普遍再暗号化によるRFIDタグのプライバシ保護の実現

齊藤 純一郎† 櫻井 幸一††

Golle らは公開鍵に関する情報がなくても再暗号化を行うことのできる普遍再暗号化（Universal Re-encryption）を提案した.[2] この手法を用いれば，公開鍵を配送することなく公開鍵暗号による暗号文を再暗号化することができる．本論文では，ElGamal 暗号ベースの普遍再暗号化を用いて Radio-Frequency Identification（RFID）タグのプライバシを保護する方法について検討する．RFID タグは IC チップと無線通信用のアンテナを組み合わせた小型で安価な装置で，リーダと呼ばれる無線通信装置の問いかけに対し，タグに固有の ID をリーダに返すものである．しかし，リーダにより簡単にタグの情報が引き出されるため，RFID システムは消費者のプライバシを侵害する可能性がある．RFID タグの ID を暗号化して利用することができるが，特定の情報を追跡することで情報の内容が分からなくても対象を追跡することが可能である．よって，RFID システムを利用した対象の追跡によるプライバシの侵害に関して，普遍再暗号化を用いてタグの ID を再暗号化することによりタグの追跡を防ぐプライバシ保護の方法について議論する．

Re-encryption Scheme Using Universal Re-encryption for RFID Privacy Protection

Junichiro Saito† and Kouichi Sakurai††

Golle, Jakobsson, Juels, and Syverson proposed Universal Re-encryption which can perform re-encryption without knowledge of public keys. We can re-encrypt the ciphertext in a public-key encryption without delivering the public key. In this paper, we note on a privacy protection in Radio-Frequency Identification (RFID) tags using Universal re-encryption based on ElGamal. A RFID tag is a small and cheap device which combined IC tip and an antenna for radio communications, and it emits an ID in response to query from a reader which is a radio communication device. However, since the information on a tag is simply drawn out by the reader, a RFID system may infringe on a consumer's privacy. Although ID of a RFID tag can be encrypted, it is possible to pursue an object, even if its contents are not understood by pursuing specific information. Therefore, we discuss the privacy protection which prevents pursuit of a tag by re-encrypting ID of a tag using universal re-encryption about infringement of the privacy by pursuit of the RFID tags.

1. はじめに

Radio-Frequency-Identification（RFID）タグは，無線通信用のアンテナと IC チップを組み合わせた小型で安価な装置である．タグに問いかけを発し，RFID タグのメモリに書き込まれた ID を読み込む無線通信装置をリーダと呼ぶ．リーダによる問いかけの際，電力も一緒に送るものもあり，その場合，RFID タグ自体に電源は必要ない．そのため，RFID タグは将来バーコードの代わりのような識別機能を期待されている[3),5),8)~10)]．バーコードと同等の普及を目指すためには，RFID タグ 1 つあたりのコストは 5 円程度で，大きさは 0.4 mm × 0.4 mm 以下で紙に埋め込めるくらい薄いことが望ましい[3),4)]．

RFID タグにはいくつかの種類があり，通信距離，メモリの種類，電源の有無によって分類される[1)]．まず，通信距離には密接型（0〜数 mm），近接型（数 mm〜数 10 cm），遠隔型（数 10 cm〜数 m）がある．メモリには読み取り専用型，一度だけの書き込みおよび読み取り型，読み書き可能型がある．書き込み可能なメモリを搭載した場合，RFID タグの ID 情報をリーダ/ライタと呼ばれる無線通信装置により書き込むことが可能である．読み取り専用型の場合は，RFID タグの製造段階でその ID が決定される．また，RFID タグの

† 九州大学大学院システム情報科学府情報工学専攻
Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyushu University
†† 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

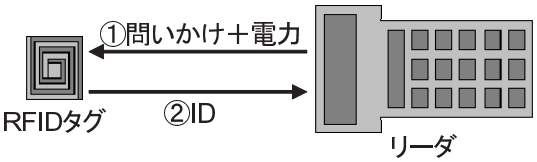

図 1 一般的な RFID システム
Fig. 1 Basic RFID system.

電源には能動型と受動型がある．能動型は RFID タグに電源を内蔵しており，受動型は前述したような方法でリーダから電力を得る．コストが低く利用が容易だという理由から，電源受動型のものが多く使われる．

このタグとリーダを利用した個別情報識別システムを RFID システムと呼ぶ．一般的な RFID タグとリーダのやりとりの様子を**図 1** に示す．RFID システムを用いれば，ダンボールの箱を開けなくても，中にあるタグの付いた商品を確認できるため，商品の在庫管理や物流管理に用いられる[3),4)]．タグは商品に取り付けられ，バーコードのような機能を果たしたり，盗難防止に役立ったりすることが期待されている．また，商品購入後も RFID システムは消費者に便利な機能をもたらす．たとえば，リーダ機能を持つ冷蔵庫がタグの付いた食料品の賞味期限を監視したり，洋服タンスが保管している衣料品から良い組み合わせを提案したりできるようになる[3)]．さらに，欧州中央銀行（ECB）はユーロ紙幣に RFID タグを埋め込むことを提案している[5)]．RFID タグの ID と紙幣に印刷されたシリアルナンバとを組み合わせた識別を用いて，高い偽造防止能力やマネーロンダリングの抑制が期待されている．

1.1 プライバシの保護

しかし，RFID タグの情報はリーダを使えば簡単に引き出すことができるため，タグの所有者のプライバシの侵害につながる[9),11)]．RFID タグには固有の ID が設定されるため，その ID を入手すれば，RFID タグの付いた対象の情報を得ることができる．たとえば，消費者の洋服のサイズや値段，財布の中身，店の商品の在庫情報などを知ることができ，所有者のプライバシが侵害される．また，RFID タグの ID 情報の内容を理解できなくても，特定の RFID タグの情報を追跡することで，RFID タグの所有者の居場所を突き止めたり，追跡したりすることが可能である．この位置情報に関するプライバシをロケーション・プライバシと呼ぶ[9)]．このため，小売店が消費者を追跡したり，商品の流通情報が漏洩したりしてしまうという問題が懸念される．これにより，所有者がさらなる被害を被ることも考えられる．紙幣に RFID タグが埋め込まれた場合，銀行で預金を引き落とした後に RFID の情報が読まれてしまい，正確に追跡され犯罪に巻き込まれてしまう可能性がある．よって，RFID タグの計算能力が低くリーダとのやりとりが簡単に傍受されてしまうという特性の下で，効果的なプライバシ保護の方法が必要になる．

本論文では，Golle らの提案した ElGamal 暗号ベースの普遍再暗号化[2)] を用いた RFID システムの安全性について検討する．このシステムは再暗号化の際に RFID タグの情報の改ざんに対して無防備であるため，攻撃者に利用される恐れがある．そこで，Golle らによって提案された普遍再暗号化を用いた RFID システムに対する RFID タグの情報改ざんを利用した攻撃方法を紹介する．Golle らは再暗号化を無効化する内容に改ざんする攻撃方法について言及していたが，本論分では攻撃者が復号化できる暗号文に改ざんする攻撃方法についても検討する．さらに，これらの攻撃方法に対処するために，再暗号化の際に RFID タグに書き込まれる情報を確認する確認付き再暗号化プロトコルを提案する．提案方式では RFID タグの計算量を最小限に抑えるために RFID タグの情報の一部のみを確認し，RFID タグの情報の改ざんによるロケーション・プライバシの侵害を防ぐ．

2. 関 連 研 究

これまでに提案された RFID タグのプライバシ保護の方法をいくつか紹介し，それらの問題点を示す．

2.1 RFID タグの機能を無効化する方法

最も単純な RFID タグのプライバシを保護する方法に，RFID タグの機能を無効化する方法がある[8)]．これは，機能を無効化する “kill” 命令により実行される．その際，RFID タグはパスワードを要求し，所有者以外この命令を実行できない．この方法を用いれば，消費者は商品を購入後，RFID タグの機能を無効化することができ，以後 RFID タグによるプライバシの侵害に悩まされることはなくなる．しかし，この方法にはいくつかの問題点がある．まず，前述したように，RFID タグには商品購入後も便利な使い方があるが，機能を無効化した場合それらを利用できない．また，返品された商品の管理に関する問題もある．返品された商品の RFID タグの機能が無効化されていた場合，その管理に RFID システムを用いることはできない．これらの問題を解決するために，機能停止命令と再開命令を用いる方法がある．この方法を用いれば，RFID タグの機能が不要なときには機能を停止し，必要になれば機能を再開させることができる．これらの命令は，機能無効化命令と同様に，命令実行の

際にパスワードを用いることが考えられる．しかし，電波による通信の特性上 RFID タグとリーダのやりとりは簡単に傍受されてしまうため，パスワードが盗まれてしまい，攻撃者にその機能を悪用される可能性がある．また，RFID タグの付いた対象が増えるにつれ，各 RFID タグの機能の状態を管理するのが煩雑になる．これらの問題を解決するために，RFID タグとリーダの通信に暗号化や認証を用いる方法がある[3]．

2.2 ハッシュ関数を用いる方法

ハッシュ関数を用いて RFID タグの情報を変化させ，RFID タグの情報漏えいとロケーション・プライバシの侵害を防ぐ方法がある[7]．この方法では，RFID タグの内部の情報を変化させるハッシュ関数と，RFID タグがリーダに送る情報に用いられるハッシュ関数が異なるため，情報が漏洩しても過去に収集した情報と一致させることが困難である．また，ハッシュ回路だけを利用するため，低コストで実装できる可能性がある．しかし，リーダ側で一致する情報を検索する際に，RFID タグで用いるハッシュ関数と同期をとるため，リーダ側の負担が大きい．また，ハッシュ関数により生成した値が他の RFID タグと衝突しないようにしなければならないため，拡張性に乏しいという欠点もある．

2.3 RFID タグとリーダの交信に暗号化や認証を用いる方法

RFID タグとリーダの交信は簡単に傍受されるためその通信に暗号化を適用したり，RFID タグが所有者や特定のリーダとだけやりとりができるように認証を用いたりする方法がある[10]．ただし，RFID タグ 1 つあたりのコストは 5 円程度が望ましいとされているため，RFID タグには限られた計算能力しか搭載できない．そのため，RFID タグが複雑な暗号化や認証プロトコルを処理するのは難しい．このような理由から，RFID タグがリーダを認証する方法を適用したとしても，認証に必要な情報を暗号化しても RFID タグはこれらの処理ができない．

しかし，リーダの能力は制限されていないため，RFID タグに書き込む内容を暗号化して書き込むことができる．これにより，RFID タグの情報が引き出されても内容を理解するのは困難になる．ただし，内容を理解することは困難であるが，情報を引き出すこと自体は可能である．そのため，暗号化された特定の情報を追跡することにより，特定の RFID タグの位置を特定したり追跡したりすることが可能である．これにより，ロケーション・プライバシが侵害されてしまう．よって，攻撃者に RFID タグの情報を理解されないように暗号化しつつ，引き出される情報を特定されないような方法が必要である．これは，暗号文を再暗号化することにより解決される．

2.4 RFID タグの情報を再暗号化する方法

前述した RFID タグの情報を暗号化する方法に加えて，暗号化された RFID タグの情報をさらに定期的に暗号化する方法がある[5),6)]．暗号文をさらに暗号化することを再暗号化と呼ぶ．これは公開鍵暗号方式を用いて実行され，鍵生成アルゴリズム，暗号化アルゴリズム，復号化アルゴリズムに加え，再暗号化アルゴリズムを必要とする．再暗号化には公開鍵が用いられる．再暗号化アルゴリズムには平文に関する情報を必要とせず暗号文を再暗号化し，何度再暗号化されても暗号文は一度の復号化により秘密鍵を用いて元の平文に復号化することができる．また，再暗号化に強秘匿の特性があれば，攻撃者は再暗号化された暗号文から元の暗号文を推測するのは困難である[2]．強秘匿性とは，どのような部分情報も部分解読困難なことを意味し，暗号文から平文に関する情報がいっさい漏れないことを表す．

この方法を用いれば，RFID タグの情報は再暗号化により定期的に変化するので，特定の RFID タグの情報を追跡することはできない．また，再暗号化の処理を書き込みのできるリーダ/ライタに処理させれば，RFID タグが複雑な処理をする必要はなく，RFID タグのコストを抑えることができる．ただし，公開鍵暗号方式の再暗号化を用いてリーダ/ライタに再暗号化を処理させる場合，再暗号化の際にリーダ/ライタに公開鍵を配送しなければならない．その際に，RFID タグとリーダ/ライタの交信を傍受され，公開鍵に関する情報が漏洩してしまう可能性がある[2]．複数の RFID タグを所持している場合，その所有者は複数の公開鍵を所持する可能性がある．そのため再暗号化をリーダ/ライタに処理させる際，RFID タグはそれぞれの公開鍵と RFID タグの情報を一致させるための情報をリーダに送信する必要がある．たとえば，複数の RFID タグを所持しており，それぞれの情報を別の公開鍵で暗号化しているとする．その場合，再暗号化の際にどの公開鍵を用いて再暗号化するのかリーダに伝えなければならない．そのためには，RFID タグの情報と再暗号化する公開鍵とを一致させるための情報が必要となる．そのような RFID タグと公開鍵を関連付ける情報をリーダに送信する際に攻撃者に傍受されてしまい，RFID タグを特定されてしまう可能性がある．よって，RFID タグ自体の情報が漏洩しなくても，特定の公開鍵に関連する RFID タグを追跡することが可能とな

り，ロケーション・プライバシが侵害されてしまう．ここで，RFID タグの内部で再暗号化を処理させるということが考えられるが，RFID タグの計算能力が制限されているためそれは困難である．

3. 普遍再暗号化を用いた RFID タグのプライバシ保護

再暗号化の際に公開鍵を利用した場合，公開鍵を特定することで関連する RFID タグを特定されてしまう．また，複数の RFID タグを利用している場合，複数の鍵を管理し配送しなければならない．そこで，再暗号化の際に Golle らによって提案された普遍再暗号化（Universal Re-encryption）を用いることができる．普遍再暗号化を用いれば，再暗号化のために鍵を配送することなくリーダ/ライタに再暗号化の処理をさせることができる[2]．この方法では，鍵により RFID タグを特定されることがないので，第三者に再暗号化を依頼することもできる．また，鍵を配送しなくてよいため，再暗号化を依頼された第三者は公開鍵から RFID タグを特定することが困難である．さらに，第三者に再暗号化を依頼することで頻繁に再暗号化を行うことができ，攻撃者は RFID タグを特定するのがより困難になる[2]．結果として，普遍再暗号化を用いた RFID システムでは，RFID タグのロケーション・プライバシに関する高い保護能力を得る．

3.1 普遍再暗号化

普遍再暗号化は Golle らによりミックスネットのために提案された公開鍵暗号方式である[2]．普遍再暗号化は通常の再暗号化とは異なり，再暗号化の際に公開鍵の知識を必要とせず，暗号化と再暗号化のための乱数を決定することによって再暗号化が行われる．また，暗号化の処理とは異なり，再暗号化には平文に関する情報はいっさい必要ない．復号化の際には，秘密鍵を用いれば何度再暗号化を行った暗号文でも一度の復号化で平文に戻すことができる．

さらに，普遍再暗号化はミックスネットにおけるプライバシ保護に必要な強秘匿性を満たす[2]．この特性は暗号化の処理と同様に，再暗号化の際にも満たされており，暗号文を再暗号化した暗号文から，元の暗号文に関する情報はいっさい漏れない．

3.2 ElGamal 暗号を基にした普遍再暗号化を用いた RFID システム

Golle らによって提案された普遍再暗号化を RFID システムに適用した場合を考える．この暗号化システムに必要なアルゴリズムは，鍵生成アルゴリズム，暗号化アルゴリズム，復号化アルゴリズム，再暗号化アルゴリズムである[2]．まず，RFID タグは読み書き可能型を用いる．再暗号化の処理は，RFID タグの所有者が再暗号化の処理を行うことができるリーダ/ライタをつねに所持しておき，それにより定期的に実行される．また，再暗号化の際に公開鍵を配送しないという普遍再暗号化の特性を利用すれば，銀行や公共機関などの信頼できる第三者が RFID タグの再暗号化サービスとして提供することも可能である[2]．考察するモデルでは，再暗号化は第三者が行うものとする．

3.3 モデルの定義

まず，RFID システムにおけるモデルを定義する．モデルには，所有者，サービス提供者，再暗号化を行う第三者，攻撃者が存在する．それぞれ，以下のように定義する．

所有者：RFID タグの所有者で，鍵を生成できるリーダ/ライタを所持する．また，リーダ/ライタを用いて最初の暗号化を行い，RFID タグにその情報を書き込む．

サービス提供者：RFID タグの情報をリーダにより引き出し，秘密鍵を用いて情報を復号化し，得られた情報からサービスを提供する機関や所有者の所持する装置．所有者とサービス提供者の間の秘密鍵の受渡しは既存の安全な方式を用いて行われるものとする．

再暗号化を行う第三者：リーダ/ライタにより再暗号化の処理を行う第三者．ここでは，正しい手順で再暗号化を行う第三者を，信頼できる第三者とする．第三者は普遍再暗号化の特性により，再暗号化に使う乱数や以前の暗号文，再暗号化した暗号文を収集してもかまわない．

攻撃者：RFID タグから情報を引き出し，所有者のロケーション・プライバシを侵害しようとする．

3.4 普遍再暗号化のプロトコル

実際に ElGamal 暗号を基にした普遍再暗号化のプロトコルを紹介する．$E[m]$ を ElGamal 暗号での平文 m に対応する暗号文とする．普遍再暗号化でのメッセージ m の暗号文は $[E[m]; E[1]]$ で表される[2]．そして ElGamal 暗号の準同型性の性質を利用する．準同型性とは暗号文 $E[a]$，$E[b]$ に対し，$E[a] * E[b] = E[ab]$ を満たす演算子 “*” の性質のことをいう[2]．この性質を利用することにより，公開鍵を配送しなくても再暗号化の処理を行うことができる．なお，ElGamal 暗号を基にした普遍再暗号化は，同じ長さのメッセージ長，鍵の長さを用いた場合 ElGamal 暗号の半分の強

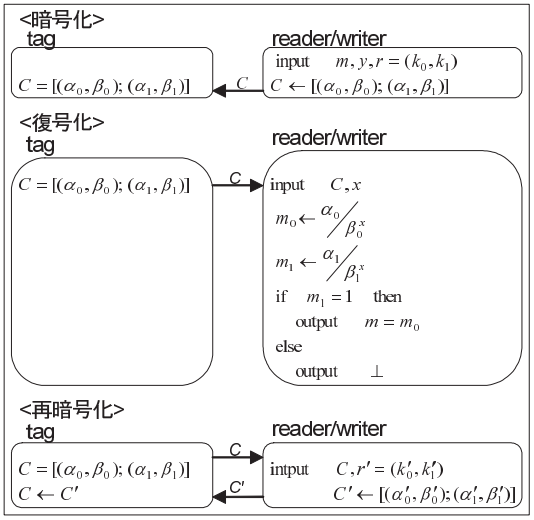

図 2 普遍再暗号化を用いた RFID システムのプロトコル
Fig. 2 RFID system using Universal Re-encryption.

度を持つ[2]．つまり，ElGmal 暗号と同等の安全性を得るためには，メッセージ長，鍵の長さをそれぞれ 2 倍にする必要がある

以下に鍵生成アルゴリズム，暗号化アルゴリズム，復号化アルゴリズム，再暗号化アルゴリズムのプロトコルを示す．

鍵生成：所有者がリーダを用いて秘密鍵 x と公開鍵 $(y = g^x)$ を生成．

暗号化：メッセージ m と公開鍵 y，乱数 $r = (k_0, k_1)$ を RFID タグの所有者のリーダ/ライタに入力する．そして，暗号文 C を以下のような式により導き出す．

$$C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$$
$$\alpha_0 = my^{k_0}, \beta_0 = g^{k_0}, \alpha_1 = y^{k_1}, \beta = g^{k_1}$$

生成された暗号文 C はリーダ/ライタによって RFID タグに書き込まれる．

復号化：サービス提供者は RFID タグから公開鍵 y で暗号化された暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ を引き出し，秘密鍵 x とともにリーダに入力．そして，$m_0 = \alpha_0/\beta_0^x$ と $m_1 = \alpha_1/\beta_1^x$ を計算し，$m_1 = 1$ ならば メッセージ $m = m_0$ として出力する．そうでなければ，復号化は失敗したことになり，記号$\perp$を出力する．その際，暗号文 C が何度再暗号化されていても，一度の復号化により平文に戻すことができる．

再暗号化：再暗号化を行う第三者は暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ を RFID タグから引き出し，乱数 $r' = (k_0', k_1')$ とともにリーダ/ライタに入力．そして再暗号化した暗号文 C' を以下のような式で導き出す．

$$C' = [(\alpha_0', \beta_0'); (\alpha_1', \beta_1')]$$
$$= [(\alpha_0 \alpha_1^{k_0'}, \beta_0 \beta_1^{k_0'}); (\alpha_1^{k_1'}, \beta_1^{k_1'})]$$

再暗号化された暗号文 C' はリーダ/ライタにより RFID タグに書き込まれる．

暗号化プロトコル，復号化プロトコル，再暗号化プロトコルにおける RFID タグとリーダ/ライタのやりとりの様子を**図 2** に示す．

4. 普遍再暗号化を用いた RFID システムの安全性の検証

普遍再暗号化を適用した RFID システムの安全性を検証する．まず，RFID タグの機密性とロケーション・プライバシの安全性について見ていく．

RFID タグの機密性について

普遍再暗号化を用いた RFID システムでは RFID タグに書き込まれる内容はあらかじめ暗号化されているため，攻撃者がその内容を理解するのは困難である．そのため，RFID タグの付いた対象を識別するのは困難となるため，所有者の所持品に関する情報を攻撃者に知られることはない．また，普遍再暗号化の強秘匿性により，再暗号化された暗号文から以前の暗号文を推測することは困難であるため，再暗号化された RFID タグを特定することはできない．このため，特定の RFID タグの情報の機密性は保護される．

ロケーション・プライバシの安全性について

再暗号化により RFID タグの情報は定期的に変化するため，特定の情報を追跡することができず RFID タグのロケーション・プライバシは保護される．また，第三者に再暗号化を依頼することで，再暗号化の処理を頻繁に行うことができ，RFID タグの追跡防止能力をさらに高めることができる[2]．

また，第三者が再暗号化のための乱数や，再暗号化する前の暗号文や再暗号化した後の暗号文を収集して追跡に利用することが考えられる．しかし，次に再暗号化が行われた際に，普遍再暗号化の強秘匿性により一致する再暗号文を識別するのが困難であるため，この方法による追跡は困難である．

しかし，再暗号化の際に RFID タグの情報を書き換えることができるため，攻撃者が RFID タグの情報を改ざんすることが考えられる．これにより，RFID タグのロケーション・プライバシが侵害される可能性がある．

4.1 普遍再暗号化を用いたシステムに対する攻撃

普遍再暗号化を用いた RFID システムでは，再暗号化の際に RFID タグの情報を書き換えることができるため，それを利用した攻撃方法が考えられる．その際，攻撃者は RFID タグの内容を書き換えることのできるリーダ/ライタを所持している．そのような状況で考えられる攻撃方法を 2 つ示す．

攻撃方法（1）：RFID タグの内容を攻撃者が復号化できる暗号文に書き換えた場合．この場合，その後再暗号化が行われても，攻撃者は RFID タグの情報を復号化することが可能である．

攻撃方法（2）：再暗号化の処理を無効化する内容に書き換えられた場合．再暗号化の際に，攻撃者が RFID タグのメモリに記録された暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ を $C' = [(\alpha'_0, \beta'_0); (1, 1)]$ となるように書き換えるかもしれない．このような攻撃は，暗号文の鍵確認を通り抜けるものである．なお，鍵確認は以下のように行っている．

$$m_1 = \alpha_1 / \beta_1^x$$

m_1 が 1 のとき，鍵確認のチェックを通る．このチェックを通る値には以下のようなものがある．

(1) $\alpha_1 = y^r$ かつ $\beta_1 = g^r$ のとき ($y = g^x$)
(2) $\alpha_1 = \beta_1 = 1$ のとき
(3) x が偶数の場合，$(\alpha_1, \beta_1) = (1, -1)$
(4) x が奇数の場合，$(\alpha_1, \beta_1) = (-1, -1)$

(2) から (4) の場合，暗号文が変化しない，もしくは変化が規則的であるため，攻撃に利用される．

攻撃方法（1）により，攻撃者は RFID タグの情報を復号化できるため，自らが設定した情報を追跡することにより，特定の RFID タグを追跡することが可能となる．また，攻撃方法（2）では，RFID タグの情報はその後再暗号化されても変化しないので，攻撃者は自らが再暗号化した暗号文を追跡することで，特定の RFID タグを追跡することが可能となる．攻撃方法 (1), (2) のやりとりの様子を**図 3** に示す．

以上の方法を用いることにより，攻撃者は特定の RFID タグを追跡することが可能となり，RFID タグのロケーション・プライバシが侵害される．

4.2 確認付き再暗号化プロトコルの提案

これらの問題を解決するために，再暗号化の際に RFID タグが書き込まれる内容を確認する確認付き再暗号化プロトコルを提案する．この方法では，なるべくコストをかけずに実現できるようにリーダ/ライタの認証は行わず，再暗号化の際に RFID タグが復号化処理の一部を行い，リーダ/ライタから送られた情報の内容を確認する．そのため，RFID タグは最初の暗号化の際に，暗号文と一緒に秘密鍵 x も受けとるものとする．RFID タグに秘密鍵が渡される際には，電波が外部に漏れない環境で行ったり，RFID タグとリーダ/ライタの通信を接触による接続で行ったりして，攻撃者に秘密鍵を傍受されないようにする．また，秘密鍵の保存には耐タンパメモリを利用し，秘密情報が漏洩しないようにする．

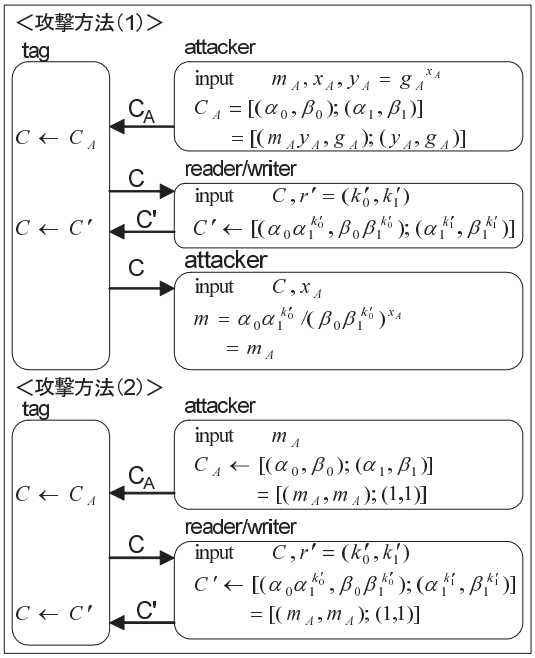

図 3 普遍再暗号化を用いた RFID システムに対する攻撃
Fig. 3 Attack on the system using Universal Re-encryption.

再暗号化の確認：RFID タグが入力として，$C = [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)]$ を受けとる．α'_1，β'_1 が 1 もしくは -1 のとき，再暗号化の処理は失敗したことになり，RFID タグの内容は書き換わらない．次に $m_1 = \alpha'_1 / \beta'^x_1$ を計算し，$m_1 = 1$ のときのみ，RFID タグの内容を C に書き換える．

この方法を加えた再暗号化のプロトコルを**図 4** に示す．再暗号化の処理に失敗したことが確認された時点で，RFID タグは処理を中断するものとし，RFID タグの情報は書き換わらない．

この方法では，α'_1 もしくは β'_1 が 1 でないか確認

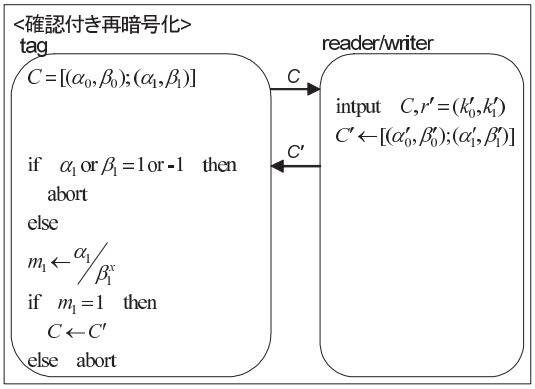

図 4 RFID タグによる内容の確認を加えた再暗号化プロトコル
Fig. 4 Re-encryption with a check.

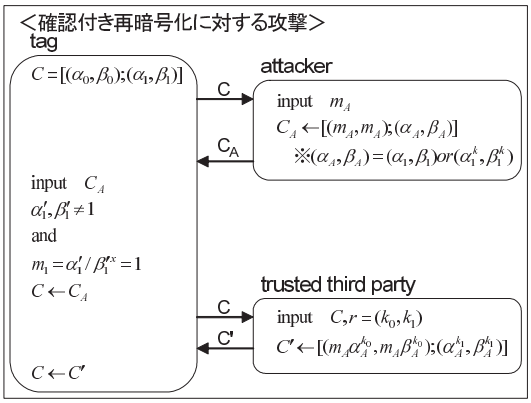

図 5 提案方式に対する攻撃
Fig. 5 Attack on our proposal.

することで攻撃方法（2）の検証を行う．次に，暗号化の鍵に関する情報である α'_1 と β'_1 の内容を秘密鍵により確認することで，暗号文が公開鍵 y により暗号化された暗号文を再暗号化されたかどうかを確認する．これにより，攻撃方法（1）を防ぐことができる．

4.3 提案方式の検証

Golle らの普遍再暗号化を RFID に適用した場合，改ざんによる攻撃が考えられたが，提案方式では書き込まれる内容を確認することで改ざんを防止する．また，提案方式ではリーダ/ライタの認証ではなく，書き込まれる内容のみを確認する．そのため，攻撃者は RFID タグの情報を引き出すことはできるが，内容を改ざんすることはできない．RFID タグの情報は暗号化されているため，攻撃者に情報が漏洩することはない．

また，提案方式では書き込まれる内容の一部しか確認しないため，確認しない部分だけが改ざんされる可能性がある．以下に提案方式に対する攻撃が行われた際の RFID タグの情報の変化と，その後正しく再暗号化が行われた場合の様子を示す．また，提案方式に対する攻撃と，その後の再暗号化の様子を**図 5** に示す．

ただし，RFID タグにはあらかじめ前述した安全な方法で秘密鍵 x，公開鍵 y による暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ が書き込まれているものとする．

提案方式に対する攻撃：暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ を攻撃者は受けとり，攻撃者が設定したメッセージ m_A を用いて，以下のような暗号文 C_A を RFID タグに書き込む．

$$C_A = [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)] = [(m_A, m_A); (\alpha_A, \beta_A)]$$

この暗号文 C_A の (α_A, β_A) は RFID タグから受けとった (α_1, β_1) 自体もしくは (α_1, β_1) を適切な再暗号化プロトコルを用いて処理した内容を用いるので，確認付き再暗号化プロトコルでこの書き込みを防ぐことはできない．

信頼できる第三者による再暗号化：第三者は，RFID タグより暗号文 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(m_A, m_A); (\alpha_A, \beta_A)]$ を再暗号化プロトコルと同様に受けとる．次に，乱数 $r' = (k'_0, k'_1)$ と暗号文 C を用いて，以下のような計算により C' を導き出し，RFID タグに書き込む．

$$\begin{aligned} C' &= [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)] \\ &= [(\alpha_0\alpha_1^{k'_0}, \beta_0\beta_1^{k'_0}); (\alpha_1^{k'_1}, \beta_1^{k'_1})] \\ &= [(m_A\alpha_A^{k'_0}, m_A\beta_A^{k'_0}); (\alpha_A^{k'_1}, \beta_A^{k'_1})] \end{aligned}$$

暗号文 $C' = [(m_A\alpha_1^{k'_0}, m_A\beta_1^{k'_0}); (\alpha_1^{k'_1}, \beta_1^{k'_1})]$ は秘密鍵 x を用いないと，復号化できない．

しかし，RFID タグの情報は最初に書き込まれていた内容とは異なるので，RFID システムの識別能力を損ねてしまう．これを防止するためには，再暗号化により書き込まれる暗号文の内容すべてを確認しなければならないが，提案方式の「RFID タグの計算能力を最小限に抑えることができる」という利点を損ねてしまう．しかし，攻撃者は再暗号化された暗号文 C' を復号化することができず，再暗号化の強秘匿性により RFID タグを追跡するのは困難である．よって，ロケーション・プライバシの保護は実現できる．

4.4 他方式との比較

提案方式では秘密鍵の保存に耐タンパ性のあるメモリを仮定しているため，秘密鍵を共有して対称鍵暗号を用いた方法も考えられる．この場合，乱数などを用いて暗号文を変化させることになるが，その値をデータベースとの間で同期をとる必要がある．提案方式で

は普遍再暗号化を用いているため，秘密鍵さえあれば同期をとることなく一度の復号化で平分に戻せるため，データベースの処理を軽くすることが可能である．また，対称鍵暗号を用いた方法ではデータベースにそれぞれの RFID タグの秘密鍵を安全に管理する必要がある．しかし，普遍再暗号化を用いた提案方式では，データベースは 1 つの秘密鍵のみを安全に管理すればよい．そのため，運用コストも低くすることができる．

安全性の面では，対称鍵暗号を用いた方式では 1 つの RFID タグの秘密鍵が漏洩したとしても他の RFID タグに影響することはない．しかし，提案方式では秘密鍵が漏洩すると，すべての RFID タグの情報が漏洩してしまう．

また，提案方式では秘密鍵を用いた復号化の処理の一部を RFID タグが行うため，秘密鍵を用いた方式やハッシュ関数を用いた方式に比べ，RFID タグの処理コストは大きくなる．ただし，提案方式では乱数の生成や暗号文全体の暗号化をリーダに依頼しているため，RFID タグ内で再暗号化の処理を行った場合に比べ，わずかではあるが RFID タグの処理コストを軽減している．

5. ま と め

本論文では，Golle らにより提案された普遍再暗号化[2] を，実際に RFID システムに適用した場合について検討した．そして，普遍再暗号化を用いた RFID システムに対する攻撃方法を考察し，その攻撃を防ぐために低コストで実現できる確認付き再暗号化プロトコルを提案した．

今後の課題として，提案手法では耐タンパメモリに格納することで秘密鍵の漏洩を防いでいるが，耐タンパメモリはコストが高いためより低コストで実現できる方法を考える必要がある．また，低コストで実装できる内容改ざんの防止方法が必要になると思われる．

謝辞 本研究の一部は，文部科学省科学研究費補助金学術創成研究課題番号 14GS0218「社会基盤を構築するためのシステム LSI 設計手法の研究」（研究代表安浦寛人九州大学システム LSI 研究センター長）の支援を受けている．また，本研究に関して有益なご助言をいただいた，九州大学櫻井研究室の今本健二氏に感謝いたします．

参 考 文 献

1) 社団法人日本自動認識システム協会 RFID 部会. http://www.aimjapan.or.jp/bkindex/rfid/rfindex.html
2) Golle, P., Jakobsson, M., Juels, A. and Syverson, P.: Universal re-encryption for mixnets, (2002). In submission. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html
3) Juels, A.: Privacy and Authentication in Low-Cost RFID Tags (2003). In submission. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html
4) Juels, A., Rivest, R. and Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, (2003). In submission. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html
5) Juels, A. and Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, *Financial Cryptography '03*, Wright, R. (Ed.), Springer-Verlag (2003).
6) 木下真吾，星野文学，小室智之，藤村明子，大久保美也子：RFID プライバシー保護を実現する可変秘匿 ID 方式，2003 年コンピュータセキュリティシンポジウム（CSS2003）予稿集，pp.497–502 (2003).
7) 大久保美也子，鈴木幸太郎，木下真吾：Forward-secure RFID Privacy Protection for Low-cost RFID，2003 年コンピュータセキュリティシンポジウム（CSS2003）予稿集，pp.491–496 (2003).
8) Sarma, S.E., Weis, S.A. and Engels, D.W.: RFID systems, security and privacy implications, Technical Report MIT-AUTO-WH-014, AutoID Center, MIT (2002).
9) Sarma, S.E., Weis, S.A. and Engels, D.W.: Radio-frequency-identification security risks and challenges, *Security Bytes*, Vol.6, No.1 (2003).
10) Weis, S.A., Sarma, S., Rivest, R. and Engels, D.: Security and privacy aspects of low-cost radio frequency identification systems, *1st International Conference on Security in Pervasive Computing* (2003). To appear. http://citeseer.nj.nec.com/weis03security.html
11) McCullagh, D.: RFID tags: Big Brother in small packages, *CNet*, 13 (Jan. 2003). Available at http://news.com.com/2010-1069-980325.html

(平成 15 年 12 月 4 日受付)
(平成 16 年 6 月 8 日採録)

齊藤純一郎

2004 年九州大学工学部電気情報工学科卒業．同年同大学大学院システム情報科学府情報工学専攻修士課程入学，現在に至る．RFID タグのプライバシ保護に関する研究に従事．

櫻井　幸一（正会員）

1988 年九州大学大学院工学研究科応用物理専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報工学部門教授．1997 年 9 月より 1 年間コロンビア大学計算機科学科客員研究員．2001 年 4 月より九州大学システム LSI 研究センター併任．暗号理論・情報セキュリティ・社会情報工学の研究に従事．博士（工学）．2000 年情報処理学会坂井特別記念賞受賞．2000 年・2004 年情報処理学会論文賞受賞．電子情報通信学会，日本数学会，ACM 各会員．