INSO
19267-4
1st.Edition
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۹۲۶۷-۴
چاپ اول
۱۳۹۳

فناوری اطلاعات - فنون امنیتی - رمزنگاری سبک - قسمت ۴ : سازوکارهای استفاده از فنون نامتقارن

nformation technology — Security techniques — Lightweight cryptography
Part 4: Mechanisms using asymmetric techniques

ICS:35.040

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات سازمان 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 یکصدو پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی ایران تغییر و طی نامه شماره ۳۵۸۳۸/ ۲۰۶ جهت اجرا ابلاغ شده است.

تدوین استاندارد در حوزه های مختلف در کمیسیون‌های 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 سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود. بدین ترتیب، استانداردهایی ملی تلقی می شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استانداردایران 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 کشو ر و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند 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 سا زمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها 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 Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrologie Legale)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - فنون امنیتی - رمزنگاری سبک –

قسمت ۴ : سازوکارهای استفاده از فنون نامتقارن»

رئیس:	**سمت و/ یا نمایندگی**
قسمتی، سیمین (کارشناس ارشد مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
دبیر:	
سروری، شبنم (کارشناس مهندسی کامپیوتر)	کارشناس شرکت گیتی گستران روشن تدبیر
اعضاء: (اسامی به ترتیب حروف الفبا)	
تفسیری، حامد (کارشناس مهندسی کامپیوتر)	کارشناس اداره کل استاندارد استان آذربایجان‌شرقی
جلالی، امیرحسین (کارشناس ارشد مهندسی کامپیوتر)	هیئت علمی دانشگاه آزاد اسلامی واحد تبریز
خاکپور، علی (کارشناس مهندسی کامپیوتر)	کارشناس شرکت دیتا سیستم
کوشنده، علی (کارشناس ارشد مهندسی کامپیوتر)	کارشناس شرکت پگاسوس
میکائیلی، هادی (کارشناس ارشد مهندسی کامپیوتر)	هیئت علمی دانشگاه آزاد اسلامی واحد شبستر

اعضاء: (اسامی به ترتیب حروف الفبا)

نوری‌زاده، سعید

(کارشناس ارشد مهندسی کامپیوتر)

هیئت علمی دانشگاه آزاد اسلامی واحد شبستر

فهرست مندرجات

پیش گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی - رمزنگاری سبک - قسمت ۴ : سازوکارهای استفاده از فنون نامتقارن» که پیش نویس آن در کمیسیون‌های مربوط توسط شرکت گیتی گستران روشن تدبیر تهیه و تدوین شده است و در سیصدو شصت و سومین اجلاسیه کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۲/۰۴ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه 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 تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 29192-4: 2013, Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques

فناوری اطلاعات - فنون امنیتی - رمزنگاری سبک –
قسمت ۴ : سازوکارهای استفاده ازفنون نامتقارن[1]

۱ هدف ودامنه کاربرد

هدف از تدوین این استاندارد، تعیین سه روش سازو کار سبک استفاده از فنون نامتقارن به ترتیب زیر است:

الف- سازوکار اعتبارسنجی یک جانبه مبتنی بر لگاریتم‌های گسسته روی منحنی بیضوی؛

ب- سازوکار تبادل کلید اعتبارسنجی شده سبک (ALIKE)[2] برای اعتبارسنجی یک جانبه و ایجاد یک کلید جلسه؛

ج- سازوکار امضا مبتنی بر هویت.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 15946-1, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General

2-2 ISO/IEC 29192-1, Information technology — Security techniques — Lightweight cryptography — Part 1: General

۳ اصطلاحات و تعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف تعیین‌شده در استاندارد ISO/IEC 29192-1، اصطلاحات و تعاریف زیر به کار می‌رود.

1- Asymmetric
2- Authenticated lightweight key exchange

۱-۳

فن رمزنگاری[1] نامتقارن

فن رمزنگاری که از دو عملیات مربوط استفاده می‌کند یک عملیات عمومی تعریف شده به وسیله یک واحد داده عمومی و دیگری عملیات خصوصی تعریف شده به وسیله یک واحد داده خصوصی.

یادآوری- هر دو عملیات این ویژگی را دارا هستند که با معلوم بودن عملیات عمومی، به دست آوردن عملیات خصوصی به صورت محاسباتی غیرممکن می‌شود.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۳]

۲-۳

جفت نامتقارن

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

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۵]

۳-۳

چالش[2]

پارامتر رویه[3] مورد استفاده در ارتباط با پارامترهای سرّی که یک پاسخ را تولید می‌کند.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۶]

۴-۳

خواهان[4]

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[5] است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۷]

۵-۳

پارامتر خواهان

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

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

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۹]

۶-۳

تابع درهم‌ساز[1] مقاوم در برابر تصادم

به تابع درهم‌ساز که نتوان برای آن دو ورودی متفاوت با خروجی یکسان یافت، تابع درهم‌ساز مقاوم در برابر تصادم گفته می‌شود.

یادآوری – عملی بودن از لحاظ محاسباتی، به الزامات خاص امنیتی و محیطی بستگی دارد.

[استاندارد ملی ایران شماره ۱-۹۵۹۸: سال ۱۳۸۶، تعریف ۳-۲]

۷-۳

کوپن[2]

جفت اعداد از پیش محاسبه شده‌ای که تنها یک مرتبه به کار می‌روند؛

یادآوری – یکی سرّی نگاه‌داشته شده و دیگری تا زمان استفاده به وسیله یک هستار سرّی می‌ماند.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۸]

۸-۳

دامنه[3]

مجموعه‌ای از هستارهای عمل‌کننده تحت یک خط‌مشی امنیتی واحد است.

یادآوری – به عنوان مثال، گواهی‌های کلید عمومی تولید شده به وسیله یک صادرکننده یا مجموعه‌ای از صادرکنندگان گواهی که از یک خط‌مشی امنیتی یکسان استفاده می‌کنند.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۱۱]

۹-۳

پارامتردامنه

کلید یا تابع عمومی پذیرفته شده و مورد استفاده به وسیله همه هستارهای درون دامنه است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۱۲]

1- Hash
2- coupon
3- Domain

۱۰-۳

اعتبار سنجی هستار[1]

تأیید آن که یک هستار همان چیزی است که ادعا می‌کند.

[استاندارد ملی ایران شماره ۱-۱۰۸۲۵، تعریف ۳-۱۴]

۱۱-۳

پارامتر تعدد تبادل

دفعات تبادل اطلاعات در یک نمونه از سازوکار اعتبار سنجی است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۱۵]

۱۲-۳

تابع درهم‌ساز

تابعی است که رشته‌هایی از بیت‌ها را به رشته‌هایی از بیت‌ها با طول ثابت می‌نگارد و خواص زیر را نیز برآورده می‌سازد:

- با داشتن یک مقدار خاص در خروجی، یافتن ورودی‌ای که آن خروجی را نتیجه دهد از لحاظ محاسباتی غیرعملی باشد.

- با داشتن یک رشته‌ی خاص در ورودی، یافتن ورودی دیگری که همان خروجی را نتیجه دهد از لحاظ محاسباتی غیرعملی باشد.

یادآوری - عملی بودن از لحاظ محاسباتی، به الزامات خاص امنیتی و محیطی بستگی دارد.

[استاندارد ملی ایران شماره ۱-۱-۹۵۹۸: سال ۱۳۸۶، تعریف ۳-۵]

۱۳-۳

کلید محرمانه اصلی[2]

واحد داده محرمانه است.

یادآوری-کلید محرمانه اصلی فقط می‌تواند به وسیله خدمت‌رسان مورد اعتماد مطابق با فرایند تولید داده امضا خصوصی استفاده شود.

۱۴-۳

کلید خصوصی[3]

واحد داده‌ی خصوصی یک جفت نامتقارن است.

1-Entity authentication
2-Master
3- Private key

یادآوری – کلید خصوصی باید سرّی نگاه‌داشته شود و تنها باید به وسیله یک خواهان مطابق با یک فرمول پاسخ مناسب مورد استفاده قرار گرفته و در نتیجه هویت آن را تعیین کند.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۱]

۳-۱۵

پارامتر رویه

واحد داده عمومی گذرای[1]مورد استفاده در یک نمونه از سازو کار اعتبار سنجی مانند شاهد[2]، چالش یا پاسخ[3] است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۲]

۳-۱۶

کلید عمومی[4]

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

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۳]

۳-۱۷

عدد تصادفی[5]

پارامتر متغیر با زمان که مقدار آن قابل پیش‌بینی نیست.

[استاندارد ملی ایران شماره ۱-۱۰۸۲۵، تعریف ۲-۲۹]

۳-۱۸

پاسخ

پارامتر رویه تولید شده توسط خواهان و پردازش شده به وسیله درستی‌سنج جهت وارسی هویت خواهان است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۵]

۳-۱۹

پارامتر محرمانه[6]

عدد یا رشته بیتی که در دامنه عمومی ظاهر نمی‌شود و تنها توسط یک خواهان مورد استفاده قرار می‌گیرد.

1- Transient public data item
2- Witness
3- Response
4-Private key
5- Random number
6-Secret parameter

یادآوری- به عنوان مثال یک کلیدخصوصی

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۶]

۲۰-۳

امضا[1]

فرایند تولید امضا که پیام و کلید امضای امضاکننده برای تولید امضا است.

۲۱-۳

امضا کننده[2]

هستار با یک رشته بیت منحصر به فرد به عنوان یک شناسه، شامل توابع و داده‌های خصوصی لازم برای شرکت در تولید امضا است.

۲۲-۳

کلید امضا[3]

واحد داده محرمانه ارائه شده به وسیله خدمت‌رسان مورد اعتماد است.

یادآوری- کلید امضا می‌تواند فقط به وسیله امضا کننده طبق فرایند تولید امضا استفاده شود.

۲۳-۳

نشان[4]

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

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۲۷]

۲۴-۳

اعتبار سنجی یک جانبه[5]

اعتبارسنجی هستاری که یک هستار را از هویت دیگری مطمئن می‌سازد اما برعکس آن صادق نیست.

[استاندارد ملی ایران شماره ۱- ۱۰۸۲۵، تعریف ۲-۳۹]

۲۵-۳

صحه‌گذار[6]

1-Sign
2-Signer
3-Signing key
4 - Token
5-unilateral authentication
6-verifier

هستار شامل توابع لازم برای مشارکت در تبادلات اعتبارسنجی از طرف یک هستار نیازمند به اعتبارسنجی هستار یا مشارکت در صحت یک امضا پیام و امضا داده شده است.

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲]

۲۶-۳

صحت

فرایند صحه‌گذاری که پیام، امضا و هویت امضا کننده را می‌گیرد تا خروجی accept (قبول) دهد که به معنی این است که امضای داده شده به وسیله امضاکننده با کلید امضا مربوطه تولید شده است یا در غیر این صورت reject (رد) می‌شود.

۲۷-۳

شاهد[1]

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

[استاندارد ملی ایران شماره ۵-۱۰۸۲۵: سال۱۳۹۲، تعریف ۲-۳۱]

۴ نمادها و اصطلاحات کوته نوشت

در این استاندارد ، نمادها و اصطلاحات کوته‌نوشت زیر به کار می‌رود:

$|A|$ اندازه بیت عدد A اگر A یک عدد صحیح غیرمنفی باشد (یعنی عدد صحیح یکتای i به طوری‌که$2^{i-1}\leq A<2^{i}$ اگر $A>0$یا اگر $A=0$ ، برای مثال$(|17=|1+2^{16}=65537|)$، یا طول بیت رشته بیت A اگر A یک رشته بیت باشد.

یادآوری- برای نمایش عدد A به عنوان رشته‌ای با α بیت با شرط$|A|<\alpha$ و $\alpha - |A|$ بیت 0 به سمت چپ بیت‌های $|A|$ افزوده می‌شود.

$\lfloor A \rfloor$ بزرگترین عدد صحیح که کمتر یا مساوی عدد واقعی A باشد.

A[I] i امین بیت عدد A، که A[1] در سمت راست بیت و A[|A|]در سمت چپ بیت است.

$B \| C$ رشته بیتی که از الحاق واحدهای داده B و C طبق ترتیب مشخص شده حاصل می‌شود. در مواردی که حاصل الحاق دو یا چند واحد داده به ورودی یک الگوریتم رمزنگاری داده می‌شود. و این الگوریتم به عنوان قسمتی از سازوکار اعتبارسنجی است، این حاصل باید به گونه‌ای ساخته شود که بتوان آن را به صورت یکتا به رشته‌های داده سازنده‌اش تجزیه کرد؛ به این صورت امکان وجود هرگونه ابهام در تفسیر از بین می‌رود. برای

1- Witness

دستیابی به ویژگی اشاره شده بسته به کاربرد، راه‌های مختلفی وجود دارد. به عنوان مثال، برای دستیابی به این ویژگی می‌توان از دو روش زیر استفاده کرد:

الف - طول هر یک از زیر رشته‌ها را در تمام دامنه با استفاده از سازوکار، ثابت نگه‌داشت یا

ب- کدبندی دنباله رشته‌های الحاق شده با استفاده از روشی که کدگشایی یکتا را تضمین می‌کند. برای مثال، با استفاده از قواعد کدبندی تعریف شده در استاندارد ISO/IEC 8825-1

D پاسخ (پارامتر رویه)

d چالش (پارامتر رویه)

E منحنی بیضوی (پارامتر دامنه)

E_K رمز بلوک تابع رمزنگاری با کلید K

e نمای عمومی (پارامتر دامنه)

$f_0(u,x)$ x^* که $f_0(u,x)=0\|x\|\dots\|0\|x\|0\|x^*$ نمایانگر مهم‌ترین بیت‌های x (به طور بالقوه بدون بیت) موردنیاز به طوری که طول $0\|x\|\dots\|0\|x\|0\|x^*$ برابر با u باشد.

$f_1(u,x)$ X^* که $f_1(u,x)=1\|x\|\dots\|1\|x\|1\|x^*$ نمایانگر مهم‌ترین بیت‌های X (به طور بالقوه بدون بیت) موردنیاز به طوری که طول $1\|x\|\dots\|1\|x\|1\|x^*$ برابر با u باشد.

h تابع درهم‌ساز

|h| طول بیت کد درهم‌ساز تولید شده به وسیله تابع درهم‌ساز h

HE تابع لایه‌گذاری مبتنی بر مسدود کردن رمز E_K (پارامتر دامنه)

ID رشته دودویی که نمایانگر اعتبار یا اطلاعات شناسایی است

L طول بیت کد لایه‌گذاری تولید شده به وسیله تابع HE (پارامتر دامنه)

m پیام

N پودمان‌های مرکب (پارامتر دامنه)

n منظور از نقطه پایان P (پارامتر دامنه)

[n]P عملیات ضربی که یک عدد صحیح مثبت n و یک نقطه P بر روی منحنی E را به عنوان ورودی گرفته و نقطه دیگر Q بر روی منحنی E را به عنوان خروجی می‌دهد به طوری که

$Q=[n]P=P+P+\ldots+P$ مجموع n رخداد P است. این عملیات روابط $[0]P=0_E$ (نقطه در بی‌نهایت) و $[-n]P=[n](-P)$ را برآورده می‌کند.

P نقطه پایه بر منحنی بیضوی E (پارامتر دامنه)

p_1 و p_2 عوامل اول از پودمان در جهت صعودی به عنوان مثال $p_1<p_2<\ldots$ (پارامترهای محرمانه)

Q و Q_i کلید خصوصی (پارامتر محرمانه)

q اندازه فیلد (پارامتر دامنه)

r عدد تصادفی جدید یا رشته جدید بیت‌های تصادفی (پارامتر محرمانه)

T نقطه عمومی (پارامتر دامنه)

t کلید محرمانه اصلی (پارامتر محرمانه)

u طول بیت کلید *K* در رمز مسدود شده تابع رمزنگاری با کلید E_K (پارامتر دامنه)

v طول بیت یک پیام مسدود در رمزنگاری رمز مسدود E_k (پارامتر دامنه)

W شاهد (پارامتر رویه)

w پارامتر امنیت (پارامتر دامنه)

'$X_1X_2...$' عددی با نمایش شانزده تایی $X_1\ X_2\ldots$ که در آن هر Xi برابر با یکی از 0-9 و A-F است.

α اندازه پودمان در بیت به طور مثال 2^{α} پودمان $\leq 2^{\alpha-1}$ ، که به صورت |پودمان| نشان داده می‌شود.

δ طول رشته‌های جدید بیت‌های تصادفی برای نمایش چالش‌ها (پارامتر دامنه)

ρ طول رشته‌های جدید بیت‌های تصادفی برای نمایش اعداد تصادفی (پارامتر دامنه)

{a, b, c, …} مجموعه شامل عناصر a, b, c, …

۵ سازو کار اعتبار سنجی یک جانبه مبتنی بر لگاریتم گسسته روی منحنی بیضوی

۵-۱ کلیات

این سازوکار GPSرمزی[1] همچنین در متون رمزنگاری قبل از آن با توجه به Girault ، Poupard و Stern، GPS نامیده می‌شود. نامی که اکنون مورد استفاده است برای جلوگیری از سردرگمی با خدمت موقعیت مکانی فیزیکی GPS است. GPSرمزی طرح شناسایی دانش صفر است که اعتبارسنجی هستار یک جانبه را فراهم می‌کند.

1- CryptoGPS

چندین گونه از GPSرمزی در استاندارد ملی ایران شماره ۵-۱۰۸۲۵ مشخص شده است و نسخه مناسب‌تر با تجهیزات محدود شده همراه با برخی بهینه‌سازی‌ها در زیر معرفی شده است.

۵-۲ الزامات امنیتی برای محیط

سازوکار GPSرمز یک صحه‌گذار 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 ISO/IEC 15946-1 داده شده است.

یادآوری ۱- این سازو کار نوعی از منحنی بیضوی طرح GPSرمز منتسب به Girault ، Poupard و Stern را پیاده‌سازی می‌کند. این سازوکار اجازه استفاده از نوع LHW[11] را می‌دهد و به ویژه برای محیط‌هایی که در منابع خواهان بسیار کم هستند مناسب است.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

الف- پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کند باید انتخاب شود. پارامترهای انتخاب شده باید به صورتی قابل اطمینان به تمامی هستارهای درون دامنه معرفی شوند.

ب- هر خواهان باید به یک منحنی بیضوی E و مجموعه‌ای از پارامترها که عبارتند از اندازه دسته (فیلد) 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.

پ- هر نقطه P که به عنوان پایه لگاریتم‌های گسسته منحنی بیضوی استفاده می‌شود باید به گونه‌ای باشدکه برای هر نقطه دلخواه J روی منحنی، پیدا کردن یک عدد k در بازه [0,n-1] (درصورت وجود) به طوری که محاسباتی J=[k]P امکان‌پذیر نباشد. امکان‌پذیر بودن به وسیله متن کاربرد سازو کار تعریف می‌شود.

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

ث- هر درستی‌سنج باید یک رونوشت با اعتبار از کلید عمومی متناظر با کلید خصوصی خواهان را به دست آورد.

یادآوری۲- ابزاری که به وسیله 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 به دست آورد.

ج- هر خواهان و هر درستی‌سنج باید ابزار تولید رشته‌های جدید بیت‌های تصادفی را در اختیار داشته باشند. وقتی کوپن‌ها استفاده می‌شود، هر خواهان باید همچنین ابزار تولید رشته های جدید بیت‌های تصادفی را در اختیار داشته باشند.

1-Low Hamming Weight

چ- اگر سازوکار از یک تابع درهم‌ساز استفاده کند، آنگاه تمامی هستارهای درون دامنه باید بر روی آن تابع درهم ساز توافق داشته باشند. برای مثال، می‌توان یکی از توابع مشخص شده در استاندارد ملی ایران شماره ۳-۹۵۹۸را به کار برد.

۵-۳ تولید کلید

برای خواهان A، یک رشته جدید باید به صورت تصادفی به طور یکنواخت از مجموعه $\{2,3,\ldots,n-2\}$ 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 به دست می‌دهد. نقطه عمومی برای خواهان A که با G(A) نشان داده می‌شود، برای هر دو حالت زیر به صورت برابر تنظیم شده است:

الف- معکوس ضرب عدد Q در نقطه پایه P است.

$$G(A)=(X_G,Y_G)= -[Q]P$$

یادآوری۱- این نسخه مناسب‌ترین نسخه برای دستگاه‌های محدود است.

ب- یا ضرب عدد Q در نقطه پایه P است.

$$G(A)=(X_G,Y_G)= [Q]P$$

چالش‌ها از یک مجموعه اعداد صحیح S انتخاب می‌شوند به طوری که برای هر عضو Δ نامساوی $2^{\delta-1} < \Delta \leq 2^{\delta}$ 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 به گونه‌ای دیگر تعریف شده باشد، مقدار δ برابر با ۴۰ قرار داده می‌شود که یک پارامتر دامنه است.

یادآوری۲- توصیه می‌شود تعداد کل چالش‌های ممکن به 2^{40} محدودشود. اگر به این توصیه عمل نشود، بهتر است ملاحظات ویژه‌ای در نظرگرفته شود تا درستی‌سنج از خواهان به عنوان پیشگوی امضاکننده استفاده نکند.

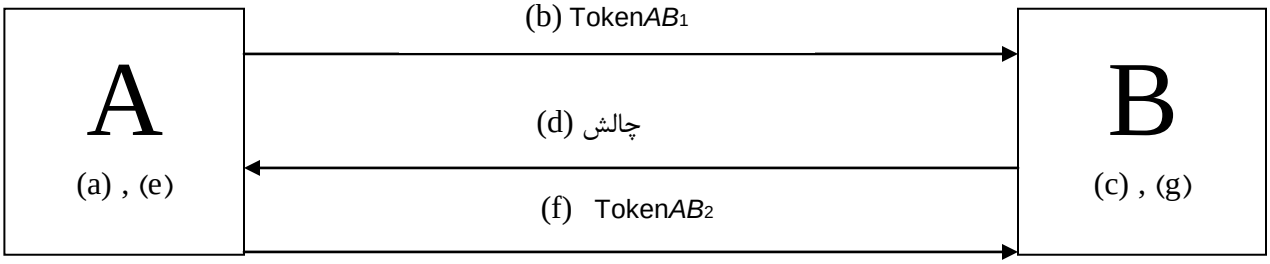
یادآوری ۳- اگر مجموعه چالش‌ها بازه $[0,\Delta-1]$ باشد، آن گاه $\beta = \delta$.

یادآوری ۴- به چالشی LHW گفته می‌شود که حداقل $\sigma-1$ بیت صفر بین هر دو بیت یک متوالی در نمایش دودویی آن وجود داشته باشد.

یادآوری ۵- تعریف نقطه عمومی G(A) اندکی از تعریفی که در استاندارد ملی ایران شماره ۵-۱۰۸۲۵ داده شده متفاوت است. این تغییر به پیاده‌سازی های جمع و جور و کارآمد تر منتج به محاسبات تگ اجازه می‌دهد زیرا فرمول پاسخ در حال حاضر ساده‌تر و جمع و جور تر برای پیاده‌سازی نسبت به تفریق عدد صحیح است.

۵-۴ سازو کار اعتبار سنجی یک جانبه

اعدادی که در شکل ۱ درون پرانتز قرار دارند مربوط به مراحل سازوکار هستند. این مراحل شامل تبادل اطلاعاتی هستندکه با جزییات در ادامه آورده شده است. خواهان با A و صحه‌گذار با B نشان داده شده‌اند.



شکل۱- سازوکاراستفاده‌کننده از یک لگاریتم گسسته نسبت به منحنی‌های بیضوی

خواهان باید عدد δ، مبنای P و کلید خصوصی Q (به صورت یک رشته σ بیتی) را ذخیره کند. در غیر این صورت $\delta = ۴۰$ در نظر گرفته شود.

در مورد راهبرد کوپن، خواهان علاوه بر یک کلید خصوصی Q و یک عدد δ، لازم است فقط مجموعه‌ای از کوپن‌ها را ذخیره کند و نیازی به داشتن ابزاری برای تولید رشته‌های جدید بیت‌های تصادفی نیست. برای این که هر کوپن فقط یک بار استفاده شود، هر یک شامل یک رشته با ρ بیت (اگر بتوان آن را به وسیله یک تابع شبه تصادفی باز تولید کرد، نیازی به ذخیره کردن آن نیست، به طور مثال یکی از توابع مشخص شده در استاندارد ISO/IEC 18031) و یک شاهد است.

صحه‌گذار 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 و n را در اختیار داشته باشد.

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

a) برای هر اعتبارسنجی:

۱) یک کوپن (r,W) استفاده می‌شود.

۲) یا یک رشته جدید ρ بیتی به صورت تصادفی و به طور یکنواخت انتخاب شود. این رشته باید محرمانه نگه‌داشته شود.

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

یادآوری۱- اگر رشته جدید ρ بیتی به صورت تصادفی انتخاب شود، آنگاه احتمال این که تمام ۸۰ 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 شاهدکه با W نشان داده می‌شود تبدیل شود.

فرمول شاهد:

$$W=EC2OSP_E([r]P,fmt)$$

$EC2OSP_E$ تابعی است برای تبدیل یک نقطه بر روی منحنی بیضوی E به یک رشته هشتایی طبق استاندارد ISO/IEC 15946-1 و fmt قالب خاصی است که یک از مقادیر نماد uncompressed, compressed یا hybrid است.

یادآوری ۲- تحت شرایط خاص پیاده سازی، برخی ممکن است با استفاده ازفرمول شاهد $W=EC2OSP_E([r \bmod n]P,fmt)$ را ترجیح دهند.

b) A، $TokenAB_1$را به B می‌فرستد. $TokenAB_1$ برای B شاهد W یا کد درهم W وTextاست. کد درهم به یکی از چهار صورت زیر است.

چهار متغیر درهم‌ساز عبارتند از $h(h(W) \| h(Text))$ و $h(W \| Text), h(W \| h(Text)), h(h(W) \| Text)$ که در آن h تابع درهم ساز و TEXT یک فیلد متنی اختیاری است. (ممکن است خالی باشد). اگر فیلد 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 با Token ارسال کند. چگونگی در دسترس قرار دادن دسته متنی برای استفاده در کاربردها خارج از محدوده این استانداردست .درپیوست الف استاندارد 10825-1 اطلاعاتی در مورداستفاده از دسته‌های متنی وجود دارد. متغیر درهم‌سازی یک پارامتر دامنه است.

c) با دریافت Token AB_1 یک رشته جدید باید به صورت تصادفی به طور یکنواخت از مجموعه S انتخاب شود.

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

یادآوری ۳- اگر از یک چالش LHW استفاده شود، می‌توان آنرا به شکل فشرده به A ارسال کرد. A باید ابزار بازیابی چالش اول پیش از مرحله ث بند ۱ را در اختیار داشته باشد .

e) با دریافت چالش، مراحل محاسباتی زیر انجام می‌شود:

۱) اگر چالش عضوی از S نباشد، آنگاه این رویه ناموفق است.

۲) پاسخ D باید از عدد تصادفیr و کلید خصوصی Q محاسبه شود.

فرمول پاسخ به شکل زیر است:

الف) اگر $G(A) = -[Q]P$ باشد $D=r+d\times Q$ است.

یادآوری ۴- اگرچالش 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.

یا:

ب) اگر $G(A)= [Q]P$ باشد $D=r-d\times Q$ است.

f) A، $TokenAB_2$ را به B می‌فرستد. $TokenAB_2$ پاسخ D است که از مرحله ث بند دو محاسبه می‌شود.

g) با دریافت $Token\ AB_2$ ، قدم‌های محاسباتی زیر انجام می‌شود:

۱) اگر پاسخ D یک رشته ρ بیتی نباشد و/یا اگر تمام ۸۰ بیت سمت چپ D برابر باشند، آن گاه این رویه ناموفق است.

۲) باید یک شاهد که با *W نشان داده می‌شود محاسبه شود.

فرمول صحه‌گذار :

$$W^* = EC2OSP_E([d]G(A) + [D]P, fmt)$$

یادآوری ۵- تحت شرایط خاص اجرای برخی ممکن است با استفاده از فرمول صحه‌گذار $W = EC2OSP_E([d]G(A) + [D \bmod n]P, fmt)$ ترجیح داده شود.

۳) اگر شاهد *W یا کد درهم *W و Text که یکی از چهار نوع درهم‌ساز هستند با $TokenAB_1$ دریافت شده در مرحله b) یکسان باشد، آن‌گاه رویه موفق است. در غیر این صورت، رویه ناموفق است.

یادآوری۶- ارسال اطلاعات دیگر به همراه هرتبادل روند مجاز است. B می‌تواند از چنین اطلاعاتی برای محاسبه مقدار فیلد متنی اختیاری کمک بگیرد.برای مثال، A مجاز است اطلاعاتی از قبیل گواهی را به همراه $TokenAB_1$ ارسال کند.

۶ سازو کار تبادل اعتبار سنجی یک جانبه کلید مبتنی بر رمزنگاری

۶-۱ کلیات

این سازوکار "ALIKE" برای تراکنش‌های با ارتباط کم طراحی شده است که در معرض محدودیت زمانی بسیار قدرتمند است. در این پروتکل، صحه‌گذار (به طور مثال خواننده یا پایانه) اعتبارسنجی یک اثبات‌کننده (به طور مثال کارت با ارتباط کم) مربوط به مرجع صدور گواهی‌نامه را می‌سنجد. به علاوه اثبات‌کننده و صحه‌گذار یک کلید جلسه برای پیام امن ایجاد می‌کند. اعتبار ALIKE آن است که اجازه می‌دهد تا از خواننده‌های کم هزینه (بدون پودمان امنیت دسترس) استفاده کند در حالی که به محدودیت زمانی قدرتمند می‌رسد. ALIKE مبتنی بر طرح رمزنگاری کلید عمومی که برای متغیر RSA نامیده می‌شود که از رمزگشایی بسیار سریع برخوردار است. در ALIKE ، رمز گشایی توسط ثابت کننده (به عنوان مثال کارت با ارتباط کم) که در آن کمک پردازنده رمزنگاری معمولا در دسترس است.

یادآوری- ALIKE به مفهوم تبادل کلید اعتبارسنجی سبک یک جانبه است. SPAK نام قبلی ALIKE بود. دلایل امنیتی ALIKE در بند ۳ کتابنامه در دسترس هستند.

۶-۲ الزامات امنیتی برای محیط

سازوکار ALIKE یک صحه‌گذار را برای اعتبارسنجی یک خواهان مربوط به مرجع صدور گواهی قادر می‌سازد و یک کلید جلسه را برای پیام امن ایجاد می‌کند.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

a) پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کند باید انتخاب شود. پارامترهای انتخاب شده باید به صورتی قابل اطمینان به تمامی هستارهای درون دامنه معرفی شوند.

b) هر خواهان باید به عوامل اولیه مجزا مجهز باشد، به طوری که دانش تولید خود یعنی پودمان‌ها (یک پارامتر خواهان) نباید به طور عملی هر هستار قادر به استنتاج آنها باشد که در آن عملی بودن با زمینه استفاده سازوکار تعریف می‌شود.

c) تمامی هستارها درون دامنه باید بر روی یک رمز بلوک E_K یعنی یکی از الگوریتم‌های مشخص شده در استاندارد ISO/IEC 29192-2 یا در استاندارد ISO/IEC 18033-3 باشد. اندازه کلید با u و اندازه بلوک با v مشخص می‌شود. u و v باید برابر یا بزرگ‌تر از ۱۲۸ بیت باشد و u باید برابر یا بزرگ‌تر از v باشد. حداکثر آنتروپی کلید محرمانه K بلوک رمز E_K به v - ۱ تنظیم می‌شود. کلید محرمانه K با طول u از یک کلید محرمانه x از طول v - ۱ با استفاده از توابع $f_0(u,x)$ و $f_1(u,x)$ محاسبه می‌شود.

یادآوری- به استناد تعریف توابع $f_0(u,x)$ و $f_1(u,x)$، اولین بیت کلید رمز بلوک به 0 یا 1 تنظیم می‌شود. این استقلال دو کاربرد متفاوت رمز بلوک را در پروتکل تضمین می‌کند.

ت- هر خواهان و هر صحه‌گذار باید ابزاری برای تولید اعداد تصادفی داشته باشد.

۶-۳ تولید کلید

عدد A که با α نشان داده می‌شود و طول بیت از پودمان‌های N را ثبت می‌کند، یعنی $2^{\alpha} \square 2^{\alpha-1} \leq$ پودمان مطابق با زمینه استفاده شده از این سازوکار است.عددA یک پارامتر دامنه است. طول بیت پودمان‌ها باید طوری انتخاب شود که پیچیدگی سریع‌ترین الگوریتم فاکتورگیری را ارزیابی کند. که زمان در حال اجرا مربوط به اندازه پودمان‌های N بزرگ‌تر از سطح امنیتی مورد نظر است.

یک عدد صحیح غیر منفی، که با w نشان داده می‌شود باید طوری انتخاب شود که $w > 2.v$ باشد. w یک پارامتر امنیتی و یک پارامتر دامنه است. w هم چنین با طول بیت p_1 بوده و باید طوری انتخاب شود که پیچیدگی سریع‌ترین الگوریتم فاکتورگیری را ارزیابی کند. که زمان در حال اجرا مربوط به اندازه |p1| که بزرگ‌تر از سطح امنیتی مورد نظر است.

خواهان A باید دو فاکتور مجزای بزرگ اصلی را محرمانه نگه دارد که با p_1 و p_2 پودمان‌های N نشان داده می‌شوند. عوامل اولیه p_1 و p_2 باید طوری انتخاب شود که پودمان‌های N با $|p_1| << |p_2|$ متعادل نباشد.

الف- دو عدد اول p_1 و p_2 به صورت زیر ایجاد می‌شود:

۱) $|p_1| = w$ و $\gcd(e,p_1-1)$ که در آن e توان عمومی است. e باید برای جلوگیری از حمله کوپر اسمیت به اندازه کافی بزرگ‌تر انتخاب شود. و سازگار محدوده تحتانی شمیر است. مقدار e=۱۱ دارای بعضی مزیت‌های عملی است.

۲) $|p_2| = \alpha - w$

۳) $|p_1 \times p_2| = \alpha$

ب- $N = p_1 \times p_2$ و $t = e^{-1} \bmod (p_1-1)$ را محاسبه کنید. کلید عمومی (N,e) و کلید خصوصی (P_1,t) است. کلید عمومی به وسیله مرجع گواهی‌نامه تایید می‌شود.

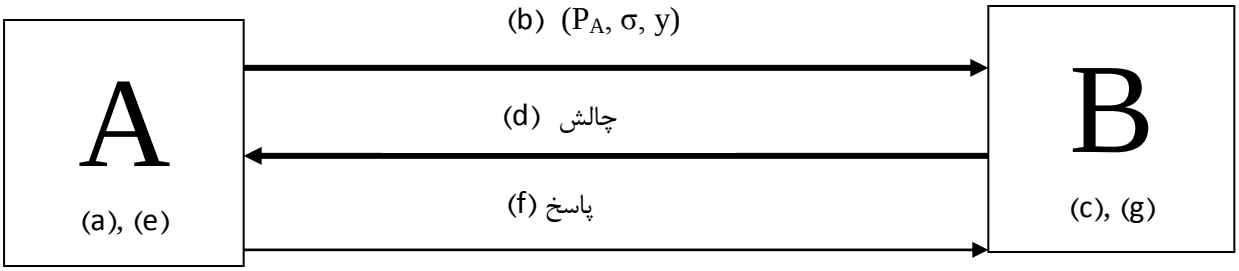
خواهان A باید با کلید خصوصی $S_A=(P_1-1)$ و کلید عمومی $P_A=(N,e)$ مربوط به پودمان‌های N مجهز شود.

خواهان A باید با گواهی‌نامه کلید عمومی P_A که با σ نشان داده می‌شود مجهز شود.

یادآوری- ابزاری که به وسیله آن خواهان یک رونوشت مورد اعتماد از این کلید عمومی را 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 به دست آورد.

۴-۶ تبادل اعتبار سنج یک جانبه

اعدادی که در شکل ۲ درون پرانتز قرار دارند مربوط به مراحل ساز وکار هستند. این مراحل شامل تبادل اطلاعاتی هستندکه با جزییات در ادامه آورده شده است. خواهان با A و صحه‌گذار با B نشان داده شده‌اند.



شکل ۲- ALIKE

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

a) عدد جدید k به طول ۱- v باید به صورت تصادفی و به طور یکنواخت به وسیله خواهان انتخاب شود. رمز بلوک برای محاسبه کاربرد y استفاده می‌شود: $y=E_{f\_0(u,k)}(0)$

b) A نشان (P_A,σ,y) را به صحه‌گذار B می‌فرستد.

c) یک عدد جدید r به طول v-1 باید به صورت تصادفی و به طور یکنواخت به وسیله صحه‌گذار انتخاب شود. مقدار لایه‌گذاری $pad= E_{f\_1(u,k)}(0)$ مشتق شده و پیام $(r\|pad)$ با P_A رمزگذاری شده است. نتیجه $d= (r\|pad)^e \bmod$ چالش است.

d) B چالش d را به A ارسال می‌کند.

e) با دریافت چالش مراحل محاسباتی زیر انجام می‌شود:

۱) اگر اندازه چالش برابر |N| نباشد، پس این رویه ناموفق خواهد بود.

۲) A کلید اختصاصی S_A را برای بازیابی متن $d^t \bmod p_1$ استفاده کرده و صحت سازوکار لایه گذاری در متن را به صورت زیر بررسی می‌کند:

الف) اگر لایه گذاری درست نباشد آنگاه این رویه ناموفق است.

ب) لایه‌گذاری برای بازیابی r حذف می‌شود.

۳) پاسخ D باید به وسیله رمزنگاری عدد k با استفاده از رمز بلوک محاسبه شود، یعنی $D= E_{f\_0(u,r)}(0\|k)$

f) A پاسخ D را به B می‌فرستد.

g) با دریافت پاسخ D، فرآیند صحه‌گذاری زیر انجام می‌شود:

۱) B درست است وقتی که σ یک رونوشت قابل اعتماد از کلید عمومی خواهان A است.

پ) اگر صحه‌گذار ناموفق باشد، رویه ناموفق است.

ت) در غیر این صورت B، k' را از پاسخ D بازیابی می‌کند.

۲) اگر $E_{f\_0(u,k)}(0)=y$ باشد، رویه موفق در غیر این صورت ناموفق خواهد بود.

۵-۶ استخراج کلید جلسه

به طور اختیاری، کلید جلسه می‌تواند بین خواهان A و صحه‌گذار B برای پیام امنیتی با استفاده از پارامترهای محرمانه مشترک (r,k) ایجاد شود.

۷ سازوکار امضا مبتنی بر هویت

۷-۱ کلیات

سامانه رمزنگاری مبتنی بر هویت، فن رمزنگاری نامتقارن است که اجازه می‌دهد کلید عمومی از یک هویت و از مجموعه پارامترهای ریاضی عمومی محاسبه شده و اجازه می‌دهد تا کلید خصوصی متناظر از هویت یک مجموعه پارامترهای ریاضی عمومی و یک مقدار دامنه گسترده محرمانه محاسبه شود. کلید عمومی کاربر می‌تواند به وسیله هر کسی که پارامترهای عمومی ضروری را دارد محاسبه شود، در حالی که برای محاسبه یک کلید خصوصی کاربر یک رمزنگاری محرمانه این محاسبات تنها توسط خدمت رسان مورد اعتمادی می تواند انجام پذیرد که این رمز را داشته باشد.

طرح امضای مبتنی بر هویت تحت این چارچوب طرح امضایی است که تایید امضا می‌تواند بدون نیاز به صحه‌گذار انجام گیرد و امضا کننده برای تعامل با یکدیگر، به طور مستقیم یا از طریق یک نماینده مانند یک پوشه یا گواهی خدمت‌رسان، قبل از تایید امضا، تعامل می‌کند. سامانه‌های دیگر ممکن است یک ارتباط به یک خدمت‌رسان برای هر عملیات صحه‌گذار نیاز داشته باشد.

شمای زیر (به بند ۹ کتابنامه ارجاع شود) به طرح شناسایی مبتنی بر هویت Bellare، Namprepre و Neven نسبت داده می‌شود (به بند ۱ کتابنامه ارجاع شود)که در واقع مبتنی بر طرح شناسایی Schnorr است اما بیشتر بهینه شده است (به بند ۱۴ کتابنامه ارجاع شود) با استفاده از متون مشخص شده در پیوست ب سازوکار امضا مبتنی بر هویت مطرح شده در این قسمت می‌تواند تبدیل به یک سازوکار بسیار کارآمد برای دستگاه‌های سبک شود.

یادآوری- دلایل امنیتی رویه‌های تعریف شده در زیر در بند ۹ کتابنامه در دسترس است.

۷-۲ الزامات امنیتی برای محیط

سازوکار امضای مبتنی بر هویت یک صحه‌گذار را قادر می‌سازد تا امضا کننده کلید امضای خود را برای تولید امضا برای پیام داده شده استفاده کند.

درون یک دامنه معین، الزامات زیر باید برآورده شوند:

الف- پارامترهای دامنه‌ای که عملیات سازوکار را اداره می‌کند باید انتخاب شود. پارامترهای انتخاب شده باید به صورتی قابل اطمینان به تمامی هستارهای درون دامنه معرفی شوند.

ب- پارامترهای دامنه‌ای باید شامل یک منحنی بیضوی E و مجموعه‌ای از پارامترها که عبارتند از یک نقطه P بر مبنای E و n (مرتبه نقطه P) باشد.

پ- هر نقطه P که به عنوان پایه لگاریتم‌های گسسته منحنی بیضوی استفاده می‌شود باید به گونه‌ای باشدکه برای هر نقطه دلخواه J روی منحنی، پیدا کردن یک عدد k در بازه [n-1, 0] (درصورت وجود) به طوری که از لحاظ محاسباتی J=[k]P امکان‌پذیر نباشد. امکان‌پذیر بودن به وسیله متن کاربرد سازوکار تعریف می‌شود.

ت- هر امضا کننده و خدمت‌رسان مورد اعتماد باید ابزاری برای تولید اعداد تصادفی داشته باشد.

ث- تمامی هستارهای درون دامنه باید بر روی آن تابع درهم‌ساز مقاوم در برابر تصادم توافق داشته باشند. برای مثال، می‌توان یکی از توابع مشخص شده در استاندارد ملی ایران شماره ۳-۹۵۹۸ را به کار برد.

ج- خدمت رسان مورد اعتماد باید به طور یکنواخت یک عدد جدید t تصادفی را انتخاب کند که غیر صفر و کمتر از n باشد. محاسبه نقطه عمومی T که برابر است با ضرب نقطه پایه P به عدد t : T=[t] P

چ- خدمت‌رسان مورد اعتماد باید t را به صورت کلید محرمانه اصلی نگه‌داشته و منحنی E، نقطه T ، نقطه پایه P و عدد n به صورت پارامترهایی منتشر می‌شود.

۷-۳ تولید کلید

امضا کننده A باید از خدمت‌رسان مورد اعتماد تولید کلید امضا خود را بخواهد. برای هر کاربرد این سازوکار، رویه زیر باید به وسیله خدمت‌رسان مورد اعتماد انجام شود.

خدمت رسان مورد اعتماد باید به طور یکنواخت عدد جدید r را به صورت تصادفی و یکنواخت انتخاب کند که باید غیر صفر و کمتر از n باشد و نقطه $R=(x_R,y_R)$ محاسبه شود که برابر با ضرب نقطه پایه P به عدد r است.

$$R=[r]P$$

الف- یک عدد s را باید از عدد تصادفی r و کلید محرمانه اصلی از خدمت‌رسان مورد اعتماد t محاسبه شود.

$$s=r+h(X_R \parallel ID)* t \bmod n$$

که در آن h تابع درهم‌ساز مقاوم در برابر تصادم است و ID یک رشته دودویی است که نماینده هویت یا اطلاعات شناسایی امضا کننده A می‌باشد.

ب- کلید امضا برای امضا کننده A باید $\{R,s\}$ باشد.

یادآوری- یک کلید خصوصی تولید شده صحیح باید از فرمول $P=R+[h(x_R \parallel ID)]T=_{[s]}$ به دست آید.

۷-۴ امضا

برای امضا پیامی به طول دلخواه m با کلید امضا، امضا کننده A است که به رویه زیر باید اجرا شود.

الف- امضا باید یک عدد تصادفی جدید y را به طور یکنواخت انتخاب کند که باید غیر صفر و کمتر از n باشد.

ب- نقطه $Y=(x_Y,y_Y)$ که برابر با ضرب نقطه P به عدد y است محاسبه می‌شود.

$$Y= [y]P$$

پ- عدد z باید از کلید خصوصی R وs محاسبه شود.

$$z=y+h\,(x_Y \| x_R \| m) \times s \bmod n$$

ت- امضا امضاکننده A و پیام m باید $\{Y,R,z\}$ باشد.

۵-۷ صحه‌گذار

برای صحه‌گذاری امضا $\{Y,R,z\}$ امضا کننده A با هویت ID برای پیام m ، صحه‌گذار باید مقدار زیر را محاسبه کند.

$$c= h\,(x_Y \| x_R \| m)$$

و برقراری تساوی زیر را بررسی نماید:

$$_{[z]}P=Y+_{[c]}R +[c\times h(x_R \| \ ID)]T$$

اگر تساوی برقرار باشد، صحه‌گذار باید خروجی accept در غیر این صورت reject را صادر کند.

پیوست الف
(الزامی)
شناسه‌های شی

```
LightweightCryptography-4{
iso(1) standard(0) lightweight-cryptography(29192)
part4(4) asn1-module(0) algorithm-object-identifiers(0)}
DEFINITIONS ::= BEGIN
EXPORTS ALL;
OID ::= OBJECT IDENTIFIER -- alias
-- Synonyms
is29192-4    OID    ::=    {iso(1)    standard(0)    lightweight-
cryptography(29192) part4(4)}
mechanism OID ::= {is29192-4 mechanisms(1)}
-- Lightweight cryptographic mechanisms
lw-discrete-logarithms-ecc-CryptoGPS OID ::= {mechanism
lw-discrete-logarithms-ecc-CryptoGPS(1)}
lw-authenticated-key-exchange-ALIKE OID ::= {mechanism
lw-authenticated-key-exchange-ALIKE(2)}
lw-identity-based-signature-IBS OID ::= {mechanism
lw-identity-based-signature-IBS(3)}

END -- LightweightCryptography-4
```

پیوست ب
(الزامی)
فن جایگزینی[1] حافظه

روش زیر (توسط لیو و همکاران او انجام شده است) می‌تواند برای ساده کردن محاسبات از به توان رساندن یا ضرب عددی استفاده شود. چنین عملیاتی در بسیاری از سازوکارهای رمز نگاری مشخص شده در ISO/IEC استفاده شده است. به ویژه آنهایی که مبتنی بر لگاریتم گسسته است. برای مثال بعضی از ساز وکارهای امضا مشخص شده در استاندارد ملی ایران شماره ۳-۹۷۹۶ و استاندارد ملی ایران شماره ۳-۱۴۸۸۸ و اعتبارسنجی هستار مطابق استاندارد ملی ایران شماره ۵-۱۰۸۲۵ می‌تواند در این مسیر پیاده‌سازی شود. با استفاده از این روش، سازوکار مبتنی بر هویت در بند ۷ این استاندارد می‌تواند تبدیل به یک سازوکار بسیار کار آمد برای دستگاه‌های سبک شود.

برای جایگزین کردن این روش محاسبه، تسهیل در افزایش حافظه مورد نیاز است.

اجازه دهید E منحنی بیضوی، P نقطه پایه بر روی E، و n رتبه نقطه P باشد.

برای هر عدد i از مجموعه [0, |n|-1] ، نقاط y برابر با ضرب عددی نقطه پایه P به r است یعنی:

$$Y_i=[2]P$$

برای محاسبه $Y_i=[2]P$ برای یک عدد غیر صفر y که کمتر از n است روش زیر را انجام دهید:

a) Set Y=[0]P

b) For i=1 to |n| compute:

if y[i]=1, then $Y=Y+Y_{i-1}$

c) Output Y

1-Trade-off

پیوست پ
(اطلاعاتی)
مثال‌های عددی

پ-۱ سازوکار GPS رمزی

پ-۱-۱ تولید کلید

منحنی بیضوی E برای این مثال منحنی P-۱۹۲ مشخص شده در FIPS PUB 186-3 است.

E: $Y^2=X^3-3X+b$ بر روی Fq

q = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF

b = 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1

نقطه پایه P بر روی E است:

$P = (x_P, y_P)$

= (188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012,
07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811)

n مرتبه نقطه P است:

n = FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831

برای تابع درهم‌ساز h، این مثال با استفاده SHA-256 انجام شده یعنی تابع درهم‌ساز چهارم مشخص شده طبق استاندارد ملی ایران شماره ۳-۹۵۹۸ است.

طول بیت برای چالش 40= δ و192= $|n| = \sigma$ بیت است.

پ-۱-۲ تبادل اعتبار سنجی

کلید خصوصی

Q = 4F1DF03A A32DCA02 652E83E7 E5FF5259 D61F5563 B3A0FA10

نقطه عمومی

در نوع اول، نقطه عمومی G(A) برابر با قرینه ضرب نقطه پایه P به وسیله عدد Q است.

G(A) = – [Q]P
= (xG, yG)

= (D753BF14 9529BC23 B1850A37 57C4D34A 0D686A95 C3B03855,
(1656B8CB 2896BFD4 BC8F94A8 F3708741 B954CC44 4FC3951A)

در نوع دوم، نقطه پایه G(A) برابر با ضرب نقطه پایه P در عدد Q است.

G(A) = [Q]*G*
= (xG, yG) G(A)
= (D753BF14 9529BC23 B1850A37 57C4D34A 0D686A95 C3B03855,
(E9A94734 D769402B 43706B57 0C8F78BD 46AB33BB B03C6AE5)

مرحله الف:

r یک رشته جدید بیت‌های تصادفی با طول $\rho = \sigma + \beta + 80 = 192+40+80=312$ bit است. w شاهدی است که $w=EC2OSP_E([r]P,\ uncompressed)$

r = 05E8B1 E1121B08 FB9A0F58 FC1E932F 9CEFE94D 629BC223
40B5F04B 554DCD2B C812A76D 98F8BA3E

[r]P= (DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF,
FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F)

W = 04 DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF
FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F

مرحله ب:

$TokenAB_1$ برابر با$h(W \| Text)$ که فیلد متن Text فارسی است. از این رو $TokenAB_1 = h(W)$ است.

h(W) = 0EB01E5E 32CA889D 099C8F6E 4CC3CB08 A3CD6008 C2849B43
0E07BCC7 B5241843

مرحله پ و ت

صحه‌گذار چالش:

d = 2D F0F5B4F2

مرحله ث و ج

در نوع اول پاسخ به چالش $TokenAB_1$، $D= r+d\times Q$ است.

D = 5E8B1 E1121B08 FB9A0F67 2ED9CE48 044BD618 3242087C ADDDA392
F2CA1F36 FDD94248 E8485D5E

در نوع دوم پاسخ به چالش $TokenAB_1$، $D= r- d\times Q$ است.

D = E8B1 E1121B08 FB9A0F4A C9635817 3593FC82 92F57BC9 D38E3D03
B7D17B20 924C0C92 49A9171E

مرحله چ

امنیتی:

W* = 04 DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF
FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F

h(W*) = 0EB01E5E 32CA889D 099C8F6E 4CC3CB08 A3CD6008 C2849B43
0E07BCC7 B5241843

اعتبارسنج معتبر است.

پ-۲ سازو کار ALIKE

پارامترهای ALIKE برای ۸۰ بیت امنیتی انتخاب شده‌اند.

اندازه بیت برای پودمان‌های N، ۱۲۸۰ بیت و برای p_1، ۳۵۲ بیت است.

رمز بلوک E_K به عنوان مثال از استاندارد ISO/IEC 29192-2 یا استاندارد ISO/IEC 18033-3 انتخاب شده است. در این مثال AES یک کلید اندازه u ، ۱۲۸ بیت است.

یادآوری- از آنجا که AES دارای اندازه بلوک ۱۲۸ بیت است u و v در این مثال برابر است.

پ-۲-۱ تولید کلید

e = 0000000B

p_1 = DD30D446 E32767CF E14885E7 44D077D0 89F82A87 37F53C4D 36AA9463
7C250E7D A516CA16 15C3B394 2B1CA791

p_2 = B544FE3B FB7D54D3 FA19B2E6 275CD79E B09CC643 44C03C6C 268F3624
5989FECC F44EC445 72A1F3C6 CD245A4D 4D17FDEC 0BF550D3 39C14EE8
4893CF1A 1E9BAF91 341AC6A9 E8B337B1 6B13B3A0 DF31E1A5 E5D63E70
0B93030D BDAF9D6B AFDBD696 6C1F09A0 95FA383C 32272D88 77A3F8FD

$N = p_1 \times p_2$
= 9C9F22B8 C7999ED9 54E7F600 63D134AB 6AF4BA29 046C2048 C7C0BC70
07686209 092D5B0B BE6E2D88 2E76E9B2 D2A43371 29490102 2401CCE7
A0143B96 13B1727B BC704892 F22B9EE6 A0C1F377 03229588 2EAC4879
3D88C4B3 800F5021 BAC0884C A05EA932 38FD8D35 50F227C6 8DB51EFE
A8051C08 8D475FC4 9A563C02 9616FDD0 650C5B66 ED2E1EFD 84732F70
F6F1A24A D5F88B5D 19864A5D 75F9124D

t = C9151E11 E5C6BB77 29E4D6D2 3E8EF88F 091026A9 78B0655D 7783CCB7
8821B015 21B7A071 2B0F0058 27315283

پ-۲-۲ تبادل اعتبارسنجی

مرحله الف و ب

k یک رشته جدید بیت‌های تصادفی به طول u-1 است که برای محاسبه y استفاده می‌شود.

k = 6C64D272 0B770A23 D5700C0B EBC63E5E

$y = E_{f\_0(k)}(0)$

= E85D2E05 D4C6592B E571EE71 9BA636E7

مرحله پ و ت

r یک رشته جدید از بیت‌های تصادفی طول u-1 است.

r = 6E5707FA 1F9171C1 D802C92C 605A3FD1

1 || r = EE5707FA 1F9171C1 D802C92C 605A3FD1

pad = HE(r) where HE(r) is equal to the L = 128 left-most bits of Ef_1(r)(0).

pad = B8C940AE B22FDB93 7A1FE295 1584A26C

صحه‌گذار چالش:

d = (r || pad) e mod N

= 18240256 E10CFD25 725AD87B 7EBAFB43 81988968 B7D35E4F 6D75A201
6480DFA6 B5E4E78A EDE764E7 49CB5880 4BFA2A81 088ECFB3 3903AA0F
31E3CE42 C653CA28 4F418EED F76D6914 D6B40C9B 205A00E5 6C8008AC
13FFD2F1 CA57FB8A B6B57001 A5E3B04D BBE14BB5 D5200511 20F744E4
9B87B87E 7F411F3D 4657E4AF A26E6D0B F4414095 816D90CD 06CF6EE5
6C244F17 F30CDB58 C6226D80 AEDC70F4

مرحله ث و ج

پاسخ به چالش:

D = E_{f_0}(r)(0 || k)

= 01203402 350C0611 F34C71BF 59F9CC3E

مرحله چ

امنیتی:

پ- ۲-۳ استخراج کلید جلسه

کلید جلسه S_k به طور اختیاری می‌تواند ایجاد شود.

s_k = r $\oplus$ k

= 0233D588 14E67BE2 0D72C527 8B9C018F

پ-۳ سازو کار امضا مبتنی بر هویت

پ-۳-۱ تولید کلید

منحنی بیضوی برای این مثال به شکل زیر است:

E: $Y^2=X^3+aX+b$ بیشتر از Fq

با

a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC

b = 1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45

q = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF

نقطه پایه P بر روی E.

P = (x_P, y_P)

= (4A96B568 8EF57328 46646989 68C38BB9 13CBFC82,

(23A62855 3168947D 59DCC912 04235137 7AC5FB32)

n رتبه نقطه P است.

n = 1 00000000 00000000 0001F4C8 F927AED3 CA752257

t کلید محرمانه اصلی است.

t = D21DF3A7 5787F180 5F00792F 9D8C317C 23FDF91B

T کلید عمومی است.

T = (x_T, y_T)

= (1B2F7E1F 831DF943 F82CFBE2 FF753A4C 9DF8040A,

1FFE799A 563024AF 86652027 CEA9A60A 00E1FB73)

ID اطلاعات شناسایی امضا است. |ID| = ۸ bit

ID = 01

r عدد جدید کمتر از n است.

r = 8A29A77B 8826FC67 2ABEA882 FEAEE9C3 6E1A78C2

R = [r]P

= (x_R, y_R) with $|x_R| = |y_R| = 160$ bits

= (1040E9BF 14546E1B 38FC74B5 31228C69 AF0BAED3,

8DC50619 E3B28AEC B8296F17 51466289 D32053F6)

برای تابع درهم‌ساز h، این مثال با استفاده SHA-1 انجام شده یعنی تابع درهم‌ساز چهارم مشخص شده طبق استاندارد ملی ایران شماره ۳-۹۵۹۸ است.

$S = r + h(X_R \| ID) \times t \bmod n$

= 49952E7E 4289DFA8 CE6ADB2F 55BA9C70 D89AA3C7

پ-۳-۲ امضا

پ-۳-۲-۱ مثال ۱

m یک پیام ۱۶۰ بیتی است.

m = 00000000 00000000 00000000 00000A73 199606B1

مرحله الف

y عدد جدید کمتر از n است.

y = 00000000 00000000 00000000 00000000 00000007

مرحله ب

$Y = [y]P$

= (x_Y, y_Y) with $|x_Y| = |y_Y| = 160$ bits

x_Y = 7A7F99D5 6472F619 577C4E8C 9B3A35E9 61472188

مرحله پ و ت

$z = y + h(X_Y \| X_R \| m) \times s \bmod n$

= 92D28A45 FFDE887E C8D297A2 7FA02CB5 7DF2CBAF

پ-۳-۲-۲ مثال ۲

پیام:

m = 00000000 00000000 00000000 00000A79 19B70693

مرحله الف

y عدد جدید کمتر از n است.

y = 00000000 00000000 00000000 00000000 00000010

مرحله ب

$Y = [y]P$

= (x_Y, y_Y)

x_Y = B32F7DFA 2A82B99B 5CAC2772 AA6661BE 5F315034

مرحله پ

$z = y + h(X_Y \| X_R \| m) \times s \bmod n$

$= \texttt{BB7A0E5A 805F67A6 CF00FF5A 0BF8B782 0803751E}$

پ-۳-۳ صحت

پ-۳-۳-۱ مثال ۱

$c = h(X_Y \| X_R \| m)$

$= \texttt{043969EF 9D9C6429 495139BD 8B37E086 FAA78FFB}$

$[z]P = (X_{[z]p}, y_{[z]p})$ with

$x_{[z]p} = \texttt{88913D78 4FD959FF 91E14157 D44799FA 674B2717}$

پ-۳-۳-۲ مثال۲

$c = h(X_Y \| X_R \| m)$

$= \texttt{F8228399 413773F9 EB23CCA0 DFD1D416 D50941B7}$

$[z]P = (x_{[z]p}, y_{[z]p})$ with

$x_{[z]p} = \texttt{E0B100B3 1CA6F0E7 251275A7 8B5F0BFB C6207A29}$

پیوست ت

(اطلاعاتی)

خصوصیات

این پیوست خواص سبک الگوریتم شرح داده شده در این استاندارد و انطباق آنها را با الزامات قسمت اول این استاندارد شرح می‌دهد. در این پیوست سازوکار IBS، سازوکار شرح داده شده در بند ۷ مطابق پیوست ب اجرا شده است.

جدول ت۱- انطباق خواص الگوریتم با الزامات استاندارد ISO/IEC 29192-1

		نام الگوریتم		
		رمز GPS	ALIKE	IBS
محدودیت	سطح تراشه	×		
	مصرف انرژی	×		×
	اندازه کد و اندازه RAM		×	×
	پهنای باند ارتباطات	×	×	×
	زمان اجرا	×	×	

جدول ت۲- مشخصات GPS رمزی

	GPS رمزی		
	محاسبات اصلی[۱۰]	محاسبات اصلی[۱۱]	ماژول کامل[۱۲]
سطح امنیتی (bits)	۸۰	۸۰	۸۰
سطح تراشه(GE)	۳۱۷	۴۳۱	۲۸۷۶
فرایند اعتبار سنجی(CLK)	۱۰۸۸	۱۳۶	۷۲۴
انرژی (GE* CLK)	۳۴۴۸۹۶	۵۸۶۱۶	۲۰۸۲۲۲۴
تکنولوژی (µm)	۰٫۱۸۰	۰٫۱۸۰	۰٫۳۵۰
یادآوری- ماژول کامل شامل مولد عدد شبه تصادفی همراه با محاسبات GPS رمزی بر روی برچسب است در حالی که "محاسبات اصلی" صرفا اشاره به محاسبات GPS رمزی بر روی برچسب دارد.			

جدول ت۳- مشخصات ALIKE

	ALIKE	
	فرایند[a] PICC	فرایند[b] PCD
سطح امنیتی	۸۰	۸۰
ویژگی‌های رمزنگاری- کمک پردازنده	مورد نیاز برای ضرب پودمان	لازم نیست
توابع مورد نیاز	تولید اعداد تصادفی. دو رمز بلوک اجرا شده بدون کانال جانبی خاص و اقدامات متقابل حملات خطا. توان پودمانی با پودمان کوچک (| p1| = ۳۵۲ bits)	تولید اعداد تصادفی. دو رمز بلوک اجرا شده توان پودمان‌ای با توان کوچک ($e \geq 11$, $\|N\| = 1248$ bits)
حافظه غیر فرار	ذخیره کردن کلید RSA برای ALIKE (۸۸ بایت برای مقایسه ۴۰۰ بایت برای RSA کلاسیک) و گواهی	کلید عمومی ذخیره CA
سایز کد	۱٫۶ kbytesروی حافظه ۸۰۵۱	
داده‌های منتقل شده با سرعت ارتباطات در 10^6 $kb.s^{-1}$	داده های ورودی ۱۶۰ byts ⇔ ۱۵٫۴۰ ms	داده های ورودی ۱۹۲ byts ⇔ ۱۸٫۸ ms
فرایند داخلی	۴ تا ۱۵ بار سریع‌تر از RSA کلاسیک مطابق با جز. برای مثال برای حافظه ۸۰۵۱: ۸۰ ms در ۳۱ MHz برای CPU و ۴۸ MHz برای رمزنگاری- کمک پردازنده	

[a] PICC : کارت مدار داخلی مجاور

[b] PCD: دستگاه اتصال مجاور

جدول ت۴- مشخصات IBS

IBS		
سطح امنیتی		۸۰
اندازه کد و اندازه RAM (byte) که مبتنی بر TinyOS 1.0. 15	فقط امضا آنلاین	flash = ۵۴۳۰۸ RAM = ۹۲۲
	فقط صحت	flash = ۵۵۳۷۴ RAM = ۹۲۲
زمان توان	امضا	۸۹۶
	صحه‌گذاری	۵۶۱۰
مصرف انرژی(µJ) که مبتنی بر MicaZ است At mel 128 L	امضا آنلاین	۱۲۳۷۰
	صحه‌گذار	۷۷۴۰۰
پهنای باند ارتباطات (بیت)		۴۸۰

پیوست
(اطلاعاتی)
کتابنامه

[1] M. Bellare, C. Namprempre, and G. Neven, *Security proofs for identity-based identification and signature schemes*, in Proc. of Eurocrypt ’04, Lecture Notes in Computer Science, Vol. 3027, pp 268-286, Springer-Verlag, 2004

[2] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology, 10:233--260, 1997

[3] J-S. Coron, A. Gouget, P. Paillier and K. Villegas, *SPAKE: a Single-party Public-key Authenticated Key Exchange Protocol for Contact-less Applications*, in Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010

[4] M. Girault and D. Lefranc, *Public key authentication with one (online) single addition*, in CHES’04, pp 413-427, 2004

[5] 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

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

[7] H. W. Jr. Lenstra, *Factoring Integers with Elliptic Curves*, Ann. Math. 126, 649-673, 1987

[8] A. K. Lenstra and H. W. Lenstra, Jr, *The development of the number field sieve*, Lecture Notes in Math. (1993) 1554, Springer-Verlag

[9] J. Liu, J. Baek, J. Zhou, Y. Yang, and J.-W. Wong, *Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network*, International Journal of Information Security, 9(4):287--296, Springer, August 2010

[10] M. McLoone and M.J.B. Robshaw, *Public Key Cryptography and RFID*, in M. Abe, editor, Proceedings of CT-RSA 07, volume 4377 of LNCS, pp 372-384, Springer, 2007

[11] M. McLoone and M.J.B. Robshaw, *New Architectures for Low-Cost Public Key Cryptography on RFID Tags*, in Proc. of IEEE International Conference on Security and Privacy of Emerging Areas in Communication Networks (SecureComm 2005), pp 1827-1830, IEEE, 2007

[12] A. Poschmann, M. Robshaw, F. Vater, and C.Paar, *Lightweight Cryptography and RFID: Tackling the Hidden Overheads*, in D. Lee and S. Hong, editors, Proc. of ICISC-2009, volume 5984 of LNCS, pp 129-145, Springer, 2010

[13] R.L Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signature and public-key cryptosystems*, in technical report LCS!TM82, MIT Laboratory for Computer Science, Cambridge, Massachusetts, 4th April 1977

[14] C.P. Schnorr, *Efficient identification and signatures for smart cards*, in Proceedings of CRYPTO ’89, volume 435 of Lecture Notes in Computer Science, pages 239–252. Springer, 1990

[15] A. Shamir, *RSA for paranoids*, in Cryptobytes, the technical newsletter from RSA Laboratories, Volume 1, Number 3 – Autumn 1995

[16] European Network of Excellence in Cryptology II, *ECRYPT II Yearly Report on Algorithms and Key Lengths (2010)*, available on http://www.ecrypt.eu.org/documents/D.SPA.13.pdf

[17] National Institute of Standards and Technology, *Digital Signature Standard (DSS), FIPS Publication 186-3*, available on http://csrc.nist.gov/publications/PubsFIPS.html

[18] ISO/IEC 18031:2011, Information technology — Security techniques — Random bit generation

[19] ISO/IEC 29192-2:2012, Information technology — Security techniques — Lightweight Cryptography — Part 2: Block ciphers

[20] 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)

[20] ISO/IEC 18033-3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers

[۲۲] استاندارد ایران – ایزو – ای ای سی شماره ۳-۹۷۹۶: سال ۱۳۸۸، فن آوری اطلاعات- فنون امنیتی- طرح های امضای دیجیتال با قابلیت بازیابی پیام گسسته -قسمت سوم: ساز و کارهای مبتنی بر لگاریتم

[۲۳] استاندارد ملی ایران شماره ۱- ۱۰۸۲۵: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیت- احراز هویت هستار- قسمت ۱: کلیات

[۲۴] استاندارد ملی ایران شماره ۵- ۱۰۸۲۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیت- احراز هویت هستار- قسمت ۵: سازوکارهای استفاده کننده از فنون دانش- صفر

[۲۵] استاندارد ملی ایران شماره ۱-۹۵۹۸: سال ۱۳۸۶، فناوری اطلاعات – روش‌های امنیتی- توابع درهم‌ساز- قسمت اول: کلیات

[۲۶] استاندارد ملی ایران شماره ۳- ۹۵۹۸: سال ۱۳۹۲، فناوری اطلاعات – روش‌های امنیتی- توابع درهم‌ساز- قسمت ۳: توابع درهم‌ساز اختصاصی

[۲۷] استاندارد ایران – ایزو – ای ای سی شماره ۳-۱۴۸۸۸: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی- امضاهای رقمی (دیجیتال) با پیوست قسمت ۳: سازوکارهای بر پایه لگاریتم پیوسته