平成 25 年度

第 7 回 喜安善市賞贈呈

（写真：敬称略）

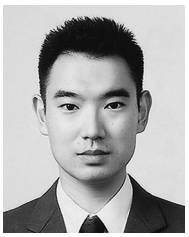
本会選奨規程第 17 条による喜安善市賞（第 7 回）は，下記の論文を選定して贈呈した．

Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight

（英文論文誌 A　平成 24 年 11 月号掲載）

受賞者 **栗原　淳**

受賞者 **植松友彦**



受賞者 **松本隆太郎**

秘密分散法とは，秘密を複数のシェア（情報片）に符号化し，シェアの特定の組合せからのみ秘密の復元を許す情報セキュリティ技術であり，分散ストレージシステム等に応用されている．なかでも，線形符号の組から構成できるランプ型線形秘密分散法はシェアのサイズを一定にしたまま秘密のサイズを幾らでも大きくできる利点を有するが，ランプ型線形秘密分散法を符号理論の観点から考察した研究は従来ほとんどなされてこなかった．

本論文では，まず任意の m 個のシェアと秘密 S の相互情報量の最大値が，線形符号の Relative Dimension/Length Profile（RDLP）と一致することを明らかにしている．更に，どの m 個のシェアも S の情報を一切与えない m の最大値 t_1，及びどの m 個のシェアからも S の一意復元を常に可能とする m の最小値 t_2 を，Relative Generalized Hamming Weight（RGHW）で正確に表せることを明らかにしている．加えて本論文では，漏えいした m 個のシェアと，ベクトルで表された S の各要素の任意の $\alpha-m+1$ 個の組合せの相互情報量が，任意の m について常にゼロとなる，秘密分散法の「α 強安全性」を山本の定義を拡張して提案している．そして，α の最大値もまた RGHW によって正確に表せることを明らかにしている．

以上のように本論文は，ランプ型線形秘密分散法に対する符号理論を用いたアプローチを新たに切り開くとともに，Forney の提案した DLP や Wei の提案した GHW に比べて従来，余り注目されず研究されてこなかった RDLP や RGHW に新たな意味付けと研究の動機付けを提供しており，これらの点から高く評価できる．