FeliCa チップへの秘密分散共有法の適用

木下研究室　　佐々木 賢　(200502689)

1　まえがき

近年、社員証や学生証・乗車券・電子マネーとして、読み取り面にカードをかざすだけで認証・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 (FeliCa:フェリカ) の利用が多くなっている。通常、認証には 1 枚のカードを利用するが、本研究では複数のカードに分散された情報のうち、任意の数の情報から認証が可能になるシステムを IC カードに構築させ、アプリケーションを作成・評価を行う。利点としては、秘密情報の複数管理者による同時認証や、データ紛失の際におけるバックアップ機能、セキュリティ性の向上などが考えられる。

2　技術的背景

FeliCa はソニー　が開発した非接触 IC カード技術である。このシステムは、「IC カード」「リーダ/ライタ」「(パソコンなどの) 上位機器」から構成される。IC チップに書き込まれたデータは「上位機器」から命令を受け、「リーダ/ライタ」を通して読み取り/書き込みが可能である。

3　研究内容

3.1　FeliCa 概要

FeliCa の IC チップが搭載された IC カードには図 1 で示すようにアンテナが付いており、リーダ/ライタから出力された電波から電力を得る。

IC のメモリ内にはチップを識別するための固有 ID が記録されている。また、ユーザが読み書きを行えるメモリも搭載されており、カード発行の際のフォーマットによってデータ容量は変化する。

3.2　秘密情報の分散・暗号方法

FeliCa カードに適用させる秘密情報の分散、および暗号化（秘密分散共有法という）には、「(k,n) しきい値法」という方法がある。

図 1 は (k,n) しきい値法の流れを表している。

- s: 秘密情報
- D: 秘密情報の保有者
- P_i: n 人の分散管理者
- v_i: D により s を分散させた情報

としたとき、n 人中 k 人から分散させた情報 v_i を集めて再構成を行うと、元の秘密情報 s を求めることができる。また、k 未満の分散情報を集めても s について何も分からないことが条件である。

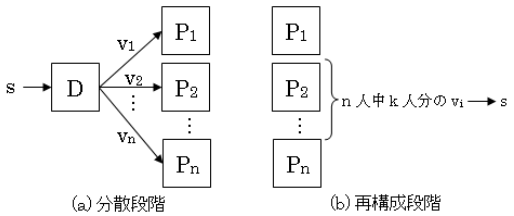

図 1: 秘密分散共有法

一般的に分散と再構成は次のように記述される。

・分散段階 (p は、$p > \max(s,n)$ となる素数)

$v_i = f(i)$ $[1 \leqq i \leqq n]$ としたとき
$f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1} \bmod p$
(a_a〜a_{k-1} はランダムな数である)

・再構成段階

$$s = f(0) = \lambda_1(0) f(i_1) + \cdots + \lambda_k(0) f(i_k) \bmod p$$
ここで、$\lambda_j(x) = \frac{(x-i_i)\cdots\overset{j}{\vee}\cdots(x-i_k)}{(i_j-i_i)\cdots\overset{j}{\vee}\cdots(i_j-i_k)} \bmod p$

3.3　システムの構築

FeliCa への秘密分散共有法は Microsoft Visual Basic 2008 Express Edition で、リーダ/ライタを制御するアプリケーションを通して構築した。リーダ/ライタは　デンソーウェーブの PR-400UDM を利用。

秘密情報のデータ形式としては半角英数字の入力に対するバイナリデータを秘密分散・暗号化した。

分散段階・再構成段階別における一連の処理は以下に示す。

分散段階
(1) 分散させる秘密情報を入力
(2) 分散させる FeliCa カードの数値を入力
(3) 認証が可能な最低値を入力
(4) 各 FeliCa カードへデータを書き込み

再構成段階
(1) データを各 FeliCa カードから読み込み
(2) 収集したデータから秘密情報を計算
(3) 復元した秘密情報の出力

以下の図 2 はシステムの GUI の一部である。

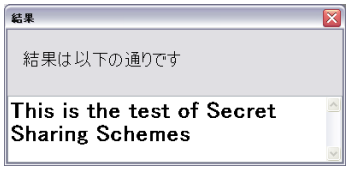

図 2: 分散された情報の再構成段階の GUI

4　評価

構築したシステムによって以下のような評価が得られた。

- 秘密情報の分散によってセキュリティ性の向上。
- USB メモリを媒体とした電子割符という製品がある。これらに比べると非接触認証であり、読み取り速度が速く、コストの面で利点がある。
- データの保存量が少ない。
- 認証可能数 (k) が大きくなる程、情報の分散後データが大きくなってしまう。

参考文献

[1] 「現代暗号の基礎数理」黒澤馨/尾形わかは (コロナ社,2004)

[2] 「PR 用開発支援ライブラリ (AID)」(DENSO WAVE INCORPORATE)