論 文 内 容 の 要 旨

博士論文題目　Efficient Key Management Schemes in Broadcast Encryption
（暗号放送における効率的な鍵管理方式）

氏　名　野島　良

近年，インターネットの普及により，映画や音楽などのデジタルコンテンツを，コンピュータネットワークや放送網を通じて配布・販売する形態のサービスが実現されつつある．この種のサービスでは正当な対価を支払ったユーザ以外がコンテンツを利用できない仕組みを実現することが必須である．その有力な実現方法の一つとして，暗号コンテンツ放送型サービス（スクランブル放送，暗号放送）の技術がある．暗号放送では，あらかじめユーザ端末に暗号鍵を配布しておき，正当な対価を支払ったユーザだけが復号可能となるよう，コンテンツを暗号化して放送する．暗号放送を実現するためには，どの鍵をどの受信機に配布しておくかを決定する鍵管理方式が必要である．これまでにも多くの研究者が多くの鍵管理方式を提案してきたが，仕組み自体が単純であること，ユーザ端末にかかる負荷が比較的小さいこと等の理由により，Complete Subtree (CS) 方式 の実用性はかなり高いと考えられている．本研究の目的の一つは，暗号関連技術を利用することによって，秘密情報のサイズ削減等，CS 方式の効率化を行うことである．CS 方式の改良版として，二つの鍵管理方式 Two Permutations (TP) 方式，One-way Hash (OH) 方式が提案されている．暗号放送を実現するためには，各端末は暗号鍵の集合を保持しておく必要がある．TP 方式，OH 方式では，端末が，一個のシード情報のみから，あらかじめ設定された鍵かつそのような鍵のみを導出することができるよう，鍵情報の割当が行われる．これにより，端末が保持すべき秘密情報サイズを，端末総数に依存せず定数に抑えることが可能となる．TP 方式では，二個の落とし戸付き一方向置換を利用することで鍵情報の割当が行われる．方式が安全となるために二個の置換が満たさないといけない性質（安全性を保証するための十分条件）について検討が行われ，strongly semi-claw-free 置換対の概念が導入されている．OH 方式では，落とし戸付き一方向置換を一個だけ利用することで，鍵情報の割当が行われる．置換が一個だけで済むという実用上の長所に加え，strongly semi-claw-free 性というやや強い仮定を置く必要がないため，より実用的な方式であると考えられる．さらに，従来の暗号放送において考えられている条件設定とはやや異なる環境が仮定され，その環境において，効率の非常に良い鍵管理方式が提案されている．

氏　名	野島　良

（論文審査結果の要旨）

暗号放送とは，情報送信者の意図した相手だけが復号可能となるよう，情報を暗号化して同報通信する仕組みである．暗号放送の概念自体はかなり以前から存在していたが，近年，デジタルコンテンツの商業配布が現実のものになりつつあるのにつれて，従来よりも大規模な環境における暗号放送の仕組みが研究されるにいたっている．そのような暗号放送の仕組みを考える上においては，完全性（意図した相手が問題なく情報を復号できる）と安全性（意図しない相手が情報を復号できない）を達成することは当然のこととして，できるだけ効率の良い方式を模索することが必要となる．衛星放送のデコーダ等，ユーザの端末が鍵管理者からの情報を常時受け取ることができる場合は，完全性，安全性，効率性の全てを達成することは比較的容易である．一方，ＤＶＤプレイヤのように，オフライン型のユーザ端末を考える場合は，上記条件を達成することは技術的に困難であり，この問題に対する解決法を与えることは，社会的にも大きな意義があると考えられる．

本論文では，暗号放送の基本的な仕組みである木構造鍵管理方式の２つの具体方式，Complete Subtree (CS) 方式と Subset Difference (SD) 方式における，鍵サイズの削減法を議論している．これらの方式では，ユーザが保有する端末（デコーダ，プレイヤ等）は，暗号を復号するための鍵集合を保有する必要がある．これらの鍵情報はユーザ自身の目に触れることのないよう管理する必要があるが，一般に情報を秘密保持するためのコストは大きく，鍵情報のサイズはできるだけ小さくすることが望まれる．

本論文の前半では，CS 方式における鍵情報のサイズを削減する手法として，二つの鍵管理方式，Two Permutations (TP) 方式および One-way Hash (OH) 方式について議論している．暗号を復号するのに必要十分な鍵情報をユーザに提供するため，両方式とも，落し戸付き一方向性置換を有効に利用している点が特徴的であり，新規性の認められる点である．元の CS 方式では，木構造の各節点に与える鍵は独立に定めていたが，TP 法，CS 法では，落し戸付き一方向性置換を利用することにより，ある種のハッシュチェーンとして各鍵が導出されるようになっている．オリジナルの CS 方式では，ユーザ総数の対数に比例するだけの秘密情報をユーザ端末に記録する必要があったが，TP 法，CS 法では，ユーザ端末は一個のシード情報のみを保持するだけでよい．これにより，端末における秘密保持コストを小さくすることが可能となり，工学的意義は高い．本論文後半では，SD 法における前

提条件をやや緩めることで，やはりユーザ端末における鍵情報を削減する手法を提案している．元の SD 法は，ユーザ端末から鍵情報そのものが取り出された場合の安全性まで考慮した設計となっているが，現実世界ではそこまで強力な攻撃を想定しなくても良い場合も多く，その分の効率改善が望まれる場合も多く存在する．論文後半の結果は，そのような状況における一解法を与えるものであり，実用上の価値は大きいと考えられる．また，論文の前半，後半を通じて，安全性の議論を厳密に行っている点も評価できる．本論文では，確率的多項式時間アルゴリズムによる計算成功確率によって安全性の概念を定式化しているが，そのアプローチは近年のセキュリティ研究において標準的な手法と認識されており，本論文にて得られた定式化は，他の関連研究においても非常に高い有用性を持つと思われる．

以上のとおり，本論文で提案する手法と得られた結果は，情報セキュリティ，とりわけネットワーク社会における鍵管理技法に関する重要な知見を与えており，博士（工学）の学位論文として価値あるものと認める．