様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月４日現在

研究種目：基盤研究（C）
研究期間：2005～2008
課題番号：１７５６０３４２
研究課題名（和文）　公開鍵暗号システム MEPKC の開発に関する研究

研究課題名（英文）　Development of a public-key cryptography MEPKC

研究代表者
葛　崎偉（QI-WEI GE）
山口大学・教育学部・教授
研究者番号：３０２６３７５０

研究成果の概要：本研究では，公開鍵暗号 MEPKC に必要な技術，①暗号化鍵が数多く存在する鍵生成器の生成法，②鍵生成器から複数の暗号化鍵の生成法，③鍵生成器を生成すると同時に生成する秘密鍵の生成法，を開発した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００５年度	900,000	0	900,000
２００６年度	800,000	0	800,000
２００７年度	900,000	270,000	1,170,000
２００８年度	800,000	240,000	1,040,000
年度			
総　計	3,400,000	510,000	3,910,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：公開鍵暗号，多段的暗号方式，ペトリネット，初等 T-invariant，NP-困難

１．研究開始当初の背景

(1) ネットワーク通信に用いられている暗号の多くはＲＳＡ暗号をコアにした仕組みのものである．ＲＳＡ暗号は素因数分解の難しさを利用した準指数オーダー強度の公開鍵暗号である．

(2) 量子力学と情報科学が融合した量子コンピュータの研究は進んでおり，特に素因数分解や離散対数問題を高速に解く量子コンピュータ上のアルゴリズムが発見されている．量子コンピュータが実用化されれば，ＲＳＡ暗号が簡単に解読できてしまい，情報化社会に計り知れないダメージを与えることになる．

２．研究の目的

(1) 情報化社会の趨勢から量子コンピュータにも耐えうる強度を備えた暗号の開発が必要不可欠である．本研究は新しい時代のニーズに応えられるような暗号技術の開発を目的とする．

(2) 具体的には，①数多くの暗号化鍵をもつ鍵生成器の構成技法を開発し，多段的に暗号化できる仕組みを設計する．②鍵生成器から暗号化鍵の生成法および鍵保護用のハッシュ関数を設計する．③復号化鍵としての逆ハッシュ関数を設計する．①～③を開発して，多段的暗号化のできる暗号システム MEPKC を実現することを目指す．

３．研究の方法

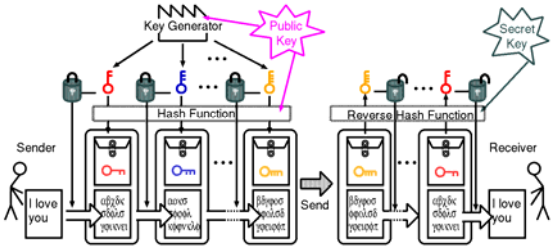
(1) 暗号システム MEPKC のコアの部分である鍵生成器はペトリネットを用い，暗号化鍵はペトリネットの初等 T-invariant を用いる．暗号化は，既存の秘密鍵暗号を用いて行う．

(2) 鍵生成器は小さいペトリネットから合成する方法で膨大な数の初等 T-invariant をもつように生成する．暗号化鍵は鍵生成器となるペトリネットから線形計画法を用いて複数求める．暗号化鍵を保護するためのハッシュ関数は，攻撃されたとき指数オーダーの計算時間を要するように設計する．また，復号化鍵は鍵生成器であるペトリネットがもつすべての初等 T-invariant とそれらの初等 T-invariant に対応するハッシュ値で構成するように設計する．

４．研究成果

(1) 暗号システム MEPKC は，図 1 に示すように，鍵生成器（Key Generator）とハッシュ関数（Hash Function）を公開鍵として公開し，逆ハッシュ関数（Reverse Hash Function: すべての初等 T-invariant と対応するハッシュ関数値）を秘密鍵とするようにした．平文の暗号化は既存の暗号である 3DES を用いた．

図 1　暗号システム MEPKC



(2) 鍵生成器となるペトリネットは，まず 1 つの閉路（k 個のプレース）だけからなるペトリネット（k-Ring(1)）を作成し，このような n 個のペトリネットを，プレースを共有させるように合成することで，多くの初等 T-invariant が存在するペトリネット（k-Ring(n)）を生成する．さらに，プレースの数が異なる複数のペトリネットを合成することで，膨大な数の初等 T-invariant が存在するペトリネット PN_M が生成できることが可能になった．図 2 に示すペトリネットは 3-Ring(1)と 5Ring(2)と 7-Ring(1)で合成されたもので，初等 T-invariant は 448 個存在する．

(3) (2)で述べた鍵生成器の生成方法で得られた PN_M に対して，我々はさらに二つの PN_M を合成する手法を提案した．また，枝の重みを付け加え，ダミーのプレースやトランジションを付加することで，初等 T-invariant の数が膨大になり，より強度の強いペトリネットの生成が可能になった．これにより，MEPKC の鍵生成器の生成が実現可能となった．

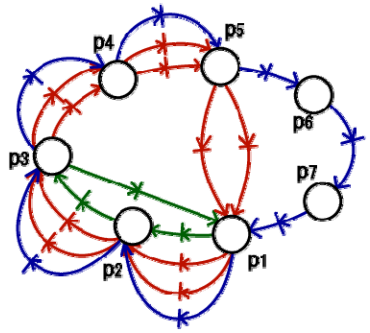


図 2 3-Ring(1)と 5Ring(2)と 7-Ring(1)で合成したペトリネット

(4) 暗号化鍵,すなわち初等 T-invariant は，線形計画法を用いて求める．①ペトリネットの構造を表す行列を A とした場合，T-invariant は AJ=0, J≠0 を満たす非負整数解である．初等 T-invariant は他の T-invariant の非負有理数の線形結合で表現できない T-invariant である．②線形計画法で定式化する際には，$\Sigma j_i=K$（整数値）と J を有理数とする制限を加える必要がある．③本研究では,線形計画法で近似的に J を求め，それから正確な初等 T-invariant を求めることにしている．④多段的に暗号化を行うために，複数の初等 T-invariant を求める必要がある．そのために，J のある一つの要素 j_s を用いて目的関数 y=MAX j_s を設定し，図 3 のように，目的関数値が最大（$y_{max}=\max\{y_1, y_2, \cdots\}$）となる解 J_{max} から探索し，複数の初等 T-invariant を求めている．

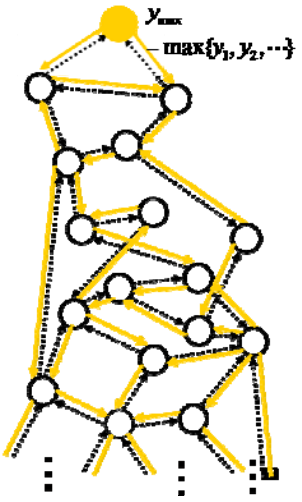


図 3　複数の初等 T-invariant を求める探索

(5) 暗号化鍵を保護するためのハッシュ関数は図 4 のように設計する.

Designing hash function H

1. **Randomly generate two vector, R_N,R_0, both with |T|-dimension.**
2. **A given elementary T-invariant**
$$J^e = (j_1^e, j_2^e, \cdots, j_{|T|}^e)^t$$
3. **A complement vector of its support**
$$\bar{S}_{J^e} = (\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_{|T|})^t$$
Where
$$\bar{s}_i = \begin{cases} 1 & \text{if } j_i^e = 0 \\ 0 & \text{otherwise.} \end{cases}$$
4. **Using R_N,R_0, we give our hash function as**
$$V = H(J^e) = (R_N)^t J^e + (R_0)^t \bar{S}_{J^e}$$

図 4　ハッシュ関数の設計

明らかに，ハッシュ値から初等 T-invariant を割り出す問題は NP-困難であり，このハッシュ関数を用いれば，暗号化鍵の保護は可能になる.

(6) MEPKC の秘密鍵は鍵生成器に含まれるすべての初等 T-invariant とそれぞれのハッシュ値からなる.すべての初等 T-invaraint は，鍵生成器を生成する際に作られる．その方法として，①(2)で述べた生成法でペトリネットを合成する際に，特定のプレース（図 2 中の p_1）を削除する．②ソーストランジションからシンクトランジションまでのすべてのパスを見つける．③見つけたパスのうち，ダミーのプレースやトランジションを含まなければ，初等 T-invariant に対応するものである．なお，図 5 に示すような階層グラフを使えば，効率的に初等 T-invariant を探すことが可能である.

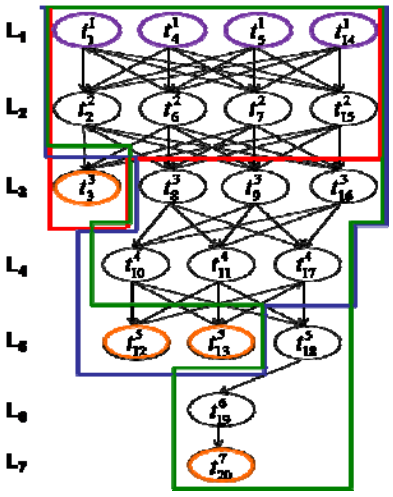


図 5　パスを見つけるための階層グラフ

以上の(1)～(6)で述べた公開鍵暗号システム MEPKC を実現するための技法を開発した．これらの成果より，従来の公開鍵暗号 RSA より強度の強い暗号システムが実現可能になった.

(7) 本研究は、斬新な発想に基づいて公開鍵システム MEPKC の仕組みおよびそれを実現するための技術開発を行った．従来の公開鍵暗号は固定の一つの公開鍵で暗号化しているが，MEPKC は異なる暗号鍵で多段的に暗号化することができる．これにより、セキュリティ強度が段数に比例して指数オーダー的に累積していく。暗号化の段数さえ増やせば、期待のセキュリティ強度が得られる。今後は，MEPKC の実用化に向けて，本研究で得られた技術をさらに改善していきたい.

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）

① R. Yamaguchi, Q.W.Ge, M. Nakata:“Construction of Petri Nets and Calculation of Elementary T-invariants for Multi-stage- Encryptions Public-Key Cryptography: MEPKC”, Proc. ITC-CSCC2008, pp.977-980, 2008 (査読有)

② S. Yamaguchi, H. Matsuo, T. Watanabe, Q.W.Ge, and M. Tanaka: “WF-Net Based Modeling and Soundness Verification of Interworkflows”, IEICE Trans. Fundamentals, Vol. E90-A No. 4, pp. 829-835, 2007（査読有）

③ S. Yamaguchi, T. Takai, T. Watanabe, Q.W.Ge, and M. Tanaka: “Complexity and a Heuristic Algorithm of Computing Parallel Degree for Program Nets with SWITCH-Nodes”, IEICE Trans. Fundamentals, Vol. E89-A No. 11, pp. 3207-3215, 2006（査読有）

④ S.Yamaguchi, T.Takai, Q.W.Ge, M.Tanaka: “Evaluation of PARAdeg of Acyclic Structured Program Nets,” Proc. ITC-CSCC2006, vol.3, pp. 453-456, 2006（査読有）

⑤ S.Yamaguchi, K.Yamada, Q.W.Ge and M.Tanaka: “Dead Problem of Program Nets”, IEICE Trans. Fundamentals, Vol.E89-A No.4, pp.887-894, 2006 (査読有)

⑥ Q.W.Ge, T.Fukunaga and M.Tanaka: “On Generating Elementary T-invariants of Petri Nets by Linear Programming”, Proceeding

of ISCAS2005, pp.168-171 , 2005 (査読有)

〔学会発表〕(計４件)

①「山口, 葛, 中田:“公開鍵暗号 MEPKC のためのペトリネットの生成法およびその初等 T-invariant の計算法”,電子情報通信学会信学技法, Vol. 108, No., pp.5-10 (CST2008-42), 2009.01.29 (神奈川県産業振興センター)

②「村上, 山口, 葛, 中田:“公開鍵暗号 MEPKC の鍵生成器として利用するペトリネットの自動生成およびその複雑化”,電子情報通信学会信学技法, Vol. 107, No. 472 (CST2007- 48), pp. 11-16, 2008.01.29 (徳島大学)

③「山口, 村上, 中田, 葛:“自動生成されたペトリネットの初等T-invariant の列挙アルゴリズム”,電子情報通信学会信学技報 , Vol.107, No.119 (CST2007-9), pp.15-20, 2007.06.29 (那覇簡易保険レクセンター)

④「T. Takai, S. Yamaguchi, Q.W.Ge, and M. Tanaka: ``On Evaluation and Application of PARAdeg of Acyclic Structured Program Nets'', IEICE Technical Report, Vol.106, No.367 (CST2006-20), pp.13-18, 2006.11.20 (長崎大学)

⑤「村上, 葛, 中田:“公開鍵暗号システム MEPKC における鍵生成器の作成について”,電子情報通信学会信学技報, Vol.105, No.573 (CST2005-42), pp.19-24, 2006.01.27 (東芝科学館 ホール)

〔図書〕(計０件)

〔産業財産権〕
○出願状況 (計０件)

○取得状況 (計０件)

〔その他〕
ホームページ等　　なし

６．研究組織

(1)研究代表者
葛　崎偉 (GE QI-WEI)
山口大学・教育学部・教授
研究者番号：30263750

(2)研究分担者
田中　稔 (TANAKA MINORU)
山口大学・大学院理工学研究科・教授
研究者番号：40112023

山口 真悟 (YAMAGUCHI SHINGO)
山口大学・大学院理工学研究科・准教授
研究者番号：00294653