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	坂下 光輝

指導教員氏名 古賀 弘樹

論文題目

低密度生成行列符号を用いた高速復号可能な秘密分散法の研究

論文概要

現代では情報は電子データとしてハードディスクや光ディスクなどの記憶装置に保管されるようになった. しかし, 紙などと比較するとハードディスクや光ディスクは故障する可能性があり, 故障による電子データの消失を防ぐため複製などを行い冗長性を持たせる必要がある. 一方電子データは漏らしてはないものであり, 複製などで冗長性をもたせた場合, 情報が漏洩するリスクが高まってしまう.

情報に冗長性を持たせた上で安全に管理する技術に秘密分散法がある. 秘密分散法は秘密情報を複数の「シェア」と呼ばれる分散情報に符号化し, あるシェアの集合になったときに元の秘密情報を復号できる. それ以外のシェアの集合からは元の秘密情報に関する情報は何も得られないか, 一部が分かる程度であり, 安全に情報を管理することができる. しかし, これまで提案されてきた秘密分散法は行列演算を用いるものが多い. 行列演算は一般に計算量が大きく, その実行速度が課題となっている.

一方, 情報の冗長性のみを考慮する技術に消失訂正符号がある. 消失訂正符号は元の情報に冗長性を持たせた符号語シンボルを生成する. 符号語シンボルの内いくつかの情報が消失しても元の情報が復元できる技術であるが, 秘密分散法とは異なり消失訂正符号は情報シンボルの安全性は考慮されていない. 消失訂正符号に LT 符号と呼ばれる低密度生成行列符号に分類される消失訂正符号があり, 元の情報シンボルの個数よりも少し多い符号語シンボルがあれば低い計算量で元の情報を復号できる符号として知られている.

本研究ではこの LT 符号をベースに高速に復号できる秘密分散法を提案する. LT 符号単独で秘密分散法を構成した場合, 安全性の尺度である条件付きエントロピーが下がるという問題があることが分かった. そこで本研究では LT 符号の前にプレコードと呼ばれる LT 符号とは異なる符号を連接することで条件付きエントロピーを増加させることを試みた. プレコードとして生成行列が置換行列と帯行列の積で定義される符号を用いることで, 9072 ビットの秘密情報に対し漏れる情報は平均高々5 ビット, 210(ms)以下の時間で復号できることを実験により確認した.

審査日 平成 25 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 教授	工学博士	水谷 孝一
副査	筑波大学 准教授	博士(工学)	掛谷 英紀