تصدیق دیجیتال کلید عمومی برای احراز اصالت کاربر و برقراری کلید جلسه برای ارتباطات شبکه‌ای امن

امیرحسین رحیمی [۱]

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

چکیده

تصدیق دیجیتال کلید عمومی به تنهایی نمی‌تواند به عنوان عاملی امن برای احراز اصالت کاربر به کار رود؛ امّا در ساختار کلید عمومی (PKI) می‌تواند به منظور تأمین احراز اصالت کلید عمومی کاربر و توافق کلید بکار رود. تصدیق دیجیتال تعمیم یافته‌ی (GDC) شامل اطلاعات عمومی کاربر از قبیل: اطلاعات تصدیق‌کننده‌ی دیجیتال کاربر، اطلاعات تصدیق تولّد دیجیتال و اطلاعات عمومی تصدیق اعتبار (گواهینامه) امضای دیجیتال (CA) و غیره می‌باشد؛ یک GDC شامل هر کلید عمومی کاربر نبوده برای این‌که کاربر هر جفت کلید خصوصی و عمومی را در اختیار ندارد. مدیریت کلید در بکارگیری GDC خیلی آسان‌تر از کاربرد تصدیق دیجیتال کلید عمومی بوده و درحقیقت امضای دیجیتال GDC به عنوان یک توکن محرمانه هر کاربر به کار برده می‌شود که به هر تصدیق‌کننده‌ای فاش نمی‌شود؛ در عوض مالک امضای دیجیتال، تصدیق امضایش را با پاسخ‌دهی به چالش تصدیق‌کننده اثبات می‌کند. لذا بر اساس این مفهوم، ما دو پروتکل بر اساس عامل‌یابی عدد صحیح (IF) و لگاریتم گسسته (DL) پیشنهاد می‌کنیم که می‌تواند احراز اصالت کاربر و برقراری کلید محرمانه را به انجام رساند.

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

۱ مقدمه

از گذشته تا حال احراز اصالت کاربرو برقراری کلید جلسه دو سرویس اساسی در ارتباطات امن بوده است و همواره تصدیق دیجیتال کلید عمومی برای احراز اصالت کاربرو برقراری کلید بکار رفته است. یک تصدیق دیجیتال ترکیبی از یک عبارت (شامل کلید عمومی و بعضی اطلاعات عمومی مرتبط به کاربر) و یک امضای دیجیتال عبارت می‌باشد.

هرچند تصدیق دیجیتال کلید عمومی فقط شامل اطلاعات عمومی بوده که می‌تواند به آسانی ثبت شده و یکبار دیگر برگشت داده شود؛ امّا برای احراز اصالت یک کاربر توصیه نمی‌شود. از تصدیق‌های دیجیتال

شناخته شده می‌توان تصدیق دیجیتال کلید عمومی X.509 را نام برد که در بسیاری از موارد در ساختار کلید عمومی (PKI) برای تأمین احراز اصالت کلید عمومی کاربر به‌کار می‌رود.

ما در طرح پیشنهادی شیوهٔ جدیدی معرفی خواهیم کرد که قادراست یک کاربر را احراز اصالت کرده و همچنین یک کلید جلسهٔ تسهیم شدهٔ محرمانه با شریک ارتباطی کاربر را با استفاده از کاربرد تصدیق‌های دیجیتال، از قبیل: یک تصدیق‌کننده دیجیتال (برنامه راه‌انداز)، یک تصدیق تولّد دیجیتال یا یک ID دیجیتال و غیره برقرار کند. این نوع تصدیق دیجیتال به عنوان یک تصدیق دیجیتال تعمیم یافتهٔ (GDC) شناخته می‌شود و همچنین توصیهٔ کاربرد این نوع تصدیق دیجیتال برای مدیریت تصدیق‌های دیجیتال کلید عمومی X.509 خیلی آسان‌تر می‌باشد.

تصدیق دیجیتال تعمیم‌یافتهٔ (GDC) به عنوان عاملی امن برای تأمین احراز اصالت کاربر می‌باشد که شامل اطلاعات عمومی کاربر (کاربر هرجفت کلید خصوصی و کلید عمومی را در دسترس ندارد) و یک امضای دیجیتال اطلاعات عمومی بوده که توسط مرکز صدور گواهینامهٔ مورد اعتماد CA امضا می‌شود. علاوه بر این مالک GDC نمی‌تواند متن اصلی امضای GDC را به هرتصدیق‌کننده‌ای فاش کند درعوض می‌تواند با یک کلید جلسهٔ محرمانه پاسخ به چالش تصدیق‌کننده را برآورد کند زیرا او تصدیق امضای دیجیتال را در دسترس دارد. پس به طورکلی امضای دیجیتال GDC به عنوان یک توکن محرمانهٔ هرکاربر برای احراز اصالت امن کاربر بکاربرده می‌شود.

تفاوت بین تصدیق دیجیتال تعمیم یافتهٔ (GDC) و تصدیق دیجیتال کلید عمومی این است که در یک GDC اطلاعات عمومی شامل هرکلید عمومی کاربر نمی‌باشد.

سه هویّت اساسی وکاربردی تصدیق دیجیتال عبارتند از:

۱. اعتبار تصدیق مرکز صدورگواهینامه (CA): CA شخص مورد اعتماد یا سازمان صلاحیت‌دار که به صورت دیجیتال یک دستور (عبارت) را با کلید خصوصی مالکش امضاء می‌کند.

۲. مالکیّت یک تصدیق دیجیتال تعمیم یافته (GDC): مالکیّت (GDC) شخصی است که (GDC) را از یک مرکز صدورگواهی مورداعتماد رویCA یک کانال امن دریافت می‌کند وهمچنین به محاسبهٔ یک «جواب» معتبردر پاسخ به چالش «سؤال» تصدیق‌گر به منظور احراز اصالت و برقراری یک کلید جلسهٔ محرمانه نیاز دارد.

۳. تصدیق‌کننده: تصدیق‌کننده شخصی است که مالک GDC را به چالش می‌کشاند و پاسخ را با به‌کار بردن اطلاعات عمومی مالک و کلید عمومی CA تأیید اعتبار می‌نماید.

دراکثر تحقیقات ثبت شده در زمینهٔ کاربردهای احراز هویّت کاربر، یک مقام صلاحیت‌دار مورد اعتماد برای صدورکارت تعیین هویّت با اطلاعات کاربری، ازقبیل نام‌کاربری و یک عکس شخصی روی کارت، برای هرکاربر مسئول بوده و هر کاربر می‌تواند بر اساس این اطلاعات کاربری با موفقیّت تعیین هویّت شود اگر همواره مالک مجاز کارت باشد.

جدول ۱: نمادگذاری‌ها

نماد	تعریف	نماد	تعریف
ID	شناسه‌ی هویّت کاربر	$\oplus$	عملگر XOR
Z_P^*	گروه ضربی p	Z_q	حلقه صحیح به پیمانه q
R_A	عدد تصادفی تولیدشده توسط A	T_A	مهر زمان کاربر A
DVS	امضاهای تصدیق‌کننده طراحی شده	$H(\cdot)$	تابع درهم‌ساز امن
GDC	تصدیق دیجیتال تعمیم‌یافته	$\|$	عملیات الحاق
DHA	فرض دفی-هلمن	$GDHA$	فرض دفی-هلمن تعمیم‌یافته
p و q	دو عدد اول بزرگ به‌طوری‌که $p = ۲q + ۱$	$H(\cdot)$	تابع درهم‌ساز امن
PKI	ساختار کلید عمومی	PKG	مولد کلید خصوصی
CA	مرکز صدور گواهینامه	m_A	چکیده پیام
DL	لگاریتم گسسته	IF	پروتکل برقراری کلید و عامل‌یابی عددصحیح
x_A	کلید خصوصی	y_A	کلید عمومی

در بخش بعدی، ما محاسن و معایب طرح‌های مرتبط گذشته را بررسی خواهیم کرد. در بخش ۳ بعضی مقدمات در زمینهٔ تصدیق دیجیتال را معرفی خواهیم کرد و همچنین احراز اصالت کاربر مبتنی بر لگاریتم گسسته (DL) و پروتکل برقراری کلید را با کاربرد GDC تشریح خواهیم کرد. در بخش ۴ احراز اصالت کاربر را بر اساس عامل‌یابی عدد صحیح و پروتکل برقراری کلید (IF) بیان خواهیم کرد و در نهایت نتیجه‌گیری را در بخش ۵ خواهیم داشت.

۲ کارهای مرتبط

درگذشته یک امضای دیجیتال سنتی به منظور احراز اصالت یک پیام معین برای دریافت‌کنندهٔ امضا به کارمی‌رفت. هرچند در این روش گاهی اوقات کلید خصوصی امضاءکننده مختل می‌شد چون گاهی اوقات یک دریافت کنندهٔ معاند می‌توانست به راحتی امضای دیجیتال ارسال‌کننده را به هر بخش سوّمی بدون موافقت ارسال‌کننده فاش کند و به دنبال آن هر شخصی می‌توانست به کلید عمومی امضاءکننده و امضای دیجیتال معتبر دسترسی یابد.

در سال ۱۹۸۹، Chaum و Antwerpen [۵] نظریهٔ امضای انکارناپذیر را معرفی کردند؛ نظریه آن‌ها امضاءکننده را به دستیابی کنترل کامل روی امضایش قادر ساخته وعلاوه براین برای تصدیق یک امضای انکارناپذیر به تسهیم امضای پیام نیاز داشت. هرچند این روند می‌توانست تصدیق‌کننده‌های نامطلوب را از اعتبار دادن امضاء جلوگیری نماید امّا مسئلهٔ واقعی انکارناپذیری امضا این بود که امضاءکننده به اعتباردهی تصدیق‌کننده نیاز داشت قبل از این‌که تصدیق کننده برای تأیید اعتبار امضای انکارناپذیر کمک کند.

امضاهای تصدیق‌کننده طراحی شده Designated Verifier Signature (DVS) به‌طور مستقل ابتدا توسط M. Jakobsson، K. Sako، و R. Impagliazzo [۶] و بعداً توسط D. Chaum [۷] هر دو در ۱۹۹۶ معرفی شدند. همواره یک DVS، احراز اصالت یک پیام معین را به یک تصدیق‌کنندهٔ معین فراهم کرده و ویژگی بارز DVS این است که یک DVS معتبر می‌تواند توسط امضاءکنندهٔ «واقعی» یا توسط تصدیق‌کنندهٔ طراحی شده ایجاد شود با این ویژگی منحصربه فرد، یک DVS از یک امضای دیجیتال سنتی در دو جنبه متمایز است: (۱) تصدیق‌کنندهٔ طراحی شده متقاعد است که DVS توسط امضاکنندهٔ واقعی ایجاد می‌شود نه توسط خود تصدیق‌کننده. هرچند امضای دیجیتال سنتی می‌تواند توسط هر تصدیق‌کننده‌ای برای DVS تصدیق شود بدون کمک بخش سوّمی که همواره می‌تواند امضا کننده واقعی DVS را حتّی با شناسایی کلید خصوصی تعیین کند. (۲) یک DVS احراز اصالت یک پیام معین را بدون هیچ ویژگی انکارامضای دیجیتال سنتی فراهم می‌کند. البتّه یک DVS می‌تواند امضای دیجیتال سنتی را در اکثر کاربردهای اساسی جایگزین کرده و خدماتی با توانایی انکارپذیری فراهم نماید.

درطرح M. Jakobsson، K. Sako، و R. Impagliazzo [۶] یک DVS بر اساس یک طرح امضای انکارناپذیر نامتقابل با یک الزام محدود پیشنهاد شده است امّا این طرح به‌طور محاسباتی کامل نمی‌باشد.

در ۲۰۰۳، S. Saeednia، S. Kremer، و O. Markowitch [۸] یک طرح DVS بر اساس لگاریتم گسسته مبتنی ترکیب امضای اچنور (Schnorr [۹]) و امضای Zheng [۱۰] پیشنهاد کردند. البتّه اخیراً طرح‌های DVS بر اساس هر دو رویه پیشنهاد می‌شوند. UDVS (DVS جامع) یک امضای دیجیتال متداول با عاملیّت اضافی بوده که اجازه می‌دهد یک امضای دیجیتال به انتخاب امضاء درون DVS هر تصدیق‌کننده میسر شود. ساختار یک طرح UDVS، (DVSBM) بر اساس یک طرح دو سویه است. سه ساختار جدید UDVS بر اساس امضای Schnorr [۹] و RSA [۲] در طرح R. Steinfeld، H. Wang و J. Pieprzyk [۱۱] پیشنهاد شده است. همچنین UDVS بر اساس امضای الجمال در طرح F. Laguillaumie و D. Vergnaud [۱۲] پیشنهاد گردید.

سه هوّیت مستقل در هرکاربرد UDVS وجود دارد: (۱) مرکز صدورگواهی CA، (۲) مالک امضای دیجیتال، (۳) تصدیق‌کننده طراحی شده. در یک UDVS، مالک به تبدیل کردن امضای دیجیتال درون یک DVS نامتقابل (بدون فعل و انفعال) به منظور اعتبار دهی یک پیام نیاز دارد. همچنین یک گواهی‌نامهٔ دیجیتال به همراه یک تصدیق‌کننده به منظور اثبات کردن تصدیق گواهی‌نامهٔ دیجیتال نیاز بوده که توسط تصدیق‌کننده احراز اصالت می‌شوند.

طرح پیشنهادی ما بر اساس طرح پیشنهادی A. Shamir [۲۳] مبتنی بر ID و با کاربرد مسئلهٔ لگاریتم گسسته (DL) و فرض دفی–هلمن (DHA) پایه‌ریزی شده است؛ در الگوریتم‌های رمزنگاری بر اساس ID هرکاربر به ثبت در یک مولّد کلید خصوصی (PKG) و تشخیص هویّت خودش قبل از پیوستن به شبکه نیاز دارد به همین منظور PKG یک کلید خصوصی برای کاربر ایجاد کرده و شناسهٔ هوّیت کاربر (به‌طور مثال نام کاربری یا آدرس ایمیل) متناظر کلید عمومی خواهد بود. همچنین در این روش یک کاربر فقط به شناخت «شناسهٔ هوّیت» شریک ارتباطی‌اش و کلید عمومی (PKG) نیاز دارد. هرچند در یک الگوریتم رمزنگاری بر اساس ID فرض می‌شود که هر کاربر شناسهٔ هوّیت شریک ارتباطی‌اش را بشناسد؛ امّا بر اساس این فرض

هیچ یک از روش‌های عملی به اعتباردهی شناسه هویّت نیازی ندارند. این یکی از مزیّت‌های اصلی رمزنگاری بر اساس ID می‌باشد. اطلاعات عمومی GDC از قبیل شناسه هویّت کاربر می‌تواند منتقل شود و توسط هر هویّت ارتباطی بررسی شود همچنین از این اطلاعات برای اعتباردهی یکدیگر نیز استفاده می‌شود؛ از کاربردهای دیگرطرح پیشنهادی مبتنی PKI به‌کارگیری درحوزه اینترنت وتجارت الکترونیک می‌باشد که در آن هویّت‌های ارتباطی به شناختن ارتباطات قبلی یکدیگر نیاز ندارند که راه‌حل پیشنهادی ما در این حوزه مبتنی امنیت پیشرو، ترکیب طرح امضای دیجیتال متداول و طرح تعمیم‌یافتهٔ فرض دفی-هلمن می‌باشد که علاوه براین می‌توان درطرح پیشنهادی از سیستم رمزنگاری نامتقارن به‌همراه سیستم DVS و گواهی دیجیتال نیز بهره برد.

۳ پروتکل پیشنهادی بر اساس لگاریتم گسسته (DL)

۱.۳ مقدمه

یک تصدیق (گواهی‌نامه) کاغذی می‌تواند به عنوان یک عملگراحراز اصالت کاربر به‌کار برده شود. امّا یک تصدیق دیجیتال کلید عمومی نمی‌تواند به عنوان یک عملگر احراز اصالت در کاربردهای شبکه به‌کار برده شود؛ برای این‌که یک تصدیق چاپی نمی‌تواند به‌آسانی جعل یا کپی شود. امّا یک تصدیق دیجیتال کلید عمومی می‌تواند به‌آسانی ثبت شده و شروع مجدد گردد.

در طرح پیشنهادی مالک تصدیق دیجیتال تعمیم‌یافتهٔ GDC اصلاً به آشکارسازی متن اصلی امضای دیجیتال GDC برای تصدیق‌کننده نیاز ندارد؛ درعوض مالک GDC فقط برای تصدیق امضای دیجیتال به احراز اصالت بر اساس چالش / پاسخ نیاز دارد و تصدیق امضای دیجیتال روی GDC می‌تواند احراز اصالت کاربر را نیز فراهم کند. پروتکل پیشنهادی برای تصدیق امضای دیجیتال بر اساس مسئلهٔ لگاریتم گسسته (DL) و فرض دفی-هلمن (DHA) پایه‌ریزی شده و همچنین باید برای احراز اصالت کاربر نیازمندی‌های امن زیر را ایفا نماید.

۱) Unforgeability (غیرقابل جعل بودن): یک پاسخ معتبر می‌تواند فقط توسط مالکیّت تصدیق ایجاد شود. (کسی که امضای دیجیتال GDC می‌شناسد.)

۲) One-Wayness (روش مرسوم تابع درهم‌ساز و الحاق): هیچ شخص سوّمی نمی‌تواند تصدیق امضای دیجیتال را بر اساس روش فعل و انفعال (برهم‌کنش) به‌دست آورد؛ زیرا معکوس تابع درهم‌ساز غیرعملی است.

۳) Nontransferrability (غیرقابل انتقال‌پذیری): در احراز اصالت بر اساس (چالش/پاسخ) یک پاسخ به چالش تصدیق‌کننده را نمی‌توان در پاسخ انتقال یافتهٔ دیگری به چالش دیگر تصدیق‌کننده به‌کار برد؛ چون در غیر این صورت زمینهٔ جعل هوّیت کاربر ایجاد می‌شود.

۲.۳ بررسی امضای دیجیتال الجمال

در طرح الجمال [۳] یک عدد اوّل بزرگ p و یک مولّد g ازمرتبهٔ $p-1$ برای تسهیم همهٔ کاربرها فرض می‌شود و امضاءکننده یک کلید خصوصی تصادفی $x \in [1, p-2]$ انتخاب کرده و کلید عمومی متناظر $y = g^x \bmod p$ را محاسبه می‌کند. پس از آن امضاءکننده به‌طور تصادفی یک پارامتر محرمانهٔ $k \in [1, p-1]$ را با فرض $\gcd(k, p-1) = 1$ انتخاب کرده و $r = g^k \bmod p$ محاسبه می‌کند، سپس با شناسایی امضای محرمانه s، کلید خصوصی x و پارامتر k چکیده پیام $m = ks + rx \bmod p - 1$ (۱) محاسبه می‌شود و به‌دنبال آن پیام m' نیز محاسبه می‌شود. سپس (r, s) به‌عنوان امضای دیجیتال پیام m' تعریف شده و امضای (r, s) می‌تواند تصدیق شود با بررسی این که آیا معادلهٔ $g^m = y^r r^s \bmod p$ (۲) صحیح می‌باشد.

دریک طرح امضای الجمال، پارامتر r امضاء می‌تواند آفلاین به‌صورت $r = g^k \bmod p$ محاسبه شده و همچنین مؤلّفهٔ s امضاء به‌صورت آنلاین محاسبه می‌شود در نتیجه برای همهٔ طرح‌های امضاء بر اساس مسئلهٔ لگاریتم گسسته DL معادلهٔ تعمیم‌یافتهٔ امضاءکننده را می‌توان به‌عنوان $ax = bk + c \bmod p - 1$ محاسبه کرد جائی که (a, b, c) سه پارامتر از مجموعهٔ مقدارهای (m, r, s) بوده و به‌طور واضح هر پارامتر می‌تواند یک ترکیب ریاضیاتی (m, r, s) باشد. برای مثال پارامتر a می‌تواند با m ،r یا s جایگزین شود درنتیجه معادلهٔ تصدیق به صورت $y^a = r^b g^c \bmod p$ تعیین خواهد شد.

۳.۳ فرض دفی-هلمن Diffe-Hellman Assumption (DHA)

به‌فرض دو شخص A و B به ترتیب کلید خصوصی x_A و x_B و متناظر آن‌ها کلیدهای عمومی $y_A = g^{x_A} \bmod p$ و $y_B = g^{x_B} \bmod p$ را در اختیار داشته باشند؛ جائی که p یک عدد اوّل صحیح بزرگ و g یک عضو اوّل گروه جمعی به پیمانهٔ p باشد. آن‌گاه فقط شخص A و B می‌توانند یک تسهیم محرمانهٔ $K_{A,B} = y_B^{x_A} = y_A^{x_B} = K_{B,A} \bmod p$ را محاسبه کنند. فرض دفی-هلمن [۱] DHA به فرضی رجوع می‌کند که به طورمحاسباتی برای تعیین $K_{A,B}$ بدون شناختن کلید خصوصی x_A یا x_B غیرعملی خواهد بود. زیرا سختی حل کردن مسئلهٔ کلید خصوصی x_A یا x_B از کلید عمومی متناظر y_A یا y_B به‌سختی حل مسئلهٔ لگاریتم گسسته وابسته می‌باشد.

۱.۳.۳ پروتکل برقراری کلید و احراز اصالت کاربر

۱) ثبت در CA: به‌فرض A مالک تصدیق و B تصدیق‌کننده باشد. شخص A به ثبت شدن در یک مرکز صدورگواهینامه CA برای بدست آوردن یک GDC نیاز دارد. CA یک امضای الجمال (r_A, s_A) را برای دستور Aام کاربر m'_A بر اساس معادلهٔ (۱) ایجاد کرده و m_A چکیده پیام عبارت (دستور) m'_A می‌باشد. از آن جائی که مؤلّفهٔ r_A امضاء یک عدد صحیح تصادفی بوده و به m_A وابسته نمی‌باشد پس به نگهداری محرمانه نیاز ندارد. هرچند مؤلّفهٔ s_A امضاء یک تابع دستوری بوده و هر مالک به نگهداری محرمانهٔ آن از تصدیق‌کننده در فرآیند احراز اصالت نیاز دارد. احراز اصالت کاربر و پروتکل برقراری کلید در شکل ۱ نشان داده می‌شود.

۲) پروتکل: پروتکل احراز اصالت و برقراری کلید شامل ۴ مرحله است:

۱. کاربر A اطلاعات کاربریش m'_A و پارامترهای (r_A, S_A) را به تصدیق‌کنندهٔ B انتقال می‌دهد جائی که $S_A = r_A^{s_A} \bmod p$.

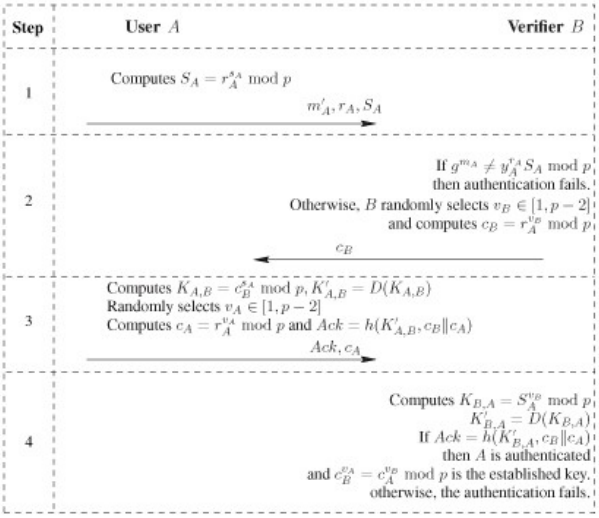
۲. تصدیق‌کننده بعد از دریافت m'_A و (r_A, S_A) بررسی می‌کند که آیا $g^{m_A} = y^{r_A} S_A \bmod p$ (۳) صحیح می‌باشد. جائی که y کلید عمومی CA می‌باشد. اگر این برابری، صحیح حفظ شود ابتدا تصدیق‌کنندهٔ B به‌طور تصادفی یک عدد صحیح $v_B \in [۱, p-۲]$ انتخاب می‌کند، سپس یک چالش $c_B = r_A^{v_B} \bmod p$ محاسبه کرده و c_B را به کاربر A ارسال می‌کند؛ درغیر این‌صورت احراز اصالت کاربر شکست خورده و پروتکل متوقف می‌شود.

۳. کاربر A ابتدا s_A محرمانه‌اش را برای محاسبهٔ کلید محرمانهٔ دفی–هلمن $K_{A,B} = c_B^{S_A} \bmod p$ و $K'_{A,B} = D(K_{A,B})$ به‌کار می‌گیرد جائی که $D(K_{A,B})$ یک روند استخراج کلید با $K_{A,B}$ به‌عنوان یک ورودی ارائه می‌دهد. سپس کاربر A به‌طور تصادفی یک عدد صحیح $v_A \in [۱, p-۲]$ انتخاب می‌کند و $c_A = r_A^{v_A} \bmod p$ محاسبه کرده و $Ack = h(K'_{A,B}, c_B||c_A)$ پاسخ می‌دهد جائی که $h(K'_{A,B}, c_B||c_A)$ یک روش تابع کلید هش شده تحت کلید $K'_{A,B}$ ارائه می‌دهد. کاربر A، Ack و c_A را دربرگشت به B ارسال می‌کند.

۴. تصدیق‌کنندهٔ B بعد از دریافت کردن Ack و c_A از کاربر A، v_B محرمانه‌اش را برای محاسبهٔ کلید محرمانهٔ تسهیم شده دفی–هلمن $K_{B,A} = S_A^{v_B} \bmod p$ و $K'_{B,A} = D(K_{A,B})$ به‌کار گرفته و بررسی می‌کند که آیا $Ack = h(K'_{B,A}, c_B||c_A)$ صحیح است. اگر این تصدیق موّفق باشد، مالک تصدیق A، توسط تصدیق‌کنندهٔ B احراز اصالت شده و یک کلید جلسهٔ محرمانهٔ یکبار مصرف $c_B^{v_A} = r_A^{v_A v_R} = c_A^{v_R} \bmod p$ بین کاربر A و B تسهیم می‌شود. این کلید تسهیم شده می‌تواند امنیت پیشروی کامل را فراهم کند.

در پروتکل پیشنهادی مالک تصدیق، به منظور احراز اصالت موّفق با تصدیق‌کننده به محاسبه و ارسال یک جفت معتبر (r_A, S_A) و Ack به تصدیق‌کننده درگام ۱ و ۳ نیاز دارد. پارامترهای (r_A, S_A) به تصدیق کردن $g^{m_A} = y^{r_A} S_A \bmod p$ نیاز دارند. این جفت عدد صحیح می‌تواند به آسانی توسط هرکسی محاسبه شود. هرچند نشان خواهیم داد که فقط مالک تصدیق A، مؤلّفهٔ محرمانهٔ S_A را برای محاسبهٔ یک Ack معتبر می‌شناسد؛ برای این‌که تصدیق‌کنندهٔ B می‌تواند کلید محرمانهٔ یکبار مصرف $K_{B,A}$ را به‌عنوان $K_{B,A} = S_A^{v_B} = r_A^{S_A v_B} \bmod p$ محاسبه کرده تا برای ایجاد Ack بکارگیرد.

بر اساس فرض دفی–هلمن DHA، مالک تصدیق A کسی است که مؤلّفهٔ محرمانه S_A را می‌شناسد و همچنین می‌تواند $K_{A,B}$ را به عنوان $K_{A,B} = c_B^{S_A} = r_A^{S_A v_B} = K_{B,A} \bmod p$ محاسبه کند بنابراین مالک تصدیق می‌تواند فعل و انفعال با تصدیق‌کننده داشته و با موفّقیّت احراز اصالت شود.



شکل ۱: پروتکل توافق کلید و احراز اصالت بر اساس DL

۴ طرح پیشنهادی

از آن جائی که احراز اصالت کاربر و برقراری کلید دو سرویس اساسی در ارتباطات امن می‌باشد از این‌رو ما طرحی بر اساس تصدیق دیجیتال کلید عمومی ID با پروتکل برقراری کلید با کاربرد GDC (تصدیق دیجیتال تعمیم‌یافته) را به‌همراه سیستم احراز اصالت کاربر مبتنی لگاریتم گسسته DL (با فرض دفی-هلمن) و پروتکل عامل‌یابی عدد صحیح (IF) برای برقراری و تسهیم کلید جلسهٔ محرمانه پیشنهاد می‌کنیم که ویژگی‌های زیر را ایفا می‌کند:

۱. غیر قابل انکارپذیری (Non-Repudiation)

۲. غیر قابل انتقال‌پذیر (Nontransferrability)

۳. غیر قابل جعل‌پذیری (Unforgeability)

۴. استفاده از چکیده پیام و خروجی تابع درهم‌ساز برای امضاء: درتابع درهم‌ساز با ورودی معین a محاسبهٔ $h(a) = b$ آسان می‌باشد ولی با b معین، به‌آسانی نمی‌توان $h^{-1}(b) = a$ را محاسبه کرد (معکوس تابع درهم‌ساز با عملگر معکوس اجراء نشدنی است).

۵. داده‌ها در فرم متن اصلی روی شبکه منتقل نمی‌شوند «گمنامی کاربر و پایداری در برابر حملهٔ تحریف و دستکاری».

۶. پایداری در برابر تصادم و مقاوم به خطر کشف رمز اطلاعات ذخیره شده درکارت هوشمند توسط اخلال‌گر «مقاوم به حملات کانال جانبی».

۷. جدول تصدیق امضا درون سرور ذخیره نمی‌شود «سربار سرور برای احراز اصالت کاهش می‌یابد». چون سرور فقط کلید محرمانه را نگهداری می‌کند.

۸. پشتیبانی از سیستم احراز اصالت متقابل (کاربر/ سرور) با توافق کلید جلسه تصدیق شده. توافق کلید می‌تواند ازحملهٔ خودی، حملهٔ تکرار، حملهٔ جلسه موازی، انعکاس، حملهٔ شخص در وسط جلوگیری نماید؛ برای پایداری در برابر برخی حملات، اگراندازه عدد تصادفی بزرگتر ازکلید محرمانهٔ باشد؛ بهتر است. پس به منظور نگهداری اطلاعات (کلید) محرمانه به عدد تصادفی نیاز است. اگر کلید محرمانه فاش شود آن‌گاه کلیدهای جلسه خطرکشف رمز دارند. حفظ گمنامی کاربر از ویژگی‌های بارز احراز اصالت متقابل به شمار می‌رود. در پروتکل پیشنهادی ترکیب یک عدد تصادفی "Nonce" با مهر زمانی و مقدار درهم‌ساز، از پیام احراز اصالت در برابر حملهٔ جلسه موازی محافظت می‌نماید از کلید جلسه به منظور نگهداری اطلاعات محرمانه استفاده می شود. بنابراین طرح پیشنهادی در برابر حملهٔ جلسه موازی امن است. فاش کلید محرمانهٔ سرور خطر کشف رمزکلیدهای جلسه را در پی خواهد داشت. بکارگیری یک عدد تصادفی یا مسئلهٔ همزمانی (مهر زمانی) $T' - T \leq \Delta T$ باعث می‌شود طرح در برابر حملهٔ جعل و حملهٔ تکرار مقاومت کند.

۹. به عنوان سامانه‌ای امن با ثُبات عملیاتی بالا با کاربرد تصدیق گواهی‌نامه دیجیتال برای تبادل داده در تراکنش‌های بانکی، سیستم‌های پرداخت الکترونیکی، هویّت الکترونیکی، سسیتم‌های دفاعی و الکترونیکی، سیستم اتوماسیون اداری، درکارت‌های هوشمند و تراشه‌های الکترونیکی به کار می‌رود.

۱۰. هزینهٔ محاسباتی و ارتباطی معقول و نحوهٔ ذخیره‌سازی مؤثّر «به‌دلیل کاربرد توابع درهم‌ساز و کارت هوشمند» هرچند کاربرد الگوریتم کلید نامتقارن سرعت بالایی ندارد برای این‌که در هر زمان محاسبات توان پیمانه‌ای که جز عملگر پیچیدگی می‌باشد را شامل می‌کند.

۱۱. طرح پیشنهادی مبتنی هردو مشخصهٔ لگاریتم گسسته «روی میدان متناهی» و تابع درهم‌ساز امن می‌تواند بیشتر حملات آنلاین وآفلاین شناخته شده از قبیل: حملهٔ تکرار، حملهٔ کانال جانبی، حملهٔ خارجی، حملهٔ جعل امضاء، حملهٔ حدس، حملهٔ خودی، حملهٔ تحریف و دستکاری پیام‌ها و داده‌ها (حمله مبتنی بر پیام آشکار)، حملهٔ جعل هویّت، حملهٔ جلسه موازی، حملات اخلال درسرویس، حملهٔ فریب سرور و حملهٔ فریب مرکز ثبت، حملهٔ کارت هوشمند مسروقه، حملهٔ کاربر مبدل شده، حملهٔ سرور، حملهٔ کلید معلوم، حملهٔ لغت‌نامه‌ای، حملهٔ یافتن کلید در نواحی آنتروپی بالا، حملهٔ آزمایش و خطا روی سیستم‌های رمزنگاری، حملهٔ بازیابی متن اصلی و حمله معکوس XOR را با هزینهٔ محاسباتی معقول محدود نماید.

۱.۴ تحلیل امنیتی طرح پیشنهادی

تمام مکانیزم‌های رمزنگاری وگواهینامهٔ دیجیتالی و روش‌های قدرتمند احراز هویّت، برای پیشگیری از دسترسی متجاوزین به حریم منابع سیستم و بهره‌برداری غیرمجاز از داده‌ها ابداع شده‌اند. اغلب این مکانیزم‌ها از لحاظ عملی غیرقابل نفوذ و مطمئن هستند ولی آیا این مکانیزم‌ها، امنیت صددرصد داده‌ها را تضمین می‌کنند؟ چگونه ممکن است که از پنجاه سال قبل تاکنون هنور یک مورد ضعیف بنیادی در روش رمزنگاری RSA [۲] گزارش نشده ولی در هر روز ده‌ها مورد از نفوذ در شبکه و وب سایت‌ها به گوش می‌رسد! شاید از خود بپرسیم که پس این مکانیزم‌ها به چه کارمی‌آیند؟ جواب بدیهی است: این مکانیزم‌ها لازمند ولی کافی نیستند! ازاین‌رو امنیت پروتکل پیشنهادی ما بر اساس ترکیب امن امضای RSA، به‌سختی محاسبهٔ لگاریتم گسسته، پایداری تصادم یک روش تابع درهم‌ساز (برای نگهداری کلید محرمانه) و GDHA تکیه می‌کند. همچنین مسئلهٔ لگاریتم گسسته هنوز یک مسألهٔ باز است و خیلی امن‌تر از روش تابع درهم‌ساز پیشنهاد می‌شود؛ هرچند به دست آوردن معکوس تابع درهم‌ساز هم غیرعملی بوده و می‌توان از آن به عنوان ابزاری برای نگهداری کلید محرمانه (درسرور) در برابرحمله‌های شناخته شده استفاده نمود. البتّه می‌توان استفاده از توافق کلید دفی-هلمن [۱] را نیز در شبکه‌های ناامن توصیه کرد؛ از این‌رو سیستم رمزنگاری طرح پیشنهادی ما مبتنی هر دو مشخصهٔ مسئله لگاریتم گسسته «روی میدان متناهی» و امنیت یک روش تابع درهم‌ساز، می‌تواند اکثر حمله‌های شناخته شده از قبیل: حملهٔ تکرار، حملهٔ کانال جانبی، حملهٔ خارجی، حملهٔ جعل امضاء، حملهٔ حدس، حملهٔ خودی، حملهٔ تحریف و دستکاری پیام‌ها و داده‌ها (حمله مبتنی بر پیام آشکار)، حملهٔ جعل هویّت، حملهٔ جلسه موازی، حملات اخلال درسرویس، حملهٔ فریب سرور و حملهٔ فریب مرکز ثبت، حملهٔ کارت هوشمند مسروقه، حملهٔ کاربر مبدل شده، حملهٔ سرور، حملهٔ کلید معلوم، حملهٔ لغت‌نامه‌ای، حملهٔ یافتن کلید در نواحی آنتروپی بالا، حملهٔ آزمایش و خطا روی سیستم‌های رمزنگاری، حملهٔ بازیابی متن اصلی و حملهٔ معکوس XOR را با هزینهٔ محاسباتی معقول محدود نماید. البتّه حمله‌های حدس آنلاین را نیز می‌توان به آسانی با محدود کردن تعداد ورود به سیستم مردود شده، جلوگیری کرد.

از این‌رو با توجّه به تحلیل و مقایسهٔ عملکرد طرح‌های مرتبط و بررسی حفره‌های آسیب‌پذیری آن‌ها، می‌توان امنیت بالا، هزینهٔ ارتباطی پایین و پایداری به انواع حمله‌های آسیب‌پذیر را برای این طرح پیشنهادی وعده داد.

۱.۱.۴ حملات به امضای الکترونیک

رایوست، حملات ممکن در مورد امضای الکترونیک را بر اساس اطلاعاتی که مهاجم در اختیار دارد؛ به دو دسته کلی تقسیم نموده است.

۱. حملات کلید (Key-Only Attack): حملاتی که درآن‌ها مهاجم تنها از کلید عمومی صاحب امضا با خبر است و در واقع تنها می‌تواند صحت یک امضای الکترونیک را کنترل کند.

۲. حملات مبتنی بر پیام (Message Attack): حملاتی که در آن‌ها مهاجم علاوه برکلید عمومی صاحب امضا، نمونه‌هایی از متن‌های عادی و معادل امضاء شده آن را نیز در اختیار دارد.

هریک از این قسم حملات ممکن است به شکست سیستم امضای الکترونیک منتهی شود؛ شکست یک سیستم امضای الکترونیک دارای تعابیر مختلفی است.

۱. شکست کامل (Total Break): شکست کامل به معنای آن است که کلید خصوصی امضاء کننده کاملاً فاش شود.

۲. جعل عمومی (Universal Forgery): جعل عمومی از طریقی محقق می‌گردد که در آن مهاجم از کلید خصوصی بی‌خبر است امّا می‌تواند هر پیام دلخواه را بصورت معتبر از سوی صاحب اصلی امضاء کند.

۳. جعل انتخابی (Selective Forgery): جعل انتخابی به معنای آن است که مهاجم می‌تواند تنها مجموعه محدودی از پیام‌ها که از پیش تعیین شده را امضا کند.

۴. جعل وجودی (Existential Forgery): جعل وجودی بدین معنا است که مهاجم می‌تواند دست کم یک پیام را که از قبل قابل تعیین نیست به طور موّفقیّت‌آمیز و معتبر از طرف صاحب اصلی امضاء کند، از آن‌جائیکه در این روش مهاجم چندان کنترلی بر روی پیام‌های امضاء شده معتبر ندارد؛ احتمال آن‌که پیام امضاء شده‌ای که تولید می‌کند پیامی با مفهوم و معنادار باشد بسیار اندک است بنابراین این نوع از شکست‌ها عملاً دشواری به بار نمی‌آورند و چندان با اهمیّت نیستند.

۲.۱.۴ تحلیل امنیتی پروتکل استقرار کلید و احراز اصالت کاربر

دراین بخش، ما امنیت پیشنهادی پروتکل استقرار کلید و احراز اصالت کاربر را به منظور توانایی غیرقابل جعل به همراه غیرقابل انتقال‌پذیری بر اساس یک روش تابع درهم‌ساز، مسئلهٔ لگاریتم گسسته و فرض دفی–هلمن تحلیل خواهیم کرد.

توانایی غیرقابل جعل: اخلال‌گر به منظور اجرای یک حملهٔ خارجی، به ارائه دادن یک جفت معتبر (r_A, S_A) درگام ۱ پروتکل و متناظر Ack درگام ۳ پروتکل برای جعل هویّت موّفق مالک تصدیق نیاز دارد. یک جفت معتبر (r_A, S_A) به‌تنهایی درگام ۱ نمی‌تواند برای احراز اصالت کردن مالکیّت تصدیق بکاربرده شود؛ لذا این جفت پارامتر می‌تواند به آسانی توسط اخلال‌گر از معادلهٔ ۳ به دست آید. امّا به طور محاسباتی حل لگاریتم گسسته S_A توسط اخلال‌گر غیر عملی بوده و همچنین طرح امضای الجمال امن می‌باشد. بنابراین از بُعد محاسباتی به‌دست آوردن جفت (r_A, s_A) توسط اخلال‌گر برای تصدیق کردن در معادلهٔ $g^{m_A} = y^{r_A} r_A^{s_A} \bmod p$ غیرعملی بوده و نیز با توجّه به فرض دفی–هلمن [۱] DHA بدون شناخت مؤلّفهٔ محرمانه S_A، توسط اخلال‌گر محاسبهٔ $K_(A, B)$ و جعل کردن یک Ack معتبر درمرحلهٔ ۳ غیرعملی خواهد بود؛ از طرفی دیگر مالک تصدیق، مؤلّفهٔ محرمانه S_A را از C_A در طول مرحلهٔ ثبت به دست آورده و می‌تواند با موّفقیّت درمرحله ۳ احراز اصالت شود. بنابراین امنیت توانایی غیرقابل جعل پروتکل پیشنهادی از طریق ترکیب امنیت طرح امضای الجمال و فرض دفی–هلمن [۱] DHA تأمین می‌شود. پس احراز اصالت پیشنهادی کاربر و پروتکل برقراری کلید در مقابل حملات خارجی امن خواهد بود.

One-Wayness (روش الحاق (فشردگی)): درگام ۱ مالک تصدیق، S_A را به تصدیق‌کننده ارائه می‌دهد. محاسبهٔ s_A محرمانه از S_A غیرعملی است زیرا نیاز به حل مسئلهٔ لگاریتم گسسته دارد. همچنین مالک تصدیق درمرحلهٔ ۳، s_A محرمانه را برای محاسبهٔ کلید دفی–هلمن $K_(A, B)$ به‌کار می‌گیرد و علی‌رغم این‌که تصدیق‌کننده کلید دفی–هلمن $K_(A, B)$ را می‌شناسد؛ امّا این روند به فرض دفی–هلمن DHA ختم می‌شود و تصدیق‌کننده نمی‌تواند s_A محرمانه را به دست آورد.

غیرقابل انتقال‌پذیری: با توجّه به فرض دفی–هلمن DHA [۱]، یک پاسخ معتبر Ack فقط می‌تواند توسط یک مالک تصدیق ایجاد شود که او مؤلّفهٔ محرمانهٔ s_A امضای دیجیتال از قبیل $r_A^{s_A} = S_A \bmod p$ و یا عدد تصادفی محرمانهٔ یک چالش تصادفی انتخابی توسط تصدیق‌کننده را می‌شناسد. نظر باینکه هربار تصدیق‌کننده یک چالش تصادفی انتخاب می‌کند؛ پاسخ فقط برای احراز اصالت یکبار مصرف معتبر خواهد بود.

از آن جائی که اصلاً امضای دیجیتال GDC به تصدیق‌کننده صادر (انتقال) نمی‌شود؛ لذا تصدیق‌کننده نمی‌تواند GDC کامل را به هر قسمت سوّمی انتقال دهد؛ از این‌رو نگرانی به دست‌یابی کلید خصوصی در پروتکل پیشنهادی وجود ندارد. پس یک پاسخ معتبر Ack نمی‌تواند درون یک پاسخ چالش تصدیق‌کنندهٔ دیگر انتقال یافته شود. پروتکل پیشنهادی قادراست یک مالک تصدیق را احراز اصالت کرده و همچنین دو کلید محرمانهٔ تسهیم شدهٔ یکبار مصرف $K_(A, B)$ و $C_B^{v_A} = r_A^{v_A v_B} = C_A^{v_B} \bmod p$ را بین کاربر A و مالک تصدیق برقرار کند. شخصی که s_A و به‌دنبال آن $r_A^{s_A} = S_A \bmod p$ و تصدیق‌کننده B را از طریق پروتکل احراز اصالت بشناسد می‌تواند طی مراحلی کلید محرمانهٔ تسهیم شده بین لA و B برقرار نماید و علاوه براین می‌تواند مالکیّت را به ارسال یک تصدیق Ack به تصدیق‌کننده قادر سازد؛ از آن‌جائی که کلید تسهیم شدهٔ محرمانهٔ دفی–هلمن می‌تواند توسط هر یک ازکاربرهای A یا B ایجاد شود از این‌رو مالک تصدیق A می‌تواند تسهیم‌کننده در پروتکل را انکار کند.

نکته ۱: در فرض دفی–هلمن DHA، فرض کردیم که مولّد g یک عضو اوّل گروه ضربی به پیمانه p است تا زمانی‌که پارامتر $r_A = g^K \bmod p$ در قضیه ۱ لزوماً یک مولّد نباشد. هرچند ما می‌توانیم مطمئن شویم که r_A یک عضو اوّل گروه ضربی به پیمانهٔ p توسط استلزام $\gcd(k, p-1) = 1$ بوده؛ به‌خصوص وقتی $p = 2p' + 1$ یک عدد اوّل امن باشد درجائی که p' هم یک عدد اوّل است ما می‌توانیم مطمئن شویم r_A یک عضو اوّل گروه ضربی به پیمانه p است اگر K یک عدد فرد باشد.

نکته ۲: به‌طور مشابه بر اساس الگوریتم‌های رمزنگاری مبتنی بر ID، پروتکل پیشنهادی مشکل ابطال کلید دارد؛ البتّه CA کلید جلسه محرمانهٔ یکبار مصرف تسهیم شده بین کاربرها را می‌شناسد. بعضی الگوریتم‌های رمزنگاری برای حل کردن مسئلهٔ ابطال کلید، امضاء بر اساس ID، (IBS) پیشنهاد کرده‌اند از قبیل امضای دیجیتال با تصدیق کمتر (CDS).

۵ پروتکل بر اساس IF (عدد صحیح)

در این بخش، ما یک پروتکل استقرار کلید و احراز اصالت کاربر بر اساس IF پیشنهاد می‌کنیم که ترکیبی از یک امضای دیجیتال آفلاین/ آنلاین بوده و فرض دفی-هلمن (GDHA) را ایجاد می‌کند.

۱.۵ بررسی امضای دیجیتال آنلاین/ آفلاین

در این قسمت خانواده تابع درهم‌ساز دریچه و طرح امضای آفلاین/ آنلاین را بررسی خواهیم کرد. یک خانواده درهم‌ساز دریچه شامل یک جفت (L, H) است؛ جائی که L یک الگوریتم مولّد کلید زمان چند جمله‌ای احتمالی و H یک خانواده درهم‌ساز تصادفی بوده که L یک جفت کلید (HK, TK) ایجاد می‌کند، به طوری‌که HK یک کلید درهم‌ساز (عمومی) و TK کلید دریچه (خصوصی) وابسته به آن می‌باشد. یک تابع درهم‌ساز دریچه تحت عنوان $h_{HK}(m, s)$ با محرمانگی کلید خصوصی فرض می‌شود جائی که m یک پیام و s یک عدد تصادفی معین خواهد بود. یک تابع درهم‌ساز دریچه باید سه نیازمندی زیر را ایفا کند:

- **بهره‌وری (راندمان):** تعیین یک کلید درهم‌ساز HK و یک جفت (m, s)، $h_{HK}(m, s)$ که در زمان چند جمله‌ای قابل محاسبه است.
- **پایداری در برابر تصادم:** الگوریتم زمان چند جمله‌ای احتمالی A، در ورودی کلید درهم‌ساز (عمومی) HK وجود ندارد که بتواند دو جفت $(m_۱, s_۱)$ و $(m_۲, s_۲)$ را ایجاد کند به طوری‌که بدون چشم پوشی $m_۱ \neq m_۲$ و $h_{HK}(m_۱, s_۱) = h_{HK}(m_۲, s_۲)$.
- **تصادم دریچه:** تعیین جفت‌های (HK, TK) و $(m_۱, s_۱)$ و یک پیام اضافی $m_۲$، با احتمال الگوریتم زمان چند جمله‌ای $s_۲$ ایجاد می‌شود به‌طوری که $h_{HK}(m_۱, s_۱) = h_{HK}(m_۲, s_۲)$. اگر $s_۱$ به‌طور یکنواخت در S توزیع شود آن‌گاه توزیع $s_۲$ به‌طور محاسباتی غیر قابل تشخیص از توزیع یکنواخت در S می‌باشد.

۲.۵ تابع درهم‌ساز دریچه بر اساس عامل‌یابی

با انتخاب تصادفی دو عدد اوّل امن p و q (به طوری که $p' = \frac{p-۱}{۲}$ و $q' = \frac{q-۱}{۲}$ عددهای اوّل باشند) $n = pq$ محاسبه می‌شود و همچنین با انتخاب تصادفی یک عضو g از مرتبه $\lambda(n)$، جائی که $\lambda(n) = \text{lcm}(p-۱, q-۱) = ۲p'q'$ محاسبه شده و کلید درهم‌ساز عمومی HK برابر (n, g) و کلید دریچه خصوصی TK برابر (p, q) خواهد بود. تابع درهم‌ساز دریچه $h_{HK}(m, s)$ تعریف می‌شود به‌عنوان: $h_{HK}(m, s) = g^{(m||s)} \bmod n$ (۴) جائی که $||$ عملگر الحاق را نشان می‌دهد.

لذا برای این‌که نشان دهیم $h_{HK}(m, s)$ یک تابع درهم‌ساز دریچه تحت فرض عامل‌یابی می‌باشد نیاز داریم نشان دهیم که آن سه مشخصهٔ اصلی یک تابع درهم‌ساز دریچه را تکمیل کرده و همچنین برای محاسبهٔ یک تصادم دریچه به جفت‌های معین (HK, TK)، $(m_۱, s_۱)$ و یک پیام اضافی $m_۲$، نیاز داریم، در ادامه $s_۲$ محاسبه می‌شود به‌طوری‌که $h_{HK}(m_۱, s_۱) = h_{HK}(m_۲, s_۲)$. بر اساس معادلهٔ ۴ باید $g^{m_۱||s_۱} =$

$g^{m_۲||s_۲} \bmod n$ به دست آید و $s_۲$ای یافت شود چنان‌که در معادلهٔ $۲^K m_۱ + s_۱ = ۲^K m_۲ + s_۲ \bmod \lambda(n)$ صدق کند جائی که K اندازهٔ پارامتر معین s می‌باشد. کلید دریچه معین $TK = (p, q)$ و $\lambda(n)$ می‌تواند با تابع زمان چند جمله‌ای محاسبه شوند و همچنین $s_۲$ می‌تواند در زمان چندجمله‌ای با حل کردن معادلهٔ خطی $s_۲ = ۲^K(m_۱ - m_۲) + s_۱ \bmod \lambda(n)$ محاسبه شود.

۳.۵ طرح امضاء

به طوراساسی هر طرح امضای دیجیتال معین با یک خانواده درهم‌ساز دریچه (L, H) می‌تواند در یک طرح امضای آنلاین/ آفلاین تعریف شود و در مرحلهٔ امضای آفلاین، یک امضاءکننده مقدار درهم‌سازی را به قصد انجام یک پیام انتخاب شدهٔ دلخواه تولید می‌کند. امّا در مرحلهٔ آنلاین، امضاءکننده برای یک پیام معین، یک تصادم درهم‌ساز دریچه را با مقدار درهم‌سازی محاسبه شدهٔ قبلی می‌یابد. نقطهٔ تصادم و امضای ایجاد شده در مرحلهٔ آفلاین می‌تواند به عنوان امضاء برای پیام ایجاد شده در مرحلهٔ آنلاین ارائه شود با فرض این‌که $h_{HK}(m, s)$ به‌عنوان تابع درهم‌ساز دریچه، HK کلید درهم‌ساز، TK کلید دریچه، VK کلید تصدیق و SK کلید امضاءکننده برای هر طرح امضای دیجیتال معین نشان داده می‌شود؛ در بخش زیر طرح امضای آفلاین/ آنلاین تشریح می‌کنیم:

- الگوریتم ایجاد کلید GEN: یک جفت (SK, VK) با بکار بردن الگوریتم ایجاد کلید عمومی و یک جفت (HK, TK) با بکاربردن الگوریتم L ایجاد می‌شوند. کلید امضاءکننده (SK, HK, TK) و کلید تصدیق (VK, HK) می‌باشد.
- الگوریتم امضاءکننده SIGN: یک کلید امضاء کننده (SK, HK, TK) تعیین می‌شود. الگوریتم امضاءکننده عمل می‌کند به عنوان زیر:

  - مرحلهٔ آفلاین: امضاءکننده به‌طور تصادفی (m, s) انتخاب کرده و $h_{HK}(m, s)$ را محاسبه می‌کند. سپس کلید محرمانهٔ SK را برای امضای $h_{HK}(m, s)$ به‌کارگرفته و $< S_{SK}(h_{HK}(m, s)) >$ را به‌دست می‌آورد. امضاءکننده $S_{SK}(h_{HK}(m, s)), s, m$ ذخیره می‌کند و به طوراختیاری از $h_{HK}(m, s)$ برای محاسبهٔ مجدد در طول مرحله آنلاین اجتناب می‌کند.
  - مرحلهٔ آنلاین: بافرض یک پیام معین m'، امضاءکننده یک تصادم درهم‌ساز دریچه را برای (m, s) می‌یابد چنان‌که $h_{HK}(m', s') = h_{HK}(m, s)$. امضای پیام m' به‌عنوان $< S_S K(h_{HK}(m, s)), s', h_{HK}(m, s) >$ تعریف می‌شود.

  الگوریتم تصدیق VERF: ابتدا $< S_{SK}(h_{HK}(m, s)) >$ را با به‌کارگیری VK و $h_{HK}(m, s)$ بررسی کرده و سپس $h_{HK}(m', s')$ محاسبه کرده برای بررسی این‌که $h_{HK}(m, s) = h_{HK}(m', s')$.

۴.۵ فرض دفی-هلمن تعمیم‌یافته (GDHA)

فرض کنید کاربر A و B کلیدهای خصوصی x_A و x_B و متناظر آن‌ها به‌ترتیب کلیدهای عمومی $y_A = g^{x_A} \bmod n$ و $y_B = g^{x_B} \bmod n$ را در اختیار دارند. حال اگر $n = pq$، جائی که p و q دو عدد اوّل بزرگ باشند، آن‌گاه فرض می‌کنیم که فقط A و B می‌توانند یک محرمانگی تسهیم‌شدهٔ $K_{A,B} = y_A^{x_B} = y_B^{x_A} \bmod n$ را محاسبه کنند.

در حقیقت GDHA رجوع می‌کند به فرضیه‌ای که به‌طور محاسباتی برای تعیین کردن $K_(A, B)$ بدون شناختن کلید خصوصی x_A یا x_B غیرعملی خواهد بود.

۵.۵ پروتکل احراز اصالت کاربر و برقراری کلید

۱) ثبت در CA: به‌فرض A مالکیّت تصدیق و B تصدیق‌کننده باشد. A به ثبت کردن در CA برای به‌دست آوردن یک GDC نیاز دارد. CA یک امضای دیجیتال آنلاین/ آفلاین $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$، برای دستور Aام کاربر m_A ایجاد می‌کند؛ در پروتکل احراز اصالت هر مالکیّت به نگهداری امضای محرمانهٔ s_A از تصدیق‌کننده نیاز دارد تا زمانی‌که تصدیق مؤلّفهٔ محرمانه به تصدیق‌کننده اثبات شود. مالکیت، مؤلّفهٔ محرمانه را به تصدیق کننده در طول مرحلهٔ احراز اصالت مطابق فرضیه GDHA پنهان می‌کند. احراز اصالت کاربر و پروتکل برقراری کلید در شکل ۲ نشان داده می‌شود.

۲) پروتکل: پروتکل برقراری کلید و احراز اصالت شامل۴ مرحلهٔ زیر می‌باشد:

۱. کاربر A اطلاعات کاربری‌اش m_A و پارامترهای $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$ را به تصدیق‌کننده B، تحت رابطهٔ $S_A = g^{S_A} \bmod n$ انتقال می‌دهد.

۲. بعد از دریافت m_A و $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$، تصدیق‌کنندهٔ B ابتدا بررسی می‌کند که آیا $(S_{SK}(h_{HK}(m', s'))$ امضای $h(m', s')$ با کاربرد VK است. سپس $h_{HK}(m_A, S_A) = g^{۲^K m_A} S_A \bmod n$ را محاسبه کرده و بررسی می‌کند که آیا رابطهٔ $h_{HK}(m_A, S_A) = h_H K(m', s')$ برقرار است، جائی که K مؤلّفهٔ محرمانهٔ s_A می‌باشد. اگر این برابری صحیح نگه داشته شود؛ تصدیق‌کنندهٔ B ابتدا به‌طور تصادفی یک عدد صحیح $v_B \in [۱, n-۱]$ انتخاب می‌کند، سپس $c_B = g^{v_B} \bmod n$ محاسبه کرده و c_B را به کاربر A ارسال می‌کند؛ درغیراین‌صورت، احراز اصالت کاربر شکست خورده و پروتکل متوقف می‌شود.

۳. ابتدا کاربر A، s_A محرمانه‌اش را برای محاسبهٔ کلید محرمانهٔ دفی-هلمن $k_(A, B) = C_B^{S_A} \bmod n$ و $K'_{A,B} = D(K_{A,B})$ به‌کار می‌گیرد. سپس کاربر A به‌طور تصادفی عدد صحیح $v_A \in [۱, n-۱]$ انتخاب می‌کند و $c_A = g^{v_A} \bmod n$ محاسبه کرده و

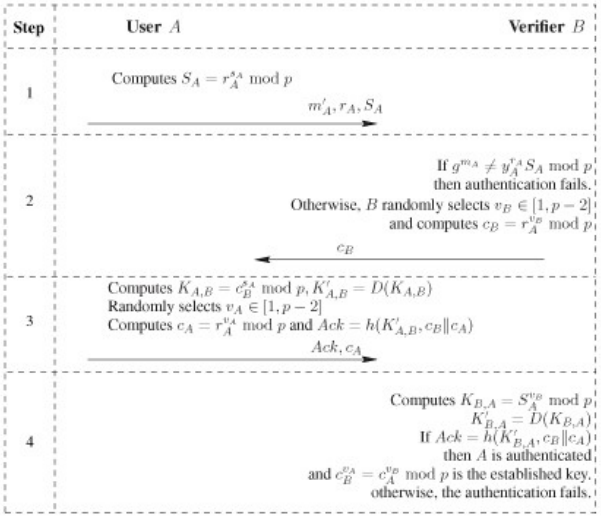
$Ack = h(K'_{A,B}, c_B||c_A)$ پاسخ می‌دهد جائی که $D(K_{A,B})$ یک روند استخراج کلید تحت $K_{A,B}$ را به عنوان یک ورودی $h(K_{A,B})', c_B||c_A)$ و یک روش تابع درهم‌ساز کلید شده تحت کلید $K'_{A,B}$ ارائه می‌دهد. کاربر A، Ack و c_A را در برگشت به B ارسال می‌کند.

۴. بعد ازدریافت Ack و c_A ازکاربر A، تصدیق‌کنندهٔ B، v_B محرمانه‌اش را برای محاسبهٔ کلید محرمانهٔ تسهیم شده دفی-هلمن $K_{B,A} = S_A^{v_B} \bmod n$ و $K'_{B,A} = D(K_{A,B})$ به‌کار گرفته و بررسی می‌کند که آیا $Ack = h(K'_{A,B}, c_B||c_A)$ صحیح است. اگراین تصدیق موفّق باشد مالکیّت تصدیق A توسط تصدیق‌کنندهٔ B احراز اصالت شده و یک کلید جلسهٔ محرمانهٔ یکبار مصرف $c_B^{v_A} = g^{v_A v_B} = c_A^{v_B} \bmod n$ بین Aو B تسهیم خواهد شد. این کلید می‌تواند امنیت کامل پیشرو را فراهم نماید؛ به منظور احراز اصالت موفّق توسط تصدیق‌کننده در پروتکل پیشنهادی، مالکیّت تصدیق به محاسبه و ارسال پارامترهای معتبر $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$ و Ack به تصدیق‌کننده درگام ۱ و ۳ نیاز دارد. پارامتر S_A به تصدیق $h_{HK}(m', s') = g^{(۲^K m_A)} S_A \bmod n$ نیاز دارد. این پارامتر می‌تواند به آسانی توسط هرکسی حل شده باشد یا به طور عمومی قابل دسترس باشد. هر چند ما نشان خواهیم داد که فقط مالکیّت تصدیق A شخصی است که مؤلّفهٔ محرمانهٔ S_A را می‌شناسد و می‌تواند یکAck معتبر محاسبه کند. این به خاطر آن است که تصدیق‌کنندهٔ B می‌تواند کلید محرمانهٔ یکبار مصرف $K_{B,A}$ بکار برده شده را در ایجادکردن Ack به‌عنوان $K_{B,A} = S_A^{v_B} = g^{S_A v_B} \bmod n$ محاسبه کند، بر اساس فرضیه GDHA، مالکیّت تصدیق A کسی است که برای شناخت مؤلّفهٔ محرمانه S_A می‌تواند $K_(A, B)$ را به عنوان $K_{A,B} = c_B^{S_A} = g^{S_A v_B} = K_{B,A} \bmod n$ محاسبه کند. بنابراین مالکیّت تصدیق می‌تواند با تصدیق‌کننده فعل و انفعال داشته باشد و با موفقیّت احراز اصالت شود.

نکته ۳: در پروتکل پیشنهادی CA یک امضای دیجیتال آفلاین/ آنلاین را برای هرکاربر ثبت شده ایجاد می‌کند. CA واقعاً نیازمند ویژگی دریچه یک روش تابع درهم‌ساز نبوده و درحقیقت CA به کلید دریچه نیاز ندارد. بلکه فقط برای بکاربردن یک ویژگی روش تابع درهم‌ساز برای محاسبهٔ یک مقدار درهم‌ساز S_A نیاز دارد. همچنین به‌منظور ایجاد یک پروتکل بر اساس IF، CA به‌کارگیری امضای RSA [۲] را برای مقدار درهم‌ساز امضای دیجیتالی $h(m', s')$ نیاز دارد.

۶.۵ تحلیل امنیتی

امنیت این پروتکل مبتنی ترکیب امن امضای RSA [۲]، پایداری تصادم یک روش تابع درهم‌ساز و فرضیه GDHA تکیه می‌کند. امضای دیجیتال آفلاین/ آنلاین در مقابل حملات پیام انتخاب شدهٔ توافقی امن خواهد بود به شرط آن که طرح اصلی درمقابل حملات انتخاب شدهٔ پیام امن باشد. همچنین به‌درستی اثبات کردیم که تابع درهم‌ساز دریچه، در برابرتصادم پایدار است. امنیت پروتکل پیشنهادی بر اساس مسئلهٔ لگاریتم گسسته DL، برقراری کلید IF، ویژگی توانایی غیرقابل جعل و توانایی غیر دریچه و همچنین توانایی غیرعملی بودن



شکل ۲: پروتکل توافق کلید و احراز اصالت بر اساس IF

معکوس تابع درهم‌ساز پایدار می‌باشد. علاوه براین پروتکل ویژگی احراز اصالت انکارپذیر را فراهم کرده و نیز تصدیق دیجیتال کلید خصوصی را هم پشتیبانی می‌کند؛ ازاین‌رو طرح ما از بعضی مفاهیم اساسی، از قبیل یک روش تابع درهم‌ساز، به‌طور مثال MD5 (توابع استخراج چکیده پیام برای نگهداری داده‌های محرمانه درمحیط کلید عمومی) یا SHA-1 (مرسوم‌تر ولی SHA-2 قوی‌تر و امن‌تر)، مسئلهٔ لگاریتم گسسته، و پروتکل توافق کلید دفی–هلمن به منظور پایداری در برابر حملات شناخته شده بهره گرفته است.

۶ نتیجه‌گیری

ما یک طراحی جدید دربه‌کارگیری GDC برای احراز اصالت کاربر و برقراری کلید پیشنهاد کردیم که در این طرح یک GDC، کلید عمومی کاربر را دراختیار نداشته و از آن جائی که کاربر هرجفت کلید خصوصی و کلید عمومی را ندارد این نوع تصدیق دیجیتال برای مدیریت تصدیق‌های دیجیتال کلید عمومی X.509 خیلی آسان‌تر به نظر می‌رسد. این شیوهٔ پیشنهادی می‌تواند هر دو سیستم رمزنگاری کلید عمومی بر اساس IF و DL پشتیبانی نماید.

مراجع

[1] W. Diffle and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, pp. 644-654, 1976J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] T. A. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inf. Theory, vol. 31, no. 4,pp. 469-472, 1985.

[4] S. Goldwasser, S. Micali, and R. L. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks,” SIAM J. Comput.,vol. 17, no. 2, pp. 281–308, 1988.

[5] D. Chaum and H. van Antwerpen, “Undeniable signatures,” Advances in Cryptology - Crypto’89, Lecture Notes in Computer Science, vol. 435,pp. 212-217, 1989.

[6] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated verifier proofs and their applications,” Advances in Cryptology - EUROCRYPT, pp. 143-154, 1996. LNCS Vol 1070.

[7] D. Chaum, “Private signature and proof systems,” 1996.

[8] S. Saeednia, S. Kremer, and O. Markowitch, “An efficient strong designated verifier signature scheme,” ICISC 2003, vol. 2836 of Springer Lecture Notes in Computer Science, pp. 40-54, 2003.

[9] C. Schnorr, “Efficient signature generation by smart cards,” J. Cryptology,vol. 4, no. 3, pp. 161-174, 1991.

[10] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption « cost (signature) + cost (encryption),” Advances in Cryptology - Crypto’97, Lecture Notes in Computer Science vol. 1294,pp. 165-179, 1997.

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

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

[13] 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.

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

[15] 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, 2008, pp. 37-44.

[16] 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.

[17] 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.

[18] 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.

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

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

[21] 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.

[22] 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(10), pp. 1842-1854, 2007.

[23] 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.

[24] 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.

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

[26] 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.