【163】

氏　名（本籍）	金沢 史明（茨城県）
学位の種類	博　士（工　学）
学位記番号	博甲第 4626 号
学位授与年月日	平成 20 年 3 月 25 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	**双線形写像を用いた放送型暗号とその応用**

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. (Combinatorics and Optimization)	藤原良叔
副　査	筑波大学教授	博士（工学）	李　頡
副　査	筑波大学准教授	博士（工学）	満保雅浩
副　査	筑波大学講師	博士（情報科学）	岡本　健

論文の内容の要旨

近年，著作物のデジタル化技術が発展したことにより，有料放送等の放送型通信サービスが普及しつつあるが，放送型暗号はこうしたサービスに適した暗号方式である。送信者と受信者が一対一である従来の暗号方式とは異なり，この方式は一対多の暗号方式である。2005 年，Boneh らは，双線形写像を用いることで，暗号文サイズと秘密鍵サイズに関し，優れた性能を有する方式を提案した。しかし，この方式はコンテンツ送信者の正当性を保障する機能を有していない。

本研究では，Boneh らの方式を改良し，送信者認証機能を備えた放送型暗号方式を提案した。提案方式では，送信者が秘密鍵を明示的に使用し，署名生成と暗号化処理を同時に行う。このため，Boneh らの方式と既存の署名方式を単純に組み合わせた方式に比べ，秘密鍵サイズが小さく，鍵管理が容易である。また，Boneh らの方式の利点も引き継いでいる。

加えて，岡本らによる双対変換を用いて，先に提案した放送型暗号方式を元に，検証者指定署名と匿名署名の一種である 1-out-of-n 署名の機能を併せ持つ署名方式を提案した。この方式は，署名サイズがシステム加入者数に依存せず固定サイズであり，署名者匿名性と検証者限定性を有するため，より安全で効率的な内部告発者の保護が達成できる。

審査の結果の要旨

本研究は，鍵サイズが短く鍵管理が容易となる特長を有し，署名生成と暗号化処理を同時に行える送信者認証機能を備えた放送型暗号方式を提案している。また，応用として，署名サイズがシステム加入者数に依存せず固定サイズであり，1-out-of-n 署名の機能を併せ持つ署名方式も提案しており，より安全で効率的な内部告発者の保護が達成できる。

これらの研究は，従来にない優れた方式であるばかりでなく，実用的な方式である。以上により，本論文は博士論文の水準に達しているとみられる。

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。