An application of the Secret Sharing Scheme to the FeliCa

KINOSHITA Lab. SASAKI KEN (200502689)

Abstract

In this paper, we focused on the process of "Authentication" of contactless IC card systems which are daily used as the train-ticket (bus-ticket) ID-card and so forth. By only touching the card to the device-face of reader/writer, we can be authenticated. Usually we use only one card in the authentication. We built the "Secret Sharing Scheme" system in this study; it can rebuild and authenticate the secret-data by reading encrypted-datum dispersed to many cards (FeliCa-chips). By introducing this system, it will be possible to prevent from flowing out and making bad use of the information by the only one administrator, to establish the backup system to avoid losing data, and to improve the security performance. Then there is the advantage of authentication-process speed by using contactless communication.

本論文では、私たちが乗車券や社員証としてよく利用している非接触型ＩＣカードの“ 認証 ”という処理に着目している。カードの利用には、装置の読み取り面にカードをかざすだけで認証が可能という事が特徴である。通常、この認証では１枚のカードを利用するのに対し、本研究では、秘密情報を複数の FeliCa チップへ分散して、その中から任意の数だけ集めた情報から認証が可能になる”秘密分散共有”システムを構築する。このシステムを導入することによって、１人の秘密情報管理者による情報の漏えいや悪用問題、データ紛失を防ぐバックアップ機能、セキュリティ性の向上などが考えられる。また、非接触方式によるデータの読み書きが可能であるため、処理速度の速さも活用することができる。