審査の結果の要旨

論文提出者氏名　岩本　貢

本論文は,「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)」と題し，９章と付録から構成されている．暗号技術は情報化社会を支える不可欠な技術であるが，その中で秘密分散法は情報の記録や通信において，破壊および漏洩の両方の脅威に対して安全な符号化法であり，情報セキュリティ技術の重要な研究テーマの一つになっている．本論文では，Part Ⅰで通常の秘密分散法(Secret Sharing Scheme, SSS)に対して，(1)SSS の符号化レートの理論的評価 (2)整数計画法に基づく一般アクセス構造の最適な実現法を取り扱っている．また，Part Ⅱでは，視覚復号型秘密分散法(Visual Secret Sharing Scheme, VSSS)に対して，(3)濃淡画像に対する VSSS の構成法および最適性の評価 (4)複数画像に対する VSSS 符号の構成法を取り扱っており，これらに対して新しい知見を与えている．

第１章「Overview of the Thesis」では，SSS 全般に対する研究の背景と目的を述べ，従来研究に対する本論文の位置付けを与えている．また，本論文の構成を示している．

第２章「Introduction to Secret Sharing Schemes」では，通常の SSS に関する研究動向を詳細に紹介すると共に，Part Ⅰに対する研究の位置付けを明らかにしている．また，しきい値型 SSS，一般アクセス構造，完全 SSS，ランプ型 SSS などの SSS に関する基本的な用語の定義を与えている．

第３章は，「Evaluations of Coding Rates in Secret Sharing Schemes」と題し，ランプ型 SSS に対する符号化レートを理論的に評価している．分散情報を「優加法的，加法的，劣加法的」の３種類に分類することにより，従来知られているものよりもタイトな符号化レートの下界を，分かりやすい手法で導出している．

第４章は「Constructions of Secret Sharing Schemes Based on Integer Programming」と題し，しきい値型の秘密分散法を用いて一般アクセス構造を効率よく実現する手法を与えている．従来知られていた cumulative map 法に比べ，本手法では，整数計画法を用いて最適な多重割り当てを行っているため，従来手法よりかなり効率がよい特長がある．また，提案手法は，ランプ型 SSS やアクセス構造が一部未定である不完備な SSS に対しても適用でき，今まで効率よく構成することが困難であった一般アクセス構造を容易に実現できるようにしている．

第５章「Conclusions of Part I」では，Part I の成果をまとめると共に，SSS に関する今後の研究課題を示している．

第６章「Introduction to Visual Secret Sharing Schemes」では，VSSS に関する詳細な研究動向を紹介すると共に，Part II で取り扱う VSSS の研究の位置付けを明らかにしている．また， VSSS のシステマティックな構成法である「代数的構成法」を詳細に紹介している．

第７章は「Visual Secret Sharing Schemes for Gray-Scale Images」と題し，濃淡画像に対する代数的構成法を与えると共に，代数的構成法で実現可能な最小の画素拡大率などを導出している．さらに，(n,n)しきい値型の場合，任意の VSSS が代数的構成法で実現可能なことを証明することにより，提案手法を用いれば全ての構成法の中で最適な VSSS を実現できることを示している．

第８章は「Visual Secret Sharing Schemes for Plural Secret Images」と題し，複数の秘密画像を一度に秘密分散する場合を取り扱っている．複数画像を符号化可能な従来の VSSS は，白黒 2 値画像に対するものしか知られておらず，さらにその幾つかの方式では，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欠点があった．これに対して，本論文では，複数の秘密画像を持つ 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な厳密な定義を与え，その定義を満たす VSSS の構成法を与えている．この VSSS は，白黒画像だけでなく，カラーや濃淡画像も扱うことができ，また，しきい値型だけでなく一般アクセス構造も実現可能である．

第９章「Conclusion of Part II」では，VSSS に関する Part II の成果をまとめると共に，今後の研究課題を示している．また，付録では，本論文で与えた構成法により作成した VSSS の具体例を，白黒画像，濃淡画像，カラー画像，複数の画像などに対して掲載している．

以上を要するに，本論文は，情報理論および数理工学的手法を用いることにより，理論的に安全性が保証され，かつ効率のよい汎用的な SSS および VSSS の構成法を与えており，その成果は，SSS や VSSS の今後の研究や応用において重要な指針を与えている．よって，本論文は，暗号理論の研究に大きく貢献するとともに，数理情報学の進歩に対して寄与するところが大であり，博士（情報理工学）の学位請求論文として合格と認められる．