JCATT ファイルフォーマット仕様書

FIPS 202 に記載された可変長出力関数

2018 年 8 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　FIPS 202 に記載された可変長出力関数

可変長出力関数 (XOF:eXtendable Output Function) SHAKE128，SHAKE256 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．これらの可変長出力関数のファイルフォーマットは，`Algorithm Name` の他は各可変長出力関数で同じである．

`Algorithm Name` は，それぞれ下記の通り．

- SHAKE128
- SHAKE256

各表において，試験方法に関する以下の略語を使用する．

- SMT: Short Messages Test
- SLMT: Selected Long Messages Test
- PGMT: Pseudorandomly Generated Messages Test
- VOT: Variable Output Test

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．

2.1　CAVS 準互換ファイルフォーマット

この章で取り扱うファイルフォーマットでは, 可変長出力関数識別子として, 表1に記載された表現を用いる．

表1　可変長出力関数識別子

可変長出力関数識別子	対応する可変長出力関数
SHAKE128	`SHAKE128`
SHAKE256	`SHAKE256`

2.1.1　パラメータファイル (*.par)

表2　FIPS 202 に記載された可変長出力関数

機能	タグ		内容	表記
ハッシュ関数	全体ヘッダ	`AlgorithmName`	(可変長出力関数識別子)	文字列
		`BitOrientedInputCapability`	ビット単位での入力する機能の有無 (有:true, 無:false)	文字列
		`UpperboundOfSLMT`	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ	10 進
		`NumberOfInnerLoopsInPGMT`	PGMT の内側ループの回数	10 進
		`NumberOfOuterLoopsInPGMT`	PGMT の外側ループの回数	10 進
		`MinBitLengthOfOutputInPGMT`	PGMT の最小ビット長	10 進
		`MaxBitLengthOfOutputInPGMT`	PGMT の最大ビット長	10 進
		`BitOrientedOutputCapability`	ビット単位での出力する機能の有無 (有:true, 無:false)	文字列
		`MinBitLengthOfOutputInVOT`	VOT の最小ビット長	10 進
		`MaxBitLengthOfOutputInVOT`	VOT の最大ビット長	10 進

2.1.2 リクエストファイル (*.req)

表3: FIPS 202 に記載された可変長出力関数 リクエストファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—ハッシュ— 上の表記との対応	値の表記	例示
可変長出力関数	全体ヘッダ		AlgorithmName	可変長出力関数識別子.		文字列	[AlgorithmName = SHAKE256]
			BitOrientedInputCapability	ビット単位での入力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedInputCapability = true]
			UpperboundOfSLMT	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ		10 進表記	[UpperboundOfSLMT = 100]
			NumberOfInnerLoopsInPGMT	PGMT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInPGMT = 1000]
			NumberOfOuterLoopsInPGMT	PGMT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInPGMT = 100]
			MinBitLengthOfOutputInPGMT	PGMT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInPGMT = 16]
			MaxBitLengthOfOutputInPGMT	PGMT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInPGMT = 65536]
			BitOrientedOutputCapability	ビット単位での出力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedOutputCapability = true]
			MinBitLengthOfOutputInVOT	VOT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInVOT = 16]
			MaxBitLengthOfOutputInVOT	VOT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInVOT = 65536]
	SMT	SMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SMT 本体 *1 *2	COUNT	可変長出力関数の入力ブロック長 (ビット数) を r として, ・ビット単位での入力する機能有 (bit-oriented) の場合 0 以上 $2r+1$ 未満の整数 ・ビット単位での入力する機能無 (byte-oriented) の場合 0 以上 $r/4+1$ 未満の整数	i	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	$i =$ ⟨COUNT の値 ⟩ に対応する入力メッセージのビット長	10 進表記	Len = 0
			Msg	可変長出力関数の入力メッセージ	$i =$ ⟨COUNT の値 ⟩ に対応する入力メッセージ	16 進表記	Msg = 00
			Output	可変長出力関数の出力であるビット列	$i =$ ⟨COUNT の値 ⟩ に対応する可変長出力	16 進表記	Output = ?
	SLMT	SLMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SLMT 本体 *3	COUNT	0 以上 UpperboundOfSLMT 未満の整数	$i-1$	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	$i =$ ⟨COUNT + 1 の値 ⟩ に対応する入力メッセージのビット長	10 進表記	Len = 2177
			Msg	可変長出力関数の入力メッセージ	$i =$ ⟨COUNT + 1 の値 ⟩ に対応する入力メッセージ	16 進表記	Msg = 2f9a . . . 3664
			Output	可変長出力関数の出力であるビット列	$i =$ ⟨COUNT + 1 の値 ⟩ に対応する可変長出力	16 進表記	Output = ?
	PGMT	PGMT ヘッダ	⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInPGMT		文字列	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInPGMT		文字列	[Maximum Output Length (bits) = 65536]
			Msg	PGMT の msg	msg	16 進表記	Msg = 50c2 . . . a265
		PGMT *4	COUNT	0 以上 NumberOfOuterLoopsInPGMT 未満の整数	j	10 進表記	COUNT = 0
			Outputlen	可変長出力関数の出力ビット長	$j =$ ⟨COUNT の値 ⟩ に対応する $Outputlen_j$	10 進表記	Outputlen = ?
			Output	可変長出力関数の出力であるビット列	$j =$ ⟨COUNT の値 ⟩ に対応する $Output_j$	16 進表記	Output = ?
	VOT	VOT ヘッダ	⟨ 可変長出力のテストの対象の種別 ⟩	ビット単位での入力する機能の有無		文字列	[Tested for Output of bit-oriented messages]
			⟨ 入力メッセージのビット数 ⟩		$input\_len$	10 進表記	[Input Length = 256]
			⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInVOT	$minoutlen$	10 進表記	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInVOT	$maxoutlen$	10 進表記	[Maximum Output Length (bits) = 65536]
		VOT *5	COUNT	0 以上 4000 以下の整数		10 進表記	COUNT = 0
			Outputlen	可変長出力関数の出力ビット長		10 進表記	Outputlen = 16
			Msg	可変長出力関数の入力メッセージ		16 進表記	Msg = 2f9a . . . 3664
			Output	可変長出力関数の出力であるビット列		16 進表記	Output = ?

*1 ビット単位での入力する機能有 (bit-oriented) の場合, $2r+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0              # i = 0 のデータの組について記述する.
Len = 0                # i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00               # i = 0 に対応する入力メッセージを記述する.
Output = ?             # i = 0 に対応する可変長出力のプレースホルダ.

COUNT = 1              # i = 1 のデータの組について記述する.
Len = 1                # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 01               # i = 1 に対応する入力メッセージを記述する.
Output = ?             # i = 1 に対応する可変長出力のプレースホルダ.

.
.
.
COUNT = ⟨2r⟩           # i = ⟨2r⟩ のデータの組について記述する.
Len = 2176             # i = ⟨2r⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2  # i = ⟨2r⟩ に対応する入力メッセージを記述する.
Output = ?             # i = ⟨2r⟩ に対応する可変長出力のプレースホルダ.
```

*2 ビット単位での入力する機能無 (byte-oriented) の場合, $r/8+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0              # i = 0 のデータの組について記述する.
Len = 0                # i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00               # i = 0 に対応する入力メッセージを記述する.
Output = ?             # i = 0 に対応する可変長出力のプレースホルダ.

COUNT = 1              # i = 1 のデータの組について記述する.
Len = 8                # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 30               # i = 1 に対応する入力メッセージを記述する.
Output = ?             # i = 1 に対応する可変長出力のプレースホルダ.

.
.
.
COUNT = ⟨r/4⟩          # i = ⟨r/4⟩ のデータの組について記述する.
Len = 2176             # i = ⟨r/4⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2  # i = ⟨r/4⟩ に対応する入力メッセージを記述する.
Output = ?             # i = ⟨r/4⟩ に対応する可変長出力のプレースホルダ.
```

*3 UpperboundOfSLMT 個の各データの組を以下のように記述する.

```
COUNT = 0                          # i = 1 のデータの組について記述する.
Len = 2177                         # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 2f9a . . . 3664              # i = 1 に対応する入力メッセージを記述する.
Output = ?                         # i = 1 に対応する可変長出力のプレースホルダ.

COUNT = 1                          # i = 2 のデータの組について記述する.
Len = 3266                         # i = 2 に対応する入力メッセージのビット長を記述する.
Msg = bbef . . . 1429              # i = 2 に対応する入力メッセージを記述する.
Output = ?                         # i = 2 に対応する可変長出力のプレースホルダ.

.
.
.
COUNT = ⟨ UpperboundOfSLMT - 1 ⟩   # i = ⟨ UpperboundOfSLMT ⟩ のデータの組について記述する.
Len = 110688                       # i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2              # i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージを記述する.
Output = ?                         # i = ⟨ UpperboundOfSLMT ⟩ に対応する可変長出力のプレースホルダ.
```

*4 NumberOfOuterLoopsInPGMT 個の各データの組を以下のように記述する.

```
COUNT = 0                              # j = 0 のデータの組について記述する.
Outputlen = ?                          # j = 0 に対応する出力のビット長のプレースホルダ.
Output = ?                             # j = 0 に対応する可変長出力のプレースホルダ.

COUNT = 1                              # j = 1 のデータの組について記述する.
Outputlen = ?                          # j = 1 に対応する出力のビット長のプレースホルダ.
Output = ?                             # j = 1 に対応する可変長出力のプレースホルダ.

.
.
.
COUNT = ⟨ NumberOfOuterLoopsInPGMT −1⟩ # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ のデータの組について記述する.
Outputlen = ?                          # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応する出力のビット長のプレースホルダ.
Output = ?                             # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応する可変長出力のプレースホルダ.
```

*5 各データの組を以下のように記述する.

```
COUNT = 0                  # j = 0 のデータの組について記述する.
Outputlen = 16             # j = 0 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced      # j = 0 に対応する入力メッセージを記述する.
Output = ?                 # j = 0 に対応する可変長出力のプレースホルダ.

COUNT = 1                  # j = 1 のデータの組について記述する.
Outputlen = 73             # j = 1 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced      # j = 1 に対応する入力メッセージを記述する.
Output = ?                 # j = 1 に対応する可変長出力のプレースホルダ.

.
.
.
COUNT = ⟨ 4000 未満の値 ⟩  # VOT の最大ビット長又はそれに近い値の出力ビット長のデータの組について記述する.
Outputlen = 65536          # VOT の最大ビット長又はそれに近い値の出力ビット長を記述する.
Msg = 5551 . . . 4ced      # VOT の最大ビット長又はそれに近い値の出力ビット長の試験に対応する入力メッセージを記述する.
Output = ?                 # VOT の最大ビット長又はそれに近い値の出力ビット長に対応する可変長出力のプレースホルダ.
```

2.1.3 Facts ファイル (*.fax)

表4: FIPS 202 に記載された可変長出力関数 Facts ファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—ハッシュ— 上の表記との対応	値の表記	例示
可変長出力関数	全体ヘッダ		AlgorithmName	可変長出力関数識別子.		文字列	[AlgorithmName = SHAKE256]
			BitOrientedInputCapability	ビット単位での入力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedInputCapability = true]
			UpperboundOfSLMT	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ		10 進表記	[UpperboundOfSLMT = 100]
			NumberOfInnerLoopsInPGMT	PGMT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInPGMT = 1000]
			NumberOfOuterLoopsInPGMT	PGMT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInPGMT = 100]
			MinBitLengthOfOutputInPGMT	PGMT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInPGMT = 16]
			MaxBitLengthOfOutputInPGMT	PGMT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInPGMT = 65536]
			BitOrientedOutputCapability	ビット単位での出力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedOutputCapability = true]
			MinBitLengthOfOutputInVOT	VOT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInVOT = 16]
			MaxBitLengthOfOutputInVOT	VOT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInVOT = 65536]
	SMT	SMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SMT 本体 *1 *2	COUNT	可変長出力関数の入力ブロック長 (ビット数) を r として, ・ビット単位での入力する機能有 (bit-oriented) の場合 0 以上 $2r+1$ 未満の整数 ・ビット単位での入力する機能無 (byte-oriented) の場合 0 以上 $r/8+1$ 未満の整数	i	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	i = ⟨COUNT の値 ⟩ に対応する入力メッセージのビット長	10 進表記	Len = 0
			Msg	可変長出力関数の入力メッセージ	i = ⟨COUNT の値 ⟩ に対応する入力メッセージ	16 進表記	Msg = 00
			Output	可変長出力関数の出力であるビット列	i = ⟨COUNT の値 ⟩ に対応する可変長出力	16 進表記	Output = e3b0 . . . b855
	SLMT	SLMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SLMT 本体 *3	COUNT	0 以上 UpperboundOfSLMT 未満の整数	$i-1$	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	i = ⟨COUNT + 1 の値 ⟩ に対応する入力メッセージのビット長	10 進表記	Len = 2177
			Msg	可変長出力関数の入力メッセージ	i = ⟨COUNT + 1 の値 ⟩ に対応する入力メッセージ	16 進表記	Msg = 2f9a . . . 3664
			Output	可変長出力関数の出力であるビット列	i = ⟨COUNT + 1 の値 ⟩ に対応する可変長出力	16 進表記	Output = 12df . . . 8e43
	PGMT	PGMT ヘッダ	⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInPGMT		文字列	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInPGMT		文字列	[Maximum Output Length (bits) = 65536]
			Msg	PGMT の msg	msg	16 進表記	Msg = 50c2 . . . a265
		PGMT *4	COUNT	0 以上 NumberOfOuterLoopsInPGMT 未満の整数	j	10 進表記	COUNT = 0
			Outputlen	可変長出力関数の出力ビット長	j = ⟨COUNT の値 ⟩ に対応する $Outputlen_j$	10 進表記	Outputlen = 16
			Output	可変長出力関数の出力であるビット列	j = ⟨COUNT の値 ⟩ に対応する $Output_j$	16 進表記	Output = 12df . . . 8e43
	VOT	VOT ヘッダ	⟨ 可変長出力のテストの対象の種別 ⟩	ビット単位での入力する機能の有無		文字列	[Tested for Output of bit-oriented messages]
			⟨ 入力メッセージのビット数 ⟩		$input\_len$	10 進表記	[Input Length = 256]
			⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInVOT	$minoutlen$	10 進表記	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInVOT	$maxoutlen$	10 進表記	[Maximum Output Length (bits) = 65536]
		VOT *5	COUNT	0 以上 4000 以下の整数		10 進表記	COUNT = 0
			Outputlen	可変長出力関数の出力ビット長		10 進表記	Outputlen = 16
			Msg	可変長出力関数の入力メッセージ		16 進表記	Msg = 2f9a . . . 3664
			Output	可変長出力関数の出力であるビット列		16 進表記	Output = 12df . . . 8e43

*1 ビット単位での入力する機能有 (bit-oriented) の場合, $2r+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0                 ♯ i = 0 のデータの組について記述する.
Len = 0                   ♯ i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00                  ♯ i = 0 に対応する入力メッセージを記述する.
Output = e3b0 . . . b855  ♯ i = 0 に対応する可変長出力の期待値を記述する.

COUNT = 1                 ♯ i = 1 のデータの組について記述する.
Len = 1                   ♯ i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 01                  ♯ i = 1 に対応する入力メッセージを記述する.
Output = 0a2c . . . ab38  ♯ i = 1 に対応する可変長出力の期待値を記述する.

.
.
.
COUNT = ⟨2r⟩              ♯ i = ⟨2r⟩ のデータの組について記述する.
Len = 2176                ♯ i = ⟨2r⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2     ♯ i = ⟨2r⟩ に対応する入力メッセージを記述する.
Output = 4b53 . . . 275b  ♯ i = ⟨2r⟩ に対応する可変長出力の期待値を記述する.
```

*2 ビット単位での入力する機能無 (byte-oriented) の場合, $r/8+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0                 ♯ i = 0 のデータの組について記述する.
Len = 0                   ♯ i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00                  ♯ i = 0 に対応する入力メッセージを記述する.
Output = e3b0 . . . b855  ♯ i = 0 に対応する可変長出力の期待値を記述する.

COUNT = 1                 ♯ i = 1 のデータの組について記述する.
Len = 8                   ♯ i = 1 に対応する入力メッセージのビット長を記述する.
Msg = d6                  ♯ i = 1 に対応する入力メッセージを記述する.
Output = 0a2c . . . ab38  ♯ i = 1 に対応する可変長出力の期待値を記述する.

.
.
.
COUNT = ⟨r/4⟩             ♯ i = ⟨r/4⟩ のデータの組について記述する.
Len = 2176                ♯ i = ⟨r/4⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2     ♯ i = ⟨r/4⟩ に対応する入力メッセージを記述する.
Output = 4b53 . . . 275b  ♯ i = ⟨r/4⟩ に対応する可変長出力の期待値を記述する.
```

*3 UpperboundOfSLMT 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 1 のデータの組について記述する.
Len = 2177                         ♯ i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 2f9a . . . 3664              ♯ i = 1 に対応する入力メッセージを記述する.
Output = 12df . . . 8e43           ♯ i = 1 に対応する可変長出力の期待値を記述する.

COUNT = 1                          ♯ i = 2 のデータの組について記述する.
Len = 3266                         ♯ i = 2 に対応する入力メッセージのビット長を記述する.
Msg = bbef . . . 1429              ♯ i = 2 に対応する入力メッセージを記述する.
Output = edcb . . . 4ddd           ♯ i = 2 に対応する可変長出力の期待値を記述する.

.
.
.
COUNT = ⟨ UpperboundOfSLMT - 1 ⟩   ♯ i = ⟨ UpperboundOfSLMT ⟩ のデータの組について記述する.
Len = 110688                       ♯ i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージのビット長を記述する.
Msg = c354 . . . 7fef              ♯ i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージを記述する.
Output = 9d88 . . . 11a1           ♯ i = ⟨ UpperboundOfSLMT ⟩ に対応する可変長出力の期待値を記述する.
```

*4 NumberOfOuterLoopsInPGMT 個の各データの組を以下のように記述する.

```
COUNT = 0                                ♯ j = 0 のデータの組について記述する.
Outputlen = 3600                         ♯ j = 0 に対応する出力のビット長の期待値を記述する.
Output = 0506 . . . 1746                 ♯ j = 0 に対応する可変長出力の期待値を記述する.

COUNT = 1                                ♯ j = 1 のデータの組について記述する.
Outputlen = 22464                        ♯ j = 1 に対応する出力のビット長の期待値を記述する.
Output = 263e . . . 1a33                 ♯ j = 1 に対応する可変長出力の期待値を記述する.

.
.
.
COUNT = ⟨ NumberOfOuterLoopsInPGMT −1⟩   ♯ j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ のデータの組について記述する.
Outputlen = 25920                        ♯ j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応する出力のビット長の期待値を記述する.
Output = 8d59 . . . 13f9                 ♯ j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応する可変長出力の期待値を記述する.
```

*5 各データの組を以下のように記述する.

```
COUNT = 0                  ♯ j = 0 のデータの組について記述する.
Outputlen = 16             ♯ j = 0 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced      ♯ j = 0 に対応する入力メッセージを記述する.
Output = 9dc2              ♯ j = 0 に対応する可変長出力の期待値を記述する.

COUNT = 1                  ♯ j = 1 のデータの組について記述する.
Outputlen = 73             ♯ j = 1 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced      ♯ j = 1 に対応する入力メッセージを記述する.
Output = 1da9 . . . a201   ♯ j = 1 に対応する可変長出力の期待値を記述する.

.
.
.
COUNT = ⟨ 4000 未満の値 ⟩  ♯ VOT の最大ビット長又はそれに近い値の出力ビット長のデータの組について記述する.
Outputlen = 65536          ♯ VOT の最大ビット長又はそれに近い値の出力ビット長を記述する.
Msg = 5551 . . . 4ced      ♯ VOT の最大ビット長又はそれに近い値の出力ビット長の試験に対応する入力メッセージを記述する.
Output = 9c42 . . . fd07   ♯ VOT の最大ビット長又はそれに近い値の出力ビット長に対応する可変長出力の期待値を記述する.
```

2.1.4 レスポンスファイル (*.rsp)

表5: FIPS 202 に記載された可変長出力関数 レスポンスファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—ハッシュ— 上の表記との対応	値の表記	例示
可変長出力関数	全体ヘッダ		AlgorithmName	可変長出力関数識別子.		文字列	[AlgorithmName = SHAKE256]
			BitOrientedInputCapability	ビット単位での入力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedInputCapability = true]
			UpperboundOfSLMT	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ		10 進表記	[UpperboundOfSLMT = 100]
			NumberOfInnerLoopsInPGMT	PGMT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInPGMT = 1000]
			NumberOfOuterLoopsInPGMT	PGMT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInPGMT = 100]
			MinBitLengthOfOutputInPGMT	PGMT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInPGMT = 16]
			MaxBitLengthOfOutputInPGMT	PGMT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInPGMT = 65536]
			BitOrientedOutputCapability	ビット単位での出力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedOutputCapability = true]
			MinBitLengthOfOutputInVOT	VOT の最小ビット長	$minoutlen$	10 進表記	[MinBitLengthOfOutputInVOT = 16]
			MaxBitLengthOfOutputInVOT	VOT の最大ビット長	$maxoutlen$	10 進表記	[MaxBitLengthOfOutputInVOT = 65536]
	SMT	SMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SMT 本体 *1 *2	COUNT	可変長出力関数の入力ブロック長 (ビット数) を r として, ・ビット単位での入力する機能有 (bit-oriented) の場合 0 以上 $2r+1$ 未満の整数 ・ビット単位での入力する機能無 (byte-oriented) の場合 0 以上 $r/8+1$ 未満の整数	i	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	$i =$ ⟨COUNT の値⟩ に対応する入力メッセージのビット長	10 進表記	Len = 0
			Msg	可変長出力関数の入力メッセージ	$i =$ ⟨COUNT の値⟩ に対応する入力メッセージ	16 進表記	Msg = 00
			Output	【出力】可変長出力関数の出力であるビット列	$i =$ ⟨COUNT の値⟩ に対応する可変長出力	16 進表記	Output = e3b0 . . . b855
	SLMT	SLMT ヘッダ	⟨ 可変長出力のビット数 ⟩			10 進数	[Outputlen = 256]
		SLMT 本体 *3	COUNT	0 以上 UpperboundOfSLMT 未満の整数	$i-1$	10 進表記	COUNT = 0
			Len	可変長出力関数の入力メッセージのビット長	$i =$ ⟨COUNT + 1 の値⟩ に対応する入力メッセージのビット長	10 進表記	Len = 2177
			Msg	可変長出力関数の入力メッセージ	$i =$ ⟨COUNT + 1 の値⟩ に対応する入力メッセージ	16 進表記	Msg = 2f9a . . . 3664
			Output	【出力】可変長出力関数の出力であるビット列	$i =$ ⟨COUNT + 1 の値⟩ に対応する可変長出力	16 進表記	Output = 12df . . . 8e43
	PGMT	PGMT ヘッダ	⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInPGMT		文字列	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInPGMT		文字列	[Maximum Output Length (bits) = 65536]
			Msg	PGMT の msg	msg	16 進表記	Msg = 50c2 . . . a265
		PGMT *4	COUNT	0 以上 NumberOfOuterLoopsInPGMT 未満の整数	j	10 進表記	COUNT = 0
			Outputlen	【出力】可変長出力関数の出力ビット長	$j =$ ⟨COUNT の値⟩ に対応する $Outputlen_j$	10 進表記	Outputlen = 16
			Output	【出力】可変長出力関数の出力であるビット列	$j =$ ⟨COUNT の値⟩ に対応する $Output_j$	16 進表記	Output = 12df . . . 8e43
	VOT	VOT ヘッダ	⟨ 可変長出力のテストの対象の種別 ⟩	ビット単位での入力する機能の有無		文字列	[Tested for Output of bit-oriented messages]
			⟨ 入力メッセージのビット数 ⟩		$input\_len$	10 進表記	[Input Length = 256]
			⟨ 可変長出力の最小ビット数 ⟩	MinBitLengthOfOutputInVOT	$minoutlen$	10 進表記	[Minimum Output Length (bits) = 16]
			⟨ 可変長出力の最大ビット数 ⟩	MaxBitLengthOfOutputInVOT	$maxoutlen$	10 進表記	[Maximum Output Length (bits) = 65536]
		VOT *5	COUNT	0 以上 4000 以下の整数		10 進表記	COUNT = 0
			Outputlen	可変長出力関数の出力ビット長		10 進表記	Outputlen = 16
			Msg	【出力】可変長出力関数の入力メッセージ		16 進表記	Msg = 2f9a . . . 3664
			Output	【出力】可変長出力関数の出力であるビット列		16 進表記	Output = 12df . . . 8e43

*1 ビット単位での入力する機能有 (bit-oriented) の場合, $2r+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0                 # i = 0 のデータの組について記述する.
Len = 0                   # i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00                  # i = 0 に対応する入力メッセージを記述する.
Output = e3b0 . . . b855  # i = 0 に対応して生成された可変長出力.

COUNT = 1                 # i = 1 のデータの組について記述する.
Len = 1                   # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 01                  # i = 1 に対応する入力メッセージを記述する.
Output = 0a2c . . . ab38  # i = 1 に対応して生成された可変長出力.

.
.
.
COUNT = ⟨2r⟩              # i = ⟨2r⟩ のデータの組について記述する.
Len = 2176                # i = ⟨2r⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2     # i = ⟨2r⟩ に対応する入力メッセージを記述する.
Output = 4b53 . . . 275b  # i = ⟨2r⟩ に対応して生成された可変長出力.
```

*2 ビット単位での入力する機能無 (byte-oriented) の場合, $r/8+1$ 個の各データの組を以下のように記述する.

```
COUNT = 0                 # i = 0 のデータの組について記述する.
Len = 0                   # i = 0 に対応する入力メッセージのビット長を記述する.
Msg = 00                  # i = 0 に対応する入力メッセージを記述する.
Output = e3b0 . . . b855  # i = 0 に対応して生成された可変長出力.

COUNT = 1                 # i = 1 のデータの組について記述する.
Len = 8                   # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = d6                  # i = 1 に対応する入力メッセージを記述する.
Output = 0a2c . . . ab38  # i = 1 に対応して生成された可変長出力.

.
.
.
COUNT = ⟨r/4⟩             # i = ⟨r/4⟩ のデータの組について記述する.
Len = 2176                # i = ⟨r/4⟩ に対応する入力メッセージのビット長を記述する.
Msg = dc6f . . . c8f2     # i = ⟨r/4⟩ に対応する入力メッセージを記述する.
Output = 4b53 . . . 275b  # i = ⟨r/4⟩ に対応して生成された可変長出力.
```

*3 UpperboundOfSLMT 個の各データの組を以下のように記述する.

```
COUNT = 0                 # i = 1 のデータの組について記述する.
Len = 2177                # i = 1 に対応する入力メッセージのビット長を記述する.
Msg = 2f9a . . . 3664     # i = 1 に対応する入力メッセージを記述する.
Output = 12df . . . 8e43  # i = 1 に対応して生成された可変長出力.

COUNT = 1                 # i = 2 のデータの組について記述する.
Len = 3266                # i = 2 に対応する入力メッセージのビット長を記述する.
Msg = bbef . . . 1429     # i = 2 に対応する入力メッセージを記述する.
Output = edcb . . . 4ddd  # i = 2 に対応して生成された可変長出力.

.
.
.
COUNT = ⟨ UpperboundOfSLMT - 1 ⟩    # i = ⟨ UpperboundOfSLMT ⟩ のデータの組について記述する.
Len = 110688                        # i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージのビット長を記述する.
Msg = c354 . . . 7fef               # i = ⟨ UpperboundOfSLMT ⟩ に対応する入力メッセージを記述する.
Output = 9d88 . . . 11a1            # i = ⟨ UpperboundOfSLMT ⟩ に対応して生成された可変長出力.
```

*4 NumberOfOuterLoopsInPGMT 個の各データの組を以下のように記述する.

```
COUNT = 0                                  # j = 0 のデータの組について記述する.
Outputlen = 3600                           # j = 0 に対応する出力のビット長.
Output = 0506 . . . 1746                   # j = 0 に対応して生成された可変長出力.

COUNT = 1                                  # j = 1 のデータの組について記述する.
Outputlen = 22464                          # j = 1 に対応する出力のビット長.
Output = 263e . . . 1a33                   # j = 1 に対応して生成された可変長出力.

.
.
.
COUNT = ⟨ NumberOfOuterLoopsInPGMT −1⟩     # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ のデータの組について記述する.
Outputlen = 25920                          # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応する出力のビット長.
Output = 8d59 . . . 13f9                   # j = ⟨ NumberOfOuterLoopsInPGMT −1⟩ に対応して生成された可変長出力.
```

*5 各データの組を以下のように記述する.

```
COUNT = 0                 # j = 0 のデータの組について記述する.
Outputlen = 16            # j = 0 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced     # j = 0 に対応する入力メッセージを記述する.
Output = 9dc2             # j = 0 に対応して生成された可変長出力.

COUNT = 1                 # j = 1 のデータの組について記述する.
Outputlen = 73            # j = 1 に対応する出力のビット長を記述する.
Msg = 5551 . . . 4ced     # j = 1 に対応する入力メッセージを記述する.
Output = 1da9 . . . a201  # j = 1 に対応して生成された可変長出力.

.
.
.
COUNT = ⟨ 4000 未満の値 ⟩  # VOT の最大ビット長又はそれに近い値の出力ビット長のデータの組について記述する.
Outputlen = 65536          # VOT の最大ビット長又はそれに近い値の出力ビット長を記述する.
Msg = 5551 . . . 4ced      # VOT の最大ビット長又はそれに近い値の出力ビット長の試験に対応する入力メッセージを記述する.
Output = 9c42 . . . fd07   # VOT の最大ビット長又はそれに近い値の出力ビット長に対応して生成された可変長出力.
```

2.1.5 結果ファイル (*.out)

表6: FIPS 202 に記載された可変長出力関数 結果ファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書 ―ハッシュ― 上の表記との対応	値の表記	例示
可変長出力関数	全体ヘッダ		AlgorithmName	可変長出力関数識別子.		文字列	[AlgorithmName = SHAKE256]
			BitOrientedInputCapability	ビット単位での入力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedInputCapability = true]
			UpperboundOfSLMT	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ		10 進表記	[UpperboundOfSLMT = 100]
			NumberOfInnerLoopsInPGMT	PGMT の内側ループの回数	*innerloop*	10 進表記	[NumberOfInnerLoopsInPGMT = 1000]
			NumberOfOuterLoopsInPGMT	PGMT の外側ループの回数	*outerloop*	10 進表記	[NumberOfOuterLoopsInPGMT = 100]
			MinBitLengthOfOutputInPGMT	PGMT の最小ビット長	*minoutlen*	10 進表記	[MinBitLengthOfOutputInPGMT = 16]
			MaxBitLengthOfOutputInPGMT	PGMT の最大ビット長	*maxoutlen*	10 進表記	[MaxBitLengthOfOutputInPGMT = 65536]
			BitOrientedOutputCapability	ビット単位での出力する機能の有無 (有:true, 無:false)		文字列	[BitOrientedOutputCapability = true]
			MinBitLengthOfOutputInVOT	VOT の最小ビット長	*minoutlen*	10 進表記	[MinBitLengthOfOutputInVOT = 16]
			MaxBitLengthOfOutputInVOT	VOT の最大ビット長	*maxoutlen*	10 進表記	[MaxBitLengthOfOutputInVOT = 65536]
	SM	SMT ヘッダ	〈 可変長出力のビット数 〉			10 進数	[Outputlen = 256]
			〈 Results 〉	OK 又は NG		文字列	OK
	SL	SLMT ヘッダ	〈 可変長出力のビット数 〉			10 進数	[Outputlen = 256]
			〈 Results 〉	OK 又は NG		文字列	OK
	PGMT	PGMT ヘッダ	〈 可変長出力の最小ビット数 〉	MinBitLengthOfOutputInPGMT		文字列	[Minimum Output Length (bits) = 16]
			〈 可変長出力の最大ビット数 〉	MaxBitLengthOfOutputInPGMT		文字列	[Maximum Output Length (bits) = 65536]
			Msg	PGMT の msg	*msg*	16 進表記	Msg = 50c2 . . . a265
			〈 Results 〉	OK 又は NG		文字列	OK
	VOT	VOT ヘッダ	〈 可変長出力のテストの対象の種別 〉	ビット単位での入力する機能の有無		文字列	[Tested for Output of bit-oriented messages]
			〈 入力メッセージのビット数 〉		*input_len*	10 進表記	[Input Length = 256]
			〈 可変長出力の最小ビット数 〉	MinBitLengthOfOutputInVOT	*minoutlen*	10 進表記	[Minimum Output Length (bits) = 16]
			〈 可変長出力の最大ビット数 〉	MaxBitLengthOfOutputInVOT	*maxoutlen*	10 進表記	[Maximum Output Length (bits) = 65536]
			〈 Results 〉	OK 又は NG		文字列	OK

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．