2009.02.16

FeliCaチップへの秘密分散共有法の適用

木下研究室
200502689
佐々木　賢

FeliCaと認証

- FeliCaは『RFID』(Radio Frequency Identification)という、電波を利用した認証(認識)技術のひとつである。ICチップを物や人物に付けて、認識・管理するために利用される。
- 通常、認証にはカード単体でのみ利用されることが多い。

図1　RFIDの利用例

図2　FeliCa導入例

“認証”での問題点

- 秘密情報が一か所に集中

↓

紛失・悪用などの被害増大

- 秘密情報を紛失から守るために、

「コピーを作成」 → 「複数の場所に保管」

↓

盗難の危険性増大

目的

- 秘密情報および管理者を複数に分散・暗号化することによって、

① **セキュリティ性**

② **バックアップ機能**

を向上し、FeliCaの非接触通信によるスムーズな処理による認証を行うシステムの構築

提案システムの導入によって

- 単独の管理者による秘密情報の紛失・流出・悪用を防ぐ
- 高度なセキュリティ性によるバックアップ
- 非接触技術を利用したスムーズな認証処理

提案システム

- 秘密分散共有法を利用

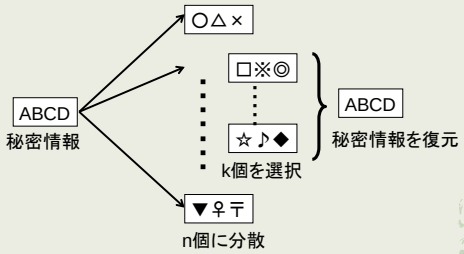


図3　秘密分散共有法

秘密分散共有法

- (k,n)しきい値法
  n個に分散させた秘密情報のうち、任意に集めたk個の分散情報から元の秘密情報sを求める。

・分散

$$f(x) = s + a_1 x + \cdots + a_{k-1}x^{k-1} \bmod p$$

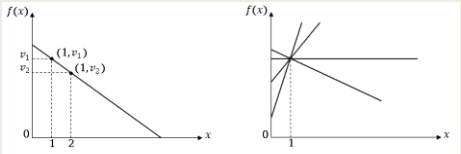
・復元（再構成）

$$s = f(0)$$
$$= \lambda_1(0) f(i_1) + \cdots + \lambda_k(0) f(i_k) \bmod p$$

ただし $\lambda_j(x) = \frac{(x-i_1)\cdots\overset{\downarrow}{\cancel{(x-i_j)}}\cdots(x-i_k)}{(i_j-i_1)\cdots\overset{\downarrow}{\cancel{(i_j-i_j)}}\cdots(i_j-i_k)} \bmod p$

(k,n)しきい値法

- (2,n)しきい値法の場合
  分散情報を2つ以上集めると、
  秘密情報を復元（再構成）することが可能



(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4 （2,n)しきい値法の例

提案システムの処理内容

FeliCa ①　FeliCa ②　FeliCa ③

分散＝暗号

①秘密情報、分散数、認証可能数を入力
↓
②分散数、認証可能数をもとに分散情報を計算
↓
③各FeliCaカードへ書き込み
↓
④秘密情報の分散が完了

再構成＝復号

①認証可能な数だけカードからデータを読み取り
↓
②読み取ったデータをもとに分散された秘密情報を計算
↓
③数・データが正しければ、正しい秘密情報の復元が成功

結果・評価

- 設定した数以下での分散情報からは、秘密情報の復元が不可能という結果が得られた。
- 秘密分散を採用したサービスとして、USBメモリを複数使用して、PCのHDDに保存されたデータを秘密分散させる管理ソフトがある。これに対し、非接触方式を利用したFeliCaを用いたことにより、スムーズな認証処理を行える効果が得られた。

結果・評価

- メモリ容量が少ないため、保存できる情報量が限られてしまう問題が発生した。

↓ 今後の課題 ↓

- 「秘密分散処理で用いた数値演算から、コンピュータ特有の論理演算を用いた処理にアルゴリズムを適用することによって、保存データ量の縮小化、処理の高速化が期待される」という研究成果を利用することによって解消。

ありがとうございました