INSO
10824-5
1st.Edition
2017
Identical with
ISO 18033-5:
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران
۱۰۸۲۴-۵
چاپ اول
۱۳۹۵

فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۵: رمزهای شناسه‌مبنا

Information technology- Security techniques- Encryption algorithms- Part 5: Identity- based ciphers

ICS: 35.030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸-۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.gov.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No. 2592 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.gov.ir

Website: http://www.isiri.gov.ir

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. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته‌شده 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 بین‌المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی‌شده در قانون، برای حمایت از مصرف‌کنندگان، 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 می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی آن را اجباری نماید. هم‌چنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. 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- الگوریتم‌های رمزگذاری- قسمت ۵: رمزهای شناسه‌مبنا»

رئیس:	**سمت و/یا محل اشتغال:**
نامجو، احسان (دکترای مخابرات)	هیأت علمی دانشگاه شهید چمران اهواز
دبیر:	
آرین‌نژاد، حسین (کارشناسی مهندسی برق- الکترونیک)	کارشناس اداره کل استاندارد خوزستان
اعضا: (اسامی به ترتیب حروف الفبا)	
خدابخشی، مونا (کارشناسی ارشد مهندسی برق- قدرت)	شرکت ایزی ارتباط پارس
داوودزاده، مجتبی (کارشناسی مهندسی برق- الکترونیک)	اداره کل تنظیم مقررات و ارتباطات رادیویی
رضازاده، آرشین (کارشناسی ارشد مهندسی کامپیوتر)	هیأت علمی دانشگاه شهید چمران اهواز
شهاوند، طیبه (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس ارشد- معاونت فناوری اطلاعات دادگستری خوزستان
عباسی، سعید (کارشناسی مهندسی برق- قدرت)	اداره کل استاندارد خوزستان
عنصری‌نیا، سعید (کارشناسی مهندسی کامپیوتر- سخت‌افزار)	مشاور فنی- شرکت ملی مناطق نفت‌خیز جنوب
فرهانی‌پور، مبین (کارشناسی ارشد مهندسی برق- مخابرات)	کارشناس فنی- صدا و سیما آبادان
موجبی، محمود (کارشناسی ارشد مهندسی مخابرات- رمز)	سازمان ملی فناوری اطلاعات ایران

اعضا: (اسامی به ترتیب حروف الفبا)	**سمت و/یا محل اشتغال:**
مهتدی، محمد (کارشناسی مهندسی برق- الکترونیک)	اداره کل تنظیم مقررات و ارتباطات رادیویی
مولوی، اردشیر (کارشناسی مهندسی برق- مخابرات)	کارشناس سوئیچ- شرکت ارتباطات زیرساخت

ویراستار:

محسنی، خلیل (کارشناسی ارشد متالوژی)	سرپرست اداره آموزش و ترویج- اداره کل استاندارد خوزستان

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۵: رمزهای شناسه‌مبنا » که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره‌شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در چهارصد و هشتاد و دومین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۱۲/۱۸ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ هم‌گامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم وخدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 18033-5: 2015, Information technology– Security techniques– Encryption algorithms– Part 5: Identity-based ciphers

مقدمه

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران به شمارهٔ ۱۰۸۲۴ است.

سایر قسمت‌های این مجموعه عبارتند از:

- ISO/IEC 18033-1: 2015, Information technology- Security techniques- Encryption algorithms- Part 1: General
- ISO/IEC 18033-2: 2015, Information technology- Security techniques- Encryption algorithms- Part 2: Asymmetric ciphers
- استاندارد ملی ایران شمارهٔ ۳-۱۸۰۳۳: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزنگاری- قسمت ۳- رمزهای بلوکی
- استاندارد ملی ایران شمارهٔ ۴-۱۸۰۳۳: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی الگوریتم‌های رمزنگاری- قسمت چهارم- رمزگذاری جریانی

استفاده از سازوکار رمزگذاری کلید عمومی نیازمند شناسایی کلید عمومی صحیح مورد استفاده برای رمزگذاری به شکلی اطمینان‌بخش است. زیرساخت کلید عمومی (PKI)[1] به منظور برقراری ارتباط مطمئن با یک هستار، کارکردهایی ارائه کرده و تعیین وضعیت جاری کلید عمومی را امکان‌پذیر می‌کند. در یک PKI، یک مرجع صدور گواهی (CA)[2]، گواهی صادر می‌کند که یک کلید عمومی را به شناسه مالکش، همراه با دیگر اطلاعات مخصوص کلید، نظیر مدت اعتبار پیوند می‌دهد. اگر کلید عمومی قبل از تاریخ انقضایش نامعتبر به حساب آید، آن‌گاه نیاز است که کاربران احتمالی کلید عمومی از این امر مطلع شوند، مثلا با صدور فهرست گواهی‌های باطل‌شده‌ای(CRL)[3] که توسط CA امضا شده است. تولید و توزیع گواهی‌نامه‌ها و CRLها مشکل مدیریتی عمده‌تری به وجود می‌آورد که سازوکارهای قرارگرفته در این استاندارد جهت مطرح نمودن آن‌ها طراحی شده‌اند. در رمزگذاری، یک رمزگذار ابتدا CRL را بدست آورده و وضعیت جاری گواهینامه را بررسی می‌کند. سپس رمزگذار گواهینامه را تصدیق می‌کند و درنهایت پیام را رمزگذاری می‌کند. بنابراین، رمزگذار باید به شیوه‌ای قادر به دسترسی به CRLهای جاری بوده و علاوه بر این توصیه می‌شود که رمزگذار در رمزگذاری هر پیام، نیازمند زمان طولانی و منابع محاسباتی وسیع برای بررسی تصدیق یک گواهی نباشد.

رمزگذاری شناسه‌مبنا (IBE) نوعی رمزگذاری نامتقارن است که به رمزگشا اجازه می‌دهد یک رشته اختیاری را به عنوان کلید عمومی خود برگزیند. رمزگذار با قراردادن رشته‌ای با قابلیت شناسایی ساده به عنوان کلید عمومی (مثلا یک رایانامه)، قادر است بدون استفاده از گواهی‌نامه از صحت آن اطمینان یابد. علاوه بر این اگر برقرارکردن دوره اعتبار کوتاهی که به شکلی چشم‌گیر، از مدت زمان به‌هنگام کردن یک CRL در یک PKI

1- Public key infrastructure
2- Certification authority
3- Certificate Revocation List

مرسوم کوتاه‌تر است امکان‌پذیر باشد، رمزگذار قادر به تولید متن رمز بدون بررسی وضعیت جاری کلید عمومی است، به دلیل این‌که ابطال اعتبار در چنین زمان کوتاهی غیرمحتمل است، درنتیجه انتظار می‌رود که IBE حجم کاری مدیریت گواهی‌نامه‌ها را کاهش دهد.

استفاده از IBE نیازمند یک مولد کلید خصوصی (PKG)[1] است، که با استفاده از کلید مخفی- اصلی خود، برای همه رمزگشاها، کلید خصوصی تولید می‌کند؛ این امر برخلاف سازوکارهای رمزگذاری متقارن سنتی هم‌چون مواردی است که در ISO/IEC 18033-2 تعیین شده است، که در آن، هستارها زوج کلید خصوصی/عمومی خود را تولید می‌کنند. در نتیجه، استفاده از IBE صرفا زمانی مناسب است که دسترسی شخص ثالثی جهت رمزگشایی همه داده‌های رمزگذاری‌شده، قابل قبول باشد.

سازوکارهای رمزگذاری شناسه‌مبنا در بندهای ۸ و ۹ تعیین می‌شود. سازوکارهای تعیین‌شده، سازوکار رمزگذاری شناسه‌مبنای BF، سازوکار رمزگذاری کپسوله‌سازی کلید شناسه‌مبنای SK، و سازوکار کپسوله‌سازی کلید شناسه‌مبنای BB1 می‌باشند.

ویژگی‌های تعیین‌شده در این استاندارد برای دستیابی قابل‌اطمینان مقادیر عمومی، جهت گواهی نمودن مالکیت یک کلید خصوصی، یا برای تصدیق مقادیر عمومی یا کلیدهای خصوصی، پروتکلی تعیین نمی‌کنند.

پیوست الف شناسه‌های شیء اختصاص داده‌شده به الگوریتم‌های تعیین‌شده در این استاندارد را تعیین می‌کند. پیوست ب ملاحظاتی امنیتی، برای هریک از سازوکارهای تعیین‌شده توصیف می‌کند و پیوست پ مثال‌هایی عددی ارائه می‌کند. پیوست ت فنونی مطرح می‌کند که به منظور حذف کردن قابلیت رمزگشایی PKG، قابل استفاده هستند و به موجب آن سطح اعتماد مورد نیاز به این هستار کاهش می‌یابد.

1- Private Key Generator

فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۵: رمزهای شناسه‌مبنا

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین ویژگی‌های سازوکارهای رمزگذاری شناسه‌مبنا است. برای هر سازوکار رابط کارکردی، عملیات دقیق سازوکار و فرمت متن رمز مشخص می‌شوند. با این وجود، ممکن است سامانه‌هایی که با این استاندارد ملی منطبق هستند، فرمت‌هایی دیگر برای ذخیره‌سازی و مخابرهٔ متون رمز استفاده کنند.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO/IEC 18033-1, Information technology–Security techniques- Encryption algorithms –Part 1: General

یادآوری- استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۴: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی الگوریتم‌های رمزنگاری-قسمت ۱- کلیات، با استفاده از استاندارد ISO/IEC 18033-1: 2005 تدوین شده است.

2-2 ISO/IEC 18033-2, Information technology- Security techniques- Encryption algorithms- Part 2: Asymmetric ciphers

2-3 ISO/IEC 18033-3, Information technology- Security techniques- Encryption algorithms- Part 3: Block ciphers

یادآوری- استاندارد ملی ایران شمارهٔ ۳-۱۰۸۲۴: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزنگاری- قسمت ۳- رمزهای بلوکی، با استفاده از استاندارد ISO/IEC 18033-3: 2005 تدوین شده است.

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه‌شده در استاندارد ISO/IEC 18033-1 اصطلاحات و تعاریف زیر نیز به کار می‌رود:

۳-۱

رمزگشا

decryptor

هستاری که متون رمز را رمزگشایی می‌کند.

۳-۲

رمزگذار

encryptor

هستاری که متون ساده را رمزگذاری می‌کند.

۳-۳

رمزگذاری ترکیبی

hybrid encryption

رمزگذاری که توسط رمز ترکیبی انجام می‌شود.

۳-۴

شناسه

identifier

شیءای که نمایانگر چیزی است و تایید هویت آن را به غیر واگذار می‌کند.

۳-۵

رشته شناسه

identity string

رشته‌ای که بیان‌گر یک شناسه است.

۳-۶

رمز شناسه‌مبنا

identity-based cipher

رمزی نامتقارن که در آن الگوریتم رمزگذاری، رشته‌ای دلخواه را به عنوان کلید عمومی اتخاذ می‌کند.

۳-۷

رمزترکیبی شناسه‌مبنا

identity-based hybrid cipher

رمزی که هم ترکیبی و هم شناسه‌مبنا است.

۳-۸

سازوکار کپسوله‌سازی کلید شناسه‌مبنا

identity-based key encapsulation mechanism

سازوکار کپسوله‌سازی کلید که در آن فرایند رمزگذاری، رشته‌ای دلخواه را به عنوان کلید عمومی اتخاذ می‌کند.

۳-۹

کلید عمومی- اصلی

master-public key

مقداری عمومی که انحصارا توسط کلید مخفی- اصلی متناظر تعیین می‌شود.

۳-۱۰

کلید مخفی-اصلی

master-secret key

مقداری مخفی که به منظور تولید کلیدهای خصوصی برای یک الگوریتم IBE، توسط مولد کلید خصوصی استفاده می‌شود.

۳-۱۱

الگوریتم استخراج کلید خصوصی

private key extraction algorithm

روشی که جهت تولید کلیدهای خصوصی برای الگوریتم IBE توسط مولد کلید خصوصی استفاده می‌شود.

۳-۱۲

مولد کلید خصوصی

private key generator

هستار یا تابعی که مجموعه‌ای از کلیدهای خصوصی را تولید می‌کند.

۳-۱۳

رمزگذاری کلید عمومی

public key encryption

رمزگذاری که با استفاده از یک رمز نامتقارن انجام می‌شود.

۳-۱۴

رشته

string

دنباله‌ای منظم از نمادها می‌باشد.

۳-۱۵

آماده‌سازی

set up

فرایندی که توسط آن پارامترهای سامانه برای یک الگوریتم IBE انتخاب می‌شوند.

۳-۱۶

الگوریتم آماده‌سازی

set up algorithm

فرایندی که کلید مخفی- اصلی و کلید عمومی- اصلی متناظر را به همراه بعضی از پارامترهای سامانه تولید می‌کند.

۳-۱۷

پارامترهای سامانه

system parameters

پارامترهایی برای محاسبات رمزنگاشتی بوده که شامل انتخاب طرح یا تابع رمزنگاشتی خاص از بین خانواده‌ای از طرح‌ها یا توابع رمزنگاشتی یا از بین خانواده‌ای از فضاهای ریاضی می‌باشند.

۳-۱۸

شخص ثالث معتمد

trusted third party

مرجع امنیتی یا نماینده او که از نظر فعالیت‌های مرتبط با امنیت مورد اعتماد طرف‌های دیگر می‌باشد.

۴ نمادها، کوته نوشت‌ها و توابع تبدیل

این بند فهرستی از نمادها،کوته نوشت‌ها و توابع تبدیل لازم را برای درک و/یا کاربرد بهتر استاندارد ارائه می‌دهد.

۴-۱ نمادها

$[a,\dots,b)$ مجموعه‌ای از اعداد صحیح $\{x: a \le x < b\}$

$\tilde{x} \oplus \tilde{y}$ اگر $\tilde{x}$ و $\tilde{y}$ رشته‌های بیتی/هشت‌تایی با طول یکسان باشند، عملیات یای‌انحصاری (XOR) بیتی دو رشته می‌باشد.

$\langle x1,\dots,xl \rangle$ چندتایی اعضا $x1,\dots,xl$

$\tilde{x} \| \tilde{y}$ اگر $\tilde{x}$ و $\tilde{y}$ رشته‌های بیتی/هشت‌تایی باشند، نتیجه الحاق دو رشته $\tilde{x}$ و $\tilde{y}$، رشته‌ای متشکل از $\tilde{x}$ بعد از $\tilde{y}$ است.

$\gcd(a,b)$ برای اعداد صحیح a و b، بزرگترین مقسوم علیه مشترک a و b، یعنی بزرگترین عدد صحیحی که هردو عدد a و b بر آن تقسیم می‌شوند (یا برابر با صفر اگر $a = b = 0$)

$a|b$ یک رابطه بین a و b که اگر و فقط اگر b بر a تقسیم‌پذیر باشد برقرار می‌شود یعنی عدد صحیح c وجود دارد به طوری‌که $b = ac$

$a \nmid b$ یک رابطه بین a و b که اگر و فقط اگر b بر a تقسیم پذیر نباشد برقرار می‌شود یعنی عدد صحیح c وجود ندارد که $b = ac$ شود.

$a \equiv b(\mathrm{mod}\ n)$ برای یک عدد صحیح مخالف صفر n، رابطه‌ای بین a و b که اگر و فقط اگر a به پیمانه n با b هم‌نهشت باشد برقرار می‌شود یعنی $n|(a-b)$

$a\ (\mathrm{mod}\ n)$ برای عدد صحیح a و عدد صحیح و مثبت n، عدد صحیح یکتای $r \in [0,\dots,n)$ وجود دارد به طوری که $r \in a\ (\mathrm{mod}\ n)$

$(\mathrm{mod}\ n)\,a^{-1}$ برای عدد صحیح a و عدد صحیح و مثبت n که $gcd(a,n) = 1$ عدد صحیح یکتای $b \in [0,\dots,n)$ وجود دارد به طوری که $ab \equiv 1\ (mod\ n)$

$GF(q)$ میدان متناهی با تعداد q عضو به طوری که q توانی از یک عدد اول است

$E / GF(q)$ یک خم بیضوی تعریف‌شده روی میدان $GF(q)$

$E(GF(q))$ گروه جمعی نقاط بر خم بیضوی $E / GF(q)$

$E(GF(q))[n]$ زیرگروهی از E(GF(q)) متشکل از همه نقاط با مرتبه n

$\#E(GF(q))$ تعداد نقاط خم بیضوی تعریف‌شده بر میدان $GF(q)$

۴-۲ کوته نوشت‌ها

CT متن رمز، یک رشته هشت‌تایی

DEM سازوکار کپسوله‌سازی داده‌ها

IBE رمزگذاری شناسه‌مبنا

IBhE رمزگذاری ترکیبی شناسه‌مبنا

ID رشته هشت‌تایی انحصارا مختص به یک رمزگشا

ID_b نمایش *ID* به شکل باینری

K کلید نشست برای DEM

κ پارامتر امنیتی

KEM سازوکار کپسوله‌سازی کلید

L برچسب، رشته‌ای هشت‌تایی

mpk کلید عمومی- اصلی IBE

Msg متن اصلی، رشته‌ای هشت‌تایی

Msg_b نمایش *Msg* به شکل باینری

msk کلید مخفی- اصلی IBE

Parms پارامترهای سامانه IBE

PKG مولد کلید خصوصی

Sk_{ID} کلید خصوصی متناظر با *ID* متعلق به IBE

۴-۳ توابع تبدیل

توابع تبدیل زیر در استاندارد ISO/IEC 18033-2 تعیین می‌شوند.

BS2IP تبدیل اولیه رشته بیتی به عدد صحیح

BS2OSP تبدیل اولیه رشته بیتی به رشته هشت‌تایی

EC2OSP تبدیل اولیه خم بیضوی به رشته هشت‌تایی

FE2OSP تبدیل اولیه عضو میدان به رشته هشت‌تایی

FE2IP تبدیل اولیه عضو میدان به عدد صحیح

I2BSP تبدیل اولیه عدد صحیح به رشته بیتی

I2OSP تبدیل اولیه عدد صحیح به رشته هشت‌تایی

OS2ECP تبدیل اولیه رشته هشت‌تایی به خم بیضوی

OS2FEP تبدیل اولیه رشته هشت‌تایی به عضو میدان

OS2IP تبدیل اولیه رشته هشت‌تایی به عدد صحیح

OS2BSP تبدیل اولیه رشته هشت‌تایی به رشته بیتی

Oct (m) هشت‌تایی که مقدار صحیح آن برابر با m می‌باشد

Len(n) تعداد بایت‌های عدد صحیح n

۵ تبدیل‌های رمزنگاشتی

۵-۱ کلیات

طرح‌هایی که در این استاندارد مشخص می‌شود از سه تبدیل رمزنگاشتی *IHF*1، *SHF*1 و *PHF*1 به شکل زیر استفاده می‌کنند. این تبدیل‌ها از توابع درهم‌ساز تعیین‌شده در استاندارد ISO/IEC 10118-3 استفاده می‌کنند.

۵-۲ تابع ***IHF*1**

*IHF*1 بر پایه چهار تابع درهم‌ساز یعنی SHA-224، SHA-256، SHA-384 می‌باشد که در استاندارد ISO/IEC 10118-3 تعیین شده‌اند. این تابع رشته بیت‌هایی را به عنوان ورودی دریافت کرده و عدد صحیحی را در محدوده‌ای مشخص، خروجی می‌دهد.

ورودی:

- رشته $str \in \{0,1\}^*$
- پارامتر امنیتی $\kappa \in \{112,128,192,256\}$
- عدد صحیح $n, 0 < n < 2^{4k}$

خروجی:

– عدد صحیح $v, 0 \le v < n$

عملیات: انجام مراحل زیر

الف – If $\kappa = 112$ then let H = SHA-224

else If $\kappa = 128$ then let H = SHA-256

else If $\kappa = 192$ then let H = SHA-384

else If $\kappa = 256$ then let H = SHA-512

ب – Let $h_0 = 2\kappa$ یک رشته بیتی تمام صفر با طول

پ- Let $t_1 = h_0 \,||\, str$

ت- Let $h_1 = H\ (t_1)$

ث- Let $v_1 = BS\ 2IP\ (h_1)$

ج- Let $t_2 = h_1 \,||\, str$

چ- Let $h_2 = H\ (t_2)$

ح- Let $a_2 = BS\ 2IP\ (h_2)$

خ- Let $v_2 = 2^{2k} v_1 + a_2$

د – صدور خروجی $v_2 \bmod n$

۵-۳ تابع *SHF1*

رشته‌ای n بیتی را برمی‌گرداند که بر پایه یک تابع درهم‌ساز رمزنگاشتی است که به یک رشته ورودی اعمال شده است.

ورودی:

– رشته $str \in \{0,1\}^*$

– پارامتر امنیتی $\kappa \in \{112,128,192,256\}$

– عدد صحیح $n, n > 0$

فرضیات: رشته str در دامنه مقادیر مجاز برای ورودی‌های تابع درهم‌ساز مرتبط است. عدد صحیح n دارای خصوصیتی است که $n \le 4\kappa$

خروجی:

- رشته $v \in \{0,1\}^n$

عملیات: استفاده از مراحل زیر

– Output $I2BSP\left(IHF1\left(str, 2^n, \kappa\right)\right)$

۵-۴ تابع *PHF1*

عضوی از یک گروه خم بیضوی $E(GF(q))[p]$ برای خم بیضوی ابرمنفرد $E/GF(q): y^2 = x^3 + b$ یا $E/GF(q): y^2 = x^3 + ax$ را برمی‌گرداند. انواع دیگری از خم‌های بیضوی زوج‌ساز-مساعد[1] وجود دارد که $PHF1$ برای آن‌ها مناسب نیست.

ورودی:

– رشته str به شکلی که $str \in \{0,1\}^*$

– پارامتر امنیتی $\kappa \in \{112,128,192,256\}$

– پرچم j با مقادیر دریافتی ۰ یا ۱ که خم بیضوی ابرمنفرد را تعیین می‌کند، برای $j = 0$ بیان‌گر خم $E/GF(q): y^2 = x^3 + b$ و برای $j = 1$ بیان‌گر خم بیضوی $E/GF(q): y^2 = x^3 + ax$ می‌باشد.

– عدد اول q به شکلی که اگر $j = 0$ باشد آن‌گاه $q = 2 \pmod 3$ است یا اگر $j = 1$ باشد آن‌گاه $q = 3 (mod\ 4)$ که میدان متناهی $GF(q)$ را تعریف می‌کند.

– اگر $j = 1$ باشد عدد صحیح $a, 0 < a < q$ یا اگر $j = 0$ باشد عدد صحیح $b, 0 < b < q$

– عدد اول p با $p \mid \#E(GF(q))$ و $p^2 \not\mid \#E(GF(q))$ برای خم بیضوی E که با پرچم j تعریف شده است.

خروجی:

– عضوی از $E(GF(q))[p]$ برای خم بیضوی منتخب

عملیات: استفاده از مراحل زیر

الف- Let $r = (q+1)/p$

1- Pairing-friendly

ب –

If $j = 0$ then

1- Let $y = IHF1(str, q, \kappa)$

2- Let $x = (y^2 - b)^{(2q-1)/3} \pmod q$

3- Let $J = (x, y)$

پ-

Else if $j = 1$

انجام مراحل زیر

1- Let $x = IHF1(str, q, \kappa)$

2- Let $z = x^3 + ax \pmod q$

3- If Jacobi symbol $(z/q) = +1$ then

- Let $y = z^{(q+1)/4} \pmod q$
- Let $J = (x, y)$

4- If Jacobi symbol (z/q) = -1 then

- Let $y = (-z)^{(q+1)/4} \pmod q$
- Let $J = (-x, y)$

ت -

Return rJ

۶ مدل کلی رمزگذاری شناسه‌مبنا

۶-۱ اجزای تشکیل‌دهنده الگوریتم‌ها

یک طرح رمزگذاری شناسه‌مبنا از چهار الگوریتم زیر تشکیل می‌شود.

IBE.Setup(κ) با دریافت پارامتر امنیتی κ، چندتایی $\langle parms, mpk, msk \rangle$ را تولید می‌کند، که *parms* به معنی پارامترهای سامانه، *msk* به معنی کلید مخفی- اصلی و *mpk* کلید عمومی- اصلی متناظر است.

IBE.Extract(parms,mpk,msk,ID) با دریافت کلید مخفی- اصلی *msk*، کلید عمومی- اصلی متناظر*mpk*، و رشته هشت‌تایی *ID*، به ازای *parms*، کلید خصوصی sk_{ID} را برای *ID* تولید می‌کند.

IBE.Enc (parms,mpk, ID, L,Msg) . با دریافت متن اصلی *Msg*، برچسب *L* و رشته هشت‌تایی *ID*، به ازای *parms* و *mpk*، رمزگذاری را بر *Msg* انجام داده و متن رمز *CT* را برای *ID* خروجی می‌دهد. توجه شود که *Msg*، *L* و *CT* رشته‌های هشت‌تایی هستند.

IBE.Dec (parms,mpk, ID, skID , L,CT) با دریافت کلید خصوصی sk_{ID} به ازای *parms*، *mpk*، *ID* و *L* متن رمز *CT* را رمزگشایی نموده و متن اصلی ضمنی را خروجی می‌دهد.

به طور کلی، الگوریتم‌های آماده‌سازی، استخراج کلید و رمزگذاری، الگوریتم‌هایی احتمالاتی هستند در حالیکه الگوریتم‌های رمزگشایی قطعی می‌باشند. توصیه می‌شود که کاربردها برای احراز هویت دسترسی به کلیدهای خصوصی، با استفاده از رشته *ID* به عنوان شناسه، روشی در یک سامانه احراز هویت مطمئن برقرار نمایند. توصیف احراز نمودن درخواست کلید به شکلی مفصل، خارج از هدف و دامنه کاربرد این استاندارد بوده اما برای امنیت یک کاربرد پیاده‌سازی‌شده، ضروری است.

یادآوری ۱- امنیت معنایی در برابر حمله متن رمز منتخب وفقی توسط انجمن‌های تحقیقات رمزنگاشتی به عنوان سطح مناسب امنیتی در نظر گرفته می‌شود که بهتر است یک سازوکار IBE ایفا نماید. هر سازوکار IBE که در این استاندارد توصیف شده است این سطح امنیتی را ایفا می‌کند. تعریف قراردادی این مفهوم امنیتی در پیوست ب شرح داده می‌شود.

یادآوری ۲- صحت، الزامی پایه برای هر سازوکار IBE می‌باشد. توصیه می‌شود برای هر زوج $ID\ /\ sk_{ID}$ و برای هر متن اصلی با طول معین، متن رمز متعلق به *ID* تحت کلید عمومی- اصلی و پارامترهای سامانه *ID*، با کلید خصوصی $ID\ /\ sk_{ID}$ تحت کلید عمومی- اصلی و پارامترهای سامانه *ID* قابل رمزگشایی به متن اصلی باشد. عدم پیروی از این الزام به شکلی که برای همه زوج $ID\ /\ sk_{ID}$ ها به جز بخش ناچیزی از آن‌ها برقرار شود مجاز است.

۶-۲ طول متن اصلی

سه نوع طول متن اصلی برای IBE به شرح زیر تعیین می‌شوند.

- یک IBE با نوع طول- متن اصلی- اختیاری، متون ساده با طول اختیاری را رمزگذاری می‌کند.
- یک IBE با نوع طول- متن اصلی- ثابت، صرفا متون ساده‌ای را رمزگذاری می‌نماید که طول آن‌ها (به هشت‌تایی) معادل با مقدار ثابت *IBE.MsgLen* باشد.
- یک IBE با نوع طول-متن اصلی- محدود صرفا متون ساده‌ای را رمزگذاری می‌کند که طول آن‌ها (به هشت‌تایی) کمتر از یا معادل با مقدار ثابت *IBE.MaxMsgLen(mpk)* باشد. در این حالت، حداکثر طول متن رمز ممکن است به پارامتر سامانه *mpk* وابسته باشد.

۶-۳ استفاده از برچسب‌ها

برچسب رشته‌ای هشت‌تایی است که مقدار آن توسط رمزگذاری و رمزگشایی استفاده می‌شود. ممکن است شامل داده‌هایی عمومی باشد که به صورت ضمنی از متن قابل درک بوده و نیازی به رمزگذاری نداشته باشد، اما با این وجود توصیه می‌شود به متن رمز الحاق نشود. یک برچسب رشته‌ای هشت‌تایی است که برای کاربردی که از طرح IBE استفاده می‌کند و کاربردی که مستقل از پیاده‌سازی طرح IBE باشند پراهمیت است. سه نوع IBE از نظر طول برچسب به شرح زیر تعیین می‌شود.

- IBE با طول-برچسب-اختیاری نوعی است که در آن الگوریتم‌های رمزگذاری و رمزگشایی، برچسب‌هایی با طول اختیاری می‌پذیرند.
- IBE با طول-برچسب-ثابت نوعی است که الگوریتم‌های رمزگذاری و رمزگشایی صرفا برچسب‌هایی را می‌پذیرند که طول آن‌ها (به هشت‌تایی) معادل با مقدار ثابت *IBE.LabelLen* می‌باشد.
- IBE با طول- برچسب- محدود نوعی است که در آن الگوریتم‌های رمزگذاری و رمزگشایی صرفا برچسب‌هایی را می‌پذیرند که طول آن‌ها (به هشت‌تایی) کمتراز یا معادل با مقدار ثابت *IBE.MaxLabelLen* باشد.

یادآوری- مفهوم سنتی امنیت در برابر یک حمله متن رمز منتخب وفقی در پیوست ب شرح داده می‌شود، به این منظور که با استدلال استنتاجی برای یک سازوکار IBE امن، توصیه می‌شود الگوریتم رمزگذاری برچسب را به متن رمز به شکلی تغییر پذیر متصل کند.

۶-۴ فرمت متن رمز

این قسمت از مجموعه استاندارد ISO/IEC 18033 فرمت متون رمز را برحسب رشته بیتی توصیف می‌کند، البته در صورت نیاز، یک پیاده‌سازی مجاز است متون رمز را با فرمت‌هایی متفاوت ذخیره و/یا انتقال دهد. علاوه بر این متون رمز توصیه‌شده ممکن است لزوما در فرایند رمزگذاری یا رمزگشایی ظاهر نشوند، زیرا ممکن است که تبدیل یک فرمت به فرمتی دیگر به تک فرایندهایی تجزیه شود که از نظر کارکردی معادل هستند.

یادآوری- توصیه کردن فرمتی برای متن رمز علاوه بر این‌که سبب افزایش تعامل‌پذیری می‌شود، به منظور ارائه مطالبات معنادار و استدلال در رابطه با امنیت یک IBE در برابر حملات متن رمز منتخب وفقی الزامی است.

۶-۵ عملیات IBE

در آماده‌سازی یک IBE، یک شخص ثالث معتمد کلید مخفی- اصلی، کلید عمومی- اصلی متناظر و پارامترهای سامانه را با کمک الگوریتم *IBE.Setup* تولید می‌کند و با حفظ کلید مخفی- اصلی نزد خود به شکل خصوصی، کلید عمومی- اصلی و پارامترهای سامانه را در اختیار عموم می‌گذارد. هنگامی که یک رمزگشا درخواست کلید خصوصی کند، صادر کننده کلید خصوصی، با کمک الگوریتم *IBE.Extract* و از طریق یک کانال امن، خروجی آن را به عنوان کلید خصوصی برای رمزگشا صادر می‌کند. رمزگذار، متن رمز را با اجرای الگوریتم *IBE.Enc* به ازای رشته شناسه رمزگشا محاسبه می‌کند. رمزگشا توسط اجرای *IBE.Dec* به ازای کلید خصوصی، متن اصلی را از متن رمز دریافتی استنتاج می‌کند.

سازوکارها و پروتکل‌های زیر خارج از هدف و دامنه کاربرد این استاندارد می‌باشند. برای طراحی عملیات مدیریت کلید به استاندارد ISO/IEC 11770 رجوع شود.

- پروتکلی برای فراهم نمودن کلید عمومی- اصلی و پارامترهای سامانه

– پروتکلی برای توزیع کلیدهای خصوصی برای رمزگشاها

– پروتکلی برای فراهم نمودن یک رشته شناسه در اختیار رمزگذارها

– سازوکاری برای ذخیره امن کلید مخفی- اصلی یا کلید خصوصی

– سازوکاری برای تصدیق کردن ارتباط بین یک کلید عمومی- اصلی یا پارامترهای سامانه و صادر کننده آن

هر کدام از سازوکارهای IBE تعیین‌شده در این استاندارد در واقع عضوی از خانواده سازوکارهای IBE هستند که تعیین خانواده سازوکارهای IBE در آن‌ها با گزینش یک IBE مشخص با انتخاب مقادیری خاص برای پارامترهای سامانه صورت می‌گیرد. قبل از تولید زوج کلید مخفی- اصلی/ کلید عمومی- اصلی برای یک سازوکار IBE که از میان خانواده‌ای از سازوکارها انتخاب شده است، توصیه می‌شود مقادیر مشخص پارامترهای سامانه برای خانواده انتخاب شوند. بسته به قراردادهای مورد استفاده برای کدگذاری کلیدهای عمومی– اصلی، بعضی از پارامترهای سامانه ممکن است در کدگذاری کلید عمومی– اصلی تعبیه شوند. این پارامترهای سامانه باید در عمرکاری کلید عمومی- اصلی ثابت باقی بمانند.

یادآوری- برای مثال، اگر یک سازوکار IBE برحسب یک تابع درهم‌ساز رمزنگاشتی نمایش داده شود، انتخاب تابع درهم‌ساز بهتر است یکبار و فقط یکبار در زمانی قبل از تولید زوج کلید مخفی- اصلی/ کلید عمومی- اصلی قطعی شود، و الگوریتم‌های رمزگذاری و رمزگشایی بهتر است از آن تابع درهم‌ساز در طول عمر کاری کلید عمومی– اصلی استفاده کنند. عدم برقراری این اصل نه تنها سبب عدم انطباق پیاده‌سازی می‌شود بلکه تجزیه و تحلیل امنیتی سازوکار را نامعتبر می‌کند، و در برخی حالات قادر است پیاده‌سازی را در معرض خطرات شدید امنیتی قرار دهد.

۷ مدل کلی رمزگذاری ترکیبی شناسه‌مبنا

۷-۱ کلیات

طرح رمزگذاری ترکیبی شناسه‌مبنا، برای رمزگذاری یک متن اصلی بزرگ با استفاده از مزایای طرح رمزگذاری شناسه‌مبنا استفاده می‌شود، که در آن به منظور رمزگذاری پیام حقیقی با استفاده از فنون متقارن رمزنگاشتی، از یک IBE برای رمزگذاری کلید رمزگشایی استفاده می‌شود. طرح رمزگذاری ترکیبی شناسه‌مبنا از دو قالب ساختاری سطح پایین‌تر تشکیل می‌شود: یک طرح کپسوله‌سازی کلید شناسه‌مبنا و یک طرح کپسوله‌سازی داده‌ها.

۷-۲ کپسوله‌سازی کلید شناسه‌مبنا

۷-۲-۱ ترکیب ساختاری الگوریتم‌ها

یک طرح کپسوله‌سازی کلید شناسه‌مبنا از چهار الگوریتم زیر تشکیل می‌شود

KEM.Setup(κ). با دریافت پارامتر امنیتی κ، چندتایی $\langle parms, mpk, msk \rangle$ را تولید می‌کند، که *parms* به معنی پارامترهای سامانه، *msk* به معنی کلید مخفی- اصلی و *mpk* کلید عمومی- اصلی متناظر است.

KEM.Extract (parms,mpk,msk,ID). با دریافت کلید مخفی- اصلی *msk*، کلید عمومی- اصلی متناظر، *mpk*، و یک رشته هشت‌تایی *ID*، به ازای *parms* کلید خصوصی sk_{ID} را برای *ID* تولید می‌کند.

KEM.Enc (parms,mpk,ID).با دریافت رشته هشت‌تایی *ID* به ازای *parms* و *mpk*، خروجی رشته هشت‌تایی K وتبدیل K به متن رمز CT_{KEM} را برای *ID* صادر می‌کند. توجه شود که CT_{KEM} رشته‌ای هشت‌تایی است.

KEM.Dec (parms,mpk,ID,sk_{ID}*,*CT_{KEM}*)*. با دریافت کلید خصوصی sk_{ID} به ازای *parms*، *mpk* و *ID*، متن رمز CT_{KEM} را رمزگشایی کرده و رشته هشت‌تایی ضمنی را خروجی می‌دهد.

در آماده‌سازی کلی، الگوریتم‌های استخراج و کپسوله‌سازی کلید، الگوریتم‌هایی احتمالاتی هستند. در حالی که الگوریتم خارج کردن از کپسوله‌سازی قطعی می‌باشد. الگوریتم خارج کردن از کپسوله‌سازی در بعضی شرایط با احتمالی قابل چشم‌پوشی مجاز به شکست است. طرح کپسوله‌سازی کلید عدد صحیح مثبت *KEM.KeyLen* را نیز مشخص می‌کند که طول کلید مخفی صادرشده به عنوان خروجی توسط *KEM.Enc* و *KEM.Dec* است.

یادآوری ۱- در پیوست ب سطح امنیت که توصیه می‌شود هر سازوکار کپسوله‌سازی کلید ضروری است برآورده کند شرح داده می‌شود.

یادآوری ۲- توصیه می‌شود هر سازوکار کپسوله‌سازی کلید خصوصیت درستی مشابه با خصوصیت درستی سازوکار IBE برآورده سازد: برای هر زوج ID / sk_{ID} و برای هر رشته هشت‌تایی K که طول آن در محدوده معین پیاده‌سازی‌اش می‌باشد، هر کپسوله‌سازی K که به ازای پارامترهای سامانه از پیش تعیین‌شده تحت یک *ID*، به ازای پارامترهای سامانه تحت *ID* به K اصلی رمزگشایی می‌شود. عدم پیروی از این الزام به صورتی که برای همه زوج ID / sk_{ID} ها به جز بخش ناچیزی از آن‌ها برقرار شود مجاز است.

۷-۲-۲ بی‌پیشوندی

سازوکار کپسوله‌سازی کلید باید خصوصیت زیر را نیز برآورده کند. توصیه می‌شود مجموعه همه خروجی‌های متن رمز ممکن برای الگوریتم رمزگذاری، زیر مجموعه‌ای از مجموعه رشته‌های هشت‌تایی کاندید باشد(که ممکن است به کلید عمومی وابسته باشد)، به شکلی که مجموعه منتخب بی پیشوند و عضوهای مجموعه منتخب به سادگی قابل شناسایی باشند(با معین بودن کلید عمومی یا کلید خصوصی)

۷-۳ کپسوله‌سازی داده‌ها

۷-۳-۱ ترکیب ساختاری الگوریتم‌ها

طرح کپسوله‌سازی داده‌ها از دو الگوریتم زیر تشکیل شده است:

الف- *DEM.Enc (K , L,Msg)* با دریافت K و L، رمزگذاری‌شده Msg را، CT_{DEM}، محاسبه می‌کند. توجه شود که Msg و CT_{DEM} رشته‌هایی هشت‌تایی و L و Msg به ترتیب مجازند طولی طبق زیر بندهای ۶-۳ و ۶-۲ داشته باشند.

ب- *DEM.Dec (K, L, CT_{DEM})* با دریافت رشته‌های هشت‌تایی K و L متن رمز CT_{DEM} را رمزگشایی کرده و متن اصلی ضمنی را خروجی می‌دهد.

اگر طول‌های L یا Msg از برخی محدودیت‌های معین پیاده‌سازی تجاوز نمایند (به میزان زیاد)، شکست الگوریتم رمزگذاری امکان‌پذیر است. تحت برخی شرایط الگوریتم رمزگشایی با احتمالی اجتناب‌پذیر قابل شکست است.

سازوکارهای کپسوله‌سازی مجاز داده‌ها، سازوکارهای رمزگذاری متقارنی هستند که در استاندارد ISO/IEC 18033-3 توصیف شده‌اند.

یادآوری- توصیه می‌شود الگوریتم‌های رمزگذاری و رمزگشایی قطعی بوده و الزامات درستی زیر را برآورده کنند: برای همه کلیدهای نشست،K، همه برچسب‌ها، L، و همه متون ساده، Msg، به طوری که L و Msg از محدودیت‌های پیاده‌سازی معین تجاوز نکنند و

پ- $DEM.Dec\left(K, L, DEM.Enc\left(K, L, Msg\right)\right) = Msg$

۷-۴ عملیات رمزگذاری ترکیبی شناسه‌مبنا

۷-۴-۱ پارامترهای سامانه

طرح رمزگذاری ترکیبی شناسه‌مبنا (کوتاه‌شده، IBhE)خانواده‌ای از طرح‌های IBE است که توسط پارامترهای سامانه زیر نمایش داده می‌شود:

– KEM: یک طرح کپسوله‌سازی کلید شناسه‌مبنا، طبق زیر بند ۷-۲

– DEM: یک طرح کپسوله‌سازی داده‌ها، طبق زیر بند ۷-۳

استفاده از هر نوع ترکیبی از KEM و DEM به شرطی که $KEM.KeyLen = DEM.KeyLen$ مجاز است.

یادآوری ۱- اگر DEM توسط سازوکار کپسوله‌سازی شناسه‌مبنا با طول- برچسب- ثابت، با برچسب‌هایی محدود به طول $DEM.LabelLen$ بیان شود، آن‌گاه IBhE سازوکار رمزگذاری شناسه‌مبنایی است با طول برچسب ثابت که $IBhE.LabelLen = DEM.LabelLen$

یادآوری ۲- اگر DEM توسط سازوکار کپسوله‌سازی شناسه‌مبنا با طول- متن اصلی- ثابت با متون ساده محدود به طول $DEM.MsgLen$ بیان شود، آن‌گاه IBhE سازوکار رمزگذاری شناسه‌مبنایی است با طول متن اصلی که $IBhE.MsgLen = DEM.MsgLen$

یادآوری ۳- برای همه مقادیر مجاز KEM، مقدار *KEM.KeyLen* پارامتر سامانه بوده که ممکن است به شکلی انتخاب شود که با *DEM.KeyLen* برابر باشد. بنابراین، همه ترکیبات مجاز احتمالی برای KEM و DEM با انتخاب پارامترهای مناسب سامانه امکان وقوع دارند.

۷-۴-۲ آماده‌سازی

الگوریتم آماده‌سازی برای IBhE مشابه با الگوریتم KEM ضمنی است. Let *parms* بیان‌گر پارامترهای سامانه و $\langle msk, mpk \rangle$ بیان‌گر زوج کلید اصلی-مخفی/کلید اصلی- عمومی است.

۷-۴-۳ استخراج کلید خصوصی

الگوریتم استخراج کلید خصوصی برای IBhE مشابه با الگوریتم KEM ضمنی است. Let sk_{ID} بیان‌گر کلید خصوصی متعلق به *ID* است.

۷-۴-۴ رمزگذاری

الگوریتم رمزگذاری *IBhE.Enc* کلید عمومی- اصلی *mpk*، برچسب *L* و متن اصلی *Msg* را همراه با پارامترهای سامانه به عنوان ورودی دریافت می‌کند. اجرای آن به صورت زیر است.

الف- محاسبه $\langle K, CT_{KEM} \rangle = KEM.Enc(parms, mpk, ID)$

ب- محاسبه $CT_{DEM} = DEM.Enc(K, L, Msg)$

پ- $\text{Set } CT = CT_{KEM} \| CT_{DEM}$

ت- صدور خروجی *CT*

۷-۴-۵ رمزگشایی

الگوریتم رمزگشایی *IBhE.Dec* کلیدخصوصی sk_{ID} رشته هشت‌تایی *ID*، برچسب *L* و متن رمز *CT* را همراه با پارامترهای سامانه *parms* دریافت می‌کند. اجرای آن به شکل زیر است:

الف- با استفاده از ویژگی بی‌پیشوندی متون رمز وابسته به KEM، *CT* را به $CT = CT_{KEM} \| CT_{DEM}$ تجزیه می‌کند که CT_{KEM} و CT_{DEM} رشته‌های هشت‌تایی هستند به صورتی که CT_{KEM} عضوی از مجموعه متون رمز کاندید محتمل وابسته به KEM است. اگر تجزیه *CT* امکان‌پذیر نباشد این مرحله مردود می‌شود.

ب- محاسبه $K = KEM.Dec(parms, mpk, ID, SK_{ID}, CT_{KEM})$

پ- محاسبه $Msg = DEM.Dec(K, L, CT_{DEM})$

ت- صدور خروجی *Msg*

یادآوری- امنیت در پیوست ب مطرح می‌شود. توجه شود که صرفا تا زمانی که KEM و DEM مشخصات امنیتی مناسب را برآورده سازند IBhE در برابر حملات متن رمز منتخب وفقی امن خواهد بود.

۸ سازوکار رمزگذاری شناسه‌مبنا

۸-۱ کلیات

در این بند سازوکار رمزگذاری شناسه‌مبنا شرح داده می‌شود تعیین این سازوکار به منظور استفاده از داده‌های اولیه زیر است. برای خم‌های ابر منفرد، تابع درهم ساز H_1 استفاده می‌شود اما برای خم‌های دیگر طرح‌هایی دیگر (احتمالا مشابه) برای درهم‌سازی یک رشته به یک نقطه ضروری است.

سازوکار با دریافت پارامتر امنیتی κ و پارامتر اندازه کلید δ نیازمند الگوریتم‌های زیر است:

الف- الگوریتمی برای تولید بیت تصادفی

- R_1 منبع مقادیر تصادفی در فضای $\{0,1\}^{\delta}$

ب- چهار تابع درهم‌ساز:

- $H_1:\{0,1\}^* \rightarrow G1$ که $H_1(s) = PHF1(s,\kappa,j,q,c,p)$ با مقدار j=0 بیان‌گر خم بیضوی $E/GF(q): y^2 = x^3 + cx$ و با مقدار j=1 بیان‌گر خم بیضوی $E/GF(q): y^2 = x^3 + c$ است و p عددی اول برای خم بیضوی E با پرچم j است که $p \mid \#E(GF(q))$ و $p^2 \nmid \#E(GF(q))$
- $H_2: G_3 \rightarrow \{0,1\}^{\delta}$ که $H_2(x) = SHF1(OS2BSP(z),\delta,k)$ و $z = FE2OSP(x)$
- $H_3: \{0,1\}^{\delta} \times \{0,1\}^{\delta} \rightarrow Z_p^*$ که $H_3(s_1,s_2) = IHF1(s_1 \| s_2, p-1, \kappa) + 1$
- $H_4: \{0,1\}^{\delta} \rightarrow \{0,1\}^{\delta}$ که $H_4(s) = SHF1(s,\delta,\kappa)$

۸-۲ سازوکار BF

۸-۲-۱ آماده‌سازی

عملیات آماده‌سازی، پارامترهای عمومی سامانه و کلید مخفی- اصلی را ایجاد می‌کند. نظر به این‌که همه کلیدهای مخفی محاسبه‌شده درون سامانه متکی به کلید مخفی- اصلی است، توصیه می‌شود امنیت کلید مخفی- اصلی توسط خود صادرکننده کلید خصوصی تامین شود. توصیه می‌شود که کاربردها برپایه اصولی منظم روشی برای تغییر کلید مخفی- اصلی، کلید عمومی- اصلی متناظر و پارامترهای سامانه برقرار کنند و روشی برای مدیریت آشکارسازی کلید مخفی- اصلی داشته باشند گرچه خارج از هدف و دامنه کاربرد این استاندارد است.

مراحل آماده‌سازی صادرکننده کلید خصوصی و پارامترهای سامانه به شرح زیر است:

الف – آماده‌سازی گروه‌های پایه G_1، G_2، G_3 و گروه‌های زوج‌ساز $e : G_1 \times G_2 \to G_3$. G_1 باید به شکل $E\ (GF\ (q))[p]$ باشد. که p و q اعداد اول هستند.

ب- انتخاب مولد تصادفی Q در G_2

پ- تولید تصادفی s مخفی- اصلی در Z_p^*. محاسبه R متناظر به شکل sQ

ت – آماده‌سازی پارامترهای سامانه و مجموعه کلید عمومی- اصلی $params = \langle Q, G_1, G_2, G_3, e \rangle$ و $mpk = R$. امن نمودن کلید مخفی- اصلی s

استاندارد ISO/IEC 15946-1 شامل توصیه‌هایی برای تولید گروه‌ها، مولدها و زوج‌سازهای گروه‌ها است.

۸-۲-۲ استخراج کلید خصوصی

عملیات استخراج یک رشته شناسه دلخواه ID_b را در $\{0,1\}^*$ اتخاذ کرده و کلید خصوصی متناظر sk_{ID} را در G_1 محاسبه می‌کند. الگوریتم محاسبه کلید خصوصی sk_{ID} که متناظر با رشته شناسه ID_b است طبق زیر است:

ورودی:

- پارامترهای سامانه $params = \langle Q, G_1, G_2, G_3, e \rangle$
- کلید عمومی- اصلی $mpk = R$
- کلید مخفی- اصلی $msk = s$
- یک رشته شناسه ID_b

خروجی:

- کلید خصوصی مشتق‌شده sk_{ID} که عنصری از G_1 است.

عملیات: استفاده از مراحل زیر به منظور محاسبه sk_{ID}

الف- محاسبه عنصر شناسه $M = H_1(ID_b)$

ب- Set $sk_{ID} = sM$

پ- Output sk_{ID}

می‌توان صحت مقدار sk_{ID} را با استفاده از الگوریتم زیر تصدیق نمود:

ورودی:

– پارامترهای سامانه $parms = \langle Q, G_1, G_2, G_3, e \rangle$

– کلید عمومی- اصلی $mpk = R$

– یک رشته شناسه ID_b

– کلید خصوصی متناظر $sk_{ID} = sM$

خروجی:

اگر sk_{ID} با $parms$، mpk و ID_b سازگار باشد صدور مقدار «معتبر» و در غیر این صورت صدور مقدار «نامعتبر»

عملیات: استفاده از مراحل زیر

الف– محاسبه عنصر شناسه $M = H_1(ID_b)$

ب– محاسبه $T_0 = e(sk_{ID}, Q)$

پ– محاسبه $T_1 = e(M, R)$

اگر $T_0 = T_1$ آن‌گاه صدور مقدار مقدار خروجی «معتبر»، در غیر این صورت صدور مقدار خروجی «نامعتبر»

۸-۲-۳ رمزگذاری

عملیات رمزگذاری یک رشته شناسه اختیاری ID_b را در $\{0,1\}^*$، یک پیام Msg_b با طول δ و کلید عمومی- اصلی $mpk = R$ را همراه با پارامترهای سامانه $parms$ اتخاذ می‌کند و پیام به متن رمز تبدیل‌شده CT را خروجی می‌دهد.

مراحل رمزگذاری پیام عبارتند از:

الف– محاسبه یک تصادفی‌ساز δ-بیتی، o ، با استفاده از R_1

ب– محاسبه عنصر شناسه $M = H_1(ID_b)$

پ- محاسبه $r = H_3(o, Msg_b)$.

ت- محاسبه $C_1 = rQ$.

ث- محاسبه $B = e(rM, R)$.

ج- محاسبه $C_2 = o \oplus H_2(B)$.

چ- محاسبه $C_3 = Msg_b \oplus H_4(o)$

ح- صدور خروجی $CT = \langle C_1, C_2, C_3 \rangle$

۸-۲-۴ رمزگشایی

عملیات رمزگشایی متن رمز CT را که برای شناسه ID محاسبه شده است، کلید خصوصی sk_{ID} که متناظر با ID است اتخاذ کرده و پیام Msg_b یا «خطا» را خروجی می‌دهد.

الف- تجزیه متن رمز CT به چندتایی $\langle C_1, C_2, C_3 \rangle$.

ب- محاسبه $B = e(sk_{ID}, C_1)$.

پ- محاسبه $o = C_2 \oplus H_2(B)$.

ت- محاسبه $Msg_b = C_3 \oplus H_4(o)$.

ث- محاسبه $r = H_3(o, Msg_b)$.

ج- بررسی برقراری $C_1 = rQ$ در غیر این صورت صادر کردن پیغام «خطا» و توقف.

چ- صدور خروجی Msg_b .

۹ سازوکارهای رمزگذاری ترکیبی شناسه‌مبنا

۹-۱ کلیات

در این بند دو سازوکار کپسوله‌سازی شناسه‌مبنا تعیین می‌شود. تعیین هر سازوکار به منظور استفاده از مقدمات زیر است.

سازوکار با دریافت پارامتر امنیتی κ و پارامتر اندازه کلید δ به الگوریتم‌های زیر نیاز دارد:

الف- الگوریتمی برای تولید بیت تصادفی

- R_1 مرجعی از مقادیر تصادفی در فضای $\{0,1\}^{\delta}$.

ب- سه تابع درهم‌ساز:

- $H_1 : \{0,1\}^* \to Z_p$ که $H_1(s) = IHF1(s, p, \kappa)$
- $H_2 : G_3 \to \{0,1\}^\delta$ که $H_2(x) = SHF1(OS2BSP(z), \delta, \kappa)$ و $z = FE2OSP(x)$
- $H_3 : \{0,1\}^* \to \{0,1\}^\delta$ که $H_3(s) = SHF1(s, \delta, \kappa)$

۹-۲ سازوکار کپسوله‌سازی کلید SK

۹-۲-۱ آماده‌سازی

عملیات آماده‌سازی پارامترهای عمومی سامانه و کلید مخفی- اصلی را ایجاد می‌کند. نظر به این‌که همه کلیدهای مخفی محاسبه‌شده درون سامانه متکی به کلید مخفی- اصلی است، توصیه می‌شود امنیت کلید مخفی- اصلی توسط خود صادر کننده کلید خصوصی تامین شود. توصیه می‌شود کاربردها روشی برای تغییر کلید مخفی- اصلی، کلید عمومی- اصلی متناظر و پارامترهای سامانه برپایه اصول منظم برقرار کنند و روشی برای مدیریت آشکارسازی کلید مخفی- اصلی داشته باشند گرچه خارج از هدف و دامنه کاربرد این استاندارد می‌باشد.

مراحل آماده‌سازی صادرکننده کلید خصوصی و پارامترهای سامانه به شرح زیر است.

الف- برقرار ساختن مجموعه گروه‌های پایه G_1،G_2،G_3 و گروه زوج‌ساز $e : G_1 \times G_2 \to G_3$. مرتبه هر گروه معادل با p است.

ب- انتخاب مولد تصادفی Q_1 در G_1 و مولد تصادفی Q_2 در G_2.

پ- تولید تصادفی s اصلی مخفی در Z_p^* . محاسبه R متناظر به شکل sQ_1

ت- محاسبه اولیه مقدار زوج‌ساز $J = e(Q_1, Q_2)$

ث-فراهم کردن پارامترهای سامانه و مجموعه کلید عمومی- اصلی $parms = \langle J, Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$ و $mpk = R$. امن نمودن کلید مخفی- اصلی s.

استاندارد ISO/IEC 15946-1 شامل توصیه‌هایی برای تولید گروه‌ها، مولدها و زوج‌سازهای گروه‌ها است.

۹-۲-۲ استخراج کلید خصوصی

عملیات استخراج رشته شناسه اختیاری ID_b را در $\{0,1\}^*$ اتخاذ کرده و کلید خصوصی متناظر sk_{ID} را در G_2 محاسبه می‌کند. الگوریتم محاسبه کلید خصوصی sk_{ID} به شرح زیر با یک رشته شناسه ID_b متناظر است:

ورودی:

– پارامترهای سامانه $parms = \langle J, Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$

– کلید عمومی- اصلی $mpk = R$

– کلید مخفی- اصلی $msk = s$

– یک رشته شناسه ID_b

خروجی:

– کلید خصوصی مشتق‌شده sk_{ID} که عنصری از G_2 است.

عملیات: استفاده از مراحل زیر به منظور محاسبه sk_{ID}

الف- محاسبه عضو شناسه $M = H_1(ID_b)$

ب- اگر $M + s \equiv 0$ به پیمانه p باشد، صدور خروجی «خطا» و توقف.

پ- محاسبه $t = (M + s)^{-1}$ به پیمانه p.

ت- محاسبه $sk_{ID} = tQ_2$.

ث- صدور خروجی sk_{ID}

صحت مقدار sk_{ID} با استفاده از الگوریتم زیر قابل تصدیق است:

ورودی:

– پارامترهای سامانه $parms = \langle J, Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$

– کلید عمومی- اصلی $mpk = R$

– یک رشته شناسه ID_b

کلید خصوصی متناظر sk_{ID}

خروجی:

– اگر sk_{ID} با $parms$، mpk و ID_b سازگار باشد مقدار «معتبر» و در غیر این صورت مقدار «نامعتبر»

عملیات: استفاده از مراحل زیر

الف- محاسبه رشته شناسه $M = H_1(ID_b)$

ب- محاسبه $T = e(MQ_1 + R, sk_{ID})$

پ- اگر $T = J$ باشد آن‌گاه صدور مقدار خروجی «معتبر»، در غیراین صورت صدور خروجی «نامعتبر»

۹-۲-۳ کپسوله‌سازی کلید نشست

عملیات کپسوله‌سازی رشته شناسه اختیاری ID_b را در $\{0,1\}^*$ و کلید عمومی- اصلی $mpk = \langle J, R, T \rangle$ را همراه با پارامترهای سامانه *parms* اتخاذ کرده و زوج $\langle K, CT_{KEM} \rangle$ را خروجی می‌دهد، که K کلید نشست مورد استفاده برای رمزگذاری پیام، و CT_{KEM}کپسوله‌سازی‌شده K جهت ارسال به دریافت‌کننده است.

محاسبه یک تصادفی‌ساز δ بیتی، m، با استفاده از R_1

الف- محاسبه $r = H_1(m)$

ب- محاسبه $E = r(MQ_1 + R)$

پ- محاسبه $B = H_2(J^r)$

ت- Set $CT_{KEM} = \langle E, B \oplus m \rangle$

ث- محاسبه $K = H_3(m)$

ج- صدور خروجی $\langle K, CT_{KEM} \rangle$

۹-۲-۴ خارج کردن کلید نشست از کپسوله‌سازی

عملیات خارج کردن از کپسوله مقدار کپسوله‌سازی‌شده CT_{KEM} را که برای شناسه ID محاسبه‌شده و کلید خصوصی K را که متناظر با ID است اتخاذ نموده، و مقدار کلید sk_{ID} را محاسبه می‌کند که می‌تواند برای رمزگشایی پیامی که توسط فرستنده رمزگذاری‌شده، استفاده شود.

مراحل محاسبه کلید خارج‌شده از کپسوله‌سازی عبارتند از:

الف- تجزیه مقدار کپسوله‌سازی‌شده CT_{KEM} به شکل چندتایی $\langle U, V \rangle$.

ب- محاسبه $B = H_2(e(U, sk_{ID}))$.

پ- محاسبه $m = B \oplus V$.

ت- محاسبه $r = H_1(m)$.

ث- محاسبه $Q = R + (H_1(ID_b).Q_1)$.

ج- تصدیق برقراری رابطه $U = rQ$. در غیر این صورت صدور پیغام «خطا» و توقف.

چ- صدور $K = H_3(m)$ به عنوان خروجی.

۹-۳ سازوکار کپسوله‌سازی کلید BB1

۹-۳-۱ آماده‌سازی

مراحل آماده‌سازی صادرکننده کلید خصوصی و پارامترهای سامانه عبارتند از:

الف- ایجاد کردن گروه‌های پایه G_1،G_2،G_3 و گروه‌های زوج‌ساز $e: G_1 \times G_2 \to G_3$. مرتبه هر گروه معادل با p است.

ب- انتخاب یک مولد اعداد تصادفی Q_1 در G_1 و یک مولد اعداد تصادفی Q_2 در G_2

پ- تولید تصادفی S_1، S_2 و S_3 مخفی- اصلی در Z_p^* . محاسبه R متناظر به شکل s_1Q_1 و T به شکل s_3Q_1

ت- محاسبه اولیه مقدار زوج‌ساز $J = e(s_1Q_1, s_2Q_2)$

ث- فراهم کردن پارامترهای سامانه و مجموعه کلید عمومی- اصلی $parms = \langle J, Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$ و $mpk = R$. امن کردن کلید مخفی- اصلی $\langle s_1, s_2, s_3 \rangle$

استاندارد ISO/IEC 15946-1 شامل توصیه‌هایی برای تولید گروه‌ها، مولدها و زوج‌سازهای گروه‌ها است.

۹-۳-۲ استخراج کلید خصوصی

عملیات استخراج رشته شناسه اختیاری ID_b را در $\{0,1\}^*$ اتخاذ کرده و عضوهای متناظرکلید خصوصی، $d_{ID,0} = tQ_2$ و $d_{ID,1} = rQ_2$، را در G_2 محاسبه می‌کند. الگوریتم محاسبه کلید خصوصی sk_{ID} متناظر با یک رشته شناسه ID_b به شرح زیر است:

- پارامترهای سامانه $parms = \langle Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$
- کلید عمومی- اصلی $mpk = \langle J, R, T \rangle$
- کلید مخفی- اصلی $msk = \langle s_1, s_2, s_3 \rangle$
- یک رشته شناسه ID_b

خروجی:

- کلید خصوصی مشتق‌شده sk_{ID} که زوجی از عضوهای G_2 است.

عملیات: استفاده از مراحل زیر به منظور محاسبه sk_{ID}

الف- محاسبه عضو شناسه $M = H_1(ID_b)$

ب- انتخاب عدد صحیح تصادفی r در Z_p^*

پ- محاسبه $t = s_1 s_2 + r(s_1 M + s_3)$ در Z_p. اگر $t = 0$ باشد برگشت به ب در غیر این صورت رفتن به ت.

ت- محاسبه $d_{ID,0} = tQ_2$

ث- محاسبه $d_{ID,1} = rQ_2$

ج- صدور خروجی $sk_{ID} = \langle d_{ID,0}, d_{ID,1} \rangle$

درستی sk_{ID} توسط الگوریتم زیر قابل تصدیق است.

ورودی:

- پارامترهای سامانه $parms = \langle Q_1, Q_2, G_1, G_2, G_3, e, p \rangle$
- کلید عمومی- اصلی $mpk = \langle J, R, T \rangle$
- رشته شناسه ID_b
- کلید خصوصی متناظر $sk_{ID} = \langle d_{ID,0}, d_{ID,1} \rangle$

خروجی:

- اگر sk_{ID} با $parms$، mpk و ID_b سازگار باشد صدور مقدار خروجی «معتبر» و در غیر این صورت صدور مقدار خروجی«نامعتبر»

عملیات: استفاده از مراحل زیر:

الف- محاسبه عضو شناسه $M = H_1(ID_b)$

ب- محاسبه $T_0 = e(Q_1, d_{ID,0})$

پ- محاسبه $T_1 = e(MR + T, d_{ID,1})$

ت- اگر $T_0 = T_1 J$ آن‌گاه صدور خروجی مقدار «معتبر»، در غیر این صورت صدور مقدار خروجی «نامعتبر»

۹-۳-۳ کپسوله‌سازی کلید نشست

عملیات کپسوله‌سازی رشته شناسه اختیاری ID_b را در $\{0,1\}^*$ و کلید عمومی- اصلی $mpk = \langle J, R, T \rangle$ را همراه با پارامترهای سامانه $parms$ اتخاذ کرده و زوج $\langle K, CT_{KEM} \rangle$ را خروجی می‌دهد، که K کلید نشست مورد استفاده برای رمزگذاری پیام، و CT_{KEM} کپسوله‌سازی‌شده K جهت ارسال به دریافت‌کننده است.

مراحل محاسبه مقادیر کپسوله‌سازی عبارتند از:

الف- محاسبه عنصر شناسه $M = H_1(ID_b)$

ب- محاسبه عدد صحیح تصادفی r' در Z_p^*

پ- محاسبه $E_0 = r'Q_1$

ت- محاسبه $E_1 = (r'M)R + r'T$

ث- محاسبه $B = J^{r'}$

ج- Set $CT_{KEM} = \langle E_0, E_1 \rangle$

چ- محاسبه $K = H_2(B)$

ح- صدور خروجی $\langle K, CT_{KEM} \rangle$

۹-۳-۴ خارج کردن کلید نشست از کپسوله

عملیات خارج کردن از کپسوله مقدار کپسوله‌سازی‌شده CT_{KEM} را که برای شناسه ID محاسبه‌شده و کلید خصوصی sk_{ID} که متناظر با ID می‌باشد را دریافت نموده و مقدار کلید K را محاسبه می‌کند که می‌تواند برای رمزگشایی پیامی که توسط فرستنده رمزگذاری‌شده است، استفاده شود.

مراحل محاسبه کلید خارج‌شده از کپسوله عبارتند از:

الف- تجزیه مقدار کپسوله‌سازی‌شده CT_{KEM} به شکل چندتایی $\langle U, V \rangle$

ب- محاسبه $B = e(U, d_{ID,0}) / e(V, d_{ID,1})$

پ- محاسبه $K = H_2(B)$

ت- صدور خروجی K

پیوست الف

(الزامی)

شناسه‌های شیء

این پیوست شناسه‌های شیء اختصاص یافته به سازوکارهای تعیین‌شده در این استاندارد را فهرست نمـوده و ساختار پارامترهای الگوریتم را تعیین می‌کند.

```
EncryptionAlgorithms-5 {
iso(1) standard(0) encryption-algorithms(18033) part5(5)
asn1-module(0) algorithm-object-identifiers(0)
}
DEFINITIONS EXPLICIT TAGS: := BEGIN
IMPORTS
HashFunction
FROM EncryptionAlgorithms-2 {
iso(1) standard(0) encryption-algorithms(18033) part2(2)
asn1-module(0) algorithm-object-identifiers(0) };
-- ID-based cipher mechanism identifiers --
OID: := OBJECT IDENTIFIER -- Alias --
is18033-5 OID: := { iso(1) standard(0) is18033(18033) part5(5) }
ib-enc OID: := { is18033-5 ib-encryption-mechanism(1) }
ib-kem OID: := { is18033-5 ib-key-encapsulation-mechanism(2) }
ib-enc-mechanism-bf OID: := { ib-enc bf(1) }
ib-kem-mechanism-sk OID: := { ib-kem sk(1) }
ib-kem-mechanism-bb1 OID: := { ib-kem bb1(2) }
-- Identity-based encryption mechanisms --
IbEncMechanismIdentifier: :=
AlgorithmIdentifier {{ IbEncMechanism }}
IbEncMechanism ALGORITHM: := {
{ OID ib-enc-mechanism-bf PARMS HashFunction },
... -- Expect additional IB-ENC mechanisms --
}
-- Identity-based key-encapsulation mechanisms --
IbKemMechanismIdentifier: :=
AlgorithmIdentifier {{ IbKemMechanism }}
```

```
IbKemMechanism ALGORITHM: := {
{ OID ib-kem-mechanism-sk PARMS HashFunction } |
{ OID ib-kem-mechanism-bb1 PARMS HashFunction },
... -- Expect additional IB-KEM mechanisms --
}
AlgorithmIdentifier { ALGORITHM:IOSet }: := SEQUENCE {
algorithm ALGORITHM.&id({IOSet}),
parameters ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
ALGORITHM: := CLASS {
&id OBJECT IDENTIFIER UNIQUE,
&Type OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }
END -- EncryptionAlgorithms-5 --
```

پیوست ب

(الزامی)

ملاحظات امنیتی

همه سازوکارهای تعیین‌شده در این استاندارد خصوصیتی را برآورده می‌کنند، که *امنیت متن رمز منتخب* نامیده می‌شود. این مفهوم امنیتی به عنوان یکی از قوی‌ترین مفاهیم برای سازوکار رمزگذاری کلید عمومی در نظر گرفته می‌شود. تجزیه و تحلیل امنیتی سازوکارهای BF، SK و BB1 به ترتیب در منابع [4]، [5] و [3] کتاب‌نامه آمده است.

پیوست پ

(الزامی)

مثال‌های عددی

در این پیوست، همه مقادیر به مبنای ۱۶ نشان داده می‌شوند مگر آن که صریحا ذکر شده باشد.

پ-۱ سازوکار رمزگذاری ID-مبنای BF

پ-۱-۱ مثال۱

پ-۱-۱-۱ آماده‌سازی

این مثال از خم بیضوی $y^2 = x^3 + 1$ که در استاندارد ملی ایران شماره INSO-IEC14888-3: سال ۱۳۹۱ به شکل یکسان به‌کار رفته است، استفاده می‌کند. یک عضو در $GF(q^2)$ به شکل $a + b\sigma$ نشان داده می‌شود که در آن a و b عضوهایی در $GF(q)$ و σ عضوی در $GF(q^2)$ است که در رابطه $\sigma^2 + 1 \equiv 0$ صدق می‌کند. از نگاشت اعوجاج به منظور تبدیل نقطه‌ای در یک گروه پیچش به عضوی از یک گروه پیچش دیگر جهت حصول غیر تبهگنی زوج‌سازها طبق زیر استفاده می‌شود:

$\varphi(Q) = \varphi(Q_x, Q_y) = (\beta Q_x, Q_y)$ که در آن $\beta \neq 1$ عضوی در $GF(q^2)$ است که در رابطه $\beta^3 - 1 = 0 \pmod q$ صدق می‌کند. زوج‌سازی دوخطی $e(P, Q)$ به شکل زوج‌سازی ویل بر دو نقطه ورودی P و $\varphi(Q)$ پیاده‌سازی می‌شود.

H_1 طبق زیر پیاده‌سازی می‌شود.

قراردهی q به عنوان عددی اول که به ازای عدد صحیح c و $p > 3$ در رابطه‌های $q = 2 \pmod 3$ و $q = cp - 1$ صدق می‌کند. قراردهی $E(GF(q))$ به عنوان خم بیضوی $y^2 = x^3 + 1$ و قراردهی G_1 به عنوان $E(GF(q))[p]$. قراردهی رشته بیتی str به عنوان ورودی H_1. سپس، محاسبه خروجی $P_{str} \in G_1$ طبق مراحل زیر:

۱. let $y_0 = IHF1(str, q, \kappa)$

۲. let $X_0 = (y_0^2 - 1)^{(2q-1)/3} \bmod q$

۳. let $J = (x_0, y_0) \in G_1$

۴. let $P_{str} = cJ$

q = b35fa5fd e47fa1ab bb1e57e9 3ba1ff96 38b89b99 5c49be81 a38e3194 a0983816
4ee51fb9 1d285832 f9a05d63 9c8d9680 10c93a35 27e561f2 fd6a45cc 70aba1fb
p= 80000000 000fffff ffffffff ffffffff ffffffff
Qx= 7ee6f118 9329adb4 1e8cd405 2295f1a7 6096631d f065dd38 85fff26b 8ed52022
7bfc3f3d
07fe9cfe 093424ba 9dbd4c0d 73fff367 3ce2c922 f0b73c50 2992093b
Qy= 67c855c9 e6b617be b24b792a e9c3e21e 95f37006 25b91058 3bc0b293 c36a762c
feba4266 038989cc 59797235 c6116d99 8a97b805 ff82c664 53720e5c 1de95e3e
s = 56e84bdc e3d76405 33612345 d6bf0725 fb7d0391
Rx= 2141437a ca95b5d1 15a11812 e779233f 2b6470d2 4678738e 95960498 10e5147a
b75daceb 299b1b4c cacfe4df 597b3d0d cb488876 36477353 562cfb8c 56bf6a6d
Ry= 1c101269 0b92fd0f 2a89a3ea 10037022 ac696e28 50123794 e0b218d3 53214505
1f669aa4 4d363612 1b54bc4f 0166e667 9a3797e8 25aca54c fbc62c7e 3e881b86

k = 256 (decimal)

پ-۱-۱-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb = 73633237 7767322d 73656372 65746172 79406970 612e676f 2e6a70
Mx = 22223f9c 4aeaf934 723d739b 6e6ea3ea ea6d1aaa b3581de8 bff77695 5a6d4327
175b44d5 0ea32c59 26fa3a1c 028ebad1 fc1b6988 701be579 9b3d6a01 b3e85c67
My = 073113c6 6fb31cb0 1c12b0f0 18ca7993 428a309c 7f6f54d5 d51651af 4ad2c829
6e5ac712 9854a077 8d8f3576 f5b56505 47fbd7bc a8c9aaa4 85a9a8a8 58175395
skIDx= 775fb86b a773f24a a32d569b aac7d4f8 2c1d99ae 9432eed5 df746842 588d053d
6b195f49 55dbcd64 84424dc8 fa6f9d6e c44ea1e4 84ed9190 fdd38fea 959eb706
skIDy= 8fba3ae1 140e919f b19b40ed c0dfe6de b47f8e9b b87e86d3 e1b12ee3 9c73489a
95e17dc3 9bb26224 8373a5e9 6dabb9f8 ba4d1ca7 884320ad 2f35c6bb a30dc698
T0.a= 4c1e2713 096f15b9 030f00f9 2bced161 dce0fd0c 66ff94d7 c57e2c85 87037e3b
8c1ed769 2f96d79d 174ca761 552ed0f7 fb5af4a1 5d987bb7 53d169aa a36edecb
T0.b= aede1726 13721ee2 4b54800e f8339e71 075d6fb0 4e68294e f066937c 71f5d69d
cb05d4f6 eb2e5d2a bcfcf174 251acfe3 a85aac0a 460b8836 252d1cc1 f81d8a53
T1.a= 4c1e2713 096f15b9 030f00f9 2bced161 dce0fd0c 66ff94d7 c57e2c85 87037e3b
8c1ed769 2f96d79d 174ca761 552ed0f7 fb5af4a1 5d987bb7 53d169aa a36edecb
T1.b= aede1726 13721ee2 4b54800e f8339e71 075d6fb0 4e68294e f066937c 71f5d69d
cb05d4f6 eb2e5d2a bcfcf174 251acfe3 a85aac0a 460b8836 252d1cc1 f81d8a53

Private key skID is valid.

پ-۱-۱-۳ رمزگذاری

Message length: 896 bits

Msgb= 01234567 89abcdef fedcba98 76543210 00112233 44556677 8899aabb ccddeeff
ffeeddcc bbaa9988 77665544 33221100 00001111 22223333 44445555 66667777
88889999 aaaabbbb ccccdddd eeeeffff ffffeeee ddddcccc bbbbaaaa 99998888
77776666 55554444 33332222 11110000
o = 32733aa5 cc085739 74f52a96 ec181a31 97f8fe02 95525b0b 4a69970f 7b631732
0e96b2e1 044c43ad e3b8c68f 3c59d046 f852e0b9 f35e892a cb837a85 ce4ae9e1
26ae3344 a1552cf3 8e523462 05f7e4ab e2aa88a5 41d5f886 9bce6c6f 3d8874bb
bf845027 ef68509c fd7f64bd 7801b627
r = 647ed607 923a6589 a90c3b48 40a1e4e7 599d86a7

C1x=	96e2f727	7af63756	cb34e4e5	13b6fee9	9be157e9	0bc69ab8	cf08902a	5f5e3fdb
a0d57c4e	09ab41b0	ece23b70	86e51ea0	0f10c7c5	d96b7a63	e6676c0a	faa1b5ea	
C1y=	a8ab6927	c7c9a15f	568d8b4c	2e30b431	c46629a6	7ea67551	a5809192	ac970935
d5882644	0f870256	bc1ee3a3	8559ad9f	f60ba485	80c22a8e	892bf3de	b738cf14	
rMx=	98013221	69e44256	bec7edd8	347dbf84	e245ba0e	4a745eb2	85834b66	45eab3b5
d9bddb0f	a7ace4b5	8d244f14	d61b6e2c	c4f41b79	2a1c5911	a31107e2	ab598c00	
rMy=	69f22e4f	b551efa8	26521a1e	aabaa1e9	f152c847	7caba380	fe3fcbd2	943fe0ae
cd6d3c29	ea2a9073	11a5ce17	f6aa86a0	e75ff57b	129bc971	e70a5c02	35bd1529	
B.a=	5888c21f	f767d71a	0cbad876	f96afab8	2a7b6fbe	c00fbb9b	ce1baaec	5aaedcc2
928f8ad0	0773746d	063d4b94	d40deee1	de33ea8f	03db24a6	972ee8bc	1aeaae28	
B.b=	2558dcb1	707636c4	5006c3ca	75d57740	62f5ecd4	327cb97a	e79e9566	89f1e6f7
0f71fd1c	68614416	b277d756	f3f07109	6415d6c0	88cb221b	c1757f8c	3c74e59f	

Within H2: z = FE2OSP(B)= I2OSP(B.a+(B.b)q, 128)

z=	1a2b1681	47e1a03b	6192811f	d8fe8e6f	f04e0035	f2f3057d	2dcedb32	68e180d8
4a82957c	056d4767	b917551a	91d7f071	bdba0b18	588125c7	130866b2	0fe00ab0	
f8e2c79b	4901d3c2	827a30e0	c3c7c9df	eace492f	b30f77dc	4488f2bd	d53feb3b	
5e4f2cc3	c0bafa58	0327c7ef	5c122321	cfffd9e1	1f36fa80	9d9a857f	d725d00d	
C2=	ea671342	3816ba62	e4d08601	a9b292b9	7f4e49ac	f65ca5ff	f7fa6f41	de227ed9
9f1bd16d	85c29f3f	15d2904e	2af8f5e7	74ac6996	61bb138b	74850241	9fab2cf5	
d589270e	5eca6437	c3970aca	be44b202	ae70211d	6058e745	21c33892	520c9671	
eb1c795c	f77430d0	e23642ec	73d9d00e					
C3=	8368728c	9d4ae8b6	434a961b	494c25c7	36159933	3701e330	e64111a8	0829368e
7e9c5a00	cd4789dd	f4c3722b	76682199	a2cf7e1b	2cf49dae	ce51cd74	2dc621f7	
9127bbec	5d44c2bd	9a6b6415	f4172ac8	1927932c	533e5962	dedc558b	32a3dbaa	
b8d1c25b	9c433a02	9492e100	66f4d9c8					

Encryption completed.

پ-۱-۱-۴ رمزگشایی

B.a=	5888c21f	f767d71a	0cbad876	f96afab8	2a7b6fbe	c00fbb9b	ce1baaec	5aaedcc2
928f8ad0	0773746d	063d4b94	d40deee1	de33ea8f	03db24a6	972ee8bc	1aeaae28	
B.b=	2558dcb1	707636c4	5006c3ca	75d57740	62f5ecd4	327cb97a	e79e9566	89f1e6f7
0f71fd1c	68614416	b277d756	f3f07109	6415d6c0	88cb221b	c1757f8c	3c74e59f	
o=	32733aa5	cc085739	74f52a96	ec181a31	97f8fe02	95525b0b	4a69970f	7b631732
0e96b2e1	044c43ad	e3b8c68f	3c59d046	f852e0b9	f35e892a	cb837a85	ce4ae9e1	
26ae3344	a1552cf3	8e523462	05f7e4ab	e2aa88a5	41d5f886	9bce6c6f	3d8874bb	
bf845027	ef68509c	fd7f64bd	7801b627					
r=	647ed607	923a6589	a90c3b48	40a1e4e7	599d86a7			
Msgb=	01234567	89abcdef	fedcba98	76543210	00112233	44556677	8899aabb	ccddeeff
ffeeddcc	bbaa9988	77665544	33221100	00001111	22223333	44445555	66667777	
88889999	aaaabbbb	ccccdddd	eeeeffff	ffffeeee	ddddcccc	bbbbaaaa	99998888	
77776666	55554444	33332222	11110000					

Decryption successful.

پ-۱-۲ مثال۲

پ-۱-۲-۱ آماده‌سازی

این مثال طبق زیر بند پ-۱-۱ پیوست پ از خم بیضوی یکسان $y^2 = x^3 + 1$ و H_1 استفاده می‌کند. زوج‌سازی دوخطی $e(P, Q)$ به صورت زوج‌سازی تیت کاهش‌یافته بر دونقطه ورودی P و $\varphi(Q)$ پیاده‌سازی می‌شود.

q=	b35fa5fd	e47fa1ab	bb1e57e9	3ba1ff96	38b89b99	5c49be81	a38e3194	a0983816

4ee51fb9	1d285832	f9a05d63	9c8d9680	10c93a35	27e561f2	fd6a45cc	70aba1fb	
p=	80000000	000fffff	ffffffff	ffffffff	ffffffff			
Qx=	7ee6f118	9329adb4	1e8cd405	2295f1a7	6096631d	f065dd38	85fff26b	8ed52022
7bfc3f3d	07fe9cfe	093424ba	9dbd4c0d	73fff367	3ce2c922	f0b73c50	2992093b	
Qy=	67c855c9	e6b617be	b24b792a	e9c3e21e	95f37006	25b91058	3bc0b293	c36a762c
feba4266	038989cc	59797235	c6116d99	8a97b805	ff82c664	53720e5c	1de95e3e	
s=	56e84bdc	e3d76405	33612345	d6bf0725	fb7d0391			
Rx=	2141437a	ca95b5d1	15a11812	e779233f	2b6470d2	4678738e	95960498	10e5147a
b75daceb	299b1b4c	cacfe4df	597b3d0d	cb488876	36477353	562cfb8c	56bf6a6d	
Ry=	1c101269	0b92fd0f	2a89a3ea	10037022	ac696e28	50123794	e0b218d3	53214505
1f669aa4	4d363612	1b54bc4f	0166e667	9a3797e8	25aca54c	fbc62c7e	3e881b86	

k = 256 (decimal)

پ-۱-۲-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

ID_b=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
Mx=	22223f9c	4aeaf934	723d739b	6e6ea3ea	ea6d1aaa	b3581de8	bff77695	5a6d4327
175b44d5	0ea32c59	26fa3a1c	028ebad1	fc1b6988	701be579	9b3d6a01	b3e85c67	
My=	073113c6	6fb31cb0	1c12b0f0	18ca7993	428a309c	7f6f54d5	d51651af	4ad2c829
6e5ac712	9854a077	8d8f3576	f5b56505	47fbd7bc	a8c9aaa4	85a9a8a8	58175395	
$skID_x$=	775fb86b	a773f24a	a32d569b	aac7d4f8	2c1d99ae	9432eed5	df746842	588d053d
6b195f49	55dbcd64	84424dc8	fa6f9d6e	c44ea1e4	84ed9190	fdd38fea	959eb706	
skIDy=	8fba3ae1	140e919f	b19b40ed	c0dfe6de	b47f8e9b	b87e86d3	e1b12ee3	9c73489a
95e17dc3	9bb26224	8373a5e9	6dabb9f8	ba4d1ca7	884320ad	2f35c6bb	a30dc698	
T0.a=	124f0489	e46f7973	0a223780	0ceaf462	943f38b7	00d8ccc0	9cc3bc2d	61283841
2fc946d4	3a4762b1	0f7e9388	35c7008a	d3e5e85e	edfd8d74	11b5ca21	67fb1ad0	
T0.b=	3374b3b6	f2547afc	0110f8e4	f4e2e852	d6239287	ae277fc5	44f088b8	905fd5b9
aa65fb79	3c96d719	0b1f7c29	f2801344	6f527d87	222cdcec	de6e8755	5c17d719	
T1.a=	124f0489	e46f7973	0a223780	0ceaf462	943f38b7	00d8ccc0	9cc3bc2d	61283841
2fc946d4	3a4762b1	0f7e9388	35c7008a	d3e5e85e	edfd8d74	11b5ca21	67fb1ad0	
T1.b=	3374b3b6	f2547afc	0110f8e4	f4e2e852	d6239287	ae277fc5	44f088b8	905fd5b9
aa65fb79	3c96d719	0b1f7c29	f2801344	6f527d87	222cdcec	de6e8755	5c17d719	

Private key skID is valid.

پ-۱-۲-۳ رمزگذاری

Message length: 896 bits

Msgb=	01234567	89abcdef	fedcba98	76543210	00112233	44556677	8899aabb	ccddeeff
ffeeddcc	bbaa9988	77665544	33221100	00001111	22223333	44445555	66667777	
88889999	aaaabbbb	ccccdddd	eeeeffff	ffffeeee	ddddcccc	bbbbaaaa	99998888	
77776666	55554444	33332222	11110000					
o=	2ef53f26	046cd174	81063fd8	1fcf7ee6	9009b433	b31f0c69	12a57558	11a25d1e
63ee9a33	8da3f2fd	99a04c76	d53c444f	2ef28fb9	44dfdcb1	0edcb29b	86dc2fa3	
bb0938f0	70109f78	08ae5e34	9cf3e92f	36709fda	d10c5049	f9d0d2c4	fd382266	
ac748d2b	4d02151d	c7d1e4c3	5763445f					
r=	5bbf2159	d859b329	cade07e3	8f9bfe51	3a41b396			
C1x=	023debf1	52cbe5cd	efadbd31	65765e0c	627ba725	00fcf66f	008c9aa2	655e3c09
241e2655	c50e677f	31162635	0cc84cce	cdd3777f	91905f8f	c0126061	785208f3	
C1y=	4df18cfe	ec316138	57a4aeba	d1c8a2e2	6f809f27	02f30dd9	09070bfd	39ba19d6
b092560d	9bfd967d	30ff6740	3af0520b	10eb138c	0c634c4a	93e377aa	cab53fe0	
rMx=	5abbf3f2	5fac96f5	c75d3795	0fa58a2f	8db666e9	1146b2d8	aad3c26c	0f2c408b
9e485d95	e7308ee8	adf9bd22	a496c60e	16909aeb	48d7e9ca	cae7d420	c7091b42	

rMy=	0abfbc77	468e16fa	3c6045e4	6d385487	65278b9a	2a6545ad	6665c146	9a69a2c1
95ac55a4	51cc879a	17ae67ed	8569a72a	048c14fe	6e0b124a	7396c99b	05d9c8fa	
B.a=	a5ca565a	b0b9e928	d1cda8da	25368ea5	1fcc27b3	3d9d429c	830f2b33	f850ba9c
210d59a2	cc97d5b8	fb5aedbd	1a1255bb	48dcd725	67cd0633	296dcae1	2b28e881	
B.b=	27845eb3	990ad135	668e6899	3564ed1a	da6d61f4	b5f59c4a	212fbd06	5f85ea78
9efd69a5	e1a0cf8a	94c72896	1393adcc	fa949c5f	1ee5baa2	826d1c5c	06782ab1	

Within H2: z = FE2OSP(B)= I2OSP(B.a+(B.b)q, 128)

z=	1bb051f6	3ac94c65	e351f306	bcae1f21	79b5f4af	eafed6d0	66227391	6f63a669
3d7f443c	5b621e7b	3fd8cfd8	b1808de1	6f417b2d	d79a637f	f71dcf92	52dc503e	
526764c9	f0239a22	306137bb	e66e65ff	51e21312	af7b634d	fd87af60	6fa2c67e	
60220dae	afb18021	5b880b7b	2797caad	183e32e3	c6395632	0319182b	0a0f150c	
C2=	8cc39c03	8facb65e	01e8970e	45de4fca	26486afb	2d2a7148	f09f733e	e6db8ac2
0c7004bf	e0a5a6f7	8ecd91a5	a0d7e25e	e34be7c0	2c1ec62c	328b9296	56ffb635	
3bf28bea	364085a3	b90b3305	a2acc06b	9ccff4d6	ed3e97e9	141820f6	a8d34c88	
4cb8df34	91079724	083db54e	4ba0de15					
C3=	f998848b	2c735001	19985202	ec285a6b	22cdb577	e6959fa2	ac6058c6	0da4c5d1
38035c1b	aaa4e33a	950a467a	c660af5a	053c5852	065906ba	39f842dc	6ee90807	
1b55497a	84c3cfb4	25a5b235	8c23712e	3c28c1de	200f9c9b	d0bc1dd1	e21a0fe0	
431718b7	58151e83	923151d7	9d982d61					

Encryption completed.

پ-۱-۲-۴ رمزگشایی

B.a=	a5ca565a	b0b9e928	d1cda8da	25368ea5	1fcc27b3	3d9d429c	830f2b33	f850ba9c
210d59a2	cc97d5b8	fb5aedbd	1a1255bb	48dcd725	67cd0633	296dcae1	2b28e881	
B.b=	27845eb3	990ad135	668e6899	3564ed1a	da6d61f4	b5f59c4a	212fbd06	5f85ea78
9efd69a5	e1a0cf8a	94c72896	1393adcc	fa949c5f	1ee5baa2	826d1c5c	06782ab1	
o=	2ef53f26	046cd174	81063fd8	1fcf7ee6	9009b433	b31f0c69	12a57558	11a25d1e
63ee9a33	8da3f2fd	99a04c76	d53c444f	2ef28fb9	44dfdcb1	0edcb29b	86dc2fa3	
bb0938f0	70109f78	08ae5e34	9cf3e92f	36709fda	d10c5049	f9d0d2c4	fd382266	
ac748d2b	4d02151d	c7d1e4c3	5763445f					
r=	5bbf2159	d859b329	cade07e3	8f9bfe51	3a41b396			
Msgb=	01234567	89abcdef	fedcba98	76543210	00112233	44556677	8899aabb	ccddeeff
ffeeddcc	bbaa9988	77665544	33221100	00001111	22223333	44445555	66667777	
88889999	aaaabbbb	ccccdddd	eeeeffff	ffffeeee	ddddcccc	bbbbaaaa	99998888	
77776666	55554444	33332222	11110000					

Decryption successful.

پ-۲ سازوکار کپسوله‌سازی مبتنی بر کلید SK_{ID}

پ-۲-۱ مثال ۱

پ-۲-۱-۱ راه اندازی

این مثال از خم بیضوی $y^2 = x^3 + 1$ که در استاندارد ملی ایران شماره INSO-IEC14888-3: سال ۱۳۹۱ به شکل یکسان به‌کار رفته استفاده می‌کند. یک عضو در $GF(q^2)$ به شکل $a + b\sigma$ نشان داده می‌شود که در آن a و b عضوهایی در $GF(q)$ و σ عضوی در $GF(q^2)$ است که در رابطه $\sigma^2 + 1 \equiv 0$ صدق می‌کند. از نگاشت اعوجاج به منظور تبدیل نقطه‌ای در یک گروه پیچش به عضوی از یک گروه پیچش دیگر جهت حصول غیر تبهگنی زوج‌سازها طبق زیر استفاده می‌شود:

$\varphi(Q) = \varphi(Q_x, Q_y) = (-Q_x, \sigma Q_y)$. زوج‌سازی دوخطی $e(P, Q)$ به شکل زوج‌سازی ویل بر دو نقطه ورودی P و $\varphi(Q)$ پیاده‌سازی می‌شود.

H_1 طبق زیر پیاده‌سازی می‌شود.

q=	80000000	00000000	00000000	00000000	00020001	40000000	00000000	00000000
00000000	00010000	80000002	00000000	00000000	00000000	00000000	00080003	
p=	80000000	00000000	00000000	00000000	00020001			
Q1x=	0db4e0f7	22dd090d	a2b6d8fe	adaf21d9	546ab265	1515af9b	a87108f3	4e1ae0e3
eb132c10	81452cc1	e52bb2a7	4287a0cb	d8ff8dd9	3a225641	5321f0e4	c8892a50	
Q1y=	762c096c	49f1ab04	7d7f37de	537a4e7c	2991c400	22e0c9a9	b3f58b1b	9df4f28a
4a4330e2	170e14d2	f55a0719	8b667d0b	01e5a482	3f07e921	8516481e	641970ac	
Q2x=	6b8f666b	cf6b4672	d4634753	1f734e71	41bcd5fd	125f3ef3	714edc28	f6426900
75ffb5f7	9e745cc0	fb03f940	3bdcefe8	acbe6286	d5d9955c	2a0e5ed7	657748c6	
Q2y=	69584e47	f3070fed	9800d6cd	e0f314b4	03955126	1c5bfef6	f3595f94	5958f7d9
34dcbd3d	63125410	ccd363f8	02df1c7e	4a3d7ac7	24cf3865	0fb16ec1	7bb30a85	
s=	37e28416	c95170c9	46ebfb30	3e422717	191b4b73			
Rx=	76c25ec0	08bc4246	263d5078	c4846a7c	a68469cf	ed65108b	bb5c5ce4	5d3597d6
fe9a2b60	17a1f7db	2f7561ef	fd2f72d9	0b7445b7	4d648674	8da13ac0	c34788bb	
Ry=	4b913c48	0cc4d1c7	04e6d7ed	9424d4bc	2a532cd3	fbac55fe	6009d92f	39c2571b
3bf0d363	29a6b810	8a0fc795	829a3cca	91472f29	5df5bdc6	219648b6	8aba737f	
J.a=	56adfd18	df69d7ac	c91f60a6	aa9620e2	482d9266	0d35fa24	ee29de58	2fb201eb
5e4fd96e	e646befc	9bd16125	265458cb	0043806e	c4b3e2b6	297d5741	a8198d71	
J.b=	65a05adc	1528b2bd	44508723	7d386249	cec79493	dc725dcd	54c08455	386ecce2
dc85e2cb	0a31abc0	56f5eee2	4b603092	7750ff0e	c40fff2d	cec6357b	5fc9c1ef	

k = 192

پ-۲-۱-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
M=	7de5a0a1	92c9b2b0	b3847381	72c16e9e	2cb63566			
skIDx=	4a884819	c9a35eb0	c910573f	00e6c679	e08d2368	15e3fb95	1cbf882e	acc10574
08ad6342	e8922973	7f2493eb	80138666	a9dc5b61	afeb158c	43251271	f101e9cb	
skIDy=	5015e072	1560366e	19a01a2c	b4eecd98	8c725f55	e22af966	409b9fcf	ed97860b
499fa4ec	9ef4ae8a	482757ba	1a36035d	d42fbed7	7b9668cf	f318c4b5	22e7e354	
T.a=	56adfd18	df69d7ac	c91f60a6	aa9620e2	482d9266	0d35fa24	ee29de58	2fb201eb

5e4fd96e	e646befc	9bd16125	265458cb	0043806e	c4b3e2b6	297d5741	a8198d71	
T.b=	65a05adc	1528b2bd	44508723	7d386249	cec79493	dc725dcd	54c08455	386ecce2
dc85e2cb	0a31abc0	56f5eee2	4b603092	7750ff0e	c40fff2d	cec6357b	5fc9c1ef	

Private key skID is valid.

پ-۲-۱-۳ کپسوله‌سازی کلید نشست

m=	5973f2f0	3a6c618d	ccf2d355	9625b18f	e462e3d7	29b9d263	ce10272a	f80946f3
r=	7d086f6b	a788dc7e	6a90f9d5	b2e0cd17	3197e14e	ef1e24b3	a18c10fe	9656375d
97af8805	96a78069	b627d018	be0b4f20	4779a1e7	73b857f3	1d840f04	175279b2	
Jr.a=	2ecb5c37	cc84ef22	3862fc40	d406c14e	d8820fab	ad8b299d	91b0c0b0	e33dce53
242fa52c	4e59d298	c487b1cc	8d8e8f34	9148d7ec	7a271ee7	e2d4e990	143e5483	
Jr.b=	310d2619	c98a845c	938d7b8d	645f5014	ef7fa880	640bbfbc	778f00c5	04a80e58
bf3f07db	bfa1f0f8	fe6a122d	aaa09eaa	04f484a7	72a71345	930c7f22	0098a6df	
Ex=	1542ebf9	39278252	1edd2691	28216053	6939e5fe	ea0ec941	9ed5157b	d0a1c0df
3e9a2d1f	02559391	51948288	9127aed1	20b2667e	de6690a8	b7ae80eb	8713fd35	
Ey=	1a5210b3	15293e58	225e3efa	fe3504b6	43d1f8c5	b5a526b1	e384ca64	7143381f
1cf9eb3b	a4665bae	88904cb1	918533c0	e1a119b2	438f5478	7ebb3ded	16e3b8e9	

Within H2: z = FE2OSP(Or)= I2OSP(Or.a+(Or.b)q, 128)

z=	1886930c	e4c5422e	49c6bdc6	b22fa80a	77c0365a	bb89e293	806dccf1	31dfaa5b
bd408707	5c318441	ba5d0478	37893b8a	bd66fd9f	e179615e	44018212	336f7041	
ca01ef9a	5b546bb8	b61df054	c727d444	ca278fcb	08609def	dae8da8f	3a7e1953	
cec12083	e24bea87	d2648b18	82c092d6	c561fb1b	6c48f11c	950a6bbb	4d004920	
B=	beeb76c3	b69c04e9	19870d88	47905d8b	bf93f4fa	dd49c84f	13ea36e8	16a2a8b4
B+m=	e7988433	8cf06564	d575dedd	d1b5ec04	5bf1172d	f4f01a2c	ddfa11c2	eeabee47
K=	26551345	9d2de791	d7f4cdcf	578c202f	11542f58	30a0c5fa	a6b2dab5	0ac0c7ff

پ-۲-۱-۴ خارج کردن از کپسوله‌سازی

B=	beeb76c3	b69c04e9	19870d88	47905d8b	bf93f4fa	dd49c84f	13ea36e8	16a2a8b4
m=	5973f2f0	3a6c618d	ccf2d355	9625b18f	e462e3d7	29b9d263	ce10272a	f80946f3
r=	7d086f6b	a788dc7e	6a90f9d5	b2e0cd17	3197e14e	ef1e24b3	a18c10fe	9656375d
97af8805	96a78069	b627d018	be0b4f20	4779a1e7	73b857f3	1d840f04	175279b2	
Qx=	1542ebf9	39278252	1edd2691	28216053	6939e5fe	ea0ec941	9ed5157b	d0a1c0df
3e9a2d1f	02559391	51948288	9127aed1	20b2667e	de6690a8	b7ae80eb	8713fd35	
Qy=	1a5210b3	15293e58	225e3efa	fe3504b6	43d1f8c5	b5a526b1	e384ca64	7143381f
1cf9eb3b	a4665bae	88904cb1	918533c0	e1a119b2	438f5478	7ebb3ded	16e3b8e9	
K=	26551345	9d2de791	d7f4cdcf	578c202f	11542f58	30a0c5fa	a6b2dab5	0ac0c7ff

Decapsulation successful

پ-۲-۲ مثال۲

پ-۲-۲-۱ راه اندازی

این مثال از خم بیضوی $y^2 = x^3 + 1$ استفاده می‌کند. تابع نگاشت دوخطی مورد استفاده در این مثال زوج-ساز تیت کاهش‌یافته است.

q=	b35fa5fd	e47fa1ab	bb1e57e9	3ba1ff96	38b89b99	5c49be81	a38e3194	a0983816
4ee51fb9	1d285832	f9a05d63	9c8d9680	10c93a35	27e561f2	fd6a45cc	70aba1fb	
p=	80000000	000fffff	ffffffff	ffffffff	ffffffff			

Q1x=	7ee6f118	9329adb4	1e8cd405	2295f1a7	6096631d	f065dd38	85fff26b	8ed52022
7bfc3f3d	07fe9cfe	093424ba	9dbd4c0d	73fff367	3ce2c922	f0b73c50	2992093b	
Q1y=	67c855c9	e6b617be	b24b792a	e9c3e21e	95f37006	25b91058	3bc0b293	c36a762c
feba4266	038989cc	59797235	c6116d99	8a97b805	ff82c664	53720e5c	1de95e3e	
Q2x=	596aabeb	e89571de	383450c5	4290a154	60bde0e2	a3a982cf	f46596f9	9121e38d
857d1362	4d445bf7	8ab3377d	ecc122e3	2c3255f0	62369c8a	7d13d2d4	af91e143	
Q2y=	4e89178d	16514938	ae638f70	76a4ca1f	6082ec4b	1c444785	6769e791	385e81da
c8f7b174	8a2ce2fd	c6080cf7	d6631e07	da57f5f9	adb85b7d	149f434e	fe2dca40	
s=	37e28416	c95170c9	46ebfb30	3e422717	191b4b73			
Rx=	2b9e01f7	b1156ea3	32e9ed27	11ea9a28	4f4a1da6	e4ac08c0	2e7991f2	8bee9cbf
c4b9c138	94a71aa8	5a79c016	680f0e16	180faf69	211705b1	da199e04	2c27b0cc	
Ry=	0599b140	2272573a	7b8209fa	a922a435	b46d4634	f6af4e81	ba810480	5120476b
da1ba5ba	f0e475b5	96ce9d90	afc8eab2	46f290da	d4e91f66	b98cdfc9	3bd321c5	
J.a=	257694ae	4281deb6	58831a07	4ead48a3	6eb03bea	94063a8f	d9b87386	a36ca231
49abaa05	a8d3bd88	ead29fbb	cdf7bd30	3aee1fa4	eae7690b	a7380c0f	386f280d	
J.b=	ac6b84b8	1113130c	4316fcdc	f1d40a9c	095a7739	2077518e	3a6b94b6	ee38079d
1a6cf29b	f904d909	54e3137c	c47eb066	b39129da	57bfe26b	0c4497e2	f4e4a251	

k = 192

پ-۲-۲-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
M=	305c1ac0	9f517694	0c6f4153	02fd22ff	dd9214c9			
skIDx=	0857e829	7f03bb71	ced24ee9	7b728d8c	9afdc7d6	c8a8b027	064a3208	0ad49829
962f0f4f	1c5dac75	fd1f351d	ebaee531	cbebceeb	79214bca	0041db9d	c1175aad	
skIDy=	3fa56ae5	67260a13	dc22a3fa	c4853085	cab75f6c	dd363363	eb5729a9	5e17dbcd
39a504da	6fd2a27d	f68a5570	4f4140ae	d25dedb3	274e1bfe	44cbd823	3d981509	
T.a=	257694ae	4281deb6	58831a07	4ead48a3	6eb03bea	94063a8f	d9b87386	a36ca231
49abaa05	a8d3bd88	ead29fbb	cdf7bd30	3aee1fa4	eae7690b	a7380c0f	386f280d	
T.b=	ac6b84b8	1113130c	4316fcdc	f1d40a9c	095a7739	2077518e	3a6b94b6	ee38079d
1a6cf29b	f904d909	54e3137c	c47eb066	b39129da	57bfe26b	0c4497e2	f4e4a251	

Private key skID is valid.

پ-۲-۲-۳ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
M=	305c1ac0	9f517694	0c6f4153	02fd22ff	dd9214c9			
skIDx=	0857e829	7f03bb71	ced24ee9	7b728d8c	9afdc7d6	c8a8b027	064a3208	0ad49829
962f0f4f	1c5dac75	fd1f351d	ebaee531	cbebceeb	79214bca	0041db9d	c1175aad	
skIDy=	3fa56ae5	67260a13	dc22a3fa	c4853085	cab75f6c	dd363363	eb5729a9	5e17dbcd
39a504da	6fd2a27d	f68a5570	4f4140ae	d25dedb3	274e1bfe	44cbd823	3d981509	
T.a=	257694ae	4281deb6	58831a07	4ead48a3	6eb03bea	94063a8f	d9b87386	a36ca231
49abaa05	a8d3bd88	ead29fbb	cdf7bd30	3aee1fa4	eae7690b	a7380c0f	386f280d	
T.b=	ac6b84b8	1113130c	4316fcdc	f1d40a9c	095a7739	2077518e	3a6b94b6	ee38079d
1a6cf29b	f904d909	54e3137c	c47eb066	b39129da	57bfe26b	0c4497e2	f4e4a251	

Private key skID is valid.

پ-۲-۲-۳ کپسوله‌سازی کلید نشست

m=	cb341a16	04f777b3	c58432b9	c937f1a1	2ce7d67c	f05e6937	804d80b4	7b636131
r=	54d92604	6c850c8b	f0a95b7d	71e49ff6	a4792df5	acae2905	7b8125d0	55a677de
1c624f0e	7212f6d9	63d74475	fbb5a69c	bf4abc59	694dfb15	98b9d32a	53f9324b	
Jr.a=	7e100de0	1f4cfbee	120b3902	49022589	5aebca4f	cc8e41eb	9fffb00b	7b49d0d1

01c5127e	85117211	eb0847e5	e2bfc40f	0245b657	cfca575c	c6bbaeae	40c815d5	
Jr.b=	361fdbe3	5e81de98	2c2cd0db	0d3d98c9	b37e732c	52cb857e	017ad3cd	ad087830
c0df9179	6f024a2d	b29ce2f5	85ff424b	ea7b8d37	d535716f	53593bf7	f0686c5e	
Ex=	7f3e916f	5e617517	0119fb05	4733b8fe	d38a2fad	86387019	38a92fb9	0a2dc631
2a879d6d	46c0f7d1	a567b614	8f656c46	35f1d405	42419e32	71e1ec62	787889e9	

Within H2: z = FE2OSP(Or)= I2OSP(Or.a+(Or.b)q, 128)

Ey=	016b9bf2	4e3d7c78	a339d895	817d66b3	2f8e8a8a	dcb059fb	d8c75acf	93454afe
c83fa158	1c26cfb5	90d893bd	c1e7d092	a468ec3b	38d9920d	d90db72c	cbeab75f	
z=	25ec7faa	cafa1847	0a45e774	f709bb02	7edea353	dc4ba6ab	1f821235	b19962f8
c895e709	e90d46f8	143ce16b	e049dead	eda63f29	2b7b596d	41dc2d8d	415ff97f	
ab1341b7	9a32c89e	66ec586c	26f80e58	2036239b	3314fe03	a102abd4	1af8988b	
e8484a92	b36b1446	80167cf4	be6192cd	12e482be	5cbdb457	a3135f0a	261b73ff	
B=	3dc6fe7b	2d8c7f35	4cffd996	0ae5274c	40780d1f	deadf5e7	2f3be147	c33c017d
B+m=	f6f2e46d	297b0886	897beb2f	c3d2d6ed	6c9fdb63	2ef39cd0	af7661f3	b85f604c
K=	3ca06eae	57a1895e	279950b7	503ce290	31b38175	4e7747f8	7092514f	91dc8202

Session key encapsulation completed.

پ-۲-۲-۴ خارج کردن از کپسوله‌سازی

B=	3dc6fe7b	2d8c7f35	4cffd996	0ae5274c	40780d1f	deadf5e7	2f3be147	c33c017d
m=	cb341a16	04f777b3	c58432b9	c937f1a1	2ce7d67c	f05e6937	804d80b4	7b636131
r=	54d92604	6c850c8b	f0a95b7d	71e49ff6	a4792df5	acae2905	7b8125d0	55a677de
1c624f0e	7212f6d9	63d74475	fbb5a69c	bf4abc59	694dfb15	98b9d32a	53f9324b	
Qx=	7f3e916f	5e617517	0119fb05	4733b8fe	d38a2fad	86387019	38a92fb9	0a2dc631
2a879d6d	46c0f7d1	a567b614	8f656c46	35f1d405	42419e32	71e1ec62	787889e9	
Qy=	016b9bf2	4e3d7c78	a339d895	817d66b3	2f8e8a8a	dcb059fb	d8c75acf	93454afe
c83fa158	1c26cfb5	90d893bd	c1e7d092	a468ec3b	38d9920d	d90db72c	cbeab75f	
K=	3ca06eae	57a1895e	279950b7	503ce290	31b38175	4e7747f8	7092514f	91dc8202

Decapsulation successful

پ-۳ سازوکار کپسوله‌سازی کلید **BB1**- مبنا

پ-۳-۱ مثال۱

پ-۳-۱-۱ آماده‌سازی

این مثال از خم بیضوی یکسان $y^2 = x^3 + 1$ و زوج‌ساز ویل استفاده می‌کند.

q=	b35fa5fd	e47fa1ab	bb1e57e9	3ba1ff96	38b89b99	5c49be81	a38e3194	a0983816
4ee51fb9	1d285832	f9a05d63	9c8d9680	10c93a35	27e561f2	fd6a45cc	70aba1fb	
p=	80000000	000fffff	ffffffff	ffffffff	ffffffff			
Q1x=	7ee6f118	9329adb4	1e8cd405	2295f1a7	6096631d	f065dd38	85fff26b	8ed52022
7bfc3f3d	07fe9cfe	093424ba	9dbd4c0d	73fff367	3ce2c922	f0b73c50	2992093b	
Q1y=	67c855c9	e6b617be	b24b792a	e9c3e21e	95f37006	25b91058	3bc0b293	c36a762c
feba4266	038989cc	59797235	c6116d99	8a97b805	ff82c664	53720e5c	1de95e3e	
Q2x=	596aabeb	e89571de	383450c5	4290a154	60bde0e2	a3a982cf	f46596f9	9121e38d
857d1362	4d445bf7	8ab3377d	ecc122e3	2c3255f0	62369c8a	7d13d2d4	af91e143	
Q2y=	4e89178d	16514938	ae638f70	76a4ca1f	6082ec4b	1c444785	6769e791	385e81da
c8f7b174	8a2ce2fd	c6080cf7	d6631e07	da57f5f9	adb85b7d	149f434e	fe2dca40	
s1=	7623d9ea	1f8beada	83952da1	7d204958	109b585d			
s2=	7fcbfded	301777ed	3dc86e24	7fcbfded	301777ed			
s3=	10a20b20	f0c0a1e0	e422555b	23abbafe	25b76ea7			
Rx=	b2888069	db9e121e	559afb38	3fe2b451	a4108bae	94ec259f	dc8aa1ba	b9fd8ab0
0a7b90f5	47abf145	7826e9f7	a57f7213	8748f0a9	4519cbed	f5de3cf9	dff95c2c	
Ry=	4802e661	5b71faab	5f9816fd	bfde04c0	1de7d0a3	c9eb05c7	84441dcd	1def44ea
d02317f4	ec8e7754	301d2ee4	1176aa94	caa49709	f03de657	05edc9b2	5f5aa2dc	

Tx=	607db02e	ce4deb26	4a935296	03234fc7	aa83c96d	0ca3e8ee	293c3cf8	730bfff5
c05c75af	a1a1e0bf	8eee41de	89f41f03	9330883d	aafd5efb	ed43239f	19826577	
Ty=	3f3dbea9	c4b05a71	7f0fce9b	282ae771	e7eace91	a72c7ca6	713d7a63	acb6fc35
7c698d9c	a4a8dfd4	a03968e5	a7e68a51	a0e7e23e	4aec721c	65580e51	675d5307	
J.a=	6b4693b7	e66ad25a	b547042c	b8f858d3	ad52a8c2	ea980ab1	c0a9326a	4b93e6ec
d3cb3a8f	29198f1d	1e4f5356	d51c116f	ffde1928	58429878	8439c2c1	11a6abb1	
J.b=	7c263a78	b70b6902	42d352e1	a89dc9f6	06e22732	8e1ee8dd	f2231c30	7ceed6c9
d6ef65a3	ac7419a0	a53a3146	af9e6dc0	dc93722a	e03992a1	53025a8b	0c47f0ed	

k = 192

پ-۳-۱-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
M=	305c1ac0	9f517694	0c6f4153	02fd22ff	dd9214c9			
r=	307df8f5	11358190	47694eae	8f2dc0c3	f4d81e56			
t=	5f2350f9	631d7095	033137d5	2f597415	304b712b			
dID0x=	2d92e629	f86c6fa8	b1bddf5e	e8872965	2cf04dce	62f08160	e84a644b	432d1a1c
ccd6272d	0bac8f18	86a6a434	f524c0fa	d73d1499	0938225a	715fba67	a7a626a2	
dID0y=	6515d933	9124341c	8ab13862	5e433278	afa8b6a7	32daf20b	5a9f3d1f	327d770b
db8a18b5	3c74c97b	b746a500	36e812c0	65c29971	e6095c5e	13968410	793a363f	
dID1x=	929cc12c	fd74beb6	4f062f55	0f8a252b	e3b8abbb	0abeb7b1	7d3ac147	d4ad83c4
4f1069f0	1616e318	e5087cec	49873cb7	fc11cfd7	e3bfbf3c	69e5337e	7899067f	
dID1y=	4e1b894e	87aebd2c	6dc24553	4e7f1e1f	62558914	e1d2a924	e7853b54	b9b741db
0517870d	ac830baf	54fb958d	ad4c3530	2a4f7d6f	b466d0fb	eb441217	220f4ed4	
T0.a=	51d0adff	dfb544ac	56867378	4ab4419d	4c86c3ad	b4f5b851	d8a1dbc8	592b007c
0e216163	4748a58b	c57690d2	0fb77466	3865c31c	e1b1a0a1	2726c483	a27fb151	
T0.b=	867bbac1	acb9ad9b	91bce537	a3b14e57	8dbe44a1	5ebea58f	c4a698f1	309f84fb
caf08027	73bc17da	be80a6e1	dac0b4cd	f8c4bedc	e8bdfe0a	7a0ddb01	fc3bcde3	
T1.a=	a68e9d1f	8b2b1afc	4eb2de87	29d058a7	4f4ac828	c3da3fc6	c6e9b9c3	d86cdeae
066e2d6f	18c6613e	393b4b39	242afddd	bc1ade14	02d3cc27	9943019b	11b7274b	
T1.b=	a8cb789e	20f1daf3	9b259428	eb63ca7b	009142f9	a0f2cc82	82a8cad2	b28ebddd
13bbb836	9b311a56	1758817a	c2d1f199	dcb6c790	f3ba5bf6	dd19ba1d	4478918b	
OT1.a=	51d0adff	dfb544ac	56867378	4ab4419d	4c86c3ad	b4f5b851	d8a1dbc8	592b007c
0e216163	4748a58b	c57690d2	0fb77466	3865c31c	e1b1a0a1	2726c483	a27fb151	
OT1.b=	867bbac1	acb9ad9b	91bce537	a3b14e57	8dbe44a1	5ebea58f	c4a698f1	309f84fb
caf08027	73bc17da	be80a6e1	dac0b4cd	f8c4bedc	e8bdfe0a	7a0ddb01	fc3bcde3	

Private key <dID0, dID1> is valid.

پ-۳-۱-۳ کپسوله‌سازی کلید نشست

r'=	798cdb57	64e9d910	fb353f92	e8d22d4b	c6ceff27			
E0x=	3ec733e6	f813c81f	f3a272cd	015ffefd	4ac02c03	e9d7aa58	7a41c238	02a55298
093268b1	696a7396	0b75318f	27ef9e36	721a435c	ebd48fbb	08c288ae	f9f420fb	
E0y=	3cde70f8	0157e267	a466061f	ffceb029	b65f0c78	b6a671cb	d9c388f9	5882abb1
6089f6a1	32f480a8	69b7210c	9aded83e	8a26bf37	521a03bd	83b3d759	16b2ff13	
E1x=	3f259b34	9f128746	8b6f9df1	f929a11f	2b060ccf	c74c9c82	befd7f35	f30e8b7b
fbdfb419	041738c5	22c1651b	cd1b5e0a	4fade396	7ddf2a5d	7f7186ae	98b0632c	

E1y=	91e827b1	c13331be	ab021930	ce980ab7	a2d32415	e155e871	4fe4f7bb	c1926196
c08a0f49	97f36c17	6075608f	9739a921	d0438e3d	76e8f6f3	47a6a3fa	0c44edf3	
B.a=	2d763660	63070c7e	ecf627b2	7086d821	07473066	3a654b19	842f9e01	0fda239f
51e72f6f	1f4a24b1	afd999f8	966ccab7	b1b4ba3b	1799e34d	019276f1	b11c928a	
B.b=	677206ed	615d812c	1fbcf31e	d7ef074e	50ec925b	c7605867	c99347f4	610e27ae
3cb7b7bc	51ee0311	f2956123	06e2a611	3e01f593	e1537d82	4db21660	416eb44e	
Within	H2:	z=	FE2OSP(B)=	I2OSP(B.a+(B.b)q,	128)			
z=	487b613b	a3a87c70	3cd80b59	5de3e836	290815da	82cc0519	f1520883	2b74e6c8
05fa7143	32f5c330	f4039bc9	65dd8935	f2d97365	e4aa01cf	4bc0a5bf	3ba3b348	
b3814906	ad5b230a	6b8faf1d	f33f91d5	e4ca174f	7f07726e	d7814d0f	9a566d96	
104de63c	aa80ee15	231b78ea	52d856d2	f070e0ab	a5a1fac5	f749c875	08266904	
K=	080d9ed8	c25802ce	df4a24da	0ae3f8c4	5fa0f9d2	5e0f875a	b39f7e52	d10e8b20

Session key encapsulation completed.

پ-۳-۱-۴ خارج کردن از کپسوله‌سازی

B.a=	2d763660	63070c7e	ecf627b2	7086d821	07473066	3a654b19	842f9e01	0fda239f
51e72f6f	1f4a24b1	afd999f8	966ccab7	b1b4ba3b	1799e34d	019276f1	b11c928a	
B.b=	677206ed	615d812c	1fbcf31e	d7ef074e	50ec925b	c7605867	c99347f4	610e27ae
3cb7b7bc	51ee0311	f2956123	06e2a611	3e01f593	e1537d82	4db21660	416eb44e	
K=	080d9ed8	c25802ce	df4a24da	0ae3f8c4	5fa0f9d2	5e0f875a	b39f7e52	d10e8b20

Decapsulation successful.

پ-۳-۲ مثال ۲

پ-۳-۲-۱ آماده‌سازی

این مثال از خم بیضوی یکسان $y^2 = x^3 + 1$ و زوج‌ساز تیت کاهش‌یافته استفاده می‌کند.

q=	80000000	00000000	00000000	00000000	00020001	40000000	00000000	
00000000	00000000	00010000	80000002	00000000	00000000	00000000	00000000	
00080003								
p=	80000000	00000000	00000000	00000000	00020001			
Q1x=	0db4e0f7	22dd090d	a2b6d8fe	adaf21d9	546ab265	1515af9b	a87108f3	4e1ae0e3
eb132c10	81452cc1	e52bb2a7	4287a0cb	d8ff8dd9	3a225641	5321f0e4	c8892a50	
Q1y=	762c096c	49f1ab04	7d7f37de	537a4e7c	2991c400	22e0c9a9	b3f58b1b	9df4f28a
4a4330e2	170e14d2	f55a0719	8b667d0b	01e5a482	3f07e921	8516481e	641970ac	
Q2x=	6b8f666b	cf6b4672	d4634753	1f734e71	41bcd5fd	125f3ef3	714edc28	f6426900
75ffb5f7	9e745cc0	fb03f940	3bdcefe8	acbe6286	d5d9955c	2a0e5ed7	657748c6	
Q2y=	69584e47	f3070fed	9800d6cd	e0f314b4	03955126	1c5bfef6	f3595f94	5958f7d9
34dcbd3d	63125410	ccd363f8	02df1c7e	4a3d7ac7	24cf3865	0fb16ec1	7bb30a85	
s1=	7623d9ea	1f8beada	83952da1	7d204958	109b585d			

s2=	7fcbfded	301777ed	3dc86e24	7fcbfded	301777ed			
s3=	10a20b20	f0c0a1e0	e422555b	23abbafe	25b76ea7			
Rx=	142d5e5d	22670c96	1fa51e66	1882a317	0541ac63	653ce2d5	0be026a7	891699c8
8d413e52	607c91c9	623de680	2268809b	b3b2b57f	437713e1	ce7f756a	f1d0809a	
Ry=	0b418104	b1b5dd7e	9144a853	5b9b7dd2	5e30ab90	97355d60	75052c0d	edd738b8
e71e0773	16b772a9	2fc72619	25d7fd83	65dd097b	56010aa9	6ada597d	3b54df7e	
Tx=	6163c179	8bd08560	79b96b62	f8e97961	bfcac250	a8dd433d	e02f2180	50cf90c1
372e2e30	438cfe0c	1be1640c	f7370d29	bb6ad4c4	163ace4a	aa7c316e	0e47801e	
Ty=	427f55b2	10f57d60	4271d022	d184ef29	fed0a2c4	7e51a99b	b7340c5f	9b084693
6142cd8e	0a89172c	d503656d	3e358164	3170ad13	c2c4b93e	d96a83e6	215a52e6	
J.a=	518c40f1	f0942278	64e49282	8ee77ac4	5d8943e8	abacf3f1	fdc8d465	1ac1cfb5
2bb1bf59	e941db84	70f92c3e	55fd0645	0888800d	0046a33a	ee4570cb	6f462617	
J.b=	5231d656	4a2b144c	4b1a38c3	804db0a3	b4930a19	1496ad21	71617cf0	0859f16f
a4bde018	9b851678	a683205d	04e0768d	cf22b1c0	2907525b	97abf0f8	09e4b7a1	

k = 192

پ-۳-۲-۲ استخراج کلید خصوصی

ID = sc27wg2-secretary@ipa.go.jp

IDb=	73633237	7767322d	73656372	65746172	79406970	612e676f	2e6a70	
M=	7de5a0a1	92c9b2b0	b3847381	72c16e9e	2cb63566			
r=	05351a22	d10f5339	dfe1eb30	30924229	2302d090			
t=	703a597c	3b7396f8	386e89b9	5af2fb1b	76969bd3			
dID0x=	5ed9195c	81863738	e8cf7a26	3e00db1c	e8a72a22	7579309d	3a11282f	964a54c0
27446231	58c24ab3	ae4c901f	a18e210b	adc60fc6	f5d310bc	a900351c	dcf782b0	
dID0y=	1a490f37	a26b205e	789f5585	a49ffd9d	9491feac	01b5b2bb	1f4fdcab	d301f533
874034f9	1a8db549	15422e4a	3ca3a83e	4eecab72	f863a746	d640d798	675ba0b5	
dID1x=	5d2a8994	ed44dca6	852a5ebb	ba7337f9	824aee7c	e904ffd1	20ddc0e7	dbca2b16
ccbe101e	e4adac32	3cb9a8ed	37c34720	16519890	44417767	e1acdf0b	ee0a4459	
dID1y=	6264b10b	9c5b5ad9	7d56ef17	5922caf4	ee8154f4	aaca86ac	a72c7b34	8e9cd873
a0659aa6	b7e0ee34	850f4def	9b5b50b6	98ff5571	827a1d64	37783bc7	db378def	
T0.a=	44084f72	c31c6b70	55dd4931	140b6a18	77db2fd4	fae3944e	a6838cb9	bd27326c
cd366fe9	c848610c	e0e0e473	97d04196	40d0e03f	0924aa21	8b6dac56	795ea605	
T0.b=	69c27507	78d5272e	c8938f17	c868c956	df8d2364	b2b8e1ff	dc73a3c9	5a6d5c9a
315d3d69	7a6a1d3d	68d551c5	68a1feef	a4dd73a5	854cfb63	16c1281f	eaf09e31	
T1.a=	6ef90912	510ba657	0121df17	2ae97124	9353f2b2	9bcf43aa	533b0e4a	0f68b6e3
f1aba24c	f8c3c018	619f6c0e	adf3452c	ac91d8c5	69451a9c	91fc7f30	ec31dd7d	
T1.b=	65ba8521	75167ea3	83ed9488	24347da3	b3541c17	dbeead01	482a3772	a1e122a8
6f06bcc3	66cfd74d	80dcdb47	32a68280	7233968b	655327be	075b7187	ab8d8a19	
JT1.a=	44084f72	c31c6b70	55dd4931	140b6a18	77db2fd4	fae3944e	a6838cb9	bd27326c
cd366fe9	c848610c	e0e0e473	97d04196	40d0e03f	0924aa21	8b6dac56	795ea605	
JT1.b=	69c27507	78d5272e	c8938f17	c868c956	df8d2364	b2b8e1ff	dc73a3c9	5a6d5c9a
315d3d69	7a6a1d3d	68d551c5	68a1feef	a4dd73a5	854cfb63	16c1281f	eaf09e31	

Private key <dID0, dID1> is valid.

پ-۳-۲-۳ کپسوله‌سازی کلید نشست

r'=	3bda4388	5211ae25	fa4ad7d8	fecf0108	786cb1bc			
E0x=	266f9cde	74752bc1	15bb0a01	a122c008	c3d50b40	6429d9e2	7ea6a6c8	f653b932
b468d332	2ee75be7	a259d6bb	5330da08	85feee12	0fe78295	33759ff9	26bc7f4a	
E0y=	202390c6	276b4df0	afba4684	a88d6deb	7005dfc4	674f866b	2e275e04	bedba792
2c901ba	aee167c6	603e35dd	e8153c98	c46d99b4	2c3eaf3	dd84aad	9270b9a	

4					b	e	d	
E1x=	26405024	f8bf9a2d	2884f055	abdae2f5	5823d52c	50498888	35b8a7b9	d1b226e3
8ae4710b	1473b6cd	f5fddc41	a96a9a47	5c065fad	ac4e5b7f	b549b7eb	25141d6d	
E1y=	644172fb	549983ab	7b8ca683	4966c1fd	14a2667e	292b34c6	5001bded	208e4e74
e49b6583	ac06c840	bf08146d	ff481576	f9e16dce	133c9b34	4cfc9ef5	fd4c7798	
B.a=	7e22bfc1	112d0bd0	d30aed86	2923563d	546157a0	1188f9d0	70c11677	f965ca25
8dcc03a2	9b5decdb	b2db93c0	92b6275e	76dfa49c	bca75f80	298d7e43	b05b2b86	
B.b=	4ffda204	0a79ed2f	82fbbae0	0dec9464	78b0588c	37e2ec87	dcb9ada7	8ffee336
5cdad0f2	df0cc9ab	97fbbb31	6e34030c	5180c4ea	0abebede	b2106de1	cd56e42f	
Within	H2:	z=	FE2OSP(B)=	I2OSP(B.a+(B.b)q,	128)			
z=	27fed102	053cf697	c17ddd70	06f64a32	3c58cc41	c3f695bc	d5d44546	a17a370c
689e1357	b77b9348	b4ec1a32	78b8f830	f47d7dea	3ca8db5b	33eceff0	d4e57c81	
d9dfe04f	ee7520a4	5d886e35	234c9bac	d1279cba	c78e6e9f	3e3d12b2	2a54f5f3	
085af0e6	b4dc5797	6f07ff52	f5b4bc89	92b24950	d3d92c9f	aecd32a0	39d7d813	
K=	9f9f10c1	2616df83	b785a730	0a57b165	92ef8790	f5869922	2a9056e0	cd0ada89

Session key encapsulation completed.

پ-۳-۲-۴ خارج کردن از کپسوله‌سازی

B.a=	7e22bfc1	112d0bd0	d30aed86	2923563d	546157a0	1188f9d0	70c11677	f965ca25
8dcc03a2	9b5decdb	b2db93c0	92b6275e	76dfa49c	bca75f80	298d7e43	b05b2b86	
B.b=	4ffda204	0a79ed2f	82fbbae0	0dec9464	78b0588c	37e2ec87	dcb9ada7	8ffee336
5cdad0f2	df0cc9ab	97fbbb31	6e34030c	5180c4ea	0abebede	b2106de1	cd56e42f	
K=	9f9f10c1	2616df83	b785a730	0a57b165	92ef8790	f5869922	2a9056e0	cd0ada89

Decapsulation successful.

پیوست ت

(آگاهی‌دهنده)

سازوکارهای جلوگیری از دسترسی اشخاص ثالث به کلیدها

هیچ IBE بدون یک شخص ثالث به نام مولد کلید خصوصی (PKG) که با استفاده از کلید مخفی- اصلی خود برای همه رمزگشاها کلید خصوصی تولید می‌کند قادر به عمل نیست. بنابر این، IBE صرفا زمانی که این چنین عملیات امان‌سپاری[1] کلید مجاز باشد قابل استفاده است. برملا شدن کلید مخفی- اصلی در یک سامانه IBE می‌تواند زیان‌بار باشد و معمولا بسیار وخیم‌تر از فاش شدن امضای کلید توسط CA در یک PKI سنتی است. ظاهرا به این دلیل ممکن است استفاده از یک IBE به گروه‌هایی کوچک، انحصاری یا به برنامه‌هایی کاربردی با الزامات امنیتی محدود شود.

الریامی[2] و پترسون[3] الگویی نوین برای رمزنگاری ابداع کردند که آن را رمزنگاری کلید عمومی بدون گواهی‌نامه نامیدند که علیرغم عدم نیاز به استفاده از گواهی‌نامه، فاقد مشخصه توکار[4] امان سپاری IBE است.

بسیاری از محققان با الهام از کار الریامی و پترسون، طرح‌های متنوع رمزگذاری کلید عمومی بدون گواهی‌نامه پیشنهاد داده‌اند. مطالعات آن‌ها در منبع [6] کتاب‌نامه آمده است.

1- Key escrow
2- Al-Riyami
3- Paterson
4- Built-in

کتاب‌نامه

[1] ISO/IEC 18031, Information technology — Security techniques — Random bit generation

[2] Al-Riyami S.S., & Paterson K.G. Certificateless public key cryptography. In: Advances in Cryptology — ASIACRYPT'03. . Springer, Vol. 2894, 2003, pp. 452–73

[3] Boneh D., & Boyen X. Efficient selective-ID secure identity based encryption without random oracles. In: Advances in Cryptology — EUROCRYPT'04. . Springer, Vol. 3027, 2004, pp. 223–38

[4] Boneh D., & Franklin M.K. Identity-based encryption from the Weil pairing. In: Advances in Cryptology — CRYPTO'01. . Springer, Vol. 2139, 2001, pp. 213–29

[5] Chen L., Cheng Z., Malone-Lee J., Smart N. Efficient ID-KEM based on the Sakai-Kasahara key construction. IEE Proceedings Information Security, 153(1):19-26, 2006

[6] Dent A. W. A survey of certificateless encryption schemes and security models, International Journal of Information Security, Volume 7 Issue 5, pages 349-377. Springer-Verlag, 2008

[7] IEEE Std 1363.3-2013, IEEE Standard for Identity-Based Cryptographic Techniques using Pairings