社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(2)
2003／7／17

Rabin Treeとブロードキャスト暗号への応用

菊池　浩明†

† 東海大学電子情報学部
神奈川県平塚市北金目 1117
E-mail: †kikn@tokai.ac.jp

あらまし　本稿はRabin暗号に基づいて，ユーザの管理しなくてはならない秘密情報の数を最小化した鍵管理方式を提案する．あるランダムなルート鍵が正しくRabin Treeを構成する確率が，ユーザ数 n に対して指数関数的に小さくなることを証明する．不正な利用者を排除するブロードキャスト暗号への応用を示す．
キーワード　コンテンツ保護，Rabin暗号

Rabin Tree and its Application to Broadcast Encryption

Hiroaki KIKUCHI†

† School of Electronics and Infromation Technology,
Tokai University,
1117 Kitakaname, Hiratsuka, Kanawaga 259-1292
E-mail: †kikn@tokai.ac.jp

Abstract　This paper presents a key management scheme based on Rabin public-key cryptosystem, which minimizes a number of secret key at recipient. A probability that a given random root key would succeed to have a full Rabin tree with $2n-i$ nodes is proved to be exponential to the number of users n. An application to broadcast encryption which allows excluding faulty recipients is proposed.
Key words　Content protection, Rabin public-key algorithm

1. はじめに

コンテンツ保護の不正利用を防止するブロードキャスト暗号技術が注目されている．この技術は，コンテンツ提供者がコンテンツを効率よく暗号化し，正しい復号鍵を持っているユーザだけが復号化してコンテンツを入手できること，そして，不正を行ったユーザがいたときに，それらのユーザの鍵を効率よく無効化することを目的としている．従って，ユーザ数 n，失効ユーザ数 r が与えられたとき，1) 暗号化コンテンツのサイズ（暗号文長），2) ユーザが記憶する秘密情報（デバイス鍵）のサイズ，3) 鍵を確立するための計算コスト，のそれぞれを最小化することが求められる．

Wangらは，木構造を導入することで，各ユーザに $\log n$ 個の秘密鍵を割り当て，$O(r\log(n/r))$ の暗号文長を実現する方式を提案している [2]．この方式は，Logical Key Hierarchy (LKH) 法と呼ばれ，マルチキャストにおけるグループ鍵管理の方式として標準化がなされている．一方，Naorらは，部分集合の差で失効鍵を定めるSubset Difference (SD) 方式を提案し，暗号文の大きさを，$2r-1$ にまで削減している．ただし，SD法ではユーザの持つ鍵情報はLKHに対して増えている．この秘密に管理しなくてはならない鍵情報の数に関しては，浅野によるRSA暗号に基づくマスター鍵技術を応用した方法 [1] により，最小の1にまで削減されている．しかし，浅野の方式（[1] の方式1) では，n 人の全ての部分集合の数だけの素数を全てのユーザで同意しておく必要がある．これらの素数は全ユーザに共通で公開してよい情報ではあるが，偽りの割り当てでだまされない為には耐改ざん性のある記憶装置が必要となる．論文 [1] では，素数をダイナミックに生成する事でこの記憶領域を削除するアイデアも述べられているが，ユーザ数に比例する数の素数を毎回生成するオーバヘッドは無視できない．

そこで，本稿では，LKH法とトラップドア付き一方向性関数を組み合わせることで，ユーザの記憶領域を最小化，すなわち，1とする方式を提案する．提案方式では，浅野の方式で必要とした素数の為を記憶装置も必要とせず，$O(\log n)$ 回のべき乗演算でのグループ鍵確立を実現している．同様の方式は，[4] で野島，楫によってより一般的な形で提案されているが，本提案方式の実装方式の方が実際の計算量が小さい．本方式は，Rabin暗号に基づいており，Rabin暗号の復号化が一意でないことを

利用して効率的に鍵の木，Rabin Tree を構成する．本稿では，まず従来方式とその性能を示した後，提案方式を定義し，その安全性と性能評価について考察する．

2. 準　　備

2.1 LKH 法 (CS)

全ユーザからなる集合を N, その部分集合で失効したユーザからなる集合を R とし，それぞれの数を $n=|N|$, $r=|R|$ とおく．簡単のため，ユーザ数 n を 2 のべき乗であると仮定する．また，以下の議論は，k 分木に自然に拡張が出来るが，ここでは $k=2$ の 2 分木の場合だけを示す．

LKH 法とは，$2n$ 個のノードからなり，各ユーザに対応した n 個の葉を持つ 2 分木 T によって定める．本稿では 2 分木を効率よく定めるために，バイナリヒープを用いる．すなわち，ノード v_i について，その左右の子を，v_{2i}, v_{2i+1}, その親を $v_{\lfloor i/2 \rfloor}$ によって指す．(厳密には，LKH はユーザでの鍵の更新を許し，再鍵割り当てを行うプロトコルであるが，ここでは鍵の更新を許さないステートレスなユーザを仮定する．論文 [3] でいうところの Complete Subtree Method と考えてよい)．

T の各節点 v_i に独立に鍵 x_i を割り当て，各利用者には対応する葉からルートに至るまでの経路上の秘密鍵 $x_i, x_{i/2}, x_{i/4}, \ldots, x_1$ (i を 2 のべき乗とした時) を秘密に配布する．暗号化を行う際には，失効したユーザに割り当てられた秘密鍵を排除するため，木 T から R のそれぞれに割り当てた秘密鍵に対応するノードを取り除き，残された部分木のルートに該当する秘密鍵 $x_{i_1}, x_{i_2}, \ldots$ のそれぞれについてセッション鍵 sk を暗号化する．メッセージ M はその sk で暗号化し，

$$E_{x_{i_1}}(sk), E_{x_{i_2}}(sk), \ldots, E_{x_{i_m}}(sk), E_{sk}(M)$$

を全ユーザに対してブロードキャストする．$N \backslash R$ の要素ならば，必ずこの暗号文の中に該当する鍵を知っており，それを用いて復号化が出来る．

Naor らによって，この時の暗号文の数の上限が $r\log(n/r)$, ユーザの管理する秘密情報の数 $\log n$, そして，鍵を導出するのに $O(\log\log n)$ 回の処理がかかることが証明されている [3].

2.2 Rabin 暗号

Rabin 暗号は素因数分解の困難さにその安全性の仮定を置いた公開鍵暗号である [5].

素数 p, q を秘密鍵とし，公開鍵 $N=pq$ とおく．メッセージ $M \in Z_n$ を暗号化するには，$c = M^2 \bmod n$ とする．復号化は，$M_p = c^{1/2} \bmod p$, $M_q = c^{1/2} \bmod q$ となる M_p, M_q を求め，(M_p, M_q), $(M_p, -M_q)$, $(-M_p, M_q)$, $(-M_p, -M_q)$ なる 4 組の値から中国人剰余定理により 4 組の解を得る．メッセージ M の中に冗長な検査ビットを埋め込み，4 つの値から一意に復号化する．

Rabin 暗号の特徴は，暗号文に対して解が一意でないことである．4 つの解の候補は，

$$M' = M_P q q^{-1} + M_q p p^{-1} \bmod N$$
$$M^* = M_P q q^{-1} - M_q p p^{-1} \bmod N$$

とおくと，$M', -M', M^*, -M^*$ で表現できる．それゆえ，もしも c から M の一つを無視できない確率で求めることの出来る $F(N)$ 時間のアルゴリズム A が存在するならば，N を $2F(N)+2\log_2 N$ 回のステップで素因数分解できることが示されている [5]．なぜならば，ランダムに選んだ $M \in Z_n$ について $c = M^2 \bmod N$ を求めれば，A を用いて M^* か $-M^*$ かのどちらかが 1/2 の確率で得られる．そのような，M^* について，$GCD(M-M^*, N)$ は p または q を与える．

Rabin 暗号によるディジタル署名 (復号化) は，任意のメッセージに対しては適用できない．メッセージ (暗号文) c が署名できるための必要十分条件は，c が N に関する平方剰余，すなわち，$c \in QR_N$ であることである．与えられた c が平方剰余であるか否かは，素数 p, q を持っている人であれば，

$$\left(\frac{c}{p}\right) = c^{(p-1)/2} \equiv 1 \pmod p \qquad (1)$$
$$\left(\frac{c}{q}\right) = c^{(q-1)/2} \equiv 1 \pmod q$$

により判別できる．

3. 提 案 方 式

3.1 Rabin Tree

安全な素数 p_L, p_R, q_L, q_R について，$N_L = p_L q_L$, $N_R = p_R q_R$ とする．一般性を失うことなく，$N_L < N_R$ とする．

Rabin Tree とは，$2n-1$ 個のノードから成る完全 2 分ヒープ $v_1, \ldots, v_{2n}$ であり，$i<n$ の全ての節点 x_i について，

$$x_i \in QR_{N_L} \cup QR_{N_R} \qquad (2)$$

を満たす鍵 x_i を持ち，かつ，

$$x_i \equiv x_{2i}^2 \pmod{N_L}, \qquad (3)$$
$$\equiv x_{2i+1}^2 \pmod{N_R}$$

を満たすものをいう．ここで，$N_R \neq N_L$ とあることに注意せよ．(後述するブロードキャスト暗号での利用を行うために，結託を防止するために定めている．)

3.2 構 成 法

Rabin Tree を構成するには，次のような確率的アルゴリズムを用いる．

(1)　ランダムにルートの鍵 $x_1 \in Z_{N_L}$ を選び，それが式 (2) を満たしているかどうかを判定し，満たすまで繰り返す．$i=1$ とする．

(2)　N_L, N_R のそれぞれについて，鍵 x_i を暗号文とみなして Rabin 復号化を行い，その解をその子節点の鍵 x_{2i}, x_{2i+1} とする．Rabin 暗号の復号化には，p, q を Blum 数とする効率のよい方法が知られている [5].

(3)　鍵 x_i が条件式 (2) を満たすかどうか，Legendre 記号による式 (1) を用いて判別する．満たさないときは，4 つの解の中から他の解を x_i に割り当てて検査を繰り返す．

(4)　もしも，ある子節点の鍵の 4 つの解が全て式 (2) を満たさないときは，その子節点は**失敗**であり，その親から作り直

す．このバックトラックを繰り返し，最終的に $2n-1$ 個の節点全てに，条件式 (3) を満たした鍵を割り当てられたら，その鍵の数列を出力して終了する．

明らかに，Rabin Tree はルートの鍵 x_1 に対して一意には決まらない．この点が，野島らの方式[4] と異なる．また，[4] では問題となっていた，

$$(x_i^2 \bmod N_R)^2 \bmod N_L = (x_j^2 \bmod N_L)^2 \bmod N_R$$

を満たすような鍵 x_i, x_j についても，一致する確率は無視できる．

上記の確率的アルゴリズムは条件を満たすまで N_L の乱数を繰り返し試し，(それでもなければ，N_L を作り直せばよいので) 必ず終わる．しかし，そのためには非常に多くのバックトラックを生じさせる可能性がある．そこで，アルゴリズムが正しく終了する確率を見積もってみよう．

[定理 1] N_L と N_R が独立に選ばれた合成数であるとき，平方剰余であるかどうかは，それぞれ独立に決まる時，ある $x_i \in Z_{N_L}$ をルートとする Rabin Tree が存在する確率 P_{RT} は，

$$P_{RT} = P_{QR}(1-P_F^4)^{n-1}$$

で与えられる．ここで，P_{QR} はある乱数が式 (2) を満たす確率，$P_F = 1 - P_{QR}$ である．

(証明) Z_p における平方剰余は $(p-1)/2+1$ 個存在するので，合成数 $N=pq$ の下で，ある $x \in Z_N$ が平方剰余である確率は

$$\frac{(p-1)/2+1}{p}\frac{(q-1)/2+1}{q} = \frac{1}{4}+\frac{1}{4p}+\frac{1}{4q}+\frac{1}{4pq} \approx \frac{1}{4}$$

で与えられる．一方，Rabin Tree の条件式 (2) を満たすためには，N_L, N_R の両方について平方剰余でなくてはならない．よって，ある与えられた $x \in Z_{N_L}$ が式 (2) を満たす確率 P_{QR} は，$P_{QR} = (1/4)^2 = 1/16$ と定まる．

次に，ある鍵 x について，その子節点が (式 (2) を) 失敗する確率は $P_F = 1 - P_{QR} = 15/16$ と求められる．4 つある解の中からどれか一つが成功すればいいので，ある子節点は $1-P_F^4$ で成功する．n 個の葉を持ち，$2n-1$ 個の節点を有する Tree が Rabin Tree となるためには，$n-1$ 個の全ての中間節点において，条件式 (2) を満たさなくてはならない．従って，ある与えられたルートが Rabin Tree の構成に成功する確率は，結局，$P_{RT} = P_{QR}(1-P_F^4)^{n-1}$ の確率となり，定理を得る．(証明終)

実際には，$P_{QR} = 1/16$, $1-P_F^4 = 0.2275$ であり，n の増加によってはその値は指数関数的に小さくなる．

3.3 安全性

安全性に関しては，応用方法に依存して色々な条件が求められる．ここでは，一般的な立場から，次の性質があることを示す．

- N_L, N_R の素因数を知らないで，親節点の鍵から子節点の鍵がわからない．

Rabin 暗号を解くことと同値．

- 葉の鍵 x_i を知ることは，そのルートに至る経路の全ての鍵を知ることである．
- 接点 v_i の鍵からその兄弟 v_{i+1} (または v_{i-1}) の節点の鍵がわからない．N_L, N_R が独立に定められているとき，Rabin 暗号文から復号化が出来ることと同値である．
- 節点 v_i とその兄弟 v_{i+1} の二つの鍵から，N_R, N_L のどちらも素因数分解できない．

3.4 Rabin Tree を用いたブロードキャスト暗号

Rabin Tree をブロードキャスト暗号に適用する方式を提案する．提案方式は，LKH と同様に，コンテンツを配信する管理者 A，受信するユーザの集合 N から成っている．

(1) 管理者 A は Rabin Tree T を生成し，その葉に対応する鍵 $x_n, x_{n+1}, \ldots, x_{2n-1}$ を N のそれぞれに秘密に配布する．

(2) LKH と同様に，木 T から R の知っている秘密鍵を取り除き，残された部分木をカバーする最小の秘密鍵 $x_{i_1}, x_{i_2}, \ldots$ についてセッション鍵 sk を暗号化する．メッセージ M はその sk で暗号化し，

$$E_{x_{i_1}}(sk), E_{x_{i_2}}(sk), \ldots, E_{x_{i_m}}(sk), E_{sk}(M)$$

を全ユーザに対してブロードキャストする．

(3) 秘密鍵 x_i を持つユーザは，$i' = 2i$ 番目の鍵

$$x_{i'} = x_{2i} = \begin{cases} x_i^2 \bmod N_L & \text{if } i \text{ is even,} \\ x_i^2 \bmod N_R & \text{otherwise.} \end{cases}$$

を更新し，$i_1, i_2, \ldots$ のどれかについて，$i' = i_j$ を満たすまで (経路をルートまで上がり) 繰り返す．

提案方式は，LKH と同様の暗号文サイズ，ユーザの秘密情報は x_i の 1 個 (N_L の大きさ)，そして，上記アルゴリズムで鍵を導出するまで $\log n$ に比例した回数べき乗剰余演算を必要とする．

提案方式は，N_L, N_R の 2 種類の法を用いることで，ユーザの結託に対してロバストである．

3.5 提案方式の評価

各種ブロードキャスト暗号の性能の比較を，表 1 示す．[1] での評価項目に基づいて，提案方式の性能をまとめている．ただし，[1] では a 分木について一般的に定めていたが，簡単のため，2 分木，n は 2 のべき乗と仮定している．また，ユーザの公開情報数は，[1] では $\log n$ 個の素数だけを管理することが主張されているが，ここでは全素数の数とした．

4. おわりに

Rabin 暗号に基づく，一方向性を満たす鍵管理木とそのブロードキャスト暗号への応用方法を提案した．Rabin Tree の構成はユーザ数の指数関数時間がかかることを示した．Tree の構成は，信頼できる管理者がサービス開始時に十分に時間をかけてオフラインで作ればよいので，多少時間がかかっても許されるプロセスである．

文献

[1] T. Asano, "A Revocation Scheme with Minimal Storage at Reveivers", in Proc. of *ASIACRYPT 2002*, Springer, LNCS 2501, pp.433-450, 2002.

[2] C. K. Wong, M. Gouda and S. S. Lam, "Secure Group

表 1　ブロードキャスト暗号アルゴリズムの性能評価

Table 1　Comparison of broadcast encrypton algorithms in effiencry

アルゴリズム	浅野 [1]	LKH(CS) [2]	SD [3]	Rabin Tree
暗号文数	$r \log n/r + 1$	$r \log n/r + 1$	$2r - 1$	$r \log n/r + 1$
ユーザの秘密鍵数	1	$\log n$	$\frac{1}{2}(\log^2 n + \log n + 1)$	1
ユーザの公開情報数	$2^n - 1$	–	–	–
ユーザの計算量	$\log n$	–	–	$\log n$

Communications Using Key Graphs", Proc. of *ACM SIGCOMM'98*, 1998.

[3] D. Naor, M. Naor and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," in Advances in Cryptology- Crypto 2001, Springer, LNCS 2139, pp.41-62, 2001.

[4] 野島, 楳,「落と戸付き一方向性関数を利用した木構造鍵管理方式」, 暗号と情報セキュリティシンポジウム SCIS 2003, pp.131-136, 2003.

[5] Michael O. Rabin, "Digitalized Signatures and Public-key Functions as Intractable as Factorization", MIT Technical Report, MIT/LCS/TR-212, 1979.