استاندارد ملی ایران
۱۰۸۲۵-۵
چاپ اول
اردیبهشت ۱۳۹۲

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO

10825-5

1st. Edition

Apr.2013

فناوری اطلاعات – فنون امنیتی– احراز هویت هستار
قسمت ۵: سازوکارهای استفاده‌کننده از فنون دانش_صفر

Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - فنون امنیتی– احراز هویت هستار

قسمت ۵: سازوکارهای استفاده‌کننده از فنون دانش _صفر»

رئیس :	**سمت و/ یا نمایندگی**
سعیدی، عذرا (کارشناسی ارشد مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
دبیر :	
میراسکندری، سید محمدرضا (کارشناسی مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (کارشناسی مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل پناه، ناصر (کارشناسی ارشد مدیریت)	کارشناس سازمان فناوری اطلاعات
خوشنویسان، نازنین (کارشناسی مهندسی نرم‌افزار)	نماینده دانشگاه شهید بهشتی
سلطانی حقیقت، الهه (کارشناسی مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
عباسپور، مقصود (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
فرهاد شیخ احمد، لیلا (کارشناسی ارشد مهندسی کامپیوتر نرم‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات

فولادیان، مجید (کارشناسی ارشد مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات
فیاضی، مهدی (کارشناسی مهندسی برق مخابرات)	کارشناس مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات
قسمتی، سیمین (کارشناسی ارشد فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
موجبی، محمود (کارشناسی ارشد مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
میرزایی رضایی، طیبه (کارشناسی ارشد فیزیک)	رئیس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (کارشناسی مهندسی فناوری اطلاعات)	نماینده دانشگاه شهید بهشتی
یعقوبی رفیع، کمال‌الدین (کارشناسی مهندسی فناوری اطلاعات)	نماینده دانشگاه شهید بهشتی

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی- احراز هویت هستار- قسمت ۵: سازوکارهای استفاده‌کننده از فنون دانش _ صفر» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در اجلاس دویست و پنجاه و چهارمین کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۱۱/۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیر است:

ISO/IEC9798-5: 2009, 3rd Ed.: Information technology – Security techniques–Entity authentication - Part 5: Mechanisms using zero-knowledge techniques

مقدمه

این استاندارد سازوکارهای احراز هویتی را مشخص می‌کند که حاوی تبادل اطلاعات[1] بین یک خواهان و یک درستی‌سنج[2] است.

مطابق با نوع محاسباتی که نیاز است به‌وسیله خواهان و درستی‌سنج انجام شوند، سازوکارها را می‌توان به چهار گروه اصلی طبقه‌بندی کرد. (به پیوست پ مراجعه شود.)

- گروه اول (به بندهای ۴ و ۵ مراجعه شود.) به‌وسیله عملکرد به نمارسانی[3] پیمانه‌ای کوتاه مشخص می‌شود. اندازه چالش باید بهینه شود، چون اثری نسبی بر بارکاری دارد.
- گروه دوم (به بندهای ۶، ۷ و ۸ مراجعه شود.) به‌وسیله امکان یک «راهبرد کوپن[4]» برای خواهان مشخص می‌شود. یک درستی‌سنج می‌تواند یک خواهان را با توان محاسباتی بسیار محدودی احراز هویت کند. در عمل اندازه چالش اثری بر حجم کار ندارد.
- گروه سوم (به زیربند ۹-۲ مراجعه شود.) به‌وسیله امکان یک راهبرد کوپن برای درستی‌سنج مشخص می‌شود. یک درستی‌سنج با توان محاسباتی بسیار محدود می‌تواند یک خواهان را احراز هویت کند. اندازه چالش اثری بر حجم کار ندارد.
- گروه چهارم (به زیربند ۹-۳ مراجعه شود.) هیچ امکانی برای یک راهبرد کوپن ندارد.

دو سازمانISO و IEC توجه را به این واقعیت جلب می‌کنند که ادعا می‌شود مطابقت با این استاندارد ممکن است شامل استفاده از حق ثبت اختراع[5]های زیر و معادل آن‌ها در دیگر کشورها شود.

US 4 995 082 issued 1991-02-19, Inventor: C.P. Schnorr,
US 5 140 634 issued 1992-08-18, Inventors: L.C. Guillou and J-J. Quisquater,
EP 0 311 470 issued 1992-12-16, Inventors: L.C. Guillou and J-J. Quisquater,
EP 0 666 664 issued 1995-02-02, Inventor: M. Girault,

این دو سازمان هیچ موضعی در قبال سندیت، اعتبار و دامنه این حق امتیازها ندارند.

دارندگان این حق امتیازها این اطمینان را به ISO و IEC داده‌اند که مایلند در مورد گواهینامه‌های تحت شرایط و ضوابط معقول و عادلانه که در سرتاسر دنیا کاربرد دارند مذاکره کنند. از این لحاظ بیانیه‌های دارندگان این حق امتیازها در ISO و IEC ثبت شده است. اطلاعات ممکن است از شرکت‌هایی که درفهرست صفحه بعد قرار دارند به‌دست آیند.

1- Claimant
2 - Verifier
3-Exponentation
4- Coupon strategy
3- Patent

RSA Security Inc. Attention General Counsel 174 Middlesex Turnpike Bedford, MA 01730, USA	US 4 995 082
France Telecom R&D Service PIV 38-40 Rue du Général Leclerc F 92794 Issy les Moulineaux Cedex 9, France	US 5 140 634, EP 0 311 470, EP 0 666 664
Philips International B.V. Corporate Patents and Trademarks P.O. Box 220 5600 AE Eindhoven, The Netherlands	US 5 140 634, EP 0 311 470
فرانس تلکام[a] خواهان است که کاربردهای حق امتیاز بندهای ۶ (GQ2)[b] و ۸ (GPS)[c] در حال بررسی است. شماره‌های این حق امتیازها به محض ارائه شدن اعلام می‌شوند. سپس ISO/IEC بیانیه مناسب را درخواست خواهد کرد.	

a. France Telecom

b. بند ۵-۱ در این استاندارد را ببینید

c. بند ۷-۱ در این استاندارد را ببینید

فناوری اطلاعات – فنون امنیتی – احراز هویت هستار
قسمت ۵ : سازوکارهای استفاده کننده از فنون دانش _ صفر

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین سازوکارهای احراز هویت هستار با استفاده از فنون دانش _ صفر است:

- سازوکارهای مبتنی بر هویت‌ها و تأمین‌کننده احراز هویت یک‌جانبه؛
- سازوکارهای مبتنی بر تجزیه به عامل‌های صحیح و تأمین‌کننده احراز هویت یک‌جانبه؛
- سازوکارهای مبتنی بر لگاریتم‌های گسسته نسبت به اعداد اول یا مرکب و تأمین‌کننده احراز هویت یک‌جانبه؛
- سازوکارهای مبتنی بر سامانه‌های رمزبندی[1] دو کلیده و تأمین‌کننده احراز هویت یک‌جانبه یا دوجانبه؛
- سازوکارهای مبتنی بر لگاریتم‌های گسسته روی منحنی‌های بیضوی و تأمین‌کننده احراز هویت یک‌جانبه.

این سازوکارها با استفاده از اصول فنون دانش - صفر ساخته می‌شوند. اما مطابق با تعریف دقیق برای هر انتخاب پارامتر، این سازوکارها همیشه دانش - صفر نیستند.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌روند:

۱-۲

نمای تأیید اعتبار[2]

عدد سرّی[3] مربوط به نمای درستی‌سنجی و مورد استفاده در تولید کلیدهای خصوصی

۲-۲

پارامتر سازگاری

کلید عمومی خاص پیمانه و مورد استفاده در تعریف کلیدهای عمومی در سازوکارهای GQ2

1- Encryption
2 - Accreditation exponent
3- Secret

۳-۲

فن رمزنگاری[1] نامتقارن

فن رمزنگاری‌که از دو عملیات مربوط استفاده می‌کند: یکی عملیات عمومی تعریف شده به‌وسیله یک واحد داده عمومی و دیگری عملیات خصوصی تعریف شده به‌وسیله یک واحد داده خصوصی (هر دو عملیات این ویژگی را دارا هستند که با معلوم بودن عملیات عمومی، به دست آوردن عملیات خصوصی به‌صورت محاسباتی غیرممکن می شود.)

۴-۲

سامانه رمزبندی نامتقارن

سامانه مبتنی بر فنون رمزنگاری نامتقارن که از عملیات عمومی آن جهت رمزبندی و از عملیات خصوصی آن جهت رمزگشایی استفاده می‌شود.

۵-۲

جفت نامتقارن

دو واحد داده وابسته که واحد داده خصوصی یک عملیات خصوصی و واحد داده عمومی یک عملیات عمومی را تعریف می‌کنند.

۶-۲

چالش

پارامتر رویه[2] مورد استفاده در ارتباط با پارامترهای سرّی که یک پاسخ را تولید می‌کند.

۷-۲

خواهان[3]

هستاری که بتوان هویت آن را احراز هویت کرد شامل توابع و داده‌های خصوصی ضروری برای شرکت در تبادلات احراز هویت از طرف یک دستوردهنده[4] است.

۸-۲

کوپن

جفت اعداد از پیش محاسبه شده‌ای که تنها یک مرتبه به‌کار می‌روند؛ یکی سرّی نگاه داشته شده و دیگری تا زمان استفاده به‌وسیله یک هستار سرّی می‌ماند.

---

1 - Cryptographic
2 - Procedure parameter
3 - Claimant
4- Principal

۹-۲

پارامتر خواهان

واحد داده عمومی به‌صورت عدد یا رشته بیتی مشخص یک خواهان مفروض درون دامنه است.

۱۰-۲

رمزگشایی

وارون یک رمزبندی متناظر

یادآوری- رمزگشایی و واپوشیده‌سازی[1] اصطلاحات معادل هستند.

۱۱-۲

دامنه

مجموعه‌ای از هستارهای عمل‌کننده تحت یک سیاست امنیتی واحد

یادآوری– به‌عنوان مثال، گواهی‌های کلید عمومی تولید شده به‌وسیله یک صادرکننده یا مجموعه‌ای از صادرکنندگان گواهی که از یک سیاست امنیتی یکسان استفاده می‌کنند.

۱۲-۲

پارامتر دامنه

کلید یا تابع عمومی پذیرفته‌شده و مورد استفاده به‌وسیله همه‌ی هستارهای درون دامنه است.

۱۳-۲

رمزبندی

عملیات وارون‌پذیر تبدیل داده به متن پوشیده، به‌وسیله الگوریتم رمزنگاری، به‌گونه‌ای که بتواند محتوای اطلاعاتی داده‌ها را سرّی کند.

یادآوری – رمزبندی**[30]** و پوشیده‌سازی **[24]** اصطلاحات معادل هستند.

۱۴-۲

احراز هویت هستار

تأیید آنکه یک هستار همان چیزی است که ادعا می‌شود.

[تعریف ۳-۳-۱۱استاندارد ملی شماره ۱-۱۰۸۲۵ : ۱۳۹۱]

1 - Decipherment

۱۵-۲

پارامتر تعدد تبادل

دفعات تبادل اطلاعات در یک نمونه از سازوکار احراز هویت است.

۱۶-۲

تابع درهم‌ساز[1]

تابعی که رشته‌های بیتی را به رشته‌های بیتی با طول ثابت می‌نگارد و دو ویژگی زیر را برآورده می‌کند:

- برای یک خروجی مفروض، یافتن ورودی‌ای که به این خروجی نگاشته می‌شود به‌طور محاسباتی امکان‌پذیر نیست.
- یافتن دو ورودی مجزا که به خروجی یکسان نگاشته شوند به‌طور محاسباتی امکان‌پذیر نیست.

[تعریف ۳-۵ ,ISO/IEC 10118-1:2000]

۱۷-۲

داده شناسایی

مجموعه‌ای از واحدهای داده عمومی (یک شماره حساب، یک تاریخ و زمان انقضاء، یک شماره سریال و غیره) که به یک هستار نسبت داده شده و به‌منظور شناسایی آن به‌کار می‌رود.

۱۸-۲

احراز هویت دوجانبه

احراز هویت هستاری که دو هستار را از هویت یکدیگر مطمئن می‌سازد.

[تعریف ۳-۳-۱۴ استاندارد ملی شماره ۱-۱۰۸۲۵ : ۱۳۹۱]

۱۹-۲

عدد

عدد طبیعی یعنی یک عدد صحیح غیرمنفی

۲۰-۲

پارامتر تعدد جفت

تعداد جفت‌های نامتقارن اعداد در نمونه‌ای از یک سازوکار احراز هویت

1- Hash function

۲-۲۱

کلید خصوصی

واحد داده‌ی یک جفت نامتقارن که باید سرّی نگاه داشته شود و تنها باید به‌وسیله یک خواهان مطابق با یک فرمول پاسخ مناسب مورد استفاده قرار گرفته و در نتیجه هویت آن را تعیین کند.

۲-۲۲

پارامتر رویه

واحد داده عمومی گذرای[1] مورد استفاده در یک نمونه از سازوکار احراز هویت مانند یک شاهد[2]، چالش یا پاسخ[3]

۲-۲۳

کلید عمومی

واحد داده‌ی یک جفت نامتقارن که می‌تواند عمومی شود و باید به‌وسیله هر درستی‌سنج برای برقرارسازی هویت خواهان مورد استفاده قرار گیرد.

۲-۲۴

عدد تصادفی

پارامتر زمان متغیر که مقدار آن غیرقابل پیش‌بینی است.

[تعریف ۳-۳-۲۴ استاندارد ملی شماره ۱-۱۰۸۲۵ : ۱۳۹۱]

۲-۲۵

پاسخ

پارامتر رویه تولیدشده توسط خواهان و پردازش‌شده به‌وسیله درستی‌سنج جهت وارسی هویت خواهان

۲-۲۶

پارامتر سرّی

عدد یا رشته بیتی که در دامنه عمومی ظاهر نمی‌شود و تنها توسط یک خواهان مورد استفاده قرار می‌گیرد، به‌عنوان مثال یک کلید خصوصی

1 - Transient public data item
2 - Witness
3 - Response

۲۷-۲

نشانه[1]

پیام حاوی دسته‌های داده که به یک ارتباط خاص مربوط است و شامل اطلاعاتی است که با استفاده از یک فن رمزنگاری تولید شده‌اند.

۲۸-۲

احراز هویت یک‌جانبه

احراز هویت هستاری که یک هستار را از هویت طرف دیگر مطمئن می‌کند اما عکس آن امکان‌پذیر نیست.

[تعریف ۳-۳-۳۳، استاندارد ملی شماره ۱-۱۰۸۲۵: ۱۳۹۱]

۲۹-۲

نمای درستی‌سنجی

کلید عمومی که به‌وسیله خواهان و درستی‌سنج به‌عنوان نما استفاده می‌شود.

۳۰-۲

درستی‌سنج

هستاری شامل توابع لازم برای شرکت در تبادلات احراز هویت از طرف یک هستار نیازمند به احراز هویت هستار

۳۱-۲

شاهد

پارامتر رویه که مدرک هویت خواهان را در اختیار درستی‌سنج قرار می‌دهد.

۳ نشانه‌گذاری[2]، نمادها و کوته‌نوشت‌ها

در این استاندارد نشانه‌گذاری، نمادها و کوته‌نوشت‌های زیر به‌کار می‌روند:

(a|n) نماد ژاکوبی عدد صحیح مثبت a نسبت به عدد صحیح مرکب فرد n

یادآوری۱- طبق تعریف، نماد ژاکوبی هر عدد صحیح مثبت a نسبت به هر عدد صحیح مرکب مثبت n برابر با حاصل‌ضرب نمادهای لژاندر a نسبت به هر عامل اول n است (با تکرار نمادهای لژاندر برای عامل‌های اول تکراری). نماد ژاکوبی[13][16] را می‌توان به‌صورت کارا و بدون دانستن عامل‌های اول n محاسبه کرد.

(a|p) نماد لژاندر عدد صحیح مثبت a نسبت به عدد صحیح اول فرد p

---

4 - Token
1- Notation

یادآوری۲- طبق تعریف، نماد لژاندر هر عدد صحیح مثبت a نسبت به هر عدد صحیح مثبت فرد p برابر است با $a^{(p-1)/2} \bmod p$.
این به معنای آن است که (a|p) برابر صفر است اگر a مضرب p باشد و یا برابر ۱+ یا ۱- باشد؛ در غیراین صورت، وابسته به این است که آیا a یک مربع به پیمانه p است یا خیر.

|A| اندازه بیت عدد A اگر A یک عدد باشد (یعنی عدد صحیح یکتای i به‌طوری‌که $2^{i-1} < A < 2^i$ اگر A>۰، یا 0 اگر A = ۰؛ برای مثال |۱۷ + ۲۱۶ = ۶۵۵۳۷|)، یا طول بیت رشته بیت A اگر A یک رشته بیت باشد.

یادآوری۳- نمایش دودویی عدد A به‌عنوان یک رشته |A| بیتی سرراست است. برای نمایش عدد A به‌عنوان رشته‌ای با α بیت با شرط $|A| < \alpha$، $\alpha - |A|$ بیت **0** به سمت چپ بیت‌های |**A**| افزوده می‌شود.

بزرگترین عدد صحیحی که کوچکتر یا مساوی عدد حقیقی A است.

B||C رشته بیتی که از الحاق واحدهای داده B و C طبق ترتیب مشخص‌شده حاصل می‌شود. در مواردی که حاصل الحاق دو یا چند واحد داده به ورودی یک الگوریتم رمزنگاری داده می‌شود و این الگوریتم به‌عنوان قسمتی از سازوکار احراز هویت است، این حاصل باید به‌گونه‌ای ساخته شود که بتوان آن را به‌صورت یکتا به رشته‌های داده سازنده‌اش تجزیه کرد؛ به این صورت امکان وجود هر گونه ابهام در تفسیر از بین می‌رود. برای دستیابی به ویژگی اشاره‌شده بسته به کاربرد، راه‌های مختلفی وجود دارد. به‌عنوان مثال، برای دستیابی به این ویژگی می‌توان از دو روش زیر استفاده کرد:
الف- طول هر یک از زیررشته‌ها را در تمام دامنه با استفاده از سازوکار، ثابت نگه داشت یا
ب-کدبندی دنباله رشته‌های الحاق شده با استفاده از روشی که کدگشایی یکتا را تضمین می‌کند. برای مثال، با استفاده از قواعد کدبندی تعریف‌شده در استاندارد ISO/IEC 8825-1[23].

CRT قضیه باقی‌مانده چینی[1]

d چالش (پارامتر رویه)

D پاسخ (پارامتر رویه)

F تعداد عامل‌های اول

1 - Chinese Remainder Theorem

gcd(a, b)	بزرگترین مقسوم‌علیه مشترک دو عدد صحیح a و b
G, G_i	کلید عمومی (پارامتر دامنه)
$G(A), G_i(A)$	کلید عمومی (پارامتر خواهان)
H	تابع درهم‌ساز
|h|	طول بیت کد درهم[1] تولیدشده به‌وسیله تابع درهم‌ساز h
H, HH	کدهای درهم
Id(A)	داده شناسایی (پارامتر خواهان)
$Id_i(A)$	قسمتی از داده شناسایی (پارامتر خواهان)
J mod n	عدد صحیح یکتای i از بازه {0, 1, … n-1} به‌طوری‌که n بر j-i بخش‌پذیر باشد.
J mod* n	عدد صحیح یکتای i از بازه {0, 1, … (n-1)/2} به‌طوری‌که n بر j-i یا بر j+i بخش‌پذیر باشد.
lcm(a, b)	کوچکترین مضرب مشترک دو عدد صحیح a و b
m	پارامتر تعدد جفت (پارامتر دامنه)
n	پیمانه مرکب (پارامتر دامنه)
n(A)	پیمانه مرکب (پارامتر خواهان)
$p_1, p_2, \ldots$	عامل‌های اول پیمانه با ترتیب صعودی یعنی ... $< p2 <$ p1(پارامترهای سرّی)
Q, Q_i	کلید خصوصی (پارامتر سرّی)
r	عدد تصادفی جدید[2] یا رشته جدید بیت‌های تصادفی (پارامتر سرّی)

1- Hash code
2 - Fresh

v	نمای درستی‌سنجی (پارامتر دامنه)
W	شاهد (پارامتر رویه)
‘X_1X_2...’	عددی با نمایش شانزده‌تایی X1X2… که در آن هر X_i برابر با یکی از 0-9 و A-F است.
	اندازه پیمانه به بیت یعنی ۲^{α} □ پیمانه ≤ $۲^{\alpha-۱}$ که با |پیمانه| نیز نمایش داده می‌شود. (پارامتر دامنه)
	طول رشته‌های جدید بیت‌های تصادفی برای نمایش چالش‌ها (پارامتر دامنه)
	طول رشته‌های جدید بیت‌های تصادفی برای نمایش اعداد تصادفی (پارامتر دامنه)
{a, b, c, …}	مجموعه شامل عناصر a, b, c, …

در بند ۵ (سازوکارهای مبتنی بر هویت[1]) نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

F	رشته بیت
t	پارامتر تعدد تبادل (پارامتر دامنه)
u	نمای تایید اعتبار نسبت به پیمانه (پارامتر سرّی)
u_j	نمای تایید اعتبار نسبت به عامل اول p_j (پارمتر سرّی)

در بند ۶ (سازوکارهای مبتنی بر تجزیه عامل‌های صحیح) نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

b	پارامتر سازگاری (مشخص شده برای پیمانه‌ها)
D_j	مؤلفه پاسخ نسبت به عامل اول p_j (پارامتر سرّی)
g_i	عدد پایه (پارامتر دامنه)

1 - Identity-based mechanisms

$g_i(A)$ عدد پایه (پارامتر خواهان)

k پارامتر امنیت (پارامتر دامنه)

$Q_{i,j}$ مؤلفه خصوصی نسبت به عدد پایه g_i و عامل اول p_j (پارامتر سرّی)

r_j عدد تصادفی جدید نسبت به عامل اول p_j (پارامتر سرّی)

u_j نمای تایید اعتبار نسبت به عامل اول p_j (پارامتر سرّی)

W_j مؤلفه شاهد نسبت به عامل اول p_j (پارامتر سرّی)

در بند ۷ (سازوکارهای مبتنی بر لگاریتم‌های گسسته نسبت به اعداد اول)، نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

g پایه لگاریتم‌های گسسته (پارامتر دامنه)

p پیمانه (پارامتر دامنه)

q عدد اول (پارامتر دامنه)

در بند ۸ (سازوکارهای مبتنی بر لگاریتم‌های گسسته نسبت به اعداد مرکب)، نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

g پایه لگاریتم‌های گسسته (پارامتر دامنه)

$g(A)$ پایه لگاریتم‌های گسسته (پارامتر خواهان)

تعداد بیت‌ها برای کلیدهای خصوصی در اولین حالت[1] (پارامتر دامنه)

در بند ۹ (سازوکارهای مبتنی بر سامانه‌های رمزبندی نامتقارن)، نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

1 - Mode

P_A عملیات عمومی یعنی رمزبندی (پارامتر خواهان)

S_A عملیات خصوصی یعنی رمزگشایی (پارامتر سرّی)

در بند ۱۰ (سازوکارهای مبتنی بر لگاریتم‌های گسسته روی منحنی‌های بیضوی)، نمادها و اصطلاحات کوتاه‌نویسی‌شده زیر به‌کار می‌رود:

[n]P عملیات ضربی که یک عدد صحیح مثبت n و یک نقطه p بر روی منحنی E را به‌عنوان ورودی گرفته و نقطه دیگر Q بر روی منحنی E را به‌عنوان خروجی می‌دهد به‌طوری‌که Q=[n]P=P+P+…+P مجموع n رخداد P است. این عملیات روابط [0]P=0E (نقطه در بی‌نهایت) و [-n]P=[n](-P) را برآورده می‌کند.

۴ سازوکارهای مبتنی برهویت‌ها

۴-۱ الزامات امنیتی برای محیط

این سازوکارها یک درستی‌سنج را قادر می‌سازند تا آگاهی یک خواهان از کد(های) خصوصی را که به‌وسیله یک کلید درستی‌سنجی به داده شناسایی مربوط می‌شود وارسی کند.

یادآوری– این سازوکارها، طرح‌ها را با توجه به فیات و شمیر[1] [**4**] که با FS یا با توجه به گویلو و کویسکواتر[2] [**11**] که با GQ1 نمایش داده می‌شود، پیاده‌سازی می‌کنند.

درون یک دامنه معین، نیازهای زیر باید برآورده شوند.

۱- پارامترهای دامنه که عملکرد سازوکار را اداره می‌کنند باید انتخاب شوند. این پارامترها شامل یک تابع درهم‌ساز مانند یکی از توابع مشخص‌شده در استاندارد ISO/IEC 10118-3 هستند[25]. پارامترهای انتخاب‌شده باید به یک روش قابل اطمینان به همه‌ی هستارهای درون دامنه شناسانده شوند.

۲- هر خواهان باید به یک پیمانه که یک پارامتر دامنه یا یک پارامتر خواهان است، مجهز شود. هر عدد که به‌عنوان پیمانه مورد استفاده قرار می‌گیرد برابر با حاصلضرب دو یا تعداد بیشتری از عوامل اول مجزا قرار داده می‌شود به‌گونه‌ای که هیچ هستاری نباید با آگاهی از مقدار آن قادر باشد، عوامل اول آن را نتیجه بگیرد و امکان‌پذیر بودن به‌وسیله متن استفاده از سازوکار، تعریف شود.

[1] - Fiat and Shamir
[2] - Guillou and Quisquater

- اگر پیمانه یک پارامتر دامنه باشد، آن‌گاه به‌وسیله n نمایش داده می‌شود. یک مرجع قابل اعتماد آن را انتخاب کرده و تنها این مرجع می‌تواند از عوامل اول متناظر استفاده کند. این مرجع هویت‌های هر خواهان درون دامنه را تضمین می‌کند.

یادآوری ۱– به‌عنوان مثال، یک صادرکننده کارت[1] دارای یک پیمانه است. یک هستار نماینده[2] داده‌های شناسایی را جهت صدور کارت‌های هوشمند امضا می‌کند؛ این هستار از عوامل اول صادرکننده استفاده می‌کند. هستار نماینده در هر کارت داده شناسایی و کلید(های) خصوصی مناسب را ذخیره می‌کند. در مدت عمر این هستار، کارت مذکور کلید(های) خصوصی خود را مطابق با یک سازوکار مبتنی بر هویت مورد استفاده قرار می‌دهد.

- اگر پیمانه یک پارامتر خواهان باشد، آن‌گاه به‌وسیله n(A) نمایش داده می‌شود. یک دستوردهنده آن را انتخاب کرده و عوامل اول متناظر، سرّی[3] دراز مدت دستوردهنده هستند. در هر نشست[4] دستوردهنده یک خواهان ایجاد می‌کند. این خواهان از کلید(های) خصوصی به‌عنوان یک رمز کوتاه مدت استفاده می‌کند.

یادآوری۲– به‌عنوان مثال، در یک شبکه محلی، یک مرجع بر روی هر عملیات ورود به سیستم درون دامنه نظارت کرده و یک فهرست راهنما را مدیریت می‌کند. در این فهرست راهنما، هر درستی‌سنجی می‌تواند یک رونوشت قابل اعتماد از یک پیمانه را برای هر دستوردهنده‌ای به‌دست آورد.

- در جریان هر عملیات ورود یعنی وقتی که رایانه نشست‌ای را باز می‌کند، عوامل اول دستوردهنده برای «ورود یک‌باره[5]» داده‌های شناسایی نشست که شامل شناسه، تاریخ و زمان انقضا، حقوق و غیره می‌شوند مورد استفاده قرار می‌گیرند.
- در جریان نشست، رایانه دیگر نمی‌تواند عوامل اول را مورد استفاده قرار دهد زیرا دیگر آنها را نمی‌شناسد. رایانه کلید(های) خصوصی را مطابق با یک سازوکار مبتنی بر هویت مورد استفاده قرار می‌دهد. کلیدهای خصوصی تنها چند ساعت دوام داشته و کارآمدی آن پس از نشست از بین می‌رود..

۳- داده شناسایی و یک یا چند کلید خصوصی باید به‌نحوی در دسترس هر خواهان قرار گیرند. در این متن، داده شناسایی یک رشته بیتی است که همگی مساوی نیستند و خواهان را به‌طور یکتا و معنادار مطابق با یک قرارداد مورد توافق شناسایی می‌کنند.

یادآوری– وجود یک تاریخ و زمان انقضا در داده‌های شناسایی آن‌ها را مجبور به ابطال کرده و وجود یک شماره سریال این ابطال را ساده می‌سازد.

۴- هر درستی‌سنج باید یک رونوشت قابل اعتماد از پیمانه صحیح خواهان را به‌دست آورد.

1 - Card issuer
2 - Delegated entity
3 - Secret
4 - Session
5 - Single-sign-on

یادآوری – نحوه دقیق دستیابی درستی‌سنج به یک رونوشت قابل اعتماد از پیمانه صحیح فراتر از حیطه‌ی این استاندارد است. به‌عنوان مثال برای دست‌یابی به نسخه درست کلید خصوصی می‌توان از گواهی‌های کلید عمومی یا دیگر ابزارهای وابسته به محیط استفاده کرد.

۵- هر خواهان و هر درستی‌سنج باید ابزار تولید اعداد تصادفی را داشته باشند.

۴-۲ تولید کلید

۴-۲-۱ جفت کلید نامتقارن

باید یک نمای درستی‌سنجی، یک پارامتر تعدد جفت و یک پارامتر تعدد تبادل انتخاب شود. اگر به‌گونه‌ای دیگر مشخص شود، این پارامترها، پارامترهای دامنه هستند که به ترتیب با v، m و t نشان داده می‌شوند.

- مقادیر معینی از v همانند اعداد اول ۲، ۲۵۷، $۲^{۱۶}+۱$، $۲^{۳۲}+۱۵$، $۲^{۱۳}+۲^{۳۶}+۱$و $۲^{۴۰}+۱۵$ چندین مزیت کاربردی دارند.
- مقدار m در صورتی که v=۲ باشد باید حداکثر هشت و درصورتی که v یک عدد اول فرد باشد باید برابر یک در نظر گرفته شود.
- مقدار $v^{-m\times t}$ یک سطح امنیت سازوکار را تعیین می‌کند. (به زیربند پ-۱-۴ مراجعه شود.) برای اکثر کاربردها مقداری بین $۲^{-۸}$ و $۲^{-۴۰}$ مقداری مناسب است.

یک عدد که با α نشان داده می‌شود اندازه پیمانه برحسب بیت را مطابق با متن استفاده‌ی سازوکار تعیین می‌کند. یعنی ۲^{α} >پیمانه> $۲^{\alpha-۱}$.

مرجع یا دستوردهنده باید دو یا تعداد بیشتری از عوامل اول بزرگ مجزا را که با p_1، p_2، ... به ترتیب صعودی نشان داده می‌شوند و حاصلضرب آن‌ها پیمانه را نتیجه می‌دهد مخفی نگه دارند.

- اگر v=۲ (طرح‌واره رابین[1]) باشد، باید تنها دو عامل اول وجود داشته باشد (یعنی f=۲) که هر دو با ۳ به پیمانه ۴ هم‌نهشت بوده اما با یکدیگر به پیمانه ۸ هم‌نهشت نباشند..
- اگر v یک عدد اول فرد باشد، (طرح RSA) ممکن است که بیش از دو عامل اول وجود داشته باشد. برای هر عامل اول، p_j و p_{j-1}باید نسبت به v اول باشند.

اگر α مضربی از تعداد عوامل اول باشد که با f نشان داده می‌شود، آن‌گاه اندازه بیت هر عامل اول باید α/f باشد. (برای جزییات بیشتر، به زیربند پ-۱-۲ مراجعه شود.) اگر v=۲باشد، پیمانه برابر با $p_1\times p_2$ و اگر v فرد باشد برابر $p_1\times\ldots\times p_f$ در نظر گرفته می‌شود. مطابق با نیازهای دوم در ۵-۱، پیمانه یا یک پارامتر دامنه مشخص شده با n و یا یک پارامتر خواهان نشان داده شده به‌صورت n(A) است.

یک نمای تأیید اعتبار نسبت به هر عامل اول p_j، که با u_j نشان داده می‌شود برابر با کمترین عدد صحیح مثبت در نظر گرفته می‌شود؛ به‌گونه‌ای که $u_j\times v+1$ اگر v=۲ باشد مضربی از $(p_j-1)/2$ یا اگر v یک عدد اول فرد باشد مضربی از p_j-1 خواهد بود.

1 - Rabin scheme

با توجه به پیمانه‌ها، نمای تأیید اعتبار با u_j نشان داده و برابر با کمترین عدد صحیح مثبت در نظر گرفته می‌شود؛ در این صورت u.v+1 مضربی از $lcm(p_1-1, p_2-1)/2$ درحالتی که v=2 یا مضربی از $lcm(p_1-1,\dots p_f-1)$ درحالتی که v یک عدد اول فرد باشد، خواهد بود.

۴-۲-۲ جفت(های) نامتقارن اعداد

۴-۲-۲-۱ موردی که v=۲

داده‌های شناسایی *Id(A)* باید با الحاق شانزده بیت نمایش‌دهنده اعداد ۱ تا m به m بخش تبدیل شوند. یعنی 0001، 0002 و به همین ترتیب به نوبت به رشته *Id(A)* افزوده می‌شوند.

$$Id_x(A) = Id(A)||\ '000X'$$

یادآوری – سازوکار زیر از سازوکار نخستین قالب که در استاندارد ISO/IEC 14888-2 مشخص شده به‌دست آمده است[**27**]. این سازوکار معروف به **PSS**[1] بوده و به بلار[2] و راگاوی[3] نسبت داده می‌شود.[**1**]

برای تبدیل هر قسمت از $Id_1(A)$ تا *Idm(A)* به یک رشته α بیتی که با نمادهای از F_1 تا F_m نشان داده می‌شوند، قدم‌های محاسباتی زیر انجام می‌شوند.

۱- رشته *Idx(A)* باید برای به‌دست آوردن یک کد درهم که با H_x نشان داده می‌شود، درهم‌سازی شود.

$$H_x = h\big(Id_x(A)\big)$$

۲- رشته‌ای (|h| +۶۴) بیتی از چپ به راست از الحاقی ۸ هشت‌تایی برابر با 00 و کد درهم H_x ساخته می‌شود. این رشته برای به‌دست آوردن یک کد درهم نشان داده شده با HH_x باید درهم‌سازی شود.

$$HH_x = h('00000000\ 00000000'||\ H_x)$$

۳- ماسکی شامل رشته‌ای از (α - |h| - 8) بیت از کد درهم HH_x ساخته می‌شود. این رویه از دو متغیر بهره می‌برد: یک رشته بیتی با طول متغیر که با String نشان داده می‌شود و یک شمارنده ۳۲ بیتی که با Counter نشان داده می‌شود.

الف- String را یک رشته خالی قرار دهید.

ب- Counter را برابر با 0 قرار دهید.

پ- String را با String || $h(HH_x$ || Counter) جایگزین کنید.

ت- Counter را با Counter + 1 جایگزین کنید.

ث- اگر α - |h| - 8 <counter×|h| آن‌گاه به قدم پ بروید.

متغیر $Mask_x$ برابر با (α - |h| - 8) بیت سمت چپ String است که سمت چپ‌ترین بیت آن برابر با 0 قرار داده شده‌است.

---

1 - Probabilistic Signature Scheme
2- Bellare
3- Rogaway

۴- رشته‌ای که با F_x نشان داده می‌شود از چپ به راست با الحاقی (8 - |h| - α) بیت ماسکی که سمت راست‌ترین بیت آن معکوس گشته، |h| بیت کد درهم HH_x و یک هشت‌تایی برابر BC قرار می‌گیرد.

$$F_x = Format\big(Id_x(A)\big) = (Mask_x \oplus (000 \dots 000 \,||\, 1))\; HH_x \,||\, 'BC'$$

کلید عمومی که با $G_x(A)$ نشان داده می‌شود از عدد نمایش داده شده به‌وسیله رشته بیتی F_x به‌صورت زیر به‌دست می‌آید. (F_x عددی زوج، غیرصفر و کوچکتر از پیمانه است.)

- اگر نماد ژاکوبی $(F_x \mid n)$ برابر 1+ باشد، آن‌گاه $G_x(A) = F_x$
- اگر نماد ژاکوبی $(F_x \mid n)$ برابر 1- باشد، آن‌گاه $G_x(A) = F_x/2$

مرجع یا دستوردهنده باید m کلید خصوصی که با Q_1 تا Q_m نشان داده می‌شود را در اختیار خواهان A قرار دهد. کلید خصوصی نشان داده شده به‌وسیله Q_x برابر با u امین توان پیمانه‌ای کلید عمومی $G_x(A)$ در نظر گرفته می‌شود.

$$Q_x = G_x(A)^u \Big(mod^*\ n \text{ یا } n(A)\Big)$$

یادآوری۱- فن **CRT** (به زیربند ث-۲-۳ مراجعه شود.) را می توان برای تبدیل هر کلید عمومی به یک کلید خصوصی به‌کار برد.

- برای هر عامل اول $\mathbf{p_j}$، یک مؤلفه $\mathbf{Z_j}$ برابر $\mathbf{G_x(A)^{u_j}}$ به پیمانه $\mathbf{p_j}$ قرار داده می‌شود.
- ترکیب CRT مجموعه مؤلفه‌های $\{Z_1, Z_2 \dots\}$ را به یک عدد Z تبدیل می‌کند.

یادآوری۲- هر جفت نامتقارن از اعداد که درستی یک رابطه اداره شده به‌وسیله کلید درستی‌سنجی را وارسی می‌کند.

$$\boldsymbol{G_x(A) \times Q_x^2 \equiv 1 \Big(mod^* n \text{ یا } n(A)\Big)}$$

یادآوری۳- در نتیجه هر عدد $\mathbf{G_x(A)}$ یا $\mathbf{Q_x}$ می‌تواند با پیمانه منهای عدد جایگزین شود.

۴-۲-۲-۲ مورد v برابر با یک عدد اول فرد

یادآوری – سازوکار زیر از سازوکار نخستین قالب که در استاندارد ISO/IEC 14888-2 مشخص شده به‌دست آمده است[**27**]. این سازوکار معروف به **PSS** است و به بلارو راگاوی[**1**] نسبت داده می‌شود.

برای تبدیل داده شناسایی Id (A) به یک رشته α بیتی که با نماد F نشان داده می‌شود، گام‌های محاسباتی زیر انجام می‌شوند.

۱- رشته Id (A) باید برای به‌دست آوردن یک کد درهم که با H نشان داده می‌شود، درهم‌سازی شود.

$$H = h\big(Id(A)\big)$$

۲- رشته‌ی (|h| +۶۴) بیتی از چپ به راست از الحاقی ۸ هشت‌تایی برابر با 00 و کد درهم H تشکیل می‌شود. این رشته برای به‌دست دادن یک کد درهم نشان داده شده با HH باید درهم‌سازی شود.

$$HH = h('00000000\ 00000000' || H)$$

۳- ماسکی شامل رشته‌ای از (α - |h|) بیت از کد درهم HH ساخته می‌شود. این رویه از دو متغیر بهره می‌برد: یک رشته بیتی با طول متغیر که با String نشان داده می‌شود و یک شمارنده ۳۲ بیتی که با Counter نشان داده می‌شود.

الف- String را یک رشته خالی قرار دهید.

ب- Counter را برابر با 0 قرار دهید.

پ- String را با (String || h(HH || Counter جایگزین کنید.

ت- Counter را با Counter + 1 جایگزین کنید.

ث- اگر |h|×counter <α - |h| آنگاه به قدم پ بروید.

ماسک برابر با (α - |h|) بیت سمت چپ String است که سمت چپ‌ترین بیت آن برابر با 0 قرار داده شده است.

۴- رشته‌ای که با F نشان داده می‌شود از چپ به راست با الحاق (α - |h|) بیت ماسکی که سمت راست‌ترین بیت آن معکوس گشته و |h| بیت کد درهم HH تشکیل می‌شود.

$$F_x = Format\big(Id(A)\big) = (Mask \oplus (000 \dots 000 \,||\, 1))\; HH$$

کلید عمومی که با G(A) نشان داده می‌شود برابر با عدد نمایش داده شده به‌وسیله رشته بیتی F به‌دست می‌آید (F عددی غیرصفر و کوچکتر از پیمانه است.)

$$G(A) = F$$

مرجع یا دستوردهنده باید یک کلید خصوصی که با Q نمایش داده می‌شود را در اختیار خواهان A قرار دهد. کلید خصوصی نشان داده شده به‌وسیله Q برابر با u امین توان پیمانه‌ای کلید عمومی G(A) در نظر گرفته می‌شود.

$$Q = G(A)^u \big(mod\ either\ n\ or\ n(A)\big)$$

یادآوری۱- فن **CRT** (به زیربند ث-۲-۳ مراجعه شود.) را می توان برای تبدیل هر کلید عمومی به کلید خصوصی به کار برد.

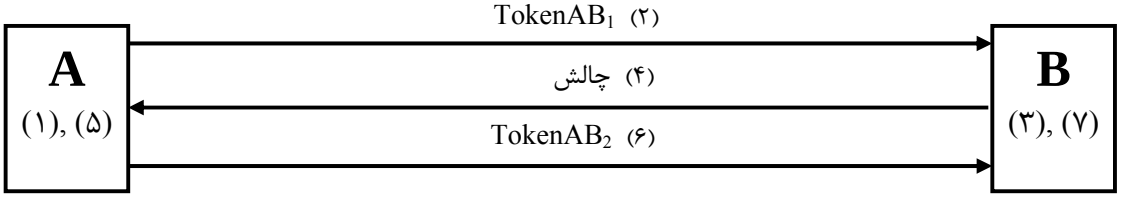
- برای هر عامل اول p_j، یک مولفه Q_j برابر $G(A)^{uj}$ به‌پیمانه p_j قرار داده می‌شود.
- ترکیب CRT مجموعه مولفه‌های $\{Q_1, Q_2 \dots\}$ را به یک عدد Q تبدیل می‌کند.

یادآوری۲- جفت نامتقارن اعداد (کلید خصوصی معکوس پیمانه‌ای امضای **RSA** است، به استاندارد **ISO/IEC 14888-2** مراجعه شود. **[27]**) درستی یک رابطه اداره شده به‌وسیله کلید درستی‌سنجی را وارسی می‌کند.

$$\boldsymbol{G(A) \times Q^v \equiv 1 \left(mod^* n \text{ یا } n(A)\right)}$$

۳-۴ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۱ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستندکه به‌تفصیل در ادامه آورده خواهند شد. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۱- سازوکار مبتنی بر هویت

خواهان باید علاوه بر داده شناسایی Id(A)، یک نمای درستی‌سنجی v (یک عدد اول)، یک پارامتر تعدد جفت m و یک پارامتر تعدد تبادل t، یک پیمانه n یا n(A) و یکی از موارد زیر را ذخیره کند:

- m کلید خصوصی Q_1 تا Q_2 اگر v = ۲ باشد،
- کلید خصوصی واحد Q اگر v یک عدد اول فرد باشد.

علاوه بر داده شناسایی Id(A)، یک نمای درستی‌سنجیv (یک عدد اول)، یک پارامتر تعدد جفت m و یک پارامتر تعدد تبادل t و یک رونوشت مورد اعتماد از یک پیمانه n یا n(A) باید در اختیار درستی‌سنج قرار گیرد. در صورت عدم آگاهی B، یک رونوشت از Id(A)، v، m و t باید به‌همراه نشانه AB_1 ارسال شود؛ نیازی به مورد اعتماد بودن چنین رونوشتی نیست.

برای هر کاربردی از سازوکار، رویه زیر باید t بار انجام شود. درستی‌سنج B باید تنها درصورتی که تمام t تکرار رویه با موفقیت به پایان رسیدند خواهان A را معتبر بداند.

۱- برای هر تکرار رویه، یک عدد جدید باید به‌طور یکنواخت به صورت تصادفی انتخاب شود. این عدد باید غیرصفر و کوچکتر از پیمانه باشد. این عدد با r نشان داده می‌شود و باید سرّی نگاه داشته شود.

عدد تصادفی جدیدr باید به یک شاهد که با W نشان داده می‌شود به‌عنوان v امین توان پیمانه‌ای تبدیل شود.

- فرمول شاهد اگر ۲=v: $W = r^2 (\mathrm{mod}\ n \text{ یا } n(A))$
- فرمول شاهد اگر v یک عدد اول فرد باشد: $W = r^v \ (\mathrm{mod}\ n \text{ یا } n(A))$

عدد W به‌وسیله رشته‌ای از α بیت نمایش داده می‌شود که این رشته هم با W نشان داده می‌شود.

۲- A نشان AB_1 را به B می‌فرستد. نشانه AB_1 ، شاهدW یا یک متغیر درهم‌سازی W وText است. متغیر درهم‌سازی به‌صورت یکی از چهار نوع زیر است.

چهار نوع متغیر درهم‌سازی عبارتند از h(W||Text)، h(W||h(Text))، h(h(W)||Text) و h(h(W)||h(Text)) که در آن h یک تابع درهم‌ساز و Text یک دسته متنی اختیاری است. (ممکن است خالی باشد.) اگر دسته متنی خالی نباشد آن‌گاه B باید ابزارهایی برای بازیابی مقدار Text داشته باشد؛ در این حالت نیاز است که A تمام یا قسمتی از دسته متنی را ارسال کند. دسته متنی برای استفاده در کاربردهای خارج از دامنه این **استاندارد** در

دسترس است. پیوست الف استاندارد ISO/IEC 9798-1 اطلاعاتی در مورد استفاده از دسته‌های متنی ارائه می‌دهد. نوع درهم‌سازی یک پارامتر دامنه است[24].

۳- با دریافت نشانه AB_1، قدم‌های محاسباتی زیر انجام می‌شود.

الف- اگر مقدار $v^{m\times t}$ کوچکتر از 2^{40} بوده و/یا اگر $m>8$ درحالی که $v=2$ و/یا اگر $m>1$ در حالی‌که v یک عدد اول فرد است، آن‌گاه رویه ناموفق خواهد بود.

ب- اگر داده شناسایی Id(A) نامعتبر باشد (به‌عنوان مثال، منقضی یا باطل شده باشد)، آن‌گاه رویه ناموفق خواهد بود.

پ- رشته جدید δ بیتی باید به‌طور تصادفی به‌صورت یکنواخت انتخاب شود.

- اگر $v=2$ آن‌گاه $\delta=m$ و رشته متشکل از m بیت است که با d_1 تا d_m نشان داده می‌شوند.
- اگر v یک عدد اول فرد باشد، آن‌گاه $\delta=|v|-1$ و رشته عددی کوچکتر از v را که می‌تواند صفر باشد، نمایش می‌دهد و با d نشان داده می‌شود.

یادآوری – توصیه می‌شود که تعداد کل چالش‌های احتمالی به ازای هر تکرار رویه به 2^{40} محدود شود. اگر به این توصیه عمل نشود آن‌گاه بهتر است ملاحظات ویژه‌ای در نظر گرفته شود. تا از درستی‌سنجی که از خواهان به‌عنوان پیشگوی[1] امضاکننده استفاده می‌کند جلوگیری شود.

۴- B رشته جدید را به‌عنوان یک چالش به A می‌فرستد.

یادآوری– بهینه‌سازی‌ها ممکن است محدودیت‌هایی را بر روی وزن همینگ[2] چالش‌ها القا کند. این بهینه‌سازی‌ها بر روی تعداد کل چالش‌های ممکن و سطح امنیت سازوکار نیز اثرگذار است.

۵- با دریافت چالش، قدم‌های محاسباتی زیر انجام می‌گیرند.

الف- اگر چالش رشته‌ای از δ بیت نباشد آن‌گاه رویه ناموفق خواهد بود.

ب- پاسخ که با D نشان داده می‌شود باید با استفاده از عدد تصادفی r و موارد زیر محاسبه شود:

- m کلید خصوصی Q_1، Q_2، ...Q_m و m بیت چالش d_1، d_2، ...d_m اگر $v=2$.

  فرمول پاسخ اگر $v=2$: $D = r \times \prod_{i=1}^{m} Q_i^{d_i} \left(mod^* \; n \text{ یا } n(A)\right)$

- کلید خصوصی واحد Q و عدد چالش d اگر v یک عدد اول فرد باشد.

  فرمول پاسخ اگر v یک عدد فرد اول باشد : $D = r \times Q^d \left(mod\; n \text{ یا } n(A)\right)$

۶- A نشانه AB_2 را به B می‌فرستد. نشانه AB_2 پاسخ D محاسبه‌شده در قدم ۵–ب است.

۷- با دریافت نشانه AB_2، قدم‌های محاسباتی انجام می‌شوند.

الف- اگر پاسخ D صفر یا برابر یا بزرگتر از پیمانه باشد، آن‌گاه رویه ناموفق خواهد بود.

ب- داده شناسایی Id(A) باید به موارد زیر تبدیل شود.

---

1 - Oracle
2 - Hamming weight

- m کلید عمومی (به زیربند ۵-۲-۲-۱ مراجعه شود.) نشان داده شده با$G_1(A)$، $G_2(A)$،... $G_m(A)$، اگر v=۲.
- کلید عمومی واحد (به زیربند ۵-۲-۲-۲ مراجعه شود.) نشان داده شده با G(A) اگر v یک عدد اول فرد باشد.

پ- شاهدی که به‌وسیله W^* نشان داده می‌شود باید محاسبه شود.

- فرمول درستی‌سنجی اگر v=۲: $W^* = D^2 \times \prod_{i=1}^{m} G_i(A)^{d_i} \left(mod^* n \text{ یا } n(A)\right)$
- فرمول درستی‌سنجی اگر v یک عدد اول فرد باشد: $W^* = D^v \times G(A)^d \left(mod\ n \text{ یا } n(A)\right)$

ت- اگر شاهد W^* یا کد درهم W^* و Text، یکی از چهارنوع درهم‌سازی، با AB_1 دریافت‌شده در قدم ۲ یکسان باشد، آن‌گاه تکرار رویه موفقیت‌آمیز است؛ در غیر این صورت رویه ناموفق خواهد بود.

یادآوری۱- ارسال اطلاعات دیگر به همراه هر تبادل روند مجاز است. **B** می تواند از چنین اطلاعاتی برای محاسبه مقدار دسته متنی اختیاری کمک گیرد.

یادآوری۲- **B** می‌تواند در هر مرحله‌ای کلید(های) عمومی را برای **A** محاسبه کند، یعنی لازم نیست که **B** تا رسیدن پاسخ **D** پیش از محاسبه آن‌ها منتظر بماند. اگر **B** دائماً درستی **A** را بسنجد آن‌گاه ممکن است **B** کلید(های) عمومی را سرّی کند.

یادآوری۳- **t** تکرار از رویه می‌تواند به‌طور موازی اجرا شود یعنی در قدم نخست **A** مجاز است که **t** عدد تصادفی $\mathbf{r_1}$، $\mathbf{r_2}$ ... $\mathbf{r_t}$ را انتخاب کرده، **t** شاهد $\mathbf{W_1}$، $\mathbf{W_2}$، ... $\mathbf{W_t}$ را محاسبه کند، آن‌ها را به‌طور همزمان به **B** بفرستد و به همین ترتیب. اگر این پیاده‌سازی موازی اتخاذ شود آن‌گاه تعداد کل تبادلات پیام، فارغ از مقدار **t**، برابر با سه خواهد بود.

یادآوری۴- استفاده از کد درهم به‌جای شاهد **W** در نخستین مبادله رویه می‌تواند با کاهش تعداد بیت‌ها در نشانه $\mathbf{AB_1}$ به افزایش کارایی منجر شود.

۵ سازوکارهای مبتنی بر تجزیه به عوامل صحیح

۵-۱ الزامات امنیتی برای محیط

این سازوکارها یک درستی‌سنج را قادر می‌سازد تا آگاهی یک خواهان از تجزیه یک پیمانه مورد ادعا را وارسی کند.

یادآوری – این سازوکارها طرح‌ها را با توجه به گویلو و کویسکاتر [12] پیاده‌سازی کرده و با **GQ2** نمایش داده می‌شوند.

درون یک دامنه معین، الزامات زیر باید برآورده شوند.

۱- پارامترهای دامنه‌ای که به عملیات سازوکار اداره می‌کنند باید انتخاب شوند. پارامترهای انتخاب شده باید به شیوه‌ای قابل اطمینان به همه هستارهای درون دامنه شناسانده شوند.

۲- عوامل اول مجزا باید به‌گونه‌ای در اختیار هر خواهان قرار گیرند که آگاهی از حاصلضرب آن‌ها داشته باشد. یعنی پیمانه‌ها (یک پارامتر خواهان) به‌طور عملی نتواند هر هستاری را قادر سازد تا آن‌ها را نتیجه بگیرد. در این‌جا امکان‌پذیری به‌وسیله متن استفاده از سازوکار تعریف می‌شود.

یادآوری – در هنگام باز کردن یک نشست (مطابق شکل ۵-۱) یک رایانه می‌تواند به‌طور تصادفی دو عامل اول را برای استفاده در طول نشست انتخاب کند. (چند ساعت) با استفاده از رمز درازمدت دستوردهنده در یک «ورود یک‌باره» داده شناسایی نشست، رایانه یک مجوز «کم دوام[1]» را امضا می‌کند که یک پیمانه کم‌دوام را پوشش می‌دهد و حاصلضرب عوامل اول کم‌دوام است.

۳- هر درستی‌سنج باید یک رونوشت مورد اعتماد از پیمانه مشخص‌شده‌ی خواهان را به‌دست آورد.

یادآوری – نحوه دقیق دستیابی درستی‌سنج به یک رونوشت مورد اعتماد از پیمانه مختص خواهان فراتر از حیطه این استاندارد است. به‌عنوان مثال ممکن است با استفاده از گواهی‌های کلید عمومی یا دیگر ابزارهای وابسته به محیط به آن دست یافت.

۴- هر خواهان و هر درستی‌سنج باید ابزارهای تولید اعداد تصادفی را داشته باشند.

۵- اگر سازوکار از یک تابع درهم‌ساز استفاده کند آن‌گاه تمامی هستارهای درون دامنه باید بر سر یک تابع درهم‌ساز توافق کنند، به‌عنوان مثال یکی از توابع مشخص شده در استاندارد ISO/IEC 10118-3[25] .

۵-۲ تولید کلید

عددی که با α نشان داده می‌شود اندازه پیمانه برحسب بیت را مطابق با متن استفاده از سازوکار تعیین می‌کند، (برای جزییات بیشتر به زیربند پ-۱-۱ مراجعه شود.)؛ یعنی $2^{\alpha-1} <$ پیمانه $< 2^{\alpha}$. این پارامتر یک پارامتر دامنه است.

یک پارامتر امنیت و یک پارامتر تعدد جفت که با k و m نمایش داده می‌شوند به همراه یکدیگر سطح امنیت سازوکار برابر با $2^{-k\times m}$ مطابق با نیازهای کاربرد را قرار می‌دهد. (به زیربند پ-۱-۴ مراجعه شود.) این پارامترها پارامترهای دامنه هستند. یک مقدار $k\times m$ از ۸ تا ۴۰ برای اکثر کاربردها مقداری مناسب است.

یادآوری ۱– توصیه می‌شود که تعداد کل چالش‌های احتمالی به ازای هر تکرار روند به 2^{40} محدود شود. اگر به این توصیه‌نامه عمل نشود، آن‌گاه بهتر است ملاحظات ویژه‌ای در نظر گرفته شود تا از استفاده درستی‌سنج از خواهان به‌عنوان پیشگوی امضاکننده اجتناب ورزید..

خواهان A باید دو یا تعداد بیشتری از عوامل اول بزرگ مجزا را سرّی نگاه دارد. این عوامل با p_1، p_2، ... به ترتیب صعودی نشان داده می‌شوند. اگر α مضربی از تعداد عوامل اول که با f نمایش داده می‌شود باشد، آن‌گاه اندازه بیت هر عامل اول باید α / f باشد. (برای جزییات بیشتر، به زیربند پ-۱-۲ مراجعه شود.)

هر عامل اول p_j یک عدد را تعیین می‌کند که با b_j نشان داده می‌شود به‌گونه‌ای که $p_j - ۱$ بر 2^{bj} بخش‌پذیر بوده اما به 2^{bj+1} بخش‌پذیر نباشد؛ یعنی $b_j +$ ۱ بیت کم‌اهمیت $p_j - ۱$ یک بیت برابر با ۱ و b_j بیت برابر با 0 هستند و $(p_j - ۱) / 2^{bj}$ عددی فرد است.

1- Ephemeral

یادآوری۲- اگر $p_j \equiv 3 \bmod 4$، عدد b_j برابر یک و اگر $p_j \equiv 1 \bmod 4$، b_j برابر دو یا بیشتر قرار داده می‌شود.

جهت هم‌ارزی با تجزیه پیمانه، نخستین ۵۴ عدد اول یعنی {۲، ۳، ۵، ۷، ۱۱، ... ۲۵۱} یا اعداد دارای اندازه بیت برابر یا کمتر از هشت برای یافتن یک عدد مناسب g مورد جستجو قرار می‌گیرند.

- نماد لژاندر یک عدد نامزد g نسبت به هر عامل اول از p_1 تا p_f مورد ارزیابی قرار می‌گیرد. اگر دو عامل اول p_j و p_i به‌صورت زیر وجود داشته باشند، عدد نامزد g عددی مناسب است.
- اگر $b_j = b_i$، نمادهای لژاندر متفاوت باشند، یعنی $(g \mid p_j) = - (g \mid p_i)$.
- اگر $b_j > b_i$، نماد لژاندر نسبت به p_j برابر ۱- باشد، یعنی $(g \mid p_j) = -1$.

یادآوری۳- به‌طور میانگین، هر عدد نامزد با شانس ۱ در 2^{f-1} مناسب است. در نتیجه احتمال نیافتن یک عدد مناسب g میان ۵۴ عدد اول نخست ناچیز است.

m عدد پایه‌ای عدد g هستند که به‌وسیله تعداد مورد نیاز از ۵۴ عدد اول نخست کامل می‌شود. همچنین اگر آن‌ها m عدد اول باشند، پارامترهای دامنه هستند که با g_1 تا g_m به‌صورت صعودی نشان داده می‌شوند، در غیر این‌صورت، پارامترهای خواهان هستند که با $g_1(A)$ تا $g_2(A)$ با ترتیب صعودی نشان داده می‌شوند.

یادآوری۴- اگر اعداد پایه‌ای m به‌صورت نظام‌مند نخستین m عدد اول بدون وارسی نمادهای لژاندر باشند، آن‌گاه برای f عامل اول بزرگ که به‌طور تصادفی تولید شده‌اند، احتمال این که آگاهی از مجموعه کلیدهای خصوصی سبب آگاهی از یک تجزیه پیمانه شود، به‌طور میانگین کمتر از $2^{-m\times(f-1)}$ است.

پارامتر سازگاری که با b نشان داده می‌شود برابر با بیشینه (b_1 تا b_f) قرار داده می‌شود. این پارامتر، پارامتر خواهان است. به ازای عدد پایه‌ای g_i یا $g_i(A)$، یک کلید عمومی که با G_i نشان داده می‌شود برابر با b امین مربع عدد پایه‌ای قرار داده می‌شود.

$$G_i = g_i^{2^b} \text{ یا } g_i(A)^{2^b}$$

نمای درستی‌سنجی که با v نشان داده می‌شود برابر با 2^{k+b} قرار داده می‌شود. به ازای هر عامل اول p_j، یک نمای تایید اعتبار که با u_j نشان داده می‌شود برابر با کوچکترین عدد صحیح مثبت قرار داده می‌شود به‌گونه‌ای که $v\times u_j+1$ مضربی از $(p_j-1)/2^{bj}$ باشد.

برای هر عدد پایه‌ای g_i یا $g_i(A)$ و هر عامل اول p_j، یک مؤلفه خصوصی که با $Q_{i,j}$ نشان داده می‌شود برابر u_j امین توان پیمانه‌ای کلید عمومی G_i قرار داده می‌شود.

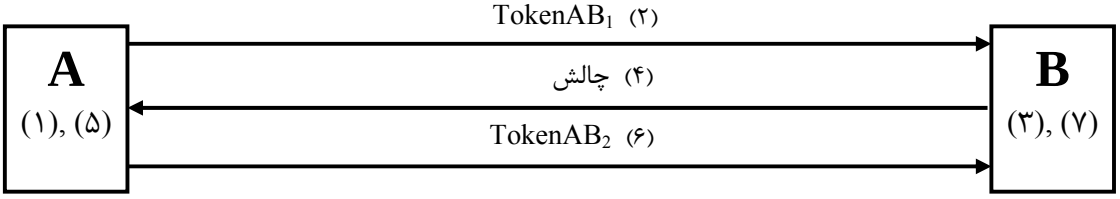
$$Q_{i,j} = G_i^{u_j} \bmod p_j$$

پیمانه برابر با حاصلضرب عوامل اول بزرگ یعنی $p_1 \times \ldots \times p_f$ قرار داده می‌شود. این پارامتر یک پارامتر خواهان است که با $n(A)$ نشان داده می‌شود.

یادآوری۵- همان پیمانه را می توان برای سازوکارهای **GQ2** و **RSA** استفاده کرد.

۳-۵ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۲ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستندکه با جزییات در ادامه آورده خواهند شد. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۲- سازوکارهای مبتنی بر تجزیه به عامل‌های پیمانه

علاوه بر پارامترهای b، k و m، m عدد پایه‌ای g_1 تا g_m یا $g_1(A)$ تا $g_m(A)$، خواهان باید یکی از دو مورد زیر را نیز ذخیره کند.

- پیمانه n(A) و m کلید خصوصی Q_1 تا Q_m یا
- f عامل اول p_1 تا p_f، f×m مؤلفه خصوصی $Q_{1,1}$ تا $Q_{m,f}$ و (f-۱) ضریب CRT (به زیربند پ-۲-۳ مراجعه شود.)

علاوه بر پارامترهای b، k و m و m عدد پایه‌ای g_1 تا g_m یا $g_1(A)$ تا $g_m(A)$، یک رونوشت مورد اعتماد از پیمانه n(A) خواهان باید در اختیار درستی‌سنج قرار گیرد. در صورت عدم آگاهی B، یک رونوشت از b، k ، m و $g_1(A)$ تا $g_m(A)$ باید به همراه نشانه AB_1 ارسال شود؛ نیازی به مورد اعتماد بودن چنین رونوشتی نیست.

برای هر کاربردی از این سازوکار، رویه زیر باید انجام شود. درستی‌سنج B باید تنها درصورتی که رویه با موفقیت به پایان رسید خواهان A را معتبر بداند.

۱- برای هر تکرار رویه، برای هر عامل اول p_j، یک عدد جدید باید به‌طور یکنواخت و به‌صورت تصادفی انتخاب شود. این عدد باید غیرصفر و کوچکتر از p_j باشد. این عدد با r_j نشان داده می‌شود و باید سرّی نگاه داشته شود.

هر عدد تصادفی جدید r باید به یک مؤلفه شاهد که با W_j نشان داده می‌شود تبدیل شود.

فرمول مؤلفه شاهد : $W_j = r_j^v \bmod p_j$

با به‌کار گرفتن مجموعه‌ای از عوامل اول و ضریب(های) CRT، یک ترکیب CRT (زیربند پ-۲-۳ را ببینید.) باید مجموعه مؤلفه‌های شاهد $\{W_1, W_2, ...\}$ را به یک شاهد که با W نشان داده می‌شود، تبدیل کند. عدد W به‌وسیله رشته‌ای از α بیت نمایش داده می‌شود که این رشته هم با W نشان داده می‌شود.

۲- A نشان AB_1 را به B می‌فرستد. نشانهAB_1 شاهدW یا یک کد درهم W و Text است. کد درهم به‌صورت یکی از چهار متغیر زیر است.

چهار متغیر درهم‌ساز عبارتند از h(W||Text)، h(W||h(Text))، h(h(W)||Text) و h(h(W)||h(Text)) که در آن h یک تابع درهم‌ساز و Text یک دسته متنی اختیاری است. (ممکن است خالی باشد.) اگر دسته متنی خالی نباشد، آن‌گاه B باید ابزاری برای بازیابی مقدار Text داشته باشد؛ در این حالت نیاز است که A

تمام یا قسمتی از دسته متنی را ارسال کند. دسته متنی برای استفاده در کاربردهای خارج از دامنه این استاندارد در دسترس است. در پیوست الف استاندارد ISO/IEC 9798-1[24]، اطلاعاتی در مورد استفاده از دسته‌های متنی وجود دارد. نوع درهم‌سازی یک پارامتر دامنه است.

۳- با دریافت نشانه AB_1، قدم‌های محاسباتی زیر انجام می‌شود:

الف- اگر حاصل $k \times m$ بزرگتر از ۴۰ باشد، رویه ناموفق است.

ب- اگر اعداد پایه‌ای اعداد اول مجزای کمتر از ۲۵۶ نباشند، آن‌گاه رویه ناموفق است.

پ- رشته جدید $k \times m$ بیتی باید به‌صورت تصادفی به‌طور یکنواخت انتخاب شود. این رشته با $d_{1,1}$ تا $d_{m,k}$ نشان داده می‌شود.

۴- B رشته جدید را به‌عنوان یک چالش به A می‌فرستد.

یادآوری- بهینه‌سازی‌ها ممکن است محدودیت‌هایی را بر روی وزن همینگ چالش‌ها القا کنند. این بهینه‌سازی‌ها بر روی تعداد کل چالش‌های ممکن و سطح امنیت سازوکار نیز اثرگذار هستند.

۵- با دریافت چالش، قدم‌های محاسباتی زیر انجام می‌گیرند:

الف- اگر چالش رشته‌ای از $k \times m$ بیت نباشد، آن‌گاه رویه ناموفق خواهد بود.

ب- برای هر عامل اول p_j، یک مؤلفه D_j را باید از چالشی که با $d_{1,1}$ تا $d_{m,k}$ نشان داده می‌شود، m مؤلفه خصوصی $Q_{1,j}$ تا $Q_{m,j}$ و عدد تصادفی r_j محاسبه کرد.

با آغاز از یک عدد که برابر یک قرار داده شده، k-1 مربع پیمانه‌ای در k دنباله از صفر تا m ضرب پیمانه‌ای جای داده می‌شود. i امین دنباله به‌صورت زیر است: برای i از ۱ تا m، بیت $d_{i,ii}$ نشان می‌دهد که آیا عدد فعلی باید به‌صورت پیمانه‌ای در مؤلفه خصوصی $Q_{i,j}$ (بیت برابر ۱) ضرب شود یا خیر (بیت برابر 0). یک ضرب پیمانه‌ای نهایی به‌وسیله عدد تصادفی r_j یک عدد نهایی را تولید می‌کند، یعنی یک مؤلفه پاسخ که با D_j نمایش داده می‌شود.

در نتیجه، با در نظر گرفتن این مطلب، از بیت $d_{i,1}$ به‌عنوان مهم‌ترین بیت تا بیت $d_{j,k}$ به‌عنوان کم‌اهمیت‌ترین بیت، هر رشته k بیتی نشان‌دهنده یک عدد کوچکتر از 2^k، شاید صفر، است که با d_i نشان داده می‌شود. فرمول مؤلفه پاسخ به‌صورت زیر است:

$$D_j = r_j \times \prod_{i=1}^{m} Q_{i,j}^{d_i} \bmod p_j$$

با به‌کار گرفتن مجموعه عوامل اول و ضریب(های) CRT، یک ترکیب CRT (به زیربند پ-۲-۳ مراجعه شود.) باید مجموعه مؤلفه‌های پاسخ {D1، D2، ... } را به یک پاسخ که با D نشان داده می‌شود، تبدیل کند.

۶- A نشانه AB_2 را به B می‌فرستد. نشانه AB_2 پاسخ D محاسبه شده در قدم ۵-ب است.

۷- با دریافت نشانه AB_2، قدم‌های محاسباتی زیر انجام می‌شوند:

الف- اگر پاسخ D **صفر** یا برابر یا بزرگتر از n(A) باشد، آن‌گاه رویه ناموفق خواهد بود.

ب- پاسخ D باید به یک شاهد که با W^* نشان داده می‌شود تبدیل شود.
با آغاز از یک عدد که برابر D قرار داده شده، k عملیات مقدماتی[1] در (b+k) مربع پیمانه‌ای جای داده می‌شود. ii امین عملیات مقدماتی بین ii امین و (ii+۱)امین مربع‌های پیمانه‌ای واقع می‌شود. ii امین عملیات مقدماتی به‌صورت زیر است: برای i از ۱ تا m، بیت $d_{i,ii}$ بیان می‌کند که آیا عدد فعلی باید به‌صورت پیمانه‌ای در عدد پایه‌ای g_i (بیت برابر ۱) ضرب شود یا خیر (بیت برابر 0).
در نتیجه، با در نظر گرفتن این مطلب، از بیت $d_{i,1}$ به‌عنوان مهم‌ترین بیت تا بیت $d_{j,k}$ به‌عنوان کم‌اهمیت‌ترین بیت، هر رشته k بیتی نشانگر یک عدد کوچکتر از ۲^k، شاید صفر، است که با d_i نشان داده می‌شود. فرمول درستی‌سنجی به‌صورت زیر است:

$$W^* = D^v \times \prod_{i=1}^{m} G_i^{d_i} \; mod \; n(A)$$

پ- اگر شاهد W^* یا کد درهم W^* و Text، یکی از چهار نوع درهم‌سازی، با نشان AB_1 دریافت‌شده در قدم ۲ یکسان باشد، آن‌گاه رویه موفقیت آمیز است، در غیر این صورت، رویه ناموفق خواهد بود.

یادآوری۱- ارسال اطلاعات دیگر به همراه هر تبادل روند مجاز است. **B** می‌تواند از چنین اطلاعاتی برای محاسبه مقدار دسته متنی اختیاری کمک بگیرد. به‌عنوان مثال، **A** می تواند اطلاعاتی مانند گواهی‌ها را با نشانه $\mathbf{AB_1}$ بفرستد.

یادآوری۲- برای محاسبه شاهد و پاسخ، فن **CRT** (به زیربند پ-۲-۳-۳ مراجعه شود.) اختیاری است.

یادآوری۳- استفاده از کد درهم به‌جای شاهد **W** در نخستین تبادل رویه می‌تواند با کاهش تعداد بیت‌ها در نشانه $\mathbf{AB_1}$ سبب دستیابی به بهره‌وری بالاتر شود. به علاوه، این موضوع از بروز خطا به هنگام استفاده از دستگاه‌های قابل‌حمل مانند کارت‌های هوشمند جلوگیری می‌کند.

۶ سازوکارهای مبتنی بر لگاریتم‌های گسسته نسبت به اعداد اول

۶-۱ الزامات امنیتی برای محیط

این سازوکارها یک درستی‌سنج را قادر می‌سازند تا آگاهی یک خواهان از لگاریتم گسسته یک کلید عمومی مورد ادعا را به ازای یک عدد اول مورد وارسی قرار دهند.

یادآوری – این سازوکارها طرح‌ها را با توجه به شنور[2] **[21]** پیاده‌سازی کرده و با **SC** نمایش داده می‌شوند.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:
۱- پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کنند باید انتخاب شوند. پارامترهای انتخابی باید به شیوه‌ای قابل اطمینان به همه هستارهای درون دامنه شناسانده شوند.
۲- عدد مورد استفاده به‌عنوان مبنای لگاریتم‌های گسسته باید به‌گونه‌ای باشد که به ازای هر عدد دلخواه j که غیرصفر و کوچکتر از پیمانه است، یافتن عددی مانند k (اگر موجود باشد.) به‌طوری‌که k امین توان

1 - Elementary
1- Schnorr

پیمانه‌ای پایه برابرj باشد، به‌طور محاسباتی امکان‌پذیر نباشد. در این‌جا امکان‌پذیر بودن به‌وسیله متن استفاده از سازوکار تعریف می‌شود.

۳- باید برای هر خواهان یک کلید شخصی فراهم شود.

۴- هر درستی‌سنج باید یک کپی مورد اعتماد از کلید عمومی مختص خواهان را به‌دست آورد.

یادآوری – نحوه دقیق دستیابی درستی‌سنج به یک رونوشت قابل اطمینان از کلید عمومی مختص خواهان فراتر از حیطه این استاندارد است. به‌عنوان مثال، ممکن است با استفاده از گواهی‌های کلید عمومی یا دیگر روش‌های وابسته به محیط به آن دست یافت.

۵- هر خواهان و هر درستی‌سنج باید ابزارهای تولید اعداد تصادفی را داشته باشند.

۶- اگر سازوکار از یک تابع درهم‌ساز استفاده کند، آن‌گاه تمامی هستارهای درون حوزه باید بر سر یک تابع درهم‌ساز توافق کنند؛ به‌عنوان مثال، یکی از توابع مشخص شده در استاندارد ISO/IEC 10118-3[25] .

۶-۲ تولید کلید

سه عدد که با p، q و g نشان داده می‌شوند، باید مطابق با متن استفاده از سازوکار انتخاب شوند:

- پیمانه p باید یک عدد اول باشد. اندازه بیت عدد p با | p | نشان داده می‌شود.
- عدد q باید یک عامل اول p -۱ باشد. اگر به‌گونه‌ای دیگر مشخص شده باشد، اندازه بیت عدد q برابر ۱۶۰ است؛ به‌عبارت دیگر، ۱۶۰=|q|.
- پایه لگاریتم‌های گسسته که با g نشان داده می‌شود باید از مرتبه q به پیمانه p باشد؛ یعنی عددی بزرگتر از ۱ به طوری که $g^q \bmod p = 1$. پایه g به راحتی به‌عنوان رشته‌ای از |p| بیت نمایش داده می‌شود.

یادآوری۱– می‌توان عدد اول p را طوری انتخاب کرد که رونوشتی از نمایش دودویی q درون نمایش دودویی p تعبیه شود[1]. در مواقعی که فضای ذخیره‌سازی یا پهنای باند از اهمیت بالایی برخوردار است، چنین روشی می‌تواند برای انتخاب p و q مفید باشد. به مثالی که در زیربند ت-۵-۱ آورده شده است مراجعه شود.

یادآوری۲– اگر عامل فرد، کوچکتر از q تقسیم بر p-1 وجود داشته باشد، آن‌گاه ممکن است کلید خصوصی به وسیله حمله‌ای که به‌وسیله لیم و لی[2] شرح داده شده است کشف شود. برای جلوگیری از چنین حمله‌ای، p و q بهتر است به گونه‌ای انتخاب شوند که $(\boldsymbol{p-1})/(\boldsymbol{2\times q})$ هیچ عامل اولی کوچکتر از q نداشته باشد. در حالت ایده‌آل، $(\boldsymbol{p-1})/(\boldsymbol{2\times q})$ بهتر است اول باشد.

به هر خواهان A باید عددی جدید داده شود که به‌طور یکنواخت و به‌صورت تصادفی انتخاب می‌شود. این عدد غیرصفر و کوچکتر از q است و یک کلید خصوصی را که با Q نشان داده می‌شود نمایش می‌دهد. این عدد به‌وسیله یک رشته |q| بیتی نمایش داده می‌شود.

کلید عمومی برای خواهانA که با G(A) نشان داده می‌شود برابر با Q امین توان پیمانه‌ای پایه g است. این کلید به‌وسیله یک رشته |p| بیتی نمایش داده می‌شود.

$$G(A) = g^{Q} \bmod p$$

---

2 - Embed

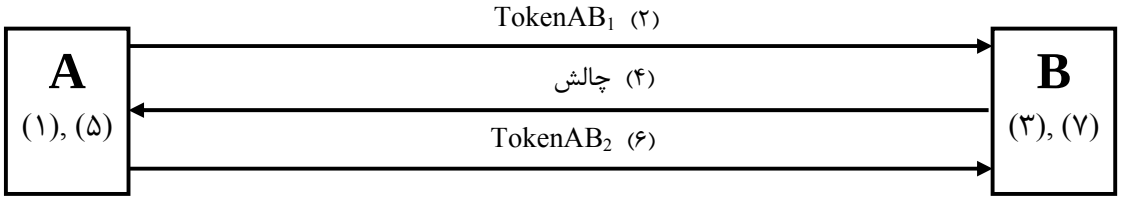
2 - Lim and Lee

عددی که با δ نشان داده می‌شود تعداد بیت‌ها را برای نمایش چالش‌ها تعیین می‌کند. یک δ با مقداری بین ۸ تا ۴۰ برای بسیاری از کاربردها مناسب است. اگر به‌گونه‌ای دیگر مشخص شده باشد، مقدار δ برابر ۴۰ قرار داده می‌شود.

یادآوری- توصیه می‌شود تعداد کل چالش‌های ممکن به 2^{40} محدود شود. اگر به این توصیه عمل نشود، آن‌گاه بهتر است ملاحظات ویژه‌ای در نظر گرفته شود تا درستی‌سنج از خواهان به‌عنوان پیشگوی امضاکننده استفاده نکند.

۳-۶ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۳ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستند که با جزییات در ادامه آورده خواهند شد. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۳ – سازوکار استفاده‌کننده از یک الگوریتم گسسته نسبت به یک عدد اول

علاوه بر اعداد اول p و q، یک عدد δ و یک پایه g، خواهان باید یک کلید خصوصی Q را ذخیره کند.
در مورد راهبرد کوپن، خواهان باید یک کلید خصوصی Q، یک عدد δ و مجموعه‌ای از کوپن‌ها را ذخیره کند. برای این‌که هر کوپن فقط یک بار استفاده شود، هر یک شامل یک عدد با |q| بیت (اگر بتوان آن را به‌وسیله یک تابع شبه‌تصادفی بازتولید کرد، نیازی به ذخیره کردن آن نیست.) و یک شاهد با α بیت (یا به‌صورت ترجیحی کد درهم آن) است.
باید علاوه بر اعداد اول p و q، یک عدد δ و یک پایه g، رونوشتی مورد اعتماد از یک کلید عمومی مورد ادعای G(A) برای درستی‌سنج فراهم کرد.
برای هر کاربرد سازوکار، باید رویه زیر انجام گیرد. اگر این رویه با موفقیت پایان پذیرد، درستی‌سنج B فقط باید خواهان A را معتبر بداند.

۱- برای هر احراز هویت، یک عدد جدید غیرصفر و کوچکتر از q باید به‌طور یکنواخت و به‌صورت تصادفی انتخاب شود. این عدد که با r نشان داده می‌شود باید سرّی نگه داشته شود. باید عدد تصادفی جدید r را به شاهدی که با W نشان داده می‌شود، تبدیل کرد. عدد W که با یک رشته α بیتی نمایش داده می‌شود نیز با W نشان داده می‌شود.
فرمول شاهد: $$W = g^r \bmod p$$
۲- A نشان AB_1 را به B می‌فرستد. نشانه AB_1 شاهد W یا کد درهم W و Text است. کد درهم به‌صورت یکی از چهار نوع زیر است.

چهار متغیر درهم‌ساز عبارتند از h(W||Text)، h(W||h(Text))، h(h(W)||Text) و h(h(W)||h(Text)) که در آن h تابع درهم‌ساز و Text یک دسته متنی اختیاری است. (ممکن است خالی باشد.) اگر دسته متنی خالی نباشد، آن‌گاه B باید ابزاری برای بازیابی مقدار Text داشته باشد؛ در این حالت نیاز است که A تمام یا قسمتی از دسته متنی را ارسال کند. دسته متنی برای استفاده در کاربردهای خارج از حیطه این استاندارد در دسترس است. پیوست الف استاندارد ISO/IEC 9798-1[24] اطلاعاتی در مورد استفاده از دسته‌های متن ارائه می دهد. نوع درهم‌سازی یک پارامتر دامنه است.

۳- با دریافت نشانه AB_1 باید یک رشته جدید δ بیتی به‌طور یکنواخت و به‌صورت تصادفی انتخاب شود.

۴- B رشته جدید را به‌عنوان چالش به A می‌فرستد. رشته جدید یک عدد را که با d نشان داده می‌شود؛ نمایش می‌دهد.

۵- با دریافت چالش، قدم‌های محاسباتی زیر انجام می‌شوند.

الف- اگر چالش یک رشته δ بیتی نباشد، رویه ناموفق است.

ب- پاسخ D باید از عدد تصادفی r و کلید خصوصی Q محاسبه شود.

فرمول پاسخ: $D = r - d \times Q \ mod \ q$

۶- A نشانه AB_1 به B می‌فرستد. نشانه AB_1 پاسخ D است که از مرحله ۵-ب محاسبه می‌شود.

۷- با دریافت نشانه AB_1، مراحل محاسباتی زیر انجام می‌شوند.

الف- اگر پاسخ D صفر بوده یا برابر یا بزرگتر از q باشد، آن‌گاه این رویه ناموفق است.

ب- شاهدی که با *W نشان داده می‌شود با استفاده از کلید عمومی G(A) محاسبه می‌شود.

فرمول درستی‌سنجی: $W^* = G(A)^d \times g^D \ mod \ p$

پ- اگر شاهد W^* یا کد درهم W^* و Text که یکی از چهار نوع درهم‌سازی هستند با نشان AB_1 دریافت شده در مرحله ۲ یکسان باشد، آن‌گاه این رویه موفق است. در غیر این صورت، ناموفق خواهد بود.

یادآوری۱- ارسال اطلاعات دیگر به همراه هر تبادل رویه مجاز است. B می‌تواند از چنین اطلاعاتی برای محاسبه مقدار دسته متنی اختیاری کمک بگیرد. برای مثال، A می‌تواند اطلاعاتی از قبیل گواهی به همراه نشانه AB_1 را ارسال کند.

یادآوری۲- استفاده از یک کد درهم به‌جای شاهد W در نشانه AB_1 می‌تواند با کاهش تعداد بیت‌های موجود در نشانه AB_1 باعث افزایش کارایی شود.

۷ سازوکارهای مبتنی بر لگاریتم‌های گسسته نسبت به اعداد مرکب

۷-۱ الزامات امنیتی برای محیط

با استفاده از این سازوکارها، یک درستی‌سنج می‌تواند آگاهی یک خواهان از لگاریتم گسسته یک کلید عمومی نسبت به عدد مرکب را وارسی کند. کلید عمومی و/ یا عدد مرکب مورد ادعا واقع شده‌اند.

یادآوری- این سازوکارها طرح‌ها را با توجه به گیرال[1]، پوپار[2] و اشترن[3] و نیز گیرال و پیه[4] به ترتیب برای GPS1 و GPS2 پیاده‌سازی کرده است.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

۱- پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کنند باید انتخاب شوند. این پارامترهای دامنه شامل یکی از دوحالت استفاده می‌شوند که از این پس مشخص می‌شوند. پارامترهای انتخاب شده باید به‌صورتی قابل‌اطمینان به تمامی هستارهای درون دامنه معرفی شوند.

۲- هر خواهان باید به یک پیمانه مجهز شود. این پیمانه پارامتر دامنه یا پارامتر خواهان است. هر عدد که به‌عنوان پیمانه استفاده می‌شود باید به‌گونه‌ای باشد که مقدار آن امکان حدس زدن عامل‌های اول آن را برای هیچ هستاری فراهم نکند. امکان‌پذیری با توجه به متن استفاده سازوکار تعریف می‌شود.

۳- هر عدد که به‌عنوان پایه لگاریتم‌های گسسته مورد استفاده قرار می‌گیرد باید به‌گونه‌ای باشد که برای هر عدد دلخواه j، غیرصفر و کوچکتر از پیمانه بوده و یافتن عدد k (در صورت وجود) به‌طوری که k امین توان پیمانه‌ای پایه برابر j باشد، به‌صورت محاسباتی امکان‌پذیر نباشد. امکان‌پذیری با توجه به متن کاربرد سازوکار تعریف می‌شود.

۴- هر خواهان باید مجهز به یک کلید خصوصی باشد.

۵- هر درستی‌سنج باید یک رونوشت مورد اعتماد از کلید(های) عمومی مشخص شده خواهان را به‌دست آورد.

یادآوری- ابزاری که به‌وسیله آن درستی‌سنج یک رونوشت مورد اعتماد از کلید(های) عمومی **مشخص شده** خواهان به‌دست می‌آورد خارج از محدوده این استاندارد است. برای مثال، این امکان وجود دارد که بتوان با استفاده از گواهی‌های کلید عمومی یا بعضی از ابزارهای وابسته به محیط این رونوشت را به‌دست آورد.

۶- هر خواهان و هر درستی‌سنج باید ابزار تولید رشته‌های جدید بیت‌های تصادفی را در اختیار داشته باشند.

۷- اگر سازوکار از یک تابع درهم‌ساز استفاده کند، آن‌گاه تمامی هستارهای درون دامنه باید بر روی آن تابع درهم‌ساز توافق داشته باشند. برای مثال، می‌توان یکی از توان مشخص شده در استاندارد ISO/IEC 10118-3[25] را به‌کار برد.

1 - Girault
2 - Poupard
3 - Stern
4 - Paillès

۷-۲ تولید کلید

۷-۲-۱ کلیات

عـددی که با α نشـان داده می‌شـود اندازه بیت پیمانه را مطابق متن اسـتفاده سـازوکار تعیین می‌کند؛ یعنی 2^{α} پیمانه $2^{\alpha-1}$ (برای جزییات بیشتر، به زیربند پ-۱-۱ مراجعه شود.) α یک پارامتر دامنه است.

عددی که با δ نشان داده می‌شود تعداد بیت‌ها برای نمایش چالش‌ها را تعیین می‌کند. مقداری بین ۸ و ۴۰ برای بسیاری از کاربردها مناسب است. اگر به‌گونه‌ای دیگر مشخص شده باشد، مقدار δ برابر ۴۰ قرار داده می‌شود. δ یک پارامتر دامنه است.

یادآوری- توصیه می‌شود تعداد کل چالش‌های ممکن به 2^{40} محدود شود. اگر به این توصیه عمل نشود، آن‌گاه بهتر است ملاحظات ویژه‌ای در نظر گرفت تا درستی‌سنج از خواهان به‌عنوان پیشگوی امضاکننده استفاده نکند..

درون دامنه، یکی از دو حالت استفاده‌ای که از این پس مشخص می‌شوند باید انتخاب شوند.

۷-۲-۲ اولین حالت استفاده (GPS1)

عددی که با δ نشان داده می‌شود تعداد بیت‌ها برای نمایش کلیدهای خصوصی را تعیین می‌کند. اگر به‌گونه‌ای دیگر مشخص شده باشد، مقدار δ برابر ۱۶۰ قرار داده می‌شود. δ یک پارامتر دامنه است.

باید برای خواهان A یک رشته جدیدσ بیتی به‌طور یکنواخت و به‌صورت تصادفی انتخاب کرد. این رشته که با Q نشان داده می‌شود کلید خصوصی را نمایش می‌دهد.

پیمانه هم می‌تواند پارامتر دامنه باشد که با n نشان داده می‌شود هم پارامتر خواهان که با n(A) نشان داده می‌شود. در هر دو مورد ممکن است عوامل پیمانه به‌طور مثال عوامل بزرگ اول آن ناشناخته باشند. (به پیوست پ-۱-۲ مراجعه شود.)

کلید عمومی برای خواهان A که با G(A) نشان داده می‌شود برابر با Q امین توان پیمانه‌ای پایه g است. این کلید به‌وسیله یک رشته α بیتی نمایش داده می‌شود.

$$G(A) = g^{Q} \pmod{n \text{ یا } n(A)}$$

۷-۲-۳ دومین حالت استفاده (GPS2)

نمای درستی‌سنجی که با نشان داده می‌شود یک پارامتر دامنه است. این پارامتر باید اول و بزرگتر از 2^{δ} باشد. از آن جایی که مقدار δ برابر ۴۰ قرار داده شود (مگر این که به‌گونه‌ای دیگر مشخص شده باشد.)، مقدار v برابر با $2^{40} + 15$ قرار داده می‌شود. (یک عدد اول)

خواهان A باید دو یا چند عامل اول بزرگ و متمایز را سرّی نگه دارد. این عامل‌ها با $p_1, p_2, \ldots$ نشان داده می‌شوند و ترتیب صعودی دارند. اگر α مضرب تعداد عامل‌های اول که با f نشان داده می‌شود باشد، آن‌گاه اندازه بیت هر عامل اول باید α / f باشد. (برای جزییات بیشتر به زیربند پ-۱-۲مراجعه شود.) p_j, p_j-1 باید نسبت به v اول باشند.

پیمانه برابر با حاصلضرب عامل‌های اول قرار داده می‌شود؛ یعنی $p_1 \times ... \times p_f$. این پیمانه یک پارامتر خواهان است و با n(A) نشان داده می‌شود.

یادآوری۱- نمای درستی‌سنجی **v** و پیمانه **n(A)** با یکدیگر یک کلید **RSA** عمومی تشکیل می‌دهند.

کلید خصوصی برای خواهانA که با Q نشان داده می‌شود کوچکترین عدد صحیح مثبت است به طوری که $v \times Q - 1$ مضربی از lcm(p_1-1, … p_f-1) است. عدد Q به وسیله یک رشته α نمایش داده می‌شود.

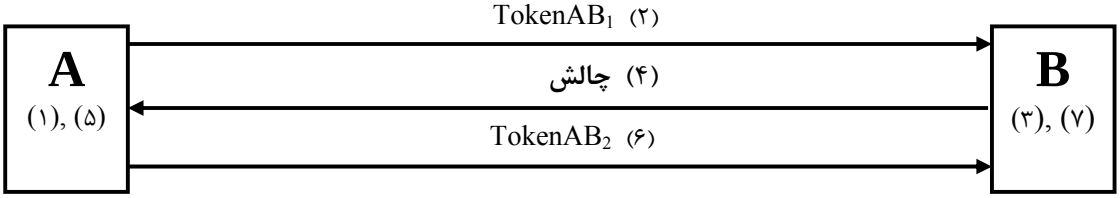
یادآوری۲- کلید خصوصی Q و پیمانه n(A) با یکدیگر یک کلید RSA خصوصی تشکیل می‌دهند.

کلید عمومی که با G نشان داده می‌شود یک پارامتر دامنه است. مقدار G= ۲ دارای مزیت‌های عملی است.

یادآوری۳- عددی که نقش پایه را بازی می‌کند **v** امین توان پیمانه‌ای G است؛ یعنی $g(A)=G^v \bmod n(A)$. این عدد به‌وسیله خواهان و درستی‌سنج مورد استفاده قرار نمی‌گیرند.

۳-۷ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۴ درون پرانتز قرار دارند مربوط به قدم‌های سازوکار هستند. این قدم‌ها شامل تبادلات اطلاعاتی هستند که به تفصیل در ادامه ارائه شده است. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۴ – سازوکار استفاده‌کننده از یک الگوریتم گسسته نسبت به یک عدد مرکب

- در حالت اول، خواهان باید یک عدد δ، یک پایه g، یک کلید خصوصی Q (به‌عنوان یک رشته σ بیتی) و پیمانه n یا n(A) را ذخیره کند. δ = ۴۰، g = ۲، σ = ۱۶۰.
- در حالت دوم، خواهان باید یک عدد δ، یک کلید عمومی G، یک نمای درستی‌سنجی v، یک کلید خصوصی Q (به‌عنوان یک رشته α بیتی) و پیمانه n(A) را ذخیره کند. δ = ۴۰، G = ۲، $v = 2^{40} + 15$.

در مورد راهبرد کوپن، خواهان باید علاوه بر یک کلید خصوصی Q و یک عدد δ، مجموعه‌ای از کوپن‌ها را ذخیره کند. برای این‌که هر کوپن فقط یک بار استفاده شود، هر یک شامل یک رشته با σ بیت (اگر بتوان آن را به‌وسیله یک تابع شبه تصادفی بازتولید کرد، نیازی به ذخیره کردن آن نیست.) و یک شاهد با α بیت (یا به‌صورت ترجیهی متغیر درهم‌سازی آن) است.

- در حالت اول، باید علاوه بر یک عدد δ، یک پایه g و یک عدد σ، یک رونوشت مورد اعتماد از کلید عمومی G(A) و یک رونوشت مورد اعتماد از پیمانه n یا n(A) در اختیار درستی‌سنج قرار داده شود.

- در حالت دوم، ، باید علاوه بر یک عدد δ، یک کلید عمومی G و یک نمای درستی‌سنجی v، یک رونوشت مورد اعتماد از پیمانه n(A) در اختیار درستی‌سنج قرار داده شود.

برای هر کاربرد سازوکار رویه زیر باید انجام گیرد. اگر رویه با موفقیت پایان پذیرد، درستی‌سنج B فقط باید خواهان A را معتبر بداند:

۱) برای هر احراز هویت، باید یک رشته جدیدρ بیتی به‌طور یکنواخت و به‌صورت تصادفی انتخاب شود. این رشته باید سرّی نگه داشته شود.

درحالت اول، $\rho = \sigma + \delta + 80$

درحالت دوم، $\rho = \alpha + \delta + 80$

یادآوری۱- اگر رشته جدید $\boldsymbol{\rho}$ بیتی به‌صورت تصادفی انتخاب شود، آن‌گاه احتمال این که تمام ۸۰ بیت سمت چپ برابر باشند ناچیز است.

عددی که با r نشان داده می‌شود و به‌وسیله رشته جدید نمایش داده می‌شود باید به یک شاهد که با W نشان داده می‌شود؛ تبدیل شود. عدد W که به‌وسیله یک رشته α بیتی نمایش داده می‌شود نیز با W نشان داده می‌شود.

فرمول شاهد در حالت اول: $W = g^r \ (mod\ n \text{ یا } n(A))$

فرمول شاهد در حالت دوم: $W = G^{r \times v}\ mod\ n(A)$

یادآوری۲- اگر عامل‌های اول در دسترس باشند، آن‌گاه محاسبه شاهد (که از قبل در حالت راهبرد کوپن انجام شده است.) با استفاده از فن CRT (به زیربند پ-۲-۳ مراجعه شود) مجاز است.

۲) A نشانه AB_1 را به B می‌فرستد. نشانه AB_1 شاهد W یا کد درهم W و Text است. متغیر درهم‌سازی به‌صورت یکی از چهار نوع زیر است.

چهار متغیر درهم‌ساز عبارتند از h(W||Text)، h(W||h(Text))، h(h(W)||Text) و h(h(W)||h(Text)) که در آن h تابع درهم‌ساز و Text یک دسته متنی اختیاری است. (ممکن است خالی باشد.) اگر دسته متنی خالی نباشد، آن‌گاه B باید ابزاری برای بازیابی مقدار Text داشته باشد؛ در این حالت نیاز است که A تمام یا قسمتی از دسته متنی را ارسال کند. دسته متنی برای استفاده در کاربردهای خارج از حیطه این استاندارد قابل دستیابی است. در پیوست الف استاندارد1-ISO/IEC 9798[24]، اطلاعاتی در مورد استفاده از دسته‌های متنی وجود دارد. نوع درهم‌سازی یک پارامتر دامنه است.

۳) با دریافت نشانه AB_1، باید یک رشته جدید δ بیتی به‌صورت تصادفی به‌طور یکنواخت انتخاب شود.

۴) B یک رشته جدید را به‌عنوان یک چالش برای A می‌فرستد. رشته جدید یک عدد را نمایش می‌دهد که با d نشان داده می‌شود.

۵) با دریافت چالش، قدم‌های محاسباتی زیر انجام می‌شوند:

الف- اگر چالش یک رشته δ بیتی نباشد، آن‌گاه رویه ناموفق است.

ب-پاسخ D باید از عدد تصادفی r و کلید خصوصی Q محاسبه شود.

فرمول پاسخ: $D = r - d \times Q$

۶) A نشانه AB_2 را به B می‌فرستد. نشانه AB_2 پاسخ D است از قدم ۵-ب محاسبه می‌شود.

۷) با دریافت نشانه AB_2، قدم‌های محاسباتی زیر انجام می‌شوند:

الف- اگر پاسخ D یک رشته ρ بیتی نباشد و/یا تمام ۸۰ بیت سمت چپ D برابر باشند، آن‌گاه رویه ناموفق است.

ب- باید یک شاهد که با W^* نشان داده می‌شود محاسبه شود.

فرمول درستی‌سنجی درحالت اول: $W^* = G(A)^d \times g^D (mod\ n \text{ یا } n(A))$

فرمول درستی‌سنجی درحالت دوم: $W^* = G^{d+v\times D}\ mod\ n(A)$

پ- اگر شاهد W^* یا کد درهم W^* و Text که یکی از چهار نوع درهم‌سازی هستند با نشان AB_1 دریافت‌شده در قدم ۲ یکسان باشد، آن‌گاه رویه موفق است. در غیر این صورت، رویه ناموفق است.

یادآوری۱- ارسال اطلاعات دیگر به همراه هر تبادل رویه مجاز است. B می‌تواند از چنین اطلاعاتی برای محاسبه مقدار دسته متنی اختیاری کمک بگیرد. برای مثال، A می تواند اطلاعاتی از قبیل گواهی به همراه نشانه AB_1 ارسال کند.

یادآوری۲- استفاده از یک کد درهم به‌جای شاهد W در نشانه AB_1 می‌تواند با کاهش تعداد بیت‌های موجود در نشانه AB_1 باعث افزایش کارایی شود.

۸ سازوکارهای مبتنی بر سامانه‌های رمزبندی نامتقارن

۸-۱ الزامات امنیتی برای محیط

با استفاده از این سازوکارها، یک درستی‌سنج می‌تواند آگاهی یک خواهان از کلید رمزگشایی متناظر با کلید رمزبندی مورد ادعا را وارسی کند.

یادآوری- این سازوکارها از طرح‌ها منتسب به برانت[1]، دامگارد[2]، لندراک[3] و پدرسون[4] نتیجه گرفته شده‌اند[2][16]. دومین سازوکار نیز از سازوکار انتقال کلید ۶ استاندارد ملی ۳-۱۰۸۲۲ [26] و میچل[5] و یون[6] نتیجه گرفته شده است [17].

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

۱) تمامی هستارهای درون دامنه باید بر روی استفاده از دو تابع رمزنگاری توافق داشته باشند: یک تابع درهم‌ساز مانند یکی از توابع مشخص شده در استاندارد ISO/IEC 10118-3 [25] و یک سامانه رمزبندی نامتقارن مانند یکی از سامانه‌های مشخص شده در استاندارد ISO/IEC 18033-2 [31].

1 - Brandt
2 - Damgard
3 - Landrock
4 - Pederson
5 - Mitchell
6 - Yeun

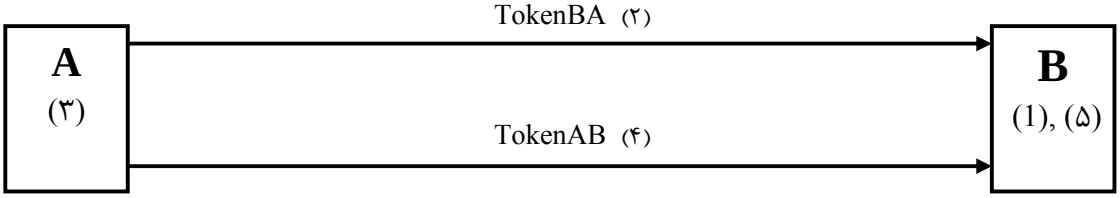
۲) هر خواهان باید به یک جفت کلید نامتقارن برای استفاده با سامانه رمزبندی نامتقارن مجهز باشد.
۳) هر درستی‌سنج باید یک رونوشت از کلید عمومی مختص خواهان به‌دست آورد.

یادآوری – ابزاری که به‌وسیله آن درستی‌سنج یک رونوشت مورد اعتماد از کلید عمومی مختص خواهان به‌دست می‌آورد خارج از حیطه این استاندارد است. برای مثال، این امکان وجود دارد که بتوان با استفاده از گواهی‌های کلید عمومی یا بعضی از ابزارهای وابسته به محیط این رونوشت را به‌دست آورد.

۴) هر درستی‌سنج باید ابزار تولید رشته جدید بیت‌های تصادفی را در اختیار داشته باشد.

۸-۲ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۵ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستند که با جزییات در ادامه آورده خواهند شد. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۵– سازوکار استفاده‌کننده از یک جفت کلید نامتقارن برای رمزبندی

خواهان باید بخش خصوصی جفت کلید نامتقارن را ذخیره کند. این بخش یک عملیات خصوصی که با S_A نشان داده می‌شود را تعریف می‌کند.
درستی‌سنج باید یک رونوشت مورد اعتماد از بخش عمومی جفت کلید نامتقارن را در اختیار داشته باشد. این بخش که با P_A نشان داده می‌شود یک عملیات عمومی را تعریف می‌کند.
اگر یک کوپن در حال استفاده باشد، درستی‌سنج باید یک مجموعه از کوپن‌ها را ذخیره کند. برای این‌که هر کوپن فقط یک بار استفاده شود، هر کوپن به یک خواهان معین اختصاص داده می‌شود؛ هر کوپن شامل یک رشته ρ بیتی (اگر بتوان آن را به‌وسیله یک تابع شبه تصادفی بازتولید کرد، نیازی به ذخیره کردن آن نیست.) و یک چالش α بیتی است.
باید طول بیت رشته‌های جدید بیت‌های تصادفی که یک عدد است و با ρ نشان داده می‌شود انتخاب شود. مقدار ρ باید حداقل $2 \times |h|$ و کوچکتر از $|n(A)| - |h|$ باشد به‌طوری‌که الحاق یک رشته جدید و یک کد درهم درون دامنه تعریف P_A قرار گیرد.
برای هر کاربرد سازوکار باید رویه زیر انجام گیرد. اگر این رویه با موفقیت پایان پذیرد، درستی‌سنج B فقط باید خواهانA را معتبر بداند.
۱) قدم‌های محاسباتی زیر انجام می‌شوند:

الف- برای هر احراز هویت، باید یک رشته جدید ρ بیتی به‌صورت تصادفی و به‌طور یکنواخت انتخاب شود. این رشته که با r نشان داده می‌شود باید سرّی نگه‌داشته شود.

مقدار ρ باید حداقل $|h| \times ۲$ و کوچکتر از $|n(A)| - |h|$ باشد به‌طوری‌که الحاق یک رشته جدید و یک کد درهم درون دامنه تعریف P_A قرار گیرد.

ب- کد درهم H باید از رشته جدید r محاسبه شود.

$$H = (r)$$

پ- عدد d باید با استفاده از P_A محاسبه شود.

$$d = P_A(r||H)$$

۲) B نشانه BA را به A می‌فرستد. نشانه BA عدد d است که از قدم ۱-پ محاسبه می‌شود.

۳) با دریافت نشانه BA، قدم‌های محاسباتی زیر انجام می‌شوند:

الف- دو رشته که با r^* و H^* نشان داده می‌شوند باید با استفاده از S_A بازیابی شوند.

$$r^* || H^* = S_A(d)$$

ب- اگر رشته H^* و r^* متفاوت باشند، آن‌گاه رویه ناموفق است.

۴) A نشانه AB را به B می‌فرستد. نشانه AB رشته r^* است که از قدم ۳-الف بازیابی می‌شود.

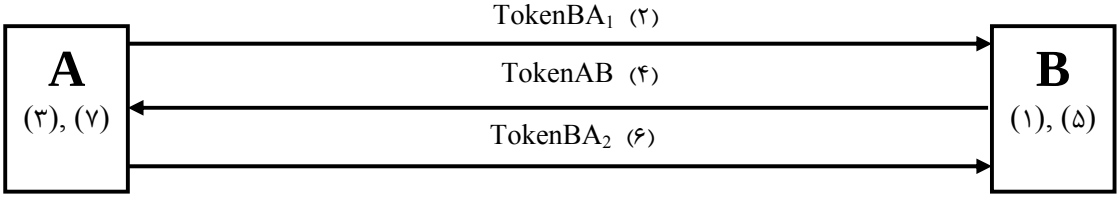
۵) با دریافت نشانه AB، رشته r^* با رشته r مقایسه می‌شود. اگر دو رشته یکسان باشند، آن‌گاه رویه موفق است؛ در غیر این‌صورت، این رویه ناموفق است.

یادآوری ۱- اگر سامانه رمزبندی مورداستفاده ویژگی عدم انعطاف[1] را فراهم کند (به استاندارد ISO/IEC 18033-2 [**31**] مراجعه شود.)، آن‌گاه حذف کردن کد درهم از نشانه BA مجاز است. در چنین حالتی، قدم ۳-ب به‌وسیله یک وارسی جایگزین می‌شود. این قدم وارسی می‌کند که آیا رویه به‌طور صحیح پایان یافته است. به هر حال بهتر است ملاحظات ویژه‌ای در نظر گرفته شود تا درستی‌سنج از خواهان به‌عنوان پیشگوی رمزگشایی استفاده نکند.

یادآوری۲- ارسال اطلاعات دیگر به همراه هر یک از تبادلات سازوکار مجاز است.

۸-۳ تبادل احراز هویت دوجانبه

اعدادی که در شکل ۶ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستند که به تفصیل در ادامه ارائه شده‌اند. هر هستار مانند A و B هم یک خواهان و هم یک درستی‌سنج است.



1 - Non-malleability

شکل ۶ – سازوکار استفاده‌کننده از دو جفت کلید نامتقارن برای رمزبندی

هر هستار باید بخش خصوصی جفت کلید نامتقارن خود را ذخیره کند. این بخش یک عملیات خصوصی را تعریف می‌کند و با S_A یا S_B نشان داده می‌شود. یک رونوشت مورد اعتماد از بخش عمومی جفت کلید نامتقارن دیگر هستارها باید در اختیار هر هستار قرار گیرد. این بخش یک عملیات عمومی را تعریف می‌کند و با P_A یا P_B نشان داده می‌شود. همچنین باید برای هر هستار داده‌های شناسایی خود که با *Id(A)* یا *Id(B)* نشان داده می‌شوند و داده‌های شناسایی دیگر هستارها که با *Id(B)* یا *Id(A)* نشان داده می‌شوند، فراهم شود.

باید طول بیت رشته‌های جدید بیت‌های تصادفی که یک عدد است و با ρ نشان داده می‌شود انتخاب شود. مقدار ρ باید حداقل $2 \times |h|$ و کمتر از کمینه $(|n(A)| - |h| - |Id(B)|, (|n(B)| - |h| - |Id(A)|)/2)$ باشد به‌طوری‌که:

- الحاق *Id(B)* و یک رشته جدید با یک کد درهم درون دامنه تعریف P_A قرار گیرد.
- الحاق *Id(A)* و دو رشته جدید با یک کد درهم درون دامنه تعریف P_B قرار گیرد.

برای هر کاربرد سازوکار باید رویه زیر انجام گیرد. دو هستار A وB تنها باید در صورتی یکدیگر را معتبر بدانند که این رویه با موفقیت پایان پذیرد.

۱) قدم‌های محاسباتی زیر انجام می‌شوند:

الف- برای هر احراز هویت، باید یک رشته جدید ρ بیتی به‌صورت تصادفی و به‌طور یکنواخت انتخاب شود. این رشته که با r_B نشان داده می‌شود باید سرّی نگه‌داشته شود.

ب- کد درهم H_B باید از داده شناسایی *Id(B)* و رشته جدید r_B محاسبه شود.

$$H_B = h(Id(B)||r_B)$$

پ- عدد d_B باید با استفاده از P_A محاسبه شود.

$$d_B = P_A(Id(B)||r_B||H_B)$$

۲) B نشانه BA_1 را به A می‌فرستد. نشانه BA_1 عدد d_B است که از قدم ۱-پ محاسبه می‌شود.

۳) با دریافت نشانه BA_1، قدم‌های محاسباتی زیر انجام می‌شود:

الف- سه رشته‌ای که با Id_B^*، r_B^* و H_B^* نشان داده می‌شوند باید با استفاده از S_A بازیابی شوند.

$$Id_B^*||\, r_B^*||\, H_B^* = S_A(d_B)$$

ب- اگر رشته H_B^* و کد درهم $h(Id_B^*||r_B^*)$ متفاوت باشند، آن‌گاه این رویه ناموفق است.

پ- اگر رشته Id_B^* و داده شناسایی Id(B) متفاوت باشند، آن‌گاه این رویه ناموفق است.

ت- مراحل محاسباتی زیر انجام می‌شود:

I- برای هر احراز هویت، باید یک رشته جدید ρ بیتی به‌صورت تصادفی و به‌طور یکنواخت انتخاب شود. این رشته که با r_A نشان داده می‌شود باید سرّی نگه‌داشته شود.

II- کد درهم‌ساز H_A باید از شناسایی داده *Id(A)*، رشته r_B^* و رشته تازه r_A محاسبه شود.

$$H_A=h(Id(A)||r_B^*||r_A)$$

III- عدد d_A باید با استفاده از P_B محاسبه شود.

$$d_A=P_B(Id(A)||r_B^*||r_A||H_A)$$

۴) A نشانه AB را به B می‌فرستد. نشانه AB عدد d_A است.

۵) با دریافت نشانه AB، قدم‌های محاسباتی زیر انجام می‌شود.

الف- چهار رشته که با Id_A^*، r_B^{**}، r_A^* و H_A^* نشان داده می‌شوند باید با استفاده از S_B بازیابی شوند.

$$H_A^*=S_B(d_A)\ ||r_A^*\ ||r_B^{**}||Id_A^*$$

ب- اگر رشته H_A^* و کد درهم $h(Id_A^*||r_B^{**}||r_A^*)$ متفاوت باشند، آن‌گاه رویه ناموفق است.

پ- اگر رشته Id_A^* و داده شناسایی Id(A) متفاوت باشند، آن‌گاه رویه ناموفق است.

ت- اگر رشته r_B^{**} و رشته r_B تولید شده در قدم (۱) متفاوت باشند، آن‌گاه رویه ناموفق است.

۶) B نشانه BA_2 را به A می‌فرستد. نشانه BA_2 رشته r_A^* است.

۷) با دریافت نشانه BA_2، رشته r_A^* با رشته r_A تولید شده در قدم (۳) مقایسه می‌شود. اگر این دو رشته یکسان باشند، آن‌گاه رویه موفق است. در غیر این‌صورت، رویه ناموفق است.

یادآوری۱- اگر سامانه رمزبندی مورد استفاده ویژگی عدم انعطاف را فراهم کند، (به استاندارد ISO/IEC 18033-2 [**31**] مراجعه شود.) آن‌گاه حذف کردن کدهای درهم از نشانه BA_1 و نشانه AB مجاز است. در چنین حالتی، قدم‌های ۳-ب و ۵-ب به‌وسیله یک وارسی جایگزین می‌شوند. این مرحله وارسی می‌کند که آیا رویه به‌طور صحیح پایان یافته است. به هر حال بهتر است ملاحظات ویژه‌ای در نظر گرفته شوند تا درستی‌سنج از خواهان به‌عنوان پیشگوی رمزگشایی استفاده نکند.

یادآوری۲- ارسال اطلاعات دیگر به همراه هر یک از تبادلات سازوکار مجاز است.

۹ سازوکار مبتنی بر لگاریتم‌های گسسته نسبت به منحنی‌های بیضوی

۹-۱ الزامات امنیتی برای محیط

این سازوکار درستی‌سنج را قادر می‌سازد تا آگاهی یک خواهان از لگاریتم گسسته منحنی بیضوی یک نقطه مورد ادعا نسبت به یک نقطه پایه را وارسی کند. یک چارچوب کلی برای فنون رمزنگاری مبتنی بر منحنی‌های بیضوی در استاندارد ملی ۱-۱۵۹۴۶ [28] داده شده است.

یادآوری۱- این سازوکار نوعی[6] از منحنی بیضوی طرح GPS [9] منتسب به گیرال، پوپار و اشترن را پیاده‌سازی می‌کند. این سازوکار اجازه استفاده از نوع LHW [1] را می‌دهد و به‌ویژه برای محیط‌هایی که در منابع خواهان بسیار کم هستند مناسب است.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

1 - Low Hamming Weight

۱) پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کنند باید انتخاب شوند. پارامترهای انتخاب شده باید به‌صورتی قابل‌اطمینان به تمامی هستارهای درون دامنه معرفی شوند.
۲) هر خواهان باید به یک منحنی بیضوی E و مجموعه‌ای از پارامترها که عبارتند از اندازه دسته q، یک نقطه پایه P روی E و n که مرتبه نقطه P است مجهز باشد. منحنی و مجموعه پارامترها، پارامترهای دامنه یا پارامترهای خواهان هستند.
۳) هر نقطه P که به‌عنوان پایه لگاریتم‌های گسسته منحنی بیضوی استفاده می‌شود باید به‌گونه‌ای باشد که برای هر نقطه دلخواه J روی منحنی، پیداکردن یک عدد k در بازه [0, n-1] (در صورت وجود) به‌طوری‌که محاسباتی J=[k] امکان‌پذیر نباشد. امکان‌پذیر بودن به‌وسیله متن کاربرد سازوکار تعریف می‌شود.
۴) هر خواهان باید مجهز به یک کلید خصوصی باشد.
۵) هر درستی‌سنج باید یک رونوشت با اصالت از کلیدعمومی متناظر با کلید خصوصی را به‌دست آورد.

یادآوری- ابزاری که به‌وسیله آن درستی‌سنج یک رونوشت مورد اعتماد از نقطه عمومی مختص خواهان به‌دست می‌آورد خارج از حیطه این استاندارد است. برای مثال، این امکان وجود دارد که بتوان با استفاده از گواهی‌های کلید عمومی یا بعضی از ابزارهای وابسته به محیط این رونوشت را به‌دست آورد.

۶) هر خواهان و هر درستی‌سنج باید ابزار تولید رشته‌های جدید بیت‌های تصادفی را در اختیار داشته باشند.
۷) اگر سازوکار از یک تابع درهم‌ساز استفاده کند، آن‌گاه تمامی هستارهای درون دامنه باید بر روی آن تابع درهم‌ساز توافق داشته باشند. برای مثال، می‌توان یکی از توابع مشخص شده در استاندارد ISO/IEC 10118-3 [25] را به‌کار برد.

۹-۲ تولید کلید

برای خواهان A، یک رشته جدید باید به‌صورت تصادفی به‌طور یکنواخت از مجموعه [2, n-2] انتخاب شود. رشته‌ای که کلید خصوصی را نمایش می‌دهد با Q نشان داده می‌شود.
عدد $\sigma = |n|$ تعداد بیت‌هایی را که برای نمایش کلیدهای خصوصی استفاده می‌شوند به‌دست می‌دهد.
نقطه عمومی برای خواهان A که با G(A) نشان داده می‌شود برابر ضرب عدد Q در نقطه پایه P قرار داده می‌شود.

چالش‌ها از یک مجموعه اعداد صحیح S انتخاب می‌شوند به‌طوری‌که برای هر عضو Δ نامساوی $2^{\delta-1} \leq \Delta < 2^{\delta}$ برقرار باشد. طول بیت بزرگترین چالش با β نشان داده می‌شود. یک δ با مقداری بین ۸ تا ۴۰ برای بسیاری از کاربردها مناسب است. اگر به‌گونه‌ای دیگر تعریف شده باشد، مقدار δ برابر با ۴۰ قرار داده می‌شود. δ یک پارامتر دامنه است.

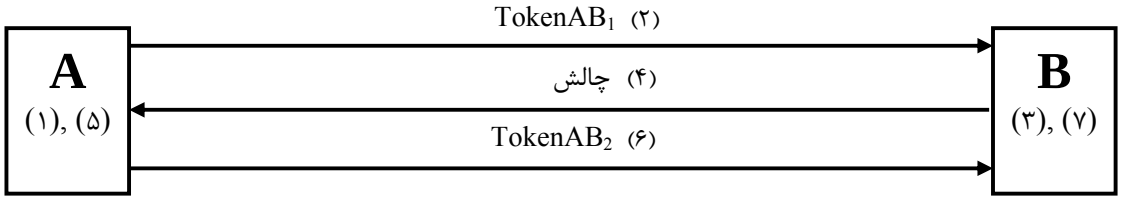
یادآوری۱- توصیه می‌شود تعداد کل چالش‌های ممکن به 2^{40} محدود شود. اگر به این توصیه عمل نشود، آن‌گاه بهتر است ملاحظات ویژه‌ای در نظر گرفته شود تا درستی‌سنج از خواهان به‌عنوان پیشگوی امضاکننده استفاده نکند.

یادآوری۲- اگر مجموعه چالش‌ها بازه $[\mathbf{0}, \boldsymbol{\Delta} - \mathbf{1}]$ باشد، آن‌گاه $\boldsymbol{\beta} = \boldsymbol{\delta}$.

یادآوری۳- به یک چالش LHW گفته می‌شود اگر حداقل σ-۱ بیت صفر بین هر دو بیت یک متوالی در نمایش دودویی آن وجود داشته باشد.

۳-۹ تبادل احراز هویت یک‌جانبه

اعدادی که در شکل ۷ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستند که با جزییات در ادامه آورده خواهند شد. خواهان با A و درستی‌سنج با B نشان داده شده‌اند.



شکل ۷ – سازوکار استفاده‌کننده از یک لگاریتم گسسته نسبت به منحنی‌های بیضوی

خواهان باید یک عدد δ، یک پایه P و یک کلید خصوصی Q (به‌صورت یک رشته σ بیتی) را ذخیره کند. اگر به‌گونه‌ای دیگر مشخص شده باشد، δ = ۴۰.

در مورد راهبرد کوپن، خواهان باید علاوه بر یک کلید خصوصی Q و یک عدد δ، مجموعه‌ای از کوپن‌ها را ذخیره کند. برای این که هر کوپن فقط یک بار استفاده شود، هر یک شامل یک رشته با ρ بیت (اگر بتوان آن را به‌وسیله یک تابع شبه تصادفی بازتولید کرد، نیازی به ذخیره کردن آن نیست.) و یک شاهد است.

خواهان باید علاوه بر یک عدد δ و یک عدد σ، یک رونوشت مورد اعتماد از نقطه عمومی G(A)، یک رونوشت مورد اعتماد از منحنی E، نقطه پایه P و پارامترهای q وn را دراختیار داشته باشد.

برای هر کاربرد سازوکار باید رویه زیر انجام گیرد. اگر این رویه با موفقیت پایان پذیرد، درستی‌سنج B فقط باید خواهانA را معتبر بداند.

۱) برای هر احراز هویت، باید یک رشته جدید ρ بیتی به‌صورت تصادفی و به‌طور یکنواخت انتخاب شود. این رشته باید سرّی نگه‌داشته شود.

$$\rho = \sigma + \beta + 80$$

یادآوری۱- اگر رشته جدید$\boldsymbol{\rho}$ بیتی به‌صورت تصادفی انتخاب شود، آن‌گاه احتمال این که تمام۸۰ بیت سمت چپ برابر باشند ناچیز است.

عددی که با r نشان داده شده و به وسیله رشته جدید نمایش داده می‌شود باید به یک شاهد که با W نشان داده می‌گردد تبدیل شود.

فرمول شاهد: $\mathrm{W} = \mathrm{P2OS}([\mathrm{r}]\mathrm{P})$

یادآوری۲- P2OS تابعی است که برای تبدیل یک نقطه به یک رشته هشت‌تایی استفاده می‌شود.

۲) A نشانه AB_1 را به B می‌فرستد. نشانه AB برای B شاهد W یا کد درهم W و Text است. کد درهم به یکی از چهار صورت زیر است.

چهار متغیر درهم‌ساز عبارتند از h(W||Text)، h(W||h(Text))، h(h(W)||Text) و h(h(W)||h(Text)) که در آن h تابع درهم‌ساز و Text یک دسته متنی اختیاری است. (ممکن است خالی باشد.) اگر دسته متنی خالی نباشد، آن‌گاه B باید ابزاری برای بازیابی مقدار Text داشته باشد؛ در این حالت نیاز است که A تمام یا قسمتی از دسته متنی را ارسال کند. چگونگی در دسترس قرار دادن دسته متنی برای استفاده در کاربردها خارج ازمحدوده این استاندارد است. در پیوست الف استاندارد ISO/IEC 9798-1 [24] اطلاعاتی در مورد استفاده از دسته‌های متنی وجود دارد. متغیر درهم‌سازی یک پارامتر دامنه است.

۳) با دریافت نشانه AB_1، یک رشته جدید باید به‌صورت تصادفی به‌طور یکنواخت از مجموعه S انتخاب شود.

۴) B یک رشته جدید را به صورت یک چالش به A می‌فرستد. رشته جدید یک عدد را نمایش می‌دهد که با d نشان داده می‌شوند.

یادآوری۳- اگر از یک چالش LHW[1] استفاده شود، می‌توان آن را به شکل فشرده به A ارسال کرد. A باید ابزار بازیابی چالش اول پیش از قدم ۵-الف را در اختیار داشته باشد.

۵) با دریافت چالش، مراحل محاسباتی زیر انجام می‌گیرد:

الف- اگر چالش عضوی از S نباشد، آن‌گاه این رویه ناموفق است.

ب- پاسخ D باید از عدد تصادفی r و کلید خصوصی Q محاسبه شود.

فرمول پاسخ: $$D = r - d \times Q$$

یادآوری۴- اگر چالش دریافتی یک چالش LHW باشد، محاسبه D به اضافه کردن سری r به یک سلسله‌بندی رونوشت‌های Q که با بیت‌های صفر جدا می‌شوند، کاهش می‌یابد.

۶) A نشانه AB_2 را به B می‌فرستد. نشانه AB_2 پاسخ D است که از مرحله ۵-ب محاسبه می‌شود.

۷) با دریافت نشانه AB_2، قدم‌های محاسباتی زیر انجام می‌شوند:

الف- اگر پاسخ D یک رشته ρ بیتی و/یا اگر تمام ۸۰ بیت سمت چپ D برابر باشند، آن‌گاه این رویه ناموفق است.

ب- باید یک شاهد که با W* نشان داده می‌شود محاسبه شود شود.

فرمول درستی‌سنجی: $$W^* = P2OS([d]G(A) + [D]P)$$

پ- اگر شاهد W^* یا کد درهم W^* و Text که یکی از چهار نوع درهم‌سازی هستند با نشان AB_1 دریافت شده در مرحله ۲ یکسان باشد، آن‌گاه رویه موفق است. در غیر این‌صورت، رویه ناموفق است.

1- Low Hamming Weight

یادآوری۵- ارسال اطلاعات دیگر به همراه هر تبادل روند مجاز است. B می‌تواند از چنین اطلاعاتی برای محاسبه مقدار دسته متنی اختیاری کمک بگیرد. برای مثال، A مجاز است اطلاعاتی از قبیل گواهی را به همراه نشانه AB_1 ارسال کند.

پیوست الف
(الزامی)
شناسه‌های شیء

الف-۱ تعریف رسمی

```
EntityAuthenticationMechanisms-9 {
   iso(1) standard(0) e-auth-mechanisms(9798)
part(5) asn1-module(0) object-identifiers(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --
-- IMPORTS None; --


OID ::= OBJECT IDENTIFIER – alias

-- Synonyms –

is9798-5 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part(5)
}

mechanism OID ::= { is9798-5 mechanisms(1) }

-- Unilateral and mutual entity authentication mechanisms –

ua-identity-based-FS OID ::= { mechanism 1 }
ua-identity-based-GQ1 OID ::= { mechanism 2 }
ua-integer-factorization-GQ2 OID ::= { mechanism 3 }
ua-discrete-logarithms-prime-number-SC OID ::= { mechanism 4 }
ua-discrete-logarithms-composite-number-GPS1 OID ::= { mechanism 5 }
ua-discrete-logarithms-composite-number-GPS2 OID ::= { mechanism 6 }
ua-asymmetric-encryption OID ::= { mechanism 7 }
ma-asymmetric-encryption OID ::= { mechanism 8 }
ua-discrete-logarithms-ecc-GPS OID ::= { mechanism 9 }


END -- EntityAuthenticationMechanisms-9 –
```

الف-۲ استفاده از شناسه‌های شیء متوالی

اگر یک سازوکار مشخص شده در این استاندارد از یک تابع درهم‌ساز استفاده کند، آن‌گاه درست پس از شناسایی سازوکار به‌وسیله یک شناسه شیء، شناسه شیء دیگر مجاز است که برای شناسایی یک تابع درهم‌ساز در ادامه بیاید. (یکی از توابع درهم‌سازی اختصاص یافته مشخص شده در استاندارد ISO/IEC 10118-3[25] مثالی برای این موضوع است.)

برای دو سازوکار آخر، شناسه شیء دیگری می‌تواند جهت ارجاع به یک سیستم رمزبندی در ادامه بیاید. (برای مثال یکی از سازوکارهای مشخص شده در استاندارد ISO/IEC 18033-2[31]) در غیاب چنین شناسه شیء متوالی، یک جایگشت RSA مورد استفاده قرار می‌گیرد.

الف-۳ مثال‌های کدگذاری مطابق با قواعد کدبندی پایه‌ای ASN.1

مطابق با استاندارد ISO/IEC 8825-1[23] ، یک شناسه شیء از یک یا تعداد بیشتری سری هشت‌تایی تشکیل شده است. هر سری یک عدد را کدگذاری می‌کند.

- بیت ۸ (پرارزش‌ترین بیت) در آخرین هشت‌تایی سری برابر با صفر است و اگر بیش از یک هشت‌تایی وجود داشته باشد، در هشت‌تایی‌های پیش از آن برابر با یک قرار داده می‌شود.
- الحاق بیت‌های ۷ تا ۱ هشت‌تایی‌های یک سری یک عدد را کدگذاری می‌کند. هر عدد باید بر روی بدترین هشت‌تایی‌های ممکن کدبندی شود، به‌عبارتی دیگر، هشت‌تایی 80 در اولین جایگاه یک سری نامعتبر است.
- اولین عدد، عدد استاندارد است؛ عدد دوم در صورت وجود، شماره قسمت در یک استاندارد چند قسمتی است.

شناسه شیء مجاز است که به هر سازوکار تعریف شده در این استاندارد اشاره کند.

- برای شناسایی یک استاندارد ISO، هشت‌تایی اول برابر 28 یعنی ۴۰ در مبنای ۱۰ قرار داده می‌شود. (به استاندارد ISO/IEC 8825-1 مراجعه شود.)
- دو هشت‌تایی بعدی برابر با CC46 قرار داده می‌شوند. ۹۷۹۸ برابر 2646 در مبنای شانزده است، یعنی 0110 0100 0110 0010 یعنی دو بلوک هفت بیتی: 1000110 1001100. پس از قرار دادن مقدار مناسب بیت ۸ در هر هشت‌تایی، کدگذاری سری به‌صورت 01000110 11001100 یعنی CC46 است.
- برای شناسایی قسمت ۵، هشت‌تایی بعدی برابر با 05 قرار داده می‌شود.
- هشت‌تایی بعدی یک سازوکار احراز هویت را شناسایی می‌کند.
  - 01 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از FS شناسایی می‌کند.
  - 02 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از GQ1 شناسایی می‌کند.
  - 03 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از تجزیه به عوامل یک پیمانه یعنی GQ2 شناسایی می‌کند.
  - 04 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از یک لگاریتم گسسته نسبت به یک عدد اول یعنی SC شناسایی می‌کند.
  - 05 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از یک لگاریتم گسسته نسبت به یک عدد ترکیبی درحالت اول کاربرد یعنی GPS1 شناسایی می‌کند.
  - 06 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از یک لگاریتم گسسته نسبت به یک عدد ترکیبی درحالت دوم کاربرد یعنی GPS2 شناسایی می‌کند.
  - 07 سازوکار اصالت‌سنجی یک‌جانبه را با استفاده از یک سامانه رمزبندی نامتقارن شناسایی می‌کند.

- 08 سازوکار اصالت‌سنجی دوجانبه را با استفاده از یک سامانه رمزبندی نامتقارن شناسایی می‌کند.

به‌عنوان مثال، عنصر داده 03 05 46 CC 28 به‌صورت{3 5 9798 standard iso} یعنی سازوکار سوم در استاندارد ISO/IEC 9798-5 یعنی GQ2 خوانده می‌شود. عنصر داده مجاز است که از طریق شیء داده -BER TLV انتقال یابد (به قوانین پایه‌ای کدبندی ASN.1، استانداردISO/IEC 8825-1 ، برچسب کلاس جهانی 06 رجوع شود.) که در آن خط تیره‌ها و آکولاد برای روشن‌تر کردن مطلب قرار داده شده‌اند و فاقد اهمیت هستند.

شیء داده = {06 – 05 -28 CC 46 05 03}

پیوست ب
(اطلاعاتی)
اصول فنون دانش- صفر

ب-۱ مقدمه

در متن استفاده از فنون رمزنگاشتی نامتقارن، یکی از ضعف‌های بالقوه یک تبادل احراز هویت این است که درستی‌سنج ممکن است از سازوکار جهت دستیابی به کلید خصوصی سوءاستفاده کند. هنگامی که رمزنگاری نامتقارن مورد استفاده قرار می‌گیرد، خواهان از کلید خصوصی جفت نامتقارن خود برای محاسبه یک پاسخ به یک چالش درستی‌سنج استفاده می‌کند. پس از آن، درستی‌سنج مجاز است که با انتخاب عاقلانه چالش اطلاعاتی را درباره کلید خصوصی خواهان به‌دست آورد. این اطلاعات را نمی‌توان تنها با آگاهی کلید عمومی خواهان به‌دست آورد.

این نوع سوءاستفاده از یک تبادل پیام‌های رمزنگاشتی شده به استفاده از خواهان به‌عنوان پیش‌گو شهرت دارد که در آن خواهان اطلاعاتی درباره کلید خصوصی خود را در دستور درستی‌سنج فراهم می‌کند. ایده‌ای که در ورای یک سازوکار احراز هویت دانش- صفر قرار دارد. از بین بردن این تهدید بالقوه با طراحی دقیق پیام‌ها به‌گونه‌ای است که درستی‌سنج نتواند از خواهان به‌عنوان پیش‌گو بهره ببرد.

ب-۲ نیاز به سازوکارهای دانش- صفر

در کاربردهای دربرگیرنده شبکه‌های رایانه‌ای مدرن، نیاز به خدمات امنیتی مانند احراز هویت، انکارناپذیری و غیره به‌طور گسترده‌ای پذیرفته شده و دائماً در حال رشد است. برای داشتن توانایی استفاده از چنین خدماتی، دسترسی کاربر به اطلاعات خصوصی مختص آن کاربر ضروری است. مثال‌های چنین خدماتی کلمات عبور، کلیدهای امضا، کلیدهای خصوصی جفت‌های نامتقارن و غیره هستند.

البته ضرورت دارد که برای امنیت سامانه، اطلاعات خصوصی، خصوصی بمانند؛ یعنی، به دیگر طرف‌های مهاجم بالقوه نشت نیابد. از سوی دیگر، اطلاعات خصوصی باید به‌عنوان ورودی برای پیمانه‌های سخت‌افزاری و نرم‌افزاری که پیام‌ها را به نمایندگی از کاربر محاسبه و ارسال می‌کنند، مورد استفاده قرار گیرد. اگر اطلاعات به‌طور مناسب مورد استفاده قرار نگیرند، پوشیدگی اطلاعات خصوصی ممکن است آسیب دیده یا حتی به‌طور کامل تخریب شود. یک مثال روشن از این حالت زمانی است که کاربران خود را به یک میزبان با ارسال کلمه عبور به‌صورت متن روشن معرفی می‌کنند. این عمل سبب افشای اطلاعات خصوصی به‌طور کامل با نتیجه آنی می‌شود به‌گونه‌ای که هر کس که خط را شنود می‌کند، می‌تواند خود را به‌جای تمام کاربرانی که کلمه عبور آن‌ها شنود شده جا بزند.

این مثالی است از حالتی که اطلاعات خیلی زیادی مخابره شده است. برای روشن ساختن این مطلب توجه داشته باشید که از نقطه نظر میزبان تنها دو احتمال وجود دارد: یا کاربر کلمه عبور صحیح را می‌داند یا نمی‌داند.

در اصطلاحات نظری اطلاعات، این به معنای آن است که تنها یک بیت از اطلاعات نیاز به مخابره شدن دارد و این پیش‌زمینه نظری برای مشکل عملی شنود است.

پرسیدن این سوال طبیعی است که «آیا کسی می‌تواند قراردادهایی را برای استفاده اطلاعات خصوصی که به‌طور دقیق اطلاعات مدنظر برای مخابره هستند طراحی کند و دیگر هیچ؟» به‌طور غیر رسمی این دقیقاً همان ویژگی‌ای است که سازوکار دانش- صفر دارا است. به‌عنوان مثال، حالتی را در نظر بگیرید که در آن به کاربر A یک جفت کلید یا اعداد نامتقارن برای یک سامانه رمزنگاری نامتقارن (P_A, S_A) تخصیص داده شده است آن‌چنان که P_A برای A عمـومی است در حالی که S_A برای A خصوصی است. آن‌گاه با استفاده از سازوکار دانش- صفر، A می‌تواند B را قانع کند که A کلید خصوصی مربوط به P_A را دارا است بدون آن‌که هیچ چیز دیگری به‌غیر از این واقعیت را افشا کند. از آن‌جا که A به‌عنوان تنها کاربر با دسترسی به S_A مشخص شده است، بنابراین از این قرارداد برای احراز هویت می‌توان استفاده کرد. در این حالت ویژگی دانش- صفر تضمین می‌کند که B هیچ چیزی را فرا نخواهد گرفت که بعداً بتواند با استفاده از آن خود را به دروغ به‌جای A جا بزند.

ویژگی دانش- صفر با طراحی یک مکالمه که می‌تواند تنها به‌وسیله درستی‌سنج شبیه‌سازی شود قابل دست‌یابی است. این ویژگی به‌طور حسی اثبات می‌کند که درستی‌سنج نمی‌تواند هیچ چیزی در مورد ویژگی‌های کلید خصوصی را از خواهان فرا گیرد که نمی‌توانسته از کلید عمومی مربوطه به‌دست آورد.

این همچنین به معنای آن است که یک شاهد تبادل پیام‌ها که سازوکار را می‌سازد در تصمیم‌گیری در مورد این‌که آیا خواهان واقعاً درگیر بوده است یا درستی‌سنج تبادل را شبیه‌سازی کرده ناتوان است.

سازوکارهای دانش- صفر به‌طور طبیعی نیاز به استفاده از فنون رمزنگاشتی نامتقارن دارند. با معلوم بودن تعریف صریح سازوکارهای دانش- صفر، پیاده‌سازی یکی از آن‌ها در واقع امکان‌پذیر نیست. در حقیقت، یک توصیف بسیار بهتر از این سازوکارها در این استاندارد سازوکارهای حفظ پوشیدگی[1] است. به‌هر حال، مفهوم سازوکار دانش- صفر قسمتی از یک نظریه مشهور و تثبیت شده در رمزنگاری است که به همین دلیل اصطلاحات فنی آن در این جا مورد استفاده قرار گرفته است.

ب-۳ تعاریف

نزدیک‌تر شدن به تعریف رسمی مشخص می‌کند که یک سازوکار دانش- صفر میان دو طرف رخ می‌دهد، یک خواهان A و یک درستی‌سنج B. خواهان تلاش می‌کند که درستی‌سنج را قانع کند که یک عبارت معین صحیح است. این عبارت به‌عنوان مثال می‌تواند «من کلید خصوصی مربوط به P_A را می‌دانم» باشد. برای قانع کردن B، خواهان و درستی‌سنج پیام‌هایی را برای لحظه‌ای تبادل می‌کنند. پس از آن، B تصمیم به پذیرش یا رد برهان A می‌گیرد.

سه ویژگی ضروری برای چنین سازوکاری مورد نیاز است.

کمال – اگر عبارت A صحیح باشد، آن‌گاه B بهتر است آن را به احتمال قریب به اتفاق بپذیرد.

---

1 - Secrecy-preserving

صحت – اگر عبارت A نادرست باشد، فارغ از رفتار A، B باید آن‌را به احتمال قریب به اتفاق رد کند.
دانش- صفر: بدون توجه به رفتار B، او تنها اطلاعاتی که با بیانیه A صحیح است را دریافت می‌کند. در بیان کمی دقیق‌تر؛ هنگام صحبت با خواهان راستگو، B جدا از هر چه دریافت کند می‌تواند به آسانی خودش را بدون گفتگو با A محاسبه کند. این بدان معنی است که B می‌تواند مکالمه را خود شبیه‌سازی کرده و مکالمه‌ای کاملاً مشابه با مکالمه‌ای را که گویی با A انجام شده است؛ شبیه‌سازی کند.

ب-۴ مثال

مثال زیر را در نظر بگیرد. این مثال یک نسخه ساده‌شده از یک سازوکار FS است[4]. در اینجا، یک پیمانه n و یک عدد به پیمانه n با نام G داده شده است. در این حالت، عبارت A به‌صورت «من از یک ریشه مربع پیمانه‌ای آگاه هستم» است. توجه کنید که Q یک ریشه مربع پیمانه‌ای از G است اگر و تنها اگر $\mathrm{mod\ n} \equiv GQ^2$.
مکالمه بین A و B به‌صورت زیر است:

- A یک عدد تصادفی جدید به نام r که عددی غیرصفر و کمتر از n است را انتخاب می‌کند، آن‌را به پیمانه n مربع کرده، و این مربع پیمانه‌ای را که با W مشخص می‌شود، برای B ارسال می‌کند.
- B یک بیت تصادفی جدید به نام d را که ممکن است ۰ یا ۱ باشد انتخاب می‌کند و آن‌را به‌عنوان یک چالش برای A می‌فرستد.
- اگر d برابر صفر باشد، آنگاه پاسخ به‌صورت $D = r$ است. اگر d برابر با یک باشد، پاسخ به‌صورت $D = r \times Q \mod n$ است. A پاسخ D را به B می‌فرستد.
- B ابتدا وارسی می‌کند که D عددی غیرصفر و کمتر از n باشد؛ اگر D برابر **صفر**، n یا بیشتر از آن باشد، آن‌گاه B، A را رد کرده و رویه بی‌نتیجه می‌ماند.
- اگر d برابر صفر باشد آن‌گاه B وارسی می‌کندکه مربع پیمانه‌ای D با W یکسان باشد. اگر d برابر با یک باشد، آن‌گاه B وارسی می‌کند که مربع پیمانه‌ای D با $W \times G \mod n$ یکسان باشد.
- اگر وارسی صحیح باشد، آن‌گاه این رویه ادامه می‌یابد؛ در غیر این‌صورت، B، A را رد کرده و رویه بی‌نتیجه می‌ماند.

این رویه پس از t تکرار موفق پیاپی به‌صورت موفقیت‌آمیز به پایان می‌رسد.
دیدن این نکته دشوار نیست که اگر هم A و هم B این رویه را دنبال کنند، آن‌گاه B هرگز A را رد نخواهد کرد؛ مربع کردن D به معنای مربع کردن r یا $r \times Q$ به پیمانه n است، که به نتیجه W یا $W \times G \mod n$ منجر می‌شود.
از سوی دیگر، اگر در هر کدام از t تکرار، A قادر به تولید پاسخ صحیح به $d = 0$ و $d = 1$ باشد، یعنی A می‌تواند هر دو D_0 و D_1 را تامین کند. در واقع، D_1 / D_0 به پیمانه n یک ریشه مربع پیمانه‌ای G است و بنابراین عبارت «A از یک ریشه مربع پیمانه‌ای G آگاهی دارد.» عبارتی صحیح است. اما به‌طور معکوس اگر A متقلب بوده و ریشه مربع پیمانه‌ای G را نداند، باید در دادن پاسخ صحیح به حداقل یک مقدار d در هر کدام از t تکرار ناتوان

باشد. بنابراین احتمال این‌که یک خواهان متقلب درستی‌سنج را قانع کند حداکثر 2^{-t} است. به‌عنوان مثال، با انجام ۲۰ تکرار، این احتمال را به یک در یک میلیون کاهش می‌دهیم. چنین مقداری «سطح امنیت سازوکار» نامیده می‌شود. (به زیربند پ-۱-۴ مراجعه شود.) بنابراین ویژگی صحت نیز برآورده می‌شود.

همانند حالت دانش- صفر، توجه داشته باشید که پس از پایان مکالمه، دو عدد D و W برای درستی‌سنج باقی می‌ماند آن‌چنان که D^2 به پیمانه n برابر با W یا W G mod n است. اما این در حقیقت چیزی است که درستی‌سنج بدون مکالمه با A می‌تواند بسازد. به این منظور B تنها یک عدد تصادفی D را انتخاب کرده و W را برابر D^2 یا D^2 / G به پیمانه n تعریف می‌کند. این حقیقت که W و D در این حالت از روشی متفاوت از روشی که خواهان برای محاسبه آن‌ها استفاده می‌کند محاسبه می‌شوند بی اهمیت است. آن‌ها دقیقاً به همان روش توزیع می‌شوند یعنی تشخیص تفاوت آن‌ها غیرممکن است. بنابراین، B هیچ چیزی را که خودش نمی‌توانسته محاسبه کند یاد نمی‌گیرد به‌جز برای این حقیقت که A از یک ریشه مربع پیمانه‌ای G آگاه است.

اجازه دهید تا در این‌جا یک پرسش متداول را پیش‌بینی کنیم. اگر درستی‌سنج می‌تواند بدون آگاهی از یک ریشه G مکالمات خوش منظری را ایجاد کند، چرا باید وقتی خواهان مکالمات مشابهی را تولید می‌کند متقاعد شود؟ جواب این است که وقتی B قرارداد را شبیه‌سازی می‌کند، آزاد است که اعداد را در جهت برعکس تولید کند؛ یعنی ابتدا D را انتخاب و سپس یک W مناسب را محاسبه کند. در یک اجرای قرارداد واقعی، A از چنین شانسی برخوردار نیست. درستی‌سنج انتظار دارد که W را پیش از این که d انتخاب شود ببیند و سپس خواهان باید یک D صحیح را بیابد.

گرچه در این‌جا چندین واژه فنی دشوار شرح و توضیح داده شد، در حقیقت این‌ها ضروریات بحث هستند که چرا یک سازوکار ویژگی دانش- صفر را دارا است.

ب– ۵ اصول طراحی پایه‌ای

مثال بخش پیشین یکی از دو ایده طراحی پایه‌ای که تقریباً تمام سازوکارهای شناخته‌شده دانش- صفر پشتیبانی می‌کند را پوشش می‌دهد:

- خواهان A یک شاهد را به درستی‌سنج B می‌فرستد. سپس B یکی از چند مجموعه سوال را از A می‌پرسد. اگر A متقلب باشد، نمی‌تواند به همه سوالات ممکن جواب دهد. بنابراین شانس به دام انداختن آن را داریم. از سویی دیگر، A هیچ‌گاه به بیش از یک سوال پاسخ نمی‌دهد و این سوال به تنهایی هیچ چیز را برای درستی‌سنج آشکار نمی‌کند.

این ایده طراحی، پایه سازوکارهای مشخص شده در بندهای ۵، ۶، ۷ و ۸ را شکل می‌دهد.

دیگر ایده طراحی و شکل‌دهنده مبنای سازوکار مشخص شده در بند ۹، بر پایه موارد زیر است:

- درستی‌سنج از خواهان یک سوال می‌پرسد که درستی‌سنج پیشتر پاسخ آن‌را می‌داند. قرارداد باید صحت این رابطه را تضمین کند. اگر A صادق باشد، می‌تواند به آسانی جواب صحیح را محاسبه کند، اما اگر متقلب باشد جوابی بهتر از یک حدس تصادفی نخواهد داشت که آن‌هم در اکثر اوقات نادرست است.

- از سوی دیگر، وقتی B جواب را دریافت می‌کند پیش‌تر از آن چه که A می‌گوید آگاه است و بنابراین سازوکار ویژگی دانش- صفر را دارا است.

یک مثال ساده از این حالت زمانی است که A باید مالکیت یک کلید خصوصی در یک سامانه کلید عمومی را اثبات کند. درستی‌سنج می‌تواند یک پیام تصادفی را تحت کلید عمومی A پوشیده ساخته و از A بخواهد که پیام پوشیده‌شده را بازگرداند. تنها کاربر آگاه از کلید خصوصی صحیح می‌تواند این کار را انجام دهد. برای به‌دست آوردن ویژگی دانش- صفر باید اطمینان حاصل شود که B پیام را از قبل می‌داند. این استاندارد شامل یک مثال یک مسیره برای انجام دادن آن است، یعنی می‌توان از B درخواست کرد که مقداری اطلاعات (شاهد) مربوط به پیام را آشکار سازد.

کتاب‌نامه یک رویکرد جامع از قراردادهای دانش- صفر [20] و یک مبنای رسمی برای درک دقیق قراردادهای دانش- صفر را نشان می‌دهد [3][10].

پیوست پ

(اطلاعاتی)

راهنمای انتخاب پارامتر و مقایسه سازوکارها

پ-۱ راهنمای انتخاب پارامتر

پ-۱-۱ اندازه‌های پیمانه

در این استاندارد، همه سازوکارهای احراز هویت از پیمانه‌ی استفاده می‌کنند که یا اول هستند (برای سازوکارهای SC) یا مرکب (برای هر نوع سازوکار دیگر).

در سال ۱۹۹۵، ادلیزکو[1] [18] آینده تجزیه به عامل‌های صحیح و لگاریتم‌های گسسته را پیش‌بینی کرد. «با سطح کنونی دانش، لگاریتم‌های گسسته برای محاسبه به پیمانه یک عامل اول که به‌طور مناسب انتخاب شده است اندکی مشکلتر از به‌دست آوردن یک عامل صحیح سخت با اندازه یکسان است، اما این اختلاف بزرگ نیست. بنابراین، برای حفظ جانب احتیاط در طراحی سامانه رمز، بهتر است فرض شود که تمامی طرح‌ریزی‌ها[2] درباره اندازه‌های اعداد صحیحی که قابل فاکتورگیری هستند، در مورد اندازه‌های اعداد اول به پیمانه لگاریتم‌های گسسته‌ای که قابل محاسبه هستند نیز صادق است.»

به‌عنوان نتیجه‌ای در پایان مقاله نقل شده[18]، کالیسکی[3] بر اهمیت اندازه‌های کلید متغیر در پیاده‌سازی‌ها تأکید و توصیه‌هایی در مورد اندازه پیمانه‌ها ارائه کرده است.

- امنیت کوتاه مدت: ۷۶۸ بیت
- امنیت میان مدت: ۱۰۲۴ بیت
- امنیت بلند مدت: ۲۰۴۸ بیت

برای تحلیل جامع طول‌های کلید به سیلورمن[4] [23]، لنسترا[5] و ورهویل[6] [14] مراجعه شود.

پ-۱-۲ پیمانه مرکب و عامل‌های اول

در سراسر استاندارد، عامل‌های اول بزرگ مجزا با ترتیب صعودی به‌صورت $p_1, p_2 \ldots$ نشان داده می‌شوند؛ پیمانه برابر با حاصلضرب عامل‌های اول یعنی $n = p_1 \times p_2 \times \ldots$ قرار داده می‌شود و α اندازه بیت پیمانه را نشان می‌دهد یعنی $2^{\alpha} / 2 < n < 2^{\alpha}$. به علاوه، استاندارد بیان می‌کند که اگر α مضرب تعداد عامل‌های اول باشد که با f نشان داده می‌شود، آن‌گاه اندازه بیت هر عامل اول باید α/f باشد یعنی $2^{\alpha/f} / 2 < p_1 \ldots < p_f < 2^{\alpha/f}$.

---

1 - Odlyzko
2 - Projection
3 - Kaliski
4 - Silverman
5- Lenstra
6- Verheul

یادآوری۱- استاندارد ملی ۱۰۸۲۳ چگونگی انتخاب اعداد اول بزرگ را مشخص می‌کند.

روش زیر بازه‌های متغیر متوالی برای انتخاب عامل‌های اول بزرگ به‌طور متوالی را تعریف می‌کند. اندازه بیت این عامل‌ها α/f است. از این پس، مقدار فعلی ضرب عامل‌های اول با z نشان داده می‌شود.

- نخستین عامل اول از بازه $۲^{\alpha/f}$ تا $۲ / ۲^{\alpha/f}$ انتخاب می‌شود. مقدار اولیه z برابر نخستین عامل اول قرار داده می‌شود.
- این مرحله f-۱ بار تکرار می‌شود. یک عامل اول جدید از بازه $۲ / ۲^{\alpha/f} \times (z / ۲^{|z|})$ تا $۲^{\alpha/f}$ انتخاب می‌شود. مقدار فعلی z در عامل اول جدید ضرب می‌شود.
- عامل‌های اول به ترتیب صعودی با p_1 تا p_f نشان داده می‌شوند و پیمانه n برابر با آخرین مقدار z قرار داده می‌شود.

روش زیر یک بازه ثابت واحد که اندکی کاهش یافته است را برای انتخاب هر عامل اول تعریف می‌کند.

- هر عامل اول از بازه $(۲^{\alpha/f}) \times \beta$ تا $۲^{\alpha/f}$ انتخاب می‌شود. fβ امین ریشه یک دوم را نشان می‌دهد.

یادآوری۲- تقریب مقدار β با یک عدد گویا بزرگتر از β مجاز است (برای مثال، پنج هفتم برای ریشه دوم یک دوم، چهار پنجم برای ریشه سوم یک دوم).

پ-۱-۳ طول‌های رشته‌های جدید بیت‌های تصادفی برای نمایش اعداد تصادفی

در سازوکارهای مشخص‌شده در بندهای ۵ تا ۸، خواهان هر عدد تصادفی r را مطابق فرمول شاهد به یک شاهد W تبدیل کرده و، سپس برای هر چالش d، مطابق فرمول پاسخ یک پاسخ D تولید می‌کند. پارامترهای روند W، d و D با یکدیگر یک اثبات دانش- صفر را تشکیل می‌دهند یعنی سه‌گانه‌ای که فرمول درستی‌سنجی را ارضا می‌کند و با $\{W, d, D\}$ نشان داده می‌شود. مجموعه اثبات‌ها یک خانواده از جایگشت‌های d را تشکیل می‌دهند. این خانواده مجموعه یا زیرمجموعه‌ای از اعداد صحیح نسبت به پیمانه است. این مجموعه اعداد صحیح یک دسته یا یک حلقه است.

از آنجایی که هر شخص ثالث می‌تواند با استفاده از فرمول درستی‌سنجی از هر چالش d و پاسخ D که به‌صورت تصادفی انتخاب شده است شاهد W (برای تولید سه‌گانه به‌صورت تصادفی) را محاسبه کند، ، حائز اهمیت است که مجموعه سه‌گانه‌ها چنان بزرگ باشد که مزیت به‌دست آمده به‌وسیله تولید سه‌گانه‌ها تا جای ممکن ناچیز باقی بماند.

این نکته حائز اهمیت است که خواهان اعداد تصادفی را به‌گونه‌ای انتخاب کند که احتمال حدس زدن آنها و عدد یکسانی که در طول عمر خواهان دو بار در حال انتخاب شدن است ناچیز باشد. برای مثال، اگر یک خواهان دوبار از یک عدد تصادفی یکسان استفاده کند، آن‌گاه او یک جفت سه‌گانه «به هم قفل‌شده[1]» را تولید خواهد کرد، یعنی پاسخ به دو چالش برای همان شاهد غیرصفر که با $\{W, d_1, D_1\}$ و $\{W, d_2, D_2\}$ نشان داده می‌شوند.

1 - Interlocked

- در سازوکار FS، از آنجایی که هر جفت از سه‌گانه‌های به هم قفل‌شده یک ترکیب ضربی پیمانه‌ای از کلیدهای خصوصی فراهم می‌کنند، هر شخص ثالث عملکرد خود برای جعل هویت خواهان را بهبود می‌دهد.
- در GQ1، سازوکارهای SC و GPS، هنگامی که هر جفت از سه‌گانه‌های به هم قفل‌شده کلیدهای خصوصی را فراهم می‌کنند، هر شخص ثالث می‌تواند هویت خواهان را جعل کند.
- در سازوکارهای GQ2، تولید کلید اطمینان می‌دهد که برای هر مقدار m و k، بیش از نیمی از تمام جفت سه‌گانه‌های به هم قفل‌شده، یک ریشه دوم پیمانه‌ای غیربدیهی از 1 را آشکار می‌کنند. آگاهی از چنین عددی، آگاهی برای تجزیه پیمانه را فراهم می‌کند یعنی تجزیه به عامل‌های صحیح در صورت وجود عامل. با تجزیه به عامل‌های صحیح هر شخص ثالث قادر به جعل هویت خواهان است.

با دریافت نشانه AB_1 یعنی یک شاهد W یا یک کد درهم W و Text، درستی‌سنج به‌صورت تصادفی یک چالش d تولید می‌کند. این نکته حائز اهمیت است که تمامی چالش‌های ممکن دارای احتمال یکسان باشند و بدین سان چالش غیرقابل پیش‌بینی باشد. هر متقلبی می‌تواند پیشاپیش با حدس زدن چالش در جعل هویت موفق شود. اگر 2^{δ} چالش دارای احتمال برابر باشند، آن‌گاه احتمال موفقیت یک متقلب یک در 2^{δ} است.

در سازوکارهای مشخص شده در بند ۹، هیچ شاهدی وجود ندارد. درستی‌سنج عدد d را از یک پارامتر تصادفی r که پاسخ D است، می‌سازد. اعداد d و D یک برهان را تشکیل می‌دهند که با {d, D} نشان داده می‌شود. چنین برهانی از نوع «دانش- صفر» است. مجموعه برهان‌ها یک بخش کوچک از جایگشت RSA است که بسیار کوچکتر از مجموعه‌های استفاده شده در سازوکارهای بندهای ۵ و ۸ است. درستی‌سنج باید پارامترهای تصادفی را به‌گونه‌ای انتخاب کند که احتمال حدس زدن و استفاده مجدد از آن‌ها ناچیز باشد. هر شخص ثالثی می‌تواند از عملیات عمومی برای تولید تصادفی جفت‌ها استفاده کند. مجموعه جفت‌ها باید آن چنان بزرگ باشد که مزیت به‌دست آمده به‌وسیله تولید پیشاپیش جفت‌ها تا جای ممکن ناچیز باقی بماند.

در نهایت، طول رشته‌های جدید بیت‌های تصادفی برای نمایش اعداد تصادفی برابر مقادیر زیر قرار داده می‌شود

- α بیت در FS، GQ1 و GQ2.
- $|q|$ بیت در SC (به‌طور نمونه $|q| = ۱۶۰$).
- $\sigma + \delta + ۸۰$ بیت در GPS1 (به‌طور نمونه $\sigma = ۱۶۰$).
- $\alpha + \delta + ۸۰$ بیت در GPS2.
- حداقل $|h| \times ۲$ ولی کمتر از $\alpha - |h|$ بیت در RSA_{UA} (به‌طور نمونه $|h| = ۱۶۰$).
- حداقل $|h| \times ۲$ ولی کمتر از $(\alpha - |h| - |ID|) \times ۰/۵$ بیت در RSA_{MA} (به‌طور نمونه $|h| = ۱۶۰$ و $|ID| = ۴۰$).

پ-۱-۴ راهبردهایی برای استفاده از سازوکارهای گوناگون

این بند چهار گروه از سازوکارها را مطابق تحلیل پیچیدگی‌های فرمول وارسی می‌کند.

الف- FS، GQ1 و GQ2 یعنی سازوکارهای مشخص شده در بندهای ۵ و۶.

ب- SC، GPS1 و GPS2 یعنی سازوکارهایی که در بندهای ۷ و ۸ مشخص شده‌اند.

پ- RSA_{UA} یعنی سازوکارهای مشخص شده در زیربند ۹-۲.

ت- RSA_{MA} یعنی سازوکارهای مشخص شده در زیربند ۹-۳.

یادآوری – یک دستگاه قابل‌حمل را در نظر بگیرید به‌طوری که تحلیل توان مربع کردن و ضرب کردن را تشخیص بدهد. برای سرّی نگه‌داشتن نماها، نیاز به اقدامات دوجانبه برای پیاده‌سازی فرمول شاهد SC و GPS و عملیات RSA خصوصی است. اما از آنجایی که نماها در فرمول‌های شاهد و پاسخ FS و GQ عمومی هستند، پیاده‌سازی مستقیم است.

در سازوکارهای FS، GQ1 و GQ2، شاهد v امین توان پیمانه‌ای عدد تصادفی r است. نمای درستی‌سنجی v کوتاه است. (تا ۴۰ بیت) فرمول شاهد یک **به‌نمارسانی پیمانه‌ای کوتاه** است. فرمول پاسخ نیز یک به‌نمارسانی پیمانه‌ای کوتاه و احتمالاً ترکیب شده است؛ این فرمولِ پاسخ، امکان مصالحه بین پیچیدگی محاسباتی و الزامات ذخیره‌سازی را فراهم می‌کند. با این وجود، فرمول پاسخ و فرمول شاهد دارای پیچیدگی مشابه هستند. فرمول درستی‌سنجی یک به نمارسانی پیمانه‌ای ترکیبی کوتاه است؛ این فرمول یک حجم کاری مشابه حجم کاری خواهان برای درستی‌سنج به‌وجود می‌آورد.

- ❖ سازوکارهای FS، GQ1 و GQ2 برای سامانه‌هایی که خواهان و درستی‌سنج دارای عملکرد مشابه هستند مناسب هستند. برای مثال، اگر خواهان یک کارت هوشمند باشد، آن‌گاه در حالی که حجم کاری درستی‌سنج و خواهان مشابه است، توان محاسباتی کارت هوشمند برای یک درستی‌سنج کافی است. در نتیجه، یک کارت پرداخت و یک کارت تجارتی می‌توانند اصالت یکدیگر را به‌صورت محلی از پایانه پرداخت یا حتی از راه دور از طریق اینترنت وارسی کنند.

در سازوکارهای FS، GQ1 و GQ2 اندازه چالش باید بهینه شود: هر چه چالش کوچکتر باشد، به توان رسانی پیمانه‌ای کوتاه‌تر است. برای مثال، $۲^{k \times m}$ چالش GQ2 ممکن وجود دارد.

- احتمال یک از ۲۳۶ می‌تواند یک سطح امنیتی مناسب در یک محیط با امنیت بالا باشد. به‌عنوان مثال، $k = ۱۸$ و دو عدد پایه‌ای یا $k = ۱۲$ و سه عدد پایه‌ای یا $k = ۶$ و شش عدد پایه‌ای.
- احتمال یک از $۲^{۲۴}$ می‌تواند یک سطح امنیتی مناسب در اینترنت باشد. به‌عنوان مثال، $k = ۱۸$ و دو عدد پایه‌ای یا $k = ۸$ و سه عدد پایه‌ای یا $k = ۴$ و شش عدد پایه‌ای.
- احتمال از ۶۵۵۳۶ می‌تواند یک سطح امنیتی مناسب برای جلوگیری[1] از «yes card» ها بر روی دستگاه‌های پرداخت خودکار ضبط‌کننده کارت‌های غیرقابل‌قبول باشد. به‌عنوان مثال، $k = ۸$ و دو عدد پایه‌ای یا $k = ۴$ و سه عدد پایه‌ای یا $k = ۲$ و هشت عدد پایه‌ای.
- احتمال در ۴ می‌تواند یک سطح امنیتی مناسب برای جلوگیری دوره‌ای از کارت‌های جعلی[2] در کدگشاهای تلویزیون پولی «رسمی» باشد. به‌عنوان مثال، $k = ۱$ و دو عدد پایه‌ای.

در سازوکارهای SC و GPS، شاهد r امین توان پیمانه‌ای یک پایه g است. عدد تصادفی r متوسط است (برای مثال، ۱۶۰ بیت برای سازوکارهای SC، ۲۴۸ تا ۲۸۰ بیت برای سازوکارهای GPS1، $\alpha+۸۸$ تا $\alpha+۱۲۰$ بیت برای سازوکارهای GPS2). فرمول شاهد یک به‌نمارسانی پیمانه‌ای متوسط یا بلند است.

1 - Deterring
2 - Pirate cards

در سازوکارهای SC و GPS، پیچیدگی فرمول پاسخ در مقایسه با فرمول شاهد ناچیز است. از آنجایی که محاسبه نشانه AB_1 نیازی به تعامل با درستی‌سنج ندارد، می‌توان مجموعه‌ای از کوپن‌ها را $(r, TokenAB_1)$ پیشاپیش محاسبه و در خواهان ذخیره کرد. به علاوه، اگر r به‌صورت شبه‌تصادفی تولید شود، نیازی به ذخیره آن نیست زیرا می‌توان آن را بازتولید کرد. فرمول درستی‌سنجی یک به‌توان‌رسانی پیمانه‌ای دوگانه متوسط است یا یک به‌توان‌رسانی پیمانه‌ای بلند؛ این فرمول یک حجم کاری مشابه حجم کاری خواهان برای درستی‌سنج به وجود می‌آورد. بهینه‌سازی اندازه چالش مجاز است اما بدون گذاشتن هیچ اثری بر روی پیچیدگی فرمول‌های شاهد و درستی‌سنجی.

- ❖ سازوکارهای SC و GPS برای سامانه‌هایی است که در آنها می‌توان «کوپن‌ها» را پیشاپیش برای خواهان آماده کرد و تعامل با یک درستی‌سنج قدرتمند باید تا جایی که امکان دارد سریع صورت گیرد. برای مثال، یک دستگاه بدون توان محاسباتی (برای مثال یک برچسب[1]) می‌تواند به سرعت پاسخ دهد.

در سازوکارهای RSA_{AU}، درستی‌سنج چالش را به‌وسیله یک به‌نمارسانی پیمانه‌ای کوتاه محاسبه می‌کند، سپس خواهان پاسخ را به‌وسیله یک **به‌نمارسانی پیمانه‌ای بلند** محاسبه می‌کند. از آنجایی که چالش باید بزرگ باشد، هیچ‌گونه فضایی برای بهینه‌سازی در رابطه با اندازه چالش وجود ندارد. چون محاسبه نشانه BA نیازی به تعامل با خواهان ندارد، می‌توان مجموعه‌ای از کوپن‌ها (r, TokenBA) را پیشاپیش در خواهان ذخیره کرد. به علاوه، اگر r به‌صورت شبه‌تصادفی تولید شود، نیازی به ذخیره آن نیست زیرا می‌توان آن را بازتولید کرد.

- ❖ سازوکارهای RSA_{AU} برای سامانه‌هایی مناسب هستند که در آنها می‌توان «کوپن‌ها» را پیشاپیش به‌صورت «ایمن» برای درستی‌سنج‌هایی که با خواهان‌های قدرتمند تعامل می‌کنند آماده کرد. به‌عنوان مثال، یک دستگاه بدون توان محاسباتی (برای مثال یک برچسب) می‌تواند اصالت یک رایانه قدرتمند را وارسی کند.

در سازوکارهای RSA_{MA}، هر دو هستار باید یک به‌توان‌رسانی پیمانه‌ای کوتاه و یک به‌توان‌رسانی پیمانه‌ای بلند را محاسبه کنند. برای چنین سازوکارهایی امکان راهبرد «کوپن» وجود ندارد.

پ-۲ مقایسه سازوکارهای احراز هویت

پ-۲-۱ نمادها و اصطلاحات کوتاه نویسی شده

این مقایسه از اقدامات زیر استفاده می‌کند: ذخیره مورد انتظار در خواهان، پیچیدگی محاسبات صورت‌گرفته به‌وسیله خواهان، پیچیدگی محاسبات صورت‌گرفته به‌وسیله درستی‌سنج، ارتباطات مورد نیاز بین خواهان و درستی‌سنج.

یادآوری – اگر خواهان یک دستگاه قابل حمل باشد (به‌عنوان مثال، یک کارت هوشمند)، از آن‌جا که ظرفیت‌های پردازش و ذخیره‌سازی کارت‌های هوشمند در مقایسه با ظرفیت‌های مجاز برای درستی‌سنج بسیار محدود است، پیچیدگی محاسبات و ارتباطات و ذخیره‌سازی ممکن است تعیین‌کننده باشد.

3 - Tag

نمادها و اصطلاحات کوتاه شده زیر در این پیوست مورد استفاده قرار می‌گیرند:

ChC	computational complexity of a CRT composition	پیچیدگی محاسباتی یک ترکیب CRT
ChD	computational complexity of a CRT decomposition	پیچیدگی محاسبات یک تجزیه CRT
CM	communication required between the claimant and the verifier (CMh when using a hash-function)	ارتباطات مورد نیاز بین خواهان و درستی‌سنج (CM_h درهنگام استفاده از یک تابع درهم‌ساز)
CPC	complexity of the computations carried out by the claimant	پیچیدگی محاسبات صورت‌گرفته به‌وسیله خواهان
CPV	complexity of the computations carried out by the verifier	پیچیدگی محاسبات صورت‌گرفته به‌وسیله درستی‌سنج
Cr	CRT coefficient	ضریب CRT
CS	storage required in the claimant	ذخیره‌سازی مورد نیاز در خواهان
HW(v)	number of bits set to 1 in the binary representation of number v, e.g. HW(65 537 = 216+1) = 2	تعداد بیت‌های برابر با 1 قرار داده شده در نمایش دودویی عدد v، به‌عنوان مثال HW(۶۵ ۵۳۷=$۲^{۱۶}$+۱)=۲
Mα	computational complexity of a modular multiplication (α is the bit size of the modulus)	پیچیدگی محاسباتی یک ضرب پیمانه‌ای (α اندازه بیت پیمانه است.)
Xα	computational complexity of a modular square (α is the bit size of the modulus)	پیچیدگی محاسباتی یک مربع پیمانه‌ای (α اندازه بیت پیمانه است.)

پ-۲-۲ پیچیدگی عملیات‌های پیمانه‌ای

این عبارت پیچیدگی محاسباتی عملیات‌های پیمانه‌ای یعنی ضرب پیمانه‌ای، مربع پیمانه‌ای، به‌نمارسانی پیمانه‌ای و به‌نمارسانی پیمانه‌ای ترکیبی را ارزیابی می‌کند.

ضرب پیمانه‌ای به‌صورت $A \times B$ به پیمانه C تعریف می‌شود و ممکن است که به‌صورت دو عملیات متوالی انجام شود: یک ضرب که با یک کاهش دنبال می‌شود. بنابرتجربه، حجم کاری ناشی از یک ضرب تقریباً با حجم کاری ناشی از یک کاهش برابر است.

- زمانی که A و B اندازه‌ای برابر با C داشته باشند، حاصلضرب آن‌ها طولی دو برابر C خواهد داشت.
- کاهش باقی‌مانده تقسیم نتیجه را با C تأمین می‌کند.

هنگامی که A و B اندازه‌ای برابر با C داشته باشند، آن‌گاه پیچیدگی ضرب پیمانه‌ای با $M_{|c|}$ نشان داده می‌شود.

اگر عدد n، f برابر درازتر از عدد p باشد یعنی اگر n و p^f اندازه یکسانی داشته باشند، یعنی $|n| = f \times |p|$، آن‌گاه نسبت بین یک ضرب به پیمانه n و یک ضرب به پیمانه p تقریبا برابر f^2 است ($M_{|n|} \approx f^2 \times M_{|p|}$).
در نتیجه، مقدار $M_{|c|}$متناسب با $|C|^2$ است.

به‌عنوان مثال، اگر n دو برابر درازتر از p باشد، یعنی $|n| = 2 \times |p|$ ، آن‌گاه $M_{|n|} \approx 4 \times M_{|p|}$.

مربع پیمانه‌ای به‌صورت A^2 به پیمانه C تعریف می‌شود. این عملیات مجاز است که به‌عنوان دو عملیات متوالی هم انجام شود: یک مربع که با یک کاهش دنبال می‌شود.

- هنگامی که A اندازه‌ای برابر C دارد، مربع کردن منجر به نتیجه‌ای با طول دو برابر C می‌شود. بنا به گفته منزس[1] ، فان اورشوت[2] و ونستون[3][16]، پیچیدگی مربع کردن نصف پیچیدگی ضرب است.

یادآوری – به ازای $A \times B = ((A+B)2 - (A-B)2) / 4$ ، مجاز است که ضرب از دو مرتبه استفاده از رویه مربع‌سازی نتیجه شود.

- کاهش، باقی‌مانده تقسیم نتیجه را با C تأمین می‌کند، پیچیدگی این عملیات مانند فوق است.

هنگامی که A اندازه‌ای برابر با C داشته باشد، آن‌گاه پیچیدگی مربع پیمانه‌ای با $X_{|c|}$ نشان داده می‌شود.

به‌نمارسانی پیمانه‌ای به‌صورت A^B به پیمانه C تعریف می‌شود. این عملیات مجاز است که به‌صورت نسخه از راست به چپ الگوریتم ضرب و مربع انجام شود[13][16]، یعنی $|B| - ۱$ مربع پیمانه‌ای شده و $HW(B) - ۱$ در A ضرب پیمانه‌ای می‌شود.

به‌نمارسانی پیمانه‌ای ترکیبی به‌صورت $A_1^{B1} \times \ldots \times A_x^{Bx}$ به پیمانه C تعریف می‌شود. این عملیات مجاز است که به‌صورت مربع پیمانه‌ای بیشینه $\{|B_1|, \ldots, |B_x|\} - ۱$ و ضرب پیمانه‌ای $HW(B_1) + \ldots + HW(B_x) - ۱$ در A_i انجام شود.

---

1 - Menezes
2 - Van Oorschot
3 - Vanstone

- اگر A_i کوچک باشد (یعنی $|A_i| \leq 8$)، آن‌گاه ضرب‌های پیمانه‌ای به موجب B در مقایسه با مربع‌های پیمانه‌ای قابل صرف‌نظر هستند.
- بسته به این که آیا اندازه بیت نما یعنی بیشینه$\{|B_1|, \ldots |B_x|\}$ کوچک یعنی حداکثر تا ۴۰، یا متوسط یعنی $\{|C|, 80+|C|$ تا $120+|C|\}$، یا بزرگ باشد یعنی $\{160, 240$ تا $280\}$، به توان رساندن پیمانه‌ای نیز کوچک، متوسط یا بزرگ است.

پ-۲-۳ فن CRT

این بند به تعریف فن CRT یعنی استفاده از قضیه باقی‌مانده چینی می‌پردازد.

دو عدد x_1 و x_2 را به‌صورت $x_2<x_1$ در نظر بگیرید به‌گونه‌ای که نسبت به هم اول باشند، اما الزاماً نیازی به اول بودنشان نیست. حاصلضرب آن‌ها را نیز با x نشان داده می‌کنیم.

یادآوری – فن CRT هر تعداد عامل اول را می‌پذیرد. دو عامل اول مجزا p1 و p2 را در نظر بگیرید به‌صورتی که $p1 < p2$ و ضرب آن‌ها به‌صورت $p1 \times p2$ است. سپس، سه عامل اول مجزا p1، p2 و p3 را در نظر بگیرید به‌صورتی که $p3 < (p1 \times p2)$ و حاصلضرب آن‌ها $(p1 \times p2) \times p3$ و به همین ترتیب.

بنابر تعریف ضریب CRT، عدد صحیح مثبت Cr است که از x_1 کوچکتر بوده و بر $Cr \times x_2 - 1$ بخش‌پذیر است.

بنا بر تعریف، ترکیب CRT هر جفت مولفه یعنی X_1 از مجموعه $\{0, 1, \ldots x_1-1\}$ و X_2 از مجموعه $\{0, 1, \ldots x_2-1\}$ را به عدد یگانه مرتبط X از مجموعه $\{0, 1, \ldots x-1\}$ تبدیل می‌کند. اعداد x_1 و x_2 و Cr ضریب CRT به صورت زیر مورد استفاده قرار می‌گیرند.

$$Y = X_1 - X_2 \; mod \; x_1; Z = Y \times Cr \; mod \; x_1; X = Z \times x_2 + X_2$$

ترکیب CRT متشکل است از یک ضرب پیمانه‌ای به پیمانه یک عامل و حاصل‌ضرب دو عدد با اندازه یکسان به‌عنوان یک عامل که منجر به یک عدد با اندازه‌ای برابر با پیمانه می‌شود. هنگامی که دو عامل اندازه یکسان دارند مانند $|p_1| = |p_2| = |n| / 2$، از ChC برای نمایش پیچیدگی ترکیب استفاده می‌شود.

هر عدد X از مجموعه $\{0, 1, \ldots x-1\}$ به یک جفت مؤلفه، یعنی X_1 از مجموعه $\{0, 1, \ldots x_1-1\}$ و X_2 از مجموعه $\{0, 1, \ldots x_2-1\}$ مانند زیر تجزیه می‌شود. تجزیه وارون عمل ترکیب است و برعکس.

$$X_1 = X \; mod \; x_1 \text{ و } X_2 = X \; mod \; x_2$$

تجزیه متشکل است از دو کاهش به پیمانه یک عامل. هنگامی که دو عامل هم‌اندازه باشند، به‌عنوان مثال، $|p_1| = |p_2| = |n| / 2$، پیچیدگی تجزیه با ChD نشان داده می‌شود.

$$ChD \approx M_{|p|} \approx 0.25 \times M_{|n|}$$

به‌عنوان مثال، فن CRT پیچیدگی یک عملیات RSA را از یک به‌نمارسانی پیمانه‌ای بلند به پیمانه n (یعنی $(5/4 \times |n| \times M_{|n|})$) به یک ChD به‌علاوه دو به‌نمارسانی پیمانه‌ای به پیمانه p_i (با کاهش نما به پیمانه $p_i - 1$) به‌علاوه یک ChC (یعنی $(1+2.5\times|p|+1.5)\times M_{|p|} = 2.5\times(|p|+1)\times M_{|p|}$) کاهش می‌دهد. به ازای $|n| = 2\times|p|$، $M_{|n|} \approx 4\times M_{|p|}$ و پیچیدگی‌های کاهش یافته $(5/16)\times|n|\times M_{|n|} \approx$ است.

پ-۲-۴ تحلیل پیچیدگی

پ-۲-۴-۱ FS

خواهان n و Q_1 تا Q_m را ذخیره می‌کند. C

فرمول شاهد $W = r^2 \, mod^* \, n$ یعنی $X_{|n|}$

فرمول پاسخ $D = r \times \prod_{i=1}^{m} Q_i^{d_i} \, mod^* \, n$ یعنی $HW(d) \times M_{|n|}$

برای t تکرار به ازای $HW(d) \approx m/2$ به‌طور میانگین C

فرمول درستی‌سنجی $W^* = D^2 \times \prod_{i=1}^{m} G_i^{d_i} \, mod^* \, n$ یعنی $X_{|n|} + HW(d) \times M_{|n|}$

برای t تکرار به ازای $HW(d) \approx m/2$ به‌طور میانگین C

نشان AB_1 = W به ازای |n| بیت یا یک کد درهم به ازای $|h|$ بیت یا d به ازای m بیت؛ نشانه $AB_2 = D$ به ازای $|n|$ بیت

برای تبادلات t (C

پ-۲-۴-۲ GQ1

خواهان n و v و Q را ذخیره می‌کند. C

فرمول شاهد $W = r^v \, mod \, n$ یعنی $(|v| - 1) \times X_{|n|} + (HW(v) - 1) \times M_{|n|}$

فرمول پاسخ $D = r \times Q^d \, mod \, n$ یعنی $M_{|n|} + (|d| - 1) \times X_{|n|} + (HW(d) - 1) \times M_{|n|}$

از آن‌جا که d از مجموعه $\{۰، ۱، \ldots ۱-v\}$ یعنی $|d| = |v|$ و $HW(d) = |v|/2$ C

فرمول درستی‌سنجی $W^* = D^v \times G^d \, mod \, n$ یعنی $(|v| - 1) \times X_{|n|} + (HW(d) + HW(v) - 1) \times M_{|n|}$

به ازای $HW(d) = |v|/2$ C

نشان AB_1 =W به ازای |n| بیت یا یک کد درهم به ازای $|h|$ بیت یا d به ازای $|v|$ بیت؛ نشانه $AB_2 = D$ به ازای $|n|$ بیت

C C

پ-۲-۴-۳ GQ2

خواهان p_1، p_2، Cr و $Q_{1,1}$ تا $Q_{m,2}$ را ذخیره می‌کند. $CS(bits) = (m + 1.5) \times |n| = (m + 1.5) \times a$

فرمول شاهد $W_j = r_j^{2^{k+b}} \bmod p_j$ یعنی $2 \times (k + b) \times X_{|p|} + ChC$

فرمول پاسخ $D_j = r_j \times \prod_{i=1}^{m} Q_{i,j}^{d_j} \bmod p_j$ $2 \times \left((k - 1) \times X_{|p|} + 0.5 \times k \times m \times M_{|p|}\right) + ChC$

به ازای $ChC \approx 1.5M_{|p|}$, ≈

به ازای $M_{|p|} \approx M_{|n|}/4$ C

فرمول‌درستی‌سنجی $W^* = D^{2^{k+b}} \times \prod_{i=1}^{m} G_i^{d_i} \bmod n$ یعنی $(k + b) \times X_{|n|}$

از آن‌جا که اعداد پایه‌ای کوچک هستند C

نشان AB_1 =W به ازای |n| بیت یا یک کد درهم به ازای $|h|$ بیت یا d به ازای $k \times m$ بیت؛ نشان $D = AB_2$ به ازای $|n|$ بیت

C

پ-۲-۴-۴ SC

خواهان p، q، g و Q را ذخیره می‌کند. C

فرمول شاهد $W = g^r \bmod p$ یعنی $(|r| - 1) \times X_{|p|} + (HW(r) - 1) \times M_{|p|}$

فرمول پاسخ $D = r - d \times Q \bmod q$ قابل‌چشم‌پوشی

به ازای $|r| = |q|$ و $HW(r) = |q|/2$، C

فرمول درستی‌سنجی $W^* = g^D \times G^d \bmod p$ یعنی $(|D| - 1) \times X_{|p|} + (HW(D) + HW(d) - 1) \times M_{|p|}$

به ازای $HW(d) = \delta/2$، $|D| = |q|$ و $HW(D) = |q|/2$ C

نشان AB_1 برابر با W به عنوان |p| بیت یا یک کد درهم به عنوان |h| بیت؛ d به عنوان δ بیت؛ نشانه AB_2 برابر D به عنوان |q| بیت.

$CM(bits) \approx \alpha + |q| + \delta$ C

پ-۲-۴-GPS15

بدون CRT، خواهان n و Q را ذخیره می‌کند. C

فرمول شاهد $W = g^r \bmod n$ که در آن $g = 2$، یعنی $(|r| - 1) \times X_{|n|}$

فرمول پاسخ $D = r - d \times Q$ قابل‌چشم‌پوشی

به ازای $|r| = \rho = \sigma + \delta + 80$، C

با CRT، خواهان p_1، p_2، Cr و Q را ذخیره می‌کند. C

فرمول شاهد $W_j = g^r \bmod p_j$ که در آن $g = 2$، یعنی $2 \times (|r| - 1) \times X_{|p|} + ChC$

فرمول پاسخ $D = r - d \times Q$ قابل‌چشم‌پوشی

به ازای $|r| = \rho$ و $\rho < 0.5 \times |n|$ و $ChC \approx 1.5 \times M_{|p|}$ ≈

به ازای $M_{|p|} \approx M_{|n|}/4$ و $\rho = \sigma + \delta + 80$، C

فرمول درستی‌سنج $W^* = g^D \times G^d \bmod n$ یعنی $(|D| - 1) \times X_{|n|} + (HW(d) - 1) \times M_{|n|}$

به ازای $HW(d) = \delta/2$ و $|D| = \rho$، C

نشان AB_1 برابر با W به‌عنوان |n| بیت یا یک کد درهم به‌عنوان |h| بیت؛ d به‌عنوان δ بیت؛ نشانه AB_2 برابر D

به‌عنوان $\rho = \sigma + \delta + 80$ بیت.

C $CM(bits) \approx \alpha + \sigma + 80$

پ-۲-۴-۶ GPS2

بدون CRT، خواهان n و Q را ذخیره می‌کند. C

فرمول شاهد $W_j = G^{r \times v} \bmod n$ که در آن $G = 2$، یعنی $(|r| + |v|) \times X_{|n|}$

فرمول پاسخ $D = r - d \times Q$ قابل‌چشم‌پوشی

$\approx (|n| + 2 \times \delta + 80) \times 0.75 \times M_{|n|}$

C

با CRT، خواهان p_1، p_2، Cr و Q را ذخیره می‌کند. C

فرمول شاهد $W_j = G^{r \times v \bmod p_j - 1} \bmod p_j$ که در آن یعنی $2 \times (|p| - 1) \times X_{|p|} + ChC$
$G = 2$،

فرمول پاسخ $D = r - d \times Q$ قابل‌چشم‌پوشی

به ازای $2 \times |p| = |n|$ و $ChC \approx 1.5 \times M_{|p|}$ ≈

به ازای $M_{|p|} \approx M_{|n|}/4$، C

فرمول درستی‌سنج $W^* = G^{d+v \times D} \bmod n$ یعنی $(|D \times v| - 1) \times X_{|n|} + (HW(D \times d) - 1) \times M_{|n|}$

به ازای $HW(D \times v) = \rho/2$، $|D \times v| = \rho$ و $\rho = \alpha + \delta + 80$، C

نشان AB_1 برابر با W به‌عنوان |n| بیت یا یک کد درهم به‌عنوان |h| بیت؛ d به‌عنوان δ بیت؛ نشانه AB_2 برابر D به‌عنوان $\rho = \alpha + \delta + 80$ بیت.

C $CM(bits) \approx 2 \times \alpha + 2 \times \delta + 80$

پ-۲-۴-۷ RSA_{UA}

خواهان p_1، p_2، s_1، s_2 و Cr را نگه می‌دارد. C

عملیات RSA عمومی: $P_X(m) = m^v \ mod \ n$ یعنی $(|v| - 1) \times X_{|n|} + (HW(v) - 1) \times M_{|n|}$

C

به‌عنوان مثال، اگر v برابر با $2^{16} + 1$ قرار داده شود، C

عملیات RSA خصوصی با استفاده از فن CRT C

نشان BA برابر با d به‌عنوان |n| بیت؛ نشانه AB برابر r^* C
به‌عنوان |h|-|n|بیت.

پ-۲-۴-۸ RSA_{MA}

هر هستار p_1، p_2، s_1، s_2 و Cr را نگه می‌دارد. C

هر هستار یک عملیات RSA خصوصی و یک عملیات RSA عمومی انجام می‌دهد.

نشان BA_1 برابر با d به‌عنوان |n| بیت؛ نشانه AB برابر d^* به‌عنوان |n| بیت؛ نشانه AB_2 برابر rr^{**} به‌عنوان $0.5 \times |n| - |h| - |ID|$ بیت.

C

پ-۲-۴-۹ خلاصه ارزیابی

جدول پ-۱ ارزیابی زیربندهای پ-۲-۴-۱ تا پ-۲-۴-۸ را خلاصه می‌کند. در سازوکارهای FS، GQ، SC و GPS ارتباط CM یا CMh مورد نیاز است. چنین طبقه‌بندی در مورد سازوکار RSA صادق نیست. در سازوکارهای GPS، استفاده ازفن CRT به‌وسیله خواهان برای CS و CPC ارزیابی شده است. جدول پ-۱ در زیربند پ-۲-۵ برای $\alpha =$ ۱۰۲۴، $|h| =$ ۱۶۰ (برای مثال، RIPEMD-160 و SHA-1) و $|ID| =$ ۴۰ به همراه مقادیر متفاوت سطح امنیتی استفاده می‌شود.

جدول پ-۱ - خلاصه ارزیابی

FS					
GQ1					
GQ2					
SC					
GPS1					
With CRT					
GPS2					
With CRT					
RSA_{UA}					
RSA_{MA}					

پ-۲-۵ مقایسه برای $\alpha =$ ۱۰۲۴ با مقادیر متفاوت سطح امنیتی

پ-۲-۵-۱ مقایسه برای $\alpha =$ ۱۰۲۴ با 2^{-8} به‌عنوان سطح امنیتی

جدول پ-۲ سازوکارها را برای $\alpha =$ ۱۰۲۴ (امنیت میان مدت) با 2^{-8} به‌عنوان سطح امنیتی مقایسه می‌کند.

FS: $m = 2$ و $t = 4$

GQ: $v = 257 = 2^8 + 1$، یعنی $|v| = 9$ و $HW(v) = 2$

GQ2: b = 1، $k = 4$ $(v = 32)$ و m = 2

SC: $|q| = 160$ و $\delta = 8$

GPS1: $\delta = 8$، $(\rho = \sigma + \delta + 80 = 248)$ $|Q| = \sigma = 160$ و $g = 2$

GPS2: $v = 257 = 2^8 + 1$، $\delta = 8$، $(\rho = \alpha + \delta + 80 = 1112)$ $|Q| = \alpha = 1024$ و $G = 2$

RSA: $v = 65537 = 2^{16} + 1$

جدول پ-۲ - مقایسه برای$\alpha = ۱۰۲۴$ با $۲^{-۸}$ به عنوان سطح امنیتی

	C				
FS	3.00	7.00	7.00	8.01	4.63
GQ1	2.01	17.50	11.50	2.01	1.17
GQ2	5.75	5.75	3.75	2.01	1.16
SC	2.31	200.00	204.00	1.16	0.32
GPS1	1.16	186.00	190.00	1.25	0.41
With CRT	1.66	93.00			
GPS2	2.00	840.00	1390.00	2.09	1.25
With CRT	2.50	192.00			
RSA_{UA}	2.50	320.00	13.00	1.84	
RSA_{MA}	2.50	334.75	334.75	2.41	

پ-۲-۵-۲ مقایسه برای$\alpha = ۱۰۲۴$ با $۲^{-۱۶}$ به‌عنوان سطح امنیتی

جدول پ-۳ سازوکارها را برای $\alpha = ۱۰۲۴$ (امنیت میان مدت) با $۲^{-۱۶}$ به‌عنوان سطح امنیتی مقایسه می‌کند.

FS: $m = 4$ و $t = 4$

GQ: $v = 65537 = 2^{16} + 1$، یعنی $|v| = 17$ و $HW(v) = 2$

GQ2: $b = 1$، $(v = 32)$ $k = 4$ و $m = 4$

SC: $|q| = 160$ و $\delta = 16$

GPS1: $\delta = 16$، $(\rho = \sigma + \delta + 80 = 256)$ $|Q| = \sigma = 160$ و $g = 2$

GPS2: $v = 65537 = 2^{16} + 1$، $\delta = 16$، $(\rho = \alpha + \delta + 80 = 1120)$ $|Q| = \alpha = 1024$ و $G = 2$

RSA: $v = 65537 = 2^{16} + 1$

جدول پ-۳ - مقایسه برای $\alpha = ۱۰۲۴$ با $۲^{-۱۶}$ به عنوان سطح امنیتی

	C				
FS	5.00	11.00	11.00	8.02	4.64
GQ1	2.02	33.50	21.50	2.02	1.17
GQ2	5.50	7.75	3.75	2.02	1.17
SC	2.31	200.00	208.00	1.17	0.33
GPS1	1.16	192.00	200.00	1.27	0.42
With CRT	1.66	96.00			
GPS2	2.00	852.00	1400.00	2.11	1.27
With CRT	2.50	192.00			
RSA_{UA}	2.50	320.00	13.00	1.84	
RSA_{MA}	2.50	334.75	334.75	2.41	

پ-۲-۵-۳ مقایسه برای $\alpha =$ ۱۰۲۴ با 2^{-36} به عنوان سطح امنیتی

جدول پ-۴ سازوکارها را برای $\alpha = ۱۰۲۴$ (امنیت میان مدت) با 2^{-36} به عنوان سطح امنیتی مقایسه می‌کند.

FS: $m = 6$ و $t = 6$

GQ: $v = 2^{36} + 2^{13} + 1$، یعنی $|v| = 37$ و $HW(v) = 3$

GQ2: $b = 1$، $k = 6$ $(v = 128)$ و $m = 6$

SC: $|q| = 160$ و $\delta = 36$

GPS1: $\delta = 36$، $(\rho = \sigma + \delta + 80 = 276)$ $|Q| = \sigma = 160$ و $g = 2$

GPS2: $v = 2^{36} + 2^{13} + 1$، $\delta = 16$، $(\rho = \alpha + \delta + 80 = 1140)$ $|Q| = \alpha = 1024$ و $G = 2$

RSA: $v = 65537 = 2^{16} + 1$

جدول پ-۲ - مقایسه برای $\alpha =$ ۱۰۲۴ با 2^{-36} به عنوان سطح امنیتی

	C				
FS	7.00	22.50	22.50	12.04	6.97
GQ1	2.04	74.50	47.50	2.04	1.19
GQ2	7.50	14.25	5.25	2.04	1.19
SC	2.31	200.00	218.00	1.19	0.35
GPS1	1.16	207.00	225.00	1.30	0.46
With CRT	1.66	103.50			
GPS2	2.00	882.00	1425.00	2.15	1.30
With CRT	2.50	192.00			
RSA_{UA}	2.50	320.00	13.00	1.84	
RSA_{MA}	2.50	334.75	334.75	2.41	

پیوست ت
(اطلاعاتی)
مثال‌های عددی

ت-۱ سازوکار FS

ت-۱-۱ تولید کلید

ت-۱-۱-۱ جفت کلید نامتقارن ($v = 2$، طرح رابین)

برای هر عامل اول، اندازه بیت ۵۱۲ و برای پیمانه $\alpha =$ ۱۰۲۴ است. وقتی که نمای درستی‌سنجی برابر $v =$ ۲ است یکی از عامل‌های اول با $3 \; mod \; 4$ و عامل اول دیگر با $7 \; mod \; 8$ هماهنگ است.

p_1 = A220780E 0E0717BE D41CD957 418C6215 D25CAE16 E4F6013F 7EFC69EF AB025A1E
42848EB6 9E0983C5 389B4037 CB7B6A2C EEF2134D CBA06201 376C39EA 33D297CB

p_2 = D4610C36 12718EF3 EAC804E2 6C2751A0 EA8A8FB2 522499DA 44105CFC 19C7A94F
06784168 DEF906A9 7AEBD153 6E3E32A4 61933F30 33006D50 F5A7B799 4FAD11FF

n = 86805974 E5195F47 C8DD033B 658151DE EF39BF57 969645CD A5610766 64D121ED
6C08EC5F 7E6DC1DF C97CD4C8 B154D5FD 21CC06FF DC2C9E44 6789AF0F 916B2B28
D75263E4 47D7FD58 8E46AFE8 99F6A36D 60DFDDA9 48066026 BE7982D8 17777F5B
30EE8A40 0C3B7508 278FD600 E7770A51 43C7DB91 CC16CE01 9DB51535 D408AE35

u = 10D00B2E 9CA32BE8 F91BA067 6CB02A3B DDE737EA F2D2C8B9 B4AC20EC CC9A243D
AD811D8B EFCDB83B F92F9A99 162A9ABF A43980DF FB8593C8 8CF135E1 F22D6564
EC1A1BF4 04EBEAD4 B9EC3A35 DD885DF6 D47F13FC 021D78A1 9F6D977D 8A55AF7D
BCFE3744 11E71D53 2E81188E B5B7ADAF FE685122 79AEBFD5 EE142476 4A11208D

ت-۱-۱-۲ داده‌های شناسایی و جفت‌های نامتقارن اعداد

پارامتر تعدد جفت برابر با $m =$ ۸ است. هر قسمت از داده‌های شناسایی از افزودن یک پسوند ۱۶ بیتی به رشته بیت نمایش‌دهنده «Alex Ample» به‌دست می‌آید.

Id_1 = 416C 6578 2041 6D70 6C65 0001 Id_2 =416C 6578 2041 6D70 6C65 0002
Id_3 = 416C 6578 2041 6D70 6C65 0003 Id_4 =416C 6578 2041 6D70 6C65 0004
Id_5 =416C 6578 2041 6D70 6C65 0005 Id_6 =416C 6578 2041 6D70 6C65 0006
Id_7 =416C 6578 2041 6D70 6C65 0007 Id_8 =416C 6578 2041 6D70 6C65 0008

سازوکار قالب از SHA-1 استفاده می‌کند. SHA-1 سومین تابع درهم‌ساز مشخص شده در استاندارد ISO/IEC 10118-3[25] است.

G_1 = 0004C24F 6F5F4A75 C3787AF2 8F50FF3B 5E3404D2 0DF52FF4 E86E132B CBF9AD8B
E5BE0CF3 C42FCD80 3AA602D3 22E1BFE3 3F08737A A47CB9AC 65870280 59E2B467
C4CED23F 7EE67A52 DB93E947 60E71AC0 1EE93894 A6B7E592 456534D6 CCD2FE2D
1AB9AA07 CDEB74FE FB12C73B 3D67898F 3F33803F C0A81C1C C64312DF 05ECF8DE

G_2 = 56BA5901 0415F74E 81B6C97F 04645BF9 6A35F1B1 C97AB20B 80EF22D7 E5DE2639
F36408DE 6C54B4EB B2B6AA41 4F18F869 4E7BFCE1 EAD07953 D3CC123C D0F15C30
64A7FEA2 93A5E2C9 3643242E D87B8E24 A8A85B84 A7D8B33A D325D60C 8B017C3A
F618DD78 8B51A8D4 AAD001BF 06D760AD DFA2663B 4DB850E7 321662CE 8F6049BC

G_3 = 12C93D02 41469023 ED09FDCC D558AA55 16055238 07DCF856 0D33A12E 0987359B
36053658 DF870009 3E0FEE03 1CCA1D25 454D62B3 3E2F00C6 51209F8C 02CD5F91
0D7D5872 3B912DE9 F26C8535 8872E424 880089EA A73EF73C 98B72346 F0794B3B
6ADFD119 D5201751 7827BB0C 6430D6A8 5D80B05E D0B28058 C8A98BDA 7F733A5E

G_4 = 5DE7CCDC AAD76847 603D036A 08B5FF85 B1138616 5AB8C615 918F5193 8F85A03F
C7E08EB7 01C1C8C9 986E8018 80BCB6B4 725380C6 962B780B 90A2AD09 9105C87A
2EE04035 ACA54A4C 764F0534 90ACCED1 3409B81B 74AD6906 45800ADA 56626EB8
C288BFC8 9D6A950A C45887D3 612B271C 80A5D6BA 3EB71986 27CCCFBB 14B257BC

G_5 = 07F5EA50 3C9022AF B22701A6 2E649D06 008AFE93 8EA136D7 1AFD6FBC 90B8EF18
FA8FE507 CD81B4BD DEC57637 C2C24DEC BB22A71F D7FE9229 7C807EDB 5A53FC35
61E40492 A24C4C9B 583CCEC0 ED475CCD 1E533241 BA93BB5A 8B1FA011 7A75F777
07B824BB B93FF810 77481989 2D248603 53891E9F 1466258E 6F7D6F51 E2F285BC

G_6 = 4CB08F35 99AC2CAB DCFF28C7 BBB42166 3FED4CB8 ADCC5B6E 48805AF2 33254C81
709677D7 64710108 A4446CF6 A8749A4D 61A7DB69 DED3074B E7B5B3B6 10CA526C
8556C54B 5E5E4751 8477C889 0D9F39F8 06B0FAD2 00AAC774 F3872D82 14BB6E26
1AFD4DBF F21C6165 49046374 7FE1AA53 A4DAFF81 1DB510A7 5AD7BAC2 64F23DBC

G_7 = 06CC5160 0D68CE69 1630AB55 17A73EF3 D1D5A685 86B3519B 34AD1D8C 5DE5AA65
C07986E1 DE78F4B9 DB6D2FFD B99381E0 3B9FC118 E5A6BA2E 332D2DB3 904A0382
0EAE7D0C 6255E089 7B060CD8 52FF8758 C98FB46F C6ECE83E 67469EB5 62A4D44C
4029744A DC0B813A 50D8CBD1 CFE51490 FB0BB736 E69D8CD2 A3C02B4B 724DC9BC

G_8 = 0ED43F5B 6872EF9B B42FFD7C 90282C3E 7EA28C45 67ABA2D3 6DBCC16A 2A572AB7
596FA852 8FCB4324 D2BAB32D 8ECB5E8E 43CCFEA0 C3824AA1 EB8D0064 07B7F980
428CDF44 F8A4B00E DB74A5D6 E46ADB80 D5C699BF DCAED10F CC7F0233 F6A4E815
5359D003 7007600F 91082261 D0090802 AA0D06BB 800ADCF9 7BE287A3 4CB1C55E

کلیدهای خصوصی به‌صورت زیر هستند:

Q_1 = 1ED15C26 52F61C4C 37D4B558 C1DAB730 B248783C 6F7AF27E 55637614 A95CAF77
BEB2B52F 52B62791 446F8400 16100B21 2BCDF5A9 AFEF74FA 83188DD3 1032721B
8ACD3DD1 702C716F 38153298 20B66048 B828C0B8 3A2D15B5 D6D276B5 41B540AC
FD41FD5C 655C3A74 67B73DB9 94DBD0AD 30D4DB7E 51D64091 F859AD28 AC98E8AA

Q_2 = 009D94EA 30D5F13A 7E5917F9 21CCC91C DA18A2F8 CB368627 16E456F0 128AAECD
749394EE 79E0623B D4027C6B F4B51D3E D0DB8804 77CA7FA9 05180ED0 8B15CFDC
71756866 8642019A 10C11009 5917E043 808307B3 8D2E9BCA 41D89D21 B7125C15
E8AA839D 10B6D84C 03F31842 B174086D FE65E984 E2A924EB 1756C4CB FD49B342

Q_3 = 147C1279 C01B355F 6B295CF1 300D20D7 8381939B 1FE54B27 7356E748 A60CC211
FDAF8E92 38EC0C3C 0B13B47C 124F217B 220C5025 F5D5BC09 92A575A5 DDBE23F1
E060A199 4AE8875A 45C81CE0 B325B800 530A0433 569689FA 66CEA72D 5B42F099
BC5ED4F2 798C847D E00603DC 379619E5 28FE742E E334AFFE F8F9F433 A2B9E86B

Q_4 = 03B6941D 904B00AF 1614F88D DC3D5879 A4402420 48855251 98761996 7B3A681D
F8393CF4 9180C8E1 9C2B115F 31DE83AB 84741615 DE1CF7B1 C32BC0E5 838DCEC3
30CDF868 FB570D6C 022F8539 14FB078F 2C069A4D 7F2B6E67 25A74AB3 112CB146
4C5C12FD F51F296E 502C3399 86148FE7 69951D21 9AAEED23 6940F665 5E821794

Q_5 = 27BA1193 CA623C79 7CCF0560 184BDBEA 57DC069C 441E0B46 9B647419 87E5AA36
57619FAD B8F176E5 2D6A1D4F 26A0904D FCFF99D4 3453EB0A F3CEEA61 45B7C087
EEF9DC15 4B9933D3 98B0829E 77F8F55C 17F2EC82 0931E239 FB4D246C 84689D7D
A5614867 E66E0754 0A26818E B52A1F24 103CCF90 E87B7E50 0C36716A AA1F9EF6

Q_6 = 194DBD80 0BB6FF60 FA77CE90 E9BD233E CD99EDE7 042E414D E9EB4E22 0B4B0046
51C28CD0 78243340 87376670 5A8CB70B 6CB4A214 01B43D37 12A5CE3B A0B45B15
076D2A53 2C6B449C 1ACFADDD E6A92279 67D2519C 81351D1B 9E8C4286 DBB60650
20B5C202 8CF306E3 72138968 7C5B01B1 2137C0F7 5C02C696 0715BB3D E07F14BC

Q_7 = 07F513BA 8A0A3280 0AFC00AB 850BCFF8 FA532993 018A6608 4301BB69 FEAEC7FC
F7AE869A F9236F6D 152FCA38 CB97291C 2D2BE82A A760E978 273DF66F 6E57D012
20BE8C90 9AF83ABD A40347A3 7C6EC83C 6B1A40A6 24BE324F 1432EB7E 22897214
5C7370FC 59A2AB1F A7554C85 CCCAEF9D 5707F4B1 0DF2C349 2E10726B 5107C051

Q_8 = 2785555C C6FDCB2C 2CA944A1 4179F7C2 B2BBD59D 1903AB62 B7ED8AB8 A8D49589
F9A644AE B1A755E1 16CEDBC0 6931D163 31EB16DF EFCFA46B DE8AABA9 9BB994FF
B77AD756 7292B51B C08526B8 F32FCE66 F2D7D1BA 55F7850B 4DD6355A 9CB6C88D
17999B0B 01BDE24F C7461F58 08E4F9F3 F1567870 15322712 33B49F97 695A582E

ت-۱-۲ تبادل احراز هویت یک‌جانبه

به ازای $m =$ ۸، اندازه بیت برای چالش‌ها برابر است با $\delta =$ ۸. پارامتر تعدد تبادل $t =$ ۳ است.

تکرار ۱

مرحله ۱

r = 46730924 DDAE318D 6D1060BF BC5508A4 1E52C997 C3A752E1 0B511436 EF884689
60AB25AF D8A75D74 E4B0DADD 1F5A9AFB 26556C5F 9EA22A95 87BF849C 462738AA
D1C144E8 61293533 5914F5C5 2A8D2323 6716C336 A4E06AE3 3DDE5A34 DC8AA982
74498C4A 6F7F6E89 83D7A2BA D51BCAF1 4629891F 6113F7DE A08E4BF2 60EDAF55

W = 1ADED7E0 6F4DE303 1E04694E 7045363D 1D62A241 4925D5BD 6A54D352 43B1C9CE
A9ADC1BC 8968D4F7 034531F1 5C717E16 4F7F9F9F 779A439F A23EA1C2 7A831B93
439DB041 C6AEFE7E 031B2FA1 FB2390E8 89EAE68F 699D5D27 4505EAB7 95D1FFB9
BC7DC6CA 6C38BCBB 4651CECD 90778FA4 E91C9D65 42BFD336 108EFE8D 6AB8FA0B

مرحله ۳

$d_1, d_2, \ldots, d_8 = 0, 0, 0, 0, 1, 1, 0, 0$

مرحله ۵

D = 37D87F34 EA4CD0E2 A825E891 1EAC4F15 C7969E59 2C6741E9 A9142922 2817650E
21D13151 7D768A55 7AC7A8CA BE50D66B D0BA0A09 7338B3F0 A1CD1236 1B9F9945
951BD90C D9CB314A D3CC8F65 ACD232FA F7152A4B 68B97B7A 7C230A7C 8099E938
62A3435E AD1F4BA6 9A6C00C3 919B5342 45E0F06F 604D6112 C7EABE7C 3D2C6D39

تکرار ۲

مرحله ۱

r = 546E4A31 5718EA7E 00779BBA DB667B34 7DC1C1B4 992AD37C 2B687927 5283389F
B6AC25F9 55E5CB70 647EBCB4 0F9D86BF EABF7308 DB6F3B12 DBE1C73F AA5EDC9A
988F6DE8 BCE672D2 1CA00EED 53E76E72 15805F9D 52BF401C 8B6B28BA CA10FEF3
498118AB B89390E3 1A685343 4F99D136 EB3016E5 7C86FEAE 58A83068 033C508C

W = 3565606D 94F1FEEC A61DC570 D99193B8 01506F0F 8E1EFF0D 8A6F488E 2E1434CD
B3D91345 F3A5D51A ED1479BA 04D2DBCC 064AFF94 058D4E07 65E4327F 2C1EB0DE
13C6DA80 D47A6DB5 27BA686C 010A93BB 426CEAAA 6A73CF42 1F78572B 5CE999AF
9D170BDA B008F088 CD379265 6F013A98 290788E3 ABD9A171 FCC9E01A 3D304E49

مرحله ۳

$d_1, d_2, \ldots, d_8 = 1, 0, 0, 0, 1, 1, 0, 1$

مرحله ۵

D = 1FA64318 C842715B 5A1404E2 445767E4 55EB9344 6EC9F311 A770B965 F34047CB
A69F7D42 E95CC9F2 AE54716F B97B765B 7CE69B8B 05795C62 EBCF6A5D AA80323F
7E1880BB B7154F60 BB6F5E2A F064D759 41458EED 951BE96C BA9E1E0E F07ACD22
7B311649 8E98C7C1 EE6AFFF5 5887C1C7 37CCCADF 37DDBCAF 5B59555E FA1D35DF

تکرار ۳

مرحله ۱

r = 2D667AD3 3F6615A2 26647FB1 889EAE85 203792B8 68DFA869 2DA3B9AA 87B14D9E
52BF5637 0065BE27 775E37E0 9896FF8F 0FB8F162 ACD7599A 18F8893A 23386E0D
E22357B2 C1A455AE 1A809F8C 1B33A9DF CE8A4E48 2C7B2A1C A96F9F0C AC33EC1E
27FB4368 04264F76 E1B68C3C BF37CB99 A865B9E1 23E3AA7D AE73540E 5DB834FA

W = 41068CBD 2F2CCA28 95E935BB 3D3F228A 3D43B2F1 61B1DA7D A62EE180 B0B3D930
C87E1F5C 88F8CEA5 F6A81C5A A2A25689 AA7D2C50 505B8689 49F41FF4 A71377C8
81E01CC4 9CCA612E 0E43BD07 D5622238 7494A0A6 3CCD433D 5782636B AB7DBB36
394F3FB5 30FEF9DE FDC72B2C D1AE4179 6B6C7AFD 2AA114A2 966E7BAB 127A458E

مرحله ۳

$d_1, d_2, \ldots, d_8$ = 0, 0, 1, 0, 0, 0, 0, 0

مرحله ۵

D = 0FDD219F 57F5FCAB 2DAC9364 3EA429D7 ECEE6833 6BD1793B 0F72FBD0 8DA133F6
5F0B46A0 F9A1CE1E 79F4F103 F37B19D8 9FF68054 3DFBCF33 01A5CB00 234FEE71
7352006E 9555977D 1F724218 74E264B4 9179435E 4DF6CA94 48EE9529 15900FB9
D94D132E 833103A0 50A22A5B ACBA97FE 00D21B99 BC171CFB 06523911 B3835D20

ت-۲ سازوکار GQ2

ت-۲-۱ تولید کلید

ت-۲-۱-۱ جفت کلید نامتقارن (v یک عدد اول فرد است، طرح RSA)

برای هر عامل اول اندازه بیت ۵۱۲ و برای پیمانه $\alpha = ۱۰۲۴$ است. نمای درستی‌سنجی برابر است با $v = ۲^{۱۶}+۱$ (عدد اول = 65537 در مبنای دهدهی = 10001 در مبنای شانزده)؛ این عدد نه بر $p_1 - 1$ و نه بر $p_2 - 1$ بخش‌پذیر است.

p_1 = D716BEA5 9AC10B1C B5CFD57D 0204C349 52240F8E 9BDD319D 4F5ADD0C D9478B7E
AF96558F 85A74A20 B6664136 DD589F35 CFF94287 1B3298BE 40ED2C86 899186E9

p_2 = FBB4E01A A4BF2952 CE9BEDD7 0EEB1EC2 51CD63D1 0BD4332F 3A822FC4 4065FBC6
0197A2F7 0C969BCA 54BF79C6 6D9A2907 C06794F6 EF40CABB B45079DD 9BEBA6F9

n = D37B4534 B4B788AE 23E1E471 9A395BBF F8A98EDB DCB39923 06C513AA A95E9A33
5221998C 20CD1344 CA50C591 93B84437 FFC1E91E 5EBEF958 76158751 02A7E836
24DA4F72 CAF28D1D F4296523 46D6F203 E17C6528 8790F6F6 D9783521 6B49F593
2728A967 D6D36561 621FF38D FC185DFA 5A160962 E7C8E087 CE90897B 16EA4EA1

u = 18384CCC 9C9A4CE6 61B06616 EF1A5CD4 436C9AD2 7A081D14 8E7ACD55 ED240B1D
AFCD2E8E 4676EA1B 259F02C3 79831FD7 F87BEB20 79EA1DF9 283BEEB5 83CBFA4B
5CAEF744 597550EB F85AE3D0 4CFC6F9F 26E035F0 E317D21F F3A241C7 92132BEC
633560E2 C9B5A3E5 88104BE0 61535C3E E4EC7220 838B3E01 53277B9F C5EA5137

ت-۲-۱-۲ داده‌های شناسایی و جفت‌های نامتقارن اعداد

داده شناسایی شامل یک رشته بیت است که «Alex Ample» را نمایش می‌دهد.

Id = 416C 6578 2041 6D70 6C65

سازوکار قالب از SHA-1 استفاده می‌کند. SHA-1 سومین تابع درهم‌ساز مشخص شده در استاندارد ISO/IEC 10118-3[25] است.

G = 3E641A22 D0D0747D 4ACC7188 4D3DFF2B 2ADFDC17 03B5A74E FD8333AB 8C4377BB
2A9B48E7 07F73409 ABFBCD2D ED69F52B 16A145CE 062FE6BD 712C1952 110DFB23
16C5F3F3 21922ED3 75A4DEB8 C41FA79B CAD86B0E A0D8FF02 C9D0D591 1BFF1E87

DBCF073F 71F18C08 EB944AE8 4883A1E1 3FB1DEA1 23B5B1EF EA2A9263 5BD5D88F

Q = 24B9559A 80BD4D89 B9802A14 36DA3BDF 8DDF8DC3 993DEB1F A7EE0B4D B9F2EFFC
3003722C 9217CE8F BFEB962A 39B32DED F02C25CF 02702195 7A103024 15A7D59A
133A2B06 840B1DCA 10445287 FF875EAD DFEAFC8B 12B7C7E3 E05375C5 4D2369B7
9DFCEC0F 9235ADB3 16427D66 70D9422D 39C4F32B E1A406B5 E26736E1 F68E3682

ت-۲-۲ تبادل احراز هویت یک‌جانبه

به ازای $v = ۲^{۱۶}+۱$، طول بیت برای چالش‌ها برابر است با $\delta = ۱۶$.

مرحله ۱

r = 487CDB00 41BEED03 23FDD3DE C8542584 FA0E6CB9 90FAD587 8DB34E9B EDDC95B6
5D22790C 108E2184 07ED7F7D 686657BA B5A28EF8 1C2E2498 5B56E37D 9934E195
A38A835C C02CEE8E BA2F56C8 7663E332 976F5A37 20DACA12 0BCD3DF0 AEF6FD78
582EBFCE E6D05E06 172A871E AB0E8F5F C22DDB60 0F541B87 CF8E1473 58374406

W = 411F7E73 D995AC63 BACAE1F2 F1BF8D03 4886E36C 5825BC31 BDB761E8 567B6762
9947B41C 56A2EC07 8D02B880 76451F4F 991892D2 2F291949 F6F462B5 9098D627
F473111C FD260FFD 4428DD0C 3D270B82 F09E51C3 CF9065BD 744F708C 5D5C08B8
39336472 208415CC 72EBF75D 5A339134 C21E68AD 7AE057AB 8B25B776 CFCE18D1

مرحله ۳

d = D783

مرحله ۵

D = 3A2B6A07 3CAEEF40 1E1792E7 D67B5F76 CB7B900B 592B344E E7D8E641 FD78FA21
3DD31D25 FF772479 037A53E8 D82A357E 43D02FEA B768685F 03E4654B 46CC2610
B7710A9F A4E6DE30 24F65AE6 54BB445B ABEE957B AAB861EF CF74F05C E577F407
8DA447CC 387ECD96 A67B53E9 11D411F0 32782455 081F5AF0 AB7D6777 B3841E0C

ت-۳ سازوکار GQ2 (مثال اول: $b > ۱$)

ت-۳-۱ تولید کلید

برای هر عامل اول اندازه‌ی بیت ۵۱۲ و برای پیمانه $\alpha = ۱۰۲۴$ است.

p_1 = EBF36016 972BFE86 E5FA0D25 21E852A8 D8D28681 973F9439 9E06DA9B AFB5B9AA
2823FD4B 6788C807 5B9581B5 2E8343F8 AC469E00 37149F01 15404132 E99EDF91

p_2 = F5ACDA1A 3C03EB5D 211AB7D1 6BDC15D8 AA624EFB 1C5CAE72 78B39C6A 86811C74
B1FE14C8 5BC9B189 7D25C467 84551316 D90C92FF B0ED7312 400E0C54 87A5DDE5

Cr = 66516ED5 D013D71D E282A841 0EF960FA F7D7F41A 57B60742 92BD1146 4E508BD4
5747413F 8E92110A 958220B7 37555D9A C474DF74 00830563 89685EEB CF94C8E5

n = E26F3B7F 9BB6527A 98C545CC 3AACDE35 234D51B7 199F409A 102EBA25 88C9A15D
4B8937A5 BAD6A5BF 7CE79F28 C95973F4 315B2C13 78BA6783 CCCE8CFE 1A45CEEA
0129B046 9A6820D4 637A5BF3 25E80B82 AFB6F274 10F9D46C 7057066C 40AF0383
BD14EDE6 21DB0B27 EF03596E 6111DDD5 7373B2CA DCC8E18A EE50C918 B19329B5

یادوآوری – مجموعه اعداد بالا در زیربند ت-۸-۱ (RSA_{UA}) نیز استفاده می‌شود.

پارامتر امنیت برابر است با $k =$ ۸. به ازای $b_2 =$ ۲ و $b_1 =$ ۱، پارامتر سازگاری $b =$ ۴ است. در نتیجه نمای درستی‌سنجی برابر است با $v =$ ۲^{۱۲} = ۴۰۹۶.

u_1 = 03F315E6 C0CDCB85 B00F7C82 541E4C8A 35891E22 61511F72 2AE62B5E C523F1B8
9A260238 681EA921 278773A8 D164507E 449A3A9B 0EEC075D 5BA41057 632B19CC

u_2 = 0AB0F9AD CC449BAA 1984CDA7 D9159FE3 61CA2F37 E587F887 7348B0FA 92C27661
040EF29F 881E92FD DFB638C0 113E43C8 AA8A1015 A88F1555 F7519C81 5DB733DC

دو عدد پایه‌ای وجود دارند ($m =$ ۲) که عبارتند از: $g_1 =$ ۲ و $g_2 =$ ۳.

$Q_{1,1}$ = 82BBA646 0DE18D07 5DE2E587 21B39EB8 DE519421 6D708F55 AD6F4931 5C5B0855
CBC2998E EFD22770 C86C1D1E 5D86262B 993BA8C1 3B68F1C4 470AA1EC 423AC707

$Q_{1,2}$ = BE7E88FC A3C077CE 99470064 720AFBD1 85EE2F86 BE030D41 CD7963E2 3F6E8F60
AF6E27B9 DADBA151 6CF69B16 689B9B79 B6551C33 31EB9306 EE5A6941 C3510295

$Q_{2,1}$ = B14DE96C 2535745A A34B3383 1851EE0D 3FB2BE8E F35481C4 F70D2C83 9A764413
837CB60F 95C48BB7 9CDA14EB A6BCC2A0 E0534B98 EF31EF9F 2728BD4A 53BAA0AF

$Q_{2,2}$ = 1F63D720 C208381A 5018521A 7A94C3B4 C9391194 CB89A591 811985DE 8D577EA4
FCF1006A 6565450C 765FB060 BE850F6B 6591058A 2EEB4EF6 1E037196 A1F6865B

ت-۳-۲ تبادل احراز هویت یک‌جانبه

به ازای $k =$ ۸ و $m =$ ۲، طول بیت برای چالش‌ها $\alpha =$ ۱۶ است.

مرحله ۱

r_1= 958FE0FE 77561815 FCCE3499 D2AA78C6 701CB4DF 3EAEF982 160F9254 592C63ED
D4692A99 336020DA 4427AD2A 5845CFDD 0153CEB3 6507C76A 9473DAC1 A764E4C2

r_2= ED1F46C6 B0143F7F A70DC68C 0E8E4324 5F22CE6C BC811A7C E90D7B0C 0D828256
C479922A C1B1CD6E 52DD82F3 75B90D0C 9EA6FD45 34611F9C 2CE4EF1E DB7DB9B7

W= 202B4E86 A41BC533 50A20AB4 BAD183E4 1362321A 6EF33B89 162CA681 C993A94D
0F009CB3 4EFEBECB FB473A02 291888C8 A73D9B90 13D814BF AEFA104D 1B551E59
DFD8A626 C74F9F85 C047D5FF E580277D 14A13B84 537B421B 5E6F8F64 64334BA9
9092041F 9EADBAF1 3EA6246B 8A1E3275 31C41AE2 904FA368 BA980C56 356E4896

مرحله ۳

d = 948C، یعنیd_1=94، یعنی10010100و d_2=8C، یعنی10001100

مرحله ۵

D= 28FCBD3D 0BACC08E 614A7AB7 F4913472 D3CD8716 0961639A 94A06ED1 A5B3289F
1C635101 5ED72C6E C2B653F5 CB09E93C 88478733 FAABFF35 D2D05E35 A895EA37
6B5998EF 1E24B090 9A45E0E8 3BC01302 CBAD5D0F 26E21179 29B15DD2 E14F8EC5
18E201FF B03FFE05 9D53B5DA 5CAC04BC DE446981 E4995C3A 75E831BD 8D86D325

ت-۴ سازوکار GQ2 (مثال دوم: $b = ۲$)

ت-۴-۱ تولید کلید

برای هر عامل اول اندازه‌ی بیت ۵۱۲ و برای پیمانه $\alpha = ۱۰۲۴$ است. به ازای $b = ۱$، هر عامل اول با $3 \ mod \ 4$ متجانس هم‌نهشت است.

p_1= EBF36016 972BFE86 E5FA0D25 21E852A8 D8D28681 973F9439 9E06DA9B AFB5B9AA
2823FD4B 6788C807 5B9581B5 2E8343F8 AC469E00 37149F01 15404101 12ECF827

p_2= F5ACDA1A 3C03EB5D 211AB7D1 6BDC15D8 AA624EFB 1C5CAE72 78B39C6A 86811C74
B1FE14C8 5BC9B189 7D25C467 84551316 D90C92FF B0ED7312 400E0BA5 327E1DF3

Cr= D09B24CA 87A42315 E6EBA6BE E6AD15D3 A3F45344 5D5D0824 FDDCAAEE F2544B7F
89316E3B 9E532F26 C3723E00 C911A4C2 E4D03F6C ECE82FA3 B9929B16 4FFE0970

n= E26F3B7F 9BB6527A 98C545CC 3AACDE35 234D51B7 199F409A 102EBA25 88C9A15D
4B8937A5 BAD6A5BF 7CE79F28 C95973F4 315B2C13 78BA6783 CCCE8C2C AC4BB5A4
FC439166 CAE4EE3B 4C8C9A58 CC18654A 87E1DD6E 2223DF5B D728EDA2 DB46D042
25E3DB20 0BF6F035 8ACA6C79 61D12407 A768CF6F B3824000 5B1C0A66 903DF805

پارامتر امنیت برابر است با $k = ۸$. به ازای $b_1 = b_2 = ۱$، پارامتر سازگاری $b = ۱$. در نتیجه نمای درستی‌سنجی برابر است با $v = ۲^{۹} = ۵۱۲$.

u_1= 0638AAC8 987C68F6 0E9057D8 BAA4E02D F3B78D0B EABCED28 84EAAE43 9AE20AA5
3C8EF2ED BCFADB46 31AA312B 86F9F60A CE8ADCAA 8173CB31 474F71B6 C73FBF8B

u_2= 4EEEC912 EDC8425E ABE2D58F 08E77604 DCBE15E0 2DDCC70C 4747B501 39B6FB64
7E2FE22D 5F7D8D4A 6C75625A 42445562 173C4A3A A6984A38 9D14833D D379051F

دو عدد پایه‌ای وجود دارند ($m = ۲$) که عبارتند از: $g_1 = ۲$ و$g_2 = ۳$.

$Q_{1,1}$= DEFF24F3 D063F874 51C7A580 FAEB9C6E 44C9A3E9 2819B83D A90A40EF C598853A
4FE073F4 BC348AA0 99EB45AF D7799C55 D28B01CE F74AA99C 4F64333F 0D92E928

$Q_{1,2}$= 75801C91 DA2595A8 C790692B E5406F07 0DC6902B 431EF20D D464FBAC 4E11F8F8
21D5A934 DBAD2E4A D9A3F4E1 2CB5E0EC 0A5DD49E 04BD19DB E1838D23 F37DD3DF

$Q_{2,1}$= 8DF2CC77 8B17D817 D02B9CC8 9802D8F1 04DC12C8 8089A937 3B82D665 EE3B8E14
6C964F32 41B43A20 3DBFC264 1E1F45FE 2172A0DE 2EA8875F 8EC5A514 89472CA4

$Q_{2,2}$= 31B059C5 56422DEE 1CEDBE9E 9A5B82C0 26DC8586 47F8ECF7 FA3032B9 28389B33
1A9825CF CC280CC1 8B671507 4F2EE897 0F8C692C 6E62796F 369DA6A7 A0188A85

ت-۴-۲ تبادل احراز هویت یک‌جانبه

به ازای $k =$ ۸ و $m =$ ۲، طول بیت برای چالش‌ها ۱۶ است.

مرحله ۱

r_1= 958FE0FE 77561815 FCCE3499 D2AA78C6 701CB4DF 3EAEF982 160F9254 592C63ED
D4692A99 336020DA 4427AD2A 5845CFDD 0153CEB3 6507C76A 9473DAC1 A764E4C2

r_2= ED1F46C6 B0143F7F A70DC68C 0E8E4324 5F22CE6C BC811A7C E90D7B0C 0D828256
C479922A C1B1CD6E 52DD82F3 75B90D0C 9EA6FD45 34611F9C 2CE4EF1E DB7DB9B7

W= 3B9C8250 E07F13D6 4A8E8F5D 8315B2F2 3368300D 54B7EC4D 66F5948C 96DE6AF9
8C2C6F7D 05F3B3D4 9E9255A2 339C2E9D 29A04F68 B007D234 483B14EA 8BF6F6FC
0FCC96C7 DFAEE6EE FC718DF8 228526F5 D8575717 EA9D726E DE91310D 2E372838
7B533EF3 667AD83F 910F153C 5CD69D89 90A3F5F2 2C532C48 F6C3D682 7C755B49

مرحله ۳

d = 948C، یعنی d_1=94، یعنی10010100 و d_2=8C، یعنی10001100

مرحله ۵

D= D94EC0C1 8D456808 2BCC6F3B B0DED48F 24466A98 4F6F90B9 9C54763F DC1774E9
56F8EDF2 F68825D1 19A2B442 5F310582 CDA7EAEE 6D782E7C 9D45711C D67509E4
46651E15 22D61A16 564EF2B8 DA46A1E7 88FF64BD ACC31045 FE98DDE9 2F56AD5B
68F56F4B 3286A34E 26ED710D 1142408C E67C4578 29C3A9DF D8F72CA1 379385AD

ت-۵ سازوکار SC

ت-۵-۱ تولید کلید

برای پیمانه p (یک عدد اول) اندازه‌ی بیت برابر است با ۱۰۲۴= α و برای عدد اول q برابر ۱۶۰ است. (یک عامل اول p-1 که به‌گونه‌ای انتخاب شده است که رونوشت q درون p تعبیه می‌شود.)

q= CB0EBC3A CCB15C36 896F67F0 703E7C69 AFC4C24B

p = EA9B8F92 26D7B2F6 729122EF 53CE81E2 567ACF40 A7DB660E BA5E4DAF CB0EBC3A
CCB15C36 896F67F0 703E7C69 AFC4C24B 221A8968 5CDCFB3E 086D8F95 702CBFC5
8E4170A2 E10DF7B5 2BF8F015 C5A689CA 48DF291B E796C443 F5E7AD19 8C159F0A
BA9D962E 60D34840 77B5993E 48BBC3ED FEF5F54C ACCDE46E 69A3F1F6 1AE08AF9

g = 26324F69 934E6733 C66367A5 AF5A08D8 455A5125 29882857 B20083E8 F72420A9
1F16A377 6DC612FF E652A2DD 05D51441 5F52C591 E8AA3127 8309CE2B CA9E5B73
5E8CC526 0DC1608D 91F32A8D 31265ADC F2F2FF5F A4A786EF 25086BDB 061355CD
96EA33F6 429AEF56 BC0C0ABA DB1EC3E0 B1140687 D60678C6 205C7F6D 6A236F87

Q= 87146299 068B4B13 017364B7 E7DDA29E CDA5547E

G= 819B36E6 62DDC4AF 146DCF3A F888D61B 560EA5EA 8BB368F7 0E822E95 EF5E45C6
68B98732 725D29DC 21BF1394 29D95DE2 98A6D595 9A7188C3 AB4B5D6D 20CA1D9E
D6BC4D7A D23A4E3B 48CBE4AC DA28D927 922C85FF DB7E1F59 71A17DD5 DC68725C
32CF50F0 BE5D8A73 F93BF113 1C55BF51 35B314BE 5067FD31 9867041D 4C96E5CF

ت-۵-۲ تبادل احراز هویت یک‌جانبه

طول بیت برای تمامی چالش‌ها برابر ۴۰= δ است.

مرحله ۱

r = 87146299 068B4B13 017364B7 E7DDA29E CDA5547A

W= 397AD6F9 B435B01B 4C43A2D1 008DDADE 1A086C2F 0EA25134 FF5A8653 A374DFBF
47F1A543 FBB58232 0357CCE1 33AEB861 6AEBD4B7 65DEA271 0DFF3A09 7C40602B
7E719499 0E9C7717 0CE73286 930E9E27 F8053B28 D2C80FD2 EC529839 27F34F46
BB9842B0 BD9C6405 1B2C58D8 C5CDCC50 69C4A430 D0F93CD0 6F2F75F3 298684F6

مرحله ۳

d = A2 CDA554A6

مرحله ۵

D= 354BF25C 5F0E8CCA F2AEA2B9 7716A2D5 CB8CEB7E

ت-۶ سازوکار GPS1

اندازه بیت برای پیمانه برابر ۱۰۲۴= α و برای کلید خصوصی (۱۶۰= σ) برابر ۱۶۰ است. پایه لگاریتم برابر است با ۲= g.

p_1= D716BEA5 9AC10B1C B5CFD57D 0204C349 52240F8E 9BDD319D 4F5ADD0C D9478B7E
AF96558F 85A74A20 B6664136 DD589F35 CFF94287 1B3298BE 40ED2C86 899186E9

p_2= FBB4E01A A4BF2952 CE9BEDD7 0EEB1EC2 51CD63D1 0BD4332F 3A822FC4 4065FBC6
0197A2F7 0C969BCA 54BF79C6 6D9A2907 C06794F6 EF40CABB B45079DD 9BEBA6F9

n= D37B4534 B4B788AE 23E1E471 9A395BBF F8A98EDB DCB39923 06C513AA A95E9A33
5221998C 20CD1344 CA50C591 93B84437 FFC1E91E 5EBEF958 76158751 02A7E836
24DA4F72 CAF28D1D F4296523 46D6F203 E17C6528 8790F6F6 D9783521 6B49F593
2728A967 D6D36561 621FF38D FC185DFA 5A160962 E7C8E087 CE90897B 16EA4EA1

Q= 8944FE65 F644C82D 2F60D423 AD3B3C21 AE3013BA

G= 84475410 6462493C D64828E4 91D70FCC 687A0A09 C7CEF778 B968DF15 4BF34A03
388D3D74 D6931CB3 072E4D6B 21D343BE 995FB060 6114BB9E A6C0E32C 54EDD73F
92F1129B 8C4BEE86 3CFAC094 83ACFEA1 81083C9B 624E9A50 7D2778E4 B651ED85
34F1730C 2A52E5D2 345C9E09 49CE84C2 A08C2A22 6FA73ABF 92EE3CA0 FEE2A7AA

ت-۶-۲ تبادل احراز هویت

اندازه بیت برای چالش‌ها برابر ۴۰= δ است و در نتیجه ۲۴۰ = ۴۰ +۸۰+ ۱۶۰ = σ برای تمام رشته‌های جدید بیت‌های تصادفی.

مرحله ۱

r = FBE252 8A24B873 01E132D0 346C29E8 8552F568 DC6FA49A 44232FF4 05F0DC65
318FFFF9

W= 7D0081A7 5C9BF2FC 78679919 EB94A740 2573FC8B 06BD1944 3FD54077 398F5252
0F3D0107 32AB7537 456354A3 97A8AAE1 011C5EF3 9B722369 3C2AF56F B7B8EFD1
5186FD48 10435B62 30765083 1AFA4782 6B57A2FA D2299D1A 79D64B3F 32730174
EFFB5F45 D33BD8CC E56EB4AB 6B223728 0F3E4069 043F9CAF 93C71632 CDFE23B5

مرحله ۳

d = C0 6AF0CD17

مرحله ۵

D= FBE252 8A24B873 01E13269 0755AD72 8542F6C8 BF5BDC3A E4F58756 10B57C24
89124843

ت-۷ سازوکار GPS2

ت-۷-۱ تولید کلید

اندازه بیت برای هر عدد اول ۵۱۲ است و برای هر پیمانه ۱۰۲۴= α. نمای درستی‌سنجی برابر است با ۱+2^{16}= v (یک عدد اول). کلید خصوصی، نمای امضای RSA است. کلید عمومی برابر است با ۲= G.

p_1= AD521B6A B4DF5E3F F9C3614B 7083CE55 DFA50D94 3F1260C5 82C72270 1A164BC2
F3B8952D 2D5442B4 497D27DB 235533F4 8751CC88 B9D7C534 BB9F2CEF B5C68125

p_2= EB4369AD 61C9161B 8DAF355F 8CDAC18D 41288DB0 8798E949 AE6D2B89 BD52ACEB
D2E0E873 2685DB36 DCADFF53 65EEA0A6 FE44C5C6 D03965AC 346F5C69 FB2E94ED

n = 9F480334 30E5EE18 E8E13560 5A91A61E 4DCC54EC C9E4F8D5 460F1828 A220DE18
4A0AD8BD E132CFC3 473A7528 9EDCDA3D 475FE45C 437DF74E A16B79F6 4F7CB0F9
E10ED6B9 30D89B76 DE10AB56 C683D315 DBC0061A BD4DBE88 A19ED2FC A442D792
296C3BF1 8BBD2FBD 40D4E085 222126DF 5994BFDC 870DEAC1 3A82BD79 8714F341

Q= 063B1F32 F6B9BBF1 7A04BB5D 905573C9 EA31B4DD C97D1D55 DC868123 AFC9F8DE
3AE1473E D0553846 F39DA011 2D7BC6C6 D068BA2A 78D26FEF 01C60E50 9A25EED7
5BA07156 CBCB37F0 6C184587 3DD86913 4E386701 0543B02A 43014BC0 430ABFDB
25D5C82F ADAFC295 F5488FF1 490C1968 815DC762 E54FAEE2 E38EBDAE 44265D75

ت-۷-۲ تبادل احراز هویت

اندازه‌ی بیت برای چالش‌ها برابر $\delta = ۱۶$ است و در نتیجه $\sigma = ۱۰۲۴ + ۸۰ + ۱۶ = ۱۱۲۰$ برای رشته‌های جدید بیت‌های تصادفی است.

مرحله ۱

```
r =  13FB6725 909D85BD 36810665 3E3A45E9 1163523C 33897DD8 56DE0E74 5628E712
     5B7FF356 BE8B1138 750C7A66 47F892C4 D6789B19 A72D10DE 324C43A4 F8F63439
     DD40A3B3 897F69C3 28747B9F AFB8D4FE 8B7AE2D2 5827ECD7 0EC2A9E0 F2C5D7EB
     AE705661 3B2157E9 CAD1FD5B E80504C3 66239446 BDC0055C 11A98907 555B4FE8
     183027AA 20B48E86 CF27645B

W=   9A66D066 D2A97254 6B57AA77 7EDC33A7 0D35312C 8B3F0A89 955131DB C29408EE
     1C4416DB 17C69105 82325953 C89B1DD8 310D7351 A4487E02 FA870E59 FCA7E71A
     639891B2 04EF8373 E901B7F8 0FB40C32 840574EF 09FAECF2 A947DA82 C53BAA14
     6FDFA3E8 824D15BD E5110456 7400464A 4E34F1FF B42878A2 D0236491 94ABBB9F
```

مرحله ۳

d = 6B26

مرحله ۵

```
D=   13FB6725 909D85BD 368103C9 9B695738 D0437E64 1C8592A1 32C97998 CC2F5AEF
     27AAB56B CA99FB72 F20CA6CD 61C0BE5E 4B4C98BE 9BE0204E B5D7A906 439AD16B
     F93B207B 7E1D995E 6BFF045C 0688BAEE 5AEF17F4 277E13EA 6CB7FF51 C3592091
     9BC28619 BE46BD5A 5908EA03 EF9D6017 27B8047F 00D0CE03 2B3F1571 EF196161
     C0435CDF B03C902C A8659DFD
```

ت-۸ سازوکار $\mathbf{RSA_{UA}}$

ت-۸-۱ تولید کلید

این مثال از عامل‌های اول (۵۱۲ بیت) و پیمانه ($\alpha = ۱۰۲۴$) ت-۳-۱، GQ2 استفاده می‌کند.

```
p1=  EBF36016 972BFE86 E5FA0D25 21E852A8 D8D28681 973F9439 9E06DA9B AFB5B9AA
     2823FD4B 6788C807 5B9581B5 2E8343F8 AC469E00 37149F01 15404132 E99EDF91

p2=  F5ACDA1A 3C03EB5D 211AB7D1 6BDC15D8 AA624EFB 1C5CAE72 78B39C6A 86811C74
     B1FE14C8 5BC9B189 7D25C467 84551316 D90C92FF B0ED7312 400E0C54 87A5DDE5

n =  E26F3B7F 9BB6527A 98C545CC 3AACDE35 234D51B7 199F409A 102EBA25 88C9A15D
     4B8937A5 BAD6A5BF 7CE79F28 C95973F4 315B2C13 78BA6783 CCCE8CFE 1A45CEEA
     0129B046 9A6820D4 637A5BF3 25E80B82 AFB6F274 10F9D46C 7057066C 40AF0383
     BD14EDE6 21DB0B27 EF03596E 6111DDD5 7373B2CA DCC8E18A EE50C918 B19329B5
```

نمای عمومی برابر است با $v = ۲^{۱۶} + ۱$ (یک عدد اول = ۶۵۵۳۷ در مبنای دهدهی = 10001 در مبنای شانزده)؛ این عدد نه بر $p_1 - 1$ و نه بر $p_2 - 1$ بخش‌پذیر است. عملیات عمومی «رساندن یک عدد صحیح مثبت کوچکتر از n به توان vام پیمانه n» است.

x = 34DD74D5 EE600302 21EC3EC7 3774B81D 4E5C6525 5B3B49CD 1E55967A A064B8C2
8C19E16E D53FFB6B 09499768 6197FBA1 29ABC84E D47B2AA3 441BFE21 6E37599E
EA8C0090 85964B87 52FF19E0 E7D13C23 90456167 643A2E06 EB3508EA B12B8D27
966FCE60 1F5781AC 3554C703 E52A039B EEE45281 34A43CF8 467624AC CD077231

ت-۸-۲ تبادل احراز هویت یک‌جانبه

طول بیت برای رشته‌های جدید بیت‌های تصادفی برابر است با ۳۸۴= σ. این مثال از SHA-1 استفاده می‌کند. SHA-1 سومین تابع درهم‌ساز مشخص شده در استاندارد ISO/IEC 10118-3[25] است.

مرحله ۱

r = EBAA9CF6 EA04B882 D312697E DC65E40E 845C85AE 0318F8CE 75A5B650 37488370
3E85216F 69C614DD CEF89D68 22BE09BE

H= FE4D80CD 009AFD8A 7A40B1EE D1CFC0D1 0D29E74E

d = 70C81D29 7A526847 26F67D41 A6EE4384 C8383E9A A1D5F30D FF2A0C20 82D5C335
424C37EA F2729019 91E88A87 0A3D89CC F51B15D0 84435C76 1C609D50 411DB058
83769C2B 542640AA C5EAE64B ACECC70F 4466C331 D52BAD21 C48BA126 A35B06F4
AE0D9B35 8CFB2167 8EEF8FD2 52CBE352 B0057E17 47AEB0B3 B5F3FAEA 49FC2FD0

مرحله ۳

$S_A(d)$= EBAA9CF6 EA04B882 D312697E DC65E40E 845C85AE 0318F8CE 75A5B650 37488370
3E85216F 69C614DD CEF89D68 22BE09BE FE4D80CD 009AFD8A 7A40B1EE D1CFC0D1
0D29E74E

ت-۹ سازوکار RSA_{MA}

ت-۹-۱ تولید کلید

این مثال از دو جایگشت RSA با ۱۰۲۴= α برای اندازه‌ی بیت پیمانه و نمای عمومی ۱ + $۲^{۱۶}$= v استفاده می‌کند (یک عدد اول = ۶۵۵۳۷ در مبنای دهدهی = 10001 در مبنای شانزده). عملیات عمومی «رساندن یک عدد صحیح مثبت کوچکتر از n به توان vام پیمانه n» است.

برای هستار A، Id(A) = AAAAAAAA

p_1= D8E1FC6B 5EF57E8A DFDFE1AA 16D166F7 31698158 A0A52504 ACA04E3D 1F6B12DA
387ABA0B ADAD8662 34BC6ED5 04E0611D C54F58EB BC173BCF 55D63165 F597BADF

p_2= DCAA6C35 3285EE3A 1DBCCB2D 3EE4BC7D BA57C624 6426286B 63E07012 A1C13787
9AC8C1FF 627C1C84 CC51A3C5 D83FBDCC FA226AE0 D6C20CDE 6648F8D6 6D03B437

n(A)= BAF296AA 4CFC3098 0C37B059 8106F940 81CDEA52 B1665F9F BC44B290 D406AEFE
AA24B26E CCFCAB59 34319D1B E35D55CC 38A58455 7A48BA48 F6CDEF59 0A4EE069
D2C7F3FA 9CE0326D 7F85AD00 43107F12 DA10E0FD 8E202E61 5C2FA31E C3D2FC16
A5797159 420AFC11 7AB315A1 0265383E 38ADB448 9CC9F01A BC1A0758 969AF1E9

x = 01264ABC E35A4DA6 31B509F5 92F08B09 D58281A5 5E87E5A0 A2D4BD50 5CAD69D8
110DC6B7 1DB5940C 296100B9 522D99C0 76BCB5D2 9CBCE3C0 5D1C2913 A0179A13
A9D25AEA 03D5EBCD 3C774553 FB19AA24 8F7997D5 0D83231A F8BF2B93 064E261B
998B5165 D8B2AD0C B0D0CDF2 F4B9B70D 275AB200 E142C494 CC022BE7 E77DF3BD

برای هستار B، Id(B) = BBBBBBBB

p_1= AA9F65CF 91FD9997 7D2418A5 AA55F70A 7FFDD510 E8DDE122 B3CB0AA7 8C01F282
0628765A EED2E80D DFF97743 8B545205 6BB2F02A D54EA275 64CA89DE 693C1175

p_2= F1C58E34 3F040078 4B9FBE72 8E2B1A77 39D404D3 837F6BF8 27A52E5E 75E5897D
3DFCDE58 7A181452 69587E45 EC4D5D43 72F9F062 EFAB684E E7D90E83 6ECB4839

n(B)= A123BA48 FE04CBBE FA6216FC 2DDF3FAB FBFD5ACE C374C025 C5856D3B 2E214269
F8C2787A B571BDD4 EB3E6CD0 6F37A4DC B67DB9BA 2B41ADC2 97A2C208 F8EE4BFF
B1B074C1 D42D072D 4C73E6DD A279FDBF 13E2B93C 8E3CD8E6 48F85231 FBF9AEDC
FE9FB915 B8926C8C EC3F7040 5D9B27C1 A7484F17 71D01C37 CE52D71F 710FCB0D

x = 03172D47 ED0218A3 B04E2ECF C5E0DB6A 04DF4A56 EBF60F54 6086FE8A E0614505
C531C7A6 11A583F8 4D00EFF3 6FA76FCE 47AF8B52 51B5F804 EFC57D36 B723ECE3
4B802990 CE9674AE F22E62B9 73386B87 E84DDCD6 BFBCC46A 44DB93BA D0BEAC82
93AAF92C 3554CA3B D4EDEFC8 EFBD211A 21F0D739 25419F9C 2945D5B9 44E4DDE9

ت-۹-۲ تبادل احراز هویت دوجانبه

طول بیت برای رشته‌های جدید بیت‌های تصادفی برابر است با ۳۸۴= σ. این مثال از SHA-1 استفاده می‌کند. SHA-1 سومین تابع درهم‌ساز مشخص شده در استاندارد ISO/IEC 10118-3[25] است.

Id(B) = BBBBBBBB

r_B= A7AD8272 F85FD5C1 4CEF982A 64347689 632DFE86 4C15BAAA D5A80CE3 877CF197
41210E0B 00254C8E D091CF32 8E8A247C

H_B= 9E640DAC 9550C381 9E9BD0CA 22BF28A8 B9BCA67A

d_B= 0C6687CB C627C016 DCAEE1A9 B0FEA668 C61374AD 4B3940D6 6398FD90 D60AFA93
8F76F1C7 C82C36E3 03AFD19E 9665E6DD 83365FFA B79A02AD 0542B679 DE40495D
0ABFCF0F 38C7F1FF FA7EFD24 FED36FD2 852FE56F F3B7AA9F 344A2EF9 17F3EAF5
3EF4B9F3 FE7B84A9 62C4F848 2FF94565 CC49B4BF 9C554A1F BBF3A2D0 CD0F5304

مرحله ۳

$S_B(d_B)$= BBBBBBBB A7AD8272 F85FD5C1 4CEF982A 64347689 632DFE86 4C15BAAA D5A80CE3
877CF197 41210E0B 00254C8E D091CF32 8E8A247C 9E640DAC 9550C381 9E9BD0CA
22BF28A8 B9BCA67A

Id(A) =AAAAAAAA

r_B^*= A7AD8272 F85FD5C1 4CEF982A 64347689 632DFE86 4C15BAAA D5A80CE3 877CF197
41210E0B 00254C8E D091CF32 8E8A247C

r_A= A8F3D122 572A6C62 FB4E531B 13E00D9A BD5FDE87 4B214BF0 C8357B48 FD26BE12
72B37C25 F461465F 13FEF403 1131639A

H_A= 4B1F473A 25AF669A 442EA348 A481F897 3A96DBEE

d_A= 9E8611FF 140D9410 883F38EB E5259D90 EB49002F BA7572D6 1A634795 EB66FCCE
11217F50 07B5A3D2 5E907509 2F768958 71699359 4C7004B7 22E769BC F4BB27A9
9A07419C 905B9AD3 04356698 5C63E8AE 908BA029 B6D27028 2CBA24C2 D270D369
60C284A8 961431AC 955E86E1 D6A32820 441A082B E48BD96B 7C9E59F2 D7758090

مرحله ۵

$S_B(d_A)$= AAAAAAAA A7AD8272 F85FD5C1 4CEF982A 64347689 632DFE86 4C15BAAA D5A80CE3
877CF197 41210E0B 00254C8E D091CF32 8E8A247C A8F3D122 572A6C62 FB4E531B
13E00D9A BD5FDE87 4B214BF0 C8357B48 FD26BE12 72B37C25 F461465F 13FEF403
1131639A 4B1F473A 25AF669A 442EA348 A481F897 3A96DBEE

کتاب‌نامه

[1] M. Bellare and P. Rogaway, The exact security of digital signatures: How to sign with RSA and Rabin, in Proc. Eurocrypt '96, U. Maurer, Ed., Lecture Notes in Computer Science, Vol. 1070, Advances in Cryptology, pp 399-416, Berlin, Springer-Verlag, 1996

[2] J. Brandt, I. Damgård, P. Landrock and T. Pedersen, Zero-knowledge authentication scheme with secret key exchange, in Proc. Crypto '88, S. Goldwasser, Ed., Lecture Notes in Computer Science, Vol. 403, Advances in Cryptology, pp 583-588, Berlin, Springer-Verlag, 1990

[3] U. Feige, A. Fiat and A. Shamir, Zero knowledge proofs of identity, in Journal of Cryptology, Vol. 1, pp 77-94, 1988

[4] Fiat and A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in Proc. Crypto '86, A.M. Odlyzko, Ed., Lecture Notes in Computer Science, Vol. 263, Advances in Cryptology, pp 186-194, Berlin, Springer-Verlag, 1987

[5] M. Girault, Self-Certified Public Keys, in Proc. Eurocrypt '91, D.W. Davies, Ed., Lecture Notes in Computer Science, Vol. 547, Advances in Cryptology, pp 490-497, Berlin, Springer-Verlag, 1992

[6] M. Girault, L. Juniot, and M.J.B. Robshaw. The feasibility of on-the-tag public key cryptography. In RFIDSEC 2007, 11-13 July 2007

[7] M. Girault and D. Lefranc. Public key authentication with one (online) single addition. In CHES'04, pages 413-427, 2004

[8] M. Girault and J.C. Paillès, On-line / off-line RSA-like, Workshop on Cryptography and Coding 2003

[9] M. Girault, G. Poupard, and J. Stern. On the fly authentication and signature schemes based on groups of unknown order. J. Cryptology, 19(4):463-487, 2006

[10] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive proof systems, in SIAM Journal on Computing, Vol. 18, pp 186-208, 1989

[11] L.C. Guillou and J.-J. Quisquater, A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, in Proc. Eurocrypt '88, C.G. Günther, Ed., Lecture Notes in Computer Science, Vol. 330, Advances in Cryptology, pp 123-128, Berlin, Springer-Verlag, 1988

[12] L.C. Guillou, M. Ugon and J.-J. Quisquater, Cryptographic authentication protocols for smart cards, in Computer Networks Magazine, Vol. 36, pp 437-451, North Holland Elsevier Publishing, July 2001

[13] D.E. Knuth, the Art of Computer Programming, Vol. 2. Addison-Wesley, 3rd edition, 1997

[14] K. Lenstra and E. R. Verheul, Selecting cryptographic key sizes, in Journal of Cryptology, Vol. 14-4, pp 255-293, 2001.

[15] C.H. Lim and P.J. Lee, A key recovery attack on discrete log based schemes using a prime order subgroup, in Proc. Crypto '97, B. Kaliski, Ed., Lecture Notes in Computer Science, Vol. 1294, Advances in Cryptology, pp 249-263, Berlin, Springer-Verlag, 1997

[16] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Handbook of Applied Cryptography, Boca Raton, CRC Press, 1997

[17] C.J. Mitchell and C.Y. Yeun, Fixing a problem in the Helsinki protocol, in ACM Operating Systems Review, Vol. 32-4, pp. 21-24, October 1998

[18] M. Odlyzko, The future of integer factorization, in Cryptobytes, Vol. 1-2, pp 5-12, Summer 1995

[19] G. Poupard and J. Stern, Security Analysis of a practical "on the fly" Authentication and Signature Generation, in Proc. Eurocrypt '98, K. Nyberg, Ed., Lecture Notes in Computer Science, Vol. 1403, Advances in Cryptology, pp 422-436, Berlin, Springer-Verlag, 1998

[20] J.-J., M., M. and M. Quisquater, L.C., M.-A., G., A., G. and S. Guillou, with the help of T. Berson, How to explain zero-knowledge protocols to your children, in Proc. Crypto '89, G. Brassard, Ed., Lecture Notes in Computer Science, Vol. 435, Advances in Cryptology, pp 628-631, Berlin, Springer Verlag, 1990

[21] C.P. Schnorr, Efficient identification and signatures for smart cards, in Proc. Crypto '89, G. Brassard, Ed., Lecture Notes in Computer Science, Vol. 435, Advances in Cryptology, pp 239-252, Berlin, Springer Verlag, 1990

[22] R. Silverman, A cost-based security analysis of symmetric and asymmetric key lengths, RSA Labs Bulletin, Vol. 13, April 2000 (revised November 2001)

[23] ISO/IEC 8825-1:2002, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[24] ISO/IEC 9798-1:1997, Information technology — Security techniques — Entity authentication — Part 1: General

[25] ISO/IEC 10118-3:2004, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions

[۲۶] استاندارد ملی ۳-۱۰۸۲۲: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی- مدیریت کلید- قسمت ۳: ساز و کارهای مبتنی بر فنون نامتقارن

[27] ISO/IEC 14888-2, Information technology — Security techniques — Digital signature with appendix — Part 2: Integer factorization based mechanisms

[۲۸] استاندارد ملی ۱-۱۵۹۴۶: سال ۱۳۸۸، فناوری اطلاعات- فنون امنیتی- فنون رمزنگاری مبتنی بر خم های بیضوی- قسمت اول: کلیات

[۲۹] استاندارد ملی ۱۰۸۲۳: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی – تولید اعداد اول

[30] ISO/IEC 18033-1:2005, Information technology — Security techniques — Encryption algorithms — Part 1: General

[31] ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers