

グローバル・グループ・セキュリティ

Global Group Security

荒木智行・山本富士男

Tomoyuki ARAKI Fujio YAMAMOTO

情報工学科

Abstract

The authors have ever proposed a global TV-conference server system which enable us to do worldwide home-working and a global autonomous decentralized computer system suitable for international cooperative work. Recently, home is being connected to the internet at all times using broadband connections. In this paper, we investigate requirements of network security for these systems, and propose cryptography which can satisfy the requirements.

Keywords: Groupwork, RSA cryptography, Agent system, Autonomous decentralized system

1. まえがき

近年、エージェント技術を使ってインターネット上の様々な資源を有効に活用するための研究が多くなされている。例えば、優れた移動性を持つ Aglets^[2]や、自らプランを生成し、それにしたがって行動する Plangent^[3]、人工社会に基づく技術を使って情報検索の研究である。また、これらに対するセキュリティ実現方式に関する研究もなされている。

近年、場所や時間の束縛されない就業形態としてテレワークの研究が盛んに行われている。著者らは、テレワーク環境の中でも、特に在宅で勤務するエンジニアを対象としたシステム環境やシステムの提案を行ってきた^[7,8,9]。これらのシステム環境は、インターネット上のユーザまたはエージェントのグループによって形成される自律分散システム環境であり、グループを単位としたエージェントシステムとして動作するものである。

広域な分散システムやエージェントを構成する際に用いるネットワークとしては、現在のところインターネット以外は考えられない。しかしながら、インターネットは、不特定多数のユーザに使用されるネットワークであり、情報セキュリティという観点では、最も危険なネットワークである。本報告は文献^[7,8,9]で提案されているような広域自律分散システム環境をインターネットを使用して構成した際の情報セキュリティに適した暗号方式の提案を行っている。(文献^[1]では、secure なエージェントについて考察しているが、本研究は、暗号方式の観点から考察している。)

暗号化の方式には慣用暗号と公開鍵暗号の二つの方式がある。一般に前者は鍵の生成が容易であるが対称鍵暗号であるため鍵を第三者から秘匿せねばならない。また、通信者は一対一が前提となり、通信する相手ごとの鍵をすべて管理しなくてはならない。これに対

し後者は、一部の鍵を第三者に公開しても暗号強度が保持できる。特にRSA暗号^[10]では一対多の通信が可能な同報通信に対応(マスター鍵)でき^[5,6]、計算機のグループ間での通信を行う上でも適している。また、鍵をマスター化することにより鍵の管理を容易にすることができる。

しかしながら、世界規模での分散システムを構成する際、計算機のグループの数は莫大な数になる可能性があり、現在のRSA暗号方式で生成できる鍵の数では、鍵長を極めて大きくしないかぎり、足りなくなる可能性がある。

本報告では、鍵長を大きくすることなく十分な数の鍵数を確保するための方式として、RSA公開暗号鍵方式に更に柔軟性を持たせたチェーン方式RSA暗号によるセキュリティ方式の提案を行う。

尚、本論文で提案するチェーン方式RSA暗号は、公開鍵暗号方式である RSA 暗号の良い性質を受け継いだ秘密鍵暗号である。

2. チェイン方式RSA暗号

以下では、RSA暗号の鍵の生成に関して、グループワークにおける実用上の安全性が保てる範囲で、より多くのグループ数、より多くのグループ構成員に対応できるような暗号方式—チェーン方式RSA暗号—の提案を行う。

2.1 RSA暗号

RSA暗号の基本原則を簡明に以下に示す。暗号化個別鍵を $K_{e_i} = (e_i, m_i)$ 、復号化個別鍵を $K_{d_i} = (d_i, m_i)$ とする。 K_{e_i} は公開されており、 K_{d_i} は利用者 U_i のみが知っている秘密鍵である。平文 P 、暗号

文をCとすると, 暗号化E, 復号化Dのアルゴリズムは, 以下で表される.

$$C = E(P) = P^{e_i} \pmod{m_i}$$

$$P = D(C) = C^{d_i} \pmod{m_i}$$

ただし, PとCは0から $m_i - 1$ の間の整数である. RSA暗号の暗号化, 復号化は一對一かつ上への写像である. EとDを代表してMで表すと,

$$M^{e_i \cdot d_i} \equiv M \pmod{m_i}$$

が成立し, i番目の個別鍵の生成に関する条件は, 以下の条件である.

$$m_i = p_i \cdot q_i$$

(ただし p_i, q_i は相異なる大きな素数)

$$\varphi(m_i) = \varphi(p_i)\varphi(q_i) = (p_i - 1)(q_i - 1)$$

(ただし \cdot はオイラー関数)

$$e_i \cdot d_i \equiv 1 \pmod{m_i}$$

RSA暗号は, m_i を二つの相異なる素数の積としている.

そしてRSA暗号の安全性は m_i の素因数分解の計算量的困難さに依存している.

通常, 法 m_i は二つの相異なる素数の積で表現されるが, ここで三つ以上の相異なる素数の積を許す, 即ち $m_i = p_i \cdot q_i \cdot r_i \cdots$ によって法を構成してもRSA暗号の基本的原理・安全性は満たされる.

2.2 マスタ鍵

暗号システムを運用する際, 鍵の管理の容易さは重要である. 一般的に鍵の管理の容易さは, 鍵の数に左右される. 本項では管理しなくてはならない鍵の数に関して, 個別鍵の場合とマスタ鍵の場合を比較する.

RSA暗号では, 複数の個別鍵(e_i, m_i)のいずれの代替にもなるようなマスタ鍵が作成できること, マスタ鍵の存在条件および安全性について小山^[5,6]により示されている. 本報告においてもマスタ鍵という場合には, 小山のマスタ鍵を意味するものとする.

ここでユーザまたはエージェント間での通信を, 個別鍵を使用した場合と, マスタ鍵を使用した場合の比較を行う.

ユーザまたはエージェント数をnとする. このとき使用される鍵の数を式で表わすと以下のようになる.

$$\text{個別鍵} \quad \sum_{i=2}^n i(i-1) \binom{n}{i}$$

$$\text{マスタ鍵} \quad 2^n - n - 1$$

このときの必要となる鍵の数の違いを図1に示す.

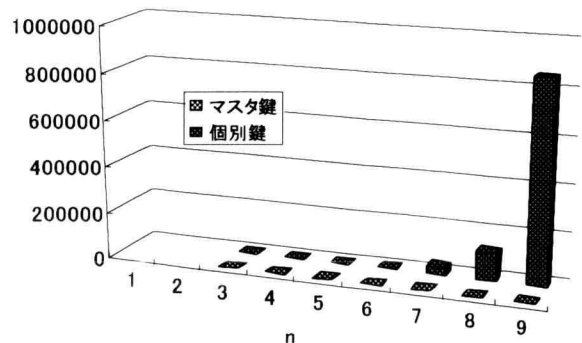


図1 個別鍵の場合とマスタ鍵の場合の比較

大規模なグループ間通信では, 相当数のグループが存在する. そのため必要となる鍵の数も大量である. そのため鍵の管理の観点からは, マスタ鍵の使用が有効となる. 更に, マスタ鍵を使用すると同報通信(インターネット上ではマルチキャスト通信)が可能となり, ネットワーク上のトラフィックの削減, 通信手順の効率化も可能となる.

2.3 RSA暗号の法の作成法の検討

RSA暗号の法の作成法に関して考察を行う. 2.2項で述べたように, 大規模なグループワーク環境を対象にする場合, 非常に多くの個別鍵(e_i, m_i)とそれに対応できるマスタ鍵が必要となることが想定される.

鍵の生成数に関しては, e_i の候補の数は, 法 m_i の数により制約を受ける. このことから本項では, 個別鍵をより多く作成するための考察, 特に法 m_i をより多く生成するための考察を行う. 従来から使用されている法の作成法(ここでは「標準方式」と呼ぶ)と, 新しい法の作成法として「チェイン方式」について述べる.

【標準方式】

一般的な法の作成法として, すべての個別鍵の法が, 互いに素になるように選ぶ. 一度使用した素数は, 他の鍵を作成するときには使用できない.

(例1) 標準方式で共通のマスタ鍵が作れる個別鍵の例
($m_i = p_i \cdot q_i$ の場合)

$$(e_1, d_1, m_1 (= p_1 \cdot q_1)) = (73, 117, 319 (= 11 \cdot 29))$$

$$(e_2, d_2, m_2 (= p_2 \cdot q_2)) = (61, 85, 323 (= 17 \cdot 19))$$

$$(e_3, d_3, m_3 (= p_3 \cdot q_3)) = (25, 37, 299 (= 13 \cdot 23))$$

・
・
・

[チェーン方式]

個別鍵の法・を決定する際に、使用する素数は同じ組み合わせにならない限り、使用してもかまわない。

(例2) チェイン方式で共通のマスタ鍵が作れる個別鍵の例 ($m_i = p_i \cdot q_i$ の場合)

$$(e_1, d_1, m_1 (= p_1 \cdot q_1)) = (73, 117, 319 (= 11 \cdot 29))$$

$$(e_2, d_2, m_2 (= p_2 \cdot q_2)) = (13, 37, 143 (= 11 \cdot 13))$$

$$(e_3, d_3, m_3 (= p_3 \cdot q_3)) = (73, 61, 377 (= 13 \cdot 29))$$

・
・
・

使用されるすべての素数を、図2(b)のように鎖でつなぐように決定していくので、この方式を**チェーン方式**、またチェーン方式で法を生成したRSA暗号を**チェーン方式RSA暗号**と名付ける。

2. 4 素数の数と個別鍵の数の関係

素数の数と、法の数との関係は、 $m_i = p_i \cdot q_i$ のとき、標準方式とチェーン方式を比べると図3のようになる。

チェーン方式では、素数の数が同じ場合には標準方式に比べ、マスタ鍵が作れる個別鍵の数は飛躍的に増大する。また、チェーン方式で m_i に使用する素数の数

を $m_i = p_i \cdot q_i \cdot r_i \dots$ と増やしたとき、図4のようになる。

チェーン方式では、図4に示すように使用する素数の数が増大すると、個別鍵数が飛躍的に増大する。以上のことから、チェーン方式は、標準方式と比べると飛躍的に多くの個別鍵を生成できることがわかる。以上のことから、大規模なグループワークにおけるユーザ数に対する鍵を効率良く生成でき、更に生成された個別鍵から小山の手法によりマスタ鍵を生成することにより、効率の良い鍵の管理が可能となる。

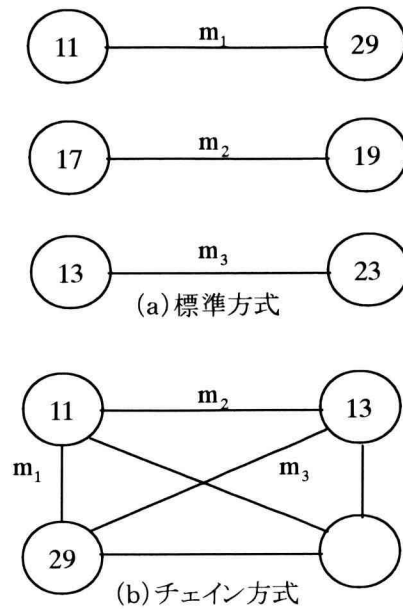


図2 両方式の違いの概念図

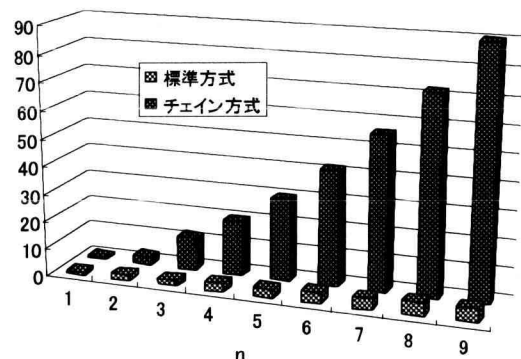


図3 標準方式とチェーン方式の比較

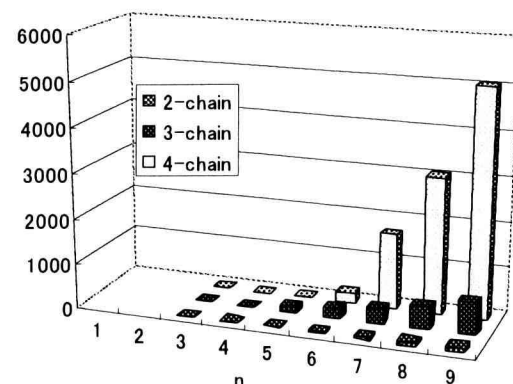


図4 チェイン方式で生成できる鍵の数の比較

3. チェイン方式RSA暗号の安全性

従来のRSA暗号では、法 m_1 の素因数分解の計算量的困難さにより安全性を保証している。本節では、チェイン方式RSA暗号を用いた際に、安全性が、従来のRSA暗号と同程度に保証されるための条件について考察する。

五つの互いに異なる素数を p, q, r, s, t とする。このときチェイン方式では、以下のような二つの法を作ることができる。

$$m_1 = p \cdot q \cdot r$$

$$m_2 = q \cdot r \cdot t$$

このとき m_1, m_2 が公開されているとすると

$\text{GCD}(m_1, m_2)$ を計算することにより $q \cdot r$ が容易に求め

られてしまう。このとき $m_1 / (q \cdot r), m_2 / (q \cdot r)$ を計算する

ことにより素数 p, t が容易に求められ、RSA暗号の安全性を保証する素因数分解が容易に行えることになる。このことから、チェイン方式で作成された複数の公開された法を用いることにより暗号としての安全性を容易に崩すことができることになる。

以上のことからチェイン方式RSAでは、公開できるのは暗号化鍵 e_i のみで、法 m_i は公開できない。したがってチェイン方式RSA暗号は、RSA暗号の良い性質を受け継いでおり、さらにチェイン方式を採用したことで、大規模グループに適した暗号方式となっているが、法 m_i を公開できないので、秘密鍵暗号として取り扱う必要があることがわかる。

4. チェイン方式 RSA 暗号の鍵生成時間

チェイン方式 RSA 暗号の法の構成素数の数の違いによる鍵生成時間を計算機により実験的に比較を行った(表1)。結果は、ランダムに 1000 個の鍵を生成し、その生成時間の平均をとったものである。

表1 鍵生成速度の比較

法 m_i の構成素数の数	鍵一つあたりの生成時間[秒]
2 (標準方式)	0.048
3 (チェイン方式)	0.082
4 (チェイン方式)	0.074
5 (チェイン方式)	0.136

表1は、法を構成する素数の数が増えても、チェイン方式 RSA 暗号では、鍵の生成時間が指数関数的に増加することではなく、標準方式の場合の高々数倍程度の時間で鍵の生成が可能であることを示している。

5. むすび

本報告では、エージェントシステムや大規模な広域自律分散環境をインターネット等のセキュリティ上危険なネットワークを使い構成した際のセキュリティ方式について提案を行った。提案したチェイン方式RSA暗号方式では、鍵長を長くすることなく、多くの鍵を生成でき、莫大なグループ数のユーザやシステムに対して、十分な数の鍵を生成できる。また、鍵の生成時間も実用可能な程度に抑えることが可能である。

RSA暗号方式は、現在、インターネット上で、実用的に用いられている方式であり、その利点・欠点は、実用の世界で十分試されており、数多く報告がなされている。しかしながら近年、数学的な安全証明付きの暗号方式が多数提案されてきている^[4]。今後は、そのような暗号方式に、本報告と同様な拡張をおこない、より使いやすいテレワークアプリケーションへの適用を検討する予定である。

参考文献

- [1] 今田, 移動エージェントシステムにおけるセキュリティ実現方式, 電子情報通信学会論文誌, B, Vol. J84-B, No. 5, pp.932-939, 2001.
- [2] 美馬, 移動するプログラム—モバイルエージェント—, 電子情報通信学会誌, vol.82, no.4, pp.360-366, 1999.
- [3] 本位田, 第5回 動き始めたモバイルエージェント, 情報処理, vol.39, no.8, pp.812-815, 1998.
- [4] 電子商取引時代の次世代暗号技術を各社が開発し, ISO/IEC へ提案, 電子通信学会誌, Vol.83, No.7, pp. 590-593, 2000.
- [5] 小山, RSA公開暗号法のマスタ鍵, 信学論(D), vol. J65-D, no. 2, pp. 163-170, 1982.
- [6] 小山, マスター鍵による同報通信の暗号方式, 信学論(D), vol. J65-D, no. 9, pp. 1151-1158, 1982.
- [7] 佐々木, 荒木, 山本, 在宅勤務向けインターネット電話サーバの構築法, 第1回日本テレワーク学会研究発表大会講演論文集, pp.59-64, 1999.
- [8] 荒木, 柳川, 山本, 国際協業に適した自律分散コンピュータシステム, 第2回日本テレワーク学会研究発表大会講演論文集, pp.1-6, 2000.
- [9] 柳川, 荒木, 山本, 自律分散キューの提案, ソフトウェアサイエンス研究会, 信学技報, SS99-65~68, pp.1-8, 2000.
- [10] 岡本, 山本, 現代暗号, 産業図書, 1997.