【119】

氏　名（国籍）	左（さ）　瑞麟（れいりん）（台　湾）
学位の種類	博　士（工　学）
学位記番号	博甲第 3951 号
学位授与年月日	平成 18 年 3 月 24 日
学位授与の要件	学位規則第 4 条第 1 項該当
審査研究科	システム情報工学研究科
学位論文題目	**A Study on Secret Sharing Schemes and Their Application to Identity-Based Key Agreement Schemes** （秘密分散とそれに基づく ID-Based 鍵共有方式に関する研究）

主　査	筑波大学教授	工学博士	岡本栄司
副　査	筑波大学教授	Ph. D.（組み合わせ論と最適化）	藤原良叔
副　査	筑波大学教授	工学博士	寅市和男
副　査	筑波大学助教授	博士（理学）	繆　瑩

論文の内容の要旨

本論文は Shamir の（k, n）閾値秘密分散法を中心に研究を行い，その方式に存在する問題点を解決し，さらに新しいプロトコルを提案した。また，Shamir 方式を用いて新しい ID-Based 鍵共有方式を提案した。具体的な研究成果は次のとおりである。

まず，shamir の方式は安全ではないため，本論文では，参加者が不正行為をした場合に元の秘密を正しく復元できるプロトコルを示し，ディーラの不正を検出する方法について提案した。次に，Shamir 方式の欠点を解決した。すなわち，参加者は自分のシェアを検証することができるが，正しくない場合，それを自分で訂正することができない。そこで，本論文では Shamir 方式を改良した新しい検証可能秘密分散法を提案し，参加者が協力してシェアを検証することができるようにした。一方，正しくないシェアを見つけた場合は，それを自分自身で訂正可能とした。さらに，Shamir 方式の拡張として，Shamir 方式を使った ID-Based3 者間鍵共有方式について提案した。従来方式では 3 者間鍵生成の前に，暗号文を送りたいユーザ（sender）は一回だけの予備通信を必要とするが，提案方式を用いると，予備通信なしの（non-interactive）3 者間鍵共有方式が可能となる。本論文の結果は，予備通信なしの ID-Based3 者間鍵共有方式を実現した初めての方式である。

審査の結果の要旨

秘密情報分散法をもとにその安全性の向上，弱点の克服，さらに応用として ID-based3 者間鍵共有方式を提案している。いずれも，新規性，有効性の観点から高い評価を受けており，申し分ない。

よって，著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。