修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　情報理工学研究科　　情報・通信工学専攻　博士前期課程		
氏　　名	重松　諭	学籍番号	1031047
論 文 題 目	標数 3 におけるペアリング暗号へのフォールトアタックの提案と検証		

要　旨

ペアリングとは 2 入力 1 出力関数で各入力に対して線形性が成り立つ双線形関数のことを指す．具体的なペアリングとしては，楕円曲線上 2 点を入力とし，ある有限体の元であるものが提案されている．ペアリングというのは最初，1993 年に楕円曲線上の離散対数問題解法として用いられ，暗号の解読に利用されていた．その後，暗号設計として 2000 年に Joux らによって，ペアリングにより Diffie-Hellman 公開鍵配送方式が三者に拡張され，暗号の分野で用いられ始めた．近年，ペアリングを利用した暗号がユビキタス技術等の分野で着目されている．ペアリングを用いた暗号には，ID データベース暗号や，効率的なブロードキャスト暗号などといった新たな暗号システムがある．

しかし，ペアリング暗号の演算速度は他の暗号に比べ数倍遅いことが問題点として挙げられている．そこで，ペアリングの実装の際の演算をより高速に行うための手法が積極的に研究されている．高速なペアリングの演算方法として，Duursma-Lee アルゴリズムを用いたものや ηT ペアリングが挙げられる．

本論文では，ペアリングに対する攻撃についての研究を行った．元々，ペアリングに対する攻撃に関しては，点の乗算といくらかの補助計算によって効果的に演算が行われるアルゴリズムであるが故に，従来の楕円曲線暗号に対するサイドチャンネル攻撃と同じであると見られており，□新しい問題とは見なされてはいなかった．しかし，近年高速化の研究が進むにつれて演算方式が点の乗算とは関係がないものとなった．そこで，ペアリングへの攻撃として暗号装置の誤作動による出力に着目したフォールトアタック攻撃や，暗号装置の消費電力に着目したサイドチャンネル攻撃といった方法が提案されていった．これまでの研究では Duursma-Lee アルゴリズムに対する攻撃方法や，標数 2 における ηT ペアリングへの攻撃手法は挙げられていた．しかしながら，標数 3 における ηT ペアリングへの攻撃方法は未だ挙げられていない．本研究では，D.Page らが提案した Duursma-Lee に対する攻撃を実際に実装を行い検証し，また，D.Page らの提案したアルゴリズムを応用し，標数 3 における ηT ペアリングへのフォールトアタックを提案し検証を行った．