論 文 内 容 の 要 旨

博士論文題目 Theoretical Classifications of Security Notions on Public-Key Cryptosystems
（公開鍵暗号における安全性指標の定式化について）

氏　名 Ako Suzuki（鈴木 亜香）

本論文では，公開鍵暗号系の安全性について形式的な定義を与え，安全性に関する複数の概念間の関係を明らかにする．公開鍵暗号系に対しては，「与えられた暗号文から平文の内容が推測できない」という一方向性以外に，識別不可能性や頑強性等，さまざまな性質が要求される．これらの性質を議論する際には，ある種の計算可能性・不可能性の概念を，客観的に定義し表現する必要がある．Bellare らは，確率的チューリング機械の概念を利用することで，暗号が満たすべき性質のうち，識別不可能性と頑強性に関する形式的な定義を与えている．また，計算理論における「問題の還元」を応用することで，頑強性は識別不可能性よりも真に強い概念であること（すなわち，頑強性を満たす暗号は常に識別不可能性を満たす），適応的選択暗号文攻撃が可能な攻撃者にとっては，識別不可能性と頑強性とは安全性の観点から等価（以下，単に等価という）であることなどを示している．

本論文前半部では，公開鍵暗号の安全性に関する重要な性質のうち，Bellare らの研究で形式的定義が与えられていない等価判定不可能性と検証不可能性に対する形式的定義を与え，それらの関係がどちらも識別不可能性と等価であることを示す．等価判定不可能性とは，「与えられた 2 つの暗号文が同じ平文を暗号化して得られたものであるか否か判定できない」ような性質であり，検証不可能性とは，「与えられた暗号文が与えられた平文を暗号化して得られたものか否か検証できない」ような性質である．３つの異なる安全性に関する性質が等価であるということは極めて興味深い結果であり，この性質の重要性を示唆するものであると考えられる．

本論文後半部では，頑強性について，Bellare らの結果を一般化するような形で新しい形式的定義を与える．Bellare らの形式的定義では，攻撃者が平文の集合 M を出題者に伝え，出題者が無作為に M から選択した平文を暗号化することで，攻撃対象となる暗号文が構成される．直観的に，M に属する要素数が少なくなると攻撃者に有利となり，要素数が多くなると攻撃者に不利となる．本論文では M の要素数を 3 段階に分類し，それぞれに対応して，頑強性の形式的定義を 3 種類与える．また，それら 3 種類の頑強性の間には本質的な差異があること，Bellare らの結果は，3 種類の中で最も強いレベルの頑強性と等価であることを示す．さらに，暗号の一方向性についても同様の議論を展開し，一方向性の形式的定義を 3 種類与える． Goldreich による一方向性の形式的定義は，3 種類の中で最も弱いレベルの一方向性と等価となる．以上の結果は，Bellare らによる研究の結果，Goldreich による研究の結果を真に含むような形となっており，同時に，従来から指摘されていた，形式的な結果と現実世界において広く支持されている現象との不整合を解決するものである．

氏 名	鈴木 亜香

（論文審査結果の要旨）

本論文は，公開鍵暗号系の安全性について，形式的な立場からアプローチする論文である．公開鍵暗号系の安全性については，その提案当初より盛んに研究が行われてきた．公開鍵暗号系の安全性を考える上において最も基本的で重要なのは，（対称鍵暗号の秘匿性に相当する）一方向性と言われる性質，すなわち「与えられた暗号文から平文の内容が推測できない」という性質である．一方，公開鍵暗号系では，誰でも暗号化操作が可能（常に選択平文攻撃が可能であることに相当）であること，落とし戸付き一方向性関数の実現に数学的な構造が利用されていること等の理由により，一方向性とは異なる意味での安全性についても考慮する必要がある．たとえば，識別不可能性，頑強性，部分領域的一方向性，意味的安全性などについて，これまでに多くの研究がなされている．

本論文に関連する分野の先行研究としては，Bellare らによるものがある．Bellare らは，公開鍵暗号系の安全性に関する性質のうち識別不可能性と頑強性について，確率的チューリング機械（確率的アルゴリズム）の概念を用いた形式的な定義を与えている．直観的には，「有意な確率で暗号文の識別に成功するような多項式時間確率的チューリング機械が存在しない場合，その暗号は識別不可能である（頑強性についても同様）」とするのが，Bellare らの定式化である．確率的チューリング機械という計算理論的な概念を用いたことで，計算理論における「問題の帰着（還元）」を安全性の間に対応させることが可能となり，たとえば「頑強性を満たす暗号は必ず識別不可能性を満たす」といった関係を明らかにすることが可能となる．

本論文の前半では，Bellare らの研究では取り扱われていない 2 つの性質，すなわち，等価判定不可能性と検証不可能性に対する形式的定義を与え，それらの関係がどちらも識別不可能性と安全性の観点から等価（以下，単に等価という）であることを証明している．等価判定不可能性，検証不可能性とも識別不可能性とは独立して発想された概念であり，その形式的な定義も，識別不可能性の形式的定義とはまったく異なるものとなっている．にもかかわらず，これら 3 つの性質が等価であると言う本研究の結果はきわめて興味深いものであり，識別不可能性（等価判定不可能性，検証不可能性）の重要性を示唆するものであると考えられる．

本論文の後半では，頑強性および一方向性の形式的定義について，Bellare らの結果から一層深く踏み込んだ議論を行っている．Bellare らの定義によると，頑強性を議論する際には，攻撃者自身が指定した平文集合 M の中から，攻撃者とは別のエンティティである出題者が一様な確率で平文を選択し，選択した平文を暗号化することで攻撃の対象となる暗号文が構成される．どのような多項式時間攻撃者も出題された暗号文の中身を改変できないとき，その暗号は頑強性を満たすと言う．一般に，M が多数の要素を含むと攻撃者に取って不利な状況となり，多少強度の劣る暗号であっても，攻撃者が成功する可能性は小さくなる．本論文では，M の要素数に着目し，従来の Bellare らの定義を一般化するような形で 3 種類の頑強性の定義を与えている．また，それら 3 種類の頑強性の間には本質的な差異があることを明らかにしている．さらに，一方向性についても同様のアプローチを採用し，多くの安全性概念間の関係を明らかにすることに成功している．

以上の結果は公開鍵暗号の安全性に関して重要な知見を与えており，その発展に寄与するところが大きい．よって博士（工学）の学位論文として価値あるものと認める．