高密度ナップザック暗号に対する攻撃

草薙 祥広 †　　長尾 篤 †　　森井 昌克 †

† 神戸大学大学院工学研究科
657-8501 兵庫県神戸市灘区六甲台町 1-1
kusanagi@stu.kobe-u.ac.jp
mmorii@kobe-u.ac.jp

あらまし　ナップザック暗号とはナップザック問題（特に部分和問題）を安全性の根拠とした公開鍵暗号の総称であり，密度が安全性の指標の一つとして用いられる．密度が 0.94 より小さい低密度な暗号は低密度攻撃により解読が可能となっている．低密度攻撃に耐性を持つには密度が 0.94 を超える必要があり，特に密度が 1 より大きい高密度なナップザック暗号が数多く提案されている．現在，高密度なナップザック暗号に対する包括的な攻撃は提案されていない．そこで筆者らは中間平文を用いた高密度ナップザック暗号に対する攻撃である中間平文偽造攻撃を提案した．中間平文偽造攻撃は部分和問題の解ではない擬似中間平文を用いた攻撃である．本稿では，中間平文偽造攻撃が有効なナップザック暗号について述べる．

Attack on High-Density Knapsack Cryptosystem

Yoshihiro Kusanagi†　　Atsushi Nagao†　　Masakatu Morii†

†Graduate School of Engineering, Kobe University,
1-1, Rokkodai, Nada, Kobe, Hyogo, 657-8501, Japan
kusanagi@stu.kobe-u.ac.jp
mmorii@kobe-u.ac.jp

Abstract　Knapsack cryptosystem is the public key cryptosystem based on the knapsack problem (especially subset sum problem). Density is used as one of the indicator in knapsack cryptosystem. Low-density knapsack cryptosystem, whose density is lower than 0.94, is broken comprehensively by Low-Density Attack. Hence, knapsack cryptosystem's density must be higher than 0.94, especially high-density knapsack cryptosystems, whose density are higher than 1, have been proposed. Until now, comprehensive attacks on high-density knapsack cryptosystem haven't proposed. Then, authors proposed an attack on high-density knapsack cryptosystem named Faked Intermediary Plaintext Attack. This attack uses pseudo intermediary plaintext that isn't the solution for subset sum problem. In this paper, we remark about the knapsack cryptosystem the attack is effective.

1　はじめに

ナップザック暗号とはナップザック問題を安全性の根拠とした公開鍵暗号の総称である．一般的にはナップザック問題の一部である部分和問題が用いられている．1978 年，Merkle と Hellman により初めてナップザック暗号が提案された（MH 暗号）[1]．しかし，MH 暗号は秘密鍵の

持つ超増加性を利用して公開鍵から秘密鍵を得ることができ，解読可能であることが示された [2]．また，1985 年 Lagarias と Odlyzko によって部分和問題そのものを精度よく求解するアルゴリズムが提案された [3]．これを低密度攻撃と呼ぶ．その後，Coster らの改良により，低密度攻撃は密度が 0.94 より小さいナップザック暗号を包括的に解読することが可能となり [4]，この攻撃に耐性を持つ密度が 1 より大きい高密度なナップザック暗号が数多く提案されている．なお，密度とはナップザック暗号の安全性を表す指標の一つである．

高密度ナップザック暗号は低密度攻撃に耐性を持つ一方，複雑な構成をとるため，低密度なナップザック暗号とは異なる脆弱性を抱える可能性がある．これは密度 1 を基準として高密度な暗号では部分和問題の解が複数生じるためである．低密度な暗号では平文を部分和問題の解とすることが一般的だが，高密度な暗号では平文の衝突が生じるためこのような構造をとることができない．そのため，高密度な暗号を実現するために何らかの前処理が必要となる．そのような前処理の一つに平文を中間平文に写像することが挙げられる．この写像は拡大写像と捉えることができ，中間平文を部分和問題の解とすることで高密度ナップザック暗号を実現することができる．中間平文を用いる暗号システムは，平文から一意に中間平文を導出される場合と，平文から複数の中間平文が導出される場合の二種類に分類できる．筆者らはこれら二種類の中間平文を用いて構成されるナップザック暗号に対する攻撃をそれぞれ提案した [5]．中間平文が一意に決定される場合は平文の一部を推定することで中間平文を多量に決定し，元の平文を導出することができる．また，中間平文が複数存在する場合は中間平分偽造攻撃が有効である．中間平文偽造攻撃は正規の中間平文と同様の働きをすることができる擬似中間平文を用いて平文を解読する．擬似中間平文は部分和問題よりも容易な問題である整数部分和問題の解を求めることで導出することができる．本稿では中間平文偽造攻撃に耐性を持つ暗号システムについて考察することで，中間平文偽造攻撃がどのような構造を持つナップザック暗号に対して有効であるのかを示す．中間平文が複数存在する場合でも擬似中間平文が満たすべき条件により擬似中間平文を生成できる確率を低くすることができる可能性がある．また，中間平文偽造攻撃に対して耐性を持つために中間平文を導出するアルゴリズムが満たすべき条件を示す．

2　ナップザック暗号

ナップザック暗号は一般的にナップザック問題の一部である部分和問題を用いる．部分和問題を以下に示す．

定義 2.1.（部分和問題：*Subset Sum Problem, SSP*）．n 個の自然数 $(a_1, \ldots, a_n)$ と，その部分和 C が与えられた際に

$$C = \sum_{i=1}^{n} a_i x_i \tag{1}$$

を満たす解 $\boldsymbol{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n$ を求める．

部分和問題は NP 困難に属する問題であり，$P \neq NP$ 予想が成立する場合，部分和問題の全てを多項式時間で解読するアルゴリズムは存在しない．また，量子コンピュータを用いた効率的な解読アルゴリズムも提案されておらず，部分和問題を利用することで量子コンピュータに耐性を持つ公開鍵暗号を設計できる可能性がある．

ナップザック暗号，特に低密度ナップザック暗号においては一般に数列 $\boldsymbol{a} = (a_1, \ldots, a_n)$ を公開鍵として公開し，メッセージの送信者は平文 $\boldsymbol{x}$ と公開鍵 $\boldsymbol{a}$ の部分和 C を導出し，暗号文とする．攻撃者は公開鍵 $\boldsymbol{a}$ と暗号文 C を得ることができるが，これらの情報から部分和問題の解である平文 $\boldsymbol{x}$ を導出することは困難である．一方，正規の復号者は自身のみが持つ秘密鍵を利用することで解 $\boldsymbol{x}$ を導出できる．公開鍵を生成する際には落とし戸関数を用いて部分和問題の求解可能な数列（秘密鍵）から求解不可能な数列（公開鍵）に変換する手法が一般的である．求解可能な数列としては，超増加数列や

奇数シフト数列が提案されている．また，落とし戸関数としては剰余変換を用いるものや中国の剰余定理を用いるものなどが存在する．前述した MH 暗号では，秘密鍵である超増加数列を剰余変換を用いて変換し，公開鍵としている．

2.1 低密度攻撃

Coster らの低密度攻撃は密度が 0.94 より小さい部分和問題を効率的に解読することができる．ここで，部分和問題の密度は以下の式で定義される．

$$d := \frac{n}{\log_2 \max_i a_i} \tag{2}$$

これはナップザック暗号においては

$$\frac{(\text{平文空間})}{(\text{暗号文空間})} \tag{3}$$

で表される空間比とみなすことができる．

Coster らの低密度攻撃は攻撃者が得ることのできる暗号文 C 及び公開鍵 $\boldsymbol{a}$ を含む以下の格子基底を利用する．

$$\boldsymbol{A} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -\lambda a_1 \\ 0 & 1 & \cdots & 0 & -\lambda a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & 1 & -\lambda a_n \\ -1/2 & \cdots & \cdots & -1/2 & \lambda C \end{pmatrix} \tag{4}$$

ただし，λ はある程度大きな整数であり，効率化のためのパラメータである．この格子に対し SVP(Shortest Vector Problem) オラクルを実行することで，平文 $(x_1, \ldots, x_n)$ を含む基底ベクトル

$$((x_1 - 1/2), (x_2 - 1/2), \ldots, (x_n - 1/2), 0)$$

を得ることができる．つまり，$d < 0.94$ の場合部分和問題の解が SVP の解から容易に計算できる可能性がある．SVP も部分和問題同様 NP 困難に属する問題である．しかし，SVP オラクルの代替として LLL[6] や BKZ[7] のような格子簡約アルゴリズムが存在し，現実的な時間で解を求めることが可能である．

以上のように密度が 0.94 を下回るナップザック暗号は低密度攻撃によって解読されてしまうため，ナップザック暗号を安全に運用するためには密度を 0.94 以上に設定しなければならない．一方，$d > 1$ の場合，平文空間より暗号文空間の方が小さいことを示している．そのため，密度が 1 を超える場合，平文から得られる暗号文が重複してしまい，平文の衝突が発生する可能性がある．よって密度が 1 より大きい高密度ナップザック暗号では，低密度攻撃に耐性を持つために本来の平文から部分和を得ることはせず，平文の衝突を避けるために何らかの前処理が必要となる．実際に提案されている高密度ナップザック暗号は高密度を実現するために様々な構造をとっている．

3 中間平文を用いる高密度ナップザック暗号

低密度ナップザック暗号に対する包括的な攻撃として低密度攻撃が存在するが，高密度ナップザック暗号に対する包括的な攻撃は存在しない．この要因としては暗号の持つ構造の多様性が挙げられる．その中で，高密度ナップザック暗号を構成する際に，中間平文を用いる場合がある．中間平文は，本来の平文を拡大写像することで得られ，中間平文を部分和問題の解とすることで高密度な部分和問題を実現する．中間平文は一つの平文から一意に一つの中間平文が導出できる場合と，一つ平文から複数の中間平文が得られ，それらの全てが正規の中間平文として機能する場合の二種類に分類される．このような中間平文を用いる高密度ナップザック暗号のモデルを以下に示す．四つのアルゴリズム (KeyGen, PreEnc, SSPEnc, Dec) のうち，PreEnc において平文から中間平文を導出し，SSPEnc において中間平文を用いて暗号文を生成している．なお，t はインスタンス数であり，$t \in \mathbb{Z}^+$ とする．

KeyGen(λ) セキュリティパラメータ λ を入力し，秘密鍵群 sk と公開鍵群 pk を出力するアルゴリズム．ただし pk には公開数列群 A$= \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t\}$ $(t \in \mathbb{Z}^+)$，$\boldsymbol{a}_i \in \mathbb{N}^n (1 \leq i \leq t)$ が含まれるとする．

PreEnc(pk,m) 公開鍵群 pk と平文 m を入力し，中間平文群 M を出力するアルゴリズム．ただし m の空間は $\{0,1\}^n$ より小さく，M=$\{\boldsymbol{M}_1,\ldots,\boldsymbol{M}_t\}$，$\boldsymbol{M}_i \in \{0,1\}^n (1 \leq i \leq t)$ とする．

SSPEnc(A,M) 公開数列群 A と中間平文群 M を入力し，暗号文群 C を出力するアルゴリズム．ただし C= $\{C_1,\ldots,C_t\}$，$C_i = \sum_{j=1}^{n}(a_i)_j(M_i)_j (1 \leq i \leq t)$ とする．

Dec(sk,C) 暗号文群 C と秘密鍵群 sk を入力し，平文 m を出力するアルゴリズム．

ここで，平文と公開鍵から中間平文を出力する PreEnc は逆計算が可能であるとする．つまり，$\mathsf{PreEnc}^{-1}(\mathsf{pk},\mathsf{M}) = m$ を満たすアルゴリズム $\mathsf{PreEnc}^{-1}(\mathsf{pk},\mathsf{M})$ が定義できるとする．

4 中間平文偽造攻撃

本章では筆者らが提案した中間平文偽造攻撃について述べる．この攻撃は複数の中間平文が存在する高密度ナップザック暗号に対して有効な攻撃である．このような構造をとるナップザック暗号には MHK 暗号 [8] や MHKⅡ 暗号 [9] が挙げられる．これらの暗号はすでに中間平文偽造攻撃により解読可能であることが示されている [5, 10]．

まず，中間平文偽造攻撃について述べるにあたり，整数部分和問題を示す．

定義 4.1.（整数部分和問題： *Integer Subset Sum Problem, ISSP*）．n 個の自然数 $(a_1,\ldots,a_n)$ と，その部分和 C が与えられた際に

$$C = \sum_{i=1}^{n} a_i x_i \tag{5}$$

を満たす解 $\boldsymbol{x} = (x_1,\ldots,x_n) \in \mathbb{Z}^n$ を求める．

整数部分和問題は部分和問題より制約が緩く，動的計画法や格子簡約を用いて多項式時間で求解が可能である．また，整数部分和問題の解は無限に存在する．ここで，整数部分和問題オラクルを以下のように定義する．

定義 4.2.（整数部分和問題オラクル）．部分和問題または整数部分和問題のインスタンスが与えられたとき，$\boldsymbol{x} = (x_1,\ldots,x_n) \in \mathbb{Z}^n \backslash \{0,1\}^n$ を満たす解を一つ出力する．また，解に対して利用者の知る情報より得られる条件を自由に追加できる．

これは 3 章で述べたモデル上において以下のアルゴリズムとして定義できる．

ISSPOracle($\boldsymbol{a}, C, \mu$) ある公開数列 $\boldsymbol{a} \in \mathbb{N}^n$ と暗号文 $C \in \mathbb{Z}$，及び条件 μ を入力し，条件 μ を満たす擬似中間平文 $\boldsymbol{M'} \in \mathbb{Z}^n \backslash \{0,1\}^n$ を出力するアルゴリズム．

ここで，擬似中間平文とは正規の中間平文空間 $\{0,1\}^n$ ではなく，整数空間 $\mathbb{Z}^n \backslash \{0,1\}^n$ に属するが，中間平文と同様の役割を持つことができる数列とする．この整数部分和問題オラクルは従来の部分和問題の解の空間 $\{0,1\}^n$ に属する解は出力できない．また，整数部分和問題オラクルは一度の実行につき一つの解のみしか出力できないとする．

中間平文偽造攻撃はナップザック暗号の安全性の根拠となっている部分和問題の解ではなく，部分和問題よりも求解が容易な整数部分和問題の解である擬似中間平文を用いて暗号を解読する．ここで，攻撃に用いるアルゴリズム FakeDec を以下のように定義する．

FakeDec(pk,M') 公開鍵群 sk と擬似中間平文群 $\mathsf{M'} = \{\boldsymbol{M}'_1,\ldots,\boldsymbol{M}'_t\}$ を入力し，平文 m を推定する確率的アルゴリズム．

以上より，中間平文偽造攻撃は以下のように定義できる．

定義 4.3.（中間平文偽造攻撃：*Faked Intermediary Plaintext Attack*）．公開鍵群 pk 及び暗号文群 C から導出できる条件 μ を用いて整数部分和問題オラクル ISSPOracle($\boldsymbol{a}, C, \mu$) を t 回実行，擬似中間平文群 M'= $\{M'_1,\ldots,M'_t\}$ を得る．各暗号に対応した FakeDec(pk,M') を設計し，平文 m を推定する．復号成功確率 $Pr[\mathsf{FakeDec}(\mathsf{pk},\mathsf{M'}) = m]$ が無視できないとき，攻撃が成功するという．

つまり，正規復号者がDec(sk,C)を用いて平文mを出力するところを，中間平文偽造攻撃ではISSPOracle($\boldsymbol{a}, C, \mu$)を用いて疑似中間平文を出力しFakeDec(pk,M')によりmを出力する．ここで，FakeDec(pk,M')は独立したアルゴリズムであるが，最も危険な場合は正規の逆計算アルゴリズムが擬似中間平文の入力を許容する，つまり

$$\mathsf{FakeDec}(\mathsf{pk}, \mathsf{M}') = \mathsf{PreEnc}^{-1}(\mathsf{pk}, \mathsf{M}') \quad (6)$$

が有り得る．

中間平文偽造攻撃はナップザック暗号の安全性の根拠となっている部分和問題を解かずに平文を解読することができる．また，条件μより様々な方法で整数部分和問題オラクルの代替アルゴリズムを設計できる自由度の高い攻撃となっている．

5 中間平文偽造攻撃が有効な高密度ナップザック暗号

本章では高密度ナップザック暗号において中間平文偽造攻撃が有効な暗号システムについて述べる．まず，中間平文偽造攻撃は複数の中間平文が存在する高密度ナップザック暗号に対して有効である．その上で，どのような構成を持つ場合中間平文偽造攻撃が有効であるのかを，中間平文偽造攻撃に耐性を持つ暗号システムについて考察することで明らかにする．

5.1 擬似中間平文の導出に関する考察

中間平文偽造攻撃は公開鍵と暗号文から中間平文を導出する際に本来の部分和問題を解くのではなく，整数部分和問題として解読する．その際に，中間平文空間よりも大きい整数空間$\mathbb{Z}^n\backslash\{0,1\}^n$に属する擬似中間平文を利用する．よって，擬似中間平文が導出できなければ中間平文偽造攻撃は行えない．本節では擬似中間平文を導出する過程においての中間平文偽造攻撃に耐性を持つ条件について述べる．まず，部分和問題と整数部分和問題の関係について以下の定理が成り立つ．

定理 5.1. 数列$\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$と$\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$から得られる部分和$C$が与えられたとき，

$$C = \sum_{i=1}^{n} a_i y_i \quad (7)$$

を満たす解$\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{Z}^n\backslash\{0,1\}^n$が必ず存在する．

証明． 数列$\boldsymbol{a}$と部分和C及び未知数$(z_1, z_2, \ldots, z_n)$を用いた以下のn元一次不定方程式について考える．

$$C = a_1 z_1 + a_2 z_2 + \cdots + a_n z_n \quad (8)$$

式(8)が整数解（一般解，無限個の整数解）を持つための必要十分条件は$d = \gcd(a_1, a_2, \ldots, a_n)$とすると，

$$d \mid C \quad (9)$$

である．ここで，式(8)の不定方程式は少なくとも$(z_1, z_2, \ldots, z_n) = (x_1, x_2, \ldots, x_n)$を解として持つため，式(9)の示す条件を満たす．よって，式(8)は一般解を持つため，$\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{Z}^n\backslash\{0,1\}^n$なる解が必ず存在する．したがって定理は満たされる． □

以上の定理より，公開鍵pk，暗号文C，それらから導出可能な条件μを整数部分和問題オラクルに入力した場合擬似中間平文$\boldsymbol{M}' \in \mathbb{Z}^n\backslash\{0,1\}^n$を必ず導出することが可能である．

しかし，実際に中間平文偽造攻撃を行う際には整数部分和問題オラクルの代替となるアルゴリズムを設計しなければならない．そのようなアルゴリズムには動的計画法や格子簡約が挙げられる．また，各暗号システムに対応したアルゴリズムを設計し使用することも可能である．しかし，これらはオラクルの代替アルゴリズムのため，擬似中間平文を導出できる確率を低くすることが可能であると考えられる．ここで，擬似中間平文が満たすべき条件μについて考える．この条件μは公開情報より導出されるものである．例えば，MHK暗号の場合擬似中間平文$\boldsymbol{M}'$が満たすべき条件μは公開されている情報より，

$$0 \leq \sum_{i=1}^{n} M'_i \leq n \quad (10)$$

と導出でき，格子簡約を用いて現実的な計算時間でこの条件を満たす擬似中間平文を導出することができる．一方で，擬似中間平文を導出できる確率を低くすることを考えたとき，条件 μ を導出する過程において秘密鍵の情報を必要とさせるなどして条件 μ そのものを導出させにくくすることが可能であると考えられる．また，導出された場合も条件 μ による制約を厳しくすることで，現実的な計算時間で擬似中間平文を導出すること不可能にすることができると考えられる．以上より，条件 μ が容易に導出でき，μ の制約が厳しくなければ，中間平文偽造攻撃に必要な擬似中間平文を導出できる可能性が高い．その場合，中間平文偽造攻撃が有効である可能性がある．

5.2 擬似中間平文導出後に関する考察

擬似中間平文導出後は各暗号システムに対応する復号アルゴリズム FakeDec を設計し，公開鍵群と導出した擬似中間平文群を入力して平文を得る．ここで，4 章で述べたように最も危険な場合，式 (6) を満たす可能性がある．本節では式 (6) が成立する，つまり擬似中間平文から平文が一意に決定され，中間平文偽造攻撃が有効となる条件を示す．なお，本節では擬似中間平文を導出することは可能であるとする．

平文及び公開鍵から中間平文を導出するアルゴリズム PreEnc(pk,m) において，平文 m を中間平文 $\boldsymbol{M}$ に変換する関数を $pe(m)$ とする．ただし，任意の平文空間を $\mathbb{V}$（$\mathbb{V}$ は $\{0,1\}^n$ より小さい空間）とし，

$$pe : \mathbb{V} \to \{0,1\}^n$$

であり，$pe(m)$ は $m \in \mathbb{V}$ を入力した際，解となる全ての数列 $\boldsymbol{M} \in \{0,1\}^n$ を出力するとする．つまり，平文から中間平文を生成する場合，

$$pe(m) = \boldsymbol{M} \tag{11}$$

より解を導出し，複数の解が導出された場合はそれらから正規の中間平文となる数列を選択するとする．また逆関数

$$pe^{-1}(\boldsymbol{M}) = m \tag{12}$$

が存在するとする．

まず，$pe(m)$ の条件にについて述べる．$pe(m)$ が一価関数，つまり一つの平文から一つの中間平文が一意に決定される場合，中間平文が複数存在する暗号システムになり得ない．よって，中間平文偽造攻撃が有効な暗号システムにおいては $pe(m)$ は多価関数である．そして出力された複数の解から一つを選択し，中間平文として用いる．なお，ここでいう一価関数とは一つの入力に対して解を一つの出力する関数であり，多価関数とは一つの入力に対して，複数の解を出力する関数である．

次に，逆関数 $pe^{-1}(\boldsymbol{M})$ について考える．本来，$pe^{-1}(\boldsymbol{M})$ は

$$pe^{-1} : \{0,1\}^n \to \mathbb{V}$$

であるが，$\{0,1\}^n \subset \mathbb{Z}^n$ より，擬似中間平文 $\boldsymbol{M'} \in \mathbb{Z}^n \backslash \{0,1\}^n$ の入力を許容するとする．まず，$pe^{-1}(\boldsymbol{M})$ が一価関数の場合，中間平文から一意に平文が導出できる．よって $pe^{-1}(\boldsymbol{M'})$ の解も一意に決定される．しかし，中間平文偽造攻撃では $pe^{-1}(\boldsymbol{M})$ に本来の中間平文より空間の大きい疑似中間平文 $\boldsymbol{M'} \in \mathbb{Z}^n \backslash \{0,1\}^n$ を入力するため，疑似中間平文を入力した際の写像先が平文空間とならない場合が考えられる．ここで，平文空間を含む任意の空間を $\mathbb{W}$（$\mathbb{V} \subset \mathbb{W}$）とする．$pe^{-1}(\boldsymbol{M})$ に疑似中間平文 $\boldsymbol{M'} \in \mathbb{Z}^n \backslash \{0,1\}^n$ を入力したとき，$pe^{-1}(\boldsymbol{M'})$ の解が平文空間 $\mathbb{V}$ に属するならば疑似中間平文から一意に平文を導出可能であり，式 (6) が成立する（図 1 の ${pe_1}^{-1}(\boldsymbol{M'})$）．よって，中間平文偽造攻撃が有効である．一方，$pe^{-1}(\boldsymbol{M'})$ の解が $\mathbb{W} \backslash \mathbb{V}$ に属する場合，疑似中間平文から平文を導出できない（図 1 の ${pe_2}^{-1}(\boldsymbol{M'})$）．つまり，中間平文偽造攻撃に対して安全な暗号と言える．よって，$pe^{-1}(\boldsymbol{M})$ が一価関数の場合，$pe^{-1}(\boldsymbol{M'})$ の解が平文空間 $\mathbb{V}$ に属さない場合は，中間平文偽造攻撃に対して安全である．

次に，$pe^{-1}(\boldsymbol{M})$ が多価関数の場合について考える．なお，正規の復号は $pe^{-1}(\boldsymbol{M})$ ではなく，Dec(sk,C) を用いるため，$pe^{-1}(\boldsymbol{M})$ は多価関数が有り得る．$pe^{-1}(\boldsymbol{M})$ が多価関数の場合，中間平文を入力したとき，平文が一意に決定されず，複数の解が存在する．よって，式 (6) の

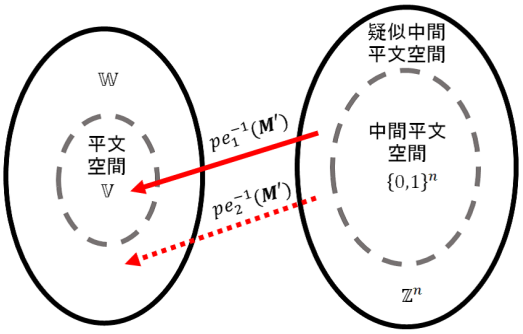

図 1: $pe^{-1}(\boldsymbol{M})$ が一価関数の場合

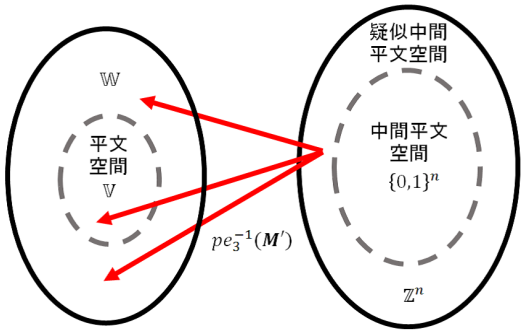

図 2: $pe^{-1}(\boldsymbol{M})$ が多価関数の場合

成立する可能性が低くなり，中間平文偽造攻撃に対して安全であると考えられるが，例外が存在する．擬似中間平文 $\boldsymbol{M'} \in \mathbb{Z}^n \backslash \{0,1\}^n$ を入力した際にただ一つの解のみが平文空間 $\mathbb{V}$ の空間内に存在し，他の解は全て $\mathbb{W} \backslash \mathbb{V}$ に存在する場合は式 (6) が成立する可能性がある（図 2 の $pe_3{}^{-1}(\boldsymbol{M'})$）．よって $pe^{-1}(\boldsymbol{M})$ が多価関数の場合は複数解のうち，ただ一つのみが平文空間内に写像されるような入力 $\boldsymbol{M'}$ のインスタンスが存在しない場合，中間平文偽造攻撃に対し耐性を持つことができる．

以上より，$pe(m)$ が多価関数である中間平文が複数存在する暗号システムが式 (6) を満たさず，中間平文偽造攻撃に対して耐性を持つために $pe^{-1}(\boldsymbol{M})$ が満たすべき条件は以下の通りになる．

- $pe^{-1}(\boldsymbol{M})$ が一価関数の場合，$pe^{-1}(\boldsymbol{M'})$ の解が平文空間外に属する．
- $pe^{-1}(\boldsymbol{M})$ が多価関数の場合，$pe^{-1}(\boldsymbol{M'})$ の複数解のうちただ一つの解のみが平文空間内に属する $\boldsymbol{M'}$ のインスタンスが存在しない．

つまり，複数の中間平文が存在する高密度ナップザック暗号において，以上の条件を満たさない場合は式 (6) が成立し，中間平文偽造攻撃が有効である．

6 結論

本稿では高密度ナップザック暗号に対する攻撃である中間平文偽造攻撃が有効な暗号システムを示すにあたり，攻撃に耐性を持つ暗号システムの条件について述べた．

まず，中間平文偽造攻撃は高密度ナップザック暗号の中でも，複数の中間平文が存在するものに対して有効である．その上で中間平文偽造攻撃に耐性を持つためには，まず擬似中間平文を生成できる確率を低くするために擬似中間平文の満たすべき条件 μ について考慮するべきである．また，擬似中間平文が導出された場合でも，平文から中間平文を導出するアルゴリズムがある条件を満たせば中間平文偽造攻撃に耐性を持つことができる．本稿では，このアルゴリズムが満たすべき条件を示した．高密度ナップザック暗号は中間平文偽造攻撃に対して耐性を持つように設計されなければならない．

謝辞

本研究の一部は，科研費（基盤研究（C）課題番号 26330155）の助成を受けたものである．

参考文献

[1] R. Merkle and M. Hellman. Hiding Information and Signatures in Trapdoor Knapsacks. *Information Theory, IEEE Transactions on*, Vol. 24, No. 5, pp. 525–530, 1978.

[2] A. Shamir. A POLYNOMIAL TIME ALGORITHM FOR BREAKING THE BASIC MERKLE-HELLMAN CRYPTOSYSTEM. *Information Theory, IEEE Transactions on*, Vol. 30, No. 5, pp. 699–704, 1984.

[3] J. C. Lagarias and A. M. Odlyzko. Solving Low-Density Subset Sum Problems. *J. ACM*, Vol. 32, pp. 229–246, January 1985.

[4] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, and J. Stern. IMPROVED LOW-DENSITY SUBSET SUM ALGORITHMS. *computational complexity*, Vol. 2, No. 2, pp. 111–128, 1992.

[5] Y.Kusanagi, A.Nagao, and M.Morii. Attack on Knapsack Cryptography by Using Intermediary Plaintext. *IEICE Technical Report, ISCC*, Vol. 114, pp. 9–14, 2014.

[6] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, Vol. 261, No. 4, pp. 515–534, 1982.

[7] C.P. Schnorr and M. Euchner. Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. *Mathematical programming*, 1994.

[8] 村上恭通, 濱正真佑, 笠原正雄. 秘密鍵に乱数を用いるナップザック暗号. 2012 年暗号と情報セキュリティシンポジウム (SCIS2012), 2012.

[9] 村上恭通, 濱正真佑, 笠原正雄. 秘密鍵に二系列の乱数を用いるナップザック暗号. 2014 年暗号と情報セキュリティシンポジウム (SCIS2014), 2014.

[10] 長尾篤, 森井昌克. ナップザック暗号における高密度化手法に関する考察. コンピュータセキュリティシンポジウム 2013(CSS2013), 2013.