社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－MBL－25 (12)
2003／7／4

閾値秘密分散法を用いた簡易認証スキーム

小川 博久 † 山本 博資 ‡

あらまし (k, L, n) 閾値分散法によって，認証情報の分散化を行い，分散化した情報の真正性を検証する事で，認証を行う簡易認証スキームを提案する．また，本稿では本提案方式を権利情報の認証にも適用し，権利認証スキームの構成例を示す．(k, L, n) 閾値分散法を権利認証スキームに適用することによって，電子チケットで必要となる回数制限及び，傾斜，割勘処理を実現できるとともに，追跡性や匿名性も実現可能である．

キーワード 秘密分散法，(k, n) しきい値法，(k, L, n) しきい値法，電子チケット，認証

A simple authentication scheme using the threshold secret sharing scheme

Hirohisa OGAWA † and Hirosuke YAMAMOTO ‡

Abstract. In this report, a simple authentication scheme is proposed, in which informations for authentication are decentralized by the theshold secret sharing scheme and the authentication is realized by verifying the validity of the decentralized informations. Furthermore, by applying the proposed authentication scheme to the information of a right, the right authentication scheme is also proposed. By the benefit of the threshold scheme, we can realize limited number of use, use of a part, split of a right, pursuit or anonymousness in a transaction, etc., which are required in E-tickets.

Key words secret sharing scheme,(k, n)-threshold secret sharing scheme, (k, L, n)-threshold secret sharing scheme,E-ticket, authentication

1 はじめに

携帯電話に代表されるモバイル端末における属性認証には，一般的に，Basic 認証，Digest 認証 (以下，CHAP 認証と略す)，Secure Sockets Layer 認証，One Time Password 認証 (以下，OTP 認証と略す) や，専用のトークンを用いたスキームが提案されている．しかし，情報家電や，Low Cost Network Appliance に代表される非 PC 系組込み機器等では，さらに軽量なプログラム容量で，通信量についても効率的なスキームが求められている．

また，権利認証については，属性認証，改竄検知，否認防止や，デジタル署名を考慮し，PKI ベースによるスキーム提案が大半であるが，一方では，電子チケット提供者が，提供サービスを行う，PKI ベースとデータベース (以下，DB と略す) アクセス制御を組合せたスキームがある [1, 2, 3, 4, 5, 6]．電子チケット提供者が提供しているスキームは，インターネットを使用した WebServer 上で稼動するプログラムにより権利認証を行う為，権利情報は WebServer 上にしかなく，権利情報の携帯性に欠ける．

本提案では，モバイル機器や非 PC 系組込み機器等でも，属性認証と権利認証を可能にするスキームを提案する．そこで，本稿での問題意識は，権利情報の携帯性や，その他の権利認証の多

† 株式会社 シーフォーテクノロジー
C4 Technology, Inc.
oga@c4t.jp

‡ 東京大学 大学院情報理工学系研究科 数理情報学専攻
Department of Mathematical Informatics, Graduate School of Information Science and Technology, the University of Tokyo.
Hirosuke@ieee.org

様性に対応でき，且つモバイル機器や非PC系組込み機器等でも動作が可能であるスキームを構築する事にある．その為に，PKIベースの計算能力を必要とする認証は行わず，該当情報の真正性が検証された場合に認証するというSomething You Have方式（以下，SYH方式と略す）で行う．この方式では，認証においては，属性認証情報を検証し，権利認証においては，権利情報を検証する事で行え，認証エンティティと検証エンティティは，検証作業と該当情報を送受信する事で完結できるというメリットがある．

本稿では，(k, L, n) 閾値秘密分散法 (以下，(k, L, n) 閾値法と略す) を用いた，SYH方式の簡易的な属性認証及び，権利認証のスキームを提案し，数点のシステム構成例を示す．第2節では，本提案方式の概要を示し，(k, L, n) 閾値法を認証スキームで利用する事によって得られる特徴を説明する．第3節では，本提案方式を用いた認証スキームの構成例を示す．第4節では，本提案方式を権利について認証を行う権利認証に展開した場合の構成例を示し，本提案方式の特徴を説明する．第5節では，各提案例に対する信頼性のモデルを定義し，各モデルに対する初期設定を示す．最後に，本提案方式を実施した実測データを示す．

2 (k, L, n) 閾値秘密分散法

秘密分散法の中で最も良く知られたものに (k, n) 閾値法がある [7]．(k, n) 閾値法は n 個の分散情報のうち，任意の k 個を集めることで秘密情報が復号できるが，$k-1$ 個以下の分散情報では秘密情報についての情報が全く得られない方式である．秘密情報 S のエントロピーを $H(S)$，n 個の分散情報 S_i，$i = 1, 2, \ldots, n$ のエントロピーを $H(S_i)$ とすると任意のアクセス構造に対して，$H(S_i) \geq H(S)$，$i = 1, 2, \ldots, n$ が成り立つことが知られている [8, 9, 10]．

(k, L, n) 閾値法とは，上記の (k, n) 閾値法に対して，パラメータ：L を用いて，ランプ型秘密分散法を構成する事で，分散化した情報（以下，shareと略す）を $1/L$ のサイズに短くすることができる効率的な秘密分散閾値法である [11]．

2.1 (k, L, n) 閾値法の特徴

閾値秘密分散法は，秘密情報を分散及び暗号することを同時に行う技術であり，2つの特性がある．

- 秘密情報を秘匿した状態で分散化する．
- 正当なshareが k 個以上持寄られた場合にのみ秘密情報を復元できる．

以上の特性から，重要な秘密情報を秘匿しながら携帯する事に適した技術である．

また，(k, L, n) 閾値法を本提案方式に利用する事による，4つの大きな特徴がある．

- 秘密情報の共有が容易である．

share生成は，k, n によって，任意に設定できる為，エンティティ同士に秘密情報を共有化させる事が可能である．通常，共通鍵暗号方式を利用した同様の認証スキーム（CHAP認証，OTP認証）では，共有させたいエンティティの分だけ異なる鍵を用意し，暗号化処理を行う事になる．本提案方式では，共有させたい秘密情報を一度の分散化処理で秘匿出来る為，都度異なる鍵で暗号化する必要が無く，効率的である．

- 回数制限の設定が容易である．

事前にshareを複数送り，share分の認証及び権利許諾を行う事が可能であり，回数制限機能の追加が容易である．

- レベルの設定が容易である．

所持しているshareの量によって許諾するレベルを設定する事が可能であり，認証レベル機能の追加が容易である．

- 通信量を軽減できる．

share生成は，L によって，送りたい秘密情報を $1/L$ のsahreサイズに短くする事が可能であり，通信量を軽減する事が容易である．

この効果は，認証スキーム及び，権利認証スキームのどちらに対しても効果的である．

2.2 安全性の保証

(k, L, n) 閾値法を認証に適応する場合には，shareに対する総当り攻撃が考えられる．この場

合，現状の現実的な計算能力を考慮し，各 share は，128bit 以上あれば総当り攻撃に耐性があると考えられる．つまり，秘密情報の選択基準は，一様ランダムで且つ，128bit 以上に規定され，生成する share も一様ランダムで且つ 128bit 以上であれば，どのようなデータであっても構わない．

また，送受信される share に対する結託攻撃も考えられる．この攻撃に対しては，利用したい share 数と，該当 share を安全に配布するための share 生成量の調整によって，対応することが可能である．配布 share 数：M．検証エンティティが持つ share 数：m．及び，n,k の関係式は下記の通りである．

$$M = m \quad (1)$$

$$n = 2M \quad (2)$$

$$k = M + 1 \quad (3)$$

3 認証スキームの構成例

前記の (k, L, n) 閾値法を認証スキームに適応した構成例を示す．本構成例は，属性認証情報を秘密情報として，分割した share を検証し，認証する方式である．

3.1 share 定義について

本構成例の初回動作時には，初期 share と，以降の認証に必要となる share 定義が存在する．初期 share とは，初回認証時に必要となる share であり，両エンティティが対応する share を持合っている．また，share 定義とは，share 生成に必要となる素数及び，n, L, k の設定情報である．携帯電話機等の計算能力の乏しい環境では，分散化処理に要する素数を生成する事なく，予め定義しておく事でより軽量なプログラムで，高速に処理する事が可能になる．

この初期設定情報は，システム登録時のオフラインによる記録媒体の取交し (USB デバイス等) や，機体認証後の (i アプリにおける unt 属性等) プログラムダウンロード時或いは，SSL 等の信頼できる通信によって，認証エンティティ及び検証エンティティが所有している．つまり，この share 定義は，プログラム内部に設定情報として複数パターンを格納する場合と，share 定義自体を share 化し，初期 share と同様に，両エンティティが対応する share を持合う場合がある．

尚，本稿では，share 定義自体を share 化する方式の認証プロトコルを説明する．

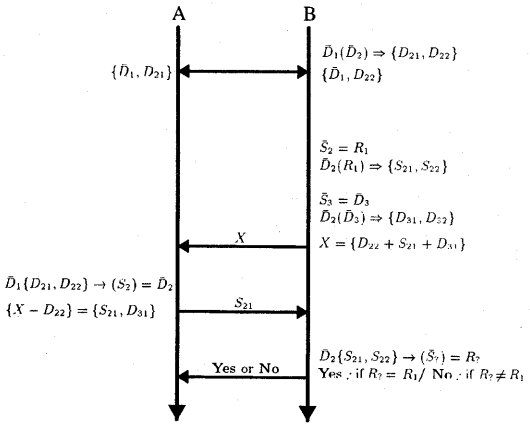

図 1: 認証プロトコル

3.2 認証プロトコル

認証プロトコルを図 1 に示す．尚，各記号の意味は下記通りであり，$k = 2, n = 2$ の $(2, 2)$ 閾値法での構成例とする．

認証エンティティ：A，検証エンティティ：B，
秘密情報：$\bar{S}_*$，認証用 share：S_*，
share 定義：$\bar{D}_*$，定義用 share：D_*，
分散化 (share 生成)：$\Rightarrow$，share 検証：$\rightarrow$，
データ連結：$+$，データ分離：$-$，
乱数：R_*，送信：$\longmapsto$，
認証及び否認：Yes or No.
また，表記方法は下記とする．
share 生成：share 定義 (秘密情報)$\Rightarrow$ {share 群 }
share 検証：share 定義 {share 群 }$\rightarrow$(秘密情報)

1, A, B は，share 定義:$\bar{D}_1$ を所持している．

(1) 初期 share 生成：
$\bar{D}_1(\bar{D}_2) \Rightarrow \{D_{21}, D_{22}\}$

(2) 初期設定：
A：$\{\bar{D}_1, D_{21}\}$，B：$\{\bar{D}_1, D_{22}\}$

2, B の決定：R_1，$\bar{D}_3$ を所持.

(3) 認証 share 生成：$\bar{S}_2 = R_1$
$\bar{D}_2(R_1) \Rightarrow \{S_{21}, S_{22}\}$

(4) 次回 share 定義生成：$\bar{S}_3 = \bar{D}_3$
$\bar{D}_2(\bar{D}_3) \Rightarrow \{D_{31}, D_{32}\}$

(5) 送信データ生成:$X = \{D_{22}+S_{21}+D_{31}\}$

(6) データ送信：$X \longmapsto A$

3, A の検証：$\bar{D}_1$,D_{22} を所持.

(7) share 定義復元：
$\bar{D}_1\{D_{21}, D_{22}\} \rightarrow (S_2) = \bar{D}_2$

(8) 認証 share 復元：
$\{X - D_{22}\} = \{S_{21}, D_{31}\}$

4, A のリクエスト：$S_{21} \longmapsto B$

5, B の検証：$\bar{D}_2, S_{12}$

(9) $\bar{D}_2\{S_{21}, S_{22}\} \rightarrow (\bar{S}_?) = R_?$

(10) Yes:$R_? = R_1$
No:$R_? \neq R_1$

3.3 認証スキームの結論

以上に説明した通り，本提案では，認証の都度に異なる share 定義及び，認証情報を用いる方式である．本提案方式は，ある時点において，正当なデータを所持していた所有者が，該当属性であるという仮定に基づき，該当データの真正性が検証されれば認証許諾する方式である．

認証を求める認証エンティティは，(k, L, n) 閾値法を用いて，share 定義を復元する処理と，share 定義から導かれた認証用 share を送信処理するだけである為，高速に動作させる事が可能である．また，先に説明した通り，CHAP 認証及び，OTP 認証と比較した場合でも，複数エンティティに対して，同一秘密情報を同時に暗号，分散処理できる為，効率的である．

4 電子チケットの構成例

以降に説明する構成例は，権利情報を秘密情報として，分割した share を検証する事で権利認証を行う方式である．先に説明した認証スキームのフローとまったく同じであるが，電子チケット・スキームを実現するにあたり，特有の課題が存在する．

4.1 電子チケットの課題

電子権利の多様性に対して，安全な状態で権利情報を携帯する携帯性は勿論の事，権利の譲渡を行う譲渡性や，傾斜支払いを行う傾斜処理，割勘，まとめ買い等への対応が，求められている．また，安全性確保に求められる電子チケット利用者の追跡可能性が必要となる場合と，電子チケット利用者の匿名性をが必要となる場合があり，利用場面によって，両要求に対応できるスキームが求められている [12, 6] .

4.2 構成例の概要

上記の電子チケット特有の課題に対し，本提案では，属性認証情報と権利情報を別々に管理する事で，権利譲渡を行う構成例と，share を再発行する事によって，傾斜処理，割勘，まとめ買いに対応できる構成例を示す.

4.3 権利譲渡が可能な構成例

本構成例では，電子チケット発行者による認証 DB 及び，チケット DB が存在し，秘密情報内容が異なるだけである．表 1 は，電子チケット発行者が所有する user-DB であり，表 2 は，電子チケット発行者が所有する ticket-DB である．表 1 にある【認証】とは，先に説明した認証用 share であり，$S_{\star 2}$ は，$(2, 2)$ 閾値法によって，$S_{\star 1}$ に対応している事とする．認証用 share の内容を表 3 に示す.

表 1: user-DB

user-ID	PIN	社名	部署名	氏名	認証
001	****	AAA	SI	OGAWA	S_{02}
002	****	AAA	SI	FUMIO	S_{12}
003	****	BBB	Dev	SYOBE	S_{22}
...	...	...	...	...	...

表 2: ticket-DB

ticket-ID	検証側 share	認証側 share
100	S_{82}	S_{81}
101	S_{92}	S_{91}
...	...	...

表 3: 認証用 share

秘密情報	内容	share
S_{00}	AAA,Gr-A,,,	$\{S_{01}, S_{02}\}$
S_{10}	AAA,Gr-B,,,	$\{S_{11}, S_{12}\}$
S_{20}	BBB,Gr-C,,,	$\{S_{21}, S_{22}\}$
...	...	...

今，表の構成で示した，user:001 が，S_{82} を行使する場面を想定する．S_{82} は，会社が購入した交通チケットだとする．

1，この場合の単純な秘密情報内容
$\bar{S}_1$={ 社名:AAA, 交通, 回数:1}

＊ 上記データには，冗長性を軽減させる乱数が追加されている．

2，送信データ

- 匿名型送信データ
  {ticket-ID:100(S_{81})}
- 追跡型送信データ
  {ticket-ID:100(S_{81}), S_{02}}

本構成例では，権利認証時には，秘密情報である，{ 社名:AAA, 交通チケット, 回数:1} が復元され，社名:AAA を確認する事ができる．その為，user-DB 内で登録されている社名:AAA を持つ属性であれば，権利譲渡が可能である．

つまり，本構成例では，権利情報と属性認証情報とが別々に秘匿された状態で管理されている為，権利譲渡は，容易に実現できる．

また，本構成例では，電子チケットの安全な携帯性に対する要求も満たす事ができる．電子チケットの携帯性における課題とは，モバイル端末に所持している電子チケットを当事者には，確認する事ができるが，非当事者には，確認できない事である．本構成例では，オフラインの環境下においても，情報を所持している事は確認できるが，(k, L, n) 閾値法によって，分散化された share である為，その情報が何に関連付けられた，どのような権利情報かは，当事者でしかわからない．当事者が，検証する場合のみオンラインで，(k, L, n) 閾値法を用いて，share 検証する事で，権利情報を知る事ができる為，安全に携帯する事が可能である．

4.4 傾斜処理が可能な構成例

次に，傾斜処理，及び団体割引やまとめ買いについては，権利情報を所有しているエンティティが，share を再発行することで上記の課題を実現できる．前の構成例と同様に，表 1,2 を用いて，フローを説明する．

今，表の構成で示した，user:002 が，user:003 に対して，S_{92} を傾斜する場面を想定する．S_{92} は，会社が購入した 3 回分の交通チケットだとする．

1，この場合の単純な秘密情報内容
$\bar{S}_1$={ 社名:AAA, 交通, 回数:3}

＊ 上記データには，冗長性を軽減させる乱数が追加されている．

2，電子チケットの再発行
user:002 は，購入した交通チケット 3 回分を，2 回と 1 回に分ける為，電子チケットの発行を行う．

- 追加データ $= Y$
  Y = {user002:2/3,user003:1/3}
- 再発行の単純な秘密情報内容
  $\bar{S}_2$= { 社名:NULL, 交通, 回数:3=Y}

4，share 生成
ticket-ID:102 = $\{S_{101}, S_{102}, S_{103}\}$

5，share 配布

- user:002 $\mapsto \{S_{101}\}$
- user:003 $\mapsto \{S_{102}\}$
- 検証エンティティ$\mapsto \{S_{103}\}$

6，送信データ

– 匿名型送信データ
$\{\text{ticket-ID:}101(S_{91}), 102(S_{10*})\}$

– 追跡型送信データ
$\{\text{ticket-ID:}101(S_{91}), 102, (S_{10*}), S_{02}\}$

本構成例では，新規にshareを配布する事によって，電子チケットの傾斜・割勘処理を行えるが，新規に生成するshareに，元の権利情報を含める事で，元本に対する追跡性も有している．

尚，権利認証スキームの構成例では，簡易的に説明を行う為，2種類のDBを用いたが，電子チケットの発行量が少ない場合では，Clientの検索処理だけで充分な場合もある．

権利認証スキームの構成例では，簡易的な認証用shareを用いて，構成したが，実際には，個人として認証を行いたい場合や，特定グループとして認証を行いたい場合など，用途によっては，様々な要件が考えられる．想定される信頼性のモデルについて定義する．

5 構成例のモデル定義

本提案で示した各構成例では，信頼性のモデルは，2種類があり，モデル定義による初期のshare定義は，4種類がある．

1, Server信頼モデル

主に，Client/Server・システムを想定したモデルであり，属性認証情報や，権利情報等，すべてのデータは，Serverを介して行われる．認証においては，システム認証等が想定される．権利認証においては，企業が提供する特定サービスの電子チケットが想定される．

2, P2Pモデル

モバイル機器や，非PC機器に適応できるモデルであり，属性認証情報や，権利情報等，用途によっては，Serverを介さず行われる．認証や，権利認証において，P2Pでの処理が想定される．

5.1 share定義の種類

●個人用のshare定義

個人用の認証及び，権利認証に用いられる初期設定情報である．システムの初期登録時に，配布されている事が前提となり，本稿の構成例では，share定義が秘密情報である．

●グループ用のshare定義

構成例のシステムにおいて，Serverが特定グループに対し，共通鍵として配布する初期設定情報である．以降，特定グループ間で，shareを配布する際に，使用するshare定義である．Serverが既知の鍵を使用するServer信頼モデルである場合と，以降に更新されServerが既知でない鍵を使用するP2Pモデルである場合の2種類ある．

●本人認証用データshare定義

権利認証時に使用される属性認証の追跡を行う為のshare定義である．特定情報の署名データ＋タイムスタンプを想定している．

尚，すべてのshare定義は，認証の都度に更新される．

6 実測データ

6.1 モジュール説明

本提案スキームを携帯電話機や情報家電へ適応する為，機能毎にモジュールを分割し，必要に応じてモジュールを追加する構成にし，各検算処理の測定を行った．モジュール構成は，下記の3つがある．

●素数生成モジュール

素数生成は，演算能力の乏しい環境での動作が遅くなる為，素数生成モジュールを分け，演算能力の乏しい環境でも本提案スキームを動作させる事を目的とした．

● share生成モジュール

share生成モジュールは，shareの生成を行う為に必要となるモジュールである．

● share検証モジュール

share 検証モジュールは，share を検証する為に必要となるモジュールであり，本提案スキームでは，必須のモジュールになる．

以上のモジュール構成で，実測した結果を各表にまとめた．表 4 は，PentiumIII-500MHz/256MB/Win2k の環境で，測定した (k,n) 及び，(k,L,n) 閾値法の share 生成，検証に要する時間を ms 単位で表した．ループ回数:10,000 の平均値である．図 2 は，表 4 をグラフにした図である．表 5 は，表 4 の環境で，L の設定による share 生成，検証に要する時間を ms 単位で表した．ループ回数:10,000 の平均値である．表 6 は，携帯電話 (N504i) での share 生成，検証に要する時間を ms 単位で表した．ループ回数:100 の平均値である．

表 4: (k,n)・(k,L,n) 閾値法の速度比較

秘密情報 bit	(k,n)		(k,L,n)	
	生成	検証	生成	検証
128	1.784	1.039	3.428	2.504
256	2.802	1.613	5.175	3.776
384	3.739	2.211	6.924	5.147
512	4.717	2.777	8.473	6.337
640	5.756	3.461	10.126	7.797
768	6.66	4.096	11.619	9.386
896	7.632	4.95	13.551	11.053
1,024	8.625	5.684	15.331	12.6

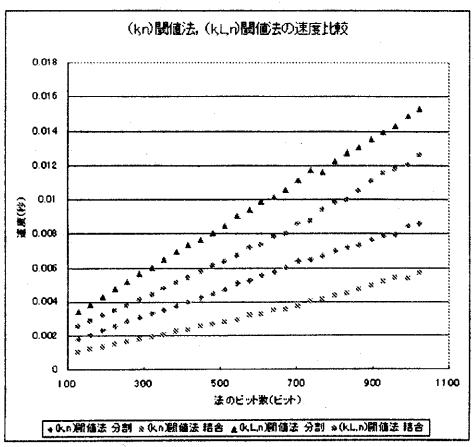

図 2: (k,n)・(k,L,n) 閾値法の速度比較

表 5: L 可変による速度調査

L 設定値	share 生成	share 検証
2	29.089	68.778
4	32.539	70.193
6	36.691	71.887
8	42.03	73.863
10	48.919	75.163
12	57.693	77.468
14	68.39	78.504
16	81.773	80.686

表 6: (k,n)・(k,L,n) 閾値法の速度比較 2

秘密情報 bit	(k,n)		(k,L,n)	
	生成	検証	生成	検証
128	3,820	1,220	2,400	1,620
256	4,840	1,730	3,110	2,400
384	6,870	3,060	4,620	4,010
512	10,760	6,290	7,960	8,290
640	18,490	14,660	14,220	17,160

7 まとめ

本稿では，(k,L,n) 閾値法を用いて，属性認証及び，権利認証スキームを提案した．本提案方式は，ある時点において，正当なデータを所持していた所有者が，該当属性であるという仮定に基づいている為，属性情報と権利情報を同時に扱え，別々の管理ができる事，また検証作業で認証ができる事を示した．

認証においては，複数エンティティに対して，同一秘密情報を同時に配布する場合は，効率的である事，権利認証においては，携帯性，譲渡性及び，傾斜処理が可能である事を示した．

本提案方式は，公開鍵暗号の特徴である，複数の鍵管理を単一の share 管理で行い，共通鍵暗号の特徴である，暗号処理するサイズを短くする事で，計算量の低減を行える．

今後の課題は，本稿の構成例で示した認証データにおける Server に対する計算委託の実装方法について検討する必要がある．

参考文献

[1] 森 謙作, “モバイル環境に適した安全な転々流通機構の研究,” *CSEC*, vol. 016, no. 022, pp. 127–132, 2001.

[2] 西郷 悟, 三浦 史光, 高橋 修, “柔軟な多対一

決済に関する研究," *CSEC*.

[3] 桜井 鐘冶, 高橋 渉, "モバイル個人認証方式の提案と実装," *CSEC*, vol. 019, no. 009, pp. 49–54, 2002.

[4] 青野 博, 石井 一彦, 森 謙作, 本郷 節之, 越塚 登, 坂村 健, "モバイル向け電子価値流通プラットホームの研究," *CSEC*, vol. 019, no. 012, pp. 67–72, 2002.

[5] 小栗 伸幸, "モバイル端末に適した検証可暗号法の提案," *CSEC*, vol. 016, no. 034, pp. 199–203, 2001.

[6] モバイル EC-WG, "モバイル電子チケットのビジネス要件・機能要件," tech. rep., 電子商取引推進協議会, 2002.

[7] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[8] R. M. Capocelli, A. D. Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *J. of Cryptology*, vol. 6, pp. 157–167, 1993.

[9] L. Csirmaz, "The size of a share must be large," *J. of Cryptology*, vol. 10, pp. 223–231, 1997.

[10] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, no. 29, pp. 35–41, 1983.

[11] 山本 博資, "(k, L, n) しきい値秘密分散システム," **電子通信学会論文誌**, vol. J68–A, no. 9, pp. 945–952, 1985.

[12] 飯野 陽一郎, "公開鍵認証基盤に基づく電子チケットの理論," **電子通信学会論文誌**, vol. J85-A, no. 11, pp. 1254–1263, 2002.