情報理論的安全性に基づく秘密鍵共有の研究

知識情報処理研究　　3602B052-2　羽田祐
指　　導　松嶋敏泰教授

A Study on Unconditionally Secure Secret Key Generation

by Yu Haneda

1　はじめに

近年，インターネットや電子政府計画，そしてユビキタス社会を見据えた世界の動向などからもわかる通り情報化社会というものが更に重要になってきている．この情報化社会を構築する際に必要となる機能として，情報の守秘，情報の伝送の効率化など様々な要求が生じてくる．この様々な機能の中で情報の守秘の機能を実現している重要な技術の１つが暗号学である．

現在，我々はインターネットに代表されるネットワークシステムを利用して多くの情報をやりとりしている．これらの情報が第 3 者に漏れたり，悪用されたりすることは情報化社会の進展・普及にとって大きな障害となる．従って，情報化社会を支える暗号にとってはその安全性というものが最も重要な課題となる．

その暗号を使用するための前提として，鍵を共有する必要がでてくる．秘密鍵の共有法の安全性には計算量的安全性からのアプローチと情報理論的安全性からのアプローチの２通りの立場が存在する．現在利用されている秘密鍵共有法には様々なものがあるが，そのほとんどは数学的な問題の難しさに安全性の根拠を置いている，すなわち計算量的安全性の立場で議論されている．しかし，計算量的安全性に基づく秘密鍵共有法は，計算機技術の発展や新たな解読アルゴリズムの出現により，将来にわたり安全であるとは言えない．一方，Shannon[1] に始まった情報理論的安全性に基づく秘密鍵共有法はまだ現実に利用するには問題が多いものの，無制限の計算能力を有する盗聴者に対しても無条件に安全であるため興味深い分野になっている．

秘密鍵共有法では安全性と同時に鍵を共有しようとする者達の持っている情報から生成できる鍵の長さが問題になってくる．鍵を生成するために多くの情報を保持する必要があると鍵を共有しようとする者達は多くのメモリを確保しなければならなくなるからである．なるべく少ない情報から長い鍵を生成するためには，そのモデルの下での理論的な限界を知り評価することが重要である．

そこで本研究では情報理論的安全性に基づく秘密鍵共有問題で扱われているモデルの１つである k-secure t-conference 秘密鍵共有モデルをより一般的なモデルへの拡張を行い，そのモデルの下で共有できる秘密鍵の長さの理論的な限界を評価する．

2　準備

まず始めに計算量的安全性と情報理論的安全性について述べ，次に本研究で必要となるについて述べる．

2.1　安全性

暗号技術はその安全性を保証するためにいかなる原理を用いるかによって２通りに分類することができる．

1）計算量的安全性

解読するために計算量がかかりすぎてしまい現実的には解読できないことに安全性を帰着させている方法．この方法の問題点として，将来コンピュータの性能が上がることや新しい解読アルゴリズムが発見されることで，安全性を保つことができなくなってしまうことがあげられる．

2）情報理論的安全性

既知情報から得られる秘密情報の情報量で安全性を評価する．一般に次式を満たすとき情報理論的に安全であるという．

$$H(X|Y) = H(X), \tag{1}$$

ここで,

$$H(X) = \sum_{x \in \mathcal{X}} P(x) \log P(x), \tag{2}$$

$$H(X) = \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} P(x, y) \log P(x, y), \tag{3}$$

である．なお定性的には既知情報 Y から秘密情報 X に関する情報がまったく漏れていないことを意味する．

3 従来法

記号のノーテーションとして下記の表記を用いる．

$\mathcal{P} = (P_1, P_2, \cdots, P_n)$:ユーザ全体の集合
D:ディーラー
$s \in S$:秘密情報
$\mathcal{A} \subseteq 2^{\mathcal{P}}$:秘密情報 s を復号できるユーザ集合の集合族（アクセス集合）
$v_i \in V_i$:秘密分散法においてユーザ P_i に送られる情報
$u_i \in U_i$:秘密鍵共有法においてユーザ P_i に送られる情報
Π_S:秘密情報 $s \in S$ の分布
Σ:秘密分散法における分散情報の分散の方法
Δ: 秘密鍵共有法における分散情報の分散の方法
k:セキュリティパラメータ
X, Y:ユーザの集合

3.1 秘密分散法（秘密情報が 1 つ）[2][5]

秘密分散法とは 2 段階の暗号プロトコルで，ディーラーが秘密情報 s に関する情報をユーザ $P_1, P_2, \cdots, P_n$ に分散情報として分け与える方法であり，その後，秘密情報 s の復号が許されている部分集合 $X \subseteq \mathcal{A}$ に含まれている各々の参加者がそれぞれの分散情報を出し合うことによって秘密情報 s を復号することができる．

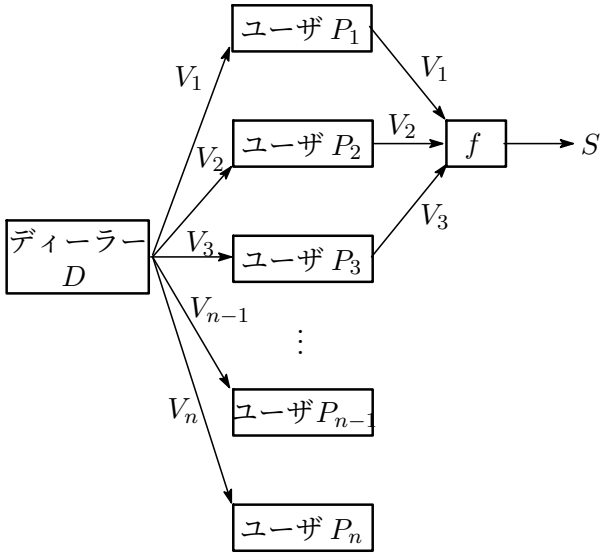

図 1: 秘密分散法

図 1 の例では，$\{P_1, P_2, P_3\} \in \mathcal{A}$ となっている．
定義 3.1 次式を満たす時，その秘密分散方法を完全秘密分散法と呼ぶ．
$X, Y \subseteq \mathcal{P}$ で，$X \in \mathcal{A}, Y \notin \mathcal{A}$ である時,

$$H(S|X) = 0, \tag{4}$$

$$H(S|Y) = H(S), \tag{5}$$

となる．完全秘密分散法とは，$\mathcal{A}$ に含まれるユーザ集合の保持している情報が集まった時のみ s を復号でき，それ以外の場合は s に関する情報を全く得られない秘密分散方法を意味している．すなわち，情報理論的安全性に基づいた秘密分散法である．
定義 3.2 完全秘密分散法において，ユーザに共有させたい秘密情報 s の大きさに対して，ディーラーが持たなければならない情報量を次式で示す．

$$\mu(\mathcal{A}, \Pi_S, \Sigma) = H(V_1, V_2, \cdots, V_n|S). \tag{6}$$

定理 3.3 完全秘密分散法において，ディーラーが持たなければならない情報量 $H(V_1, V_2, \cdots, V_n|S)$ の下限を次式で示す．

$$H(V_1, V_2, \cdots, V_n) \geq m \log |S|. \tag{7}$$

3.2 秘密分散法（秘密情報が複数）[10]

ここでは複数の秘密情報に関する情報をユーザ $P_1, P_2, \cdots, P_n$ に分散情報として分け与える方法

を考える．秘密情報 s_i の復号が許されている部分集合 $X \in \mathcal{A}_i$ に含まれている各々の参加者がそれぞれの分散情報を出し合うことによって秘密情報 s_i を復号することができる．

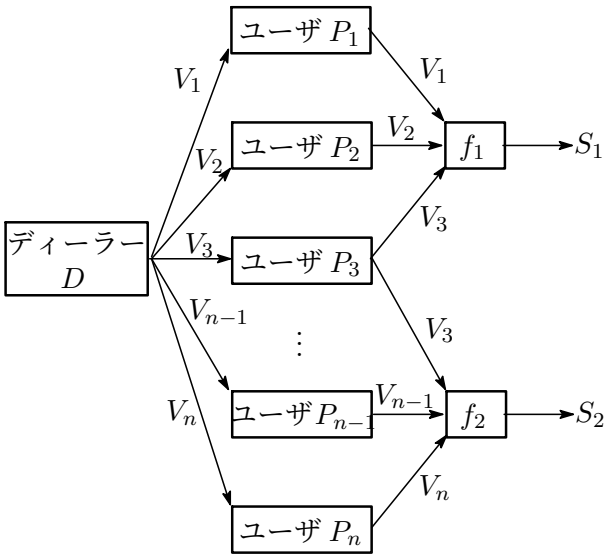

図 2: 秘密分散法（秘密情報が複数の場合）

図 2 の例では，

$$\{P_1, P_2, P_3\} \in \mathcal{A}_1, \{P_3, P_{n-1}, P_n\} \in \mathcal{A}_2. \quad (8)$$

となっている．ユーザ P_1, P_2, P_3 の分散情報を集めれば s_1 を復号できること，ユーザ P_3, P_{n-1}, P_n の分散情報を集めれば s_2 を復号できることを言っている．

3.3 秘密鍵共有 [3]

鍵共有法とは，信頼のおける 1 人のディーラー D と，ID 番号 $i \in \mathcal{I} = \{1, 2, \cdots, n\}$ が付けられている n 人のユーザからなるネットワークにおいて，ディーラー D が各ユーザへ個別の情報 $u_i \in U_i$ を送信し，ユーザが個別に共有する秘密鍵を計算する方式である．この方式では共有する秘密鍵 $s_j \in S_j$ を共有するユーザの集合 $X \in \mathcal{A}$ の内のユーザ $P_i \in X$ が，個別情報 u_i と X に属するユーザの ID 番号から秘密鍵 $s_j \in S_j$ を計算をすることができ，X に属さないユーザは，ある特定の人数が集まらないと秘密鍵 $s_j \in S_j$ を計算できないようになっている．ここで全ユーザの ID 番号はネットワークに対して既知の情報である．

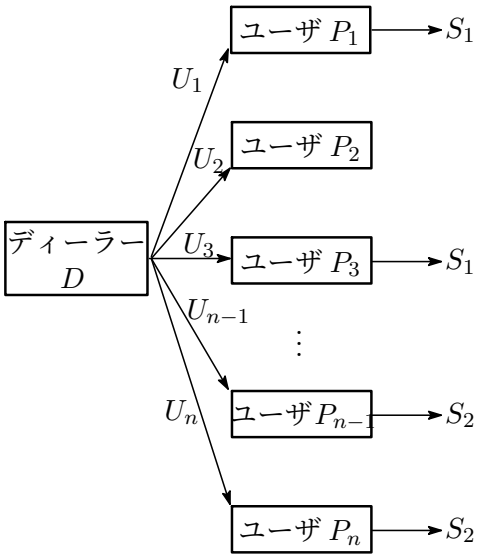

図 3: 秘密鍵共有法

図 3 の例では，$P_1, P_3 \in X_1$，$P_{n-1}, P_n \in X_2$ となっている．次式を満たすとき，その鍵分散法を k-secure t-conference 秘密鍵共有法と呼ぶ．
$X_j, Y \subseteq \mathcal{P}$ で，$X_j \subseteq \mathcal{P}, Y \subseteq \mathcal{P} \setminus X_j, |X_j| = t$，$P_i \in X_j$ である時

$$H(S_j|U_i) = 0. \quad (9)$$

$$H(S_j|Y) = 0 \quad (if\ |Y| \geq k). \quad (10)$$

$$H(S_j|Y) = H(S_j) \quad (if\ |Y| < k). \quad (11)$$

k-secure t-conference 秘密鍵共有法とは，ある X に含まれるすべてのユーザはそれぞれの保持している情報から秘密鍵 s_j を復号できるが，それ以外のユーザは k 人未満の情報を集めたとしても秘密鍵 s_j を復号できない秘密鍵共有法である．

定義 3.4　ここではユーザに共有させる鍵の長さに対して，ディーラーが持たなければならない情報量を次式で示す．

$$\gamma(k, t, n, H(S), \triangle) = H(U_1, U_2, \cdots, U_n). \quad (12)$$

定理 3.5[3][4]　ディーラーが持たなければならない情報量の下限は次式となる．

$$H(U_1, U_2, \cdots, U_n) \geq \begin{pmatrix} k+t \\ t \end{pmatrix} H(S). \quad (13)$$

$$H(U_i) \geq \left(\begin{array}{c} k+t-1 \\ t-1 \end{array} \right) H(S). \qquad (14)$$

4 提案法

本研究では，秘密鍵共有法に対して次の定義を導入する．

定義 4.1 複数のアクセス集合 $(\mathcal{A}_1, \cdots, \mathcal{A}_i)$ が存在し，$i = 1, \cdots, l$ で，
(1) 全ての $X \in \mathcal{A}_i$ は，

$$H(S_i|X) = 0, \qquad (15)$$

(2) 全ての $Y \notin \mathcal{A}_i$ は

$$H(S_i|Y) = H(S_i|S_{\mathcal{I}(Y)}), \qquad (16)$$

となる．この時，$\mathcal{I}(Y) = \{i : Y \in \mathcal{A}_i\}$ である．ここでアクセス集合はネットワークにつながっている全てのユーザとディーラーの同意の下に構成する．

この定義の導入により，秘密鍵共有における秘密鍵に相関がある場合，すなわちより一般的な場合に対してもディーラーが必要とする情報量 $H(U_1, \cdots, U_n)$ を評価できるようになった．

5 まとめ

本研究では，秘密鍵共有法のモデルの一つである k-secure t-conference 秘密鍵共有をより一般的なモデルへ拡張し，その下で共有できる秘密鍵の長さの理論的な評価を行った．これにより，本研究で提案したモデルにおいて実際にプロトコルの構成を行うときに，そのプロトコルにより生成される鍵長と理論的な限界とを比較し評価することができるようになった．

今後の課題としては，今回提案したモデルで鍵長の理論的な限界を達成するようなプロトコルを見つけることがある．

参考文献

[1] C.E.Shannnon,"Communication Theory of secrecy system," Bell System Technical Journal,Vol.28, 1949, pp656-715

[2] Blundo C., De Santis A., Gargano I., and Vaccaro U., "On the Information Rate of Secret Sharing Schemes,"Theoretical Computer Science, Vol.154, 1996, pp283-306

[3] Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro,"Randomness in Distribution Protocols,"Information and Computation, Vol.131, 1996, pp111-139

[4] Blundo C., De Santis A., Herzberg A., Kutten S., Vaccaro U., and Yung M.,"Perfectly-Secure Key Distribution for Dynamic Conferences,"Lecture Notes in Computer Science, Vol740, 1993, pp478-493

[5] Blundo C., De Santis A., and Vaccaro U.,"On Secret Sharing Schemes,"Technical Report, University of Salerno, 1995

[6] Cover T.M. and Thomas J.A.,"Elements of Information Theory,"John Wiley &Sons, 1991

[7] Matsumoto T.and Imai.H.,"On the Key Predistribution System: A Practical Solution to the Key Distribution Problem,"Proceedings of Crypto87, Lecture Notes in Computer Science, Vol.239, 1987, pp185-193

[8] Shamir A.,"How to Share a Secret," Communications of the ACM.22, 1979, pp612-613

[9] Imre Csiszar and Janos Korner,"Information Theory coding theorems for discrete memoryless systems,"Akademiai Kiado,Budapest, 1985

[10] Bar Bara Masucci, Carlo Blundo,"Randomness in Multi-Secret Sharing Schemes,"submitted, 1998