情報量的に安全な鍵事前配布方式の一般化に関する研究

A study of the generalization of unconditionally secure key predistribution systems

2010年7月

吉田　隆弘

情報量的に安全な鍵事前配布方式の一般化に関する研究

A study of the generalization of unconditionally secure key predistribution systems

2010年7月

早稲田大学大学院 基幹理工学研究科

吉田　隆弘

目 次

第1章　序論

1.1　研究背景

1.1.1　情報量的安全性を有する暗号方式

近年，インターネット環境等で様々な情報通信サービスを享受できるようになってきたが，その一方で，通信内容の盗聴，個人情報の漏洩，プライバシーの侵害，不正アクセス，サイバーテロ等の犯罪の増加といったセキュリティに関する様々な問題が発生している．このようなセキュリティに関する問題の対策として，暗号を用いた秘匿通信，認証，電子署名，秘密分散法，鍵配布方式等の暗号方式が広く利用されている．

これらの暗号方式では，悪意の第三者による攻撃に対して，ある種の安全性が要求される．一般の暗号方式に対する安全性を定義するためには，暗号方式への攻撃に対していくつかの仮定をおく必要がある．これらの仮定の1つに，攻撃者の攻撃能力に関する仮定がある．この仮定は，攻撃者が目標を達成するために実行できる計算時間や計算資源等に関する仮定である．攻撃能力に対して何も仮定せずに保証できる安全性を，情報量的安全性という．情報量的安全性では，攻撃能力に何も仮定をおかないので，無限の計算能力を持つ攻撃者に対しても安全性が保証される．一方，攻撃能力に対し，現実的に実行可能な計算時間等の仮定をおいたときに保証される安全性を，計算量的安全性という．計算量的安全性では，攻撃能力に制限を設けているので，この安全性が保証されていても，計算機能力の急速な進展等によって，将来的に攻撃者の目標が達成される可能性がある．よって，計算量的安全性を満たす暗号方式では，長期的な安全性が保証できないという欠点があるため，攻撃に対するその他の仮定が全て同じであれば，情報量的安全性は計算量的安全性よりも高い安全性を持つことになり，長期的な安全性が保証できる極めて高度な安全性

となる．

情報量的安全性が保証された暗号方式は，情報量的に安全な暗号方式，または情報量的安全性を有する暗号方式という．一般に，情報量的安全性を有する暗号方式に関する研究では．まず，対象とする暗号方式の定義，暗号方式の機能性，安全性，効率性に対する評価基準の定義，暗号方式に要求する機能性と安全性に対する制約条件の定義を行う．情報量的安全性を有する暗号方式に関する研究では，制約条件を満たすもとで，効率性を最大化することを重要な目標としている．従来研究では，この目標を達成するために，定義した制約条件を満たすもとでの効率性の理論的限界を導出し，その理論的限界を達成する暗号方式の具体的な構成法を示している．情報量的安全性を有する暗号方式に関する研究では，このようなアプローチが重要な課題として取り組まれている．

秘密分散法や鍵配布方式 (詳細は後述) に代表される複数の利用者が参加する暗号方式では，複数の利用者が結託して別の利用者へ不正を行うといった攻撃を仮定することが多い．このような仮定のもとでの安全性に対する制約条件には，次のような 2 つの制約条件がある．1 つ目は，しきい値型安全性に対する制約条件である．しきい値型安全性とは，攻撃者数 (結託数) があるしきい値以下であるとき，攻撃対象の情報が全く得られないという性質である [3, 4, 14, 18, 19, 26]．2 つ目は，しきい値ランプ型安全性に対する制約条件である．しきい値ランプ型安全性とは，結託数があるしきい値以下であるとき，攻撃者は攻撃対象に関する情報が全く得られず，しきい値を超えると結託数の増加に従ってその情報が段階的に得られていくという性質である [2, 5, 33]．しきい値ランプ型安全性は，しきい値型安全性を拡張した性質となり，この性質を有する暗号方式は，しきい値型安全性を有する暗号方式と比較すると，安全性は弱くなるが効率性の向上や，利用者が保有するメモリ等のリソースに制限が設けられている場合にリソースの有効な活用が可能となる．

1.1.2　情報量的安全性を有する鍵配布方式

インターネット環境等の大規模なコンピュータネットワークにおいて，不特定多数のユーザと呼ばれる利用者からなるグループで暗号を用いた秘匿通信を行う場合，通信前にグループ内で鍵と呼ばれる情報を共有する必要が生じる．このような場合

に必要となる技術が鍵配布方式である．

鍵配布方式には，センターと呼ばれる利用者を用いる方式と，そのような利用者を用いない方式がある．センターを用いる鍵配布方式には，センターとユーザ間で共通鍵暗号方式を用いる方式 [17]，センターのデジタル署名及び公開鍵暗号方式を用いる方式 [24]，利用者の ID 情報 (識別子) を用いる方式 [1, 3, 4, 5, 9, 18, 19, 22, 23, 30] などがある．また，センターを用いない鍵配布方式には，Diffie-Hellman 鍵配布方式 [10]，RSA 暗号 [25] などの公開鍵暗号を利用した方式，雑音のある通信路を用いる方式，量子通信路を用いる方式 [6, 7, 11, 32] などがある．高度な安全性である情報量的安全性を有する鍵配布方式には，センターを用いる鍵配布方式と量子通信路を用いる鍵配布方式が提案されている．しかし，量子通信路を用いる鍵配布方式は，実装上の面で問題が残されているので，本研究では，高度な安全性を有し，実装に対する技術的な問題が少ない方式となるセンターを用いる鍵配布方式を研究対象とする．

センターを用いる鍵配布方式の各利用者は，個体識別のための情報である ID 情報を持つ n_D 個のセンターと n_P 人のユーザで構成されており，鍵逐次配布方式と鍵事前配布方式の 2 つの方式が存在する．ここでセンターは，ユーザに鍵を配布するための機関として設置されている．鍵逐次配布方式は，複数のユーザで構成される任意のグループが秘匿通信を行う際に，センターへ鍵のリクエストを送り，そのグループの鍵をセンターから受け取る方式である [5, 9, 22]．一方，鍵事前配布方式は，各ユーザが自身の属している全てのグループの鍵を，事前にセンターから受け取る方式である [3, 4, 18, 19]．この方式では，最初にセンターが n_P 人の全ユーザへ，そのユーザが属している全てのグループに対する鍵の情報を安全な通信路を用いて送信する．各ユーザは送られてきた情報を記憶しておき，鍵を使用する際に，記憶している情報と公開情報であるユーザの ID 情報から，自身が属しているグループの鍵を他のユーザやセンターとの通信を行わずに個別に生成することができる．鍵事前配布方式は，センターとユーザとの通信が 1 回のみであることから，ユーザの利便性の面から考えると鍵逐次配布方式より優れている．本研究では，利用者の利便性に優れた鍵事前配布方式を研究対象とする．

センターを用いる鍵配布方式の機能性，安全性，効率性を測るための評価基準としては，一般に次のような評価基準が用いられている．機能性に対する評価基準は

整合度と呼ばれ，鍵配布方式の目的であるグループ内での鍵の共有が，正しくできているかどうかを測る基準となる．安全性に対する評価基準は安全度と呼ばれ，複数の利用者が結託して別の利用者へ不正を行うといった攻撃の仮定に基づいて定義されている．すなわち，攻撃対象の鍵を共有するグループに属していない複数のユーザ，及びセンターが利用可能な情報から得られる攻撃対象の鍵の情報量を測る基準となる．また，効率性に対する評価基準は記憶容量が用いられる．これは，各センター及び各ユーザに対する固有の情報を記憶するために必要なメモリ量を測る基準となる．

鍵配布方式では，複数の利用者による攻撃を仮定するので，安全性に対する制約条件には，1.1.1 節で述べたしきい値型安全性を保証する制約条件としきい値ランプ型安全性を保証する制約条件の 2 つの条件が考えられる．鍵配布方式におけるしきい値型安全性とは，2 つのしきい値 m_P と m_D に対して，任意の m_P 人以下のユーザと任意の m_D 個以下のセンターが結託しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られないという性質である．一方，しきい値ランプ型安全性とは，任意の m_P 人以下のユーザと任意の m_D 個以下のセンターが結託しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られず，しきい値を超えると結託数の増加に従ってその情報が段階的に得られるという性質である．しかし，しきい値型安全性からしきい値ランプ型安全性への安全性の拡張は，鍵逐次配布方式に対してのみ行われており [5]，鍵事前配布方式に対しては，まだ拡張がなされていない．

1.1.3　鍵事前配布方式の概要と従来方式の問題点

従来の鍵事前配布方式は，任意の t 人のユーザからなるグループの鍵が共有できる方式で，次のようなプロトコルとして定義される．

1. 各センターは独立に，秘密の情報を生成する．
2. 各センターは他の全てのセンターと盗聴や改ざんが不可能な安全な通信路上で通信を行う．

3. 各センターは，2. で得た情報から各センター固有の情報を生成し，安全な記憶領域であるメモリに記憶する．

4. 各ユーザは，一部のセンターとそれぞれ盗聴や改ざんが不可能な安全な通信路上で通信を行う．

5. 各ユーザは，4. で得た情報から各ユーザ固有の情報を生成し，メモリに記憶する．

上記のプロトコルを正しく行うことで，任意の t 人のグループの鍵が，グループ内の各ユーザの固有の情報と公開情報であるユーザとセンターの ID 情報から個別に生成可能となる．しかし，このような鍵事前配布方式では，全てのセンターが秘密の情報を生成し，他の全てのセンターと通信を行っているため，センター間の通信は合計で $n_D\,(n_D-1)$ 回の通信を行うことになり，センターの総数 n_D が大きい場合はセンター間の総通信量が膨大になる．また，センター間の通信で用いる安全な通信路は，インターネット回線のような公開通信路とは異なる特別な通信路となるため，利用するためには非常に大きなコストがかかってしまう．したがって，センター間の通信量の増大は，非常に重大な問題となる．

1.2　研究の目的と位置づけ

本研究では，高度な安全性である情報量的安全性を有する鍵配布方式の中でも，利用者の利便性に優れ，かつ実装に対する技術的な問題が少ない鍵事前配布方式の安全性に対して，安全性の拡張とセンター間の通信量の削減を行う．また，本研究においても，1.1.1 節で述べたような情報量的安全性を有する暗号方式に関する研究と同様のアプローチで研究を行う．

具体的には，まず従来の鍵事前配布方式に対して，センターの通信量を削減した鍵事前配布方式を定義する．この新たな方式に対して，従来と同様に鍵事前配布方式の機能性，安全性，効率性の評価基準である整合度，安全度，記憶容量を定め，鍵事前配布方式に要求する制約条件の定義を行う．要求する制約条件の 1 つである安全性に対する制約条件について，従来用いられていたしきい値型安全性からしきい

値ランプ型安全性へ安全性の拡張を行い，しきい値ランプ型安全性に対する制約条件の定義を行う．このとき，しきい値ランプ型への安全性の拡張として，結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られるという性質，結託センター数の増加に従って情報が段階的に得られるという性質，結託センター及び結託ユーザの結託数の増加に従って情報が段階的に得られるという 3 つの性質が考えられる．本研究では，これら 3 つ性質に対する制約条件をそれぞれ定義する．次に，それぞれの制約条件を満たすもとで，記憶容量の理論的限界を導出し，理論的限界を達成する鍵事前配布方式の構成法を示す．更に，本研究で新たに導入したしきい値ランプ型安全性は，従来の用いられていたしきい値型安全性を特別な場合に含む一般的な安全性となることを示す．

第2章　準備

2.1　情報理論における基本事項

本節では，情報理論で用いられるエントロピーと相互情報量の定義，及び本研究で用いるエントロピーと相互情報量の基本的な性質 [8] について述べる．

可算集合 $\mathcal{X}$ に値をとる確率変数を X とおき，確率変数 X の確率関数を

$$p_X(x) = \Pr\{X = x\},\ x \in \mathcal{X}, \tag{2.1}$$

とする．以下，本論文では任意の確率変数に対する確率関数を上記のように表す．また，任意の 2 つの整数 m, n に対して，長さ $n-m+1$ の任意の系列 $Z_m, Z_{m+1}, \cdots, Z_n$ を Z_m^n とおく場合がある．ただし，$n < m$ のときは空系列とする．

2.1.1　エントロピーの定義

確率変数 X のエントロピー $H(X)$ は，

$$H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x) \tag{2.2}$$

として定義される．また，可算集合 $\mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_N$ に値をとり，同時確率関数

$$\begin{aligned} p_{X_1^N}(x_1^N) &= \Pr\{X_1 = x_1, X_2 = x_2, \cdots, X_N = x_N\}, \\ &\qquad (x_1, x_2, \cdots, x_N) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_N \end{aligned} \tag{2.3}$$

を持つ N 個 $(N \geq 2)$ の確率変数の組 $(X_1, X_2, \cdots, X_N)$ に対するエントロピー

$$\begin{aligned} &H(X_1, X_2, \cdots, X_N) \\ &\quad = -\sum_{x_1 \in \mathcal{X}_1} \cdots \sum_{x_N \in \mathcal{X}_N} p_{X_1 \cdots X_N}(x_1, \cdots, x_N) \log p_{X_1 \cdots X_N}(x_1, \cdots, x_N) \end{aligned} \tag{2.4}$$

を同時エントロピーと呼ぶ.

可算集合 $\mathcal{X} \times \mathcal{Y}$ に値をとり，同時確率関数 $p_{XY}(x, y)$ を持つ 2 つの確率変数 X, Y に対し，X が与えられたときの Y の条件付きエントロピー $H(Y \mid X)$ は,

$$\begin{aligned} H(Y \mid X) &= \sum_{x \in \mathcal{X}} p_X(x) H(Y \mid X = x) \\ &= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p_{XY}(x, y) \log p_{Y|X}(y \mid x) \end{aligned} \tag{2.5}$$

として定義される．ここで，$p_{Y|X}(y \mid x)$ は条件 $X = x$ のもとでの $Y = y$ の条件付き確率関数で，次のように定義される.

$$p_{Y|X}(y \mid x) = \frac{p_{XY}(x, y)}{p_X(x)}. \tag{2.6}$$

以下，本論文では任意の確率変数に対する条件付き確率関数を上記のように表す.

2.1.2　エントロピーの基本的性質

エントロピーは，次のような性質を持つ.

1. エントロピーは常に非負値をとる．すなわち,

   定理 2.1 ([8], Lemma 2.1.1)

   任意の確率変数 X に対して,

   $$H(X) \geq 0 \tag{2.7}$$

   が成り立つ. □

   このような非負性は，同時エントロピーと条件付きエントロピーについても同様に成り立つ.

2. 複数の確率変数に対して，次のようなチェイン則が成り立つ.

定理 2.2 ([8], Theorem 2.5.1)

任意の N 個の確率変数 $X_1, X_2, \cdots, X_N$ に対して，

$$H\left(X_1^N\right) = \sum_{i=1}^{N} H\left(X_i \mid X_1^{i-1}\right) \tag{2.8}$$

が成り立つ．　□

2.1.3　相互情報量の定義

2 つの確率変数 X, Y に対して，X と Y の相互情報量 $I(X;Y)$ は，

$$\begin{aligned} I(X;Y) &= H(X) - H(X \mid Y) \\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y) \log \frac{p_{XY}(x,y)}{p_X(x)p_Y(y)} \end{aligned} \tag{2.9}$$

として定義される．また，3 つの確率変数 X_1, X_2, X_3 に対して，X_3 が与えられたときの X_1 と X_2 の条件付き相互情報量 $I(X_1; X_2 \mid X_3)$ は，

$$I(X_1; X_2 \mid X_3) = H(X_1 \mid X_3) - H(X_1 \mid X_2, X_3) \tag{2.10}$$

として定義される．

2.1.4　相互情報量の基本的性質

相互情報量の基本的性質を述べるために，まず，(単純）マルコフ連鎖を定義する．確率変数の列 $X_1, X_2, \cdots, X_N$ がマルコフ連鎖をなすとは，任意の $2 \le i \le N-1$ に対して，X_i が与えられたもとで X_1^{i-1} と X_{i+1}^N が条件付き独立であることをいう．本研究では，確率変数の列 X_1^N がマルコフ連鎖をなすとき，

$$X_1 \to X_2 \to \cdots \to X_N \tag{2.11}$$

と表すことにする．マルコフ連鎖の定義より，ただちに以下の結果が導かれる [8]．

- 任意の N 個の確率変数 $X_1, X_2, \cdots, X_N$ に対して，

$$X_1 \to X_2 \to \cdots \to X_N \tag{2.12}$$

であれば，

$$X_N \to X_{N-1} \to \cdots \to X_1 \tag{2.13}$$

も成り立つ．

- 任意の N 個の確率変数 $X_1, X_2, \cdots, X_N$，及び任意の関数 $\varphi_i, 2 \leq i \leq N-1$ に対して，$\varphi_i(X_i) = X_{i+1}$ であれば，

$$X_1 \to X_2 \to \cdots \to X_N \tag{2.14}$$

が成り立つ．

次に，相互情報量の基本的性質について述べる．

1. 相互情報量は対称性を持つ．すなわち，

   定理 2.3 ([8], Theorem 2.4.1)

   任意の確率変数 X_1, X_2, X_3 に対して，

$$I(X_1; X_2) = I(X_2; X_1), \tag{2.15}$$

$$I(X_1; X_2 \mid X_3) = I(X_2; X_1 \mid X_3) \tag{2.16}$$

   が成り立つ． □

2. エントロピーと同様に，相互情報量，及び条件付き相互情報量は常に非負値をとる．すなわち，

   定理 2.4 ([8], Theorem 2.6.3)

   任意の確率変数 X_1, X_2, X_3 に対して，

$$I(X_1; X_2) \geq 0,$$

$$I(X_1; X_2 \mid X_3) \geq 0 \tag{2.17}$$

   が成り立つ． □

3. 相互情報量の非負性から，以下の関係が成り立つ．

   定理 2.5 ([8], Theorem 2.6.5)

   任意の確率変数 X, Y に対して，

   $$H(X \mid Y) \leq H(X) \tag{2.18}$$

   が成り立つ．等号は X と Y が互いに独立であるとき，かつそのときに限られる．□

   この定理は，条件付きエントロピーに条件を加えることで，その量が減少することはあっても増加することはないことを示している．

4. 複数の確率変数に対して，エントロピーと同様に，次のようなチェイン則が成り立つ．

   定理 2.6 ([8], Theorem 2.5.1)

   任意の $N+1$ 個の確率変数 $X_1, X_2, \cdots, X_N, Y$ に対して，

   $$I\left(X_1^N; Y\right) = \sum_{i=1}^{N} I\left(X_i; Y \mid X_1^{i-1}\right). \tag{2.19}$$

   が成り立つ．□

5. マルコフ連鎖をなす確率変数列に対して，次のような不等式が成り立つ．

   定理 2.7 ([8], Problem 2.15)

   任意の N 個の確率変数 $X_1, X_2, \cdots, X_N$ に対して，

   $$X_1 \to X_2 \to \cdots \to X_N \tag{2.20}$$

   のとき，

   $$I\left(X_1; X_2^N\right) = I\left(X_1; X_2\right) \tag{2.21}$$

   が成り立つ．□

2.2　暗号方式の安全性

2.2.1　暗号方式への攻撃の仮定

暗号方式の安全性を保証するためには，暗号方式への攻撃に対して以下の 5 つの条件を仮定する必要がある．

前提条件： 暗号方式の安全性を保証するための仮定．この仮定が弱いほど攻撃者にとって有利な状況となる．

攻撃者： 暗号方式を攻撃する悪意の第三者．

攻撃対象： 攻撃者が特定したい情報で，確率変数として与えられる．

利用可能情報： 攻撃者が攻撃を行う際に利用可能な情報で，確率変数として与えられる．利用可能な情報が多いほど攻撃者にとって有利な状況となる．

攻撃能力： 攻撃者が目標を達成するために実行できる計算の量に対する仮定．実行可能な計算の量が大きいほど，すなわち仮定が弱いほど攻撃者にとって有利な状況となる．

暗号方式の安全性は，これらの条件の仮定の強さによって分類することができる．暗号方式における情報量的安全性と計算量的安全性という安全性は，攻撃者の攻撃能力に対する仮定によって分類される．以下では，情報量的安全性と計算量的安全性の 2 つの安全性について説明する．

2.2.2　情報量的安全性の概念

情報量的安全性を有する暗号方式は，攻撃者が攻撃に成功するための十分な情報を持っていないという意味で安全な方式となる．情報量的安全性では，攻撃者の計算能力に関して全く制限を設けない．すなわち，攻撃者が無限の計算資源や計算時間を使えることを許容した条件となる．また，情報量的安全性を考える場合，前提条件は仮定しない．

以下では，ある暗号方式 Π_0 の情報量的安全性について考える．Π_0 への攻撃に対して，前述した 5 つの条件をそれぞれ次のように仮定する．

前提条件： 仮定しない．

攻撃者： 任意の攻撃者 A.

攻撃対象： X.

利用可能情報： Y.

攻撃能力： 無限の計算能力を持つ．

本研究では，情報量的安全性を有する暗号方式 Π_0 の安全性を測る評価基準を安全度と呼ぶ．安全度は，利用可能情報 Y と攻撃対象 X の条件付きエントロピー $H(X \mid Y)$ として定義される．このとき，上記 5 つの仮定のもとで暗号方式 Π_0 の安全度が，

$$0 < H(X \mid Y) \leq H(X) \tag{2.22}$$

を満たすとき，暗号方式 Π_0 は情報量的に安全，または情報量的安全性を有するという．また，暗号方式 Π_0 の安全度が，

$$H(X \mid Y) = H(X) \tag{2.23}$$

を満たすとき，利用可能情報と攻撃対象は互いに独立となるので，攻撃者は攻撃対象の情報を全く得ることができない．暗号方式 Π_0 が (2.23) を満たすとき，暗号方式 Π_0 は完全守秘性を有するという．一方，暗号方式 Π_0 の安全度が，

$$0 < H(X \mid Y) \tag{2.24}$$

を満たしている場合は，利用可能情報と攻撃対象に相関があるので，攻撃者は攻撃対象の情報を完全にではないが部分的に得ることができる．すなわち，暗号方式 Π_0 は，安全度 $H(X \mid Y)$ が大きいほどより安全な暗号方式となる．また，任意の $x \in \mathcal{X}$ と任意の $y \in \mathcal{Y}$ に対して，

$$p_{X|Y}(x \mid y) = p_X(x) \tag{2.25}$$

を満たすことと，(2.23) を満たすことが等価であるので，(2.25) を完全守秘性の定義とする場合もある．

ここでは，暗号方式 Π_0 の安全性評価基準について述べているが，暗号方式 Π_0 の機能性や効率性に対する評価基準も方式に応じて与えられる．機能性及び効率性に対する評価基準については，2.3 節で共通鍵暗号方式を例にとって説明する．

2.2.3　計算量的安全性の概念

計算量的安全性を有する暗号方式は，攻撃者が攻撃に成功するための十分な時間や計算資源を持っていないという意味で安全な方式となる．計算量的安全性では，攻撃者の攻撃能力に関しては，攻撃を行う時間に現実的な制限を設けた条件が与えられる．このため計算量的安全性では，任意の自然数 n の多項式関数 γ で攻撃の実行可能時間を表している．このパラメータ n は，一般にセキュリティパラメータと呼ばれており，攻撃者にも既知の値となる．ここで，正の整数全体の集合を $\mathbb{N}^+$，正の値をとる多項式全体の集合を Γ とおき，任意の $n \in \mathbb{N}^+$ と任意の $\gamma \in \Gamma$ に対し，多項式時間 $\gamma(n)$ で実行できる確率的アルゴリズムを確率的多項式時間アルゴリズムと呼ぶ．計算量的安全性では，攻撃者の攻撃能力と任意の確率的多項式時間アルゴリズムが等価であると仮定する．暗号方式の利用者も同様に，任意の確率的多項式時間アルゴリズムと等価であると仮定するが，攻撃者より計算能力が劣っていても良いものとする．また，2.2.2 節で述べたように，情報量的安全性を考える場合には前提条件を仮定しなかったが，計算量的安全性を考える場合には，ある関数の存在性やある数学的問題 (例えば，素因数分解問題や離散対数問題など) の困難性に関する仮定をおく．

ここで，2.2.2 節と同様に，ある暗号方式 Π_0 の計算量的安全性について考える．Π_0 の計算量的安全性を保証するために，2.2.2 節で仮定した 5 つの条件のうち，前提条件，攻撃能力を以下のように変更する．また，与えられる仮定はセキュリティパラメータ n によって異なることに注意しておく．

前提条件： ある性質を持った関数が存在する．

攻撃能力： 任意の確率的多項式時間アルゴリズムと等価．

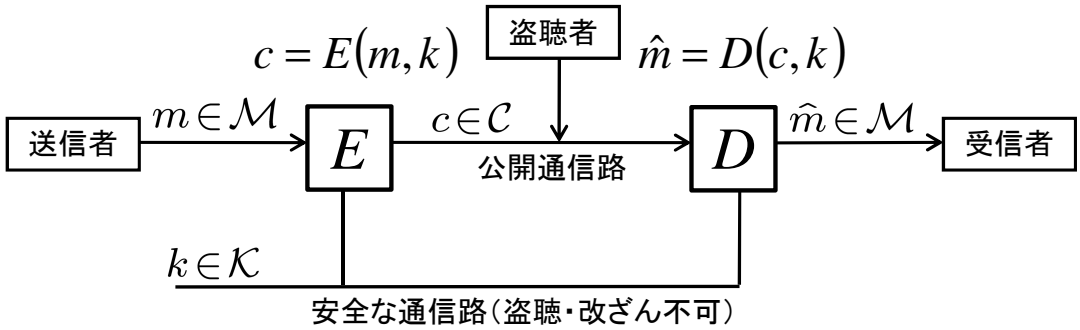

図 2.1: 共通鍵暗号方式

上記仮定のもとで暗号方式 Π_0 は，全ての $\gamma \in \Gamma$ に対し，攻撃に成功する確率が $1/\gamma(n)$ より小さいとき計算量的に安全，または計算量的安全性を有するという．

2.2.2 節，及び 2.2.3 節では，情報量的安全性と計算量的安全性に対する直観的な条件の仮定のみで，厳密な仮定を与えていない．2.3 節では，実際に多くの場面で利用されている共通鍵暗号方式を例にとり，より厳密な安全性の定義を与える．

2.3　共通鍵暗号方式の安全性

2.3.1　共通鍵暗号方式の概要

インターネット等の公開通信路上での通信内容を第三者に知られたくない場合，秘匿通信を行う必要がある．秘匿通信は，暗号を用いることで実現できる．暗号を用いた秘匿通信には，共通鍵暗号方式と公開鍵暗号方式があり，暗号化と復号の計算処理効率の面で共通鍵暗号方式が優れているので，多くの情報を暗号化する必要がある場合は共通鍵暗号方式が用いられる．共通鍵暗号方式は，暗号化と復号に用いる鍵が同一の暗号方式で，暗号化する情報をブロック単位で暗号化するブロック暗号と，情報要素ごとに逐次的に暗号化するストリーム暗号方式がある．

簡略化した共通鍵暗号方式を，図 2.1 に示す．送信者は，受信者に送りたい平文 $m \in \mathcal{M}$ を鍵 $k \in \mathcal{K}$ と符号器 $E : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ を用いて暗号文 $c \in \mathcal{C}$ に暗号化し，公開通信路を用いて暗号文 c を受信者へ送信する．このとき，暗号文 c は盗聴者に

よって盗聴されている可能性がある．暗号文 c を受信した受信者は，鍵 k と復号器 $D : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ を用いて復号文 $\hat{m} \in \mathcal{M}$ を復号する．送信者と受信者で用いる鍵 k は，暗号化する前に盗聴や改ざんが不可能な安全な通信路を用いて伝送される．ここで，平文全体の集合，暗号文全体の集合，及び鍵全体の集合を，それぞれ $\mathcal{M}, \mathcal{C}, \mathcal{K}$ とおいた．また，これらの集合上に値をとる確率変数を，それぞれ M, C, K とする．これらの確率変数に対する確率関数は，共通鍵暗号方式に依存して決まる．

2.3.2　情報量的安全性を有する共通鍵暗号方式

共通鍵暗号方式の定義

一般的な共通鍵暗号方式の定義は，次のように与えられる．

定義 2.1 平文全体の集合 $\mathcal{M}$，暗号文全体の集合 $\mathcal{C}$，鍵全体の集合 $\mathcal{K}$，符号器 E，復号器 D，$\mathcal{M}$ 上の確率関数 $p_M(m)$，$\mathcal{K}$ 上の確率関数 $p_K(k)$ を共通鍵暗号方式 Π に対する公開情報とする．共通鍵暗号方式 Π は，次の 3 つのステップから構成されるプロトコルである．

鍵生成ステップ: 鍵全体の集合 $\mathcal{K}$ 上の確率関数 $P_K(k)$ に従って，鍵 $k \in \mathcal{K}$ を確率的に生成し，安全な通信路を用いて送信者及び受信者に伝送する．

暗号化ステップ: 送信者は送りたい平文 m を，鍵 k と符号器 E を用いて暗号文 $c = E(m, k)$ に暗号化し，公開通信路を用いて受信者へ送信する．

復号ステップ: 暗号文 c を受信した受信者は，鍵 k と復号器 D を用いて復号文 $\hat{m} = D(c, k)$ に復号する．　□

共通鍵暗号方式 Π への攻撃に対する条件

定義 2.1 で定義した共通鍵暗号方式 Π への攻撃に対して，次のような仮定を設ける．

仮定 2.1 共通鍵暗号方式 Π への攻撃は，以下の 5 つの条件を満たす．

前提条件： 仮定しない．

攻撃者： 送受信者ではない任意の攻撃者 A.

攻撃対象： 平文 M の部分情報.

利用可能情報： 暗号文 C.

攻撃能力： 無限の計算能力を持つ. □

共通鍵暗号方式の評価基準

仮定 2.1 を満たす攻撃に対して，共通鍵暗号方式 Π の安全性を測る評価基準となる安全度を

$$H(M \mid C) = -\sum_{c \in \mathcal{C}} p_C(c) \sum_{m \in \mathcal{M}} p_{M|C}(m \mid c) \log p_{M|C}(m \mid c) \tag{2.26}$$

とする．確率関数 $p_C(c)$ と条件付き確率関数 $p_{M|C}(m \mid c)$ は，確率関数 $p_K(k)$，確率関数 $p_M(m)$，及び符号器 E に依存して決まる．ここで，(2.26) の安全度は，暗号文のみから得られる平文の情報量を表しており，この量が小さいほど攻撃者が平文 M の部分情報を得ていることになる.

一方，共通鍵暗号方式の機能性と効率性に対する評価基準として，次のように定義される整合度と記憶容量を用いる.

$$\begin{aligned} &H(M \mid C, K) \\ &\quad = -\sum_{c \in \mathcal{C}} \sum_{k \in \mathcal{K}} p_{C|K}(c \mid k)\, p_K(k) \sum_{m \in \mathcal{M}} p_{M|CK}(m \mid c, k) \log p_{M|CK}(m \mid c, k)\,, \end{aligned} \tag{2.27}$$

$$H(K) = -\sum_{k \in \mathcal{K}} p_K(k) \log p_K(k)\,. \tag{2.28}$$

条件付き確率関数 $p_{C|K}(c \mid k)$ 及び $p_{M|CK}(m \mid c, m)$ は，確率関数 $p_K(k)$, $p_M(m)$，及び符号器 E に依存して決まる．(2.27) は，復号文が元の平文をどの程度復元できたかの尺度になっており，この量が小さいほど復元できていることになる．(2.28) は，送信者と受信者が鍵を安全に記憶するための記憶領域の大きさになっており，この量が小さいほど記憶領域が小さくなり，効率が良いことになる.

共通鍵暗号方式 Π に要求する制約条件

次に，(2.26) の安全度と (2.27) の整合度の 2 つの評価基準を用いて，共通鍵暗号方式 Π に要求する安全性と機能性に対する制約条件を定義する．

定義 2.2 仮定 2.1 を満たす攻撃者に対して，共通鍵暗号方式 Π が以下の制約条件を満たすとき，完全守秘性を有するという．

$$H(M \mid C) = H(M), \tag{2.29}$$

$$H(M \mid C, K) = 0. \tag{2.30}$$

□

2.2.2 節と同様に考えると，(2.29) は任意の $m \in \mathcal{M}$ と任意の $c \in \mathcal{C}$ に対して，

$$p_{M|C}(m \mid c) = p_M(m) \tag{2.31}$$

を満たすことと等価になる．また，(2.30) は，暗号文と鍵から平文を完全に復元できることを意味しており，任意の $m \in \mathcal{M}$ と任意の $k \in \mathcal{K}$ に対して，

$$p_{M|CK}(m \mid E(m,k),k) = 1 \tag{2.32}$$

を満たすことと等価になる．

記憶容量の理論的限界

定義 2.2 で定義した完全守秘性を有する共通鍵暗号方式 Π に対して，(2.28) で定義される記憶容量の理論的限界が導出されている．

定理 2.8 [27]
任意の完全守秘性を有する共通鍵暗号方式 Π は，以下を満たす．

$$H(M) \leq H(K). \tag{2.33}$$

□

この定理は，完全に安全な共通鍵暗号を実現するためには，少なくとも平文と同じ量 (長さ) の鍵を送受信者間で共有する必要があることを意味している．

完全守秘性を有する共通鍵暗号方式 Π の構成法

定義 2.2 で定義した完全守秘性を有する共通鍵暗号方式 Π の代表的な構成法に，ワンタイムパッド暗号がある [31]．ワンタイムパッド暗号では，平文全体の集合 $\mathcal{M}$，暗号文全体の集合 $\mathcal{C}$，及び鍵全体の集合 $\mathcal{K}$ は，全て長さ N の 2 値系列の集合 $\{0,1\}^N$ として定義される (N は任意)．このとき暗号化に用いる鍵 $k \in \{0,1\}^N$ は，確率

$$p_K(k) = 2^{-N},\ k \in \{0,1\}^N \tag{2.34}$$

に従って確率的に生成する，暗号化は平文 $m \in \{0,1\}^N$ と生成した鍵 k に対して，ビットごとに排他的論理和 (2 を法とする加算) をとり暗号文 $c \in \{0,1\}^N$ を生成する．ここで，ビットごとに排他的論理和をとる演算を $\oplus$ で表すと，暗号文は

$$c = m \oplus k \tag{2.35}$$

と表すことができる．したがって，暗号文 c と平文 m は互いに独立となるので，(2.29) を満たす．また，復号は暗号文 c と鍵 k をビットごとに排他的論理和をとると

$$c \oplus k = m \oplus k \oplus k = m \tag{2.36}$$

となり，一意に平文 m を復元することができるので，(2.30) を満たす．

例 2.1 図 2.2 にワンタイムパッド暗号による暗号化と復号の例を示す．まず，送信者と受信者の間で秘密鍵 0110010 を安全に共有しておく．その後，送信者が送りたい平文 1101100 に対して，秘密鍵 0110010 を用いて，ビットごとに排他的論理和をとり暗号文 1011110 を生成し，その暗号文を受信者に送信する．暗号文 1011110 を受信した受信者は，暗号文 1011110 と秘密鍵 0110010 に対して，ビットごとに排他的論理和をとり，元の平文 1101100 を得る．□

ワンタイムパッド暗号は，Shannon によって完全守秘性を有することが証明された [27]．また，ワンタイムパッド暗号における記憶容量は，定理 2.8 の限界を達成するので，完全守秘性を有する最適な共通鍵暗号方式となる．すなわち，以下の定理が成り立つ．

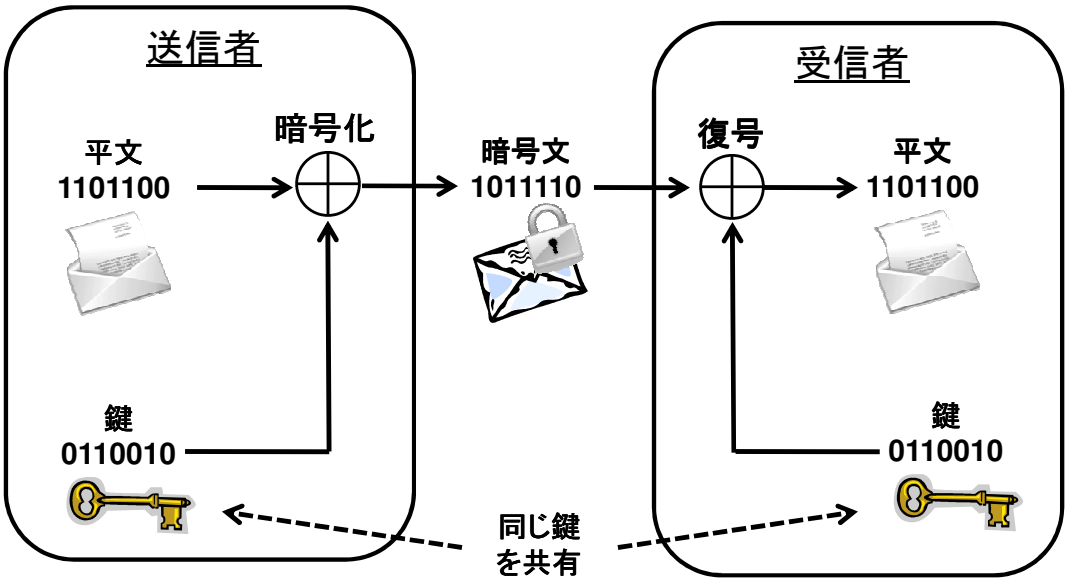

図 2.2: ワンタイムパッド暗号による暗号化と復号の例

定理 2.9 *[27]*

ワンタイムパッド暗号への攻撃が仮定 2.1 を満たすとき，ワンタイムパッド暗号は，完全守秘性を有する．また，ワンタイムパッド暗号は定理 2.8 の理論的限界を達成する最適な共通鍵暗号方式となる．　□

ワンタイムパッド暗号は平文と鍵の排他的論理和をとるだけで暗号化できるので，非常に高速な共通鍵暗号方式となるが，既知平文攻撃[1]による攻撃対象にされやすい．よって，平文を暗号化するたびに，その平文に対する新しい鍵を生成し，その鍵を送信者側と受信者側で安全に共有することが必要となる．さらに，共有した鍵は暗号化に使用するまでは安全に保管され，使用後は完全に消去されなければ安全性が損なわれてしまう．この性質は，軍事，及び外交上の文書などの暗号化では問題はないが，一般的な適用においては大きな障害となる．以上のことから，十分な長さの秘密鍵が安全に共有できていれば，ワンタイムパッド暗号によって情報量的に安全な秘匿通信は達成できるが，その鍵を共有するための鍵配布方式が情報量的

[1]詳細は割愛するが，既知平文攻撃とは，攻撃者が平文とそれに対応する暗号文を利用する攻撃である．暗号方式に対するその他の攻撃としては，暗号文単独攻撃，選択平文攻撃，選択暗号文攻撃がある [15, 29].

に安全な方式になっていなければ，暗号化された平文に対する安全性は保証されない．したがって，ワンタイムパッド暗号を用いて情報量的に安全な秘匿通信を達成するためには，情報量的安全性を持つ鍵配布方式が必要不可欠となる．

2.3.3　計算量的安全性を有する共通鍵暗号方式

共通鍵暗号方式の定義

共通鍵暗号方式の計算量的安全性を定義するために，定義 2.1 の共通鍵暗号方式 Π を，次のように変更した共通鍵暗号方式 Π' について考える．$l(n) \in \mathbb{N}^+$ をセキュリティパラメータ n に依存した関数とし，平文全体の集合を $\mathcal{M} = \{0,1\}^{l(n)}$，鍵全体の集合 $\mathcal{K}$ は $\log|\mathcal{K}| \geq n$ を満たす集合とする．ここで，$|\cdot|$ は集合の大きさを表す．

定義 2.3 共通鍵暗号方式 Π' に対する公開情報は，定義 2.1 の公開情報に加え，セキュリティパラメータ n を公開情報とする．共通鍵暗号方式 Π' は，定義 2.1 と同様の 3 つのステップから構成されるプロトコルとする．ただし，各ステップは，任意の確率的多項式時間アルゴリズムで実行される．　□

セキュリティパラメータ n は，共通鍵暗号方式の設計者が任意に決めることができる．

共通鍵暗号方式 Π' への攻撃に対する条件

ここで，$\{0,1\}$ 上に値をとる確率変数を B とし，その確率関数を

$$p_B(b) = \frac{1}{2},\ b \in \{0,1\} \tag{2.37}$$

とおく．定義 2.3 で定義した共通鍵暗号方式 Π' の計算量的安全性を定義するために，次のような仮定を設ける．

仮定 2.2 共通鍵暗号方式 Π' への攻撃は，以下の 5 つの条件を満たす．

前提条件： ある性質を持った関数が存在する．

攻撃者： 送受信者ではない任意の攻撃者 A．

攻撃対象： 平文 M_B.

利用可能情報： 2 つの平文 M_0, M_1 と暗号文 $C = E(M_B, K)$ (B と K は未知).

攻撃能力： 任意の確率的多項式時間アルゴリズムと等価. □

この仮定を仮定 2.1 と比較すると，攻撃者の仮定以外は全て異なる条件になる.

共通鍵暗号方式の評価基準

仮定 2.2 を満たす攻撃に対して，共通鍵暗号方式 Π' の安全性を測る評価基準となる安全度を定義するために，共通鍵暗号方式 Π'，攻撃者 (確率的多項式時間アルゴリズム) A，セキュリティパラメータ n に依存して結果を出力する識別試験 $\Omega(\Pi', \mathrm{A}, n)$ の定義を行う.

定義 2.4 識別試験 $\Omega(\Pi', \mathrm{A}, n)$ は，次の 4 つのステップから構成されるプロトコルである.

1. 攻撃者 A は，2 つの平文 $m_0, m_1 \in \{0,1\}^{l(n)}$ を選択し，試験者に渡す.
2. 試験者はランダムに $b \in \{0,1\}$ を選択し，共通鍵暗号方式 Π' に従って，鍵 $k \in \mathcal{K}$ を生成し，暗号文 $c = E(m_b, k)$ を計算する．試験者は，この暗号文 c を攻撃者 A に渡す.
3. 攻撃者 A は，$b' \in \{0,1\}$ を出力する.
4. $b' = b$ の場合は $\Omega(\Pi', \mathrm{A}, n) = 1$ とし，それ以外の場合は $\Omega(\Pi', \mathrm{A}, n) = 0$ とする. □

識別試験では，攻撃者 A が与えられた暗号文 c から 2 つの平文 m_0 と m_1 のどちらを暗号化したものか識別できるかどうかを判定している．したがって，全く平文に関する情報がない場合でも，1/2 の確率で識別に成功する.

この識別試験 $\Omega(\Pi', \mathrm{A}, n)$ を用いて，共通鍵暗号方式 Π' の安全性評価基準となる安全度を攻撃成功確率

$$\Pr\{\Omega(\Pi', \mathrm{A}, n) = 1\} \tag{2.38}$$

と定義する．攻撃成功確率は，共通鍵暗号方式 Π' と識別試験 $\Omega(\Pi', \mathrm{A}, n)$ に依存し，1/2 から 1 の間の値をとる．したがって，(2.26) の安全度とは逆に，安全度が低いほど安全性が高くなる．一方，共通鍵暗号方式 Π' の機能と効率に対する評価基準は，2.3.2 節と同様に整合度と記憶容量を用いる．

共通鍵暗号方式 Π' に要求する制約条件

次に，(2.38) の安全度と (2.27) の整合度の 2 つの評価基準を用いて，共通鍵暗号方式 Π' に要求する安全性と機能性の制約条件を定義する．

定義 2.5 仮定 2.2 を満たす攻撃者に対して，共通鍵暗号方式 Π' が以下の 2 つの制約条件を満たすとき，計算量的に安全，または計算量的安全性を有するという．

1. $H(M \mid C, K) = 0$ を満たす．
2. 全ての多項式 $\gamma \in \Gamma$ と全ての攻撃者 (確率的多項式時間アルゴリズム) A に対して

$$\Pr\{\Omega(\Pi', \mathrm{A}, n) = 1\} < \frac{1}{2} + \frac{1}{\gamma(n)}. \tag{2.39}$$

を満たす． □

(2.39) を満たす性質を，一般に識別不可能性という．厳密に言うと，定義 2.5 で定義している計算量的に安全な共通鍵暗号方式 Π' は，識別不可能性の意味で計算量的に安全となる．

識別不可能性と異なる安全性として，強秘匿性 (Semantically Secure) [13] がある．強秘匿性とは，暗号文 c から平文 m に関するどんな部分情報も得られないという性質で，計算量的安全性の中で最も強い安全性と考えられている．強秘匿性を保証するためには，攻撃に対して次のような仮定が与えられる．

前提条件： ある性質を持った関数が存在する．

攻撃者： 送受信者ではない任意の攻撃者 A.

攻撃対象： 平文 M の部分情報.

利用可能情報： 暗号文 C.

攻撃能力： 任意の確率的多項式時間アルゴリズムと等価.

この仮定は，仮定 2.1 における前提条件と攻撃能力の 2 つの条件を変更したものとなっている．上記の仮定を満たす攻撃者に対して，強秘匿性の意味で計算量的に安全な共通鍵暗号方式が定義されている．強秘匿性は最も強い安全性として定義されたが，定義 2.5 の識別不可能性と等価であることが証明されているので [13, 20]，強秘匿性を証明する場合，数学的に扱いやすい識別不可能性を証明することが多い.

記憶容量の理論的限界

情報量的安全性を有する共通鍵暗号方式に対しては，定理 2.8 のように記憶容量の理論的限界が導出されているが，計算量的安全性を有する共通鍵暗号方式における記憶容量の理論的限界は導出されていない．したがって，計算量的安全性を有する共通鍵暗号方式に対しては，記憶容量が最適な構成法の存在性が証明されていない.

計算量的安全性を有する共通鍵暗号方式 Π' の構成法

定義 2.5 を満たす共通鍵暗号方式 Π' の構成法の 1 つに，疑似乱数生成器を用いた方式がある [15]．疑似乱数生成器は，多項式時間アルゴリズムとして次のように定義する.

定義 2.6 $l : \mathbb{N}^+ \to \mathbb{N}^+$ を多項式関数，$G : \{0,1\}^n \to \{0,1\}^{l(n)}$ を多項式時間アルゴリズムとする．G は以下の制約条件を満たすとき，疑似乱数生成器という.

1. 全ての $n \in \mathbb{N}^+$ に対して，$l(n) > n$ を満たす.
2. 全ての確率的多項式時間アルゴリズム D と全ての $\gamma \in \Gamma$ に対して，

$$|\Pr\{D(R) = 1\} - \Pr\{D(G(S)) = 1\}| < \frac{1}{\gamma(n)}. \tag{2.40}$$

を満たす．ここで，R は $\{0,1\}^{l(n)}$ 上に値をとる確率変数で，その確率関数を $\{0,1\}^{l(n)}$ 上の一様分布とし，S は $\{0,1\}^n$ 上に値をとる確率変数で，その確率

関数を $\{0,1\}^n$ 上の一様分布とした．また，(2.40) の確率は，R と S の確率関数と D に依存する．

□

直観的に言うと，(2.40) は真の乱数と疑似乱数生成器の出力はほとんど見分けがつかないということを意味している．詳細は割愛するが素因数分解の困難性を仮定することで，疑似乱数生成器の存在性が証明されている [15]．疑似乱数生成器 G を用いた次のような構成法によって，計算量的に安全な共通鍵暗号方式 Π' が実現できる．

【疑似乱数生成器を用いた構成法】

平文全体の集合 $\mathcal{M}$ と暗号文全体の集合 $\mathcal{C}$ を $\{0,1\}^{l(n)}$ とおき，鍵全体の集合 $\mathcal{K}$ を $\{0,1\}^n$ とおく．また，$\{0,1\}^n$ 上の確率関数 p_K を

$$p_K(k) = 2^{-n},\ k \in \{0,1\}^n \tag{2.41}$$

とする．

鍵生成ステップ: 鍵全体の集合 $\{0,1\}^n$ 上の確率関数 $p_K(k)$ に従って，鍵 $k \in \mathcal{K}$ を確率的に生成し，安全な通信路を用いて送信者及び受信者に伝送する．

暗号化ステップ: 送信者は送りたい平文 $m \in \{0,1\}^{l(n)}$ を決定し，鍵 k と符号器 E を用いて暗号文

$$c = E(m,k) = m \oplus G(k). \tag{2.42}$$

を生成し，公開通信路を用いて受信者へ送信する．

復号ステップ: 暗号文 c を受信した受信者は，鍵 k と復号器 D を用いて復号文

$$\hat{m} = D(c,k) = c \oplus G(k) \tag{2.43}$$

に復号する． □

この構成法の計算量的安全性を保証するために，次のような仮定を設ける．

仮定 2.3 疑似乱数を用いた構成法への攻撃は，以下の条件を満たす．ただし，前提条件以外は仮定 2.2 と同じ条件となる．

前提条件： 疑似乱数生成器が存在する． □

この仮定を満たすとき，以下の定理が成り立つ．

定理 2.10 [*15*]
仮定 2.3 を満たすとき，疑似乱数生成器を用いた構成法は，計算量的安全性を有する． □

2.3.4　情報量的安全性と計算量的安全性の比較

情報量的安全性と計算量的安全性を比較するために，定義 2.4 の識別試験と同様に，定義 2.1 の共通鍵暗号方式 Π と攻撃者 A に依存して結果を出力する識別試験 Ω' を定義する．

定義 2.7 識別試験 $\Omega'(\Pi, \mathrm{A}, n)$ は，次の 4 つのステップから構成されるプロトコルである．

1. 攻撃者 A は，2 つの平文 $m_0, m_1 \in \mathcal{M}$ を選択し，試験者に渡す．
2. 試験者はランダムに $b \in \{0,1\}$ を選択し，共通鍵暗号方式 Π に従って，鍵 $k \in \mathcal{K}$ を生成し，暗号文 $c = E(m_b, k)$ を計算する．試験者は，この暗号文 c を攻撃者 A に渡す．
3. 攻撃者 A は，$b' \in \{0,1\}$ を出力する．
4. $b' = b$ の場合は $\Omega'(\Pi, \mathrm{A}) = 1$ とし，それ以外の場合は $\Omega'(\Pi, \mathrm{A}) = 0$ とする． □

識別試験 $\Omega'(\Pi, \mathrm{A})$ は，定義 2.4 の判別試験 $\Omega(\Pi', \mathrm{A}, n)$ と同様に，攻撃者 A が与えられた暗号文 c から 2 つの平文 m_0 と m_1 のどちらを暗号化したものか識別できるかどうかを判定している．したがって，全く平文に関する情報がない場合でも，1/2

の確率で識別に成功する．この識別試験 $\Omega'(\Pi, \mathrm{A})$ を用いて，共通鍵暗号方式 Π の安全性評価基準となる安全度を攻撃成功確率 $\Pr\{\Omega'(\Pi, \mathrm{A}) = 1\}$ と定義する．

共通鍵暗号方式 Π の識別不可能性の意味での情報量的安全性を保証するために，次のような仮定を設ける．

仮定 2.4 共通鍵暗号方式 Π への攻撃は，以下の 5 つの条件を満たす．

前提条件： 仮定しない．

攻撃者： 送受信者ではない任意の攻撃者 A．

攻撃対象： 平文 M_B．

利用可能情報： 2 つの平文 M_0, M_1 と暗号文 $C = E(M_B, K)$ (B と K は未知)．

攻撃能力： 無限の計算能力を持つ． □

以上の定義と仮定を用いて，識別不可能性の意味で情報量的に安全な共通鍵暗号方式 Π を定義する．

定義 2.8 仮定 2.4 を満たす攻撃者に対して，共通鍵暗号方式 Π が以下の制約条件を満たすとき，完全識別不可能性を有するという．

$$\Pr\{\Omega(\Pi', \mathrm{A}, n) = 1\} = \frac{1}{2}, \tag{2.44}$$

$$H(M \mid C, K) = 0. \tag{2.45}$$

□

以下の定理は，定義 2.2 の安全性と定義 2.8 の安全性の等価性を示している．

定理 2.11 [*15*]
共通鍵暗号方式 Π が完全守秘性を有するための必要十分条件は，完全識別不可能性を有することである． □

定理 2.11 により，共通鍵暗号方式の情報量的安全性と計算量的安全性の比較が容易になる．計算量的安全性の定義である定義 2.5 と情報量的安全性の定義と等価な定義 2.8 より，2 つの安全性は，前提条件，攻撃能力，及び安全度である攻撃成功確率に要求する制約条件の違いにある．前提条件と攻撃能力に対しては，情報量的安全性では仮定をおいていないが，計算量的安全性では仮定がおかれている．したがって，仮定が成り立たない場合，計算量的安全性は保証できない．また，攻撃成功確率に要求する制約条件については，情報量的安全性では最小の 1/2 である必要があるが，計算量的安全性では 1/2 より大きい場合も許容している．すなわち，計算量的安全性を有する共通鍵暗号方式は，攻撃対象の部分情報が攻撃者に洩れていることになる．一方，情報量的安全性では，攻撃対象の部分情報が全く洩れないことを保証しているので，情報量的安全性の方が攻撃者にとって厳しい条件となる．

計算量的安全性は，上述したように情報量的安全性で考えられている仮定を部分的に強めることで定義される．前提条件については，情報量的安全性では何も仮定しなかったが，計算量的安全性では，ある関数が存在するといった仮定や，数学的問題を解くことが困難であるという仮定をおいている．また，前提条件の仮定で用いられる関数の存在性を保証するためには，数学的問題を解くことが困難であることを仮定する必要があるため，本質的には数学的問題の困難性の仮定が前提条件となる．したがって，仮定に用いた数学的問題の効率的な解法が発見されると，暗号方式の安全性も保証されなくなるという欠点がある．また，情報量的安全性では攻撃者の計算能力に対しては何も制限しないので，無限の計算能力を持つ攻撃者に対しても安全性が保証される．一方，計算量的安全性は攻撃者の計算能力に現実的な仮定をおいたときに保証される安全性として定義されるので，この仮定を満たしていない場合は，攻撃者に攻撃対象の情報を特定されてしまうことになる．現在，インターネット上のセキュリティシステムとして現在広く利用されている RSA 暗号 [25], ElGamal 暗号 [12]，楕円曲線暗号 [16, 21] などの暗号方式の多くは，このような計算量的安全性に基づいているため，計算機能力の急速な向上，暗号攻撃技術の進展, 及び将来実現する可能性がある量子計算機によって秘密情報の不正な抽出が可能となってしまう．実際，量子アルゴリズムである Shor のアルゴリズム [28] を利用することで，素因数分解問題や離散対数問題が現実的な時間で解くことができる．このため，現在主流の暗号方式では，長期的な安全性は保証されず，今後はより高度な

安全性を持つセキュリティシステムが必要不可欠となる．このような理由から，情報量的に安全な暗号方式は，次世代の暗号方式として期待されている．

しかし，情報量的に安全な暗号方式は，一般に安全に記録しておかなければならない情報量が膨大になってしまうという欠点がある．例えば，情報量的に安全な共通鍵暗号方式を実現するためには，メッセージと同じ長さの鍵が必要となる [27] ので，多くの長いメッセージを暗号化する必要がある場合を考えると現実的な方式ではない．したがって，現実的に利用可能な共通鍵暗号方式を実現するためには，安全性のレベルを弱める必要が生じる．このような場合，現実的に妥当な時間内に妥当な確率で攻撃に成功することができなければ，十分安全であるという立場に立った計算量的安全性を有する暗号方式を用いることが有効となる．

以上より，情報量的安全性を有する暗号方式は，高い安全性を保証するが効率の面で欠点があり，計算量的安全性を有する暗号方式は，効率の面では優れているが長期的な安全性が保証されないという欠点があることがわかる．したがって，安全性と効率性のバランスを十分考慮した上で，情報量的に安全な暗号方式と計算量的に安全な暗号方式を利用する場面に応じて使い分けることが最も肝要である．

2.4　情報量的安全性を有する秘密分散法

2.4.1　情報量的安全性を有する暗号方式の研究アプローチ

1.2 節で簡単に述べたが，情報量的安全性を有する暗号方式に関する研究においては，特に以下のようなアプローチが重要であると考えられている．

- 対象とする暗号方式の定義を行う．
- 暗号方式の機能性，安全性，効率性を測る評価基準を定義する．
- 暗号方式に要求する制約条件を定義する．すなわち，機能性と安全性に対する条件を定義する．
- 定義した制約条件を満たすもとで，効率性を最大化することを研究目標とする．具体的には，以下のような課題に取り組む．

– 定義した制約条件を満たす暗号方式に対して，効率の理論的限界を導出する．

– 定義した制約条件を満たし，かつ導出した理論的限界を達成する暗号方式の具体的な構成法を提案する．

例えば，2.3.2 節では，情報量的安全性を有する共通鍵暗号方式を上記のアプローチに基づいて説明している．共通鍵暗号方式の定義は定義 2.1 で，各評価基準は (2.26), (2.27), (2.28) で，要求する制約条件は定義 2.2 で定義している．また，定義した制約条件を満たす共通鍵暗号方式に対する効率 (記憶容量) の理論的限界は，定理 2.8 で与えられており，その理論的限界を達成する具体的な構成法として，2.3.2 節で述べたワンタイムパッド暗号がある．

以下，本節では情報量的安全性を有する代表的な暗号方式である秘密分散法について説明する．

2.4.2　秘密分散法の定義

秘密分散法 (SSS : secret sharing scheme) とは，ある重要な秘密情報を安全に分散して管理する暗号方式である [2, 14, 26, 33]．秘密分散法の参加者は，ディーラーと呼ばれる信頼できる機関 D と分散情報が与えられる n 人のユーザ $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ から構成される．ただし，$\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ を各ユーザの ID 情報 (識別子) として用いる場合もあることに注意しておく．秘密分散法では，まず，ディーラー D が秘密情報 s と符号器 $E : \mathcal{S} \to \mathcal{W}^n$ から n 個の分散情報 $w_1, w_2, \cdots, w_n$ を生成する．ここで，s と w_j, $1 \leq j \leq n$ はそれぞれ可算集合 $\mathcal{S}$, $\mathcal{W}$ の要素とし，ユーザ集合を $\mathcal{P} = \{\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n\}$ と定義する．また，s と w_j, $1 \leq j \leq n$ に対応する確率変数を S, W_j, $1 \leq j \leq n$ とする．生成した分散情報 w_j, $1 \leq j \leq n$ は，それぞれユーザ P_j に配られる．秘密情報 s を完全に復元できるユーザの集合 $\mathcal{B} \subset \mathcal{P}$ を有資格集合と呼び，有資格集合全体の集合 Γ を有資格集合族と呼ぶ．秘密情報 s を復元は，任意の有資格集合 $\mathcal{B} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{B}|}}\right\}$ が持つ分散情報と復号器 $D : \mathcal{W}^* \to \mathcal{S}$ を用いることで可能となる．ここで，秘密分散法の定義を行う．

定義 2.9 ユーザ集合 $\mathcal{P}$，秘密情報全体の集合 $\mathcal{S}$，分散情報全体の集合 $\mathcal{W}$，符号器 E，復号器 D，有資格集合族 Γ，$\mathcal{S}$ 上の確率関数 $p_S(s)$ を秘密分散法 SSS に対する公開情報とする．秘密分散法 SSS は，次の 2 つのステップから構成されるプロトコルである．

秘密分散ステップ: ディーラー D は秘密情報 $s \in \mathcal{S}$ と符号器 E を用いて，n 個の分散情報 $E(s) = (w_1, w_2, \cdots, w_n)$ を生成する．各分散情報 w_j, $1 \leq j \leq n$ は，安全な通信路を用いてユーザ P_j へそれぞれ配布される．各ユーザ P_j, $1 \leq j \leq n$ は，分散情報 w_j を安全な場所に記憶する．

秘密復元ステップ: 任意の有資格集合

$$\mathcal{B} = \left\{ \mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{B}|}} \right\} \in \Gamma \tag{2.46}$$

は，記憶している分散情報 $w_{j_1}, w_{j_2}, \cdots, w_{j_{|\mathcal{B}|}}$ と復号器を用いて秘密情報

$$D\left(w_{j_1}, w_{j_2}, \cdots, w_{j_{|\mathcal{B}|}} \right) = s \tag{2.47}$$

を復元する．□

2.4.3　秘密分散法の評価基準の定義

ここで，秘密分散法 SSS への攻撃に対して，次のような仮定を設ける．

仮定 2.5 秘密分散法 SSS への攻撃は，以下の 5 つの条件を満たす．

前提条件： 仮定しない．

攻撃者： 任意のユーザ集合 $\mathcal{F} = \left\{ \mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{F}|}} \right\} \subset \mathcal{P}$.

攻撃対象： 秘密情報 S の部分情報.

利用可能情報： $\mathcal{F}$ が持つ分散情報 $W_{j_1}, W_{j_1}, \cdots, W_{j_{|\mathcal{F}|}}$.

攻撃能力： 無限の計算能力を持つ.　□

次に，秘密分散法の安全性を測る評価基準となる安全度を

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{F}|}}\right) = -\sum_{w_{j_1}^{j_{|\mathcal{F}|}} \in \mathcal{W}^{|\mathcal{F}|}} p_{W_{j_1}^{j_{|\mathcal{F}|}}}\left(w_{j_1}^{j_{|\mathcal{F}|}}\right) \sum_{s \in \mathcal{S}} p_{S|W_{j_1}^{j_{|\mathcal{F}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{F}|}}\right) \log p_{S|W_{j_1}^{j_{|\mathcal{F}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{F}|}}\right),$$

$$\forall \mathcal{F} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{F}|}}\right\} \subset \mathcal{P}, \tag{2.48}$$

と定義する．確率関数 $p_{W_{j_1}^{j_{|\mathcal{F}|}}}\left(w_{j_1}^{j_{|\mathcal{F}|}}\right)$，及び条件付き確率関数 $p_{S|W_{j_1}^{j_{|\mathcal{F}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{F}|}}\right)$ は，確率関数 $p_S(s)$，及び符号器 E に依存して決まる．(2.48) の安全度は，任意の集合 $\mathcal{F}$ が持つ分散情報から得られる秘密情報の情報量を表しており，この量が小さいほど，攻撃者が攻撃対象となる秘密情報の部分情報を得ていることになる．

一方，秘密分散法の機能性と効率性に対する評価基準となる復元度と記憶容量を，それぞれ次のように定義する．

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{B}|}}\right) = -\sum_{w_{j_1}^{j_{|\mathcal{B}|}} \in \mathcal{W}^{|\mathcal{B}|}} p_{W_{j_1}^{j_{|\mathcal{B}|}}}\left(w_{j_1}^{j_{|\mathcal{B}|}}\right) \sum_{s \in \mathcal{S}} p_{S|W_{j_1}^{j_{|\mathcal{B}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{B}|}}\right) \log p_{S|W_{j_1}^{j_{|\mathcal{B}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{B}|}}\right),$$

$$\forall \mathcal{B} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{B}|}}\right\} \in \Gamma, \tag{2.49}$$

$$H\left(W_j\right) = -\sum_{w_j \in \mathcal{W}} p_W(w_j) \log p_W(w_j),\ 1 \leq j \leq n. \tag{2.50}$$

確率関数 $p_{W_{j_1}^{j_{|\mathcal{B}|}}}\left(w_{j_1}^{j_{|\mathcal{B}|}}\right)$，及び条件付き確率関数 $p_{S|W_{j_1}^{j_{|\mathcal{B}|}}}\left(s \mid w_{j_1}^{j_{|\mathcal{B}|}}\right)$ は，確率関数 $p_S(s)$，及び符号器 E に依存して決まる．(2.49) は，任意のアクセス集合が持つ分散情報から秘密情報をどの程度復元できたかの尺度になっており，この量が小さいほど復元できていることになる．(2.50) は，ユーザが分散情報を安全に記憶するための記憶領域の大きさになっており，この量が小さいほど記憶領域が小さくなる．

2.4.1 節で述べたように，情報量的安全性を有する暗号方式の研究では，対象となる暗号方式に要求する制約条件を定義し，その制約条件のもとで効率性を最大化することが重要な目的となる．次節以降では，秘密分散法に対して，従来用いられて

いる制約条件，その制約条件下における記憶容量の理論的限界，及び理論的限界を達成する秘密分散法の構成法について述べる．

2.4.4　秘密分散法に要求する制約条件の定義

次に，秘密分散法 SSS に要求する制約条件の定義を行う．従来の秘密分散法 SSS に要求されている安全性に対する制約条件は，しきい値型安全性に対する制約条件 [14, 26] としきい値ランプ型の安全性に対する制約条件 [2, 33] がある．以下で，それぞれの制約条件の定義を行う．

定義 2.10 *[14]*

秘密分散法 SSS への攻撃が，仮定 2.5 を満たすとする．任意の正整数 $k \leq n$ に対して，有資格集合族 $\Gamma = \{\mathcal{B} \mid |\mathcal{B}| \geq k, \mathcal{B} \subseteq \mathcal{P}\}$ の秘密分散法 SSS が以下の制約条件を満たすとき，(k, n) しきい値型安全性を有する秘密分散法 (以下では，簡単のため (k, n) しきい値型秘密分散法と呼ぶ) という．

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{B}|}}\right) = 0,\ \forall \mathcal{B} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{B}|}}\right\} \in \Gamma, \tag{2.51}$$

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{F}|}}\right) = H\left(S\right),\ \forall \mathcal{F} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{F}|}}\right\} \in \bar{\Gamma}, \tag{2.52}$$

ここで，$\bar{\Gamma}$ は Γ の補集合を表す．　□

この定義の対象となる秘密分散法 SSS における有資格集合族は，任意の k 人以上のユーザとなるので，(2.51) の制約条件は，任意の k 個以上の分散情報から秘密情報を一意に復元できることを意味している．また，(2.52) の制約条件は，任意の $k-1$ 個以下の分散情報から秘密情報 S の情報は全く得られないことを意味している．この制約条件 (2.52) が，しきい値型安全性に対する制約条件となる．

(2.52) を弱めた制約条件が，しきい値ランプ型安全性を保証する制約条件である．しきい値ランプ型安全性を有する秘密分散法は，定義 2.10 と同様の有資格集合族に対する秘密分散法に対して定義される．

定義 2.11 [33]

秘密分散法 SSS への攻撃が，仮定 2.5 を満たすとする．任意の正整数 $k \leq n$ と $1 \leq L \leq k$ に対して，有資格集合族 $\Gamma = \{\mathcal{B} \mid |\mathcal{B}| \geq k, \mathcal{B} \subseteq \mathcal{P}\}$ の秘密分散法 SSS が以下の制約条件を満たすとき，(k, L, n) しきい値ランプ型安全性を有する秘密分散法 (以下では，簡単のため (k, L, n) しきい値ランプ型秘密分散法と呼ぶ) という．

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{B}|}}\right) = 0, \ \forall \mathcal{B} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{B}|}}\right\} \in \Gamma, \quad (2.53)$$

$$H\left(S \mid W_{j_1}, W_{j_2}, \cdots, W_{j_{|\mathcal{F}|}}\right) = \frac{k - \varphi_{k-L}\left(|\mathcal{F}|\right)}{L} H\left(S\right), \quad \forall \mathcal{F} = \left\{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_{|\mathcal{F}|}}\right\} \in \bar{\Gamma}, \quad (2.54)$$

ここで，関数 $\varphi_{k-L} : \{0, 1, \cdots, k-1\} \to \{k-L, k-L+1, \cdots, k-1\}$ は，

$$\varphi_{k-L}\left(|\mathcal{F}|\right) = \begin{cases} k-L & \text{for} \quad |\mathcal{F}| \leq k-L \\ |\mathcal{F}| & \text{for} \quad k-1 \geq |\mathcal{F}| > k-L \end{cases} \quad (2.55)$$

とした． □

定義 2.10 の (k, n) しきい値型秘密分散法は，任意の k 個以上の分散情報が集まれば秘密情報を復元でき，任意の $k-1$ 個以下の分散情報では秘密情報を全く得ることができない．これに対して，定義 2.11 の (k, L, n) しきい値ランプ型秘密分散法は，任意の k 個以上の分散情報が集まれば秘密情報を復元でき，任意の $k-L$ 個以下の分散情報では秘密情報を全く得られず，任意の $k-l$ 個 $(1 \leq l \leq L-1)$ の分散情報では l が小さくなるにつれて，段階的に秘密情報が得られる．この制約条件 (2.54) が，しきい値ランプ型安全性に対する制約条件となる．

定義より，(k, L, n) しきい値ランプ型秘密分散法は，(k, n) しきい値型秘密分散法を拡張した形になっているが，安全性は (k, n) しきい値型秘密分散法より低くなってしまう．しかし，秘密情報の集合のサイズが大きい場合は，$H(S)/L$ も十分大きくなり実用的に十分な安全性を持たせることができる．

2.4.5　秘密分散法における記憶容量の理論的限界

定義 2.10，及び定義 2.11 で定義した (k, n) しきい値型秘密分散法，及び (k, L, n) しきい値ランプ型秘密分散法に対して，記憶容量 $H(W_j)$, $1 \leq j \leq n$ の理論的限界

がそれぞれ導出されている．

定理 2.12 [14]
任意の (k, n) しきい値型秘密分散法は，以下を満たす．

$$H(W_j) \geq H(S),\ 1 \leq j \leq n. \tag{2.56}$$

□

この定理は，(k, n) しきい値型秘密分散法を実現するためには，少なくとも秘密情報と同じ量 (長さ) の分散情報が必要となることを意味している．このため，(k, n) しきい値型秘密分散法は，効率の面から考えると性能が低くなってしまう．一方，(k, L, n) しきい値ランプ型秘密分散法は，2.4.4 節でも述べたように，安全性の面では (k, n) しきい値型秘密分散法より劣るが，効率の面では優れた性能を持つ．次の定理は，(k, L, n) しきい値ランプ型秘密分散法における効率性，すなわち記憶容量の理論的限界を示している．

定理 2.13 [33]
任意の (k, L, n) しきい値ランプ型秘密分散法は，以下を満たす．

$$H(W_j) \geq \frac{1}{L} H(S),\ 1 \leq j \leq n. \tag{2.57}$$

□

これらの定理から，(k, L, n) しきい値ランプ型秘密分散法は，(k, n) しきい値型秘密分散法より安全性は低いが，その一方で，記憶容量を削減できることがわかる．

2.4.6　秘密分散法の構成法

(2.56) を等号で達成する最適な (k, n) しきい値型秘密分散法の代表的な構成法に，有限体上の多項式を用いた構成法が提案されている [26]．ここで，q を任意の素数のべき乗とし，位数 q の有限体を $\mathbb{F}_q$ と表す．有限体 $\mathbb{F}_q$ 上の多項式を用いた最適な (k, n) しきい値型秘密分散法の構成法は，次のようになる．

【多項式を用いた (k,n) しきい値型秘密分散法の構成法】

公開情報であるユーザ集合 $\mathcal{P}$，秘密情報全体の集合 $\mathcal{S}$，分散情報全体の集合 $\mathcal{W}$ を $\mathbb{F}_q$ とおき，有資格集合族を $\Gamma = \{\mathcal{B} \mid |\mathcal{B}| \geq k, \mathcal{B} \subseteq \mathcal{P}\}$ とする．

秘密分散ステップ: ディーラーは $\mathbb{F}_q$ 上の $k-1$ 個の乱数 $a_1, a_2, \cdots, a_{k-1}$ を独立に生成し，次のように n 個の分散情報 $w_j,\ 1 \leq j \leq n$ を生成する．

$$\begin{aligned} E(s) &= (w_1, w_2, \cdots, w_n) \\ &= (P(\mathrm{P}_1), P(\mathrm{P}_2), \cdots, P(\mathrm{P}_n)). \end{aligned} \tag{2.58}$$

ここで,

$$P(\mathrm{P}_j) = s + \sum_{i=1}^{k-1} a_i (\mathrm{P}_j)^i,\ 1 \leq j \leq n \tag{2.59}$$

とおいた．各分散情報 $w_j,\ 1 \leq j \leq n$ は，安全な通信路を用いてユーザ P_j へそれぞれ配布される．各ユーザは $\mathrm{P}_j,\ 1 \leq j \leq n$ は，分散情報 w_j を安全な場所に記憶する．

秘密復元ステップ: 任意の有資格集合 $\mathcal{B} \in \Gamma$ は，記憶している分散情報から任意の k 個の分散情報 $w_{j_l} = P(\mathrm{P}_{j_l}),\ 1 \leq l \leq k$ を選択し，ラグランジュ補間を用いて以下の計算を行い秘密情報 s を復元する．

$$\begin{aligned} \sum_{l=1}^{k} \lambda_{j_l} P(\mathrm{P}_{j_l}) &= P(0) \\ &= s. \end{aligned} \tag{2.60}$$

ここで,

$$\lambda_{j_l} = \prod_{m=1:m\neq l}^{k} \frac{-\mathrm{P}_{j_m}}{\mathrm{P}_{j_l} - \mathrm{P}_{j_m}} \tag{2.61}$$

とした．　□

一方，(2.57) を等号で達成する最適な (k, L, n) しきい値ランプ型秘密分散法の構成法は，秘密情報全体の集合を

$$\mathcal{S} = \mathcal{S}_0 \times \mathcal{S}_1 \times \cdots \times \mathcal{S}_{L-1} \tag{2.62}$$

のように L 個の集合に分割し，$\mathcal{S}_l = \mathbb{F}_q, 0 \leq l \leq L-1$ とおく．このとき，秘密情報 $s = (s_0, s_1, \cdots .s_{L-1}) \in \mathcal{S}$ の分散情報 $w_j, 1 \leq j \leq n$ は次のように計算される．

$$w_j = \sum_{l=0}^{L-1} s_l + \sum_{i=L}^{k-1} a_i (\mathrm{P}_j)^i,\ 1 \leq j \leq n. \tag{2.63}$$

分散情報から秘密情報の復元は，多項式を用いた (k, n) しきい値型秘密分散法の構成法と同様に，ラグランジュ補間を用いることで実現できる．

第3章　鍵事前配布方式に関する従来研究

本章では，情報量的に安全な鍵事前配布方式に関する従来研究について述べる．従来の鍵事前配布方式では，任意の t 人のユーザ間で鍵を共有する方式が考えられている．本研究では，このような鍵事前配布方式を t 会議鍵事前配布方式 (t-KPS: t-conference Key Predistribution System) と呼ぶ．以下では，t-KPS に関する従来結果について述べる．

3.1　t 会議鍵事前配布方式 (t-KPS) の定義

t-KPS の利用者は，個体識別のための情報である ID 情報を持つ n_D 個のセンターと n_P 人のユーザで構成されている．各センターの ID 情報を D_k, $1 \leq k \leq n_D$ とし，各ユーザの ID 情報を P_i, $1 \leq i \leq n_P$ とおく．本研究では，t-KPS を定義するために，次のような集合と関数を用いる．

- $\mathcal{D} = \{\mathrm{D}_1, \mathrm{D}_2, \cdots, \mathrm{D}_{n_D}\}$: センターの ID 情報全体の集合.
- $\mathcal{P} = \{\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_{n_P}\}$: ユーザの ID 情報全体の集合.
- $\mathcal{A}_j \subset \mathcal{P}$, $1 \leq j \leq \binom{n_P}{t}$: 任意の t 人のユーザの ID 情報からなる集合 (以下ではグループと呼ぶ).
- $\mathcal{A}(\mathcal{P}, t) = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\binom{n_P}{t}}\right\}$: グループ全体の集合.
- $\mathcal{K}$: グループで共有する鍵全体の集合.
- $\mathcal{S}$: センターが生成する秘密情報全体の集合.

- $\mathcal{V}$: センターが生成するセンター間通信情報全体の集合，及びセンターが記憶するセンター記憶情報全体の集合.
- $\mathcal{U}$: センターが生成するユーザ受信情報全体の集合，及びユーザが記憶するユーザ記憶情報全体の集合.
- $f_T : \mathcal{S} \times \mathcal{D} \to \mathcal{V}$: センター間通信情報生成関数.
- $f_M : \mathcal{V}^{n_D} \to \mathcal{V}$: センター記憶情報生成関数.
- $F_T : \mathcal{V} \times \mathcal{P} \to \mathcal{U}$: ユーザ受信情報生成関数.
- $g_M : \mathcal{U}^L \to \mathcal{U}$: ユーザ記憶情報生成関数.
- $g_K : \mathcal{U} \times \mathcal{P}^{t-1} \to \mathcal{K}$: 鍵生成関数.

上記の記法を用いて t-KPS を，次のように定義する.

定義 3.1 6 つの集合 $\mathcal{D}, \mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V}, \mathcal{U}$，5 つの関数 f_T, f_M, F_T, g_M, g_K，及び確率関数 $p_S(s),\ s \in \mathcal{S}$ を公開情報とする．t-KPS は，次の 6 つのステップから構成されるプロトコルである.

＜ *Step1*： 秘密情報の生成＞

各センター $\mathrm{D}_k, 1 \le k \le n_D$ は，それぞれ独立に秘密情報 $s_k \in \mathcal{S}$ を確率分布 p_S にしたがって生成する.

＜ *Step2:* センター間の通信＞

$1 \le k, k' \le n_D$ 対して，センター D_k は関数 f_T を用いて，センター $\mathrm{D}_{k'}$ に対するセンター間通信情報 $v_{k,k'} = f_T\left(s_k, \mathrm{D}_{k'}\right)$ を生成し，安全な通信路を用いて送信する[1].

＜ *Step3:* センター記憶情報の計算・記憶＞

$1 \le k \le n_D$ に対して，センター D_k は関数 f_M を用いて，センター D_k に対するセンター記憶情報 $v_k = f_M\left(v_{1,k}, v_{2,k}, \cdots, v_{n_D,k}\right)$ を生成・記憶する.

＜ *Step4:* センターとユーザ間の通信＞

各ユーザ $\mathrm{P}_i, 1 \le i \le n_P$ は，通信可能なセンターの中から任意の L 個のセンター集

[1] $k = k'$ の場合も，D_k は $v_{k,k'} \in \mathcal{V}_{k,k'}$ を計算し，自身にもセンター間通信情報を送信することにする.

合 $\mathcal{D}_i = \{\mathrm{D}_{i_1}, \mathrm{D}_{i_2}, \cdots, \mathrm{D}_{i_L}\} \subseteq \mathcal{D}$ を選択する．選択された各センター $\mathrm{D}_{i_j}, 1 \leq j \leq L$ は，関数 F_T を用いて，ユーザ受信情報 $u_{i_j,i} = F_T\left(v_{i_j}, \mathrm{P}_i\right)$ を生成し，安全な通信路を用いて送信する．

＜ *Step5:* ユーザ記憶情報の計算・記憶＞

各ユーザ $\mathrm{P}_i, 1 \leq i \leq n_P$ は，送られてきた L 個のユーザ受信情報 $u_{i_j,i}, 1 \leq j \leq L$ と関数 g_M を用いて，ユーザ記憶情報 $u_i = g_M\left(u_{i_1,i}, u_{i_2,i}, \cdots, u_{i_L,i}\right)$ を生成・記憶する．

＜ *Step6:* グループの鍵の生成＞

任意の t 人のグループ $\mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\}$ に対して，ユーザ $\mathrm{P}_{j_i}, 1 \leq i \leq t$ は，ユーザ記憶情報 u_{j_i}, $\mathcal{A}_j$ に属する P_{j_i} 以外の ID 情報 $\left(\mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right)$, 及び関数 g_K を用いて，グループ $\mathcal{A}_j$ の鍵 $k_j = g_K\left(u_i, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right)$ を生成する．　□

Step1 において，各センターの秘密情報が確率的に生成されるので，Step2 以降で生成する情報は全て確率関数 $p_S(s)$ と公開情報である 5 つの関数に依存する．ここで，集合 $\mathcal{S}$ の中に値をとる確率変数を S_k, $1 \leq k \leq n_D$ とし，S_k に対する確率関数は，k に依らず $p_S(\cdot)$ とする．S_k は，センター D_k が生成する秘密情報 s_k に対応する確率変数となる．同様に，センター間通信情報 $v_{k,k'}$, $1 \leq k, k' \leq n_D$ に対する確率変数を $V_{k,k'}$，センター記憶情報 v_k, $1 \leq k \leq n_D$ に対する確率変数を V_k，ユーザ受信情報 $u_{k,i}$, $1 \leq k \leq n_D$, $1 \leq i \leq n_P$ に対する確率変数を $U_{k,i}$，ユーザ記憶情報 u_i, $1 \leq i \leq n_P$ に対する確率変数を U_i，グループ $\mathcal{A}_j$, $1 \leq j \leq \binom{n}{t}$ の鍵 k_j に対する確率変数を K_j とする．また，簡単のため，$U_{\mathcal{D}_i,i} = (U_{i_1,i}, U_{i_2,i}, \cdots, U_{i_L,i})$ とおく．

3.2　t-KPS の評価基準の定義

ここで，t-KPS への攻撃に，次のような仮定を設ける．

仮定 3.1 t-KPS への攻撃は，以下の 5 つの条件を満たす．

前提条件： 仮定しない．

攻撃者： 任意の複数のセンター (以下では，結託センターと呼ぶ)

$$\mathcal{X} \;=\; \left\{\mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{|\mathcal{X}|}}\right\} \subset \mathcal{D} \tag{3.1}$$

とユーザ (以下では，結託ユーザと呼ぶ)

$$\mathcal{Y} \;=\; \left\{\mathrm{P}_{i_1}, \mathrm{P}_{i_2}, \cdots, \mathrm{P}_{i_{|\mathcal{Y}|}}\right\} \subset \mathcal{P}. \tag{3.2}$$

攻撃対象： $\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意のグループ $\mathcal{A}_j$ の鍵 K_j の部分情報.

利用可能情報： 攻撃者が t-KPS において正規に得ることができる全ての情報．すなわち,

$$\begin{aligned}
U(\mathcal{Y}) &= \left(U_{\mathcal{D}_{i_1},i_1}, U_{\mathcal{D}_{i_2},i_2}, \cdots, U_{\mathcal{D}_{i_{|\mathcal{Y}|}},i_{|\mathcal{Y}|}}\right), \\
V(\mathcal{X}) &= \Big(V_{k_{|\mathcal{X}|+1},k_1}, V_{k_{|\mathcal{X}|+1},k_2}, \cdots, V_{k_{|\mathcal{X}|+1},k_{|\mathcal{X}|}}, V_{k_{|\mathcal{X}|+2},k_1}, V_{k_{|\mathcal{X}|+2},k_2}, \\
&\qquad \cdots, V_{k_{|\mathcal{X}|+2},k_{|\mathcal{X}|}}, \cdots, V_{k_{n_D},k_1}, V_{k_{n_D},k_2}, \cdots V_{k_{n_D},k_{|\mathcal{X}|}}\Big), \\
S(\mathcal{X}) &= \left(S_{k_1}, S_{k_2}, \cdots, S_{k_{|\mathcal{X}|}}\right).
\end{aligned}$$

ここで，$\mathcal{D} = \left\{\mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{n_D}}\right\}$ とおいた.

攻撃能力： 無限の計算能力を持つ. □

ここで，確率変数 $U(\mathcal{Y})$, $V(\mathcal{X})$, $S(\mathcal{X})$ は，それぞれ $\mathcal{U}$, $\mathcal{V}$, $\mathcal{S}$ の直積集合 $\mathcal{U}(\mathcal{Y}) = \mathcal{U}^{L\cdot|\mathcal{Y}|}$, $\mathcal{V}(\mathcal{X}) = \mathcal{V}^{|\mathcal{X}|\cdot(n_D-|\mathcal{X}|)}$, $\mathcal{S}(\mathcal{X}) = \mathcal{S}^{|\mathcal{X}|}$ に値をとる.

仮定 3.1 に基づいて，t-KPS の安全性を測る評価基準となる安全度を，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の攻撃者 $\mathcal{X}, \mathcal{Y}$ と任意の鍵 K_j に対して,

$$\begin{aligned}
&H\left(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})\right) \\
&\quad = -\sum_{u(\mathcal{Y})\in\mathcal{U}(\mathcal{Y})} \sum_{v(\mathcal{X})\in\mathcal{V}(\mathcal{X})} \sum_{s(\mathcal{X})\in\mathcal{S}(\mathcal{X})} p_{U(\mathcal{Y})V(\mathcal{X})S(\mathcal{X})}\left(u(\mathcal{Y}), v(\mathcal{X}), s(\mathcal{X})\right) \\
&\qquad \times \sum_{k_j\in\mathcal{K}} p_{K_j|U(\mathcal{Y})V(\mathcal{X})S(\mathcal{X})}\left(k_j \mid u(\mathcal{Y}), v(\mathcal{X}), s(\mathcal{X})\right) \\
&\qquad\qquad \times \log p_{K_j|U(\mathcal{Y})V(\mathcal{X})S(\mathcal{X})}\left(k_j \mid u(\mathcal{Y})\, v(\mathcal{X})\, s(\mathcal{X})\right)
\end{aligned} \tag{3.3}$$

と定義する．(3.3) の確率関数及び条件付き確率関数は，確率関数 $p_S(s)$ 及び 5 つの関数 f_T, f_M, F_T, g_M, g_K に依存して決まる．(3.3) の安全度は，攻撃者が利用可能な

情報から得られる鍵の情報量を表しており，この量が小さいほど，攻撃者が攻撃対象となる鍵の情報を得ていることになる．

また，t-KPS の機能性を測る評価基準を (3.4)，効率性を測る評価基準を (3.5), (3.6) のように定義する．

$$H\left(K_j \mid U_{j_i}\right) = -\sum_{u_{j_i}\in\mathcal{U}} p_{U_{j_i}}\left(u_{j_i}\right) \sum_{k_j\in\mathcal{K}} p_{K_j}\left(k_j \mid u_{j_i}\right) \log p_{K_j}\left(k_j \mid u_{j_i}\right),\ 1 \le i \le t,$$

$$\forall \mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\} \in \mathcal{A}\left(\mathcal{P}, t\right), \quad (3.4)$$

$$H\left(U_i\right) = -\sum_{u_i\in\mathcal{U}} p_{U_i}\left(u_i\right) \log p_{U_i}\left(u_i\right), \quad (3.5)$$

$$H\left(V_k\right) = -\sum_{v_k\in\mathcal{V}} p_{V_k}\left(v_k\right) \log p_{V_k}\left(v_k\right). \quad (3.6)$$

上式の確率関数及び条件付き確率関数は，確率関数 $p_S(s)$ 及び 5 つの関数 f_T, f_M, F_T, g_M, g_K に依存して決まる．(3.4) の整合度は，グループ内で正しく鍵が共有できるかどうかを測る評価基準で，この量が小さいほど正しく鍵が共有できたことになる．また，(3.5) と (3.6) の記憶容量は，各ユーザ，及び各センターに対する固有の情報であるユーザ記憶情報，及びセンター記憶情報を記憶するために必要なメモリ量を測る評価基準で，この量が小さいほどメモリ量が小さいことになる．

2.4.1 節で述べたように，情報量的安全性を有する暗号方式の研究では，対象となる暗号方式に要求する制約条件を定義し，その制約条件のもとで効率性を最大化することが重要な目的となる．次節以降では，t-KPS に対して，従来要求している制約条件，その制約条件下における記憶容量の理論的限界，及び理論的限界を達成する t-KPS の構成法について述べる．

3.3　t-KPS に要求する制約条件の定義

本節では，前節で述べた t-KPS において，従来要求している制約条件の定義を行う．

定義 3.2 [4, 18]
t-KPS への攻撃が，仮定 3.1 を満たすとする．$m_D < n_D$，$m_P + t \leq n_P$ を満たす非負整数 m_D，m_P，t に対し，以下の制約条件 (C1), (C2) を満たす t-KPS を (m_D, m_P, t) KPS という．

(C1：完全整合性) 任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ における，任意の $\mathrm{P}_i \in \mathcal{A}_j$ に対し，

$$H(K_j \mid U_i) = 0 \tag{3.7}$$

が成立する．

(C2：しきい値型安全性) $|\mathcal{X}| \leq m_D$，$|\mathcal{Y}| \leq m_P$，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ と結託ユーザ $\mathcal{Y} \subset \mathcal{P}$，及び任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ に対して，

$$H(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) = H(K_j) \tag{3.8}$$

が成立する． □

制約条件 (C1) は，任意のグループに属するユーザは必ず鍵を共有できることを要求し，制約条件 (C2) は，しきい値 m_D, m_P 以下の結託センター及び結託ユーザに対しては，攻撃対象となる鍵の情報が全く得られないことを要求している．本研究では，前者の性質を完全整合性，後者の性質をしきい値型安全性と呼ぶ．

3.4　(m_D, m_P, t) KPS における記憶容量の理論的限界

(m_D, m_P, t) KPS に対して，各ユーザと各センターの記憶容量，すなわち，$H(U_i), 1 \leq i \leq n_P$ と $H(V_k), 1 \leq k \leq n_D$ の理論的限界が示されている．また，各記憶容量の理論的限界を導出するために，グループの鍵のエントロピーに関して以下のような仮定を設ける．

仮定 3.2 任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ の鍵 k_j に対して，

$$H(K_j) = H(K) \tag{3.9}$$

が成立する．ここで，K は $\mathcal{K}$ の中に値をとる確率変数とした． □

この仮定のもとで，(m_D, m_P, t) KPS における各ユーザ，及び各センターの記憶容量 $H(U_i), 1 \leq i \leq n_P$, $H(V_k), 1 \leq k \leq n_D$ の理論的限界は，次の定理として与えられる．

定理 3.1 [4, 18]
仮定 3.2 を満たす任意の (m_D, m_P, t) KPS において，

$$H(U_i) \geq \binom{m_P + t - 1}{t - 1} H(K), \quad 1 \leq i \leq n_P, \tag{3.10}$$

$$H(V_k) \geq \binom{m_P + t}{t} H(K), \ 1 \leq k \leq n_D \tag{3.11}$$

が成立する． □

次節では，定理 3.1 の理論的限界を達成する，最適な (m_D, m_P, t) KPS の構成法について述べる．

3.5　最適な (m_D, m_P, t) KPS の構成法

本節では，定理 3.1 で示した各ユーザと各センターの記憶容量の理論的限界を達成する最適な (m_D, m_P, t) KPS の構成法 [18] について述べる．また，本研究では簡単のため，この構成法を (m_D, m_P, t) 構成法と呼ぶことにする．

3.5.1　準備

(m_D, m_P, t) 構成法では，以下のように定義される対称多項式の性質を利用する．

定義 3.3 ここで，q を素数のべき乗とおく．任意の $t \geq 2$ と任意の $m > 0$ に対して，有限体 $\mathbb{F}_q$ 上で定義される t 変数 m 次多項式を

$$P\left(x_1, x_2, \cdots, x_t\right) = \sum_{0 \leq r_1, r_2 \cdots, r_t \leq m} a_{r_1 r_2 \cdots r_t} \left(x_1\right)^{r_1} \left(x_2\right)^{r_2} \cdots \left(x_t\right)^{r_t} \tag{3.12}$$

とおく．このとき，任意の置換 $\sigma : \{1, 2, \cdots, t\} \to \{1, 2, \cdots, t\}$ に対し，

$$P\left(x_1, \cdots, x_t\right) = P\left(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(t)}\right) \tag{3.13}$$

を満たす多項式 $P\left(x_1, x_2, \cdots, x_t\right)$ を対称多項式という．　□

$P\left(x_1, \cdots, x_t\right)$ が対称多項式であれば，任意の置換 σ に対して，

$$a_{r_1 r_2 \cdots r_t} = a_{r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(t)}},\ 0 \leq r_1, \cdots, r_t \leq m \tag{3.14}$$

が成り立つ．したがって，$\binom{m+t}{t}$ 個の $\mathbb{F}_q$ 上の元から，t 変数 m 次対称多項式が一意に定まる [4].

(m_D, m_P, t) 構成法では，定義 3.3 の対称多項式の性質を含んだ次のような n_D 個の $\mathbb{F}_q$ 上の $t+1$ 変数多項式を用いる．

$$P_k\left(x_0, x_1, \cdots, x_t\right) = \sum_{\substack{0 \leq r_0 \leq m_D, \\ 0 \leq r_1, \cdots, r_t \leq m_P}} a^{(k)}_{r_0 \cdots r_t} \left(x_0\right)^{r_0} \left(x_1\right)^{r_1} \cdots \left(x_t\right)^{r_t},\ 1 \leq k \leq n_D. \tag{3.15}$$

ただし，$\mathbb{F}_q$ 上の任意の元 b，及び任意の置換 $\sigma : \{1, 2, \cdots, t\} \to \{1, 2, \cdots, t\}$ に対し，

$$P_k\left(b, x_1, \cdots, x_t\right) = P_k\left(b, x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(t)}\right),\ 1 \leq k \leq n_D \tag{3.16}$$

を満たす．よって，$\mathbb{F}_q$ 上の任意の元 b，及び任意の置換 σ に対して，

$$a^{(k)}_{r_0 r_1 r_2 \cdots r_t} = a^{(k)}_{r_0 r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(t)}},\ 0 \leq r_0 \leq m_D,\ 1 \leq k \leq n_D \tag{3.17}$$

が成り立つので，$(m_D + 1)\binom{m_P+t}{t}$ 個の $\mathbb{F}_q$ 上の元から (3.15) の各多項式が一意に定まる．また，$\mathbb{F}_q$ 上の任意の元 b に対し，

$$P_k\left(b, x_1, \cdots, x_t\right) = \sum_{\substack{0 \leq r_0 \leq m_D, \\ 0 \leq r_1, \cdots, r_t \leq m_P}} a^{(k)}_{r_1 \cdots r_t} \left(b\right)^{r_0} \left(x_1\right)^{r_1} \cdots \left(x_t\right)^{r_t},\ 1 \leq k \leq n_D \tag{3.18}$$

は，それぞれ t 変数 m_P 次対称多項式となる．すなわち，任意の $1 \leq k \leq n_D$ と任意の置換 σ に対して，

$$\sum_{0 \leq r_0 \leq m_D} a^{(k)}_{r_0 r_1 r_2 \cdots r_t} (b)^{r_0} = \sum_{0 \leq r_0 \leq m_D} a^{(k)}_{r_0 r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(t)}} (b)^{r_0}, 1 \leq r_1, \cdots, r_t \leq m_P \quad (3.19)$$

が成り立つので，$\binom{m_P+t}{t}$ 個の $\mathbb{F}_q$ 上の元から (3.18) の各多項式が一意に定まる．同様に，$\mathbb{F}_q$ 上の任意の元 b_0, b_1 と任意の $1 \leq k \leq n_D$ に対して，

$$P_k (b_0, b_1, x_2 \cdots, x_t) = \sum_{\substack{0 \leq r_0 \leq m_D, \\ 0 \leq r_1, \cdots, r_t \leq m_P}} a^{(k)}_{r_1 \cdots r_t} (b_0)^{r_0} (b_1)^{r_1} \cdots (x_t)^{r_t} \quad (3.20)$$

は，$t-1$ 変数 m_P 次対称多項式となるので，$\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元から (3.20) の各多項式が一意に定まる．

3.5.2　(m_D, m_P, t) 構成法

$\mathbb{F}_q$ 上の (m_D, m_P, t) 構成法 [18] では，$L = m_D + 1$ とし，t-KPS の公開情報である各集合，及び確率関数を次のようにおく．

$$\mathcal{P} = \mathcal{D} = \mathbb{F}_q \backslash \{0\}, \quad (3.21)$$

$$\mathcal{K} = \mathbb{F}_q, \quad (3.22)$$

$$\mathcal{S} = \mathbb{F}_q^{(m_D+1)\binom{m_P+t}{t}}, \quad (3.23)$$

$$\mathcal{V} = \mathbb{F}_q^{\binom{m_P+t}{t}}, \quad (3.24)$$

$$\mathcal{U} = \mathbb{F}_q^{\binom{m_P+t-1}{t-1}}, \quad (3.25)$$

$$p_S(s) = q^{-(m_D+1)\binom{m_P+t}{t}}, \ s \in \mathcal{S}. \quad (3.26)$$

ここで，任意の自然数 n に対し，$\mathbb{F}_q^n$ を集合 $\mathbb{F}_q$ に対する n 個の直積集合とした．更に，各センターの ID 情報は，$k \neq k'$ となる任意の $1 \leq k, k' \leq n_D$ に対し，$\mathrm{D}_k \neq \mathrm{D}_{k'}$ を満たす．同様に，各ユーザの ID 情報は，$i \neq i'$ となる任意の $1 \leq i, i' \leq n_P$ に対し，$\mathrm{P}_i \neq \mathrm{P}_{i'}$ を満たす．

また，t-KPS で用いる各関数は，それぞれ次のような計算を行う．

- $v_{k,k'} = f_T\left(s_k, \mathrm{D}_{k'}\right)$, $1 \leq k, k' \leq n_D$ の計算：
  秘密情報 s_k から (3.15) と同様の性質を持つ $t+1$ 変数多項式 $P_k\left(x_0, x_1, \cdots, x_t\right)$ を定め，$x_0 = \mathrm{D}_{k'}$ とした

$$P_k\left(\mathrm{D}_{k'}, x_1, \cdots, x_t\right) = \sum_{\substack{0 \leq r_0 \leq m_D, \\ 0 \leq r_1, \cdots, r_t \leq m_P}} a^{(k)}_{r_1 \cdots r_t} \left(\mathrm{D}_{k'}\right)^{r_0} \left(x_1\right)^{r_1} \cdots \left(x_t\right)^{r_t} \tag{3.27}$$

  を計算する．この多項式は，(3.18) と同様に t 変数 m_P 次対称多項式となるので，対応する $\binom{m_P+t}{t}$ 個の $\mathbb{F}_q$ 上の元を $\binom{m_P+t}{t}$ 次元のベクトル集合 $\mathcal{V}$ の元 $v_{k,k'}$ とおく．

- $v_k = f_M\left(v_{1,k}, v_{2,k}, \cdots, v_{n_D,k}\right)$, $1 \leq k \leq n_D$ の計算：

$$v_k = \sum_{k'=1}^{n_D} v_{k',k} \in \mathcal{V}. \tag{3.28}$$

  このとき，v_k は以下で定義される t 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, x_1, \cdots, x_t\right)$ と 1 対 1 対応する．

$$Q\left(\mathrm{D}_k, x_1, \cdots, x_t\right) = \sum_{k'=1}^{n_D} P_{k'}\left(\mathrm{D}_k, x_1, \cdots, x_t\right). \tag{3.29}$$

- $u_{i_j,i} = F_T\left(v_{i_j}, \mathrm{P}_i\right)$, $1 \leq i \leq n_P$, $1 \leq j \leq m_D + 1$ の計算：
  $\binom{m_P+t}{t}$ 次元のベクトル集合 $\mathcal{V}$ の元 v_{i_j} から，(3.29) で定義した t 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, x_1, \cdots, x_t\right)$ を定め，$x_1 = \mathrm{P}_i$ とした

$$Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) = \sum_{k=1}^{n_D} \sum_{\substack{0 \leq r_0 \leq m_D, \\ 0 \leq r_1, \cdots, r_t \leq m_P}} a^{(k)}_{r_1 \cdots r_t} \left(\mathrm{D}_{i_j}\right)^{r_0} \left(\mathrm{P}_i\right)^{r_1} \left(x_2\right)^{r_2} \cdots \left(x_t\right)^{r_t} \tag{3.30}$$

  を計算する．この多項式は $t-1$ 変数 m_P 次対称多項式となるので，対応する $\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元を $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 $u_{i_j,i}$ とおく．

- $u_i = g_M\left(u_{i_1,i}, u_{i_2,i}, \cdots, u_{i_{m_D+1},i}\right)$, $1 \leq i \leq n_P$ の計算：
  $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 $u_{i_j,i}, 1 \leq j \leq m_D+1$ から，m_P 次 $t-1$ 変数対称多項式 $Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right)$ をそれぞれ定め，ラグランジュ補間を用いて以下の計算を行う．

$$\begin{aligned}
\sum_{j=1}^{m_D+1} \lambda_{i_j} Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) &= \sum_{j=1}^{m_D+1} \lambda_{i_j} \sum_{k=1}^{n_D} P_k\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\
&= \sum_{k=1}^{n_D} \sum_{j=1}^{m_D+1} \lambda_{i_j} P_k\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\
&= \sum_{k=1}^{n_D} P_k\left(0, \mathrm{P}_i, x_2, \cdots, x_t\right) \\
&= Q\left(0, \mathrm{P}_i, x_2, \cdots, x_t\right). \qquad (3.31)
\end{aligned}$$

  ここで，

$$\lambda_{i_j} = \prod_{k=1:k\neq j}^{m_D+1} \frac{-\mathrm{D}_{i_k}}{\mathrm{D}_{i_j} - \mathrm{D}_{i_k}} \qquad (3.32)$$

  とした．この多項式 $Q\left(0, \mathrm{P}_i, x_2, \cdots, x_t\right)$ は，m_P 次 $t-1$ 変数対称多項式となるので，対応する $\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元を $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 u_i とおく．

- $k_j = g_K\left(u_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right), 1 \leq i \leq t, \mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\} \in \mathcal{A}(\mathcal{P}, t)$ の計算：
  $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 u_{j_i} から，m_P 次 $t-1$ 変数対称多項式 $Q\left(0, \mathrm{P}_{j_i}, x_2, \cdots, x_t\right)$ を定め，以下の計算を行い鍵 k_j を生成する．

$$k_j = Q\left(0, \mathrm{P}_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right). \qquad (3.33)$$

この (m_D, m_P, t) 構成法に対して，以下の定理が与えられている．

定理 3.2 *[18]*

(m_D, m_P, t) 構成法は，定義 3.2 の (m_D, m_P, t)-KPS を実現し，ユーザ及びセンターの記憶容量の記憶容量が定理 3.1 の理論的限界をそれぞれ達成する．　□

3.6　従来研究の課題

本節では，これまでに述べた t-KPS に関する従来研究の課題点について述べる．

3.6.1　センター間の総通信量削減

本章で定義した t-KPS は，全てのセンターが秘密情報を生成し，他の全てのセンターにセンター間通信情報を送信している．したがって，センター間の通信は合計で $n_D\,(n_D-1)$ 回の通信を行うことになり，センターの総数 n_D が大きい場合はセンター間の総通信量が膨大になってしまう．また，通信で用いる安全な通信路は，インターネット回線のような公開通信路とは違い高価な通信路となるため，利用するためには非常に大きなコストがかかってしまう．したがって，センター間の通信量の増大は，非常に重大な問題となる．

3.6.2　しきい値ランプ型安全性の適用

本章で述べたように，t-KPS に要求する従来の制約条件は，完全整合性としきい値型安全性に対する制約条件となっている．t-KPS は，2.4 節で述べた秘密分散法と同様に，複数の利用者が結託して不正を行うといった攻撃を仮定しているので，しきい値ランプ型安全性を適用することも考えられる．

定義 3.2 の制約条件 (C2) より，しきい値型安全性はセンターとユーザの結託数がそれぞれしきい値 m_D, m_P 以下であるとき，攻撃者は攻撃対象に関する情報が全く得られないという性質となるが，しきい値を超える結託数の場合は，何の安全性も保証しない．一方，しきい値ランプ型安全性では，結託数があるしきい値以下であるとき，攻撃者は攻撃対象に関する情報が全く得られず，しきい値を超えると結託数の増加に伴い攻撃対象の情報が段階的に得られていくという性質をもった安全性となる．しきい値ランプ型安全性は，しきい値型安全性を拡張した安全性で，しきい値ランプ型安全性を持つ暗号方式を用いることで，安全性は弱くなるが記憶容量の削減ができる．また，利用者が保有するメモリ等のリソースに制限が設けられている場合に，リソースの有効な活用が可能となり，柔軟な暗号方式の設計ができる．

これまでに，しきい値ランプ型安全性を満たす t-KPS は定義されていなかったが，この安全性を導入することで上記のようなメリットが期待できる．

第4章　しきい値型安全性を満たすセンター間通信量削減型t会議事前配布方式(t-KPS')

定義 3.1 で定義した t-KPS は，全てのセンターが秘密情報を生成し，他の全てのセンターにセンター間通信情報を送信しているため，センター間の通信量が膨大になってしまうという問題がある．本章では，まずセンターの総通信量を削減するために，従来の t-KPS を拡張したセンター間通信量削減型 t 会議鍵事前配布方式 (以下では，簡単のため t-KPS' と呼ぶ) を提案する．この新たな t-KPS' に要求する制約条件として，従来と同様に完全整合性としきい値型安全性に対する制約条件を定義し，この制約条件を満たす t-KPS' における記憶容量の理論的限界の導出，及びその理論的限界を達成する構成法の提案を行う．

4.1　定義

4.1.1　t-KPS' の定義

$n_S \leq n_D$ に対して，秘密情報を生成するセンターの ID 情報全体の集合を $\mathcal{D}_S = \{\mathrm{D}_1, \mathrm{D}_2, \cdots, \mathrm{D}_{n_S}\} \subseteq \mathcal{D}$ とおく．また，t-KPS' を定義するために，3.1 節で定義した集合及び関数と同様の記法を用いる．ただし，センター記憶情報生成関数 f_M の定義域を $\mathcal{V}^{n_S}$ に変更する．

次に，t-KPS' を定義する．

定義 4.1 定義 3.1 で定義した t-KPS における公開情報に加え，集合 $\mathcal{D}_S$ を公開する．t-KPS' は，定義 3.1 の t-KPS における *Step1* から *Step3* を以下のように変更した鍵事前配布方式である．

＜*Step1*： 秘密情報の生成＞

各センター $\mathrm{D}_k, 1 \leq k \leq n_S$ は，それぞれ独立に秘密情報 $s_k \in \mathcal{S}$ を確率分布 p_S にしたがって生成する．

＜*Step2:* センター間の通信＞

$1 \leq k \leq n_S$, $1 \leq k' \leq n_D$ に対して，センター D_k は関数 f_T を用いて，センター $\mathrm{D}_{k'}$ に対するセンター間通信情報 $v_{k,k'} = f_T\left(s_k, \mathrm{D}_{k'}\right)$ を生成し，安全な通信路を用いて送信する．

＜*Step3:* センター記憶情報の計算・記憶＞

$1 \leq k \leq n_D$ に対して，センター D_k は関数 f_M を用いて，センター D_k に対するセンター記憶情報 $v_k = f_M\left(v_{1,k}, v_{2,k}, \cdots, v_{n_S,k}\right)$ を生成・記憶する． □

ここで定義した t-KPS' において，$\mathcal{D}_S = \mathcal{D}$，すなわち $n_S = n_D$ のとき t-KPS と等価になることが容易に確かめられる．したがって，本研究で新たに定義した t-KPS' は，従来の t-KPS を含む一般的な鍵事前配布方式となる．

4.1.2　t-KPS' の評価基準と要求する制約条件の定義

ここで，t-KPS' への攻撃に，次のような仮定を設ける．

仮定 4.1 t-KPS' への攻撃は，仮定 3.1 の条件のうち，利用可能情報を次のように変更した条件を満たす．

利用可能情報： 攻撃者が t-KPS' において正規に得ることができる全ての情報．すなわち，

$$U\left(\mathcal{Y}\right) = \left(U_{\mathcal{D}_{i_1},i_1}, U_{\mathcal{D}_{i_2},i_2}, \cdots, U_{\mathcal{D}_{i_{|\mathcal{Y}|}},i_{|\mathcal{Y}|}}\right),$$

$$V(\mathcal{X}) = \Big(V_{k'_1,k_1}, V_{k'_1,k_2}, \cdots, V_{k'_1,k_{|\mathcal{X}|}}, V_{k'_2,k_1}, V_{k'_2,k_2}, \cdots, V_{k'_2,k_{|\mathcal{X}|}}, \cdots, V_{k'_{|\mathcal{D}_S\setminus\mathcal{X}|},k_1}, \cdots V_{k'_{|\mathcal{D}_S\setminus\mathcal{X}|},k_{|\mathcal{X}|}}\Big),$$

$$S(\mathcal{X}) = \left(S_{k''_1}, S_{k''_2}, \cdots, S_{k''_{|\mathcal{X}\cap\mathcal{D}_S|}}\right).$$

ここで,

$$\mathcal{D}_S\setminus\mathcal{X} = \{\mathrm{D} \mid \mathrm{D}\in\mathcal{D}_S, \mathrm{D}\notin\mathcal{X}\} = \left\{\mathrm{D}_{k'_1}, \mathrm{D}_{k'_2}, \cdots, \mathrm{D}_{k'_{|\mathcal{D}_S\setminus\mathcal{X}|}}\right\},$$

$$\mathcal{X}\cap\mathcal{D}_S = \{\mathrm{D} \mid \mathrm{D}\in\mathcal{D}_S, \mathrm{D}\in\mathcal{X}\} = \left\{\mathrm{D}_{k''_1}, \mathrm{D}_{k''_2}, \cdots, \mathrm{D}_{k''_{|\mathcal{X}\cap\mathcal{D}_S|}}\right\}$$

とおいた.

ここで，確率変数 $U(\mathcal{Y})$, $V(\mathcal{X})$, $S(\mathcal{X})$ は，それぞれ $\mathcal{U}$, $\mathcal{V}$, $\mathcal{S}$ の直積集合 $\mathcal{U}(\mathcal{Y}) = \mathcal{U}^{L\cdot|\mathcal{Y}|}$, $\mathcal{V}(\mathcal{X}) = \mathcal{V}^{|\mathcal{X}|\cdot|\mathcal{D}_S\setminus\mathcal{X}|}$, $\mathcal{S}(\mathcal{X}) = \mathcal{S}^{|\mathcal{X}\cap\mathcal{D}_S|}$ に値をとる．

t-KPS' に対する安全性，機能性，効率性の評価基準は，全て従来の t-KPS と同様の評価基準を用いる．すなわち，(3.3)〜(3.6) をそれぞれの評価基準として用いる．

次に，t-KPS' に要求する制約条件の定義を行う．ここでは，従来と同様に完全整合性としきい値型安全性に対する制約条件を定義する．t-KPS' がしきい値型安全性を満たすなら，任意のしきい値 m_D, m_P に対して，任意の m_P 人以下の結託ユーザと m_D 個以下の結託センターが攻撃しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られないことを保証する．また，攻撃対象の鍵を共有するグループに，結託ユーザは 1 人も属さないことになるので，結託ユーザは最大で $n_P - t$ 人まで考えられる．したがって，しきい値型安全性を満たす t-KPS' は，$m_P \le n_P - t$ を満たす必要がある．

定義 4.2 t-KPS'への攻撃が，仮定 4.1 を満たすとする．$m_D < n_D$，$m_P \le n_P - t$ を満たす非負整数 m_D，m_P，t に対し，定義 3.2 と同様の制約条件 (C1), (C2) を満たす t-KPS'を (m_D, m_P, t) KPS'という． □

4.2　(m_D, m_P, t) KPS' における記憶容量の理論的限界

本節では，定義 4.2 で定義した (m_D, m_P, t) KPS' に対して，各ユーザと各センターの記憶容量，すなわち，$H(U_i), 1 \leq i \leq n_P$ と $H(V_k), 1 \leq k \leq n_D$ の理論的限界を導出する．

4.2.1　準備

センターとユーザの記憶容量の理論的限界を導出するために，以下の補題を用いる．

補題 4.1 $N \geq 2$ を満たす，任意の $N+1$ 個の確率変数 $X_1, X_2, \cdots, X_N, Y$ に対して，確率変数の列 $X_1, X_2, \cdots, X_N$ がマルコフ連鎖をなす，すなわち，

$$X_1 \to X_2 \to \cdots \to X_N \tag{4.1}$$

ならば，

$$H(X_1 \mid X_2) \leq H(X_1 \mid X_N), \tag{4.2}$$

$$H(X_1 \mid X_2, Y) \leq H(X_1 \mid X_N, Y) \tag{4.3}$$

が成立する．□

（**証明**）エントロピー及び相互情報量の基本的性質を用いることで，この補題を証明する．相互情報量のチェイン則より，

$$I\left(X_1; X_2^N\right) \geq I(X_1; X_N) \tag{4.4}$$

が成り立つ．また，$X_1, X_2, \cdots, X_N$ がマルコフ連鎖をなしているので，定理 2.7 より，

$$I\left(X_1; X_2^N\right) = I(X_1; X_2) \tag{4.5}$$

したがって，(4.4) と (4.5) より，

$$I(X_1; X_2) \geq I(X_1; X_N) \tag{4.6}$$

が成り立ち，相互情報量の定義より (4.6) は，

$$H(X_1) - H(X_1 \mid X_2) \;\geq\; H(X_1) - H(X_1 \mid X_N) \tag{4.7}$$

となり，

$$H(X_1 \mid X_2) \;\leq\; H(X_1 \mid X_N) \tag{4.8}$$

が得られる．

同様にして，

$$H(X_1 \mid X_2, Y) \;\leq\; H(X_1 \mid X_N, Y) \tag{4.9}$$

も証明できる． □

補題 4.2 $\eta_{\mathcal{Y}}$ を $\mathcal{Y} \cap \mathcal{A} \neq \emptyset$ となる集合 $\mathcal{A} \in \mathcal{A}(\mathcal{P}, t)$ の総数とする．任意の (m_D, m_P, t) KPS' において，$|\mathcal{X}| \leq m_D$, $|\mathcal{Y}| \leq m_P$，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset$，$\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta_{\mathcal{Y}}$ を満たす任意の結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$, 及び任意のグループ $\mathcal{A}^*, \mathcal{A}^*_{j_i}$ に対し，

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right) = H(K^*),\ \eta' \leq \eta_{\mathcal{Y}} \tag{4.10}$$

が成立する．ここで，K^* および $K^*_{j_i}, 1 \leq i \leq \eta_{\mathcal{Y}}$ を，それぞれグループ $\mathcal{A}^* \in \mathcal{A}(\mathcal{P}, t)$ 及び $\mathcal{A}^*_{j_i} \in \mathcal{A}(\mathcal{P}, t), 1 \leq i \leq \eta_{\mathcal{Y}}$ の鍵に対応する確率変数とした． □

（**証明**）この補題は，補題 4.1 を用いることで証明される．

制約条件 (C2) より，任意の (m_D, m_P, t) KPS' に対して，

$$H(K^* \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) = H(K^*) \tag{4.11}$$

が成り立つ．また，$\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta_{\mathcal{Y}}$ であること，及び t-KPS' の定義 (定義 4.1) より，確率変数 $\left(U_{i_1}, U_{i_2}, \cdots, U_{i_{|\mathcal{Y}|}}\right), \left(K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta_{\mathcal{Y}}}}\right)$ は，適当な関数 φ_2, φ_3 を用いて，

$$\left(U_{i_1}, U_{i_2}, \cdots, U_{i_{|\mathcal{Y}|}}\right) \;=\; \varphi_2(U(\mathcal{Y})), \tag{4.12}$$

$$\left(K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta_{\mathcal{Y}}}}\right) \;=\; \varphi_3\left(U_{i_1}, U_{i_2}, \cdots, U_{i_{|\mathcal{Y}|}}\right) \tag{4.13}$$

と表すことができる．よって，(2.14) の関係性から，

$$K^* \to U(\mathcal{Y}) \to \left(U_{i_1}, U_{i_2}, \cdots, U_{i_{|\mathcal{Y}|}}\right) \to \left(K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}\right),\ \eta' \leq \eta_{\mathcal{Y}} \quad (4.14)$$

が成り立つ．よって，$\eta' \leq \eta_{\mathcal{Y}}$ に対して，

$$\begin{aligned} X_1 &= K^*, \\ X_2 &= U(\mathcal{Y}), \\ X_3 &= \left(U_{i_1}, U_{i_2}, \cdots, U_{i_{|\mathcal{Y}|}}\right), \\ X_4 &= \left(K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}\right), \\ Y &= (V(\mathcal{X}), S(\mathcal{X})) \end{aligned} \quad (4.15)$$

とおくと補題 4.1 がそれぞれ適用でき，

$$\begin{aligned} H(K^*) &\geq H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right) \\ &\geq H(K^* \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})),\ \eta' \leq \eta_{\mathcal{Y}} \end{aligned} \quad (4.16)$$

が成り立つ．ここで，1 番目の不等号は相互情報量の非負性（定理 2.5）を用いた．

したがって，(4.11) と (4.16) より，

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right) = H(K^*),\ \eta' \leq \eta_{\mathcal{Y}} \quad (4.17)$$

を得る．□

補題 4.2 において，結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$ が正規の方法で共有できる全ての鍵が $k^*_{j_i}, 1 \leq i \leq \eta_{\mathcal{Y}}$ となる．したがって，(4.10) は結託ユーザが生成できる全ての鍵，及びセンターが利用できる全ての情報を用いても，結託ユーザが属さないグループの鍵 k^* に関する情報は全く得られないことを意味する．

4.2.2　ユーザの記憶容量の理論的限界

(m_D, m_P, t) KPS' におけるユーザの記憶容量 $H(U_i), 1 \leq i \leq n_P$ の理論的限界は，次の定理として与えられる．

定理 4.1 仮定 3.2 を満たす任意の (m_D, m_P, t) KPS'において，

$$H(U_i) \geq \binom{m_P + t - 1}{t - 1} H(K), \quad 1 \leq i \leq n_P \tag{4.18}$$

が成立する．□

（**証明**）定理 4.1 は，文献 [4] の Theorem 3.2 の証明と同様にして導かれる．

任意のユーザ P_i に対し，$\mathrm{P}_i \notin \mathcal{I}^{(i)}$, $\left|\mathcal{I}^{(i)}\right| = m_P + t - 1$ を満たす任意の集合 $\mathcal{I}^{(i)} \subset \mathcal{P}$ を定める．この $\mathcal{I}^{(i)}$ に対して，

$$\mathcal{M}\left(\mathcal{I}^{(i)}\right) = \left\{\mathcal{A}' \cup \{\mathrm{P}_i\} \mid \mathcal{A}' \subset \mathcal{I}^{(i)}, |\mathcal{A}'| = t - 1\right\} \tag{4.19}$$

とし，$\mathcal{M}\left(\mathcal{I}^{(i)}\right)$ 内のグループ $\mathcal{A}_j$ のインデックス j を

$$\mathcal{M}\left(\mathcal{I}^{(i)}\right) = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\rho(m_P,t)}\right\} \tag{4.20}$$

としてインデックスを付け直す．ここで，

$$\rho(m_P, t) = \binom{m_P + t - 1}{t - 1} \tag{4.21}$$

とした．以後，(4.20) のように新たに付け直したインデックスを用いることとし，鍵 K_j についても同様のインデックスを用いる．よって，ユーザ P_i の記憶容量 $H(U_i)$ に関して，

$$\begin{aligned}
H(U_i) &= H\left(K_1^{\rho(m_P,t)}\right) - H\left(K_1^{\rho(m_P,t)} \mid U_i\right) + H\left(U_i \mid K_1^{\rho(m_P,t)}\right) \\
&\geq H\left(K_1^{\rho(m_P,t)}\right) - \sum_{j=1}^{\rho(m_P,t)} H(K_j \mid U_i) \\
&= H\left(K_1^{\rho(m_P,t)}\right) \\
&= \sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}\right)
\end{aligned} \tag{4.22}$$

が成立する．ここで，1 番目の等号は相互情報量の対称性 (定理 2.3)，1 番目の不等号はエントロピー，及び相互情報量の非負性 (定理 2.1，定理 2.5) とエントロピー

のチェイン則 (定理 2.2)，2 番目の等号は制約条件 (C1)，3 番目の等号はエントロピーのチェイン則 (定理 2.2) を用いた．また，相互情報量の非負性 (定理 2.5) により，$|\mathcal{X}| \leq m_D$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ に対して，

$$\sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}\right) \geq \sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \tag{4.23}$$

が成り立つ．よって，(4.22) と (4.23) より，

$$H\left(U_i\right) \geq \sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \tag{4.24}$$

を得る．

次に，(4.24) の各項に対し，

$$\mathcal{A}^* = \mathcal{A}_j, \quad \mathcal{Y} = \mathcal{I}^{(i)} \backslash \mathcal{A}_j,$$
$$\left\{\mathcal{A}_{j_1}^*, \mathcal{A}_{j_2}^*, \cdots, \mathcal{A}_{j_{\eta'}}^*\right\} = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{j-1}\right\},\ 1 \leq j \leq \rho^{(m_P,t)},$$

とおくと，$\mathrm{P}_i \notin \mathcal{I}^{(i)}$ かつ $\mathrm{P}_i \in \mathcal{A}_j$ なので，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset$, $\mathcal{Y} \cap \mathcal{A}_{j_i}^* \neq \emptyset, 1 \leq i \leq \eta'$, $|\mathcal{Y}| = m_P$ が成り立つ．したがって，$|\mathcal{X}| \leq m_D$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ に対して，各項で補題 4.2 がそれぞれ適用でき，

$$\begin{aligned} \sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) &= \sum_{j=1}^{\rho(m_P,t)} H\left(K_j\right) \\ &= \rho(m_P,t) H\left(K\right) \end{aligned} \tag{4.25}$$

を得る．最後の等号は，仮定 3.2 より導かれる．したがって，(4.24) と (4.25) より，

$$H\left(U_i\right) \geq \binom{m_P + t - 1}{t - 1} H\left(K\right), \quad 1 \leq i \leq n_P, \tag{4.26}$$

が成立し，(4.18) を得る． □

4.2.3　センターの記憶容量の理論的限界

(m_D, m_P, t) KPS' におけるセンターの記憶容量 $H\left(V_k\right), 1 \leq k \leq n_D$ の理論的限界は，次の定理として与えられる．

定理 4.2 仮定 3.2 を満たす任意の (m_D, m_P, t) KPS'において，

$$H(V_k) \geq \binom{m_P + t}{t} H(K),\ 1 \leq k \leq n_D \tag{4.27}$$

が成立する．□

（**証明**）定理 4.2 は，定理 4.1 の証明と同様にして導かれる．

まず，$|\mathcal{J}| = m_P + t$ を満たす任意の集合 $\mathcal{J} \subset \mathcal{P}$ を定める．この $\mathcal{J}$ に対して，

$$\mathcal{N}(\mathcal{J}) = \{\mathcal{A} \mid \mathcal{A} \subset \mathcal{J}, |\mathcal{A}| = t\} \tag{4.28}$$

とし，$\mathcal{N}(\mathcal{J})$ 内のグループ $\mathcal{A}_j$ のインデックス j を

$$\mathcal{N}(\mathcal{J}) = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\varrho(m_P,t)}\right\} \tag{4.29}$$

としてインデックスを付け直す．ここで，

$$\varrho(m_P, t) = \binom{m_P + t}{t} \tag{4.30}$$

とした．以後，(4.29) のように新たに付け直したインデックスを用いることとし，鍵 K_j についても同様のインデックスを用いる．

次に，$\mathrm{D}_k \notin \mathcal{X}^{(k)}, |\mathcal{X}^{(k)}| = m_D$ を満たす任意の結託センター

$$\mathcal{X}^{(k)} = \left\{\mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{m_D}}\right\} \subset \mathcal{D} \tag{4.31}$$

定めると，センター D_k に必要な記憶容量 $H(V_k)$ に関して，

$$\begin{aligned}
H(V_k) &\geq H\left(V_k \mid V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right) \\
&= H\left(K_1^{\varrho(m_P,t)} \mid V_{k_1}, \cdots, V_{k_{m_D}}\right) - H\left(K_1^{\varrho(m_P,t)} \mid V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right) \\
&\qquad + H\left(V_k \mid K_1^{\varrho(m_P,t)}, V_{k_1}, \cdots, V_{k_{m_D}}\right) \\
&\geq H\left(K_1^{\varrho(m_P,t)} \mid V_{k_1}, \cdots, V_{k_{m_D}}\right) - H\left(K_1^{\varrho(m_P,t)} \mid V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right) \\
&\geq H\left(K_1^{\varrho(m_P,t)} \mid V_{k_1}, \cdots, V_{k_{m_D}}\right) - \sum_{j=1}^{\varrho(m_P,t)} H\left(K_j \mid V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right)
\end{aligned} \tag{4.32}$$

が成立する．ここで，1 番目の不等号は相互情報量の非負性 (定理 2.5)，1 番目の等号は相互情報量の対称性 (定理 2.3)，2 番目の不等号はエントロピーの非負性 (定理 2.1)，3 番目の不等号はエントロピーのチェイン則 (定理 2.2) 及び相互情報量の非負性 (定理 2.5) を用いた．

t-KPS' の定義 (定義 4.1) より，確率変数 $\left(V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right)$ は適当な関数 φ_2 を用いて，

$$\left(V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right) = \varphi_2\left(V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \tag{4.33}$$

と表すことができるので，(2.14) の関係性から，

$$K_1^{\varrho(m_P,t)} \to \left(V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \to \left(V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right) \tag{4.34}$$

が成り立つ．したがって，

$$\begin{aligned} X_1 &= K_1^{\varrho(m_P,t)}, \\ X_2 &= \left(V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right), \\ X_3 &= \left(V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right) \end{aligned} \tag{4.35}$$

とおくことで，補題 4.1 が適用でき，

$$H\left(K_1^{\varrho(m_P,t)} \mid V_{k_1}, \cdots, V_{k_{m_D}}\right) \geq H\left(K_1^{\varrho(m_P,t)} \mid V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \tag{4.36}$$

が成立する．

同様に定義 4.1 より，任意の P_i に対し，2 つの確率変数 $\left(U_{k,i}, U_{k_1,i}, \cdots, U_{k_{m_D},i}\right)$, U_i は適当な関数 φ_2, φ_3 を用いて，それぞれ，

$$\left(U_{k,i}, U_{k_1,i}, U_{k_2,i}, \cdots, U_{k_{m_D},i}\right) = \varphi_2\left(V_k, V_{k_1}, V_{k_2}, \cdots, V_{k_{m_D}}\right), \tag{4.37}$$

$$U_i = \varphi_3\left(U_{k,i}, U_{k_1,i}, U_{k_2,i}, \cdots, U_{k_{m_D},i}\right) \tag{4.38}$$

と表すことができる．よって，(2.14) の関係性から，$1 \leq j \leq \varrho(m_P, t)$ に対し，

$$K_j \to \left(V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right) \to \left(U_{k,i}, U_{k_1,i}, \cdots, U_{k_{m_D},i}\right) \to U_i \tag{4.39}$$

が成り立つ．したがって，$1 \leq j \leq \varrho(m_P, t)$ に対して，

$$\begin{aligned} X_1 &= K_j, \\ X_2 &= \left(V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right), \\ X_3 &= \left(U_{k,i}, U_{k_1,i}, \cdots, U_{k_{m_D},i}\right), \\ X_4 &= U_i \end{aligned} \tag{4.40}$$

とおくことで，補題 4.1 が適用でき，

$$H\left(K_j \mid V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right) \leq H\left(K_j \mid U_i\right),\ 1 \leq j \leq \varrho(m_P, t) \tag{4.41}$$

が成立する．また，$\mathcal{A}_j$, $1 \leq j \leq \varrho(m_P, t)$ に属している任意のユーザ $\mathrm{P}_{j_i} \in \mathcal{A}_j$ は，ユーザ記憶情報 U_{j_i} から正しい $\mathcal{A}_j$ の鍵 K_j を生成できるので，

$$H\left(K_j \mid U_{j_i}\right) = 0,\ 1 \leq j \leq \varrho(m_P, t) \tag{4.42}$$

が成り立つので，(4.41)，(4.42)，及びエントロピーの非負性 (定理 2.1) より，

$$H\left(K_j \mid V_k, V_{k_1}, \cdots, V_{k_{m_D}}\right) = 0,\ 1 \leq j \leq \varrho(m_P, t) \tag{4.43}$$

を得る．よって，(4.32), (4.36), (4.43) より，

$$H\left(V_k\right) \geq H\left(K_1^{\varrho(m_P,t)} \mid V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right),\ 1 \leq k \leq n_D \tag{4.44}$$

を得る．

また，(4.44) の右辺はエントロピーのチェイン則 (定理 2.2) より，

$$\begin{aligned} & H\left(K_1^{\varrho(m_P,t)} \mid V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \\ &= \sum_{j=1}^{\varrho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \end{aligned} \tag{4.45}$$

となるので，(4.45) の右辺の各項に対し，

$$\begin{aligned} & \mathcal{A}^* = \mathcal{A}_j,\ \ \mathcal{X} = \mathcal{X}^{(k)},\ \ \mathcal{Y} = \mathcal{J} \backslash \mathcal{A}_j, \\ & \left\{\mathcal{A}_{j_1}^*, \mathcal{A}_{j_2}^*, \cdots, \mathcal{A}_{j_{\eta'}}^*\right\} = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{j-1}\right\},\ 1 \leq j \leq \varrho(m_P, t), \end{aligned}$$

とおくと，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset$, $\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta'$, $|\mathcal{X}| = m_D$, $|\mathcal{Y}| = m_P$ が成り立つ．したがって，各項で補題 4.2 がそれぞれ適用でき，

$$\begin{aligned} \sum_{j=1}^{\varrho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) &= \sum_{j=1}^{\varrho(m_P,t)} H\left(K_j\right) \\ &= \varrho(m_P,t) H\left(K\right) \end{aligned} \tag{4.46}$$

を得る．最後の等号は仮定 3.2 より導かれる．

したがって，(4.44)，(4.45)，(4.46) より，

$$\begin{aligned} H\left(V_k\right) &\geq \varrho(m_P,t) H\left(K\right) \\ &= \binom{m_P+t}{t} H\left(K\right),\ 1 \leq k \leq n_D \end{aligned} \tag{4.47}$$

が成立し，(4.27) を得る． □

4.3　最適な (m_D, m_P, t) KPS' の構成法

本節では，前節で導出したユーザとセンターの記憶容量の理論的限界を達成する最適な (m_D, m_P, t) KPS' の構成法を提案する．また，本研究では簡単のため，この構成法をセンター通信量削減型 (m_D, m_P, t) 構成法と呼ぶことにする．提案する構成法では，従来の構成法で用いられている (3.15) の多項式と同様の性質を持つ，n_S 個の $\mathbb{F}_q$ 上の多項式 $P_k\left(x_0, x_1, \cdots, x_t\right)$, $1 \leq k \leq n_S$ を利用する．

次に，$\mathbb{F}_q$ 上のセンター通信量削減型 (m_D, m_P, t) 構成法を示す．この構成法では，$n_S = m_D + 1$, $L = m_D + 1$ とおき，t-KPS' の公開情報である ID 情報，各集合，及び確率関数を，従来の (m_D, m_P, t) 構成法と同様とする．すなわち，(3.21)〜(3.26) とおく．また，関数 f_T, F_T, g_M, g_K の計算は，3.5.2 節で示した (m_D, m_P, t) 構成法と同様の計算を行い，

$$v_k = f_M\left(v_{1,k}, v_{2,k}, \cdots, v_{n_D,k}\right),\ 1 \leq k \leq n_D \tag{4.48}$$

は，次のように計算する．

$$v_k = \sum_{k'=1}^{m_D+1} v_{k',k} \in \mathcal{V}. \tag{4.49}$$

このとき，v_k は以下で定義される t 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, x_1, \cdots, x_t\right)$ と 1 対 1 対応する．

$$Q\left(\mathrm{D}_k, x_1, \cdots, x_t\right) = \sum_{k'=1}^{m_D+1} P_{k'}\left(\mathrm{D}_k, x_1, \cdots, x_t\right). \tag{4.50}$$

この構成法は，$n_S = n_D$ のとき (m_D, m_P, t) 構成法と等価となるので，提案したセンター通信量削減型 (m_D, m_P, t) 構成法は，(m_D, m_P, t) 構成法を含む一般的な構成法となる．また，センター通信量削減型 (m_D, m_P, t) 構成法に対して，以下の定理が成り立つ．

定理 4.3 センター通信量削減型 (m_D, m_P, t) 構成法は，定義 4.2 の (m_D, m_P, t) *KPS'* を実現し，ユーザ及びセンターの記憶容量が，それぞれ定理 4.1 及び定理 4.2 の理論的限界を達成する．□

(**証明**) まず，センター通信量削減型 (m_D, m_P, t) 構成法が，制約条件 (C1) を満たすことを示す．構成法の Step5 より，任意の t 人のグループ $\mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\}$ に対して，ユーザ $\mathrm{P}_{j_i}, 1 \leq i \leq t$ が生成する鍵は，

$$k_j = Q\left(0, \mathrm{P}_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right). \tag{4.51}$$

となる．$Q\left(0, x_1, x_2, \cdots, x_t\right)$ は m_P 次 t 変数対称多項式なので，任意の置換 σ に対し，

$$Q\left(0, x_1, \cdots, x_t\right) = P\left(0, x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(t)}\right) \tag{4.52}$$

が成り立つ．したがって，$i \neq i'$ となる任意の $1 \leq i, i' \leq t$ に対して，

$$\begin{aligned} & Q\left(0, \mathrm{P}_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right) \\ = \;& Q\left(0, \mathrm{P}_{j_{i'}}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i'-1}}, \mathrm{P}_{j_{i'+1}}, \cdots, \mathrm{P}_{j_t}\right) \end{aligned} \tag{4.53}$$

が成立するので，グループ $\mathcal{A}_j$ の各ユーザは同じ鍵 k_j を一意に生成できる．よって，センター通信量削減型 (m_D, m_P, t) 構成法は，制約条件 (C1) を満たす．

次に，センター通信量削減型 (m_D, m_P, t) 構成法が，制約条件 (C2) を満たすことを示す．ここで．結託センターを $\mathcal{X} = \{\mathrm{D}_1, \cdots, \mathrm{D}_\tau\}, \tau \leq n_D$ とすると，$m_D + 1 \leq \tau$

の場合，結託したセンターが全ての秘密情報 s_k,$1 \leq k \leq m_D + 1$ を得る．すなわち，多項式 $P_k\left(x_0, x_1, \cdots, x_t\right), 1 \leq k \leq m_D + 1$ を得ることになるので，全てのグループの鍵を不正に求めることができる．一方，$\tau \leq m_D$ の場合は，少なくとも 1 つの秘密情報 s_{m_D+1} が結託センターに対して未知となる．各秘密情報は互いに独立に生成されるので，結託センターはグループの鍵を生成するために必要な多項式，

$$Q\left(x_0, x_1, \cdots, x_t\right) = \sum_{k=1}^{m_D+1} P_k\left(x_0, x_1, \cdots, x_t\right) \tag{4.54}$$

に関する情報を全く得ることができない．よって，文献 [18] の安全性証明と上記の安全性の条件を組合わせることにより，センター通信量削減型 (m_D, m_P, t) 構成法は，制約条件 (C2) を満たす.

また，各センター，及び各ユーザの記憶容量は (m_D, m_P, t) 構成法に対する記憶容量と等しいので，センター通信量削減型 (m_D, m_P, t) 構成法も従来法と同様に，センター及びユーザの記憶容量の理論的限界を達成する最適な構成法となる．　□

4.4　比較・考察

本節では，従来の構成法である (m_D, m_P, t) 構成法と，前節で提案したセンター通信量削減型 (m_D, m_P, t) 構成法の性能について比較する．

定義 3.2 及び定義 4.2 より，(m_D, m_P, t) KPS と (m_D, m_P, t) KPS' に対する制約条件は等価となる．したがって，(m_D, m_P, t) KPS，(m_D, m_P, t) KPS' をそれぞれ実現する (m_D, m_P, t) 構成法とセンター通信量削減型 (m_D, m_P, t) 構成法の機能性及び安全性は等価であることがわかる．

定義 3.1 より，(m_D, m_P, t) KPS は，全てのセンターが秘密情報を生成し，他の全てのセンターにセンター間通信情報を送信している．したがって，センター間の通信は合計で $n_D\left(n_D - 1\right)$ 回となり，センターの総数 n_D が大きい場合はセンター間の総通信量が膨大になるという問題があった．一方，定義 4.1 より，(m_D, m_P, t) KPS' は，センター間の総通信回数が $\left(m_D + 1\right)\left(n_D - 1\right)$ 回となる．したがって，センター数 n_D が大きい場合，センター通信量削減型 (m_D, m_P, t) 構成法は，(m_D, m_P, t) 構成法と比較してセンター間の総通信量を大幅に削減できる．

また，センター，及びユーザの記憶容量の大きさは，どちらの構成法も理論的限界を達成するが，同じ大きさになる．

第5章　しきい値-しきい値ランプ型安全性を満たすt-KPS'

第3章の定義3.2や第4章の定義4.2では，完全整合性としきい値型安全性を満たす鍵事前配布方式を定義した．しきい値型安全性は，結託ユーザ及び結託センターの数が，それぞれのしきい値m_D及びm_P以下であるとき，攻撃対象である鍵に関する情報が全く得られないという性質であったが，結託ユーザ数と結託センター数のどちらかがしきい値を超えた場合は，何の安全性も保証しない．

本研究では，しきい値型安全性を2.4節で述べたようなしきい値ランプ型安全性へ拡張することを考える．t-KPS' に対して，しきい値ランプ型安全性を導入する場合，以下の3つの性質が考えられる．

- 結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られるという性質．
- 結託センター数の増加に従って情報が段階的に得られるという性質．
- 結託センター及び結託ユーザそれぞれの数の増加に従って情報が段階的に得られるという性質．

本研究では，これら全ての性質について検討する．本章では，まず結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られるという性質について検討する．この性質は，結託センターと結託ユーザを独立に考えたとき，結託センター数に対してはしきい値型安全性を満たし，結託ユーザ数に対してはしきい値ランプ型安全性を満たすので，本研究では，この性質をしきい値-しきい値ランプ型安全性と呼ぶ．

以下では，t-KPS' に要求する制約条件として，完全整合性としきい値-しきい値ランプ型安全性に対する制約条件を定義し，その制約条件を満たすもとでのt-KPS' における記憶容量の理論的限界の導出，及びその理論的限界を達成する構成法の提案を行う．また，t-KPS' の評価基準は，第4章と同様に(3.3)〜(3.6)とする．

5.1　t-KPS' に要求する制約条件の定義

t-KPS' がしきい値-しきい値ランプ型安全性を満たすなら，任意のしきい値 m_D, m_P, c_P に対して，結託数が m_P 以下の結託ユーザと m_D 以下の結託センターが攻撃しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られず，結託ユーザ数が m_P+1 から m_P+c_P かつ結託センター数が m_D 以下の場合には，結託ユーザ数が大きくなるにつれて段階的に情報が得られていく．また，攻撃対象の鍵を共有するグループに，結託ユーザは 1 人も属さないことになるので，結託ユーザ数は最大で n_P-t まで考えられる．したがって，しきい値-しきい値ランプ型安全性を満たす t-KPS' は，$m_P+c_P \leq n_P-t$ を満たす必要がある．何故なら結託ユーザ数が m_P+c_P で $m_P+c_P > n_P-t$ の場合，全てのグループの鍵がわかってしまう．これは，結託数が m_P+c_P までの結託ユーザに対して鍵の情報が完全に得られないという性質に矛盾する．したがって，条件 $m_P+c_P \leq n_P-t$ が必要となる．

定義 5.1 t-KPS'への攻撃が，仮定 4.1 を満たすとする．$m_D < n_D$，$m_P+c_P \leq n_P-t$ を満たす非負整数 m_D，m_P，c_P，t に対し，定義 3.2 と同様の制約条件 (C1)，及び以下の制約条件 (C3) を満たす t-KPS' を $(m_D, *, m_P, c_P, t)$ KPS という．

(C3：しきい値-しきい値ランプ型安全性) $|\mathcal{X}| \leq m_D$，$|\mathcal{Y}| \leq m_P+c_P$，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ と結託ユーザ $\mathcal{Y} \subset \mathcal{P}$，及び任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ に対して，

$$H(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) = \frac{c_P+1-\varphi_{m_P}(|\mathcal{Y}|)}{c_P+1} H(K_j) \tag{5.1}$$

が成立する．ここで，関数 $\varphi_{m_P} : \{0,1,\cdots,m_P+c_P\} \to \{0,1,\cdots,c_P\}$ を

$$\varphi_{m_P}(i) = \begin{cases} 0 & \text{for} \quad i \leq m_P \\ i-m_P & \text{for} \quad m_P+c_P \geq i > m_P \end{cases} \tag{5.2}$$

とした．　□

5.2　$(m_D, *, m_P, c_P, t)$ KPS における記憶容量の理論的限界

本節では，$(m_D, *, m_P, c_P, t)$ KPS における各ユーザと各センターの記憶容量，すなわち，$H(U_i), 1 \leq i \leq n_P$ と $H(V_k), 1 \leq k \leq n_D$ の理論的限界を導出する．

センターとユーザの記憶容量の理論的限界を導出するために，以下の補題を用いる．この補題は，補題 4.2 と同様にして導かれる．

補題 5.1 任意の $(m_D, *, m_P, c_P, t)$ KPS において，$|\mathcal{X}| \leq m_D$, $|\mathcal{Y}| \leq m_P + c_P$，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset$，$\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta_{\mathcal{Y}}$ を満たす任意の結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$, 及び任意のグループ $\mathcal{A}^*, \mathcal{A}^*_{j_i}$ に対し，

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right) \geq \frac{c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|)}{c_P + 1} H(K^*),\ \eta' \leq \eta_{\mathcal{Y}} \tag{5.3}$$

が成立する．□

（**証明**）制約条件 (C3) より，任意の $(m_D, *, m_P, c_P, t)$ KPS に対して，

$$H(K^* \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) = \frac{c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|)}{c_P + 1} H(K^*) \tag{5.4}$$

が成り立つ．また，補題 4.2 の証明における (4.16) の導出と同様にして，

$$H(K^*) \geq H(K^* \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})),\ \eta' \leq \eta_{\mathcal{Y}} \tag{5.5}$$

を得る．したがって，(5.4) と (5.5) より，

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right) \geq \frac{c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|)}{c_P + 1} H(K^*) \tag{5.6}$$

を得る．□

補題 5.1 において，結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$ が正規の方法で共有できる全ての鍵が $k^*_{j_i}, 1 \leq i \leq \eta_{\mathcal{Y}}$ となる．

5.2.1　ユーザの記憶容量の理論的限界

$(m_D, *, m_P, c_P, t)$ KPS におけるユーザの記憶容量 $H(U_i), 1 \leq i \leq n_P$ の理論的限界は，次の定理として与えられる．

定理 5.1 仮定 3.2 を満たす任意の $(m_D, *, m_P, c_P, t)$ KPS において，

$$H(U_i) \geq \sum_{\zeta=0}^{c_P} \binom{m_P + t - 1 + \zeta}{t-1} \frac{H(K)}{c_P + 1},\ 1 \leq i \leq n_P \tag{5.7}$$

が成立する．　□

（**証明**）任意のユーザー P_i に対し，$\mathrm{P}_i \notin \mathcal{I}_\zeta^{(i)},\ \mathcal{I}_\zeta^{(i)} \subset \mathcal{I}_{\zeta+1}^{(i)},\ \left|\mathcal{I}_\zeta^{(i)}\right| = m_P + t - 1 + \zeta$ となるように集合 $\mathcal{I}_\zeta^{(i)} \subseteq \mathcal{P},\ 0 \leq \zeta \leq c_P$ を定める．この集合 $\mathcal{I}_\zeta^{(i)}$ に対して，

$$\mathcal{M}\left(\mathcal{I}_\zeta^{(i)}\right) = \left\{\mathcal{A}' \cup \{\mathrm{P}_i\} \mid \mathcal{A}' \subset \mathcal{I}_\zeta^{(i)}, |\mathcal{A}'| = t-1\right\}, 0 \leq \zeta \leq c_P \tag{5.8}$$

とし，この集合 $\mathcal{M}\left(\mathcal{I}_\zeta^{(i)}\right)$ を用いて，集合

$$\widetilde{\mathcal{M}}\left(\mathcal{I}_\zeta^{(i)}\right) = \left\{\mathcal{A} \mid \mathcal{A} \in \mathcal{M}\left(\mathcal{I}_\zeta^{(i)}\right), \mathcal{A} \notin \mathcal{M}\left(\mathcal{I}_{\zeta-1}^{(i)}\right)\right\}, 0 \leq \zeta \leq c_P \tag{5.9}$$

を定める．ここで，$\mathcal{M}\left(\mathcal{I}_{-1}^{(i)}\right) = \emptyset$ とおいた．このとき，

$$\widetilde{\mathcal{M}}\left(\mathcal{I}_{\zeta'}^{(i)}\right) \cap \widetilde{\mathcal{M}}\left(\mathcal{I}_{\zeta''}^{(i)}\right) = \emptyset,\ 0 \leq \zeta', \zeta'' \leq c_P,\ \zeta' \neq \zeta'', \tag{5.10}$$

かつ

$$\left|\mathcal{M}\left(\mathcal{I}_\zeta^{(i)}\right)\right| = \binom{m_P + t - 1 + \zeta}{t-1},\ 0 \leq \zeta \leq c_P \tag{5.11}$$

となるので，$\widetilde{\mathcal{M}}\left(\mathcal{I}_\zeta^{(i)}\right)$ 内のグループ $\mathcal{A}_j$ のインデックス j を

$$\widetilde{\mathcal{M}}\left(\mathcal{I}_\zeta^{(i)}\right) = \left\{\mathcal{A}_{\mu(m_P,t,\zeta-1)+1}, \mathcal{A}_{\mu(m_P,t,\zeta-1)+2}, \cdots, \mathcal{A}_{\mu(m_P,t,\zeta)}\right\}, \tag{5.12}$$

$$\mu(m_P, t, \zeta) = \begin{cases} 0 & \text{for } \zeta = -1 \\ \binom{m_P+t-1+\zeta}{t-1} & \text{for } 0 \leq \zeta \leq c_P \end{cases} \tag{5.13}$$

としてインデックスを付け直すことができる．以後，この付け直したインデックスを用いることとし，鍵 K_j についても同様のインデックスを用いる．このとき，ユーザ P_i の記憶容量 $H(U_i)$ に関して，

$$\begin{aligned} H(U_i) &= H\left(K_1^{\mu(m_P,t,c_P)}\right) - H\left(K_1^{\mu(m_P,t,c_P)} \mid U_i\right) + H\left(U_i \mid K_1^{\mu(m_P,t,c_P)}\right) \\ &\geq H\left(K_1^{\mu(m_P,t,c_P)}\right) - \sum_{j=1}^{\mu(m_P,t,c_P)} H(K_j \mid U_i) \\ &= H\left(K_1^{\mu(m_P,t,c_P)}\right) \\ &= \sum_{\zeta=0}^{c_P} H\left(K_{\mu(m_P,t,\zeta-1)+1}^{\mu(m_P,t,\zeta)} \mid K_1^{\mu(m_P,t,\zeta-1)}\right) \\ &= \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}\right) \end{aligned} \tag{5.14}$$

が成立する．ここで，

$$\Psi(m_P,t,\zeta) = \mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1) \tag{5.15}$$

とした．また，1 番目の等号は相互情報量の対称性 (定理 2.3)，不等号はエントロピー，及び相互情報量の非負性 (定理 2.1，定理 2.5) とエントロピーのチェイン則 (定理 2.2)，2 番目の等号は制約条件 (C1)，3 番目と 4 番目の等号はエントロピーのチェイン則 (定理 2.2) を用いた．また，相互情報量の非負性 (定理 2.5) により，$|\mathcal{X}| \leq m_D$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ に対して，

$$\begin{aligned} &\sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}\right) \\ &\quad \geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}, V(\mathcal{X}), S(\mathcal{X})\right) \end{aligned} \tag{5.16}$$

が成り立つ．よって，(5.14) と (5.16) より，

$$H(U_i) \geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}, V(\mathcal{X}), S(\mathcal{X})\right) \tag{5.17}$$

を得る．

ここで，(5.17) 右辺の各項に対して，

$$\begin{aligned}
\mathcal{A}^* &= \mathcal{A}_{\mu(m_P,t,\zeta-1)+j}, \\
\mathcal{Y} &= \mathcal{I}_\zeta^{(i)} \backslash \mathcal{A}_{\mu(m_P,t,\zeta-1)+j}, \\
\left\{\mathcal{A}_{j_1}^*, \mathcal{A}_{j_2}^*, \cdots, \mathcal{A}_{j_{\eta'}}^*\right\} &= \Big\{\mathcal{A}_1, \cdots, \mathcal{A}_{\mu(m_P,t,\zeta-1)+j-1}, \\
&\qquad \mathcal{A}_{\mu(m_P,t,\zeta-1)+j+1}, \cdots, \mathcal{A}_{\mu(m_P,t,\zeta-1)+\Psi(m_P,t,\zeta)}\Big\}
\end{aligned}$$

とおくと，$\mathrm{P}_i \notin \mathcal{I}_\zeta^{(i)}$，かつ $\mathrm{P}_i \in \mathcal{A}_{\mu(m_P,t,\zeta-1)+j}$ なので，

$$\begin{aligned}
\mathcal{Y} \cap \mathcal{A}^* &= \emptyset, \\
\mathcal{Y} \cap \mathcal{A}_{j_i}^* &\neq \emptyset, \quad 1 \le i \le \eta', \\
|\mathcal{Y}| &= m_P + \zeta \\
&\le m_P + c_P
\end{aligned}$$

が成り立つ．したがって，各項で補題 5.1 がそれぞれ適用でき，$|\mathcal{X}| \le m_D$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ に対して，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\Big(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}, V(\mathcal{X}), S(\mathcal{X})\Big) \\
&\qquad \ge \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} \frac{c_P + 1 - \varphi_{m_P}(m_P+\zeta)}{c_P+1} H\left(K_{\mu(m_P,t,\zeta-1)+j}\right) \\
&\qquad = \sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{c_P+1} H(K) \qquad (5.18)
\end{aligned}$$

を得る．等号は，仮定 3.2 より導かれる．

よって，(5.17)，(5.18) より，

$$H(U_i) \ge \sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{c_P+1} H(K),\ 1 \le i \le n_P \quad (5.19)$$

を得る．また，(5.19) の右辺は，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta)-\mu(m_P,t,\zeta-1)\right)\frac{c_P+1-\zeta}{c_P+1}H\left(K\right)\\
&= \Big[\left(c_P+1-0\right)\left\{\mu(m_P,t,0)-\mu(m_P,t,-1)\right\}\\
&\quad +\left(c_P+1-1\right)\left\{\mu(m_P,t,1)-\mu(m_P,t,0)\right\}+\cdots\\
&\quad +\left(c_P+1-2\right)\left\{\mu(m_P,t,2)-\mu(m_P,t,1)\right\}+\cdots\\
&\quad +\left(c_P+1-(c_P-1)\right)\left\{\mu(m_P,t,c_P-1)-\mu(m_P,t,c_P-2)\right\}\\
&\quad +\left(c_P+1-c_P\right)\left\{\mu(m_P,t,c_P)-\mu(m_P,t,c_P-1)\right\}\Big]\frac{H\left(K\right)}{c_P+1}\\
&= \sum_{\zeta=0}^{c_P}\mu(m_P,t,\zeta)\frac{H\left(K\right)}{c_P+1}\\
&= \sum_{\zeta=0}^{c_P}\binom{m_P+t-1+\zeta}{t-1}\frac{H\left(K\right)}{c_P+1} \qquad (5.20)
\end{aligned}$$

となり，(5.19) と (5.20) から (5.7) を得る．よって，定理が証明された．　□

5.2.2　センターの記憶容量の理論的限界

$(m_D,*,m_P,c_P,t)$ KPS におけるセンターの記憶容量 $H\left(V_k\right), 1\le k\le n_D$ の理論的限界は，次の定理として与えられる．

定理 5.2 仮定 3.2 を満たす任意の $(m_D,*,m_P,c_P,t)$ KPS において，

$$H\left(V_k\right)\ge\sum_{\zeta=0}^{c_P}\binom{m_P+t+\zeta}{t}\frac{H\left(K\right)}{c_P+1},\ 1\le k\le n_D \qquad (5.21)$$

が成立する．　□

（**証明**）まず，$\mathcal{J}_\zeta\subset\mathcal{J}_{\zeta+1}$，$|\mathcal{J}_\zeta|=m_P+t+\zeta$ を満たす任意の集合 $\mathcal{J}_\zeta\subset\mathcal{P}, 0\le\zeta\le c_P$ を定める．この $\mathcal{J}_\zeta$ に対して，

$$\mathcal{N}\left(\mathcal{J}_\zeta\right)=\Big\{\mathcal{A}\mid\mathcal{A}\subset\mathcal{J}_\zeta,|\mathcal{A}|=t\Big\}, 0\le\zeta\le c_P \qquad (5.22)$$

とし，この集合 $\mathcal{N}(\mathcal{J}_\zeta)$ を用いて，集合

$$\widetilde{\mathcal{N}}(\mathcal{J}_\zeta) = \left\{ \mathcal{A} \mid \mathcal{A} \in \mathcal{N}(\mathcal{J}_\zeta), \mathcal{A} \notin \mathcal{N}(\mathcal{J}_{\zeta-1}) \right\}, 0 \leq \zeta \leq c_P \tag{5.23}$$

を定める．ここで，$\mathcal{N}(\mathcal{J}_{-1}) = \emptyset$ とおいた．このとき，

$$\widetilde{\mathcal{N}}(\mathcal{J}_{\zeta'}) \cap \widetilde{\mathcal{N}}(\mathcal{J}_{\zeta''}) = \emptyset,\ 0 \leq \zeta', \zeta'' \leq c_P,\ \zeta' \neq \zeta'', \tag{5.24}$$

かつ

$$|\mathcal{N}(\mathcal{J}_\zeta)| = \binom{m_P + t + \zeta}{t},\ 0 \leq \zeta \leq c_P \tag{5.25}$$

となるので，$\widetilde{\mathcal{N}}(\mathcal{J}_\zeta)$ 内のグループ $\mathcal{A}_j$ のインデックス j を，

$$\widetilde{\mathcal{N}}(\mathcal{J}_\zeta) \ = \ \left\{ \mathcal{A}_{\nu(m_P,t,\zeta-1)+1}, \mathcal{A}_{\nu(m_P,t,\zeta-1)+2}, \cdots, \mathcal{A}_{\nu(m_P,t,\zeta)} \right\}, \tag{5.26}$$

$$\nu(m_P, t, \zeta) \ = \ \begin{cases} 0 & \text{for } \ \zeta = -1 \\ \binom{m_P+t+\zeta}{t} & \text{for } \ 0 \leq \zeta \leq c_P \end{cases} \tag{5.27}$$

としてインデックスを付け直すことができる．以後，この付け直したインデックスを用いることとし，鍵 K_j についても同様のインデックスを用いる．

次に，$\mathrm{D}_k \notin \mathcal{X}^{(k)}, |\mathcal{X}^{(k)}| = m_D$ を満たす任意の結託センター

$$\mathcal{X}^{(k)} = \left\{ \mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{m_D}} \right\} \subset \mathcal{D} \tag{5.28}$$

定めると，定理 4.2 の証明における (4.44) の導出と同様にして，

$$H(V_k) \geq H\left(K_1^{\nu(m_P,t,c_P)} \mid V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right) \right),\ 1 \leq k \leq n_D \tag{5.29}$$

を得る．また，(5.29) の右辺は，エントロピーのチェイン則 (定理 2.2) より，

$$\begin{aligned} & H\left(K_1^{\nu(m_P,t,c_P)} \mid V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right) \right) \\ &= \sum_{\zeta=0}^{c_P} H\left(K_{\nu(m_P,t,\zeta-1)+1}^{\nu(m_P,t,\zeta)} \mid K_1^{\nu(m_P,t,\zeta-1)}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right) \right) \\ &= \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} H\left(K_{\nu(m_P,t,\zeta-1)+j} \mid K_1^{\nu(m_P,t,\zeta-1)+j-1}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right) \right) \end{aligned} \tag{5.30}$$

となる．ここで，

$$\Phi\left(m_P, t, \zeta\right) = \nu(m_P, t, \zeta) - \nu(m_P, t, \zeta - 1),\ 0 \leq \zeta \leq c_P \tag{5.31}$$

とした．(5.30) 右辺の各項に対して，

$$\begin{aligned}
\mathcal{A}^* &= \mathcal{A}_{\nu(m_P,t,\zeta-1)+j}, \\
\mathcal{X} &= \mathcal{X}^{(k)}, \\
\mathcal{Y} &= \mathcal{J}_\zeta \backslash \mathcal{A}_{\nu(m_P,t,\zeta-1)+j}, \\
\left\{\mathcal{A}^*_{j_1}, \mathcal{A}^*_{j_2}, \cdots, \mathcal{A}^*_{j_{\eta'}}\right\} &= \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\mu(m_P,t,\zeta-1)+j-1}\right\}
\end{aligned}$$

とおくと，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset, \mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta', |\mathcal{X}| = m_D, |\mathcal{Y}| \leq m_P + c_P$ が成り立つので，各項で補題 5.1 がそれぞれ適用でき，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} H\left(K_{\nu(m_P,t,\zeta-1)+j} \mid K_1^{\nu(m_P,t,\zeta-1)+j-1}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right) \\
&\geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} \frac{c_P + 1 - \varphi_{m_P}\left(m_P + \zeta\right)}{c_P + 1} H\left(K_{\nu(m_P,t,\zeta-1)+j}\right) \\
&= \sum_{\zeta=0}^{c_P} \left(\nu(m_P, t, \zeta) - \nu(m_P, t, \zeta - 1)\right) \frac{c_P + 1 - \zeta}{c_P + 1} H\left(K\right)
\end{aligned} \tag{5.32}$$

を得る．等号は，仮定 3.2 より導かれる．よって，(5.29)，(5.30)，(5.32) より，

$$H\left(V_k\right) \geq \sum_{\zeta=0}^{c_P} \left(\nu(m_P, t, \zeta) - \nu(m_P, t, \zeta - 1)\right) \frac{c_P + 1 - \zeta}{c_P + 1} H\left(K\right),\ 1 \leq k \leq n_D \tag{5.33}$$

が成り立つ．また，(5.33) の右辺は，定理 5.1 における (5.20) の導出と同様にすると，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \left(\nu(m_P, t, \zeta) - \nu(m_P, t, \zeta - 1)\right) \frac{c_P + 1 - \zeta}{c_P + 1} H\left(K\right) \\
&= \sum_{\zeta=0}^{c_P} \binom{m_P + t + \zeta}{t} \frac{H\left(K\right)}{c_P + 1}
\end{aligned} \tag{5.34}$$

となり，(5.33) と (5.34) から (5.21) を得る．よって，定理が証明された．　□

5.3　最適な $(m_D, *, m_P, c_P, t)$ KPS の構成法

本節では，前節で導出したユーザとセンターの記憶容量の理論的限界を達成し，$(m_D, *, m_P, c_P, t)$ KPS を実現する最適な構成法を提案する．また，本研究では簡単のため，この構成法を $(m_D, *, m_P, c_P, t)$ 構成法と呼ぶことにする．提案する構成法は，4.3 節で提案したセンター通信量削減型 (m_D, m_P, t) 構成法をサブルーチンとして用いる．

ここで，$0 \leq \zeta \leq c_P$ に対して，$\mathbb{F}_q$ 上の多項式を用いるセンター通信量削減型 $(m_D, m_P + \zeta, t)$ 構成法の各情報，及び秘密情報の確率関数を次のように表す．ただし，各センター及び各ユーザの ID 情報は ζ に依らず同じ値とする．

- 秘密情報：$s_k^{(\zeta)}$, $1 \leq k \leq m_D + 1$.
- センター間通信情報：$v_{k,k'}^{(\zeta)}$, $1 \leq k \leq m_D + 1$, $1 \leq k' \leq n_D$.
- センター記憶情報：$v_k^{(\zeta)}$, $1 \leq k \leq n_D$.
- ユーザ受信情報：$u_{i_j,i}^{(\zeta)}$, $1 \leq i \leq n_P$, $1 \leq j \leq m_D + 1$.
- ユーザ記憶情報：$u_i^{(\zeta)}$, $1 \leq i \leq n_P$.
- グループ $\mathcal{A}_j$ の鍵：$k_j^{(\zeta)}$, $1 \leq j \leq \binom{n_P}{t}$.
- 確率関数：$p_S^{(\zeta)}(s^{(\zeta)})$.

次に，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, *, m_P, c_P, t)$ 構成法を示す．この構成法では，t-KPS' の公開情報である各集合，及び確率関数を次のようにおく．

$$\mathcal{D} = \mathcal{P} = \mathbb{F}_q \backslash \{0\}, \tag{5.35}$$

$$\mathcal{K} = \mathbb{F}_{q^{c_P+1}}, \tag{5.36}$$

$$\mathcal{S} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}(m_D+1)\binom{m_P+t+\zeta}{t}}, \tag{5.37}$$

$$\mathcal{V} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}\binom{m_P+t+\zeta}{t}}, \tag{5.38}$$

$$\mathcal{U} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}\binom{m_P+t-1+\zeta}{t-1}}, \tag{5.39}$$

$$p_S(s) = \prod_{\zeta=0}^{c_P} p_S^{(\zeta)}\left(s^{(\zeta)}\right). \tag{5.40}$$

更に，適当な全単射の写像 $\pi_1 : \mathbb{F}_q^{c_P+1} \to \mathbb{F}_{q^{c_P+1}}$ も公開情報とする．このとき，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, *, m_P, c_P, t)$ 構成法の各情報を，次のように表す．

$$s_k = \left(s_k^{(0)}, s_k^{(1)}, \cdots, s_k^{(c_P)}\right) \in \mathcal{S},\ 1 \le k \le m_D + 1, \tag{5.41}$$

$$v_{k,k'} = \left(v_{k,k'}^{(0)}, v_{k,k'}^{(1)}, \cdots, v_{k,k'}^{(c_P)}\right) \in \mathcal{V},\ 1 \le k \le m_D + 1,\ 1 \le k' \le n_D, \tag{5.42}$$

$$v_k = \left(v_k^{(0)}, v_k^{(1)}, \cdots, v_k^{(c_P)}\right) \in \mathcal{V},\ 1 \le k \le n_D, \tag{5.43}$$

$$u_{i_j,i} = \left(u_{i_j,i}^{(0)}, u_{i_j,i}^{(1)}, \cdots, u_{i_j,i}^{(c_P)}\right) \in \mathcal{U},\ 1 \le i \le n_P,\ 1 \le j \le m_D + 1, \tag{5.44}$$

$$u_i = \left(u_i^{(0)}, u_i^{(1)}, \cdots, u_i^{(c_P)}\right) \in \mathcal{U},\ 1 \le i \le n_P, \tag{5.45}$$

$$k_j = \pi_1\left(k_j^{(0)}, k_j^{(1)}, \cdots, k_j^{(c)}\right) \in \mathcal{K},\ 1 \le j \le \binom{n_P}{t}. \tag{5.46}$$

$\mathbb{F}_q$ 上の多項式を用いる $(m_D, *, m_P, c_P, t)$ 構成法は，$c_P = 0$ のとき明らかに $\mathbb{F}_q$ 上の多項式を用いるセンター通信量削減型 (m_D, m_P, t) 構成法と同様の計算を行っている．

$(m_D, m_P + \zeta, t)$ 構成法 $(0 \le \zeta \le c_P)$ の性質から，$(m_D, *, m_P, c_P, t)$ 構成法に対して，以下の定理が導かれる．

定理 5.3 $(m_D, *, m_P, c_P, t)$ 構成法は，定義 5.1 の $(m_D, *, m_P, c_P, t)$ KPS を実現し，ユーザ及びセンターの記憶容量が定理 5.1 及び定理 5.2 の理論的限界をそれぞれ達成する．□

(**証明**) 定理 4.3 より，グループ $\mathcal{A}_j$ のユーザーは同じ $k_j^{(\zeta)}, 0 \le \zeta \le c_P$ を共有できる．また，$(m_D, *, m_P, c_P, t)$ 構成法で用いる写像 π_1 が全単射であることから，グループの鍵 k_j もグループ内のユーザー間で共有することができる．したがって，$(m_D, *, m_P, c_P, t)$ 構成法は，制約条件 (C1) を満たす．

$(m_D, *, m_P, c_P, t)$ 構成法では，$0 \le \zeta \le c_P$ に対して，センター通信量削減型 $(m_D, m_P + \zeta, t)$ 構成法が独立に実行されるので，$|\mathcal{X}| \le m_D$, $|\mathcal{Y}| \le m_P + c_P$, $\mathcal{Y} \cap \mathcal{A}_j =$

$\emptyset$ を満たす任意の結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$, 及び任意のグループ $\mathcal{A}_j$ に対して,

$$H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = \begin{cases} 0 & \text{for } \zeta < \varphi_{m_P}(|\mathcal{Y}|) \\ H\left(K_j^{(\zeta)}\right) & \text{for } \zeta \geq \varphi_{m_P}(|\mathcal{Y}|) \end{cases} \tag{5.47}$$

が成り立つ. ここで, $k_j^{(\zeta)}$ に対応する確率変数を $K_j^{(\zeta)}$ とした. また, (m_D, c_D, m_P, c_P, t) 構成法で用いる写像 π_1 は全単射なので,

$$H\left(K_j\right) = \sum_{\zeta=0}^{c_P} H\left(K_j^{(\zeta)}\right) \tag{5.48}$$

が成り立つ. よって,

$$\begin{aligned} H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) &= \sum_{\zeta=0}^{c_P} H\left(K_j^{(\zeta)} \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \\ &= \sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)} \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \\ &\quad + \sum_{\zeta'=0}^{\varphi_{m_P}(|\mathcal{Y}|)-1} H\left(K_j^{(\zeta')} \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \\ &= \sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)}\right) \end{aligned} \tag{5.49}$$

を得る. また, $(m_D, *, m_P, c_P, t)$ 構成法で用いる写像 π_1 は全単射なので,

$$H\left(K_j\right) = H\left(K_j^{(0)}, K_j^{(1)}, \cdots, K_j^{(c)}\right) \tag{5.50}$$

が成り立ち, 確率変数 $K_j^{(\zeta)}, 0 \leq \zeta \leq c_P$ は互いに独立かつ $\mathbb{F}_q$ 上で一様に分布するので, 任意のグループ $\mathcal{A}_j$ に対して,

$$H\left(K_j^{(\zeta)}\right) = \log q^{c_D+1} \tag{5.51}$$

を得る．したがって，

$$\begin{aligned}\sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)}\right) &= \left(c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)\right)\log q \\ &= \frac{\left(c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)\right)\left(c_P+1\right)}{c_P+1}\log q \\ &= \frac{c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)}{c_P+1}H\left(K_j\right) \qquad (5.52)\end{aligned}$$

となり，(5.49) と (5.52) から，

$$H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = \frac{c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)}{c_P+1}H\left(K_j\right)$$

を得る．したがって，$(m_D, *, m_P, c_P, t)$ 構成法は，制約条件 (C3) を満たす.

$\mathbb{F}_q$ 上の多項式を用いる $(m_D, *, m_P, c_P, t)$ 構成法は，$0 \le \zeta \le c_P$ に対して，$\mathbb{F}_q$ 上の多項式を用いるセンター通信量削減型 $(m_D, m_P+\zeta, t)$ 構成法を独立に実行する構成法なので，このセンター通信量削減型 $(m_D, m_P+\zeta, t)$ 構成法 $(0 \le \zeta \le c_P)$ におけるユーザ及びセンターの記憶容量の合計が，$(m_D, *, m_P, c_P, t)$ 構成法におけるユーザ及びセンターの記憶容量となる．センター通信量削減型 $(m_D, m_P+\zeta, t)$ 構成法における $k_j^{(\zeta)}, 0 \le \zeta \le c$ は，互いに独立で $\mathbb{F}_q$ 上の一様分布に従うので，センター通信量削減型 $(m_D, m_P+\zeta, t)$ 構成法におけるユーザ及びセンターの記憶容量は，それぞれ，

$$\begin{aligned}\binom{m_P+t-1+\zeta}{t-1}\log q &= \binom{m_P+t-1+\zeta}{t-1}\frac{c_P+1}{c_P+1}\log q \\ &= \binom{m_P+t-1+\zeta}{t-1}\frac{H\left(K\right)}{c_P+1}, \qquad (5.53) \\ \binom{m_P+t+\zeta}{t}\log q &= \binom{m_P+t+\zeta}{t}\frac{c_P+1}{c_P+1}\log q \\ &= \binom{m_P+t+\zeta}{t}\frac{H\left(K\right)}{c_P+1} \qquad (5.54)\end{aligned}$$

となる．したがって，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, *, m_P, c_P, t)$ 構成法における，ユー

ザー及びセンターの記憶容量は，それぞれ

$$H(U_i) = \sum_{\zeta=0}^{c_P} \binom{m_P+t-1+\zeta}{t-1} \frac{H(K)}{c_P+1},\ 1 \le i \le n_P, \tag{5.55}$$

$$H(V_k) = \sum_{\zeta=0}^{c_P} \binom{m_P+t+\zeta}{t} \frac{H(K)}{c_P+1},\ 1 \le k \le n_D \tag{5.56}$$

となり，定理 5.1 及び定理 5.2 の理論的限界とそれぞれ一致する．

以上により，定理が証明された．　□

5.4　比較・考察

定義 4.2 と定義 5.1 から，$c_P = 0$ のとき，制約条件 (C2) と制約条件 (C3) が等価となる．すなわち，$(m_D, *, m_P, 0, t)$ KPS と (m_D, m_P, t) KPS' が等価であることがわかる．したがって，$(m_D, *, m_P, c_P, t)$ KPS は，(m_D, m_P, t) KPS 及び (m_D, m_P, t) KPS' を特別な場合に含む一般的な方式となる．

定理 5.1，及び定理 5.2 によって示されたセンターとユーザの記憶容量の理論的限界は，$c_P = 0$ のとき，それぞれ定理 4.1，及び定理 4.2 で示した理論的限界と一致する．したがって，$(m_D, *, m_P, c_P, t)$ KPS に対する記憶容量の理論的限界は，(m_D, m_P, t) KPS' に対する理論的限界を含んだ一般的な結果となっている．この理論的限界は，センターの個数 n_D やセンターの結託数に対するしきい値 m_D に依存しない量となる．よって，センターの結託やセンターとユーザ間が一部通信不能になった場合の問題に対する耐性をより強くするために m_D や n_D を大きくとっても，ユーザとセンターの記憶容量には全く影響しない．しかし，m_D や n_D を大きくとった場合，センター間の総通信量が増加する．

次に，4.3 節で提案したセンター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法と 5.3 節で提案した $(m_D, *, m_P, c_P, t)$ 構成法の安全性と記憶容量の比較を行う[1]．これら 2 つの構成法は，両者とも結託ユーザ数が $m_P + c_P + 1$ 人以上のとき，鍵の情報が完全に得られる．一方，結託センターに対する安全性は，結託センター数が m_D 以下の場合，

[1]センター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法と $(m_D, m_P + c_P, t)$ 構成法の安全性と記憶容量は同じなので，$(m_D, m_P + c_P, t)$ 構成法と $(m_D, *, m_P, c_P, t)$ 構成法を比較しても同じ結果となる

表 5.1: センター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法と $(m_D, *, m_P, c_P, t)$ 構成法の安全性と記憶容量の比較例 (単位：ビット)

結託ユーザ数	$(1, 20, 2)$	$(1, *, 13, 7, 2)$	$(1, *, 5, 15, 2)$
$\omega \leq 5$	128	128	128
$6 \leq \omega \leq 13$	128	128	120 〜 64
$14 \leq \omega \leq 20$	128	112 〜 16	56 〜 8
$21 \leq \omega$	0	0	0
記憶容量 (ユーザ)	2688	2240	1728
記憶容量 (センター)	29568	21056	13888

鍵の情報が全く得られないことを保証し，$m_D + 1$ 以上の場合には保証されない．すなわち，結託センター数に対しては，段階的に鍵の情報が得られる性質になっていない．更に，ユーザの記憶容量は m_D に依存しない量となるので，両者の構成法の比較においては，$m_D = 1$ の場合のみについて考える．

表 5.1 は，簡単な比較例として $\mathbb{F}_{2^{128}}$ 上の多項式を用いるセンター通信量削減型 $(1, 20, 2)$ 構成法，$\mathbb{F}_{2^{16}}$ 上の多項式を用いる $(1, *, 13, 7, 2)$ 構成法，及び $\mathbb{F}_{2^8}$ 上の多項式を用いる $(1, *, 5, 15, 2)$ 構成法の安全性と記憶容量を示している．これら 3 つの構成法における鍵の長さおよび鍵のエントロピーは全て 128 ビットとなる．また，結託センター数は全ての構成法で 1 個以下と仮定する．表 5.1 の 2〜5 行目は，結託ユーザ数 ω に対する各構成法の安全性の評価基準である安全度 (条件付エントロピー) を示しており，6 行目と 7 行目はそれぞれ各構成法に対するユーザとセンターの記憶容量を示している（単位は全てビット）．これら 3 つの構成法では，結託ユーザ数が 21 以上になると鍵の情報が完全に得られてしまい，安全度が 0 になる．一方，結託ユーザ数が 20 以下の場合は，全ての構成法において，鍵の情報が完全に得られることはないがしきい値-しきい値ランプ型安全性を満たす $(1, *, 13, 7, 2)$ 構成法と $(1, *, 5, 15, 2)$ 構成法では，結託ユーザ数がそれぞれ $14 \leq \omega \leq 20$ と $6 \leq \omega \leq 20$ のときに鍵の情報が部分的に得られる．したがって，部分的に得られる範囲が狭いほど，すなわち，安全性が高いほど記憶容量が増加することがわかる．

以上により，同じ長さの鍵を共有する場合，$(m_D, *, m_P, c_P, t)$ 構成法は部分的に

鍵の情報が得られる範囲を許容することで，センター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法より記憶容量を削減した効率的な構成法となる．また，記憶容量を削減することにより，安全性が低下してしまうが，鍵のエントロピーを十分大きくとることで，十分高い安全性を実現できる．

第6章　しきい値ランプ-しきい値型安全性を満たすt-KPS'

第5章では，結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られるしきい値-しきい値ランプ型安全性を満たすt-KPS'について検討した．本章では，結託センター数の増加に従って攻撃対象の情報が段階的に得られていくという性質について検討する．この性質は，結託センターと結託ユーザを独立に考えたとき，結託センター数に対してはしきい値ランプ型安全性を満たし，結託ユーザ数に対してはしきい値型安全性を満たすので，本研究では，この性質をしきい値ランプ-しきい値型安全性と呼ぶ．

以下では，t-KPS'に要求する制約条件として，完全整合性としきい値ランプ-しきい値型安全性に対する制約条件を定義し，その制約条件を満たすもとでのt-KPS'における記憶容量の理論的限界の導出，及びその理論的限界を達成する構成法の提案を行う．また，t-KPS'の評価基準は，第4章と同様に(3.3)〜(3.6)とする．

6.1　t-KPS'に要求する制約条件の定義

t-KPS'がしきい値ランプ-しきい値型安全性を満たすなら，任意のしきい値m_D, c_D, m_Pに対して，結託数がm_P以下の任意の結託ユーザとm_D以下の任意の結託センターが攻撃しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られず，結託センター数がm_D+1からm_D+c_Dかつ結託ユーザ数がm_P以下の場合には，結託センター数が大きくなるにつれて段階的に情報が得られていく．また，攻撃対象の鍵を共有するグループに，結託ユーザは1人も属さないことになるので，結託ユーザ数は最大n_P-tまで考えられる．したがって，しきい値ランプ-しきい値型安全性を満たすt-KPS'は，$m_P \leq n_P-t$を満たす必要がある．

定義 6.1 t-KPS'への攻撃が，仮定 4.1 を満たすとする．$m_D+c_D < n_D$，$m_P+t \leq n_P$ を満たす非負整数 m_D，c_D，m_P，t に対し，定義 3.2 と同様の制約条件 (C1)，及び以下の制約条件 (C4) を満たす t-KPS'を $(m_D, c_D, m_P, *, t)$ KPS という．

(C4：しきい値ランプ-しきい値型安全性) $|\mathcal{X}| \leq m_D + c_D$，$|\mathcal{Y}| \leq m_P$，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ と結託ユーザ $\mathcal{Y} \subset \mathcal{P}$，及び任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ に対して，

$$H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H\left(K_j\right) \tag{6.1}$$

が成立する．ここで，関数 $\varphi_{m_P} : \{0, 1, \cdots, m_D + c_D\} \to \{0, 1, \cdots, c_D\}$ を

$$\varphi_{m_D}(i) = \begin{cases} 0 & \text{for} \quad i \leq m_D \\ i - m_D & \text{for} \quad m_D + c_D \geq i > m_D \end{cases} \tag{6.2}$$

とした． □

6.2　$(m_D, c_D, m_P, *, t)$ KPS における記憶容量の理論的限界

本節では，$(m_D, c_D, m_P, *, t)$ KPS における各ユーザと各センターの記憶容量，すなわち，$H\left(U_i\right), 1 \leq i \leq n_P$ と $H\left(V_k\right), 1 \leq k \leq n_D$ の理論的限界を導出する．

センターとユーザの記憶容量の理論的限界を導出するために，以下の補題を用いる．この補題は，補題 4.2 と同様にして導かれる．

補題 6.1 任意の $(m_D, c_D, m_P, *, t)$ KPS において，$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P$, $\mathcal{Y} \cap \mathcal{A}^* = \emptyset$，$\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta_{\mathcal{Y}}$ を満たす任意の結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$, 及び任意のグループ $\mathcal{A}^*, \mathcal{A}^*_{j_i}$ に対し，

$$H\Big(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\Big) \geq \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H(K^*), \tag{6.3}$$

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}\right) = H\left(K^*\right), \ \eta' \leq \eta_{\mathcal{Y}} \tag{6.4}$$

が成立する． □

（**証明**）制約条件 (C4) より，任意の $(m_D, c_D, m_P, *, t)$ KPS に対して，

$$H\left(K^* \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \geq \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H\left(K^*\right), \tag{6.5}$$

$$H\left(K^* \mid U\left(\mathcal{Y}\right)\right) = H\left(K^*\right) \tag{6.6}$$

が成り立つ．また，補題 4.2 の証明における (4.16) の導出と同様にして，

$$H\left(K^* \mid K^*_{j_1}, \cdots, K^*_{j_{\eta'}}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \geq H\left(K^* \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right), \tag{6.7}$$

$$H\left(K^*\right) \geq H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}\right)$$

$$\geq H\left(K^* \mid U\left(\mathcal{Y}\right)\right),\ \eta' \leq \eta_{\mathcal{Y}} \tag{6.8}$$

を得る．したがって，(6.5), (6.6), (6.7), (6.8) より，

$$H\left(K^* \mid K^*_{j_1}, \cdots, K^*_{j_{\eta'}}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \geq \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H\left(K^*\right), \tag{6.9}$$

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}\right) = H\left(K^*\right),\ \eta' \leq \eta_{\mathcal{Y}} \tag{6.10}$$

を得る．　□

補題 6.1 において，結託センター $\mathcal{X}$ と結託ユーザ $\mathcal{Y}$ が正規の方法で共有できる全ての鍵が $k^*_{j_i}, 1 \leq i \leq \eta_{\mathcal{Y}}$ となる．

6.2.1　ユーザの記憶容量の理論的限界

$(m_D, c_D, m_P, *, t)$ KPS におけるユーザの記憶容量 $H\left(U_i\right), 1 \leq i \leq n_P$ の理論的限界は，次の定理として与えられる．

定理 6.1 仮定 3.2 を満たす任意の $(m_D, c_D, m_P, *, t)$ KPS において，

$$H\left(U_i\right) \geq \binom{m_P + t - 1}{t - 1} H\left(K\right),\ 1 \leq i \leq n_P \tag{6.11}$$

が成立する．　□

（**証明**）まず，定理 4.1 の証明と同様にして，(4.22) と同様の不等式

$$H\left(U_i\right) \geq \sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}\right) \tag{6.12}$$

を得る．(6.12) の右辺の各項に対し，

$$\begin{aligned}
&\mathcal{A}^* = \mathcal{A}_j, \quad \mathcal{Y} = \mathcal{I}^{(i)} \backslash \mathcal{A}_j, \\
&\left\{\mathcal{A}_{j_1}^*, \mathcal{A}_{j_2}^*, \cdots, \mathcal{A}_{j_{\eta'}}^*\right\} = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{j-1}\right\}, \ 1 \leq j \leq \rho^{(m_P,t)},
\end{aligned}$$

とおくと，$\mathrm{P}_i \notin \mathcal{I}^{(i)}$ かつ $\mathrm{P}_i \in \mathcal{A}_j$ なので，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset$, $\mathcal{Y} \cap \mathcal{A}_{j_i}^* \neq \emptyset, 1 \leq i \leq \eta'$, $|\mathcal{Y}| = m_P$ が成り立つ．したがって，$|\mathcal{X}| \leq m_D + c_D$ を満たす任意の集合 $\mathcal{X} \subset \mathcal{D}$ に対し，各項で補題 6.1 の (6.4) がそれぞれ適用でき，

$$\begin{aligned}
\sum_{j=1}^{\rho(m_P,t)} H\left(K_j \mid K_1^{j-1}\right) &= \sum_{j=1}^{\rho(m_P,t)} H\left(K_j\right) \\
&= \rho(m_P,t) H\left(K\right)
\end{aligned} \tag{6.13}$$

を得る．最後の等号は，仮定 3.2 より導かれる．

よって，(6.12)，及び (6.13) より，

$$H\left(U_i\right) \geq \binom{m_P + t - 1}{t - 1} H\left(K\right), \quad 1 \leq i \leq n_P, \tag{6.14}$$

が成立し，(6.11) を得る．　□

6.2.2　センターの記憶容量の理論的限界

$(m_D, c_D, m_P, *, t)$ KPS におけるセンターの記憶容量 $H\left(V_k\right), 1 \leq k \leq n_D$ の理論的限界は，次の定理として与えられる．

定理 6.2 仮定 3.2 を満たす任意の $(m_D, c_D, m_P, *, t)$ KPS において，

$$H\left(V_k\right) \geq \binom{m_P + t}{t} \frac{H\left(K\right)}{c_D + 1}, \ 1 \leq k \leq n_D \tag{6.15}$$

が成立する．　□

（**証明**）定理 6.2 は，定理 4.2 の証明と同様にして導かれる．

$\mathrm{D}_k \notin \mathcal{X}^{(k)}, |\mathcal{X}^{(k)}| = m_D + c_D$ を満たす任意の結託センター

$$\mathcal{X}^{(k)} = \left\{\mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{m_D+c_D}}\right\} \subset \mathcal{D} \tag{6.16}$$

定めると，(4.44) と (4.45) と同様の式が導かれ，

$$H\left(V_k\right) = \sum_{j=1}^{\varrho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\right),\ 1 \le k \le n_D \tag{6.17}$$

を得る．ここで，(6.17) の右辺の各項に対し，

$$\mathcal{A}^* = \mathcal{A}_j,\quad \mathcal{X} = \mathcal{X}^{(k)},\quad \mathcal{Y} = \mathcal{J}\backslash\mathcal{A}_j,$$
$$\left\{\mathcal{A}^*_{j_1}, \mathcal{A}^*_{j_2}, \cdots, \mathcal{A}^*_{j_{\eta'}}\right\} = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{j-1}\right\},\ 1 \le j \le \varrho(m_P, t),$$

とおくと，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset, \mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \le i \le \eta', |\mathcal{X}| = m_D + c_D, |\mathcal{Y}| = m_P$ が成り立つ．したがって，各項で補題 6.1 の (6.3) がそれぞれ適用でき，

$$\begin{aligned}
\sum_{j=1}^{\varrho(m_P,t)} H\left(K_j \mid K_1^{j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) &\ge \sum_{j=1}^{\varrho(m_P,t)} \frac{H\left(K_j\right)}{c_D+1} \\
&= \varrho(m_P, t)\frac{H\left(K\right)}{c_D+1} \\
&= \binom{m_P+t}{t}\frac{H\left(K\right)}{c_D+1}
\end{aligned} \tag{6.18}$$

を得る．1 番目の等号は，仮定 3.2 より導かれる．したがって，(6.17) と (6.18) より，(6.15) を得る． □

6.3　最適な $(m_D, c_D, m_P, *, t)$ KPS の構成法

本節では，前節で導出したユーザとセンターの記憶容量の理論的限界を達成する最適な $(m_D, c_D, m_P, *, t)$ KPS の構成法を提案する．また，本研究では簡単のため，

この構成法を $(m_D, c_D, m_P, *, t)$ 構成法と呼ぶことにする．提案する構成法は，(3.15) で定義される多項式と同様の性質を持つ n_S 個の $\mathbb{F}_q$ 上の多項式

$$P_k(x_0, x_1, \cdots, x_t) = \sum_{\substack{0 \le r_0 \le m_D + c_D, \\ 0 \le r_1, \cdots, r_t \le m_P}} a^{(k)}_{r_0 \cdots r_t} (x_0)^{r_0} (x_1)^{r_1} \cdots (x_t)^{r_t}, \ 1 \le k \le n_S \quad (6.19)$$

を用いる．

次に，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, c_D, m_P, *, t)$ 構成法を示す．この構成法では，$n_S = m_D + c_D + 1$, $L = m_D + c_D + 1$ とおき，t-KPS' の公開情報である集合 $\mathcal{D}$, $\mathcal{P}$, $\mathcal{V}$, $\mathcal{U}$ は，従来の (m_D, m_P, t) 構成法と同様に，それぞれ (3.21), (3.24), (3.25) に従う．また，集合 $\mathcal{S}$, $\mathcal{K}$ 及び確率関数 $p_S(s)$ は次のようにおく．

$$\mathcal{S} = \mathbb{F}_q^{(m_D + c_D + 1)\binom{m_P + t}{t}}, \quad (6.20)$$

$$\mathcal{K} = \mathbb{F}_{q^{c_D+1}}, \quad (6.21)$$

$$p_S(s) = q^{-(m_D + c_D + 1)\binom{m_P + t}{t}}, \ s \in \mathcal{S}. \quad (6.22)$$

更に，適当な全単射の写像 $\pi_2 : \mathbb{F}_q^{c_D+1} \to \mathbb{F}_{q^{c_D+1}}$ をプロトコルの公開情報とする．このとき，各関数の計算は，それぞれ次のように行う．

- $v_{k,k'} = f_T(s_k, \mathrm{D}_{k'})$, $1 \le k \le m_D + c_D + 1$, $1 \le k' \le n_D$ の計算：
  (m_D, m_P, t) 構成法と同様にして，秘密情報 s_k から (6.19) で定義した $t+1$ 変数多項式 $P_k(x_0, x_1, \cdots, x_t)$ を定め，$x_0 = \mathrm{D}_{k'}$ とした

$$P_k(\mathrm{D}_{k'}, x_1, \cdots, x_t) = \sum_{\substack{0 \le r_0 \le m_D + c_D, \\ 0 \le r_1, \cdots, r_t \le m_P}} a^{(k)}_{r_1 \cdots r_t} (\mathrm{D}_{k'})^{r_0} (x_1)^{r_1} \cdots (x_t)^{r_t} \quad (6.23)$$

  を計算する．この多項式 $P_k(\mathrm{D}_{k'}, x_1, \cdots, x_t)$ は，t 変数 m_P 次対称多項式となるので，対応する $\binom{m_P+t}{t}$ 個の $\mathbb{F}_q$ 上の元を $\binom{m_P+t}{t}$ 次元のベクトル集合 $\mathcal{V}$ の元 $v_{k,k'}$ とおく．

- $v_k = f_M(v_{1,k}, v_{2,k}, \cdots, v_{n_D,k})$, $1 \le k \le n_D$ の計算：
  (m_D, m_P, t) 構成法と同様にして，

$$v_k = \sum_{k'=1}^{m_D + c_D + 1} v_{k',k} \in \mathcal{V}. \quad (6.24)$$

このとき，v_k は以下で定義される t 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, x_1, \cdots, x_t\right)$ と 1 対 1 対応する．

$$Q\left(\mathrm{D}_k, x_1, \cdots, x_t\right) = \sum_{k'=1}^{n_S} P_{k'}\left(\mathrm{D}_k, x_1, \cdots, x_t\right). \tag{6.25}$$

- $u_{i_j,i} = F_T\left(v_{i_j}, \mathrm{P}_i\right)$, $1 \le i \le n_P$, $1 \le j \le m_D + c_D + 1$ の計算：
  $\binom{m_P+t}{t}$ 次元のベクトル集合 $\mathcal{V}$ の元 v_{i_j} から，(6.25) で定義した t 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, x_1, \cdots, x_t\right)$ を定め，$x_1 = \mathrm{P}_i$ とした

$$\begin{aligned} &Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ &\quad = \sum_{k=1}^{n_S} \sum_{\substack{0 \le r_0 \le m_D + c_D, \\ 0 \le r_1, \cdots, r_t \le m_P}} a^{(k)}_{r_1 \cdots r_t} \left(\mathrm{D}_{i_j}\right)^{r_0} \left(\mathrm{P}_i\right)^{r_1} \left(x_2\right)^{r_2} \cdots \left(x_t\right)^{r_t} \end{aligned} \tag{6.26}$$

  を計算する．この多項式は $t-1$ 変数 m_P 次対称多項式となるので，対応する $\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元を $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 $u_{i_j,i}$ とおく．

- $u_i = g_M\left(u_{i_1,i}, u_{i_2,i}, \cdots, u_{i_{m_D+1},i}\right)$, $1 \le i \le n_P$ の計算：
  $\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 $u_{i_j,i}, 1 \le j \le m_D + c_D + 1$ から，$t-1$ 変数 m_P 次対称多項式 $Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right)$ をそれぞれ定め，ラグランジュ補間を用いて以下の計算を行う．

$$\begin{aligned} &\sum_{j=1}^{m_D+c_D+1} \lambda_{i_j} Q\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ &= \sum_{j=1}^{m_D+c_D+1} \lambda_{i_j} \sum_{k=1}^{m_D+c_D+1} P_k\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ &= \sum_{k=1}^{m_D+c_D+1} \sum_{j=1}^{m_D+c_D+1} \lambda_{i_j} P_k\left(\mathrm{D}_{i_j}, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ &= \sum_{k=1}^{m_D+c_D+1} P_k\left(x_0, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ &= Q\left(x_0, \mathrm{P}_i, x_2, \cdots, x_t\right). \end{aligned} \tag{6.27}$$

ここで,

$$\lambda_{i_j} = \prod_{k=1:k\neq j}^{m_D+c_D+1} \frac{x_0 - \mathrm{D}_{i_k}}{\mathrm{D}_{i_j} - \mathrm{D}_{i_k}} \tag{6.28}$$

とした．多項式 (6.19) の性質から，このように求めた t 変数多項式

$$\begin{aligned} & Q\left(x_0, \mathrm{P}_i, x_2, \cdots, x_t\right) \\ & \quad = \sum_{k=1}^{m_D+c_D+1} \sum_{\substack{0\leq r_0\leq m_D+c_D,\\ 0\leq r_1,\cdots,r_t\leq m_P}} a^{(k)}_{r_0\cdots r_t} \left(x_0\right)^{r_0} \left(\mathrm{P}_i\right)^{r_1} \cdots \left(x_t\right)^{r_t} \end{aligned} \tag{6.29}$$

は，$\mathbb{F}_q$ 上の任意の元 b，及び任意の置換 $\sigma' : \{2, 3, \cdots, t\} \to \{2, 3, \cdots, t\}$ に対し，

$$Q\left(b, \mathrm{P}_i, x_2, \cdots, x_t\right) = Q\left(b, \mathrm{P}_i, x_{\sigma'(2)}, x_{\sigma'(3)}, \cdots, x_{\sigma'(t)}\right) \tag{6.30}$$

を満たす t 変数多項式となる．したがって，任意の置換 σ' に対して,

$$\begin{aligned} \sum_{k=1}^{m_D+c_D+1} \sum_{r_1=0}^{m_P} a^{(k)}_{r_0 r_1 r_2\cdots r_t} \left(\mathrm{P}_i\right)^{r_1} = \sum_{k=1}^{m_D+c_D+1} \sum_{r_1=0}^{m_P} a^{(k)}_{r_0 r_1 r_{\sigma'(2)}\cdots r_{\sigma'(t)}} \left(\mathrm{P}_i\right)^{r_1}, \\ 0 \leq r_0 \leq m_D + c_D + 1,\ 0 \leq r_2, \cdots, r_t \leq m_P \end{aligned} \tag{6.31}$$

が成り立つので，$(m_D + c_D + 1)\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元から，(6.29) の多項式が一意に定まる．ここで，(6.29) の多項式に対応する，$(m_D + c_D + 1)\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元から,

$$\sum_{k=1}^{m_D+c_D+1} \sum_{r_1=0}^{m_P} a^{(k)}_{r_0 r_1 r_2\cdots r_t} \left(\mathrm{P}_i\right)^{r_1},\ 0 \leq r_0 \leq c_D,\ 0 \leq r_2, \cdots, r_t \leq m_P$$

と 1 対 1 対応する $(c_D + 1)\binom{m_P+t-1}{t-1}$ 個の $\mathbb{F}_q$ 上の元を $(c_D + 1)\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 u_i とおく.

- $k_j = g_K\left(u_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right), 1 \leq i \leq t, \mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\} \in \mathcal{A}\left(\mathcal{P}, t\right)$ の計算：

$(c_D+1)\binom{m_P+t-1}{t-1}$ 次元のベクトル集合 $\mathcal{U}$ の元 u_{j_i} から，c_D+1 個の $t-1$ 変数 m_P 次対称多項式

$$R_{r_0}\left(\mathrm{P}_{j_i}, x_2, \cdots, x_t\right) = \sum_{k=1}^{m_D+c_D+1} \sum_{0\le r_1,\cdots,r_t\le m_P} a^{(k)}_{r_0 r_1 \cdots r_t} \left(\mathrm{P}_i\right)^{r_1} (x_2)^{r_2} \cdots (x_t)^{r_t},\ 0 \le r_0 \le c_D$$

を定め，以下の計算を行い，各多項式の値 $k_j^{(r_0)}$ を生成する．

$$k_j^{(r_0)} = R_{r_0}\left(\mathrm{P}_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right),\ \ 0 \le r_0 \le c_D. \tag{6.32}$$

最後に，公開情報である π_2 を用いて，次のようにグループ $\mathcal{A}_j$ の鍵 k_j を生成する．

$$k_j = \pi_2\left(k_j^{(0)}, k_j^{(1)}, \cdots, k_j^{(c_D)}\right) \tag{6.33}$$

この構成法は，$c_D = 0$ のときセンター通信量削減型 (m_D, m_P, t) 構成法と等価となる．この $(m_D, c_D, m_P, *, t)$ 構成法に対して，以下の定理が成り立つ．

定理 6.3 $(m_D, c_D, m_P, *, t)$ 構成法は，定義 6.1 の $(m_D, c_D, m_P, *, t)$ KPS を実現し，ユーザ及びセンターの記憶容量が，それぞれ定理 6.1 及び定理 6.2 の理論的限界を達成する．□

（**証明**）(6.32) の $k_j^{(r_0)}$, $1 \le r_0 \le c_D$ は，対称多項式 R_{r_0} によって計算されるので，任意のグループ

$$\mathcal{A}_j = \{\mathrm{P}_{j_1}, \mathrm{P}_{j_2}, \cdots, \mathrm{P}_{j_t}\} \in \mathcal{A}\left(\mathcal{P}, t\right) \tag{6.34}$$

に対して，

$$k_j^{(r_0)} = R_{r_0}\left(0, \mathrm{P}_{j_i}, \mathrm{P}_{j_1}, \cdots, \mathrm{P}_{j_{i-1}}, \mathrm{P}_{j_{i+1}}, \cdots, \mathrm{P}_{j_t}\right),\ 1 \le i \le t \tag{6.35}$$

となる．また鍵 k_j は，全単射写像 π_2 を用いて (6.33) に従って生成されるので，任意のグループ $\mathcal{A}_j$ に属するユーザは全て同じ鍵を一意に生成できる．したがって，$(m_D, c_D, m_P, *, t)$ 構成法は，制約条件 (C1) を満たす．

ここで，センターのみが結託し攻撃する場合を考えると，鍵の安全性は，2.4 節で述べたしきい値ランプ型秘密分散法 [33] の安全性と同様の性質が成り立つ．したがって，任意の結託センター $\mathcal{X} \subset \mathcal{D}$ に対する安全度は，

$$H\left(K_j \mid V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H\left(K_j\right) \tag{6.36}$$

になる．また，文献 [18] の Theorem 5 と Theorem 6 より，$V\left(\mathcal{X}\right)$ と $S\left(\mathcal{X}\right)$ が与えられたとき，K_j と $U\left(\mathcal{Y}\right)$ が条件付き独立となるので，

$$H\left(K_j \mid V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \tag{6.37}$$

が成立する．よって，(6.36) と (6.37) より，

$$H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) = \frac{c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)}{c_D + 1} H\left(K_j\right) \tag{6.38}$$

を得る．したがって，$(m_D, c_D, m_P, *, t)$ 構成法は，制約条件 (C4) を満たす．以上より，$(m_D, c_D, m_P, *, t)$ 構成法は，定義 6.1 の $(m_D, c_D, m_P, *, t)$ KPS を実現する構成法であることが示された．

また，$(m_D, c_D, m_P, *, t)$ 構成法において，鍵 k_j, $0 \leq j \leq \binom{n_P}{t}$ は，互いに独立に $\mathbb{F}_{q^{c_D+1}}$ 上の一様分布に従うので，ユーザ及びセンターの記憶容量は，それぞれ，

$$\begin{aligned}
\left(c_D + 1\right) \binom{m_P + t - 1}{t - 1} \log q &= \binom{m_P + t - 1}{t - 1} \log q^{c_D+1} \\
&= \binom{m_P + t - 1}{t - 1} H\left(K\right), \qquad (6.39) \\
\binom{m_P + t}{t} \log q &= \binom{m_P + t}{t} \frac{c_D + 1}{c_D + 1} \log q \\
&= \binom{m_P + t}{t} \frac{H\left(K\right)}{c_D + 1} \qquad (6.40)
\end{aligned}$$

となり，定理 6.1 及び定理 6.2 の理論的限界と一致する．　□

6.4　比較・考察

定義 4.2 と定義 6.1 から，$c_D = 0$ のとき，制約条件 (C2) と (C4) が等価となる．すなわち，$(m_D, 0, m_P, *, t)$ KPS と (m_D, m_P, t) KPS' が等価であることがわかる．し

表 6.1: センター通信量削減型 $(m_D + c_D, m_P, t)$ 構成法と $(m_D, c_D, m_P, *, t)$ 構成法の安全性と記憶容量の比較例 (単位：ビット)

結託センター数	$(20, 1, 2)$	$(13, 7, 1, *, 2)$	$(5, 15, 1, *, 2)$
$\omega \leq 5$	128	128	128
$6 \leq \omega \leq 13$	128	128	120 〜 64
$14 \leq \omega \leq 20$	128	112 〜 16	56 〜 8
$21 \leq \omega$	0	0	0
記憶容量 (ユーザ)	256	256	256
記憶容量 (センター)	384	48	24

たがって，$(m_D, c_D, m_P, *, t)$ KPS は，(m_D, m_P, t) KPS 及び (m_D, m_P, t) KPS' を特別な場合に含む一般的な方式となる．

$(m_D, *, m_P, c_P, t)$ KPS におけるユーザの記憶容量の理論的限界は，定理 6.1 によって示された．この理論的限界は，m_D と c_D の大きさに依らず，(m_D, m_P, t) KPS' におけるユーザの記憶容量の理論的限界と等しい．一方，定理 6.2 によって示されたセンターの記憶容量の理論的限界は，$c_D = 0$ のとき，(m_D, m_P, t) KPS' におけるユーザの記憶容量の理論的限界と一致する．

次に，5.4 節と同様に，4.3 節で提案したセンター通信量削減型 $(m_D + c_D, m_P, t)$ 構成法と 6.3 節で提案した $(m_D, c_D, m_P, *, t)$ 構成法の安全性と記憶容量の比較を行う．これら 2 つの構成法は，両者とも結託センター数が $m_D + c_D + 1$ 以上のとき，鍵の情報が完全に得られる．一方，結託ユーザ数が m_P 以下の場合は，鍵の情報が全く得られないことを保証しているが，$m_P + 1$ 以上の結託数に対しては何も保証されない．すなわち，結託ユーザ数に対しては，段階的に鍵の情報が得られる性質になっていない．更に，ユーザーの記憶容量は m_P に依存しない量となるので，両者の構成法の比較においては，$m_P = 1$ の場合のみについて考える．

表 5.1 は，簡単な比較例として $\mathbb{F}_{2^{128}}$ 上の多項式を用いるセンター通信量削減型 $(20, 1, 2)$ 構成法，$\mathbb{F}_{2^{16}}$ 上の多項式を用いる $(13, 7, 1, *, 2)$ 構成法，及び $\mathbb{F}_{2^8}$ 上の多項式を用いる $(5, 15, 1, *, 2)$ 構成法の安全性と記憶容量を示している．これら 3 つの構成法における鍵の長さおよび鍵のエントロピーは全て 128 ビットとなる．また，結

託ユーザ数は全ての構成法で 1 個以下と仮定する．表 6.1 の 2〜5 行目は，結託センター数 ω に対する各構成法の安全性評価基準である安全度 (条件付エントロピー) を示しており，6 行目と 7 行目はそれぞれ各構成法に対するユーザとセンターの記憶容量を示している（単位は全てビット）．これら 3 つの構成法では，結託センター数が 21 以上になると鍵の情報が完全に得られてしまい，安全度が 0 になる．一方，結託センター数が 20 以下の場合は，全ての構成法において，鍵の情報が完全に得られることはないがしきい値ランプ-しきい値型安全性を満たす $(13, 7, 1, *, 2)$ 構成法と $(5, 15, 1, *, 2)$ 構成法では，それぞれ $14 \leq \omega \leq 20$ と $6 \leq \omega \leq 20$ のときに鍵の情報が部分的に得られる．したがって，部分的に得られる範囲が狭いほど，すなわち，安全性が高いほどセンターの記憶容量が増加することがわかる．一方，ユーザの記憶容量は，全て同じ大きさになる．

以上により，同じ長さの鍵を共有する場合，$(m_D, c_D, m_P, *, t)$ 構成法は部分的に鍵の情報が得られる範囲を許容することで，センター通信量削減型 $(m_D + c_D, m_P, t)$ 構成法よりセンターの記憶容量を $1/(c_D + 1)$ に削減した効率的な構成法となる．また，$(m_D, *, m_P, c_P, t)$ 構成法と同様に，センターの記憶容量を削減することにより，安全性が低下してしまうが，鍵のエントロピーを十分大きくとることで，十分高い安全性を実現できる．

第7章　しきい値ランプ型安全性を満たすt-KPS'

第5章と第6章では，しきい値-しきい値ランプ型安全性を満たすt-KPS'としきい値ランプ-しきい値型安全性を満たすt-KPS'について検討した．これらの安全性は，センターとユーザのどちらか一方の結託数の増加に従って攻撃対象の情報が段階的に得られていく性質であった．本章では，結託センター数と結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られていく性質について検討する．この性質は，結託センターと結託ユーザを独立に考えたとき，結託センター数と結託ユーザ数に対し，それぞれしきい値ランプ型安全性を満たすので，本研究では，この性質をしきい値ランプ型安全性と呼ぶ．

以下では，t-KPS'に要求する制約条件として，完全整合性としきい値ランプ型安全性に対する制約条件を定義し，その制約条件を満たすもとでのt-KPS'における記憶容量の理論的限界の導出，及びその理論的限界を達成する構成法の提案を行う．また，t-KPS'の評価基準は，第4章と同様に(3.3)〜(3.6)とする．

7.1　t-KPS'に要求する制約条件の定義

t-KPS'がしきい値ランプ型安全性を満たすなら，任意のしきい値m_D, c_D, m_P, c_Pに対して，結託数がm_P以下の結託ユーザとm_D以下の結託センターが攻撃しても，結託ユーザが属していない任意のグループの鍵に関する情報が全く得られず，結託ユーザ数がm_P+1からm_P+c_Pかつ結託センター数がm_D+1からm_D+c_Dの場合には，結託ユーザ数と結託センター数が大きくなるにつれて段階的に情報が得られていく．すなわち，結託数がm_P+c_P以下の結託ユーザとm_D+c_D以下の結託センターに対しては，攻撃対象とする鍵の情報が部分的に得られることはあっても，

完全に得られることはない．また，攻撃対象の鍵を共有するグループに，結託ユーザは1人も属さないことになるので，結託ユーザは最大で $n_P - t$ 人まで考えられる．したがってしきい値ランプ型安全性を満たす t-KPS' では，$m_P + c_P \leq n_P - t$ を満たす必要がある．

定義 7.1 t-KPS'への攻撃が，仮定 4.1 を満たすとする．$m_D + c_D < n_D$，$m_P + c_P \leq n_P - t$ を満たす非負整数 m_D, c_D, m_P, c_P, t に対し，定義 3.2 と同様の制約条件 (C1)，及び以下の制約条件 (C5) を満たす t-KPS' を (m_D, c_D, m_P, c_P, t) KPS という．

(C5：しきい値ランプ型安全性) $|\mathcal{X}| \leq m_D + c_D$，$|\mathcal{Y}| \leq m_P + c_P$，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の結託センター $\mathcal{X} \subset \mathcal{D}$ と結託ユーザ $\mathcal{Y} \subset \mathcal{P}$，及び任意のグループ $\mathcal{A}_j \in \mathcal{A}(\mathcal{P}, t)$ に対して，

$$H(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) = \frac{(c_D + 1 - \varphi_{m_D}(|\mathcal{X}|))(c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|))}{(c_D + 1)(c_P + 1)} H(K_j) \tag{7.1}$$

が成立する．ここで，関数 φ_{m_P}, φ_{m_D} は，それぞれ (5.2)，(6.2) の定義と同様とした．　□

7.2　(m_D, c_D, m_P, c_P, t) KPS における記憶容量の理論的限界

本節では，(m_D, c_D, m_P, c_P, t) KPS における各ユーザと各センターの記憶容量，すなわち，$H(U_i), 1 \leq i \leq n_P$ と $H(V_k), 1 \leq k \leq n_D$ の理論的限界を導出する．

センターとユーザの記憶容量の理論的限界を導出するために，以下の補題を用いる．この補題は，補題 4.2 と同様にして導かれる．

補題 7.1 任意の (m_D, c_D, m_P, c_P, t) KPS において，$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P + c_P$, $\mathcal{Y} \cap \mathcal{A}^* = \emptyset$，$\mathcal{Y} \cap \mathcal{A}^*_{j_i} \neq \emptyset, 1 \leq i \leq \eta_{\mathcal{Y}}$ を満たす任意の結託センター $\mathcal{X}$ と結託ユーザ

$\mathcal{Y}$, 及び任意のグループ $\mathcal{A}^*, \mathcal{A}^*_{j_i}$ に対し,

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right)$$
$$\geq \frac{(c_D + 1 - \varphi_{m_D}(|\mathcal{X}|))(c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|))}{(c_D + 1)(c_P + 1)} H(K_j),\ \eta' \leq \eta_{\mathcal{Y}} \quad (7.2)$$

が成立する. □

(**証明**) 制約条件 (C5) より, 任意の (m_D, c_D, m_P, c_P, t) KPS に対して,

$$H(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X}))$$
$$= \frac{(c_D + 1 - \varphi_{m_D}(|\mathcal{X}|))(c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|))}{(c_D + 1)(c_P + 1)} H(K_j) \quad (7.3)$$

が成り立つ. また, 補題 4.2 の証明における (4.16) の導出と同様にして,

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right)$$
$$\geq H(K^* \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})),\ \eta' \leq \eta_{\mathcal{Y}} \quad (7.4)$$

を得る. したがって, (7.3) と (7.4) より,

$$H\left(K^* \mid K^*_{j_1}, K^*_{j_2}, \cdots, K^*_{j_{\eta'}}, V(\mathcal{X}), S(\mathcal{X})\right)$$
$$\geq \frac{(c_D + 1 - \varphi_{m_D}(|\mathcal{X}|))(c_P + 1 - \varphi_{m_P}(|\mathcal{Y}|))}{(c_D + 1)(c_P + 1)} H(K_j),\ \eta' \leq \eta_{\mathcal{Y}} \quad (7.5)$$

を得る. □

7.2.1　ユーザの記憶容量の理論的限界

(m_D, c_D, m_P, c_P, t) KPS におけるユーザの記憶容量 $H(U_i), 1 \leq i \leq n_P$ の理論的限界は, 次の定理として与えられる.

定理 7.1 仮定 3.2 を満たす任意の (m_D, c_D, m_P, c_P, t) KPS において,

$$H(U_i) \geq \sum_{\zeta=0}^{c_P} \binom{m_P + t - 1 + \zeta}{t - 1} \frac{H(K)}{c_P + 1},\ 1 \leq i \leq n_P \quad (7.6)$$

が成立する. □

（**証明**）定理 5.1 の証明における (5.14) の導出と同様にして，

$$H\left(U_i\right) \geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\mu(m_P,t,\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}\right) \tag{7.7}$$

を得る．ここで，(7.7) 右辺の各項に対して，

$$\mathcal{A}^* = \mathcal{A}_{\mu(m_P,t,\zeta-1)+j},\ \mathcal{X} = \emptyset,\ \mathcal{Y} = \mathcal{I}_\zeta^{(i)} \backslash \mathcal{A}_{\mu(m_P,t,\zeta-1)+j},$$

$$\left\{\mathcal{A}_{j_1}^*, \mathcal{A}_{j_2}^*, \cdots, \mathcal{A}_{j_{\eta'}}^*\right\} = \left\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{\mu(m_P,t,\zeta-1)+j-1}\right\}$$

とおくと，$\mathrm{P}_i \notin \mathcal{I}_\zeta^{(i)}$，かつ $\mathrm{P}_i \in \mathcal{A}_{\psi(\zeta-1)+j}$ なので，$\mathcal{Y} \cap \mathcal{A}^* = \emptyset, \mathcal{Y} \cap \mathcal{A}_{j_i}^* \neq \emptyset,\ 1 \leq i \leq \eta'$，$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P + c_P$ が成り立つ．したがって，各項で補題 7.1 がそれぞれ適用でき，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\psi(\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}\right) \\
&= \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} H\left(K_{\psi(\zeta-1)+j} \mid K_1^{\mu(m_P,t,\zeta-1)+j-1}, V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \\
&\geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Psi(m_P,t,\zeta)} \frac{\left(c_D + 1 - \varphi_{m_D}\left(|\mathcal{X}|\right)\right)\left(c_P + 1 - \varphi_{m_P}\left(|\mathcal{Y}|\right)\right)}{(c_D+1)(c_P+1)} H\left(K_{\mu(m_P,t,\zeta-1)+j}\right) \\
&= \sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{c_P+1} H\left(K\right)
\end{aligned} \tag{7.8}$$

を得る．最後の等号は，仮定 3.2 より導かれる．よって，(7.7)，(7.8) より，

$$H\left(U_i\right) \geq \sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{c_P+1} H\left(K\right),\ 1 \leq i \leq n_P \tag{7.9}$$

が成り立つ．また，(7.9) の右辺は，定理 5.1 における (5.20) の導出と同様にすると，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \left(\mu(m_P,t,\zeta) - \mu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{c_P+1} H\left(K\right) \\
&\qquad = \sum_{\zeta=0}^{c_P} \binom{m_P+t-1+\zeta}{t-1} \frac{H\left(K\right)}{c_P+1}
\end{aligned} \tag{7.10}$$

となり，(7.9) と (7.10) から (7.6) を得る．よって，定理が証明された．　□

7.2.2　センターの記憶容量の理論的限界

(m_D, c_D, m_P, c_P, t) KPS におけるセンターの記憶容量 $H(V_k), 1 \leq k \leq n_D$ の理論的限界は，次の定理として与えられる．

定理 7.2 仮定 3.2 を満たす任意の (m_D, c_D, m_P, c_P, t) KPS において，

$$H(V_k) \geq \sum_{\zeta=0}^{c_P} \binom{m_P + t + \zeta}{t} \frac{H(K)}{(c_D+1)(c_P+1)},\ 1 \leq k \leq n_D \tag{7.11}$$

が成立する．　□

（**証明**）まず，定理 5.2 の証明と同様に，任意の集合 $\mathcal{J}_\zeta \subset \mathcal{P},\ 0 \leq \zeta \leq c_P$ に対し，(5.26)，(5.27) によって定められる集合 $\widetilde{\mathcal{N}}(\mathcal{J}_\zeta)$ を定義する．

次に，$\mathrm{D}_k \notin \mathcal{X}^{(k)}, |\mathcal{X}^{(k)}| = m_D + c_D$ を満たす任意の結託センター

$$\mathcal{X}^{(k)} = \left\{\mathrm{D}_{k_1}, \mathrm{D}_{k_2}, \cdots, \mathrm{D}_{k_{m_D+c_D}}\right\} \subset \mathcal{D} \tag{7.12}$$

に対し，定理 5.2 の証明と同様にして，(5.29)，(5.30) と同様の不等式

$$H(V_k) \geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} H\Big(K_{\nu(m_P,t,\zeta-1)+j} \mid K_1^{\nu(m_P,t,\zeta-1)+j-1}, V\big(\mathcal{X}^{(k)}\big), S\big(\mathcal{X}^{(k)}\big)\Big) \tag{7.13}$$

を得る．したがって，(7.13) の右辺の各項に対して，補題 7.1 が適用でき，

$$\begin{aligned}
&\sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} H\Big(K_{\nu(m_P,t,\zeta-1)+j} \mid K_1^{\nu(m_P,t,\zeta-1)+j-1}, V\left(\mathcal{X}^{(k)}\right), S\left(\mathcal{X}^{(k)}\right)\Big) \\
&\quad \geq \sum_{\zeta=0}^{c_P} \sum_{j=1}^{\Phi(m_P,t,\zeta)} \frac{c_P + 1 - \varphi_{m_P}(m_P+\zeta)}{(c_D+1)(c_P+1)} H\left(K_{\nu(m_P,t,\zeta-1)+j}\right) \\
&\quad = \sum_{\zeta=0}^{c_P} \left(\nu(m_P,t,\zeta) - \nu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{(c_D+1)(c_P+1)} H(K)
\end{aligned} \tag{7.14}$$

を得る．よって，(7.13) と (7.14) より，

$$H(V_k) \geq \sum_{\zeta=0}^{c_P} \left(\nu(m_P,t,\zeta) - \nu(m_P,t,\zeta-1)\right) \frac{c_P+1-\zeta}{(c_D+1)(c_P+1)} H(K),\ 1 \leq k \leq n_D \tag{7.15}$$

が成り立つ．(7.15) の右辺は，(5.34) と同様に考えると，

$$\sum_{\zeta=0}^{c_P} \left(\nu(m_P,t,\zeta)-\nu(m_P,t,\zeta-1)\right)\frac{c_P+1-\zeta}{c_P+1}H\left(K\right)$$

$$=\sum_{\zeta=0}^{c_P}\binom{m_P+t+\zeta}{t}\frac{H\left(K\right)}{(c_D+1)(c_P+1)} \tag{7.16}$$

となり，(7.15) と (7.16) から (7.11) を得る．よって，定理が証明された．　□

7.3　最適な (m_D, c_D, m_P, c_P, t) KPS の構成法

本節では，前節で導出したユーザとセンターの記憶容量の理論的限界を達成し，(m_D, c_D, m_P, c_P, t) KPS を実現する最適な構成法を提案する．また，本研究では簡単のため，この構成法を (m_D, c_D, m_P, c_P, t) 構成法と呼ぶことにする．提案する構成法は，6.3 節で提案した $(m_D, c_D, m_P, *, t)$ 構成法をサブルーチンとして用いる．

$0 \le \zeta \le c_P$ に対して，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, c_D, m_P+\zeta, *, t)$ 構成法の各情報，及び秘密情報の確率関数を次のように表す．ただし，各センター及び各ユーザの ID 情報は ζ に依らず同じ値とする．

- 秘密情報：$s_k^{(\zeta)}$, $1 \le k \le m_D + c_D + 1$.
- センター間通信情報：$v_{k,k'}^{(\zeta)}$, $1 \le k \le m_D + c_D + 1$, $1 \le k' \le n_D$.
- センター記憶情報：$v_k^{(\zeta)}$, $1 \le k \le n_D$.
- ユーザ受信情報：$u_{ij,i}^{(\zeta)}$, $1 \le i \le n_P$, $1 \le j \le m_D + c_D + 1$.
- ユーザ記憶情報：$u_i^{(\zeta)}$, $1 \le i \le n_P$.
- グループ $\mathcal{A}_j$ の鍵：$k_j^{(\zeta)}$, $1 \le j \le \binom{n_P}{t}$.
- 確率関数：$p_S^{(\zeta)}(s^{(\zeta)})$.

次に，$\mathbb{F}_q$ 上の多項式を用いる (m_D, c_D, m_P, c_P, t) 構成法を示す．t-KPS' の公開情報である ID 情報，各集合，及び確率関数を次のようにおく．

$$\mathcal{K} = \mathbb{F}_{q^{(c_D+1)(c_P+1)}}, \tag{7.17}$$

$$\mathcal{S} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}(m_D+c_D+1)\binom{m_P+t+\zeta}{t}}, \tag{7.18}$$

$$\mathcal{V} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}\binom{m_P+t+\zeta}{t}}, \tag{7.19}$$

$$\mathcal{U} = \mathbb{F}_q^{\sum_{\zeta=0}^{c_P}\binom{m_P+t-1+\zeta}{t-1}}, \tag{7.20}$$

$$p_S(s) = \prod_{\zeta=0}^{c_P} p_S^{(\zeta)}\left(s^{(\zeta)}\right). \tag{7.21}$$

更に，適当な全単射の写像 $\pi_3 : \mathbb{F}_{q^{c_D+1}}^{c_P+1} \to \mathbb{F}_{q^{(c_D+1)(c_P+1)}}$ も公開情報とする．このとき，(m_D, c_D, m_P, c_P, t) 構成法における各情報は，次のように表される．

$$s_k = \left(s_k^{(0)}, s_k^{(1)}, \cdots, s_k^{(c_P)}\right) \in \mathcal{S},\ 1 \le k \le m_D + c_D + 1, \tag{7.22}$$

$$v_{k,k'} = \left(v_{k,k'}^{(0)}, v_{k,k'}^{(1)}, \cdots, v_{k,k'}^{(c_P)}\right) \in \mathcal{V},\ 1 \le k \le m_D + c_D + 1,\ 1 \le k' \le n_D, \tag{7.23}$$

$$v_k = \left(v_k^{(0)}, v_k^{(1)}, \cdots, v_k^{(c_P)}\right) \in \mathcal{V},\ 1 \le k \le n_D, \tag{7.24}$$

$$u_{i_j,i} = \left(u_{i_j,i}^{(0)}, u_{i_j,i}^{(1)}, \cdots, u_{i_j,i}^{(c_P)}\right) \in \mathcal{U},\ 1 \le i \le n_P,\ 1 \le j \le m_D + c_D + 1, \tag{7.25}$$

$$u_i = \left(u_i^{(0)}, u_i^{(1)}, \cdots, u_i^{(c_P)}\right) \in \mathcal{U},\ 1 \le i \le n_P, \tag{7.26}$$

$$k_j = \pi_3\left(k_j^{(0)}, k_j^{(1)}, \cdots, k_j^{(c)}\right) \in \mathcal{K},\ 1 \le j \le \binom{n_P}{t}. \tag{7.27}$$

$(m_D, c_D, m_P + \zeta, *, t)$ 構成法の性質から，(m_D, c_D, m_P, c_P, t) KPS の構成法に対して，以下の定理が導かれる．

定理 7.3 (m_D, c_D, m_P, c_P, t) 構成法は，定義 7.1 の (m_D, c_D, m_P, c_P, t) KPS を実現し，ユーザ及びセンターの記憶容量が，それぞれ定理 7.1 及び定理 7.2 の理論的限界を達成する．□

（**証明**）定理 5.3 より，グループ $\mathcal{A}_j$ のユーザーは同じ $k_j^{(\zeta)}, 0 \le \zeta \le c_P$ を共有できる．また，(m_D, c_D, m_P, c_P, t) 構成法で用いる写像 π_3 が全単射であることから，

グループの鍵 k_j もグループ内のユーザー間で共有することができる．したがって，(m_D, c_D, m_P, c_P, t) 構成法は，制約条件 (C1) を満たす．

(m_D, c_D, m_P, c_P, t) 構成法では，$0 \leq \zeta \leq c_P$ に対して，$(m_D, c_D, m_P + \zeta, t)$ 構成法が独立に実行されるので，$|\mathcal{X}| \leq m_D + c_D$, $|\mathcal{Y}| \leq m_P + c_P$，$\mathcal{Y} \cap \mathcal{A}_j = \emptyset$ を満たす任意の集合 $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}_j$ に対して，

$$\begin{aligned} & H\left(K_j^{(\zeta)} \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})\right) \\ &= \begin{cases} 0 & \text{for } \zeta < \varphi_{m_P}(|\mathcal{Y}|) \\ \frac{c_D+1-\varphi_{m_D}(|\mathcal{X}|)}{c_D+1} H\left(K_j^{(\zeta)}\right) & \text{for } \zeta \geq \varphi_{m_P}(|\mathcal{Y}|) \end{cases} \end{aligned} \tag{7.28}$$

が成り立つ．ここで，$k_j^{(\zeta)}$ に対応する確率変数を $K_j^{(\zeta)}$ とした．また，(m_D, c_D, m_P, c_P, t) 構成法で用いる写像 π_3 は全単射なので，

$$H(K_j) = \sum_{\zeta=0}^{c_P} H\left(K_j^{(\zeta)}\right) \tag{7.29}$$

が成り立つ．よって，

$$\begin{aligned} H(K_j \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})) &= \sum_{\zeta=0}^{c_P} H\left(K_j^{(\zeta)} \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})\right) \\ &= \sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)} \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})\right) \\ &\quad + \sum_{\zeta'=0}^{\varphi_{m_P}(|\mathcal{Y}|)-1} H\left(K_j^{(\zeta')} \mid U(\mathcal{Y}), V(\mathcal{X}), S(\mathcal{X})\right) \\ &= \frac{c_D + 1 - \varphi_{m_D}(|\mathcal{X}|)}{c_D + 1} \sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)}\right) \end{aligned} \tag{7.30}$$

を得る．確率変数 $K_j^{(\zeta)}, 0 \leq \zeta \leq c_P$ は互いに独立かつ $\mathbb{F}_{q^{c_D+1}}$ 上で一様に分布するので，任意のグループ $\mathcal{A}_j$ に対して，

$$H\left(K_j^{(\zeta)}\right) = \log q^{c_D+1} \tag{7.31}$$

を得る．したがって，

$$\begin{aligned}\sum_{\zeta=\varphi_{m_P}(|\mathcal{Y}|)}^{c_P} H\left(K_j^{(\zeta)}\right) &= \left(c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)\right)\log q^{c_D+1} \\ &= \frac{\left(c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)\right)\left(c_P+1\right)}{c_P+1}\log q^{c_D+1} \\ &= \frac{c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)}{c_P+1}H\left(K_j\right) \qquad (7.32)\end{aligned}$$

となり，(7.30) と (7.32) から，

$$\begin{aligned}&H\left(K_j \mid U\left(\mathcal{Y}\right), V\left(\mathcal{X}\right), S\left(\mathcal{X}\right)\right) \\ &\quad= \frac{\left(c_D+1-\varphi_{m_D}(|\mathcal{X}|)\right)\left(c_P+1-\varphi_{m_P}\left(|\mathcal{Y}|\right)\right)}{\left(c_D+1\right)\left(c_P+1\right)}H\left(K_j\right) \qquad (7.33)\end{aligned}$$

を得る．したがって，(m_D, c_D, m_P, c_P, t) 構成法は，制約条件 (C5) を満たす．

$\mathbb{F}_q$ 上の多項式を用いる (m_D, c_D, m_P, c_P, t) 構成法は，$0 \le \zeta \le c_P$ に対して，$\mathbb{F}_q$ 上の多項式を用いる $(m_D, c_D, m_P+\zeta, *t)$ 構成法を独立に実行する構成法なので，$(m_D, c_D, m_P+\zeta, *, t)$ 構成法 $(0 \le \zeta \le c_P)$ におけるユーザ及びセンターの記憶容量の合計が，(m_D, c_D, m_P, c_P, t) 構成法におけるユーザ及びセンターの記憶容量となる．$(m_D, c_D, m_P+\zeta, *, t)$ 構成法におけるユーザ及びセンターの記憶容量は，それぞれ，

$$\begin{aligned}\binom{m_P+t-1+\zeta}{t-1}\log q^{c_D+1} &= \binom{m_P+t-1+\zeta}{t-1}\frac{c_P+1}{c_P+1}\log q^{c_D+1} \\ &= \binom{m_P+t-1+\zeta}{t-1}\frac{H\left(K\right)}{c_P+1}, \qquad (7.34) \\ \binom{m_P+t+\zeta}{t}\frac{\log q^{c_D+1}}{c_D+1} &= \binom{m_P+t+\zeta}{t}\frac{c_P+1}{c_P+1}\cdot\frac{\log q^{c_D+1}}{c_D+1} \\ &= \binom{m_P+t+\zeta}{t}\frac{H\left(K\right)}{(c_D+1)(c_P+1)} \qquad (7.35)\end{aligned}$$

となる．したがって，$\mathbb{F}_q$ 上の多項式を用いる (m_D, c_D, m_P, c_P, t) 構成法に対する，

ユーザー及びセンターの記憶容量は，それぞれ

$$H(U_i) = \sum_{\zeta=0}^{c_P} \binom{m_P+t-1+\zeta}{t-1} \frac{H(K)}{c_P+1},\ 1 \le i \le n_P, \tag{7.36}$$

$$H(V_k) = \sum_{\zeta=0}^{c_P} \binom{m_P+t+\zeta}{t} \frac{H(K)}{(c_D+1)(c_P+1)},\ 1 \le k \le n_D \tag{7.37}$$

となり，定理 7.1 及び定理 7.2 の理論的限界とそれぞれ一致する．

以上により，定理が証明された．　□

7.4　比較・考察

定義 7.1 で定義した (m_D, c_D, m_P, c_P, t) KPS において，$c_D = 0$ のとき制約条件 (C3) と (C5) が等価となり，$c_P = 0$ のとき制約条件 (C4) と (C5) が等価となる．また，$c_D = c_P = 0$ のときは，制約条件 (C2) と (C5) が等価となる．したがって，(m_D, c_D, m_P, c_P, t) KPS は，これまでに定義した (m_D, m_P, t) KPS，(m_D, m_P, t) KPS'，$(m_D, *, m_P, c_P, t)$ KPS，$(m_D, c_D, m_P, *, t)$ KPS の全てを特別な場合に含む一般的な方式となる．

(m_D, c_D, m_P, c_P, t) KPS におけるユーザの記憶容量の理論的限界は，定理 7.1 によって示された．この理論的限界は，m_D と c_D の大きさに依らず，定理 5.1 で示した $(m_D, *, m_P, c_P, t)$ KPS におけるユーザの記憶容量の理論的限界と一致する．また，$c_P = 0$ のときは，定理 4.1 で示した (m_D, m_P, t) KPS' におけるユーザの記憶容量の理論的限界と一致する．一方，定理 7.2 によって示された，(m_D, c_D, m_P, c_P, t) KPS におけるセンターの記憶容量の理論的限界は，$c_D = 0$ のとき，定理 5.2 で示した $(m_D, *, m_P, c_P, t)$ KPS におけるセンターの記憶容量の理論的限界と一致し，$c_P = 0$ のとき，定理 6.2 で示した $(m_D, c_D, m_P, *, t)$ KPS におけるセンターの記憶容量の理論的限界と一致する．また，$c_D = c_P = 0$ のときは，定理 4.2 で示した (m_D, m_P, t) KPS' におけるセンターの記憶容量の理論的限界と一致する．以上より，(m_D, c_D, m_P, c_P, t) KPS におけるユーザとセンターの記憶容量の理論的限界は，(m_D, m_P, t) KPS，(m_D, m_P, t) KPS'，$(m_D, *, m_P, c_P, t)$ KPS，及び $(m_D, c_D, m_P, *, t)$

KPS の全てにおけるユーザとセンターの理論的限界を，それぞれ特別な場合として含む最も一般的な結果になっている．

次に，5.4 節及び 6.4 節と同様に，センター通信量削減型 $(m_D + c_D, m_P + c_P, t)$ 構成法と，7.3 節で提案した，(m_D, c_D, m_P, c_P, t) 構成法の安全性と記憶容量の比較を行う．

表 7.1: センター通信量削減型 $(m_D + c_D, m_P + c_P, t)$ 構成法と (m_D, c_D, m_P, c_P, t) 構成法の安全性の比較例 (単位：ビット)

	$\omega_2 \leq 13$	$14 \leq \omega_2 \leq 20$	$21 \leq \omega_2$
$\omega_1 \leq 13$	$H_{(20,20)} = 128$ $H_{(20,0,13.7)} = 128$ $H_{(13,7,20,0)} = 128$ $H_{(13,7,13,7)} = 128$	$H_{(20,20)} = 128$ $16 \leq H_{(20,0,13.7)} \leq 112$ $H_{(13,7,20,0)} = 128$ $16 \leq H_{(13,7,13,7)} \leq 112$	$H_{(20,20)} = 0$ $H_{(20,0,13.7)} = 0$ $H_{(13,7,20,0)} = 0$ $H_{(13,7,13,7)} = 0$
$14 \leq \omega_1 \leq 20$	$H_{(20,20)} = 128$ $H_{(20,0,13.7)} = 128$ $16 \leq H_{(13,7,20,0)} \leq 112$ $16 \leq H_{(13,7,13,7)} \leq 112$	$H_{(20,20)} = 128$ $16 \leq H_{(20,0,13.7)} \leq 112$ $16 \leq H_{(13,7,20,0)} \leq 112$ $2 \leq H_{(13,7,13,7)} \leq 98$	$H_{(20,20)} = 0$ $H_{(20,0,13.7)} = 0$ $H_{(13,7,20.0)} = 0$ $H_{(13,7,13,7)} = 0$
$21 \leq \omega_2$	$H_{(20,20)} = 0$ $H_{(20,0,13.7)} = 0$ $H_{(13,7,20.0)} = 0$ $H_{(13,7,13,7)} = 0$	$H_{(20,20)} = 0$ $H_{(20,0,13.7)} = 0$ $H_{(13,7,20.0)} = 0$ $H_{(13,7,13,7)} = 0$	$H_{(20,20)} = 0$ $H_{(20,0,13.7)} = 0$ $H_{(13,7,20.0)} = 0$ $H_{(13,7,13,7)} = 0$

表 7.1 は，簡単な比較例として $\mathbb{F}_{2^{128}}$ 上の多項式を用いるセンター通信量削減型 $(20, 20, 2)$ 構成法，$\mathbb{F}_{2^{16}}$ 上の多項式を用いる $(20, 0, 13, 7, 2)$ 構成法と $(13, 7, 20, 0, 2)$ 構成法，$\mathbb{F}_2$ 上の多項式を用いる $(13, 7, 13, 7, 2)$ 構成法における，ユーザとセンターの各結託数に対する安全度の変化を示している．ここで，結託センター数を ω_1，結託ユーザ数を ω_2 とおき，センター通信量削減型 $(20, 20, 2)$ 構成法，$(20, 0, 13, 7, 2)$ 構成法，$(13, 7, 20, 0, 2)$ 構成法，$(13, 7, 13, 7, 2)$ 構成法の安全度を，それぞれ $H_{(20,20,2)}$, $H_{(20,0,13,7,2)}$, $H_{(13,7,20,0,2)}$, $H_{(13,7,13,7,2)}$ とした．これら 4 つの構成法では，センターとユーザの結託数のどちらかが 21 以上になると鍵の情報が完全に得られるので安全度

が 0 になる．一方，センターとユーザの結託数が共に 20 以下の場合は，全ての構成法において，鍵の情報が完全に得られることはないがしきい値ランプ型安全性を満たす構成法では，センターとユーザの結託数のどちらかが $14 \leq \omega \leq 20$ のときに鍵の情報が部分的に得られる．また，鍵の情報が部分的に得られる範囲は，$(13, 7, 13, 7, 2)$ 構成法が最も広くなっている．

表 7.2: センター通信量削減型 $(m_D + c_D, m_P + c_P, t)$ 構成法と (m_D, c_D, m_P, c_P, t) 構成法の記憶容量の比較例 (単位：ビット)

	$(20, 20, 2)$	$(20, 0, 13, 7, 2)$	$(7, 13, 20, 0, 2)$	$(7, 13, 7, 13, 2)$
ユーザの記憶容量	2688	2240	2688	2240
センターの記憶容量	29568	21056	3696	2632

表 7.2 は，表 7.1 の例と同様の構成法におけるセンターとユーザの記憶容量を示している．センターとユーザの記憶容量は，共にセンター通信量削減型 $(20, 20, 2)$ 構成法が最も大きく，$(13, 7, 13, 7, 2)$ 構成法が最も小さくなる．したがって，鍵の情報が部分的に得られる範囲が狭いほど，すなわち，安全性が高いほど各記憶容量は増加する．特に，センターの記憶容量の増加が膨大になる．

以上により，同じ長さの鍵を共有する場合，(m_D, c_D, m_P, c_P, t) 構成法は部分的に鍵の情報が得られる範囲を許容することで，センター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法より記憶容量を削減した効率的な構成法となる．特に，センターの記憶容量を大幅に削減できる．また，$(m_D, *, m_P, c_P, t)$ 構成法や，$(m_D, c_D, m_P, *, t)$ 構成法と同様に，記憶容量を削減することにより，安全性が低下してしまうが，鍵のエントロピーを十分大きくとることで，十分高い安全性を実現できる．

第8章　結論

8.1　まとめ

本研究では，情報量的に安全な鍵事前配布方式に対して，センター間の総通信量の削減と安全性の拡張を行った．安全性の拡張に対しては，従来のしきい値型安全性から次の 3 つの性質への拡張を検討した．

- ユーザの結託数の増加に従って，攻撃対象の情報が段階的に得られるという性質．
- センターの結託数の増加に従って，攻撃対象の情報が段階的に得られるという性質．
- センター及びユーザそれぞれの結託数の増加に従って，攻撃対象の情報が段階的に得られるという性質．

第 4 章では，まずセンターの総通信量を削減するために従来の t 会議鍵事前配布方式 (t-KPS) を拡張したセンター間通信量削減型 t 会議鍵事前配布方式 (t-KPS') を提案し，t-KPS' に要求する制約条件として，従来と同様の完全整合性としきい値型安全性に対する制約条件を与えた (m_D, m_P, t) KPS' を定義した．この (m_D, m_P, t) KPS' に対して，センターとユーザの記憶容量の理論的限界を導出し，従来の (m_D, m_P, t) KPS における理論的限界と等価となることを示した．更に，この理論的限界を達成する最適なセンター通信量削減型 (m_D, m_P, t) 構成法を提案した．提案したセンター通信量削減型 (m_D, m_P, t) 構成法は，従来の (m_D, m_P, t) 構成法と同様の記憶容量と安全性を達成し，かつセンター間の総通信量を削減した構成法となる．

第 5 章では，しきい値型安全性を結託ユーザ数の増加に従って攻撃対象の情報が段階的に得られるという性質に拡張したしきい値-しきい値ランプ型安全性を検討し，

t-KPS' に要求する制約条件として，従来のしきい値型安全性からしきい値-しきい値ランプ型安全性に対する制約条件に拡張した $(m_D, *, m_P, c_P, t)$ KPS を定義した．$(m_D, *, m_P, c_P, t)$ KPS は，従来の (m_D, m_P, t) KPS，及び (m_D, m_P, t) KPS' を特別な場合に含む一般的な定義となることを示した．次に，$(m_D, *, m_P, c_P, t)$ KPS に対する，センターとユーザの記憶容量の理論的限界を導出し，導出した理論的限界を達成する最適な $(m_D, *, m_P, c_P, t)$ 構成法を提案した．この $(m_D, *, m_P, c_P, t)$ 構成法は，結託ユーザ数に対し部分的に鍵の情報が得られる範囲を許容することで，従来の $(m_D, m_P + c_P, t)$ 構成法やセンター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法よりセンターとユーザの記憶容量を削減することができる．

第 6 章では，第 5 章のしきい値-しきい値ランプ型安全性とは異なる性質として，しきい値型安全性を結託センタ数の増加に従って攻撃対象の情報が段階的に得られるという性質に拡張したしきい値ランプ-しきい値型安全性を検討し，t-KPS' に要求する制約条件として，従来のしきい値型安全性からしきい値ランプ-しきい値型安全性に対する制約条件に拡張した $(m_D, *, m_P, c_P, t)$ KPS を定義した．$(m_D, *, m_P, c_P, t)$ KPS は，従来の (m_D, m_P, t) KPS，及び (m_D, m_P, t) KPS' を特別な場合に含む一般的な定義となる．次に，$(m_D, c_D, m_P, *, t)$ KPS に対する，センターとユーザの記憶容量の理論的限界を導出し，導出した理論的限界を達成する最適な $(m_D, c_D, m_P, *, t)$ 構成法を提案した．この $(m_D, c_D, m_P, *, t)$ 構成法は，センターの結託数に対し部分的に鍵の情報が得られる範囲を許容することで，従来の $(m_D, m_P + c_P, t)$ 構成法やセンター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法よりセンターの記憶容量をを $1/(c_D + 1)$ に削減することができる．

第 7 章では，結託センター及び結託ユーザそれぞれの結託数の増加に従って情報が段階的に得られていく安全性に拡張したしきい値ランプ型安全性を検討し，t-KPS' に要求する制約条件として，従来のしきい値型安全性からしきい値ランプ型安全性に対する制約条件に拡張した (m_D, c_D, m_P, c_P, t) KPS を定義した．(m_D, c_D, m_P, c_P, t) KPS は，(m_D, m_P, t) KPS，(m_D, m_P, t) KPS'，$(m_D, *, m_P, c_P, t)$ KPS，$(m_D, c_D, m_P, *, t)$ KPS の全てを特別な場合に含む最も一般的な方式となる．次に，(m_D, c_D, m_P, c_P, t) KPS に対する，センターとユーザの記憶容量の理論的限界を導出し，導出した理論的限界を達成する最適な (m_D, c_D, m_P, c_P, t) 構成法を提案した．この (m_D, c_D, m_P, c_P, t) 構成法は，センター及びユーザの結託数に対し，部分的に鍵の情報が得られる範囲を

許容することで，従来の $(m_D, m_P + c_P, t)$ 構成法やセンター通信量削減型 $(m_D, m_P + c_P, t)$ 構成法よりセンター及びユーザの記憶容量を削減することができる．特に，センターの記憶容量を大幅に削減できることがわかった．

8.2 今後の展望

本研究では，情報量的に安全な鍵事前配布方式である t-KPS' に要求する安全性として，しきい値型安全性，しきい値-しきい値ランプ型安全性，しきい値ランプ-しきい値型安全性，しきい値ランプ型安全性を導入し，それぞれの性質を満たす t-KPS' におけるセンターとユーザの記憶容量の理論的限界を導出した．しかし，センター間の通信量やセンターとユーザ間の通信量に対する理論的限界が導出されていないため，本研究で提案した各構成法に対する通信量の最適性が保証されていないが，センター間の通信量とセンターとユーザ間の通信量に対する理論的限界の導出は，今後の課題の 1 つとしたい．

また，本研究で提案した構成法は，記憶容量の最適性は保証されるが，多くの有限体上の演算が必要となるため，IC カード等の計算能力が低いデバイスに実装する場合には，鍵の生成に時間がかかってしまうといった実用上の問題が生じてしまう．この問題を解決するためには，線形演算のみを用いる構成法や XOR 演算のみを用いる構成法の実現性を検討する必要があるが，この検討については今後の課題の 1 つとしたい．

参考文献

[1] A. Beimel, and B. Chor, "Communication in key distribution schemes," IEEE Trans. Information Theory, vol.42, no.1, pp.19–28, Jan. 1996.

[2] G. R. Blakley, and C. Meadows, "Security of ramp scheme," Proc. CRYPT'84, Lecture Notes in Computer Science, vol.196, pp.242–268, 1984.

[3] R. Blom, "An optimal class of symmetric key generation systems," Proc. EUROCRYPT'84, Lecture Notes in Computer Science, vol.209, pp.335–338, 1985.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly secure key distribution for dynamic conference," Information and Computation, vol.146, no.1, pp.1–23, 10 October 1998.

[5] C. Blundo, P. D'Arco, and C. Padró, "A ramp model for distributed key distribution schemes," Discrete Applied Mathematics, vol.128, pp.47–64, 2003.

[6] C. H. Bennett, and G. Brassard, "Quantum Cryptography: Public Key Distribution andCoin Tossing," in Proc. of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179, 1984.

[7] C. H. Bennet, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. 68, 3121–3124, 1992.

[8] T.M. Cover, and J.A. Thomas, Elements of Information Theory, 2nd Edition, Wiley-Interscience, 2006.

[9] P. D'Arco, "On the distribution of a key distribution center," Proc. ICTCS '01, Lecture Notes in Computer Science, vol.2202, pp.357–369, 2001.

[10] W. Diffie, and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Information Theory, vol.22, no.6, pp.644–654, Nov. 1976.

[11] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. 67, pp.661–663, 1991.

[12] T. Elgamal, “A public-Key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Information Theory, vol.31, no.4, pp.469–472, 1985.

[13] S. Goldwasser, and S. Micali, “Probabilistic encryption,” Journal of Computer and System Sciences, vol.28, no.2, pp.270–299, 1984.

[14] E. D. Karnin, J. W. Greene, and M. E. Hellman “On secret sharing systems,” IEEE Trans. Information Theory, vol.29, no.1, pp.35–41, Jan. 1983.

[15] J. Katz, and Y. Lindell, Introduction to modern cryptography: principles and protocols, Chapman & Hall, 2007.

[16] N. Koblitz, “Elliptic curves in cryptography,” Mathematics of Computation, vol.48, no.177, pp.203–209, 1987.

[17] J. Kohl, and C. Neuman, The Kerboros network authentication service, Network working group, Network working group request for comments: 1510, Sept. 1993.

[18] K. Kurosawa, K. Okada, and K. Sakano, “Security of the center in key distribution schemes,” Proc. ASIACRYPT’94, Lecture Notes in Computer Science, vol.917, pp.333–341, 1994.

[19] 松本勉，今井秀樹,“ 暗号鍵を通信なしで共有する方法，”電子情報通信学会論文誌 (A)，vol.J71-A，no.11，pp.2046-2053，1988.

[20] S. Micali, C. Rackoff, and B. Sloan, “The notion of security for probabilistic cryptosystems,” SIAM Journal on Computing, vol.17, no.2, pp.412–426, 1988.

[21] V. S. Miller, “Use of elliptic curves in cryptography,” Proc. Crypto’85, Lecture Notes in Computer Science, vol.218, pp.417–426, 1985.

[22] M. Naor, B. Pinkas, and O. Reingold, “Distributed pseudo-random functions and KDCs,” Proc. EUROCRYPT’99, Lecture Notes in Computer Science, vol.1592, pp.327–346, 1999.

[23] E. Okamoto, and K. Tanaka, “Identity-Based Information Security Management System for Personal Computer Networks,” Journal on Selected Areas in Communication, The Institute of Electrical and Electronics Engineers, vol.7, no.2, pp.290–294, 1989.

[24] 岡本龍明, 山本博資, 現代暗号, 産業図書, 1997.

[25] R. L. Rivest, A. Shamir, and L. M. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol.21, no.2, pp.120–126, 1978.

[26] A. Shamir, “How to share a secret,” Communications of the ACM, vol.22, no.11, pp.612–613, 1979.

[27] C. Shannon, ”Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28(4), pp.656–715, 1949.

[28] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, pp.124–134, 1994.

[29] D.R. Stinson, Cryptography: Theory And Practice, Chapman & Hall, 2005.

[30] S. Tsujii, K. Araki, M. Kasahara, E. Okamoto, R. Sakai, Y. Maeda, and T. Yagisawa, “On Ambiguity in Coppersmith’ Attacking Method against NIKS-TAS Scheme,” IEICE Trans. Fundamentals, vol.E79-A, no.1, pp.66–75, 1996.

[31] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” Journal of the American Institute of Electrical Engineers, vol.55, pp.109–115, 1926.

[32] S. Wiesner, “Conjugate coding,” ACM SIGACT News, vol.15, no,1, pp.78–88, 1983.

[33] 山本博資, “(k, L, n) しきい値秘密分散システム,” 電子情報通信学会論文誌, vol.J68-A, no.9, pp.945–952, 1985.

謝辞

本論文をまとめるにあたり主査として御指導頂いた，早稲田大学応用数理学科松嶋敏泰教授に心より感謝いたします．大学院進学以来 10 年余り，松嶋教授には研究はもとより，教育や仕事，社会人としての姿勢など数え切れないほど多くの有益な御指導，御助言を賜りました．

また，副査として大変貴重な御時間を賜り御指導頂いた，早稲田大学平澤茂一名誉教授，早稲田大学応用数理学科大石進一教授に深く感謝いたします．特に平澤教授には，大学院進学以来の長きに亘り，研究の細部に及ぶ適確な御指導，御助言を頂きました．

中央大学今井秀樹教授には，本論文をまとめるにあたり格別の御支援と御協力を賜り，心より御礼申し上げます．

武蔵工業大学俵信彦名誉教授には，著者が研究の道に進むきっかけを与えて戴き，以来 15 年，様々な御指導，御助言を頂きました．改めて御礼申し上げます．

また，早稲田大学後藤正幸准教授，横浜商科大学浮田善文准教授，北見工業大学前田康成助教，専修大学野村亮講師，日本電気株式会社峯松一彦氏，青山学院大学斎藤友彦助手，サイバー大学小泉大城助手，早稲田大学須子統太助教，早稲田大堀井俊佑助手の各氏には，数多くの御支援，御協力を賜り，深く感謝申し上げます．

本論文は以上をはじめとする，多くの方々の御指導，御支援の賜物です．お世話になった方々に心より御礼申し上げます．最後に，著者の研究生活に理解を示し支えてくれた，妻，父，母ら家族に心より感謝いたします．

2010 年 7 月

研究業績

種類別	題名，　発表掲載誌名，　　発表発行年月，　著者
1. ○論文	複数の鍵配送センターを用いたランプ型鍵事前配布方式 電子情報通信学会論文誌 A，Vol.J93-A, No.4, pp.277-288, (2010-4) 吉田隆弘，松嶋敏泰，今井秀樹
2. ○論文	A ramp scheme for key predistribution system against collusion of users and centers Proceeding of 2008 International Symposium on Information Theory and its Applications, (2008-12) Takahiro Yoshida, Toshiyasu Matsushima, and Hideki Imai
3.　論文	Achievable rates of random number generators for an arbitrary prescribed distribution from an arbitrary given distribution Proceedings of IEEE International Symposium on Information Theory, p.155, (2000-6) Takahiro Yoshida, Toshiyasu Matsushima, and Shigeichi Hirasawa
4.　論文	A universal code considering the codeword cost Proceedings of International Symposium on Information Theory and Its Applications, pp.165-168, (1998-10) Takahiro Yoshida, Toshiyasu Matsushima, and Shigeichi Hirasawa
5.　論文	共役勾配法における探索効率向上法に関する一考察 日本経営工学会論文誌, Vol.48, No.5, pp.257-263, (1997-12) 吉田隆弘，後藤正幸，俵信彦

種類別	題名，　発表掲載誌名，　　発表発行年月，　著者
6.　論文	KL 情報量を制約とした Resolvability 問題における達成可能条件の評価 電子情報通信学会論文誌 A，Vol.J93-A, No.3, pp.216-221, (2010-3) 野村亮，吉田隆弘，松嶋敏泰
7.　論文	Bounds on the number of users for random 2-secure codes Proceedings of 18th Symposium on Applied algebra, Algebraic algorithms and Error Correcting Codes (AAECC-18), Lecture Notes In Computer Science Vol. 5527, pp.239-242, (2009-6) Manabu Hagiwara, Takahiro Yoshida, and Hideki Imai
8.　講演	相互通信可能な情報源符号化に関する一研究 第 29 回情報理論とその応用シンポジウム予稿集, pp.355-358, (2006-12) 吉田隆弘，松嶋敏泰，平澤茂一
9.　講演	ID 情報に基づくランプ型分散鍵配送方式について 第 27 回情報理論とその応用シンポジウム予稿集, pp.327-360, (2004-12) 吉田隆弘，松嶋敏泰，平澤茂一
10.　講演	ランプ型鍵配送方式について 電子情報通信学会技術報告, ISEC2004-11, pp.69-74, (2004-5) 吉田隆弘，松嶋敏泰，平澤茂一
11.　講演	多端子情報源符号化に基づいた分散協調問題の定式化について 電子情報通信学会技術報告 IT2004-22，pp.23-28，(2004-7) 吉田隆弘，松嶋敏泰，平澤茂一
12.　講演	情報システム演習の実績報告 2002 PC カンファレンス論文集, (2002-8) 吉田隆弘，小林学，平澤茂一
13.　講演	多端子情報理論に基づく分散協調問題について 第 24 回情報理論とその応用シンポジウム予稿集, pp.367-370, (2001-12) 吉田隆弘，松嶋敏泰，平澤茂一
14.　講演	多端子モデルに基づく分散協調問題の定式化について 電子情報通信学会技術報告, IT2001-17, pp.37-42, (2001-7) 吉田隆弘，松嶋敏泰，平澤茂一

種類別	題名，　発表掲載誌名，　　発表発行年月，　著者
15. 講演	コスト付き情報源符号化定理について 第 22 回情報理論とその応用シンポジウム予稿集, pp.57-60, (1999-12) 吉田隆弘，松嶋敏泰，平澤茂一
16. 講演	符号語コストを考慮した情報源符号化について 日本経営工学会 平成 10 年度春季大会予稿集, (1998-5) 吉田隆弘，後藤正幸，俵信彦
17. 講演	共役勾配法における探索効率向上法について 日本経営工学会 平成 8 年度春季大会予稿集, (1996-5) 吉田隆弘，後藤正幸，俵信彦
18. 講演	電波伝搬の特性を利用した鍵共有方式の情報量的安全性評価 2010 年暗号と情報セキュリティシンポジウム (SCIS2010) 予稿集，(2010-1) 松永雄斗，吉田隆弘，萩原学，古原和邦，今井秀樹
19. 講演	情報理論的に安全なリング署名方式 2010 年暗号と情報セキュリティシンポジウム (SCIS2010) 予稿集，(2010-1) 千葉慎平，吉田隆弘，今井秀樹
20. 講演	電力解析攻撃の体系的な分類と比較について 2010 年暗号と情報セキュリティシンポジウム (SCIS2010) 予稿集，(2010-1) 野口正俊，堀洋平，吉田隆弘，今井秀樹
21. 講演	情報理論的に安全な鍵無効化機能付きメッセージ秘匿・認証方式 電子情報通信学会技術報告，IT2008-90，ISEC2008-148，WBS2008-103，pp.301-306, (2009-3) 千葉慎平，吉田隆弘，ナッタポンアッタラパドゥン，今井秀樹
22. 講演	電波の相反性を用いた鍵共有方式における情報量的安全な誤り訂正方式 2009 年暗号と情報セキュリティシンポジウム (SCIS2009) 予稿集, (2009-1) 松永雄斗，萩原学，吉田隆弘，古原和邦，今井秀樹
23. 講演	Set delegation 機能付き階層的 ID ベース暗号方式 2009 年暗号と情報セキュリティシンポジウム (SCIS2009) 予稿集, (2009-1) 吉田雅広，ナッタポンアッタラパドゥン，吉田隆弘，今井秀樹

種類別	題名，　発表掲載誌名，　　発表発行年月，　著者
24. 講演	ノートパソコンへのパスワード入力過程ののぞき見耐性について 2009 年暗号と情報セキュリティシンポジウム (SCIS2009) 予稿集, (2009-1) 佐古武志，吉田隆弘，古原和邦，今井秀樹
25. 講演	積符号化を利用した階層的な秘密分散法の検討 2008 年暗号と情報セキュリティシンポジウム (SCIS2008) 予稿集, (2008-1) 川島千種，吉田隆弘，松嶋智子
26. 講演	多重符号化を利用した階層的な秘密分散法の検討 電子情報通信学会技術報告, ISEC2007-76, pp.17-23, (2007-9) 川島千種，吉田隆弘，松嶋智子
27. 講演	初学者に対する e-learning の試み 平成 16 年度情報処理教育研究集会, (2004-11) 石田則道，犬伏雄一，金榮基，黒澤敦子，時井聰，山崎由美子，吉田隆弘，和高慶夫，山田正行，山内美恵子
28. 講演	ポアソン分布に従う非定常な時系列の予測に関する一考察 電子情報通信学会技術報告, IT2003-39, pp.93-97, (2003-7) 岩田錦弥，吉田隆弘，松嶋敏泰
29. 講演	誤り訂正符号を用いた直交計画の構成法に関する一考察 第 25 回情報理論とその応用シンポジウム予稿集, pp.663-666, (2002-12) 斉藤友彦，吉田隆弘，松嶋敏泰
30. 講演	ベイズ決定理論に基づくロバストなパターン認識に関する一考察 第 25 回情報理論とその応用シンポジウム予稿集, pp.283-286, (2002-12) 桑田修平，吉田隆弘，松嶋敏泰
31. 講演	状態空間モデルを用いた時系列解析に関する一考察 ーモンテカルロフィルタにおけるリサンプリング方法についてー 日本経営工学会 平成 13 年度秋季研究大会予稿集, pp.218-219, (2001-11) 桑田修平，吉田隆弘，松嶋敏泰
32. 講演	不確実な知識の演繹推論における二項述語への拡張に関する一考察 人工知能学会全国大会（第 14 回）論文集, (2000-7) 水野洋，吉田隆弘，松嶋敏泰