JCATT ファイルフォーマット仕様書

$\mathbb{F}_p$ 上 ECDSA

2018 年 11 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，試験対象実装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

- JCATT 互換ファイルフォーマットの選択時, [　　] で囲まれた “タグ” の次の行に値を記述する．
- CAVS 準互換ファイルフォーマットの選択時, 〈 タグ 〉=〈 値 〉 の形式で 1 行で記述する．
- ヘッダ部分については各行について [〈 タグ 〉=〈 値 〉] の形式で 1 行で記述する．
- レスポンスファイルにおいては，【出力】と記述したタグが，試験対象実装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]

3 $\mathbb{F}_p$ 上 ECDSA

$\mathbb{F}_p$ 上 ECDSA 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．

3.1 JCATT2 互換ファイルフォーマット

各表において，試験方法に関する以下の略語を使用する．

- RGT: Random Generation Test(「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.」に対する試験)

試験方法の詳細は，暗号アルゴリズム実装試験仕様書を参照のこと．
各表中，ハッシュ関数識別子は下表の通りである．

表1　ハッシュ関数識別子

ハッシュ関数識別子	対応するハッシュ関数
M_Hash_SHA1	SHA-1
M_Hash_SHA224	SHA-224
M_Hash_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512

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．

3.1.1 パラメータファイル (*.par)

表2 $\mathbb{F}_p$ 上 ECDSA パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
署名生成	[Function Name]	Sign
	[Domain Parameter]	ドメインパラメータ
	[Hash]	ハッシュ関数識別子
	[Seed P]	ランダムな平文を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed P]	Seed P のビット長
	[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
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Seed S]	一時秘密鍵 k を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed S][1]	常に 0 と記述する．
	[Flag of Ephemeral Secret Keys][1]	常に 0 と記述する．
	[Number of Signatures for RGT]	RGT で生成する署名の個数．
署名検証	[Function Name]	Verification
	[Domain Parameter]	署名生成と同じ
	[Hash]	
	[Seed P]	
	[Bitlength of Seed P]	
	[Seed K]	
	[Bitlength of Seed K]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Seed S]	一時秘密鍵 k を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed S]	Seed S のビット長
	[Rate of Fail Data]	署名検証が不合格になる割合

注

1. 署名生成機能に対して，Known Answer Test する場合，この 2 つのタグで，どの試験を実施するか識別することができる．ただし，本 JCATT では Known Answer Test は行わないため，この 2 つのタグは常に 0 と記述する．Known Answer Test する場合，タグ [Flag of Ephemeral Secret Keys] および [Bitlength of Seed S] の値を下表のように使用することを想定している．

([Flag of Ephemeral Secret Keys], [Bitlength of Seed S])	実行する試験項目
(0,0)	本 JCATT の試験
(0,≠0)	擬似乱数生成関数と乱数シードを指定することによる署名値の Known Answer Test
(≠0,≠0)	一時鍵 k の値を指定することによる署名値の Known Answer Test
(≠0,0)	エラー

表3　$\mathbb{F}_p$ 上 ECDSA パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
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
公開鍵検証	[Function Name]	Public Key Validation
	[Domain Parameter]	ドメインパラメータ
	[Seed K]	公開鍵を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[Number of Keys]	鍵の数
	[Rate of Fail Data]	公開鍵検証が不合格になる割合
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Bitlength of p]	p のビット長
	[Bitlength of SEED][1]	曲線のランダム性検証用 SEED のビット長
	[Number of Domain Parameters]	生成するドメインパラメータの個数
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Bitlength of p]	p のビット長
	[Domain Parameter]	ドメインパラメータ
	[SEED]	曲線のランダム性検証用 SEED
	[Bitlength of SEED][2]	曲線のランダム性検証用 SEED のビット長

1. ドメインパラメータ生成機能に対する 2 つの試験項目のうちどちらを実施するかをタグ [Bitlength of SEED] で識別する．タグの値と実施する試験項目との関係は次の通りである．

[Bitlength of SEED]	試験項目
0	試験 1
≠0	試験 2

2. ドメインパラメータ検証機能に対する 2 つの試験項目のうちどちらを実施するかをタグ [Bitlength of SEED] で識別する．タグの値と実施する試験項目との関係は次の通りである．

[Bitlength of SEED]	試験項目
0	試験 1
≠0	試験 2

3.1.2 リクエストファイル (*.req)

表4 $\mathbb{F}_p$ 上 ECDSA リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
署名生成	[Function Name]	Sign
	[Domain Parameter]	ドメインパラメータ
	[Hash]	ハッシュ関数識別子
	[Private Key]	プライベート鍵 [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts][1]	平文 [16 進数表記]
	[Number of Signatures for RGT]	RGT で生成する署名の個数．[10 進数表記]
署名検証	[Function Name]	Verification
	[Domain Parameter]	署名生成と同じ
	[Hash]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Public Keys][2]	公開鍵 [16 進数表記]
	[Plaintexts][2]	平文 [16 進数表記]
	[Signatures][2]	署名．1 つの署名を r と s の順に 1 行で記述する．[16 進数表記]

注

1. [Number of Plaintexts] 個の平文を (各平文を 1 行で) 記述する．
2. [Number of Plaintexts] 個の公開鍵，平文および署名を (各 1 行で) 記述する．

表5　$\mathbb{F}_p$ 上 ECDSA リクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
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]
公開鍵検証	[Function Name]	Public Key Validation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	公開鍵の数 [10 進数表記]
	[Public Keys][1]	公開鍵 [16 進数表記]
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Bitlength of p]	p のビット長 [10 進数表記]
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．[10 進数表記]
	[Number of Domain Parameters]	生成するドメインパラメータの個数 [10 進数表記]
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Number of Domain Parameters]	検証するドメインパラメータの個数 [10 進数表記]
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．[10 進数表記]
	[Domain Parameter][2]	ドメインパラメータ
	[SEED][2]	曲線のランダム性検証用 SEED [16 進数表記]

注

1. [Number of Keys] 個の公開鍵 (1 つの公開鍵につき 1 行) を記述する．
2. [Number of Domain Parameters] 個の [Domain Parameter]，[SEED] を記述する．ただし，[Bitlength of SEED] が 0 の時は [SEED] の値は記述しない．

3.1.3 Facts ファイル (*.fax)

表6 $\mathbb{F}_p$ 上 ECDSA Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
署名生成	[Function Name]	Sign
	[Domain Parameter]	ドメインパラメータ
	[Hash]	ハッシュ関数識別子
	[Private Key]	プライベート鍵
	[Public Key]	公開鍵
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts][1]	平文
	[Ephemeral Secret Keys][2]	一時秘密鍵 k
	[Flag of Ephemeral Secret Keys]	一時秘密鍵 k のフラグ．0 : k を指定しない，1 : k を指定する．今回は常に 0.
	[Seed S]	一時秘密鍵 k 生成用乱数シード
	[Bitlength of Seed S]	Seed S のビット長
	[Signatures][3]	署名．1 つの署名を r と s の順に 1 行で記述する．
	[Number of Signatures for RGT]	RGT で生成する署名の個数．
署名検証	[Function Name]	Verification
	[Domain Parameter]	署名生成と同じ
	[Hash]	
	[Private Key]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Public Keys][4]	公開鍵
	[Plaintexts][4]	平文
	[Signatures][4]	署名．1 つの署名を r と s の順に 1 行で記述する．
	[Results][4]	署名検証結果．検証合格の時 0，不合格の時 1 と記述する．

注

1. [Number of Plaintexts] 個の平文，署名 (各平文，署名を 1 行で) を記述する．
2. [Flag of Ephemeral Secret Keys] が 0 でない時，[Number of Plaintexts] 個の一時秘密鍵 [Ephemeral Secret Keys] を記述する．
3. [Flag of Ephemeral Secret Keys] または [Bitlength of Seed S] が 0 でない時，[Number of Plaintexts] 個の署名からなる [Signatures] を記述する．そうでない時，[Signatures] の値は記述しない．
4. [Number of Plaintexts] 個の公開鍵，平文，署名，および署名検証結果を (各 1 行で) 記述する．

表7　$\mathbb{F}_p$ 上 ECDSA Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
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
公開鍵検証	[Function Name]	Public Key Validation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	鍵の数
	[Public Keys][1]	公開鍵
	[Results][1]	検証結果．検証合格の時 0，不合格の時 1 と記述する．
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Bitlength of p]	p のビット長
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．
	[Number of Domain Parameters]	生成するドメインパラメータの個数
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Number of Domain Parameters]	検証するドメインパラメータの個数
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．
	[Domain Parameter][2]	ドメインパラメータ
	[SEED][2]	曲線のランダム性検証用 SEED
	[Result][2]	検証結果．検証合格の時 0，不合格の時 1 と記述する．

注

1. [Number of Keys] 個の公開鍵 (1 つの公開鍵につき 1 行) および検証結果 (1 つの検証結果につき 1 行) を記述する．
2. [Number of Domain Parameters] 個の [Domain Parameter]，[SEED]，[Result] を記述する．ただし，[Bitlength of SEED] が 0 の時は [SEED] の値は記述しない．

3.1.4 レスポンスファイル (*.rsp)

表8 $\mathbb{F}_p$ 上 ECDSA レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
署名生成	[Function Name]	Sign
	[Domain Parameter]	ドメインパラメータ
	[Hash]	ハッシュ関数識別子
	[Private Key]	プライベート鍵 [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts][1]	平文 [16 進数表記]
	[Signatures][1]	【出力】署名．1 つの署名を r と s の順に 1 行で記述する．[16 進数表記]
	[Number of Signatures for RGT]	RGT で生成する署名の個数．[10 進数表記]
	[Signatures for RGT][2]	【出力】RGT で生成された署名．1 つの署名を r と s の順に 1 行で記述する．[16 進数表記]
署名検証	[Function Name]	Verification
	[Domain Parameter]	署名生成と同じ
	[Hash]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Public Keys][3]	公開鍵 [16 進数表記]
	[Plaintexts][3]	平文 [16 進数表記]
	[Signatures][3]	署名．1 つの署名を r と s の順に 1 行で記述する．[16 進数表記]
	[Results][3]	【出力】署名検証結果．検証合格の時 0，不合格の時 1 と記述する．

注

1. [Number of Plaintexts] 個の平文 (1 つの平文につき 1 行)，署名 (1 つの署名につき 1 行) を記述する．
2. [Plaintexts] データの 1 番目の平文を用いて生成した [Number of Signatures for RGT] 個の署名データを記述する．
3. [Number of Plaintexts] 個の公開鍵，平文，署名および署名検証結果を (各 1 行で) 記述する．

表9　$\mathbb{F}_p$ 上 ECDSA レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	ECDSA
	[Characteristic]	標数．p と記述すること．
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][1]	【出力】鍵ペア [16 進数表記]
公開鍵検証	[Function Name]	Public Key Validation
	[Domain Parameter]	ドメインパラメータ
	[Number of Keys]	公開鍵の数 [10 進数表記]
	[Public Keys][2]	公開鍵 [16 進数表記]
	[Results][2]	【出力】検証結果．検証合格の時 0，不合格の時 1 と記述する．
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Bitlength of p]	p のビット長 [10 進数表記]
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．
	[Number of Domain Parameters]	生成するドメインパラメータの個数 [10 進数表記]
	[Domain Parameter][3]	【出力】ドメインパラメータ
	[SEED][3]	【出力】曲線のランダム性検証用 SEED [16 進数表記]
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Number of Domain Parameters]	検証するドメインパラメータの個数 [10 進数表記]
	[Bitlength of SEED]	曲線のランダム性検証用 SEED のビット長．ビット長が 0 ではない時試験 2 を実行し，ビット長が 0 の時試験 1 を実行する．[10 進数表記]
	[Domain Parameter][4]	ドメインパラメータ
	[SEED][4]	曲線のランダム性検証用 SEED [16 進数表記]
	[Result][4]	【出力】検証結果．検証合格の時 0，不合格の時 1 と記述する．

注

1. [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．
2. [Number of Keys] 個の公開鍵 (1 つの公開鍵につき 1 行) および検証結果 (1 つの検証結果につき 1 行) を記述する．
3. [Number of Domain Parameters] 個の [Domain Parameter]，[SEED] を記述する．ただし，[Bitlength of SEED] が 0 の時は [SEED] を記述しても無視される．
4. [Number of Domain Parameters] 個の [Domain Parameter]，[SEED]，[Result] を記述する．ただし，[Bitlength of SEED] が 0 の時は [SEED] の値は記述しない．

3.1.5 結果ファイル (*.out)

表10 $\mathbb{F}_p$ 上 ECDSA 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何番目 (COUNT，# 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．

- 鍵ペア生成機能やドメインパラメータ試験機能に対する試験において試験不合格の場合，下記のようにどの条件で不合格 (NG) となったかも表示される．
  NG(#2 :n is not prime)
  この例では n は素数であるという条件を満たしていないことを示す．詳細は別紙の試験項目を記述した文書を参照のこと．