修士論文要旨 (2010 年度)

# プライバシを考慮したRFIDシステムの研究
## A Study of Privacy Enhanced RFID Systems

電気電子情報通信工学専攻 関野 智啓
Tomohiro SEKINO

## 1 序論

近年，電子社会の進展に伴い，いつでも，どこでもネットワークにアクセスできるユビキタス社会の実現が求められている．ユビキタス社会を実現するための一つの技術として，非接触で ID を認証する Radio Frequency Identification(RFID)[1] システムが注目されている．RFID システムは現在でも電車の改札や建物への入退室管理など私たちの身近なところで広く利用されており，Suica や ID カード等の低コストデバイスである RFID タグを無線通信を介してリーダが認証する技術である．

しかし，最近では RFID システムによるプライバシの侵害が問題となっている．通常の RFID システムは RFID タグ，RFID リーダ，サーバから構成され (図 1)，認証時には RFID タグから RFID リーダに無線通信を介して固有の ID 情報が送られる．そのため，離れた場所から読み取り可能な RFID タグを人が持ち歩く場合，第三者により気づかれないようリーダを近づけるなどしてその人の位置が特定されたり行動履歴が追跡されたりする可能性があり，プライバシが侵害される危険がある．そこで，RFID ユーザのプライバシを守るために，第三者が同一の RFID タグから送信される ID 情報を二つ以上入手したとしても，それらが同一の RFID タグから送られているか否かを識別できない性質を持たせる必要がある．この性質をリンク不可能性と呼ぶ．なお，この場合においても特定のサーバは入手した ID 情報から RFID タグを特定することが可能である．リンク不可能性を満たす RFID システムの既存方式として，ハッシュロック方式 [1] とハッシュ連鎖方式 [2] がある．しかしながら，これらの方式はサーバ側で管理している ID の数に応じてタグの特定にかかる処理が重くなるという問題がある．近年の RFID ユーザの増加を考えると ID の探索効率は軽視できない問題となっている．

この問題を解決するため，本研究は公開鍵暗号方式を用いることで，リンク不可能性を満たしつつ，ID の数に探索効率が依存しない RFID システムについて検討する．公開鍵暗号方式を用いた RFID システムでは，RFID タグが ID と乱数を公開鍵で暗号化してリーダに送ることで，リーダは秘密鍵を使い一度の復号だけで ID を特定することができる．そのため，たとえ膨大な数の ID をサーバで管理している場合でも探索効率を落とすことなく ID を特定することが可能である．しかし，現在，最も広く利用されている RSA 暗号は暗号化処理に多倍長のべき乗剰余演算を必要とし，その計算コストが高いため，RFID タグのような低計算能力のデバイスに安価に導入することは容易ではない．そこで，本研究は暗号化処理に多倍長のべき上剰余演算を必要としない Niederreiter 暗号 [3] に着目した．Niederreiter 暗号の暗号化処理は排他的論理和の計算のみで行えるため多倍長のべき乗剰余演算を必要とする RSA 暗号に比べて暗号化処理が軽く，RFID タグのような低コストデバイスに向いている．しかし，Niederreiter 暗号には公開鍵のサイズが大きいという問題がある．RSA 暗号の公開鍵サイズは 2,048 ビットであるのに対し，同程度の安全性を持つ Niederreiter 暗号の公開鍵サイズは 650,000 ビットと大きくなる．本研究では，RFID タグに実装できるように Niederreiter 暗号の鍵サイズを小さくする方法について検討する．Niederrieter 暗号の公開鍵暗号を小さくする方式である準ダイアディック公開鍵暗号 (Quasi-Dyadic Public Key Cryptosystem)[4] と個別化公開鍵暗号 (Personalized Public Key Cryptosystem)[5] という二つの方式, それぞれについて改良し，それらを組み合わせることで，鍵のさらなる縮小法を提案する．

[1] ここでいう RFID とは IC チップが埋め込まれた RFID タグから電波などを用い，近距離 (数 mm〜数 m) で無線通信を介して情報のやり取りをし，認証する技術である．

また，その安全性について考察し，暗号鍵のサイズを 3,520 ビットまで削減できることを示す．

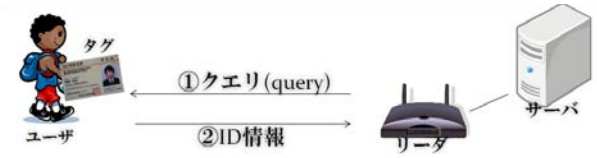


図 1: RFID システム

## 2 本研究で対象とするRFIDシステム

本研究では RFID ユーザ，RFID タグ，RFID リーダ，サーバから構成される RFID システムを考える (図 1 参照)．本研究の目的は，RFID タグと RFID リーダ間で ID の情報漏えいなしに認証することである．プロトコルの流れは次のようになる．RFID ユーザはサーバから RFID タグを安全な通信路で受け取り，RFID タグと RFID リーダ間は無線通信を介して認証を行い，サーバが検証する．ここで，サーバとリーダ間は安全な通信路で通信可能であり，サーバは ID の情報を一切漏えいしないとする．

### 2.1 RFID システムが満たすべき要件

RFID システムが満たすべき要件として以下の二つがあげられる．一つは許可されたものだけが認証にせいくする守秘性，もう一つは RFID ユーザの行動をひもつっげできない（行動の追跡ができない）リンク不可能性である．

- 守秘性：
  正規のユーザは認証に成功する．
  不正なユーザは認証に失敗する．
- リンク不可能性：
  リンク不可能性を持つ

### 2.2 攻撃者のモデル

攻撃者はタグとリーダ間の情報をすべて盗聴できるとする．攻撃者の目的はその得られた情報から正規のユーザへのなりすまし，ID 情報の取得，ユーザの行動を追跡することである．

## 3 Niederreiter 暗号

1986 年に提案された Niederreiter 暗号は，線形符号の復号問題であるシンドローム復号問題の困難性を安全性の根拠とする公開鍵暗号方式である．その問題は NP 困難問題 [6] であることが示されている．Niederreiter 暗号の暗号化処理は二次元の行列計算で行え，暗号化処理が排他的論理和のみで計算できるため，暗号化処理が軽いという特徴を持つ．しかし，Niederreiter 暗号では安全に使える公開鍵のサイズがおよそ 650,000 ビットであり，現在最も広く利用されている RSA 暗号の公開鍵のサイズ 2,048 ビットに比べて，非常に大きくなってしまう．現在でも，この問題に対して解決策が求められている．本研究でも鍵サイズを小さくするために様々な方法について検討し，提案する．

### 3.1 準ダイアディック公開鍵暗号

Niederreiter 暗号は公開鍵のサイズが大きいという問題がある．その問題を解決するために準ダイアディック公開鍵暗号 (Quasi-Dyadic Public Key Cryptosystem) という方法が Rafael Misoczki らによって提案された [4]．この方式により鍵サイズを減らすことができ，実用的に使えるレベルに達したといえる．しかし，R. Misoczki らによって提案された方式は公開鍵を生成する際に無駄な計算を有している部分がある．本研究は効率的に公開鍵を生成し，柔軟にパラメータを設定できる準ダイアディック公開鍵暗号 (Flexible Quasi-Dyadic Public Key Cryptosystem) を提案する．また，提案方式を利用することにより R. Mizsocski によって提案された準ダイアディック公開鍵暗号の鍵サイズをより小さくすることができる．

## 4 個別化公開鍵暗号方式

公開鍵暗号において，復号者は対となる公開鍵と秘密鍵を生成し，公開鍵を公開する．暗号者が平文をその復号者に送信する時，全ての暗号者が同じ公開鍵を使用するため復号者は誰が送ったメッセージか分からな

い．一方，個別化公開鍵暗号方式 (Personalized Public Key Cryptosystem:P$^2$KC) では Niederreiter 暗号の公開鍵に対して個別化を行い，それぞれの暗号者に個別化した暗号鍵 ($PersonalizedPublicKey$ : $ppk$) を作る．復号者はその暗号鍵で暗号化された暗号文を復号すると，平文を出力すると同時に暗号者を識別できる．また，暗号鍵を作る際には事前計算を行うため，暗号鍵のサイズを小さくでき，暗号化処理の計算量も小さくできる．個別化公開鍵暗号方式の中には幾つかの構成方法が提案されている．本研究のモデルに従う既存方式である ID に対応する固定領域法 (Fix Domain Shrinking(FDS)) に対して，以下で説明する提案方式と比較を行う．

## 5 暗号鍵を削減する提案手法

本研究では要件を満たしつつ暗号鍵サイズを小さくする方式を提案する．具体的には以下の方法を提案する．

### 5.1 指定 ID に対応する固定領域を縮小する準ダイアディック暗号の提案

上記の FQD-PKC と FDS を組み合わせる (Flexible Quasi-Dyadic Fix Domain Shrinking:FQD-FDS) を提案する．本研究のモデルに従うように提案方式 FQD-FDS をチャレンジレスポンス認証に適用し，RFID システムの安全性の評価を行い，RFID システムの要件を満たすことを示す．この方式を利用することによって，小さいもので $4,928$ ビットまで暗号鍵のサイズを削減することに成功した．その結果を表 1 に示す．表 1 では，$2^{80}$ の計算量を必要とする[2] セキュリティレベルを設定し，ID の数と鍵サイズを示している．

### 5.2 ランダムな指定 ID に対応する固定領域を縮小する準ダイアディック暗号の提案

本研究では暗号鍵サイズを小さくする個別化公開鍵暗号の新たな構成方法，ランダムな指定 ID に対応する固定領域縮小法 (Random Fix Domain Shrinking:RFDS) を提案し，さらに FQD-PKC と組み合わせるランダムな指定 ID に対応する固定領域を縮小する準ダイアディック暗号 (Flexible Quasi Dyadic-Random Fix Domain Shrinking:FQD-RFDS) を提案することによって暗号鍵サイズを小さくする．本研究では FQD-RFDS をチャレンジレスポンス認証に適用し，RFID システムの安全性評価を行い，要件評価を行った．表 2 では，$2^{80}$ の計算量を必要とする[2] セキュリティレベルを設定し，ID の数と鍵サイズを示している．FQD-RFDS を用いることにより，セキュリティレベルを $2^{80}$，ID の数を $2^{30}$ を保ちながら，暗号鍵サイズを $3,520$ ビットまで小さくできることを示した．

[2]現在，解読に要する計算量が $2^{80}$ の場合に安全であるといわれている [7]

表 1: FQD-FDS のパラメータ

| 安全性 | ID の数 | 鍵サイズ (ビット) |
|---|---|---|
| $2^{82}$ | $2^{19}$ | 5984 |
| $2^{83}$ | $2^{34}$ | 4928 |
| $2^{91}$ | $2^{97}$ | 5280 |
| $2^{80}$ | $2^{72}$ | 4928 |

表 2: FQD-FDS のパラメータ

| 安全性 | ID の数 | 鍵サイズ (ビット) |
|---|---|---|
| $2^{82}$ | $2^{30}$ | 5984 |
| $2^{83}$ | $2^{30}$ | 4928 |
| $2^{91}$ | $2^{30}$ | 5280 |
| $2^{80}$ | $2^{30}$ | 4928 |

## 6 結論

表 3 は，$2^{80}$ のセキュリティレベルを保ちつつ，ID の数，RFID タグに記憶する鍵サイズ，また暗号化処理時間に対して，本研究のモデルと同じ条件を満たす方式である FDS，FQD-FDS, FQD-RFDS を比較した表である．表 3 より，既存方式である FDS の RFID に記憶する鍵サイズは $134,200$ ビットであるのに対し，本研究で提案した FQD-FDS の RFID タグに記憶する鍵サイズは $4,928$ ビット，FQD-RFDS の RFID に記憶する鍵サイズは $3,520$ ビットである．この結果から明らかなように本研究で提案した FQD-RFDS が RFID に記憶する鍵サイズが最小となり，RFID システムに適しているいえる．また，現在最も利用されて

表 3: 既存方式と提案方式の比較

| 方式 | 安全性 | ID の数 | 鍵サイズ (ビット) | 暗号化処理時間 (ms) |
|---|---|---|---|---|
| FDS | $2^{80.2}$ | $2^{13.5}$ | 134,200 | 0.021 |
| FQD-FDS | $2^{83}$ | $2^{34}$ | 4,928 | 0.018 |
| FQD-RFDS | $2^{81}$ | $2^{30}$ | 3,520 | 0.022 |

いる RSA 暗号の暗号化処理時間は $39ms$ であるのに対し，FQD-RFDS の暗号化処理時間は $0.022ms$ であり，FQD-RFDS は RSA 暗号の暗号化処理時間の 0.056% で暗号化処理が行える．

今後，RFID システムはさらに大規模化し，大量の ID を管理することが想定される．そのような RFID システムでは提案方式である FQD-RFDS は非常に有効な方式となる．

## 謝辞

本研究は，産業技術総合研究所情報セキュリティ研究センターとの共同研究として行われました．関係者の皆様に深く感謝すると共にこの場を借りて厚く御礼申し上げます．

### 発表論文（国内学会）

1. 関野智啓, 古原和邦, 今井秀樹: “複数の独立した端末と認証方式を使ったボットウィルス対策”，2008 年コンピュータセキュリティシンポジウム (CSS2008), pp.863-869, 2008 年 10 月.
2. 関野智啓, 古原和邦, 今井秀樹: “複数の独立した端末と認証方式を使ったマルウェアに強い命令（電子商取引）方式”，2009 年暗号と情報セキュリティシンポジウム (SCIS2009), 3E3-4, 2009 年 1 月.
3. 関野智啓, 崔洋, 古原和邦, 今井秀樹: “プライバシを考慮した RFID 向け個別化公開鍵暗号方式に関する考察”, 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 3E2-4, 2010 年 1 月.
4. 関野智啓, 崔洋, 古原和邦, 今井秀樹: “プライバシを考慮した RFID 向け個別化公開鍵暗号方式の新たなモード Random Fix Domain Shrinking の提案”, 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), 2E2-3, 2010 年 1 月.
5. 関野智啓, 崔洋, 古原和邦, 今井秀樹: “Flexible Quasi-Dyadic の実装・評価に関する考察”, 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), 3A3-1, 2010 年 1 月.

### 発表論文（国際学会，査読あり）

1. Tomohiro Sekino, Kazukuni Kobara, Hideki Imai: “Anti-malware Order System Using Multiple Independent Terminals and Authentication Schemes”, 2009 Wireless Personal Multimedia Communications(WPMC2009), S43-1, Sendai, Japan, September 7-10, 2009.
2. Tomohiro Sekino, Yang Cui, Kazukuni Kobara, Hideki Imai: “Privacy Enhanced RFID Using Quasi-Dyadic Fix Domain Shrinking”, IEEE Globecom 2010, Maiami, Florida, USA, December 6-10, 2010.
3. Rei Yoshida, Yang Cui, Tomohiro Sekino, Rie Shigetomi, Akira Otsuka, Hideki Imai: “Practical Searching Over Encrypted Data by Private Information Retrieval”, IEEE Globecom 2010, Maiami, Florida, USA, December 6-10, 2010.

### 受賞

1. “ISS 研究奨励賞”, ISS スクエアシンポジウム 2010
2. “Early Bird Student Award”, IEEE Globecom 2010, Maiami, Florida, USA, December 6-10, 2010
3. “辻井重男セキュリティ学生論文賞　情報セキュリティ学生賞奨励賞”, 2011 年 3 月 9 日

## 参考文献

[1] S. A. Weis, “Security and Privacy in Radio-Frequency Identification Devices”, Master Thesis, MIT, 2003.

[2] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic approach to ‘Privacy Friendly’ tags”, RFID Privacy workshop, 2003.

[3] H. Niederreiter,“Knapsack-type Cryptosystems and Algebraic Coding Theory,” Problems of Control and Information Theory, vol. 15, no. 2, pp. 159–166, 1986.

[4] R. Misoczki and P. S. L. M. Barreto,“Compact McEliece Keys from Goppa Codes,” Selected Areas in Cryptography 2009 (SAC 2009), LNCS 5867,pp.376-392, Springer,2009.

[5] K. Kobara and H. Imai,“Personalized-Public-Key Cryptosystem($P^2$KC)-Application Where Public-Key Size of Niederreiter PKC Can Be Reduced”, Workshop on Codes and Lattices in Cryptography (CLC2006), pp. 61–68, 2006.

[6] M. Sudan, I. Dumer, and D. Mcciancio,“Hardness of approximating the minimum distance of a lineareode,” IEEE Trans. Inf. Theory, vol.49, no.1, pp.22–37, 2003

[7] 独立行政法人情報通信研究機構, 独立行政法人情報処理推進機構, “CRYPTREC Report 2009”, http://www.cryptrec.go.jp/report/c09_sch_web_final.pdf.