企業・個人の情報セキュリティ対策事業

暗号アルゴリズム試験ツールの開発

開発成果概要資料

三菱電機株式会社

概要

独立行政法人 情報処理推進機構(IPA)では，暗号モジュール試験及び認証制度(JCMVP: Japan Cryptographic Module Validation Program)の試行運用を 2006 年度から開始し，2007 年度から正式運用を開始することを予定している．JCMVP では暗号モジュールの試験を行う．暗号モジュール試験は，暗号アルゴリズムの試験とその他の試験に大別される．我々は，JCMVP の暗号アルゴリズム試験において使用するための暗号アルゴリズム試験ツール(JCATT: Japan Cryptographic Testing Tool)を開発した．本報告書では，JCATT の概要を述べる．

1．はじめに

近年，CRYPTREC や NESSIE など様々な機関において暗号アルゴリズムの評価が実施され，推奨暗号のリストが作成された．各機関では，各国の第一線の暗号研究者が評価作業に携わってきた．専門家による暗号の安全性と実装性に関する厳しい評価による“お墨付き”を与えられた暗号は，電子政府を含めた各種情報セキュリティシステムにおいて使用が進んでいる．

各暗号評価プロジェクトは，暗号の“アルゴリズム”に関する評価を行うものであった．アルゴリズムが優れていると判定された暗号を使用することは，安全で信頼できる情報セキュリティシステムを構築する上での第一の要件である．しかし，暗号アルゴリズムが実際に使用される時には，ソフトウエアやハードウエアで実装された“暗号モジュール”という形態になることに注意しなければならない．暗号モジュールは，暗号アルゴリズムの仕様書を元に実際に運用するシステムに合わせて実装されるものである．暗号アルゴリズムと暗号モジュールとの間には，暗号モジュール開発者の手作業が入るものであり，暗号モジュール開発者には相応のスキルを有していることが要求される．暗号アルゴリズムの実装には，ソフトウエアやハードウエアの実装スキルだけでなく，数学的スキルも要求されるため，実装は易しい課題ではない．

正しく実装されていない暗号モジュールを使用すれば，情報セキュリティシステムの安全性と信頼性が破綻することになる．すなわち，優れた暗号を使用することと，優れた情報セキュリティシステムを構築することとは等価ではなく，暗号モジュールが暗号アルゴリズムを正しく実装したもの

であるかどうかの検証が欠かせない．暗号モジュール評価法を規定した FIPS 140-2 の中でも暗号アルゴリズム実装の試験の必要性が述べられている．

最近数年間，特に 2004 年度中に，NIST から FIPS に記述されたいくつかの暗号アルゴリズムに対して暗号アルゴリズム試験方法が公開された[2〜12]．しかし，日本国内メーカによる提案の多い電子政府推奨暗号は，多くの暗号について試験方法が定められていなかった．また，NIST から公開されている試験方法は，ごく単純な試験を行うだけという問題があった．

我々は，NIST の暗号アルゴリズム試験方法も調査した上で，暗号アルゴリズム試験方法を考察し，JCATT の開発を行った．本開発により，電子政府推奨暗号に対する暗号アルゴリズム試験が可能となった．

2．暗号アルゴリズム試験方法

2.1．NIST の動向

NIST から次の暗号アルゴリズムの試験方法が公開された．

- ブロック暗号：AES[2]，Triple DES[10]，DES[11]，Skipjack[11]
- ブロック暗号の利用モード：CCM mode of operation[12]
- ハッシュ関数[5]：SHA-1，SHA-224，SHA-256，SHA-384，SHA-512
- メッセージ認証(鍵付きハッシュ関数)：HMAC[6]
- ディジタル署名：RSASSA-PKCS1-v1_5[4]，RSA-PSS[4]，DSA[7]，ECDSA[8]
- 擬似乱数生成：ANSI 9.31 の方法[9]

上記のうち CCM 以外の暗号は本開発においても試験対象暗号としている．本開発で検討した暗号アルゴリズム試験方法と，開発した JCATT は，NIST により公開された試験方法をカバーし，さらにより詳細な試験を行っている．

2.2．試験対象暗号

JCATT は以下の暗号を試験対象とした．

- 全ての電子政府推奨暗号[1]
- メッセージ認証(鍵付きハッシュ関数) …HMAC
- ハッシュ関数…SHA-224
- 公開鍵暗号…HIME(R)
- 擬似乱数生成関数…電子政府推奨暗号と ISO 18031 に記述された擬似乱数生成関数．

以下に試験対象暗号を示す．

ディジタル署名

DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS

公開鍵暗号(守秘)

HIME(R)，RSA-OAEP，RSAES-PKCS1-v1_5

鍵共有

DH，ECDH，PSEC-KEM

ブロック暗号

CIPHERUNICORN-E，Hierocrypt-L1，MISTY1，3-key Triple DES，AES，Camellia，CIPHERUNICORN-A，Hierocrypt-3，SC2000

ストリーム暗号

MUGI，MULTI-S01，128-bit RC4

ハッシュ関数

RIPEMD-160，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512

メッセージ認証(鍵付きハッシュ関数)

HMAC

擬似乱数生成関数

CTR_DRBG (ISO/IEC 18031),
OFB_DRBG (ISO/IEC 18031),
Hash_DRBG (ISO/IEC 18031),
PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1 (CRYPTREC),
PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1 (CRYPTREC),
PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 (CRYPTREC)

上記試験対象暗号は電子政府推奨暗号[1]を全て含み, NESSIE, ISO/IEC, FIPS, ANSI などで標準化されている暗号アルゴリズムも広くカバーしている．

次節以降で，各暗号に対する試験方法の概要を記述する．

2.3．試験項目作成の方針

試験項目は次の 2 つを基本方針として作成した．

- 暗号モジュールが暗号アルゴリズム仕様書に記述された事項に従って実装されているかどうかを試験する．
- 多くのプラットフォーム上で実装された暗号モジュールを試験できるように，汎用性の高い試験方法を作成する．

まず暗号アルゴリズムごとの機能を抽出した．例えばブロック暗号の場合，暗号化，復号のように，暗号ライブラリ等で独立した API として提供されることが多いものを機能として抽出した．次に，機能ごとに，暗号アルゴリズムが仕様書通りに実装されていることを確認するために必要な試験項目を設定した．

2.4．ディジタル署名

DSA

試験対象機能は次の通り．

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能
- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

試験項目を以降に示す．

1. ドメインパラメータ生成機能

- IUT(試験対象モジュール)が生成した SEED および counter を JCATT に入力し, JCATT は FIPS 186-2 Appendix 2 のアルゴリズムに従って 2 つの素数 p’，q’を計算する．この p’，q’と，IUT が生成した p, q がそれぞれ等しいこと．
- $g^q \equiv 1 \bmod p$ であること．
- IUT が生成した複数のドメインパラメータ(p，q，g)が全て異なるものであること．

2. ドメインパラメータ検証機能

- JCATT が与えた前節に記述したドメインパラメータ生成機能に対する試験に適合するようなドメインパラメータに対して, IUT が合格と判定すること．

- JCATT が与えた前節に記述したドメインパラメータ生成機能に対する試験に違反するようなドメインパラメータに対して, IUT が不正と判定すること.

3. 鍵ペア生成機能

- $y \equiv g^x \bmod p$ であること.
- $1 \leqq x \leqq q-1$, $2 \leqq y \leqq p-2$ であること.
- $y^q \equiv 1 \bmod p$ であること.
- IUT が生成した複数の鍵ペアが全て異なるものであること.

4. 署名生成機能

- JCATT が与えたプライベート鍵および平文に対して, IUT が生成した署名を, JCATT が署名検証した時に署名検証合格となること.
- 同じ平文, 同じプライベート鍵に対して複数(別途規定する数) 署名を生成させた時, IUT が同じ署名を生成しないこと.

5. 署名検証機能

- JCATT が与えた正しい公開鍵, 平文および署名, ならびに指定されたハッシュ関数に対して, IUT が正しく署名検証合格と判定すること.
- JCATT が改竄した平文, 署名, または公開鍵に対して, IUT が署名検証不合格と判定すること.

<u>ECDSA</u>

試験対象機能は次の通り.

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能
- 鍵ペア生成機能
- 公開鍵検証機能
- 署名生成機能
- 署名検証機能

試験項目を以降に示す.

1. ドメインパラメータ生成機能

- 生成されたドメインパラメータが正しい数学的関係を持つこと(仕様書に記載されている関係式をすべて満たすこと). ECDSA は定義体標数によって試験項目が異なることに注意.
- 生成された複数のドメインパラメータが全て異なるものであること.

2. ドメインパラメータ検証機能

- DSA と同様.

3. 鍵ペア生成機能

標数 p の場合を以下に記述する. 標数 2 の場合も同様である.

- $Q \neq O$ であること.
- $(Q_y)^2 \equiv (Q_x)^3 + a(Q_x) + b \bmod p$ であること.
- $nQ = O$ であること.
- $Q = dG$ であること.
- IUT が生成した複数の鍵ペアが全て異なるものであること.

4. 公開鍵検証機能

- DSA と同様.

5. 署名生成機能

- DSA と同様.

6. 署名検証機能

- DSA と同様.

<u>RSASSA-PKCS1-v1_5</u>

試験対象機能は次の通り.

- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

試験項目を以降に示す.

1. 鍵ペア生成機能
- nが指定されたビット長であること.
- p と q はビット長が等しい素数であること.
- n=pq であること.
- 生成された複数の鍵ペアが全て異なること

CRT 無しの場合
- ed≡1 mod λ(n)であること

CRT 有りの場合
- e dP≡1 mod p-1 であること
- e dQ≡1 mod q-1 であること
- q qInv≡1 mod p であること

2. 署名生成機能
- JCATT が与えたプライベート鍵および平文，ならびに指定されたハッシュ関数に対して IUT が正しい署名を生成すること.

3. 署名検証機能
- DSA と同様

RSA-PSS

試験対象機能は次の通り.
- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

試験項目を以降に示す.

1. 鍵ペア生成機能
- RSASSA-PKCS1-v1_5 と同様

2. 署名生成

試験 1(既定の試験)
- JCATT が与えたプライベート鍵, 平文に対して IUT が生成した署名を，JCATT が署名検証した時に署名検証合格となること.
- salt 長が 0 でない場合，同じ平文，同じプライベート鍵に対して，複数署名を生成させた時，IUT が同じ署名が生成しないこと.

試験 2(任意で実施する試験)
- JCATT が与えたプライベート鍵(n, d)または(p, q, dP, dQ, qInv)，平文，ならびに指定されたハッシュ関数，擬似乱数生成関数，乱数シードに対して IUT が正しい署名を生成すること.

試験 3(任意で実施する試験)
- JCATT が与えたプライベート鍵(n, d)または(p, q, dP, dQ, qInv)，平文，ならびに指定されたハッシュ関数，salt に対して IUT が正しい署名を生成すること.

3. 署名検証
- RSASSA-PKCS1-v1_5 と同様

2.5. 公開鍵暗号(守秘)

HIME(R)

試験対象機能は次の通り.
- 鍵ペア生成機能
- 暗号化機能
- 復号機能

試験項目を以降に示す.

1. 鍵ペア生成機能
- p と q は指定されたビット長の素数であること.
- p≡3 mod 4 を満たすこと.
- q≡3 mod 4 を満たすこと.
- p≠q であること.
- $n=p^dq$ を満たすこと.
- 生成された複数の鍵ペアが全て異なる

ものであること.

2. 暗号化機能

- JCATTが与えたシステムパラメータd, 公開鍵n，ラベルLおよび平文，ならびに指定されたハッシュ関数および鍵導出関数KDFに対してIUTが生成した暗号文を，JCATTが復号した時に，もとの平文に復号されること.
- 同じ平文，同じ公開鍵，同じラベル値に対して，複数暗号文を生成させた時，IUTが同じ暗号文を生成しないこと.

3. 復号機能

- JCATTが与えたシステムパラメータd, プライベート鍵(p, q)，公開鍵n，ラベルLおよび平文，ならびに指定されたハッシュ関数，指定された鍵導出関数KDFおよび暗号文に対して，もとの平文に復号できること.
- JCATTが与えたシステムパラメータd, プライベート鍵(p, q)，公開鍵n，ラベルLおよび平文，ならびに指定されたハッシュ関数，指定された鍵導出関数KDFおよび改ざんされた暗号文に対して，フォーマット違反を検出できること.

RSA-OAEP

試験対象機能は次の通り.

- 鍵ペア生成機能
- 暗号化機能
- 復号機能

試験項目を以降に示す.

1. 鍵ペア生成機能

- RSASSA-PKCS1-v1_5と同様

2. 暗号化機能

試験1(既定の試験)

- JCATTが与えた公開鍵および平文，ならびに指定されたハッシュ関数およびマスク生成関数およびラベルに対してIUTが生成した暗号文を，JCATTが復号した時に，もとの平文に復号されること.
- 同じ平文，同じ公開鍵，同じラベル値に対して，複数暗号文を生成させた時，同じ暗号文が生成されないこと.

試験2(任意で実施する試験)

- JCATTが与えた公開鍵，平文およびラベル，ならびに指定された擬似乱数生成関数，指定されたハッシュ関数およびマスク生成関数と，乱数シードに対して正しい暗号文をIUTが生成すること.

試験3(任意で実施する試験)

- JCATTが与えた公開鍵，平文およびラベル，ならびに指定されたハッシュ関数，マスク生成関数および中間値seed対して正しい暗号文をIUTが生成すること.

3. 復号機能

- 与えられたプライベート鍵と，与えられたラベルと，指定されたハッシュ関数及びマスク生成関数と，与えられた暗号文に対して，もとの平文に復号できること.
- 与えられたプライベート鍵と，与えられたラベルと，指定されたハッシュ関数及びマスク生成関数と，改竄された暗号文に対して不正検出を正しく行うこと.

RSAES-PKCS1-v1_5

試験対象機能は次の通り.

- 鍵ペア生成機能
- 暗号化機能
- 復号機能

試験項目を以降に示す.

1. 鍵ペア生成機能
- RSASSA-PKCS1-v1_5 と同様
2. 暗号化機能

試験 1(既定の試験)

- JCATT が与えた公開鍵(n, e)および平文に対して IUT が生成した暗号文を, JCATT で復号した時に, もとの平文に復号されること.
- 同じ平文, 同じ公開鍵に対して, 複数暗号文を生成させた時, IUT が同じ暗号文を生成しないこと.

試験 2(任意で実施する試験)

- JCATT が与えた公開鍵および平文, ならびに指定された擬似乱数生成関数および乱数シードに対して正しい暗号文を IUT が生成すること.

試験 3(任意で実施する試験)

- JCATT が与えた公開鍵および平文, ならびに指定された中間値 PS に対して正しい暗号文を IUT が生成すること.

3. 復号機能
- 与えられたプライベート鍵と, 与えられた暗号文に対して, もとの平文に復号できること.
- 与えられたプライベート鍵と, 改竄された暗号文に対して不正検出を正しく行うこと.

2.6. 鍵共有

DH

試験対象機能は次の通り.

- ドメインパラメータ生成機能
- ドメインパラメータ検証
- 鍵ペア生成機能
- 公開鍵検証機能
- 鍵共有機能

試験項目を以降に示す.

1. ドメインパラメータ生成機能

試験 1(既定の試験)

- IUT が生成した seed および pgenCounter を JCATT に入力し, JCATT は ANSI X9.42 Annex B.1.3 記載のアルゴリズムに従って 2 つの素数 p', q'を JCATT が計算する. この p', q'と, IUT が生成した p, q がそれぞれ等しいこと.
- $g^q \equiv 1 \bmod p$ であること.
- IUT が生成した複数のドメインパラメータ(p, q, g)が全て異なるものであること.

試験 2(任意で実施する試験)

- IUT が生成した seed および pgenCounter を JCATT に入力し, JCATT は ANSI X9.42 Annex B.1.3 記載のアルゴリズムに従って 2 つの素数 p', q'を JCATT が計算する. この p, q と, IUT が生成した p, q がそれぞれ等しいこと.
- $1< h<p-1$ であること.
- $g \equiv h^{(p-1)/q} \bmod p$ であること.
- IUT が生成した複数のドメインパラメータ(p, q, g)が全て異なるものである

こと.

2. ドメインパラメータ検証

- DSA と同様

3. 鍵ペア生成機能

- DSA と同様

4. 公開鍵検証機能

- 公開鍵 y およびドメインパラメータ(p, q, g)が以下の条件全てを満たしている時には，合格と判定し，そうでなければ不正と判定すること.
  - 2≦y≦p-2 であること
  - yq≡1 mod p であること

5. 鍵共有機能

- JCATT が与えた(複数の)プライベート鍵と公開鍵に対して，IUT が正しい共有鍵を生成すること.

ECDH(cofactor ECDH)

試験対象機能は次の通り.

- ドメインパラメータ生成機能
- ドメインパラメータ検証
- 鍵ペア生成機能
- 公開鍵検証機能
- 鍵共有機能

試験項目を以降に示す.

1. ドメインパラメータ生成機能

- ECDSA と同様

2. ドメインパラメータ検証機能

- ECDSA と同様

3. 鍵ペア生成機能

- ECDSA と同様

4. 公開検証機能

- ECDSA と同様

5. 鍵共有機能

- JCATT が与えた(複数の)プライベート鍵と公開鍵に対して，IUT が正しい共有鍵を生成すること.

PSEC-KEM

試験対象機能は次の通り.

- 鍵ペア生成機能
- セッション鍵暗号化機能
- セッション鍵復号機能

試験項目を以降に示す.

1. 鍵ペア生成機能

- ECDSA と同様

2. セッション鍵暗号化機能

- JCATT が与えた公開鍵に対して, IUT が生成した暗号文を, JCATT で復号化した時に，暗号文正当性の検証が合格となること.
- 同じ公開鍵に対して複数の暗号文を生成させた時，IUT が同じ暗号文を生成しないこと.

3. セッション鍵復号機能

- JCATT が与えた鍵ペアおよび暗号文に対して, IUT が正しく復号すること.
- JCATT が改竄した暗号文に対して, IUT が正しく棄却すること.

2.7. ブロック暗号

ブロック暗号の試験対象機能は次の通り.

- 暗号化機能
- 復号機能

ブロック暗号は動作モードを含めて実装されることが多いため，試験は動作モードを含めて実装された暗号モジュールに対して行うこととした．対象とした動作モードは

次の通り.

- ECB
- CBC
- OFB
- CFB
- CTR

ただし，AES と 3-key Triple DES に対してはCFB-1 とCFB-8 も対象とした. また，CTR モードは，NIST SP 800-38A に記載されているインクリメンタルカウンタによるものを対象とした.

ブロック暗号の試験項目を次に示す.

全てのブロック暗号に共通な検証項目

- Variable Plaintext (Ciphertext) Known Answer Test
- Variable Key Known Answer Test
- Multi-block Message Test
- Monte Carlo Test

AES 専用の検証項目

- GFSbox Known Answer Test
- KeySbox Known Answer Test

Triple DES 専用の検証項目

- Inverse Permutation Known Answer Test
- Permutation Operation Known Answer Test
- Substitution Table Known Answer Test

他のブロック暗号用の検証項目

- Sbox Known Answer Test

Sbox Known Answer Test は，AES の場合の GFSbox Test と KeySbox Test，Triple DES の場合の Substitution Known Answer Test に相当するものである.

2.8. ストリーム暗号

ストリーム暗号の試験対象機能は次の通り.

- 暗号化機能
- 復号機能

試験項目を次に示す.

- Variable Plaintext (Ciphertext) Known Answer Test
- Variable Key Known Answer Test
- Multi-block Message Test
- Monte Carlo Test

ただし，MULTI-S01 は復号の際にメッセージ認証も行うことができるので，メッセージ認証機能の試験も行う.

2.9. ハッシュ関数

ハッシュ関数の試験項目を次に示す.

- The short messages test
- The selected long messages test
- The pseudo randomly generated messages test

2.10. メッセージ認証

メッセージ認証の試験項目を次に示す.

- The short messages test
- The selected long messages test
- The pseudo randomly generated messages test

2.11. 擬似乱数生成関数

擬似乱数生成関数の試験項目を次に示す.

- Variable Seed Test
- Monte Carlo Test

3. まとめ

JCATT は「暗号モジュールが“暗号アルゴリズム仕様書”に従って実装されているかどうかを検査する」ものである. 実際の暗号モジュールの試験にあたっては, JCATT に実装された試験項目以外にも, 適切なエラー処理がされているかどうかなど, 暗号アルゴリズム仕様書には記述されていない様々な項目の試験が必要である. 現時点の JCATT でカバーしていない試験項目をどう定め, どう試験するかなどの検討は今後の課題である. また, いくつかのブロック暗号動作モードなど, 現時点の JCATT に含まれていない. 暗号も存在する. それらの暗号に対する試験機能の追加も今後の課題である.

参考文献

[1] “CRYPTREC Report 2002 (暗号技術評価報告書),” IPA, TAO, 2003.

[2] L. E. Bassham III, “AESAVS,” NIST, 2002.

[3] L. E. Bassham III, “DSSVS,” NIST, 2001.

[4] S. S. Keller, “RSAVS,” NIST, 2004.

[5] L. E. Bassham III, “SHAVS,” NIST, 2004.

[6] L. E. Bassham III, “HMACVS,” NIST, 2004.

[7] L. E. Bassham III, “DSAVS,” NIST, 2004.

[8] L. E. Bassham III, “ECDSAVS,” NIST, 2004.

[9] L. E. Bassham III, “RNGVS,” NIST, 2005.

[10] NIST SP 800-17, “Modes of Operation Validation (MOVS): Requirements and Procedures,” S. Keller and M. Smid, NIST, 1998.

[11] NIST SP 800-20, “Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS) : Requirements and Procedures,” S. Keller, NIST, 2000.

[12] L. E. Bassham III, “CCMVS,” NIST, 2004.