報告番号	甲　第　11911　号

主　論　文　の　要　旨

論文題目　関連鍵攻撃に対する公開鍵暗号要素技術の安全性に関する研究
(A Study on the Security of Cryptographic Public Key Primitives against Related-Key Attacks)

氏　名　森田　啓

論　文　内　容　の　要　旨

現代暗号の大きな分類として，共通鍵暗号系と公開鍵暗号系とがある．共通鍵暗号系では，通信のやりとりをする二者が同一の鍵を共有してデータの秘匿や認証などを行う．一方，公開鍵暗号系では，二者がそれぞれに秘密鍵と公開鍵のペアを持ち，公開鍵のみを公開し，秘密鍵は自身で保持した状態でデータの秘匿や認証などを行う．本論文においては，後者の公開鍵暗号系に着目し，その要素技術の中でも，非対話型鍵交換（Non-Interactive Key Exchange，略して NIKE）および署名方式について取り上げる．

NIKE は，二者が公開鍵の交換以外のやりとりをせずに共有鍵を計算することのできる公開鍵暗号要素技術である．これは，どのように二者間で秘密鍵を共有するのかという共通鍵暗号系特有の問題を解決する公開鍵暗号系の技術であり，Diffie-Hellman 鍵共有法が代表的な例の一つとして挙げられる．また，署名方式は，送りたいメッセージの偽造や改ざんを防ぐ公開鍵暗号要素技術であり，日常生活における印鑑やサインの役割を電子的に達成する技術である．Schnorr 署名方式，DSA，ElGamal 署名方式など，これまでに様々な方式が提案されてきた．

これまでに，NIKE 方式に対して Freire ら（PKC 2013）は，攻撃者の行える攻撃の種類の違いに関連して 4 つの安全性を定義し，それら安全性が実際には等価であることを示した．これにより，攻撃の種類が少なく記述の簡易な攻撃者に対して安全性を示せば十分であることが示された．加えて，Freire らは安全性証明の可能な NIKE 方式を提案した．なお，NIKE の安全性定義において攻撃者は，様々なユーザのペアが共有した鍵に関する知

識のみを用いて，新たなユーザのペアの共有鍵と乱数との識別をするよう要求される．署名方式に対する通常の安全性モデルでは，複数の正当なメッセージと署名のペアの知識だけを用いて，新たなメッセージに対する署名を偽造しようとする攻撃者を考える．偽造にはその種類によって，選択的偽造や存在的偽造と呼ばれるものがあり，攻撃者の動作には，これまでに得た情報を用いて適応的に攻撃を行うか，非適応的に攻撃を行うかなどいくつかの種類が考えられる．それら偽造の種類と攻撃者の動作の違いによって，複数の安全性モデルがこれまでに考えられている．暗号技術の研究・開発において，どのような安全性モデルを考慮するかは，対象とする暗号要素技術がどのような場面で利用されるかという現実問題に関連しており，最も説得力のある安全性モデルが採用される．

近年，タンパリングやフォルトインジェクション攻撃といったサイドチャネル攻撃を考慮に入れるために，Bellare と Kohno (Eurocrypt 2003) はより強力な攻撃者を考える理論的枠組みである，関連鍵攻撃 (related-key attacks，略して RKA) を定式化した．これは，通常の安全性では考慮されなかった，秘密鍵に変更を加え，その上で計算されたアルゴリズムの出力を得ることの出来る攻撃者を考えるものである．本論文では，今後の暗号技術の安全な利用のためには，これまで考えられていた通常の安全性では不十分だと考え，サイドチャネル攻撃を考慮に入れたこの RKA に着目し，NIKE 方式および署名方式の RKA 安全性について議論した．

各章の概要は以下の通りである．

第 1 章において，RKA，NIKE，署名方式の基本概念について説明し，本論文での貢献および関連研究について述べた．まず，暗号技術が実装されたハードウェアに対する電磁波等を用いた物理的な攻撃が，今後現実的な脅威となることを示し，そうした攻撃を理論的に扱う RKA について記述した．続いて，RKA の対象とする暗号要素技術である NIKE と署名方式について基本概念を説明し，関連研究を取り上げた．

第 2 章において，本論文で必要となる記法，証明に用いる計算量的仮定および補題を導入した．

第 3 章において，NIKE 方式に関する RKA について考察した．まず，Freire らの定義した安全性に基づいて，NIKE 方式に対して 4 つの RKA 安全性定義を与えた．これらの定義において，ユーザの秘密鍵を改ざんでき，その変更された秘密鍵を用いて計算された共有鍵を得られるような攻撃者を考える．ここで RKA 安全性は，攻撃者に許される秘密鍵への変更に対応する関連鍵導出関数 (related-key derivation function，略して RKD 関数) に関して定義される．この RKD 関数として，線形関数，アフィン関数，多項式などがこれまでに考えられている．本論文では，4 つの安全性定義間の含意関係および分離を示す．具体的には，本論文で RKA-CKS-light 安全性と呼ぶ安全性以外の 3 つの安全性定義は等価である一方，線形関数に関する RKA を考慮するならば，RKA-CKS-light 安全性はその他 3 つの安全性定義とは等価ではないことを示した．また本論文では，Freire らによって提案された NIKE 方式の一つが，符号付剰余群 (group of signed quadratic residues) 上で定義さ

れた Double Strong Diffie-Hellman (DSDH) 仮定のもと，ランダムオラクルモデルにおいて，最も強い RKA 安全性を満たすことを証明した．なお DSDH 仮定は，よく知られた素因数分解仮定から含意される仮定である．

第 4 章において，署名方式に関する RKA について考察した．特に，Schnorr 署名方式，DSA の変型，ElGamal 署名方式の変型の 3 つのよく知られた署名方式の，RKA 安全性について議論した．署名方式に対する RKA 安全性モデルでは，署名鍵を改ざんでき，その変更された署名鍵を用いて計算された署名を得られる攻撃者を考える．このとき RKD 関数は攻撃者が署名鍵に変更を加えることに相当する関数である．まず初めに，上記の 3 つの署名方式は，多項式に関する弱い RKA 安全性に関して安全であることを示した．次に，その一方で，Schnorr 署名方式も DSA も ElGamal 署名方式も線形関数に関する RKA 安全を達成できないことを，具体的な攻撃を示すことで証明した．最後に，Schnorr 署名方式，DSA（の変型），および ElGamal 署名方式の変型に軽微な修正を加えると多項式に関する RKA 安全性を満たすことを示した．

本論文では，NIKE 方式および署名方式の RKA 安全性のみを扱った．RKA 安全性は既存の安全性よりも強い安全性であるため，暗号技術が RKA 安全であることは，今後は暗号技術が満たすべき基本的な要件になると予想される．RKA 安全性に関して同様の議論を暗号化方式やサインクリプションなどその他の公開鍵暗号要素技術に対しても行うことで，より安全で安心な暗号技術の発展に貢献するものと期待される．