平成20年度

論文題目

FeliCaチップへの
秘密分散共有法の適用

神奈川大学 工学部 電気電子情報工学科

学籍番号 200502689

佐々木 賢

指 導 担 当 者　　木 下　宏 揚　教授

目 次

図 目 次

表 目 次

第1章　まえがき

近年、乗車券や電子マネーをはじめとして、社員証・学生証・会員証などといったカードで、読み取り面にかざすだけで認証・データの読み書きという処理が可能な非接触型 IC カード [3] の利用が多くなっている。これらのカードの内部は IC チップとアンテナで構成されており、リーダ/ライタと呼ばれるカードに読み書きができる装置にかざすと、装置から発せられる電波を受けて、カードはアンテナによって電力を得て IC チップが動作をする。IC チップには個々のカードを認識するために固有に記録されている ID や、利用者がデータを記録するためのメモリが組み込まれている。我々に最も身近な非接触型 IC カードの技術として「FeliCa」(フェリカ) [1] [9] [10] [17] がある。これを駅の改札を例に説明すると、IC カードは関東圏で利用されている「Suica」[14] や「PASMO」[15] といった IC 乗車券、リーダ/ライタは改札機である。利用者が改札機にカードをかざすと改札機から電波が発せられているため、カード内の IC チップが動作をして改札機にカード内に記録された情報を返す。カード内の情報は、この場合は乗降駅・残金などのデータであり、データを受け取った改札機はそれらの読み取ったデータを記録・処理するサーバーなどへ転送される。そのため、改札機としてのリーダ/ライタを制御する上位機器としてサーバーがあてられる。

ここまでは非接触 IC カードの簡単な利用方法を記述したが、これらはすべてカードという媒体を通して、個人およびその本人が有する情報をやり取りするための認証を行っているということである。認証という処理・動作は秘密情報が外部に漏えいするのを防ぐために認証情報（鍵・キーなど）によって所有者（本人）である確認を行う。通常、カードを利用した認証には１枚のカードのみであったり、暗証番号を入力するなど１人の管理者による認証が行われるが、本研究では、認証情報および秘密情報のそれ自体を複数の情報に分散して、管理者を複数にすることによって、任意に決められた２つ以上の情報が集まらなければ秘密情報を得ることができないという「秘密分散共有法」[2] [11] を非接触 IC カードに適用することを目的としている。

このシステムの利点として、秘密情報をある一人の管理者のみに預けるのではなく、一定の人数以上の承諾を得なければ秘密情報を閲覧することができない場合や、データの一部を紛失してしまった場合のバックアップ機能など、また管理者による情報漏えいや悪用を防ぐことが可能となる。

第2章　基礎知識

2.1　非接触IC カードとは

認証（認識・識別）の技術として現在私たちの身の回りには、商品を購入する際には“ バーコード ”から、代金を支払う際に“ クレジットカード ”で、また現金を ATM から引き出す際には“ キャッシュカード ”、万引き防止のために商品に“ タグ ”をつけて管理する、といった認証技術が多く利用されている。

この中でも、近年利用が増えているものに RFID[3] という技術がある。

2.1.1　RFID とは

RFID(Radio Frequency Identification) とは、電波を利用して人物や物品を自動的に認証する技術の総称である。これは、タグやラベル状に加工されたアンテナ付 IC チップを物や人に付与し、そこに記憶された情報をリーダ/ライタと呼ばれる装置で読み取ることで、物体や個人の認証を行おうとするものである。

最近では、RFID の持つ特性を情報システムに応用することにより、現在人の手により行われている多くの業務オペレーションを自動化し、あるいは簡素化することができるため、RFID を導入した企業は膨大なコストを削減できるといわれている。さらに人為的なミスの防止やシステムのリアルタイム性が向上することにより、情報の質が向上し、企業リソースの正確な把握や、迅速な意思決定を支援するものとしても期待されている。今では、人物や商品だけでなく、家畜の管理などにも利用されている。

RFID の利点として、無線を使用しているため読み取りが柔軟であり、現在の物体認証の主流であるバーコードや、近年携帯電話端末のカメラなどで多く利用されるようになってきた 2 次元バーコードなどにくらべ、読み取り面が必要ない。また、クレジットカードなどのような磁気カードといった接触が必要ないため、識別距離が長くなっている。その他に偽造がしにくく、安全性が高いという点もある。

2.1.2 接触式と非接触式の違い

RFID の技術が埋め込まれたカードを通称“ IC カード ”と呼ぶ。IC カードには、キャッシュカード大のプラスチック製カードに、メモリやマイクロプロセッサを内蔵した IC チップを搭載している。IC カードは、磁気ストライプカードと比べ、多くの情報を保存することができ、接触式 IC カードと非接触式 IC カードに区別される。

接触式 IC カード

接触式 IC カードには、カードの読み取り面に端子があり、それを読み取り装置の端子と接触させることにより、IC チップとの間でデータを読み書きすることができる。接触式 IC カードは、データを送受信する際に読み取り装置にカードを挿入し、接触電極をそれぞれ接触させなければならないため、摩耗や汚れなどから接触不良が発生する可能性があり、それを防止するためには定期的に点検を行う必要がある。また、カードの読み取り面は決まっているため、表裏、前後左右などを誤ると読み書きができなくなるため、利用者にとってはカードの取り扱いが煩わしい場面ができてしまう。

非接触式 IC カード

非接触 IC カードは、カード内部にアンテナの役割を果たすコイルを搭載しており、カードを読み取り装置にかざすことによってそこから発生している電波（磁界）の無線通信を利用してデータの送受信を行う。非接触 IC カードは、データの読み書きが可能な距離や通信方式の違いによって分類されている。距離の違いでは、密着型（〜2mm）、近接型（〜10mm）、近傍型（〜70mm）に分類される。また、通信方式の違いによって TypeA、TypeB、TypeC（FeliCa）に分類される。

2.2 FeliCa 概要

非接触型 IC カードには、2.1.2 で述べたように通信方式の違いによってカードタイプが分類されている。本研究では、システムを構築する非接触型 IC カードとして現在私たちが最も多く利用し身近なものであろう、IC 乗車券（関東圏では Suica、PASMO）に採用されている方式である“ FeliCa（フェリカ）”[1] を用いることにした。

FeliCa はソニー　が開発・商標登録した方式であり、「felicity:至福」から名前が由来している。当初は非接触 IC カード (ISO 14443)TypeC として採用される予定であったが、その計画は最終的に非接触型 IC カードとしては世界で初めて、セキュリティ評価基準の国際標準である ISO/IEC 15408 EAL4 の認定を受けた。

非接触型 IC カードの規格には様々な種類があるが、FeliCa には、次のような仕様や活用方法・利点がある。[4]

2.2.1 FeliCa の活用

電子チケット・乗車券

FeliCa は瞬時にデータを読み取って処理することが可能である。よって、利用金額の追加 (チャージ) も簡単に行え、繰り返し利用することが可能である。そのため乗車券への応用に非常に適しており、大手鉄道会社の IC カード乗車券に採用され、定期券やプリペイドカードとして利用者が増えている。さらに、さまざまな地域においてのバス乗車券としての運用も広がりつつある。

電子マネー

FeliCa 技術を採用した電子マネー“ Edy [1] ”の利用が進んでおり、このマークのある加盟店であれば全国で利用が可能で、大手コンビニエンスストアや大規模複合施設でのショッピングを始め、自動販売機などでも利用することができます。また、レジ処理は店側にとっても快適な処理となる。利用金額のチャージには店舗などの入金機だけでなく、インターネット上からも簡単に行うことができる。

社員証・学生証・会員証

出退勤管理やオフィス・事業所、研究室などの入退室管理、個人認証などに利用することができる。[6] [7] [8] また、電子マネーの機能と併用することにより、社内・学内の売店・自動販売機・食堂などでの買い物に利用することが可能である。

携帯電話端末への搭載

カード内に搭載されている FeliCa の IC チップを携帯電話端末内に搭載したものをモバイル FeliCa と呼ぶ。これによって、普段持ち歩いている携帯電話端末を FeliCa の非接触型 IC カードと同様のサービスを利用できるほか、FeliCa チップとのデータ送受信を利用したアプリケーションサービスの利用が可能となる。代表的なサービスとして“ おサイフケータイ ”があり、電子マネーとして利用するほか、残高状況を携帯アプリによって閲覧することができる。

[1] ビットワレット株式会社のプリペイド型電子マネーサービス

2.2.2　FeliCa の暗号方式

FeliCa がもつ暗号処理として、通信路に DES [2] もしくはトリプル DES [3]、相互認証にトリプル DES を採用している。Dual カードタイプ (接触/非接触兼用) では公開鍵暗号方式の処理が可能なものがある。

1 枚のカード (1 つのチップ) に複数のサービス（IC カード乗車券、電子マネー、社員証など）を搭載可能であるが、サービス利用時には、個々のサービスごとにアクセス鍵（共通鍵）を使って相互認証を行うのではなく、複数のアクセス鍵を暗号化し合成させた“ 縮退鍵 ”を用いて、一度に最大１６のサービスを相互認証することが可能である。縮退された鍵から元の鍵は生成できないことから、セキュリティレベルを落とすことなく処理速度の高速化を行っている。

2.2.3　FeliCa のファイルシステム

FeliCa チップ内におけるメモリのフォーマット例を以下の図 2.1 に示す。
なお実際のフォーマットはカードを発行する事業者によって異なっている。

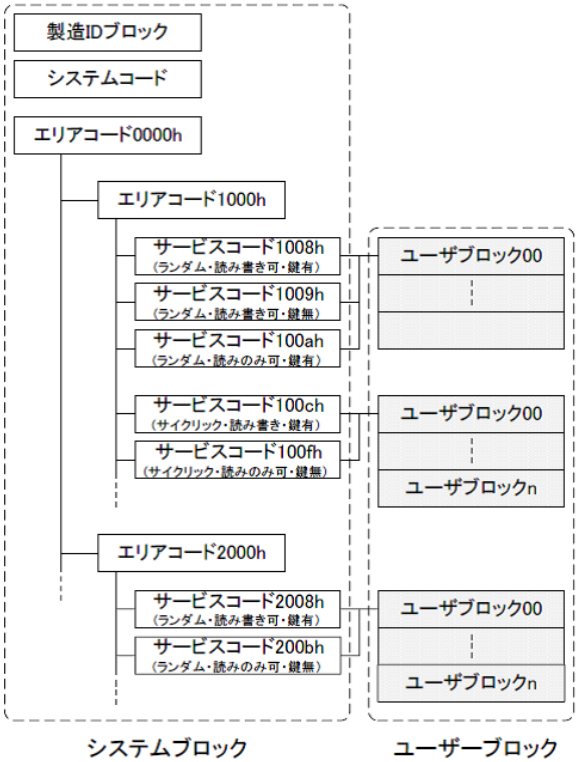


図 2.1: FeliCa メモリのフォーマット例

[2] IBM 社によって開発された秘密鍵暗号化アルゴリズム。
[3] DES を三重に適用するようにした方式のこと。コンピュータの性能向上に伴って DES 暗号を解読される危険性が高まったため、同じ方式を三重にかけることにより、強度を高めた。

2.2.4 システムブロック・サービス

ブロック

FeliCa 内のメモリ管理は 16 バイト毎に行われている。この 16 バイトの単位をブロックと呼ぶ。ユーザーがメモリにアクセスする際は、エリアコード・サービスコードと呼ばれる 2 バイトのコードを使用する。

また、FeliCa 内のメモリはユーザーデータが書き込まれるユーザーブロックと、FeliCa の構成情報が保存されているシステムブロックと呼ばれる領域に分けて管理されている。

製造 ID ブロック (製造 ID、製造パラメータ)

製造 IC ブロックの構成は、製造 ID(IDm) と製造パラメータ (PMm) のそれぞれ 8 バイトで構成されている。IDm は FeliCa を識別するために固有の番号が記録されており、認証などに利用することができる。PMm は製品のバージョン情報などが記録されている。これらの値はカード発行時に登録され、書き換えることができない。

ユーザーブロック

ユーザーブロックは、ユーザーデータが書き込まれる領域であるが、直接読み書きすることはできない。アクセスにはユーザーブロックに関連付けられたサービスを使って間接的に行われる。

システムコード

システムコードはカード発行者を識別するためのコード (2 バイト) である。

エリアコード・サービスコード

エリアコード (2 バイト) は、使用可能なサービスコードの範囲を示し、ユーザーブロック数などを設定コードである。(Windows のフォルダに該当する)

サービスコード (2 バイト) は、ユーザーブロックへアクセスするためのコードである。(Windows ではファイルへのショートカット名に該当する)

サービスコードによって以下のような属性が定義されている。

- サービスの種類 (ランダムサービス、サイクリックサービス、パースサービスの 3 種類があり、Windows では拡張子に該当する)
- ユーザーブロックに対するアクセス権 (読み書き可/読み込みのみ可、また、読み書き時の鍵の有無を設定する)

2.2.5 FeliCa のデータアクセスサービスの種類

ランダムサービスタイプ

ランダムサービスは、ブロック単位で自由にデータを書き込みできる汎用的なサービスである。属性は以下の 4 通りを持たせることができる。

- リード/ライトアクセス (セキュリティ認証必要)
- リード/ライトアクセス (認証不要)
- リードオンリアクセス (セキュリティ認証必要)
- リードオンリアクセス (認証不要)

サイクリックサービスタイプ

サイクリックサービスは、ブロック単位で任意のデータを読み書きできるサービスである。ユーザーブロックの中で、書き込みが行われた順番が記録されており、常に未書き込みブロック、または一番古いブロックに対して書き込みを行う。そのため、ブロックを指定して読み込むことは可能であるが、ブロックを指定して書き込むことはできない。属性は以下の 4 通りを持たせることができる。

- リード/ライトアクセス (セキュリティ認証必要)
- リード/ライトアクセス (認証不要)
- リードオンリアクセス (セキュリティ認証必要)
- リードオンリアクセス (認証不要)

パースサービスタイプ

パースサービスは、料金徴収などを想定して減算する機能を付加したサービスである。

2.3 秘密情報の分散

秘密情報を紛失などから守るためには、そのコピーを作って複数の場所に保存することが望ましが、コピーの数を多くすると盗難の危険が増大してしまう。一方、コピーの数を少なくすると、すべてを紛失してしまう危険が増大する。この相矛盾する二つの問題を解決する方法が“ 秘密分散共有法 ”[2] である。

2.3.1 秘密分散を利用したサービス

秘密分散を利用したサービスとして HITACHI が開発した“ 電子割符 ”[12] と呼ばれるものがある。そもそも割符とは従来からある考えであり、

1. 木片・竹片・紙片などに文字・図・絵を記し複数に分割する。
（ひとつひとつでは意味をなさない。）
↓
2. 全ての符が組み合わされる事により、始めて元の形に復元される。
（１つでも欠けたら復元できない。）

というものである。

この割符の機能をパソコンのデータに常時適用して、セキュアなデータ管理を実現するサービスがある。このサービスは「USB フラッシュメモリ」「電子割符クライアント」から構成されるシステムであり、以下のような特徴がある。

- 常に分割して管理するため「盗難・紛失」に強い
設定したフォルダの配下のファイルは、常に PC のローカルドライブと専用 USB フラッシュメモリに割符化（分散）された状態で格納される。盗難・紛失しても割符ファイルから、内容を推測することはできない。
- セキュアな USB フラッシュメモリにより情報を二重保護
専用のツールを使ってログインしないと、専用 USB フラッシュメモリ内のデータが見られない。万が一、専用 USB フラッシュメモリを紛失しても、第三者に参照されないため安心である。
- 専用画面によるファイル管理
割符ファイルを通常ファイルのように一覧表示する専用画面により、ユーザにファイル参照時やファイル登録時の割符化・復元を意識させない。また、専用画面から、ファイルの参照・更新を行うことで、終了時に自動的に割符化を行う。

- バックアップ・リストア機能/ロギング機能
  万が一の備えとして、専用 USB フラッシュメモリ内の割符ファイルのバックアップおよび、リストアが可能である。また、ユーザが専用画面で行った操作をログ情報として出力する。

2.3.2 (k,n) しきい値法

以降では、本研究で利用した秘密分散共有法の一つである“ (k,n) しきい値法 ”について述べる。

この秘密分散共有法では、秘密情報を n 人の管理者に分散させておくと、k 人未満の管理者では秘密情報は分からないが、秘密情報を紛失したときに k 人以上が集まると秘密を復元できるということが可能である。

以下では (k,n) しきい値法の概要を説明する。

(k,n) しきい値法のモデル

秘密分散共有法は、秘密情報 s の保有者 (ディーラ) と、複数の分散管理者の間で行われる。以降、ディーラを D、n 人の分散管理者を $P_1,\cdots,P_n$ で表す。秘密分散共有法は以下の図 2.2 のように分散段階と再構成段階によって構成される。

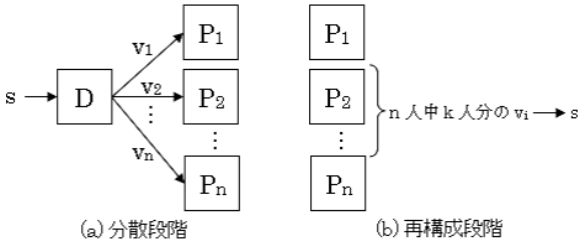


図 2.2: 秘密分散共有法

- **分散段階** 図 (a) のように、D は秘密情報 s から、n 個のシェアと呼ばれる $v_1,\cdots,v_n$ を計算し、v_i を P_i に与える。
- **再構成段階** 図 (b) のように、n 人の分散管理者のうち何人かが集まり、シェアから s を求める。

(k,n) しきい値法では、$v_1,\cdots,v_n$ は次の条件を満たすように作成されなければならない。

・$v_1,\cdots,v_n$ のうち、任意の k 個から元の秘密情報 s を復元できる。
・どの $k-1$ 個を集めても、s について何もわからない。

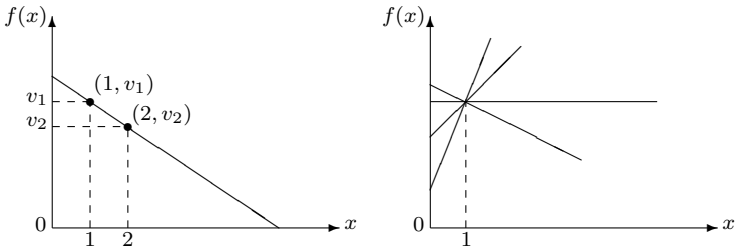
(k,n) しきい値法の例

(k,n) しきい値法の実現方法として、多項式補間を利用した Shamir(シャミア) の方法がよく知られている。以下に例を示す。

例 $(2,n)$ しきい値秘密分散共有法は、次のようになる。

- **分散段階** 秘密 s に対し D は a_1 をランダムに選び、$f(x) = s + a_1x$ とおく。D は次に、$v_i = f(i)$ を計算し、シェア v_i を P_i に与える。ただし、$1 \leqq i \leqq n$ である。

- **再構成段階** P_1, P_2 が集まったと仮定すると、図 2.3(a) に示すように 2 点 $(1, v_1), (2, v_2)$ を通る直線 $y = f(x)$ は一意に決まる。これより、$s = f(0)$ が求まる。このように、任意の 2 人が集まると s がわかる。しかし、P_i 一人だけでは、図 (b) に示すように直線は決まらないので、s について何もわからない。



(a)2 点から直線が求まる (b)1 点では直線は定まらない

図 2.3: 秘密分散共有法

2.3.3 実現方法

(k, n) しきい値法の一般的な実現方法を以下に記述する。(p が素数のとき、mod$p$ の世界を $GF(p)$ というのであった)

1. **分散段階**

   (a) D は、$p >\max(s, n)$ となる素数 p を選ぶ。

   (b) D は、$f(0) = s$ となる $GF(p)$ 上の高々$k-1$ 次の多項式
   $$f(x) = s + a_1 x + \cdots + a_{k-1}x^{k-1} \bmod p \qquad (1)$$
   をランダムに選ぶ。

   (c) D は、$v_i = f(i)$ を計算し、シェア v_i を P_i に与える。ただし、$1 \leqq i \leqq n$ である。

2. **再構成段階**

   k 人の分散管理者 $P_{i_1}, \cdots, P_{i_k}$ が集まったとき
   $$v_{i_j} = f(i_j) \bmod p \qquad (2)$$
   が $j = 1, \cdots, k$ で満たされるような高々$k-1$ 次の多項式 $f(x)$ を考える。実際、任意の $k-1$ 次以下の多項式 $f(x)$ は、$(i, f(i))$ の組が k 個あれば復元できる。具体的には、次の Lagrange(ラグランジェ) の補間公式が知られている。
   $$f(x) = \lambda_1(x)f(i_1) + \cdots + \lambda_k(x)f(i_k) \bmod p \qquad (3)$$
   ただし
   $$\lambda_j(x) = \frac{(x-i_i)\cdots\overset{j}{\vee}\cdots(x-i_k)}{(i_j-i_i)\cdots\overset{j}{\vee}\cdots(i_j-i_k)} \bmod p \qquad (4)$$
   式 (3) が成り立つことは、$x = i_1, \cdots, i_k$ を両辺に代入することにより、容易に確かめられる。式 (3) により、次式が得られる。
   $$s = f(0) = \lambda_1(0)f(i_1) + \cdots + \lambda_k(0)f(i_k) \bmod p \qquad (5)$$
   これより、任意の k 人が集まると、s を復元できることがわかる。

第3章　秘密分散システムの概要

本章では、第2章で述べてきた内容をもとに、FeliCa カードへ (k, n) しきい値秘密分散共有法を構築させる。

この提案システムによって、認証に必要とされる鍵情報のような秘密情報の管理を一か所（一部）から複数の互いに異なった情報へと分散させる。このシステムには、分散された情報からは、任意に設定された数の情報からでないと、元の秘密情報を復元することができず、設定数未満での情報からでは、秘密情報を何も知ることができない、という特徴を持っている。この秘密分散共有法の技術は“ 割符 ”の考え方を利用したものである。

このシステムを導入することによって、認証処理におけるセキュリティの安全性を向上させるだけでなく、秘密情報の紛失・漏えい、単独管理者による悪用を防ぎ、バックアップ効果を得られる。また、非接触型 IC カードの普及によるスキミング対策としても利用できる。さらに非接触技術を利用したスムーズな処理が期待できる。

3.1 システム構築の準備と手順

3.1.1 開発環境

本システムは、

- FeliCa チップを搭載した RFID
- FeliCa リーダ/ライタ
- リーダ/ライタを制御、
  および分散・再構成の計算行う上位機器

から構成される。

上位機器として、Windows を搭載したパソコンによるアプリケーションから Windows フォームを利用して、秘密情報の入力や計算などを行う。システムの構築は以下の環境で行った。

表 3.1: 開発環境

OS	Microsoft Windows XP Professional Service Pack 2
開発言語	Basic (Microsoft Visual Basic 2005 Express Edition) [16]
リーダ/ライタ	株式会社デンソーウェーブ製 PR-400UDM
カード	株式会社デンソーウェーブ発行 サンプルカード

なお、リーダ/ライタの制御はデンソーウェーブ独自のライブラリ [5] を用いることによって、プログラム中では関数として FeliCa のコマンドを利用することができる。

3.1.2 秘密分散システムの流れ

Windows フォームを利用して、以下のように分散段階（暗号）と再構成段階（復号）とに分けて処理が進行する。

分散段階（暗号）

1. 秘密情報 s の入力フォームを表示
2. テキスト入力 (半角英数字) で s を入力
3. カードに分散させる数値 n の入力フォームを表示
4. n を半角数字で入力
5. 再構成可能な数値 k の入力フォームを表示
6. k を半角数字で入力
7. 各カード $P_1, \cdots, P_n$ に書き込むデータ $v_1, \cdots, v_n$ を計算
8. 各カード P_i をリーダ/ライタにかざす確認をするフォームを表示
9. カードに v_i を書き込み
10. 8 から 9 を繰り返し（ただし $1 \leqq i \leqq n$）
11. 秘密情報の分散処理が完了

再構成段階（復号）

1. 再構成に利用するカード P_{i_j} をリーダ/ライタにかざす確認をするフォームを表示
2. カードから v_{i_j} を読み取り
3. 集めたカードの読み取りが完了するまで 1 から 2 を繰り返し（ただし $1 \leqq j \leqq k$）
4. 読み取った各 v_{i_j} から秘密情報 s を計算
5. カードの枚数・データの内容が正しければ s の復元は完了

3.2 システムのモデル

構築したシステムのモデルを分散段階、再構成段階の処理別にフローチャートで示した。分散段階の処理は図 3.2、再構成段階の処理は図 3.3 である。

今回提案するシステムでのカードに書き込むデータは、研究のしやすさを考えて以下のような形式とする。[18]

- 1 ブロック（16 バイト）ごとに、偶数ブロックを仮数部データ、奇数ブロックを指数部データとして保存する。
- 計算された結果である整数の下位 1 バイトごとに、偶数ブロックへ順次保存し、その指数は奇数ブロックへ保存する。
- 偶数ブロックの先頭バイト（0 番目）にはカード番号 i （$1 \leqq i \leqq n$）を格納し、
  奇数ブロックの先頭バイト（0 番目）には、チェック用に $(\mathrm{FF})_{16}$ を格納する。

以下の図 3.1 に、10 進整数「1234567」を保存する場合を例として示す。
（表示は 16 進数であるため $(1234567)_{10} \rightarrow (12\mathrm{D}687)_{16}$ である）
ここで、カード番号 $i = 1$、ブロック 0、1 に書き込むこととする。

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ブロック 0	01	87	D6	12	00	00	00	00	00	00	00	00	00	00	00	00
ブロック 1	FF	01	02	03	00	00	00	00	00	00	00	00	00	00	00	00

図 3.1: 10 進整数「1234567」の保存形式

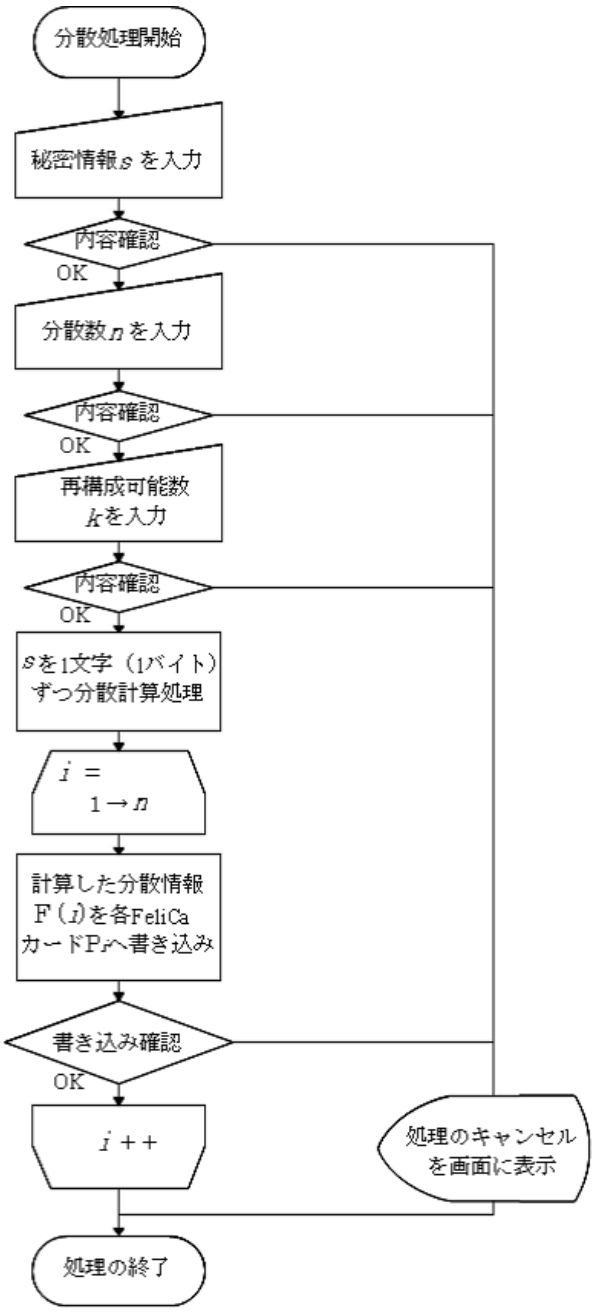


図 3.2: 分散段階の処理図

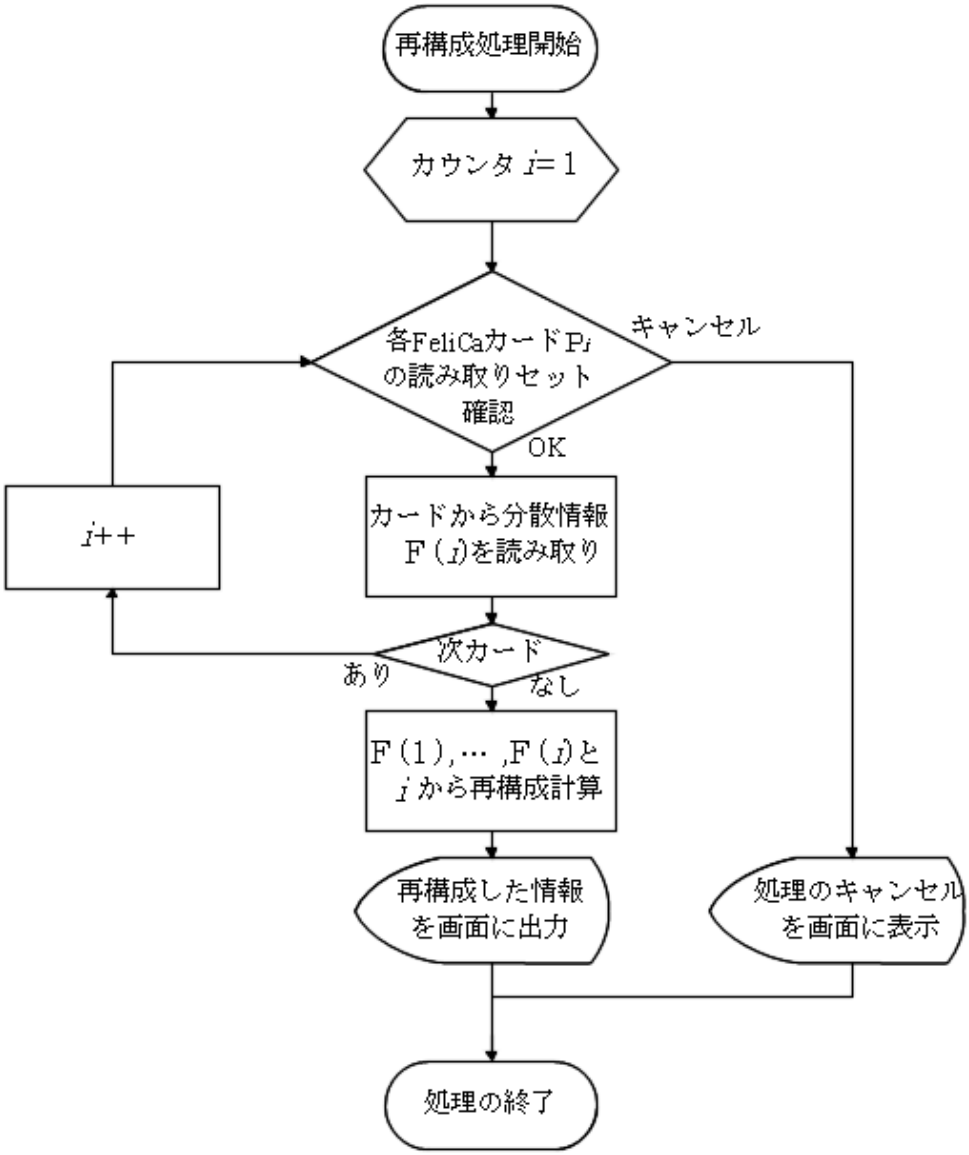


図 3.3: 再構成段階の処理図

3.3 システムの実行

提案したシステムの現段階における構築、および動作内容を次に示す。

3.3.1 実行テスト

例 以下の条件から実行テストを行った。

表 3.2: テスト内容

秘密情報 s	“ Hello!! ”
分散数 n	3
再構成可能数 k	2

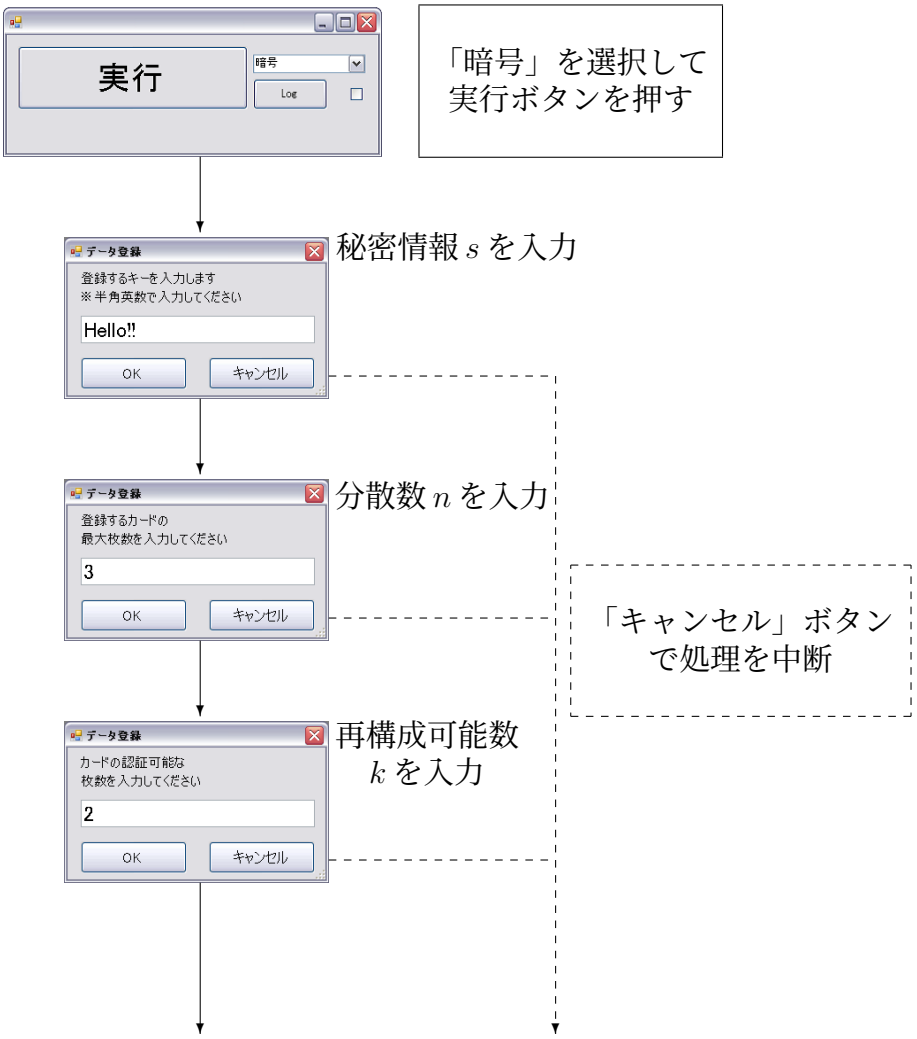
なお、秘密情報 s はバイナリデータに変換すると、

“ Hello!! ”→ 0x(48 65 6C 6F 21 21)

となる。これらを 1 文字ずつ計算して、分散処理を行う。

3.3.2 テスト結果

上記の例より各カードに分散情報を書き込み（暗号化）を行い、再構成（復号化）を行った結果、各カードすべての組み合わせにて秘密情報 s である“ Hello!! ”のデータを取得することができた。これらの実行結果を次の GUI 画面と共に次に示す。
（なお、実行内容は分散段階を暗号、再構成段階を復号とし、それぞれ図 3.4 & 3.5 および図 3.6 として区別して図に示している。）
また、カードに書き込まれたデータをそれぞれブロックごとに１６進数表示で図 3.7 に示す。



次ページへ

図 3.4: 分散処理（暗号）の実行テスト (1)

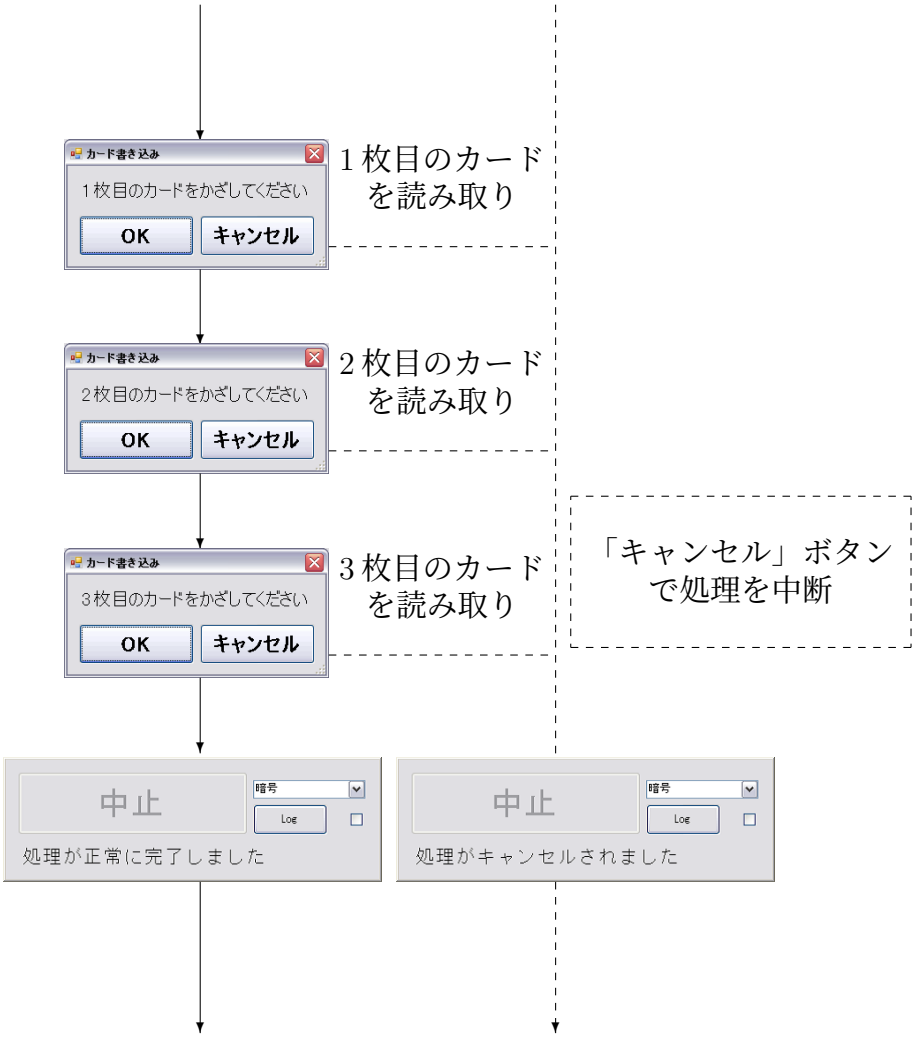


図 3.5: 分散処理（暗号）の実行テスト (2)

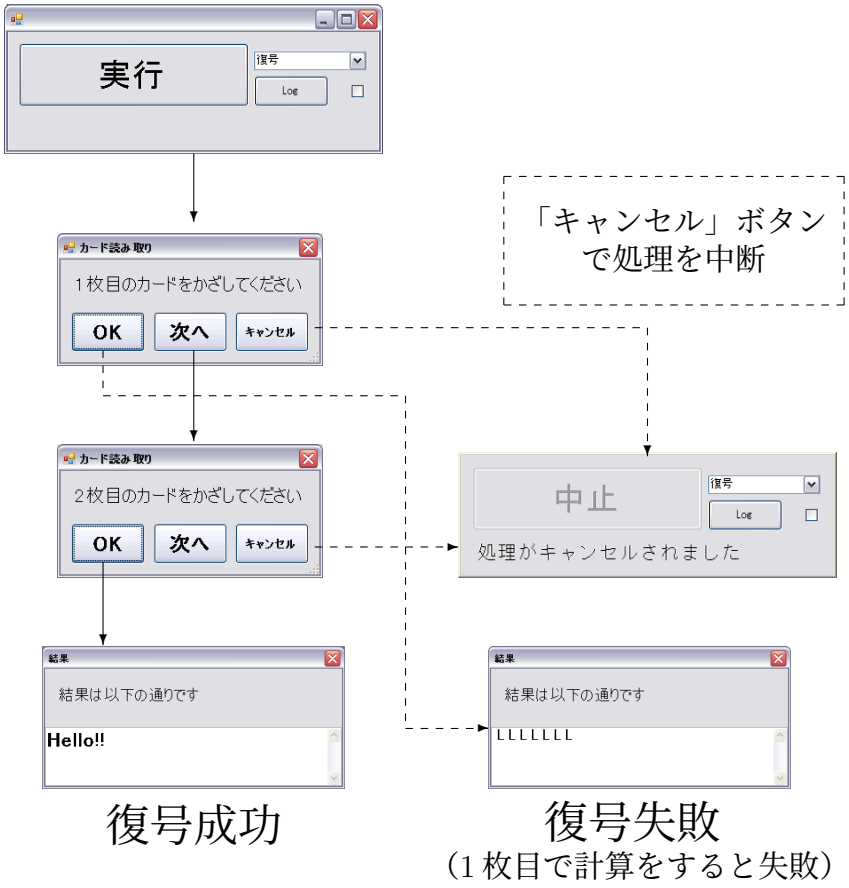


図 3.6: 再構成処理（復号）の実行テスト

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ブロック 0	01	27	01	44	01	4B	01	4B	01	4E	01	00	01	00	01	00
ブロック 1	FF	01	02	01	02	01	02	01	02	01	02	01	02	01	02	00

(a) カード 1 のデータ

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ブロック 0	02	06	02	23	02	2A	02	2A	02	2D	02	DF	01	DF	01	00
ブロック 1	FF	01	02	01	02	01	02	01	02	01	02	01	02	01	02	00

(b) カード 2 のデータ

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ブロック 0	03	E5	02	02	03	09	03	09	03	0C	03	BE	02	BE	02	00
ブロック 1	FF	01	02	01	02	01	02	01	02	01	02	01	02	01	02	00

(c) カード 3 のデータ

図 3.7: 各カードから読み取ったデータ

前述の図 3.7 より、3.2 の形式を参考にして秘密情報 s の各文字の分散情報を 10 進整数値に変換すると、以下の表 3.3 に示すとおりとなった。

表 3.3: 各カードの文字毎における分散結果

文字	分散値
1（H）	295
2（e）	324
3（l）	331
4（l）	331
5（o）	334
6（!）	256
7（!）	256

(a) カード 1

文字	分散値
1（H）	518
2（e）	547
3（l）	554
4（l）	554
5（o）	557
6（!）	479
7（!）	479

(b) カード 2

文字	分散値
1（H）	741
2（e）	770
3（l）	777
4（l）	777
5（o）	780
6（!）	702
7（!）	702

(c) カード 3

これらを 2.3.2 での再構成段階による式 (5) より、各秘密情報 s を復元すると、もとの s=“ Hello!! ”と同じ数値を得ることができたため、システムの動作を確認することができた。

第4章　評価

今回提案した秘密分散システムでの実行結果から得られた評価には以下のような内容が得られた。

- (k, n) しきい値秘密分散共有法を利用することにより、任意に決定した数よりも少ない情報では、秘密情報を得ることができなくなり、一人（一つ）の管理状態に比べてセキュリティ性の向上がみられると考えられる。
- 非接触によるデータの読み書きを行うため、処理がスムーズになり、システム運用などの面で利点がある。
- 本論文で述べたテスト運用では秘密情報 s に“ Hello!! ”の 7 文字（7 バイト）を用いたが、研究の中では、“ This is the test of Secret Sharing Schemes ”の 42 文字（42 バイト）の分散が可能であった。再構成可能数（認証可能数）によって、計算量が変化するため正確な分散可能文字数を求めることができなかった。
- 再構成可能数（認証可能数）が大きくなるにつれて、分散段階における計算値が大きくなり、１つの FeliCa チップに対するデータの量が大きくなってしまう。したがって、現在の FeliCa チップのメモリ容量は数 k バイトであるため、大容量のデータ保存に向いていない可能性がある。
- 今回のカードに保存するデータ形式は研究のしやすさを考え、簡易的な形式としたため保存量が少なくなってしまったが、分散段階における、計算値の保存に関するフォーマットを変えることによって現段階以上に保存できるデータ量が増えるのではないかと考えられる。
- FeliCa チップ搭載製品の利用に際して、サービスブロックやメモリとしての使用で自主利用をするためのフォーマット（発行）が必要となってくるため、その手続きなどが必要となってくる。

次の表 4.1 には、
テキストデータ“ A ”(16 進表記で 65) 1 文字を秘密情報 s として分散した場合の、
最大分散数 n を 10 までとしたとき、
再構成可能数 k を $2 \leqq k \leqq 10$ を条件として、各カード P_x に分散（書き込み）させる値、またそのバイト数を計算したものである。

表のようにカード (n) が増加および、カード番号が大きいもの程、書き込みに要するデータ量が必要となる。また同様に、再構成可能数 k が増加するほどデータ量が 10 倍されていることが分かり、網掛けされている部分に該当する条件下では、コンピュータの整数計算が桁あふれを起こし、処理が停止してしまうという結果が出てしまう。これらを改善するために更に分散・再構成での計算、カードへの書き込みのフォーマットの変更などが課題となった。

表 4.1: 分散条件の違いによる変換後データ（容量）の比較

( ) 内はバイト数

	$f(x)$								
カード P_x	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$	$k=10$
1	188 (1)	311 (2)	434 (2)	557 (2)	680 (2)	803 (2)	926 (2)	1049 (2)	1172
2	311 (2)	803 (2)	1787 (2)	3755 (2)	7691 (2)	15563 (2)	31307 (2)	62795 (2)	125771
3	434 (2)	1541 (2)	4862 (2)	14825 (2)	44714 (2)	134381 (3)	403382 (3)	1210385 (3)	3631394
4	557 (2)	2525 (2)	10397 (2)	41885 (2)	167837 (3)	671645 (3)	2686877 (3)	10747805 (3)	42991517
5	680 (2)	3755 (2)	19130 (2)	96005 (3)	480380 (3)	2402255 (3)	12011630 (3)	60058505 (4)	300292880
6	803 (2)	5231 (2)	31799 (2)	191207 (3)	1147655 (3)	6886343 (3)	41318471 (4)	247911239 (4)	1487467847
7	926 (2)	6953 (2)	49142 (2)	344465 (3)	2411726 (3)	16882553 (4)	118178342 (4)	827248865 (4)	5790742526
8	1049 (2)	8921 (2)	71897 (3)	575705 (3)	4606169 (3)	36849881 (4)	294799577 (4)	2358397145	18867177689
9	1172 (2)	11135 (2)	100802 (3)	907805 (3)	8170832 (3)	73538075 (4)	661843262 (4)	5956589945	53609310092
10	1295 (2)	13595 (2)	136595 (3)	1366595 (3)	13666595 (3)	136666595 (4)	1366666595 (4)	13666666595	136666666595

第5章　結論

現在、秘密分散共有法を適用した製品（電子割符 [12]）として USB メモリを利用したものがある。これは、コンピュータに搭載されているハードディスク（以下、HDD）に保存する秘密データを分散させ、その一部を USB メモリに格納することによって次回からの利用では USB メモリをコンピュータに接続して認証するという方法である。この製品の場合は、データの一部が認証を行う本体（コンピュータ）の HDD 内に保存されており、データの漏えいなどのセキュリティ性に少々不安がある。また、USB 接続であるため接触点が必要となってしまい、スムーズな認証が行えなくなるほか、現在最も汎用性があるインターフェースであるため、こちらにもセキュリティ性の面でも不安点がある。したがって、本研究での FeliCa を電子割符として、秘密分散共有法を適用したシステムを用いることにより、スムーズかつ安全な認証・データ暗号が期待できるのではないかと考えられる。また、前章にてメモリ容量が少ないことを述べたが、技術向上によりこの問題も徐々に解決されるものと考えられる。これには、現在の秘密分散法では処理に時間がかかってしまうことが問題とされていたが、数値演算を行う処理をコンピュータが効率よく処理できる論理演算のみを用いることによって高速化するという研究成果が株式会社 KDDI 研究所 [13] によって発表された。このアルゴリズムを用いることによって処理の高速化だけでなく、データ量の縮小化も実現できるのではないかと考えられる。FeliCa チップ（カード）の発行に関しても、セキュリティカードの利用としてこのシステムが多く利用されてくるのであれば、専用のフォーマットなどがされてくるのではないかと考えられる。

謝辞

本研究を行うにあたり、終始熱心に様々な面で数多くの有益なご助言・ご指導をしていただいた木下宏揚教授に心から感謝いたします。また、ご多忙の折大学に足を運びご指導いただいたネッツエスアイ東洋株式会社の森住哲也氏、ならびに研究活動に様々なご助力をいただきました鈴木一弘氏に深く感謝いたします。さらに、公私にわたり良き研究生活を送らせていただいた木下研究室の方々に感謝いたします。

参考文献

[1] SonyJapanFeliCa
＜ http://www.sony.co.jp/Products/felica/＞

[2] 『現代暗号の基礎数理』黒澤馨/尾形わかは
（コロナ社,2004）

[3] Microsoft: 流通サービスサイト RFID 入門
＜ http://www.microsoft.com/japan/business/rfid/about/default.mspx ＞

[4] FeliCa Networks （フェリカネットワークス株式会社）
＜ http://www.felicanetworks.co.jp/index.html ＞

[5] 機密による外部秘書類
デンソーウェーブより リーダ/ライタおよびソフトウェア付属使用説明書
「AID リファレンスマニュアル」
「PR-400UDM UsersManual」
「PR-CommandManual」
「PR 用開発支援ライブラリ 300-500F」
「PR-301/PR-400/PR-500FeliCa カード制御コマンドマニュアル」
「PR-301/PR-400/通信セキュリティマニュアル」
「サンプルカードフォーマット仕様表」

[6] 土居絵美 指導教員 清水明宏
高知工科大学 フロンティア工学コース 学士学位論文
携帯電話端末を用いた FeliCa 統合認証システム
＜ http://www.kochi-tech.ac.jp/library/ron/2006/2006info/
full/1070425.pdf ＞

[7] 寺尾良 指導教員 清水明宏
高知工科大学 情報システム工学科 学士学位論文
RFID システムへのワンタイムパスワード認証方式の適用
＜ http://www.kochi-tech.ac.jp/library/ron/2004/2004info/1050344.pdf ＞

[8] 井山幸大 指導教員 野口健一郎
FeliCa を利用したインテリジェント学生証の実装実験
＜ http://www.nol.info.kanagawa-u.ac.jp/research/2006/iyama.pdf ＞

[9] 非接触 IC に最適化された「FeliCa」の正体－@ IT
＜ http://www.atmarkit.co.jp/frfid/special/felica/felica01.html ＞

[10] トッパン・フォームズ株式会社 FeliCa
＜ http://www.rdsc.jp/felica/index.html ＞

[11] 注目の情報管理方式「しきい値秘密分散法」－@ IT
＜ http://www.atmarkit.co.jp/fsecurity/special/53tsss/tsss.html ＞

[12] HITACHI 電子割符シリーズ　株式会社 日立製作所
＜ http://www.hitachi.co.jp/Prod/comp/warifu/index.html ＞

[13] 超高速秘密分散方式の開発　株式会社 KDDI 研究所
＜ http://www.kddilabs.jp/press/detail_99.html ＞

[14] Suica ホームページ
＜ http://www.jreast.co.jp/suica ＞

[15] PASMO ホームページ
＜ http://www.pasmo.co.jp/＞

[16] Microsoft Visual Studio ホームページ
＜ http://www.microsoft.com/japan/msdn/vstudio ＞

[17] 東光電気株式会社 FeliCa
＜ http://www.tokodenki.co.jp/solution/felica/index.html ＞

[18] 『プログラミングに活かす データ構造とアルゴリズムの基礎知識』
今泉貴史（ASCII,2004）

質疑応答

1. Q：この提案システムで推奨される、認証可能数はどのくらいですか？
   （能登教授）
   A：分散させる秘密情報の容量によって異なりますが、３～４が推奨数です。

2. Q：FeliCa のカードに保存できる容量はどのくらいですか？
   （豊嶋教授）
   A：製品によって保存容量は違いますが、9K バイトの FRAM が搭載されているものがあります。
   また、フォーマットによって利用可能なブロックが決められるため、保存容量もそれに応じて変化します。