論文の内容の要旨

論文題目　General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes

（秘密分散法および視覚復号型秘密分散法の一般的構成法）

氏名　岩本　貢

秘密分散法（Secret Sharing Scheme, SSS）は，秘密情報 S を n 個の分散情報に分散符号化し，秘密を復号できる集合（有資格集合，qualified set）に属する分散情報が全て集まると S が復号できるが，秘密情報を復号できない集合（禁止集合，forbidden set）に属する分散情報が集まっても秘密情報は全く洩れない符号化システムである．有資格集合の族と禁止集合の族の対をアクセス構造と呼ぶ．例えば，SSS として最初に提案された(k,n)しきい値法では，n 個の分散情報のうち任意の k 個以上から秘密情報を復号できるが，任意の $k-1$ 個以下の分散情報からは S に関する情報は情報量的に 1 ビットも漏洩しないように設計されている．このため，(k,n)しきい値法は分散情報の $n-k$ 個以下の破壊および $k-1$ 個以下の盗難の両方に対して安全性を保つことができ，データの保存や通信に有効な符号化法である．さらに，SSS はマルチパーティプロトコルの構成などにおいても重要な役割を果たすことが知られており，情報セキュリティにおける重要な基本技術のひとつとなっている．

一般の SSS では秘密情報は計算機上で復号される．これに対して，視覚復号型秘密分散法（Visual SSS, VSSS）では秘密情報が画像であり，それを分散画像に分散符号化する．復号は分散画像を重ね合わせるだけで行うことができ，復号に計算機を要しないという特徴をもつ．そのため，VSSS は災害時などでも使用可能な暗号として知られており，また理論的にも興味深い面を有している．本論文では，SSS および VSSS の符号化効率や安全性を議論し，新しい構成法を提案する．論文は 2 部から成り，第 1 部では SSS について，第 2 部では VSSS について扱う．

第 1 部では始めに，ランプ型 SSS の符号化効率について議論する．ランプ型 SSS とは有資格集合，禁止集合以外に秘密情報を部分的に漏洩するような集合を許すことで，符号化レートを従来の SSS（ランプ型と区別し，完全 SSS と呼ぶ）より小さくし，符号化効率を上げる方式である．また，完全 SSS は，部分的に漏洩する集合が存在しないランプ型 SSS と考えることができるため，ランプ型 SSS の特殊な場合と考えることもできる．本論文では，ランプ型 SSS の符号化レートの下限を導出するために，分散情報を super-additive, additive, sub-additive と呼ばれる 3 種類に分類する．完全 SSS においてはすべての分散情報が super-additive であることが暗黙のうちに仮定されており，この分類はランプ型 SSS において初めて必要となる．上記の分類に従うと，sub-additive な分散情報の符号化レートの下限は他の 2 種類の分散情報より明らかに大きくなることが示される．また，super-additive または additive な分散情報に対し，符号化レートの下限を導出する．

完全 SSS では，SSS はその符号化レートから ideal, non-ideal の 2 種類に分類され，それぞれの SSS の特徴が考察されてきた．これに対して本論文では ideal SSS の拡張として well-realized ランプ型 SSS を新たに定義し，どのようなアクセス構造をもつランプ型 SSS が well-realized となり得ないかを考察する．これらの考察は完全 SSS における，non-ideal SSS

の特徴づけの拡張に相当し，ランプ型 SSS の符号化効率の評価に関する従来研究のほとんどの結果を特殊な場合として含んでいる．

次に SSS の符号化手法を提案する．従来，(k,n)しきい値 SSS は任意の k, n に対し効率よく構成できることが知られている．しかし，一般アクセス構造に対する SSS 符号化法は非常に符号化効率の悪いものしか知られていない．例えば，伊藤らによる cumulative map は一般アクセス構造をもつ SSS を構成する簡単な方法であるが，アクセス構造が(k,n)しきい値法に近いと符号化効率が悪くなる．そこで本論文では「複数割り当て法」と呼ばれる一般アクセス構造をもつ SSS 構成法について考察する．複数割り当て法は，(k,n) しきい値法の分散情報を複数の参加者に割り当てることで，一般アクセス構造をもつ SSS を構成する手法の総称であり，cumulative map は複数割り当て法の一つの実現方法と考えることが出来るが，最適な符号化レートを達成する複数割り当て法の構成法は知られていない．本論文では，整数計画法を用いて最適な複数割り当て法を設計する方法を提案し， cumulative map による構成法と比較して符号化レートを大きく改善できることを示す．また，提案手法は容易に実装でき，従来は構成法がほとんど研究されていなかった，ランプ型 SSS や不完全なアクセス構造をもつ SSS などの，拡張された SSS を構成する際にも有効であることを示す．

第 2 部では，VSSS の構成法や安全性について議論する．まず，古賀らによって提案された VSSS の代数的構成法を紹介する．この代数的構成法は，カラー画像に対する VSSS に関して極めて効率よく，簡便な構成法を与えるものであったが，白黒画像に対して適用できないという問題点があった. この問題点は桑門らによって解決されたが, 彼らはその構成法しか与えておらず, この構成法の効率に関しては言及していない．そこで，本論文では VSSS の代数的構成法が，白黒濃淡画像を秘密画像とする(n,n)しきい値法の VSSS に対して最適な解を与えることを証明し，実際に最適な符号化手法を示す．この手法により，(n,n)しきい値法の濃淡画像 VSSS は極めて簡単に最適なものが構成できる．

次に，複数の画像を秘密画像とする VSSS に関して考察する．従来の複数画像を符号化可能な VSSS は白黒 2 値画像に対するものしか知られておらず，さらにそのうちいくつかの VSSS の定義では, 復号された秘密画像が他の秘密画像に関する情報を洩らしてしまうような場合があった．そこで本論文では，一般アクセス構造に対して画像を複数隠すことのできる VSSS に対して，復号された画像が他の画像に関する情報を全く洩らさないように厳密な定義を与え，そのような定義を満足する VSSS の構成法を与える．この VSSS の定義はカラー濃淡画像を扱うことができ，従来のほとんどの VSSS の定義を特殊な場合として含んでいる．以上のように，本論文では VSSS の定義，構成法を広範な範囲で与えることに成功している．