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　　情報工学専攻　　博士前期課程		
氏　　名	Le Thi Ngoc Anh	学籍番号	0631033
論 文 題 目	A Scalable and Efficient Scheme for Privacy-Protected RFID Systems （プライバシー保護大規模RFIDシステムにおける識別処理の効率化）		

要　旨

RFID（Radio Frequency Identification、無線タグ、電子タグ）は物流、交通、文化、医療などに応用される。しかしながら、RFIDは常に同じ応答（タグＩＤ）を出力するため、人の行動が追跡される恐れがある。プライバシーを保護するため、要求に対しタグＩＤをハッシュして応答を変える手法がある。データベースは応答からＩＤを求め、タグを識別する。大規模RFIDシステムではタグ識別時間が膨大になり問題となる。Rainbow table を使ってタグ識別時間を減らす従来手法では、マージのため False alarm が生じる。False alarm が生じるとタグ識別時間が増える。例えば、長さ4666の1600万チェーンを持つRainbow tableでは、False alarmが生じる確率は96%である。従って、False alarmへの対策が必要となっている。Rainbow tableの各チェーンはstarting point SP, endpoint EPのペアで構成される。

False alarm が生じる場合、それらのマージ位置がわかると識別のためのハッシュ計算回数が削減できる。そこで、本研究は、Rainbow tableにマージ位置（merging position MP）を付加することにより、False alarmを制御する手法を提案する。マージ位置を付加したRainbow tableをMerging Position Rainbow Table（MPRT)と呼ぶ。ＭＰＲＴの各チェーンはSP, EP とMPで構成される。MPのビット長はチェーンの長さで決まる。MPでソートされたＭＰＲＴを使ってタグを識別する。

提案手法を実装し、タグ識別時間を測定した。タグを 99.9%の確率で識別できる条件のもとで、従来手法と比較し、チェーン長1024、タグ数130万、ひとつのタグに対する異なる応答数1024のとき、16.1%のメモリ量の増加で20.2%のタグ識別時間が削減できた。メモリ量を一定とすると、例えば300Mbとすると、タグの数が約300万以下では提案手法は従来手法よりタグ識別時間は短く、効率的に識別できることがわかった。