システム情報工学研究科修士論文概要

年 度	平成 26 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	島崎 憲明

指導教員氏名　古賀 弘樹

論文題目

(k, n) しきい値法における多数決ルールに基づいた不正検出とその性能評価

論文概要

秘密分散法の一種である「(k,n)しきい値法」では秘密情報 S から n 個の分散情報(シェア)が生成され，対応する n 人の参加者へそれぞれ配布される．もし任意の k 人以上の参加者が集まったならば，その k 個のシェアから秘密が正しく復元することができ，k 人未満しか集まらなかった場合，秘密に関する情報は一切漏れない。この手法の代表例として高々k-1 次の多項式を用いる Shamir 法が挙げられる。しかし Shamir 法では，参加者の中に配布されたシェアの値を改ざんする者(不正者)が存在し，k 個のシェアの中に改ざんされたシェアが含まれていた場合に，S の復元に必ず失敗してしまうという問題点があった。

改善策として筆者らは，シェアの改ざんを行う不正者の総数 c について $c \geqq k$ が満たされる状況において，n 個すべてのシェアを用いて復元を行う「改良多数決法」を提案した。しかしこの手法では，S の復元が可能となるのは $n-c>c+k-1$ が満たされる場合に限られていた。

そこで本稿では成功条件を拡張するべく，c が既知である状況下において，(c+2,n)しきい値法で生成されるチェックシェアを導入した「票数法」を提案する．本手法においてチェックシェアは，S に基づいて生成，各参加者に配布され，復元時には n 個すべてのシェアとチェックシェアが回収される。復元のアルゴリズムにおいては，考えうるすべての k 個のシェアの組み合わせから多項式が復元され，その中で重複するものが一定の個数以上存在する多項式のみを選ぶ。これらの多項式を復元可能なシェアを提出した参加者集合に対してチェックシェアを使った検査を行うことで，本来の正しい秘密 S の特定と不正者全員の検出を実現させる。このとき，もし $n-c=c+k-1$ あるならば，1 に近い確率で S が復元され，さらに不正者全員の特定も可能となる．また $n-c<c+k-1$ においても，(k,n)の組み合わせによっては，本来の正しい秘密 S の値と c 人の不正者の集合の候補を 2 つにまで絞り込むことができ，$n-c=c+k-1$ の場合と同等の結果を得ることが可能となる。

審査日　平成 27 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