修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　電気通信　学研究科　情報通信工学　専攻　博士前期課程		
氏　　名	塙　知剛	学籍番号	0830048
論 文 題 目	Cryptanalysis of Lightweight Protocols Based on Learning Parity with Noise Problem		

要　旨

近年，RFID タグに代表される計算資源（計算能力，記憶容量）の乏しい機器向けの軽量な暗号プロトコルの研究が活発である．軽量向け暗号プロトコルとして HB#認証プロトコルが有望視されている．

HB#方式はリーダと計算資源の乏しいタグの間で行われる秘密鍵認証方式である．HB#の安全性は Learning Parity with Noise 問題の困難性に基づいており，受動的攻撃となりすまし攻撃に対する安全性が証明されている．なりすまし攻撃とは，攻撃者がリーダになりすましてタグと通信を行うことで，タグから秘密情報を不正に入手できる攻撃である．しかし，2008 年に HB#に対する中間者攻撃が考案されている．中間者攻撃とは，タグとリーダの間で行われる通信を改ざんし，認証結果から秘密情報を不正に入手できる攻撃である．

中間者攻撃による通信の改ざんを防ぐため，2009 年，Rizomiliotis はメッセージの改ざんを検出するメッセージ認証コード（MAC）として，軽量向けメッセージ認証方式 R-MAC を提案した．さらに，R-MAC を HB#方式に組み込んだ HB-MAC 認証プロトコルを提案した．彼は MAC の機能を用いると通信の改ざんを検出できるので，HB-MAC 方式は安全であると主張している．

本稿では，R-MAC で検出できない通信の改ざん攻撃と HB-MAC に対する受動的攻撃を提案して，R-MAC が中間者攻撃の対策にならないこと，HB-MAC が受動的攻撃に対して脆弱であることを示す．通信の改ざんを防ぐには R-MAC のセキュリティパラメータを約４倍に設定しなければならず，受動的攻撃を防ぐには HB-MAC 方式のセキュリティパラメータを約４倍にしなければならないことを示し，R-MAC 及び HB-MAC 方式が軽量機器向けの暗号プロトコルとしては不十分であることを示す．