システム情報工学研究科修士論文概要

年 度	平成 25 年度	学位名	修士(工学)
専 攻	知能機能システム 専攻	著者氏名	本庄 俊太郎

指導教員氏名 古賀 弘樹

論文題目

消失誤り訂正符号に基づくランプ型秘密分散法の安全性解析

論文概要

秘密分散法とは，秘密情報を分散符号化することで，紛失や盗難に対して安全に保管することのできる手法である．Shamir によって提案された(k,n)しきい値法では，n 個に分散したシェアのうち，任意の k 個のシェアからは秘密情報を復元でき，いかなる $k-1$ 個以下のシェアからも秘密情報は一切漏れない．しかし，(k,n)しきい値法を構成するためには，各シェアのサイズを秘密情報のサイズ以上にしなければならないことが知られており，符号化効率をよくするためにランプ型秘密分散法という手法が考案されている．ランプ型秘密分散法は，(k,n)しきい値法と異なり，秘密情報 L 個を n 個のシェアに分散し，$k-L$ 個以上のシェアからはその個数に比例して秘密情報が漏えいするが，シェアのサイズを秘密情報全体の $1/L$ にすることができる．一般に情報漏えい量は秘密情報全体のエントロピーに関して評価されるが，この際秘密情報の一部に関しても秘匿性を持つようなランプ型秘密分散法を，強いランプ型秘密分散法として区別している．強いランプ型秘密分散法においては，$k-1$ 個以下のいかなるシェアからも秘密情報の一部がシンボル単位で完全に復号されることはない．本稿では，MRD 符号を用いて強いランプ型秘密分散法を構成する手法を提案する．提案手法において，まず秘密情報 L 個と一様乱数 $k-L$ 個をある生成行列 G によって k 個の中間シンボルへと符号化し，k 個の中間シンボルを任意の生成行列 B によって n 個のシェアに分散符号化する．G は MRD 符号の検査行列の逆行列からなり，これによって任意の行列 B に対して，強いランプ型秘匿性を達成することを示している．さらに，提案手法はシェアの任意の線形変換によって生成された新たなシェアに対しても，強いランプ型秘匿性を維持することができる．また，行列 B に LT 符号の生成行列を使うことで，k 個に近いシェアから高い確率で秘密情報を復元することができる．

審査日 平成 26 年 1 月 29 日

審査員	（大学名 職名）	（学位）	（氏名）
主査	筑波大学 准教授	博士(工学)	古賀 弘樹
副査	筑波大学 准教授	博士(工学)	掛谷 英紀
副査	筑波大学 准教授	博士(工学)	延原 肇