2007 情財第 866 号

企業・個人の情報セキュリティ対策事業

暗号アルゴリズム実装試験ツールの機能追加

JCATT ファイルフォーマット仕様書

PSEC-KEM

2010 年 1 月

独立行政法人 情報処理推進機構

目 次

1　はじめに

暗号アルゴリズム実装試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する．JCATT が使用するファイルには次のようなものがある．

ファイルの種類

- パラメータファイル (*.par)
  試験項目の設定を記述する．JCATT を用いて作成する．
- リクエストファイル (*.req)
  暗号モジュール開発ベンダに対する要求を記述する．JCATT を用いて作成する．
- Facts ファイル (*.fax)
  テストベクタを記述する．JCATT を用いて作成する．
- レスポンスファイル (*.rsp)
  ベンダからの回答を記述する．リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する．
- 結果ファイル (*.out)
  試験結果を記述する．JCATT を用いて作成する．

これらのファイルの名前は，次の規則に従ってつけること．

ファイル名の規則

- 拡張子は，上記 ( ) 内に指定したものを使用すること．
- 拡張子以外の名前は，試験対象暗号モジュールごとに同じ名称をつけること．
  リクエストファイル (*.req) と Facts ファイル (*.fax) の生成時には，リクエストファイル (*.req) と Facts ファイル (*.fax) に対してパラメータファイル (*.par) と同じ名称を JCATT が自動的につける．
  試験実行時には，同じ名称のレスポンスファイル (*.rsp) と Facts ファイル (*.fax) に対して試験が行われる．また，試験実行時は，結果ファイル (*.out) に対して，Facts ファイル (*.fax) と同じ名称を JCATT が自動的につける．

ファイルフォーマット詳細は次章以降に記述する．各ファイルに共通の規則は次の通りである．

共通規則

- [　] で囲まれた “タグ” の次の行に値を記述する．
- タグは各ファイルフォーマットに記述した順番通りに記述すること．
- レスポンスファイルにおいては,【出力】と記述したタグが，試験対象モジュールが出力するデータを記述する箇所である．
- 半角英数字を用いること．
- タグおよび値は大文字小文字の区別をするので，大文字小文字を含めて正確に記述すること．ただし，数値を 16 進数で記述する場合は，大文字小文字は区別しない．
- 一文字目が ♯(半角) で始まるコメント行を自由に書き込むことができる．
- 平文，暗号文，鍵などのデータの区切り文字は改行 (CR+LF または LF) とする．
- 平文，暗号文，署名，鍵などのデータは 16 進表記とする．
- ビット数，個数などの数値は 10 進表記とする．
- ACSII コードを使用すること．
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)．

2　楕円曲線ドメインパラメータ

パラメータ a, b で定義された楕円曲線上の点 $P = (x_P, y_P)$ のオクテット列表現は，“SEC 1: Elliptic Curve Cryptography”の 2.3.3 節 (または 2.3.4 節) の記述に従うこと．すなわち，オクテット列は先頭バイトの値に従って以下のように解釈される．($\|$ はオクテット列の連接を表す．)

オクテット列	点への変換法
00	P は無限遠点とする
02 $\|$ X	$x_P = X$ とする．y_P は以下に記載する方法で導出する
03 $\|$ X	$x_P = X$ とする．y_P は以下に記載する方法で導出する
04 $\|$ X $\|$ Y	$P = (x_P, y_P) = (X, Y)$ とする

オクテット列の先頭バイトが 02 あるいは 03 の場合，以下の方法で y_P を導出する．一般に，与えられた x_P に対して y_P の候補は高々2 個である．そのうち，以下の基準で選択されたものを y_P 座標とする．

1. オクテット列の先頭バイトが 02 の場合，$\tilde{y} = 0$ とする．
   オクテット列の先頭バイトが 03 の場合，$\tilde{y} = 1$ とする．
2. 体の位数が素数 p の場合，2 で割った余りが $\tilde{y}$ と等しいものを y_P とする．
3. 体の位数が 2^m で，$X = 0$ の場合，$y_P = b^{2^{m-1}}$ とする．
4. 体の位数が 2^m で，$X \neq 0$ の場合，$y_P x_P^{-1}$ の (多項式表現における) 定数項の値が $\tilde{y}$ と等しいものを y_P とする．

楕円曲線暗号ドメインパラメータは，タグ [Domain Parameter] の下に，以下の順 (各パラメータにつき 1 行) でオクテット列で記述すること．ただし，h は 32 ビット未満の整数で記述すること．

標数 p の場合

- 標数 p [16 進数表記]
- 曲線パラメータ a [16 進数表記]
- 曲線パラメータ b [16 進数表記]
- ベースポイント G [16 進数表記]
- G の位数 n [16 進数表記]
- コファクター h [10 進数表記]

標数 2 の場合

- 拡大次数 m [10 進数表記]
- m 次既約多項式 $f(x)$ [16 進数表記]
- 曲線パラメータ a [16 進数表記]
- 曲線パラメータ b [16 進数表記]
- ベースポイント G [16 進数表記]
- G の位数 n [16 進数表記]
- コファクター h [10 進数表記]

楕円曲線暗号アルゴリズムのドメインパラメータ生成機能から出力される SEED(検証可能なランダム曲線であることを証明するために必要なパラメータ) をファイルに記述する場合，上記ドメインパラメータの直後にタグ [SEED] を記述し，その下の行に SEED 値を記述すること．

つまり，楕円曲線ドメインパラメータは次のように記述する．

[Domain Parameter]
. . . ♯ 1 つ目のドメインパラメータ (SEED 以外) を記述する．
[SEED]
. . . ♯ 1 つ目のドメインパラメータの SEED 値 [16 進数表記]
[Domain Parameter]
. . . ♯ 2 つ目のドメインパラメータ (SEED 以外) を記述する．
[SEED]
. . . ♯ 2 つ目のドメインパラメータの SEED 値 [16 進数表記]

3 PSEC-KEM

PSEC-KEM の暗号アルゴリズム実装試験のためのファイルフォーマットを記述する.
各表中，鍵導出関数識別子, マスク生成時の点形式は下表の通りである.

表 1: 鍵導出関数識別子

識別子	対応する鍵導出関数
M_Kdf_ISO18033_2_KDF1_SHA1	ISO/IEC 18033-2 KDF1 with SHA-1
M_Kdf_ISO18033_2_KDF1_SHA224	ISO/IEC 18033-2 KDF1 with SHA-224
M_Kdf_ISO18033_2_KDF1_SHA256	ISO/IEC 18033-2 KDF1 with SHA-256
M_Kdf_ISO18033_2_KDF1_SHA384	ISO/IEC 18033-2 KDF1 with SHA-384
M_Kdf_ISO18033_2_KDF1_SHA512	ISO/IEC 18033-2 KDF1 with SHA-512

表 2: マスク生成時の点形式

識別子	対応する点形式
M_ECP_ISO18033_2_UNCOMPRESSED	ISO/IEC 18033-2 第 5.4.3 節記載の uncompressed 形式
M_ECP_ISO18033_2_COMPRESSED	ISO/IEC 18033-2 第 5.4.3 節記載の compressed 形式
M_ECP_ISO18033_2_HYBRID	ISO/IEC 18033-2 第 5.4.3 節記載の hybrid 形式

リクエストファイル，Facts ファイル，レスポンスファイルの各表中，薄い網掛け のタグは脚注に補足説明があることを表す。濃い網掛け は，脚注の説明から参照されているタグであることを表す.

3.1 パラメータファイル (*.par)

表 3: PSEC-KEM パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	PSEC-KEM
	[Characteristic]	標数．標数に応じて p または 2 と記述すること．
セッション鍵暗号化	[Function Name]	Encryption
	[Domain Parameter]	ドメインパラメータ
	[Seed K]	鍵ペア生成のための擬似乱数生成用乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること)
	[Bitlength of Session Key]	セッション鍵のビット長
	[Number of Session Keys]	セッション鍵の個数
セッション鍵復号	[Function Name]	Decryption
	[Domain Parameter]	ドメインパラメータ
	[Seed K]	鍵ペア生成のための擬似乱数生成用乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること)
	[Bitlength of Session Key]	セッション鍵のビット長
	[Rate of Fail Data]	暗号文を改ざんする割合
	[Number of Session Keys]	セッション鍵の個数
鍵ペア生成	[Function Name]	Key Generation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	鍵の数

3.2 リクエストファイル (*.req)

表 4: PSEC-KEM リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	PSEC-KEM
	[Characteristic]	標数．標数に応じて p または 2 と記述すること．
セッション鍵暗号化	[Function Name]	Encryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること)
	[Bitlength of Session Key]	セッション鍵のビット長 [10 進数表記]
	[Public Key]	公開鍵 [16 進数表記]
	[Number of Session Keys]	セッション鍵の個数 [10 進数表記]
セッション鍵復号	[Function Name]	Decryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること) [10 進数表記]
	[Bitlength of Session Key]	セッション鍵のビット長 [10 進数表記]
	[Private Key]	プライベート鍵 [10 進数表記]
	[Number of Session Keys]	セッション鍵の個数 [10 進数表記]
	[Ciphertexts][1]	暗号文 C_0 [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	鍵の数 [10 進数表記]

注

1. [Number of Session Keys] 個の暗号文 C_0 を記述する．

3.3 Facts ファイル (*.fax)

表 5: PSEC-KEM Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	PSEC-KEM
	[Characteristic]	標数．標数に応じて p または 2 と記述すること．
セッション鍵暗号化	[Function Name]	Encryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること)
	[Bitlength of Session Key]	セッション鍵のビット長
	[Private Key]	プライベート鍵
	[Public Key]	公開鍵
	[Number of Session Keys]	セッション鍵の個数
セッション鍵復号	[Function Name]	Decryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること)
	[Bitlength of Session Key]	セッション鍵のビット長
	[Private Key]	プライベート鍵
	[Public Key]	公開鍵
	[Number of Session Keys]	セッション鍵の個数
	[Ciphertexts][1]	暗号文 C_0
	[Session Keys][1]	セッション鍵
鍵ペア生成	[Function Name]	Key Generation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	鍵の数

注

1. [Number of Session Keys] 個の暗号文 C_0 およびセッション鍵を記述する．復号に失敗した場合は，[Session Keys] データの該当行に `decryption error` と記述する．

3.4 レスポンスファイル (*.rsp)

表 6: PSEC-KEM レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	PSEC-KEM
	[Characteristic]	標数．標数に応じて p または 2 と記述すること．
セッション鍵暗号化	[Function Name]	Encryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること) [10 進数表記]
	[Bitlength of Session Key]	セッション鍵のビット長 [10 進数表記]
	[Public Key]	公開鍵 [16 進数表記]
	[Number of Session Keys]	セッション鍵の個数 [10 進数表記]
	[Ciphertexts][1]	【出力】暗号文 C_0 [16 進数表記]
セッション鍵復号	[Function Name]	Decryption
	[Domain Parameter]	ドメインパラメータ
	[KDF]	鍵導出関数識別子
	[ECP Format]	マスク生成時の点形式
	[Bitlength of Seed]	擬似乱数生成用乱数シードのビット長 (KDF に使用されるハッシュ関数のハッシュ長以上 512 ビット以下であること) [10 進数表記]
	[Bitlength of Session Key]	セッション鍵のビット長 [10 進数表記]
	[Private Key]	プライベート鍵 [16 進数表記]
	[Number of Session Keys]	セッション鍵の個数 [10 進数表記]
	[Ciphertexts][2]	暗号文 C_0 [16 進数表記]
	[Session Keys][2]	【出力】セッション鍵 [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	鍵の数 [10 進数表記]
	[Key Pair][3]	【出力】鍵ペア [16 進数表記]

注

1. [Number of Session Keys] 個の暗号文 C_0 を記述する．
2. [Number of Session Keys] 個の暗号文 C_0 およびセッション鍵を記述する．復号に失敗した場合は，[Session Keys] データの該当行に `decryption error` と記述する．

3. [Number of Keys] 個の [Key Pair] データ．ただし，鍵ペアデータは，プライベート鍵と公開鍵を 2 行で以下のように記述する．

   [Key Pair]
   . . . ♯ 1 つ目のプライベート鍵を記述する．
   . . . ♯ 1 つ目の公開鍵を記述する．
   [Key Pair]
   . . . ♯ 2 つ目のプライベート鍵を記述する．
   . . . ♯ 2 つ目の公開鍵を記述する．

3.5 結果ファイル (*.out)

表 7: PSEC-KEM 結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Characteristic]	標数．標数に応じて p または 2 と記述する．
[Function Name]	試験対象機能名
[Results]	試験結果

注

- 試験合格の場合，[Results] に OK と表示される．
- 試験不合格の場合，[Results] に何らかの形式で NG と表示される．また，[Results] には，レスポンスファイル内の不合格となったデータが記述されているタグ名と，そのタグ内の何番目 (No.，#等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし,【出力】と記述したタグが 1 つしかない場合，タグ名は省略することがある．

改版履歴

改訂年月日	作成者・承認者	改訂内容
2008 年 4 月 11 日	櫻井・近藤	新規公開
2010 年 1 月 21 日	橋本・近藤	楕円曲線ドメインパラメータについての記述を修正