1

記法

	自然数の集合
$a := b$	b の値を a に代入する. または, a は b で定義される.

: ビット長のビット列

処理手順

オクテット列 $M = M\ M_1 \ldots M_{n-1}$ をビット列 = $_1 \ldots$ $_{-1}$ へ以下の様に変換する:

1. 0 $\leq n-1$ の整数 に関して以下とする:

$-8-8(n-1-)$ - -

3　データ型 及び 変換　　*A*

基本的には 整数を q

入力:

M : オクテット列

: 整数

出力:

$\boldsymbol{a}$: 有限体の要素

処理手順:

以下の $\boldsymbol{a}$ を出力する.

$$\boldsymbol{a} := \text{I2RE} \quad \text{2I} \quad M,$$

3.9 楕円曲線上の点からオクテット列への変換 (P2 P

2.2.　:=　2RE　*X*,　とする.

2. .　= 02$_{16}$ なら ˜ := 0 とし,　= 0 $_{16}$ なら ˜ := 1 とし, それ以外なら “invali ” をエラー出力し停止する.

2. .　及び ˜ より楕円曲線上の点　=　,　を以下のように求める:

2. .1. q が奇数の場合, 有限体の要素 $\boldsymbol{w}$:=　+ $\boldsymbol{a}$　+　遵

- F, 鍵導出関数の選択
- h n, 非負整数

楕円曲線パラメータ は以下の九つ組 q, , β , a, , , p, p n, q n C

5 プリミティブ CR R RA R C R VES 1

: 非負整数

入力: l D 公開鍵
オクテット列

g オクテット列

. .1 1

MGF1

C

D 高速実装法

EC- EM を実装する場合, 以下の高速化技法を用いることができる.

- 楕円曲線演算を高速化する, 通常使える方法.
- 秘密鍵

F.1 推奨パラメータ変更の理由

推奨パラメータの変更のし

F.2 互換性が異のる場合のユーザーの不利益

EC-1, EC-2, EC- ,