد کرد امّا این روش جعل هویّت آلیس نباید اخلال‌گر را قادر به جعل هویّت کردن اشخاص مرتبط به آلیس کند.

۵. قابلیّت ارتجاع تسهیم کلید نامعلوم: یعنی هویّتی مانند آلیس نباید به تسهیم یک کلید با هر هویّت هم جنس دیگری به جای باب قادر باشد. یعنی آلیس نباید تصورکند که او با هر هویّت دیگر مبدل شده به جای باب تسهیم کلید می‌کند.

۶. امنیت اطلاعات موقتی- ثابت جلسه معلوم: برخی اطلاعات خصوصی به صورت تصادفی به عنوان یک ورودی تابع تولید کلید جلسه بکار برده می‌شوند؛ فاش‌کردن این اطلاعات موقتی خصوصی نباید امنیت کلید جلسه‌های دیگر را به خطر بیندازد.

امنیت اطلاعات موقتی- ثابت جلسه معلوم ابتدا توسط Canetti-Krawczyk [۶] در ۲۰۰۱ بررسی شد و او به این نتیجه رسید که این مشخصهٔ امن اساسی نیاز می‌باشد و اگر امنیت زودگذر جلسات به صورت تصادفی برای اخلال‌گر فاش شده باشد آن‌گاه امنیت کلید جلسهٔ معین نباید تحت تأثیر قرارگیرد. هرچند درطرف مقابل فاش‌سازی اطلاعات خصوصی هم قابل چشم‌پوشی نبوده و ممکن است در برخی طرح‌های عملی این اتّفاق افتاده باشد.

در ۲۰۰۹ و ۲۰۱۰، Cao etc. [۷]، [۸] دو طرح مستقل توافق کلید احراز اصالت شده براساس شناسهٔ هویّت (ID) دو سویه با دو یا سه مرحلهٔ انتقال پیشنهاد کرد که همهٔ مشخصه‌های امن اساسی را بانجام رسانده و به عملگرهای جفتی هم نیاز نبود. امّا می‌دانیم این پروتکل‌ها یک ویژگی امن اساسی با تحت عنوان امنیت اطلاعات موقتی-ثابت جلسه معلوم را پشتیبانی نمی‌کنند که یکی از مشخصه‌های امن زودگذر بوده که برامنیت کلید جلسه اثر می‌گذارد.

۷. بدون کنترل کلید: هیچکدام از هویّت‌ها قادر به استفاده مجدد کلید جلسه برای مقادیر پیش فرض نمی‌باشند. قابلیّت اجرای بدون اعتبارکلید تحت رویدادهای معین به خصوص درکاربردهای گروهی معین از قبیل ارتباطات امن در حرفهٔ مراقبت سلامتی(بهداشت) مطلوب است. چون قابلیت اعتماد جزء نیازمندی های مجاز می‌باشد.

تاکنون برخی پروتکل‌های توافق کلید احراز اصالت شده براساس شناسهٔ هویّت با قابلیّت اجرا در طرح‌های [۱۰]، [۱۲]، [۱۳]، [۱۴] و [۱۷] پیشنهاد شده‌اند. امّا با بررسی و تحلیل ساختار وعملکردشان متوجّه می‌شویم که اکثر آن‌ها مشخصهٔ امن پیشروکامل را فراهم نمی‌کنند. علی‌رغم این‌که Shim [۱۵] در ۲۰۰۳ مدعی بود که پروتکلی پیشنهادی‌اش همهٔ مشخصه‌های امن را فراهم می‌کند امّا در همان سال Sun and Hsieh [۱۶] آسیب‌پذیری پروتکل Shim [۱۵] را به حملهٔ شخص در وسط اثبات کردند. در ۲۰۰۶، Gentry [۱۱] یک سیستم رمزنگاری براساس شناسهٔ هویّت پیشنهاد کرد که امنیت را در مدل استاندارد کامل کرده و مزیّت‌هایی هم نسبت به سیستم‌های قبلی داشت.

باقیمانده مقاله سازمان‌دهی می‌شود به عنوان زیر:
در بخش ۳ پس‌زمینه‌های تکنیکی ضروری پروتکل بیان می‌شود و همچنین طرح رمزنگاری براساس شناسه هویّت Gentry و طرح Cao بازبینی خواهند شد و دربخش ۴ طرح پیشنهادی جدید را ارائه می‌دهیم دربخش ۵ تحلیل امنیتی و پروتکل‌های پیشنهادی کارآمد و همچنین مقایسهٔ پروتکل‌های قابل مقایسه را ارائه خواهیم داد.

۳ پس‌زمینه‌های تخصصی

۱.۳ گراف‌های خطی (دوسویه)

به‌فرض G_1 و G_2 دو گروه دوری ضربی از مرتبهٔ اوّل p و g یک مولّد G_1 باشد و از آن‌جائی‌که حل مسئلهٔ لگاریتم گسسته در هر دو گروه G_1 و G_2 مشکل می‌باشد گراف خطی (دوسویه) $e : G_1 \times G_1 \to G_2$ را

در نظر بگیرید که سه ویژگی زیر را ایفا می‌کند:

- خطی بودن (دوسویه): برای همهٔ $u, v \in G_1$ و $a, b \in Z_p^*$، داریم $e(u^a, v^b) = e(u, v)^{ab}$.
- بدون تبهگنی (بدون هم‌ارزی): $e(g, g) \neq 1$.
- قابل مقایسه: اگر $u, v \in G_1$ آن‌گاه می‌توان به‌صورت بهینه در زمان چندجمله‌ای $e(u, v) \in G_2$ را محاسبه کرد.

۲.۳ گروه‌های خم بیضوی

رمزنگاری خم بیضوی برای تأمین امنیت در سیستم رمزنگاری RSA یا DSA با مسئلهٔ لگاریتم گسسته (DLP) مرسوم می‌باشد. رمزنگاری خم بیضوی کمترین سربار محاسباتی و اندازه کلید کوچکتر و امنیت و کارآمدی بالایی دارد. گروه خم بیضوی از بُعد محاسباتی، گروهی با متغیر و ضرایب خم بیضوی محدود شده به عناصر میدان متناهی می‌باشد. سمبل E/Fp نشانگر یک خم بیضوی E روی میدان متناهی اوّل Fp بوده که به کمک یک معادلهٔ $y^2 = (x^3 + ax + b) \bmod p$ با فرض $a, b \in Z_p$ و $8a^3 + 81b^2 \bmod p \neq 0$ تعریف می‌شود. البتّه نقاط روی E/Fp با یک نقطهٔ اضافی o به فرم : $G = \{(x, y) : x, y \in F_p, E(x, y) = 0\} \cup o$ تعریف می‌شود. G یک گروه جمعی دوری تحت عمل جمع نقاط "+" به‌صورت زیرتعریف می‌شود: فرض $p, q \in G$، l خطی شامل نقاط p, q (خط مماس به E/Fp اگر $p = q$ باشد) و R فصل مشترک نقطه سوّم l با E/Fp است. فرض خط l' نقاط R و o را مرتبط می‌کند. سپس $p + q$ نقطه‌ای است به‌طوری‌که l'، E/Fp را در R، o و $p + q$ قطع می‌کند. همچنین ضرب اسکالر روی E/Fp با یک عدد صحیح با فرض تکراری کردن جمع یعنی $kp = p + p + \cdots + p \ \ (k \text{ times})$ تعریف می‌شود.

۳.۳ فرضیات پیچیدگی محاسبات

مسائل تعریف شدهٔ زیر بر روی گروه خم بیضوی در زمان چندجمله‌ای رام‌نشدنی (غیرعملی) فرض شده‌اند.

تعریف ۱: فرض محاسباتی دفی-هلمن (CDH): P مولّد گروه خم بیضوی G و بازاء $a, b \in Z_p^*$ و با تعیین aP و bP، محاسبه کردن abP مشکل است.

تعریف ۲: فرض قطعی دفی-هلمن (DDH): مولّد گروه خم بیضوی G و بازاء $a, b, c \in Z_p^*$ با معین کردن aP و bP و cP، تعیین این‌که آیا $cP = abP$ مشکل می‌باشد.

تعریف ۳: شکاف فرض دفی-هلمن (Gap-DH): با معین کردن سه‌تایی $\{P, aP, bP\} \in G$ جائی که بازاء $a, b, c \in Z_p^*$، محاسبهٔ abP به‌کمک اوراکل (غیب‌گو) DDH مشکل می‌باشد (پاسخ‌دهی به‌طوری‌که یک چهارگانهٔ معین یک چهارگانهٔ DH است یا خیر).

۴ طرح پیشنهادی جدید

در این بخش، ما یک پروتکل توافق کلید کارآمد و احراز اصالت شدهٔ یک طرفه امن براساس شناسهٔ هویّت پیشنهاد می‌کنیم که تقریباً همهٔ مشخصه‌های امن شناخته شده، مخصوصاً امنیت داده موقتی-ثابت جلسه معلوم را بانجام می‌رساند. امنیت پروتکل پیشنهادی می‌تواند فرض محاسباتی دفی‌هلمن CDH را در مدل اوراکل تصادفی کاهش دهد. پروتکل شامل ۴ مرحله راه‌اندازی، تولید کلید، توافق کلید و تصدیق صحیح می‌باشد؛ که ۳ مرحلهٔ اوّل تقریباً با اندکی اصلاحات با طرح Cao [۶] یکسان بوده امّا در تولید کلید جلسه متفاوت است. ما تمایل داریم یک پروتکل توافق کلید براساس یک شناسهٔ هویّت قابل اجرا را طوری پیشنهاد کنیم که کلید جلسه کاربر بتواند توسط PKG بازیابی شود در حالی که در طرح‌های مرتبط دیگر اشخاص می‌توانند کلیدهای جلسهٔ گذشته کاربر را بازیابی کنند حتّی اگر طول کلید بزرگ باشد.

پروتکل شامل ۳ هویّت می‌باشد: دو کاربر به نام آلیس و باب به برقراری یک کلید جلسهٔ محرمانهٔ تسهیم شده تمایل دارند و PKG مرکز تولید و توزیع کلیدهای خصوصی کاربر با کاربرد کلید اصلی آنها مسئول می‌باشد.

ما به‌منظور حفظ تشریح یکپارچگی مراحل، پروتکل را به‌صورت زیر ارائه می‌دهیم:

۱. **راه‌اندازی:** مولّد کلید خصوصی PKG ابتدا پارامترهای سیستم و سپس جفت کلید خصوصی/عمومی را تولید می‌کند به عنوان زیر:

مولّد کلید خصوصی PKG با تعیین یک پارامترامن سیستم به عنوان K، ۳گانهٔ $\{E/Fp, G, p\}$ و کلید خصوصی اصلی $x \in Z_p^*$ را انتخاب می‌کند و کلید عمومی را به‌عنوان $P_{pub} = kp^x$ محاسبه کرده و سپس G و G_T دو گروه از مرتبهٔ اوّل p، سه تابع درهم‌سازی رمزنگاری امن و یک نگاشت خطی انتخاب می‌کند و خواهیم داشت:

$$
\begin{aligned}
e &: G \times G \to G_T \quad \text{(نگاشت خطی)} \\
H_1 &: \{0,1\}^* \times G \to Z_p^* \\
H_2 &: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \to \{0,1\}^k, \\
H_3 &: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \to \{0,1\}^k
\end{aligned}
$$

$$
\text{Let} \quad g, p, t \in G, t = g^x \bmod p, g_T = e(g,t) \in G_T.
$$

سپس PKG پارامترهای عمومی سیستم را به‌عنوان $< E/Fp, G, P_{pub}, t, g_T, H_1, H_2, H_3 >$ منتشر می‌کند. در ضمن کلید خصوصی اصلی PKG، متغیر x می‌باشد.

۲. **تولید کلید:** مرکز تولید کلید به‌منظوراحراز هویّت کاربر در Z_p^*، یک کلید خصوصی طولانی ایجاد کرده و همچنین برای یک کاربر با شناسهٔ هویّت $ID \in Z_p^*, ID \neq x$، یک عدد تصادفی $r_ID \in Z_p^*$ متناسب با شناسهٔ هویّت معین ID نسبت داده و معادلهٔ $R_{ID} = (kp^{-r_{ID}})^{\overline{(x-ID)}}, h_{ID}$

$H_1(ID||R_{ID})$ را محاسبه کرده و کلید خصوصی $d_{ID} =< R_{ID}, s_{ID} >$ را به‌عنوان خروجی می‌دهد جائی که $s_{ID} = r_{ID} + h_{ID}x$.

سپس کلید خصوصی طولانی کاربر به همراه شناسهٔ هویّت کاربری از طریق کانال امن به کاربر منتقل شده و کاربر با شناسهٔ هویّت ID می‌تواند کلید خصوصی طولانی‌اش را با بررسی کردن معادلهٔ $s_{ID}p = R_{ID} + H_1(ID||R_ID)P_{pub}$ تصدیق کند.

کلید خصوصی طولانی معتبر است اگر معادله صحیح نگه داشته شود و بالعکس. فرض کنید دو هویّت به نام آلیس (عمل‌کنندهٔ آغازگر) و باب (به‌عنوان پاسخ‌دهنده) وجود داشته باشند که می‌خواهند کلید جلسه برقرار شود.

۳. **توافق کلید:** ID_A و ID_B شناسهٔ تعیین هویّت آلیس و باب بوده که یک کلید جلسهٔ تسهیم شده را با احراز اصالت در پروتکل زیر اجرا خواهند کرد.

Scheme 1.

(1) $A \to B : ID_A, R_A$. B chooses $b \in Z_p^*$ and computes the message $T_B = g_B^{b(R_A + H_1(ID_A||R_A)P_{pub})} \bmod p$

(2) $B \to A : ID_B, R_B, T_B$. A chooses $a \in Z_p^*$ and computes the message $T_A = g_A^{a(R_B + H_1(ID_B||R_B)P_{pub})} \bmod p$

(3) $A \to B : T_A$. B computes $K_{BA} = (b+1)s_B^{-1}T_A + H_1((ID_A||R_A)P_pub) + bp$ and $SK_{BA} = H_2(ID_A||ID_B||T_A||T_B||K_{BA})$; Finally A computes $K_{AB} = (a+1)s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + aP$ and $SK_{BA} = H_2(ID_A||ID_B||T_A||T_B||K_{BA})$.

۴. **صحت تصدیق:** درپایان اجرای پروتکل، آلیس و باب روی کلید جلسه یکسان توافق می‌کنند. ما می‌توانیم به آسانی تصدیق کنیم که $sk = SK_{BA} = SK_{AB}$. همچنین ازفرم معادله SK_BA و SK_AB می‌توان تشخیص داد که اگر اخلال‌گر a و b جلسات محرمانهٔ موقت-معین را بشناسند آن‌ها نمی‌توانند کلید جلسه‌ی SK_{BA} یا SK_{AB} فرا گیرند؛ برای‌این‌که اخلال‌گر نمی‌تواند $H_1((ID_B||R_B)P_{pub})$، T_A، T_B و همچنین s_A^{-1} و s_B^{-1} را محاسبه کند، زیرا به‌طور محاسباتی معکوس تابع درهم‌ساز بدون شناختن کلید محرمانهٔ سرور غیرعملی است و همچنین طرح مشخصهٔ

امن اضافی، امنیت داده موقتی/ ثابت (معین) جلسه معلوم را به آسانی پشتیبانی می‌کند زیرا:

$$\begin{aligned} K_{AB} &= (a+1)s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + ap \\ &= as_A^{-1}T_B + s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + ap \\ &= abp + ap + bp + s_Bp \\ &= bap + bp + ap + s_Ap \\ &= bs_B^{-1}T_A + s_B^{-1}T_A + H_1((ID_A||R_A)P_{pub}) + bp \\ &= (b+1)s_B^{-1}T_A + H_1((ID_A||R_A)P_{pub}) + bp = K_{BA} \end{aligned}$$

بنابراین ما کلید جلسهٔ توافق شده یکسان را به‌دست می‌آوریم به صورت $sk = SK_{BA} = SK_{AB}$.

Scheme 2.

(1) $A \rightarrow B : ID_A, R_A, T_A$. The initiator A chooses a random ephemeral key $a \in Z_p^*$,
and compute the message $T_A = aP$

(2) $B \rightarrow A : ID_B, R_B, T_B$ On receiving the message from A, The responder B chooses a random ephemeral key and compute the message $T_B = bP$;

Finally, A computes $K_{AB} = (T_B + R_B + H_1(ID_B||R_B)P_{pub})(a + s_A)$;
B computes $K_{BA} = (T_A + R_A + H_1(ID_A||R_A)P_{pub})(b + s_B)$;
It is easy to validate that $K_{AB} = (T_B + R_B + H_1(ID_B||R_B)P_{pub})(a + s_A)$;
$= (bP + s_BP)(a + s_A) = (aP + s_AP)(b + s_B)$
$= (T_B + R_B + H_1(ID_B||R_B)P_{pub})(b + s_B) = K_{BA}$
$= (a + s_A)(b + s_B)P = abP + as_BP + bs_AP + s_As_BP$

ما می‌توانیم بررسی کنیم که آیا $sk = SK_{BA} = SK_{AB}$.

۵ تحلیل امنیتی و کارآمدی

دراین بخش، تحلیل امنیتی جامع، راندمان طرح پیشنهادی و مقایسهٔ کارآمدی پروتکل‌های کاربردی را ارائه می‌دهیم.

۱.۵ تحلیل امنیتی

حال اثبات خواهیم کرد که پروتکل پیشنهادی تعدادی مشخصهٔ امن مطلوب از قبیل: امنیت کلید معلوم، امنیت پیشرو PKG، قابلیّت ارتجاع جعل هویّت دربرابر خطرکشف رمزکلید، قابلیّت ارتجاع تسهیم کلید نامعلوم، کنترل نکردن کلید پشتیبانی کرده و همچنین به طورخاص امنیت پیشرو کامل را بانجام می‌رساند.

۱.۱.۵ امنیت کلید معلوم

اگر یک کلید جلسه کشف رمز شود به معنای این نیست که هرکلید جلسهٔ دیگری کشف رمز خواهد شد در حقیقت هر اجرای پروتکل یک کلید جلسه متفاوت را محاسبه می‌کند که به کلیدهای خصوصی موقت x و y وابسته است. تا جائی که x و y به‌طور تصادفی توسط آلیس و باب به‌طور مستقل انتخاب می‌شوند.

۲.۱.۵ قابلیت ارتجاع جعل هویّت در برابر خطرکشف رمزکلید

فرض یک اخلال‌گر از جنس مؤنّث کلید طولانی خصوصی را شناسایی کرده و تمایل داشته باشد به عنوان باب به آلیس مبدل شود. علی‌رغم این‌که جنس مؤنّث می‌تواند با شناسهٔ هویّت باب خودش را بشناساند و T_B را به آلیس ارسال کند. امّا او نمی‌تواند بدون شناختن کلید خصوصی باب، K_{BA} را برای محاسبهٔ کلید جلسهٔ یکسان همانند آلیس بکار گیرد.

۳.۱.۵ قابلیت ارتجاع تسهیم کلید نامعلوم

اخلال‌گر برای حمله کردن به پروتکل پیشنهادی، به یادگیری کلید خصوصی هویّت یکسان نیاز دارد. هر چند می‌دانیم که مشخصهٔ قابلیّت ارتجاع تسهیم کلید نامعلوم با احراز اصالت کلید ضمنی دلالت داشته و از این‌رو اخلال‌گر به آسانی نمی‌تواند به کلید خصوصی دسترسی یابد.

۴.۱.۵ بدون کنترل کلید

در این پروتکل، x و y توسط آلیس و باب به طور تصادفی انتخاب می‌شوند و هویّت دیگری قادر به مجبورکردن کلید جلسه به منظور انتخاب مقدار پیش فرض نمی‌باشد. حال اگر اخلال‌گری از جنس مؤنّث پیام معاوضه شده با چنین فرضی را اصلاح کند آن–گاه آلیس و باب می‌توانند به سختی کلید جلسه یکسان را محاسبه کنند.

۵.۱.۵ امنیت توافق کلید

کشف یک کلید جلسه امن نباید باعث خطر کشف رمز کلیدهای جلسه دیگر شود. بنابراین توافق کلید می‌تواند از کشف رمز کلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار و حمله خودی جلوگیری نماید و همچنین به منظور پایداری در برابر حملهٔ جستجوی جامع برای بازیابی عدد تصادفی محرمانه، اگر اندازه عدد تصادفی بزرگتر از کلید جلسه محرمانه باشد بهتر است. بنابراین به منظور نگهداری اطلاعات محرمانه (کلید جلسه محرمانه) به عدد تصادفی نیاز است چون اگر کلید محرمانه فاش شود آن‌گاه کلیدهای جلسه خطر کشف رمز دارند.

۶.۱.۵ امنیت پیشرو کامل

اگرکلیدهای طولانی دو بخشی کشف رمز شوند یک شخص (به‌جز PKG) می‌تواند K_{AB_1}، K_{BA_1} و $< as_BP, bs_AP, s_As_BP, T_A, T_B, s_A^{-1}, s_B^{-1}, H_1((ID_B||R_B)P_{pub}) >$ محاسبه کند. امّا او نمی‌تواند

K_{AB_2} و K_{BA_2} را بدون شناختن کلید جلسهٔ یکسان توافق شده با $sk = SK_{BA} = SK_{AB}$ محاسبه کند؛ چون به منظور محاسبه‌ی K_{AB_1}، K_{BA_1}، K_{AB_2} و K_{BA_2} در دو طرح پیشنهادی فوق، باید مسئله‌ی سخت محاسبه‌ی دفی–هلمن و معکوس تابع درهم‌ساز حل شود.

۷.۱.۵ امنیت پیشرو PKG

اگر اخلال‌گر کلید اصلی سیستم راPKG به دست آورد به این معناست که اخلال‌گر می‌تواند کلید خصوصی هر دوی آلیس و باب را به دست آورد. امّا هنوز قادر نیست کلید خصوصی را محاسبه کند زیرا حل مسئلهٔ محاسباتی دفی‌هلمن و معکوس تابع درهم‌ساز غیرعملی است.

۸.۱.۵ امنیت داده موقت– معین(ثابت) جلسه معلوم

اگر اخلال‌گر پارامتر a و b محرمانه‌ی جلسه‌ی موقت را شناسایی کند آن‌گاه او می‌تواند فقط $< abP, as_BP, bs_AP, R_{ID} > s_As_BP, s_{ID}$ محاسبه کند امّا نه هردو کلید طولانی. برای محاسبه‌ی s_As_BP، نیاز است حداقل یکی ازکلیدهای خصوصی طولانی آلیس و باب به دست آید که هنوز یک مسئله‌ی سخت محاسباتی دفی–هلمن می‌باشد در این طرح محاسبهٔ K_{AB} یا K_{BA} فقط به دو عملگر اسکالر جمع و دو عملگر اسکالر ضرب نیاز دارد. اگر ما پیش پردازش محاسبه‌ی $R_{ID} + H_1(ID_{ID}||R_{ID})P_{pub})$ را در نظر بگیریم آن‌گاه فقط هزینهٔ محاسباتی یک عملگر اسکالر جمع و یک عملگر اسکالر ضرب نیاز می‌باشد. پس طرح پیشنهادی خیلی کارآمدتر از طرح Cao خواهد بود.

۹.۱.۵ پایداری به حملهٔ اصلاح (تحریف و دستکاری)

در پروتکل پیشنهادی هر پیام احراز هویّت با عدد تصادفی محرمانهٔ جدید و مهر زمانی به همراه تابع درهم‌ساز پشتیبانی می‌شود و بدون عدد تصادفی، مهاجم قادر نبوده مقدار درهم‌ساز صحیحی برای پیام احراز هویّت محاسبه نماید. بنابراین ایجاد یک پیام تحریف شدهٔ موفّق از پیام معتبر بسیار دشوارخواهد بود.

۱۰.۱.۵ پایداری به حملهٔ فاش کلید محرمانهٔ سرور

اگرکلید محرمانهٔ سرور "x" فاش شود، با این‌حال اخلال‌گر نمی‌تواند ID_{ID} و h_{ID} را از $R_{ID} + H_1(ID_{ID}||R_{ID})P_{pub})$ بازیابی نماید. چون به دلیل کاربرد یک روش تابع درهم‌ساز $h(\cdot)$ سرور می‌تواند به آسانی کلید محرمانه‌ی "x" را تغییر و اصلاح کرده و دوباره بازگرداند. یادآوری می‌کنیم فاش شدن کلید محرمانه‌ی سرور خطر کشف رمز کلیدهای جلسه را درپی خواهد داشت.

۱۱.۱.۵ پایداری به حملهٔ فریب سرور

در حملهٔ فریب سرور، یک اخلال‌گر نمی‌تواند به عنوان یک سرور مجاز مبدل شود برای این‌که نمی‌تواند s_As_BP, s_{ID}, R_{ID} را بدون شناسایی ID_{ID}، r_{ID} و x محاسبه نماید. بنابراین سرور نمی‌تواند $sk = SK_{BA} = SK_{AB}$ را بدون شناسایی ID_{ID} محاسبه نماید و همچنین کلید جلسه برای کاربر یکسان در جلسهٔ ورود مختلف متفاوت است. پس طرح در برابر حمله‌ی فریب سرور امن است.

۱۲.۱.۵ پایداری به حملهٔ جلسه موازی

اگر فرض کنیم اخلال‌گر بتواند به عنوان کاربر مجاز U_i با تکرار مجدد پیام درخواست ورود به سیستم $\{ID_A, R_A\}, \{ID_B, R_B, T_B\}$، در چارچوب زمان معتبر مبدل شود امّا در مرحلهٔ بعد اخلال‌گر نمی‌تواند پیام تصدیق $sk = SK_{BA} = SK_{AB}$ را محاسبه نماید؛ زیرا پیام تصدیق شامل هرداده‌ای برای ایجاد مراحل بعدی نمی‌باشد و علاوه براین امنیت پیام احرازاصالت طرح پیشنهادی در برابر حملهٔ جلسه موازی به پیچیدگی محاسباتی لگاریتم گسسته، روش تابع درهم‌ساز، خم بیضوی و پروتکل توافق کلید دفی–هلمن وابسته است.

۱۳.۱.۵ پایداری به حملهٔ خودی

اگر یک خودی مصون سرور، اطلاعات محرمانه‌ی سرور از قبیل $< abP, as_BP, bs_AP, R_{ID} >$ به‌دست آورد. او نمی‌تواند اطلاعات حسّاس مشابه مانند s_As_BP, s_{ID} و $R_{ID}+H_1(ID_{ID}||R_{ID})P_{pub})$ استخراج نماید برای این‌که از نظر محاسباتی معکوس یک روش تابع درهم‌ساز غیر عملی است و علاوه براین، حل‌کردن مسئلهٔ لگاریتم گسسته مشکل است و نیز توافق کلید جلسه می‌تواند از حمله خودی جلوگیری نماید.

۱۴.۱.۵ پایداری به حملهٔ تکرار (اجرای مجدد)

فرض کنیم اخلال‌گر پیام تقاضای ورود به سیستم $\{ID_A, R_A\}$، $\{ID_B, R_B, T_B\}$ از کاربر U_i جعل هویّت کند و بتواند پیام یکسانی را به سرور تکرار نماید. (البتّه این کار به ندرت اتّفاق می‌افتد) هر چند او نمی‌تواند یک حمله اجرای مجدد روی پروتکل احراز اصالت جدید ایجاد نماید زیرا پیام احراز هویّت سرور با اعداد تصادفی و تمبر زمانی ترکیب شده است؛ در این مورد اگر مهاجم یک پیام قدیمی را از طرف سرور اجرای مجدد کند آن‌گاه سرور می‌تواند به آسانی حمله اجرای مجدد را با بررسی پیام ورود به سیستم با عدد تصادفی فعلی و مهر زمان کشف نماید زیرا در هر مرحله عدد تصادفی جدیدی برای هر تقاضای ورود به سیستم جدید انتخاب می‌کند. از این‌رو طرح پیشنهادی در برابر حملهٔ تکرار پایدار است.

۲.۵ مقایسهٔ پروتکل با پروتکل‌های موجود

یک مثال از پروتکل توافق کلید احرازاصالت شده براساس یک شناسه در سبک قابل اجرا، پروتکل پیشنهادی توسط Kudla and Chen [۱۴] می‌باشد. یک بازخورد این پروتکل (و همچنین پروتکل توافق کلید احراز اصالت شده براساس شناسهٔ هوشمند [۱۰]) این می‌باشد که هر دوی آن‌ها مشخصهٔ امنیت کامل پیشرو را فراهم نمی‌کنند. علی‌رغم اینکه Shim [۱۵] در پروتکل پیشنهادی‌اش ادعا می‌کند چنین مشخصه‌ای را فراهم می‌کند. امّا او بعداً در طرح [۱۶] یافت که طرحش به حملهٔ شخص در وسط آسیب‌پذیر است. در سال ۲۰۰۵، Wang [۱۷] یک پروتکل توافق کلید احراز اصالت شده براساس یک شناسهٔ هویّت پیشنهاد کرد که امنیت پیشرو کامل را در سبک قابل‌اجرا بانجام می‌رساند امّا طرح او برای اجرا به ۳ عملگر توان در G، یک ضرب در G و یک جفت‌کننده نیاز داشت. علی رغم این‌که پروتکل ما نیاز دارد که یک عملگر توان در G_T، ۴ عملگر توان در G، و یک جفت‌کننده را اجرا کند. بازدهی محاسباتی دو طرح فوق تقریباً یکسان بوده

و همچنین خیلی کارآمدتر از طرح Cao می‌باشد برای‌این‌که می‌تواند ازکشف رمز کلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار، فریب سرور و حمله خودی جلوگیری کند.

۳.۵ تحلیل هزینه و عملکرد

در طرح پیشنهادی، کلید محرمانهٔ سرور، ID (شناسهٔ هویّت) و خروجی تابع درهم‌ساز همگی به طول ۱۶۰ بیت هستند. تابع درهم‌ساز امن (SHA-1) مقدارهایی به طول ۱۶۰ بیت اجرا می‌کند. همچنین مهر زمانی به طول ۴۰ بیت و شناسه به طول ۳۲ بیت است.

۶ نتیجه‌گیری

امنیت کامل داده موقت- ثابت (معین) جلسه یک ویژگی امن اساسی برای پروتکل‌های توافق کلید احراز اصالت شده به حساب می-آید (در هر دو سبک قابل اجرا و بدون اجرا). ما یک پروتکل توافق کلید احراز اصالت شده براساس یک شناسه ارائه دادیم که در سبک قابل‌اجرا امن می‌باشد و همچنین نشان دادیم که پروتکل پیشنهادی تقریباً همهٔ مشخصه‌های امن شناخته شده، مخصوصاً مشخصهٔ امنیت کامل داده موقت- ثابت (معین) جلسه را با بهره‌وری محاسباتی خوب فراهم می‌کند و نیز در برابر اکثر حملات شناخته شده مقاوم است.

مراجع

[1] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, “Universal designated verifier signatures,” in *Asiacrypt’03*, vol. LNCS 2894, pp. 523-542, 2003.

[2] F. Laguillaumie and D. Vergnaud, “Designated verifier signatures:anonymity and efficient construction from any bilinear map,” IACR eprint.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology: Proc. Crypto’84*, Lecture Notes in Computer Science vol. 196, (Berlin), pp. 47-53, Springer-Verlag, 1985.

[4] A. Shamir, Identity-Based Cryptosystems and Signature Schemes. In: Blakely,G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS Vol. 196, Springer,Heidelberg. pp. 47–53.

[5] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. Proc. of the 11th Annual Asian Computing Science Conference (ASIAN’06), Secure Software and Related Issues, LNCS 4435, Berlin/Heidelberg: Springer-Verlag, pp. 37-44, 2008.

[6] Canetti R, Krawczyk H. Analysis of key exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology (EUROCRYPT’01), LNCS 2045, Berlin/Heidelberg: Springer-Verlag, 2001. pp. 453–474.

[7] Cao Xue-fei, Kou Wei-dong, Fan Kai, Zhang Jun, "An Identity-Based Authenticated Key Agreement Protocol without Bilinear Pairing," Chinese Journal of Electronics & Information Technology 31(5), 2009, pp.1241–1244.

[8] X.F. Cao,W.D. Kou,X.N. Du, "A Pairing-free Identity-Based Authenticated Key Agreement Protocol with minimal Message Exchanges," Information Sciences 180(15), 2010, pp. 2895–2903.

[9] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, Elliptic curve cryptography engineering, Proceedings of the IEEE, 94(2), 2006, pp. 395–406.

[10] N.P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," Electronics Letters, 38(13), pp. 630–632, 2002.

[11] C. Gentry, "Practical identity-based encryption without random oracles," Proc. of the EUROCRYPTO'06, Lecture Notes in Computer Science 4004, Berlin: Springer-Verlag, pp 445–464, 2006.

[12] S.B. Wang, Z.F. Cao, and X.L. Dong, "Provably secure identity-based authenticated key agreement protocols in the standard model," Chinese Journal of Computers 30(1), pp. 1842-1854, 2007.

[13] N. McCullagh, and P.S.L.M. Barreto. "A new two-party identity-based authenticated key agreement," Proc. of CT-RSA 2005, LNCS vol. 3376, Springer-Verlag, New York, pp. 262-274, 2005.

[14] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," Proc. of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society, pp. 219–213, 2002. See also Cryptology ePrint Archive, Report 2002/184.

[15] K. Shim, " Efficient ID-based authenticated key agreement protocol based on the Weil pairing," Electronics Letters 9(8), pp. 653–654, 2003.

[16] H. Sun, and B. Hsieh. "Security analysis of Shim's authenticated key agreement protocols from pairings," Cryptology ePrint Archive, Report 2003/113, 2003. Available at http://eprint.iacr.org/2003/113.

[17] Y. Wang, "Efficient identity-based and authenticated key agreement protocol," Cryptology ePrint Archive, Report 2005/108, 2005. Available at http://eprint.iacr.or

[18] Boyd, C., Choo, K.-K.R.: Security of Two-Party Identity-Based Key Agreement.In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS Vol. 3715, Springer, Heidelberg. pp. 229–243.

[19] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," Proc. of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society, 2002, pp. 219–213.

[20] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security, Okinawa, Japan, 2000.

[21] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. In: Darnell M, ed. Proc. of the 6th IMA International Conference on Cryptography and Coding, LNCS 1355, Berlin/Heidelberg: Springer-Verlag, 1997, pp. 30–45.