グループ利用クライアント／サーバ・システムのセキュリティ

大前義次、　荒木智行、　小高泰陸、　平山勉

神奈川工科大学　情報工学科
e-mail:{ohmae, araki}@ic.kanagawa-it.ac.jp

あらまし

本報告では、ＲＳＡ公開暗号方式における新しいマスター鍵方式を提案し、その応用としてクライアント，サーバグループ、セキュリティ・サーバで構成されるクライアント／サーバ・システムにおいて、複数のサーバグループがあり、グループ間でのセキュリティが保たれる必要のある環境においての認証方式を提案し，有効性を示す。その有効性は，要約すると以下の３点である。（１）マスタ鍵方式を採用しているため、鍵の管理が容易であり，また同報通信が可能である。（２）サーバグループ内のサーバ数が増加しても、十分な数のサーバの個別鍵に対応したマスタ鍵の生成が容易にできる。（３）ケルベロス方式に比べ，認証のために必要な手順の簡略化，時間の短縮化が可能である。

Security of Client/Server Systems for Group Cooperation Work

Yoshitsugu OHMAE, Tomoyuki ARAKI, Yoshimichi KOTAKA and Tsutomu HIRAYAMA

Dept. of Information and Computer Sciences,
Kanagawa Institute of Technology
e-mail:{ohmae, araki}@ic.kanagawa-it.ac.jp

Abstruct

This paper proposes a new master-key-style method of RSA public key encryption, and as its application, describes on security in applications for group cooperation work based on Client/Server systems that are composed of clients, servers' groups and security servers. Then, it is assumed that there are some groups in the same system and secrecy must be kept each other among groups. We show that the proposed method is effective in such environment and applications. The effectiveness is summarized as follows: (1) It is easy to administrate keys because the proposed method adopts master-key-style. And multi-address communication is available. (2) We can generate easily the sufficient number of keys corresponding to the master key even if the number of member of servers' group would be increasing. (3) It is possible to shorten the time for authentication in comparison with Kerberos-style's because the proposed process is simpler than Kerberos-style's.

１．まえがき

計算機システムの新しい構成方法としてクライアント／サーバ・システム[3]が注目されている。本研究は，ある一つのクライアント／サーバ・システムの環境の中にサーバのグループが存在し，各グループ間で互いに機密保護が実現されなければならない場合のセキュリティ方式について考察している。まず，通信路上での機密保護という意味で，通信文を暗号化する。このとき，暗号化／復号化にはＲＳＡ公開暗号方式を用いる。ＲＳＡ公開暗号方式は，公開暗号方式の中でもマスタ鍵を作成できる方式であり[1]，また，その同報通信への応用についての考察も一部なされている[2]。クライアント／サーバ・システムにおけるセキュリティ・システムとしてケルベロス方式が提案されている[3]。本研究は，クライアント／サーバ・システムのグループ協調作業に不可欠となる同報通信において，今回提案するＲＳＡ公開暗号方式における新しいマスタ鍵を適用して，（１）マスタ鍵による容易な鍵管理，（２）サーバグループ内のサーバ数が増加しても，十分な数のマスタ鍵が生成でき，（３）認証に必要となる手順数を減らすことにより，認証のために必要となる時間を短縮することを試みた。

その結果，（1），（2）の条件を満たしながら，ケルベロス方式よりも短い時間で，クライアント／サーバ・システムにおける分散セキュリティ・システムでの認証を可能とした。

2．ＲＳＡ公開暗号方式における新しいマスタ鍵

以下では，拡張定義されたＲＳＡ暗号，マスタ鍵などについて説明する。

2．1　ＲＳＡ暗号

ＲＳＡ暗号の基本原理を簡明に以下に示す。暗号化個別鍵を$K_{ei}=(e_i,m_i)$，復号化個別鍵を$K_{di}=(d_i,m_i)$とする。K_{ei}は公開されており，K_{di}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。

$$C=E(P)=P^{e_i} \pmod{m_i} \tag{2.1}$$

$$P=D(C)=C^{d_i} \pmod{m_i} \tag{2.2}$$

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，復号化は一対一かつ上への写像である。ＰとＣを代表してＭで表すと，

$$M^{e_i\cdot d_i}\equiv M \pmod{m_i} \tag{2.3}$$

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。

$$m_i=p_i\cdot q_i \quad (\text{ただし，}p_i,\ q_i\text{は相異なる大きな素数}) \tag{2.4}$$

$$\varphi(m_i)=\varphi(p_i)\varphi(q_i)=(p_i-1)(q_i-1) \quad (\text{ただし}\varphi\text{はオイラー関数}) \tag{2.5}$$

$$e_i\cdot d_i\equiv 1 \pmod{\varphi(m_i)} \tag{2.6}$$

従来より使用されてきている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。

2．2　拡張定義されたＲＳＡ暗号

以下では，m_iの構成に着目してＲＳＡ暗号を拡張定義する。

［定義2.1］　(2.6)式において，通常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$m_i=p_i\cdot q_i\cdot r_i\cdots$によって式(2.6)を置き換えたものを拡張されたＲＳＡ暗号と呼ぶ。 □

しかしながら，定義１で定義される方式がＲＳＡ暗号であるという保障はないが，以下の定理１において，その保障を与える。

［定理１］　拡張定義されたＲＳＡ暗号は，従来のＲＳＡ暗号同様，

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

が成立し，暗号化，復号化は一対一かつ上への写像である。

（証明）　まず，m_iが三つの相異なる素数p_i，q_i，r_iの積である（$m_i=p_i\cdot q_i\cdot r_i$）ときについて証明する。(2.6)式より，あるｋが存在して

$$e_i\cdot d_i=k\varphi(m_i)+1=k(p-1)(q-1)(r-1) \tag{2.7}$$

である。また，フェルマーの小定理[4]より，

$$M^{p_i-1}\equiv 1 \pmod{p_i} \tag{2.8}$$

(2.8)式の両辺を$k(q-1)(r-1)$乗してＭをかけると，

$$M^{k(p_i-1)(q_i-1)(r_i-1)+1}\equiv M^{k\varphi(m_i)+1}\equiv M^{e_i\cdot d_i}\equiv M \pmod{p_i} \tag{2.9}$$

また，素数p_i，q_iについても同様の結果を得るので，$m_i=p_i\cdot q_i\cdot r_i$について

$$M^{e_i\cdot d_i}\equiv M \pmod{m_i} \tag{2.10}$$

を得る。m_iが四つ以上の相異なる素数の積の場合についても，式(2.9)は任意の$\varphi(m_i)$について成立していることから同様に成立する。

また，暗号化，復号化は一対一かつ上への写像であることは明らかである。　（証明終）

定理１より，拡張されたＲＳＡ暗号は，本質的に従来のＲＳＡ暗号と同じものである。これにより，以降混乱の恐れのない限り，従来および拡張されたＲＳＡ暗号を同一視してＲＳＡ暗号と呼ぶ。

2．3　ＲＳＡ暗号のマスタ鍵

ここでは，従来から使用されているマスタ鍵の作成法（ここでは「標準方式」と呼ぶ）と，新しいマスタ鍵の作成法として「チェイン方式」を説明する。

[標準方式]

ごく一般的なマスタ鍵の作成法である。すべての個別鍵の法 m 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）標準方式でマスタ鍵の作れる個別鍵の例　（$m_i = p_i \cdot q_i$ の場合）

$(e_1, d_1, m_1\ (p_1, q_1)) = (73, 117, 319(=11\times29))$
$(e_2, d_2, m_2\ (p_2, q_2)) = (61, 85, 323(=17\times19))$
$(e_3, d_3, m_3\ (p_3, q_3)) = (25, 37, 299(=13\times23))$
⋮

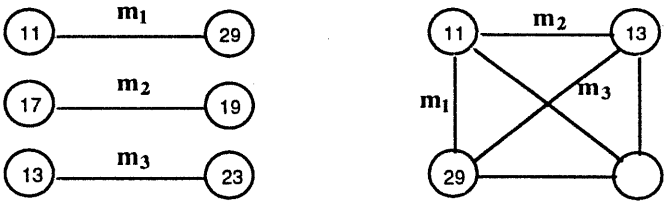
[チェイン方式]

個別鍵の法 m 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，何度使用してもかまわない。

（例２）チェイン方式でマスタ鍵の作れる個別鍵の例　（$m_i = p_i \cdot q_i$ の場合）

$(e_1, d_1, m_1\ (p_1, q_1)) = (73, 117, 319(=11\times29))$
$(e_2, d_2, m_2\ (p_2, q_2)) = (13, 37, 143(=11\times13))$
$(e_3, d_3, m_3\ (p_3, q_3)) = (73, 61, 377(=13\times29))$
⋮

使用されるすべての素数を，図２－１(b)のように鎖でつなぐように決定していくので，この方式をチェイン方式と名付ける。



(a)標準方式　　(b)チェイン方式

図２－１　各方式の概念図

2．4　素数の数とマスタ鍵を作れる個別鍵の関係

マスタ鍵に使用できる素数の数と，マスタ鍵の作成できる個別鍵の数は，$m_i = p_i \cdot q_i$ のとき，標準方式とチェイン方式を比べると図２－２のようになる。

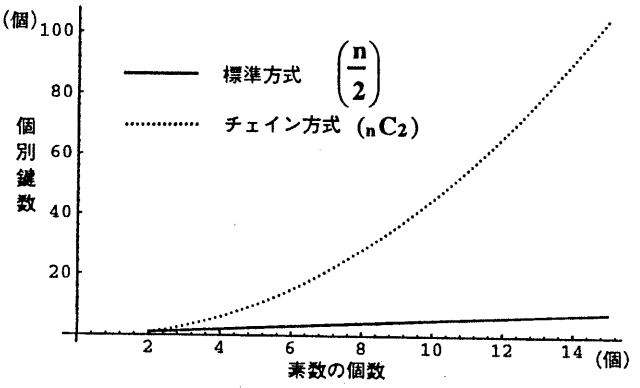


図２－２　素数の数と個別鍵の数の関係

チェイン方式では，素数の数が同じ場合には標準方式に比べ，マスタ鍵の作れる個別鍵の数は飛躍的に増大する。また，チェイン方式で m_i に使用する素数の数を $m_i = p_i \cdot q_i \cdot r_i \cdots$ と増やしたとき，図２－３のようになる。

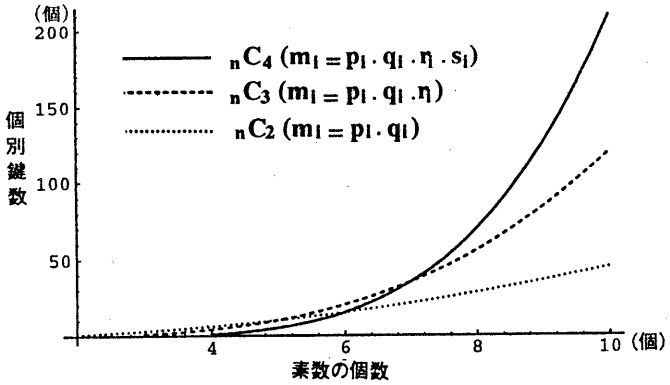


図２－３　チェイン方式における素数の数と個別鍵数の関係

チェイン方式では，図に示すように使用する素数の数が増大すると，マスタ鍵の作れる個別鍵数が飛躍的に増大する。以上のことから，チェイン方式は，一つのマスタ鍵で標準方式と比べると飛躍的に多くの個別鍵をマスタ化できることがわかる。

ＲＳＡ暗号における安全性を考慮して，鍵の生成時における条件が指摘されている[6]。チェイン方式では，以上で示したように，素数の数に対して標準方式よりも多くの鍵を生成できることが判明した。そこで，その中でも，どのような暗号化鍵が，より安全であるかについて考察を行った。その結果，次のような条件を満たす鍵が，より安全であるという結果を得た。（詳細は略す。）

（条件）異なる暗号化鍵 e_1，e_2 は互いに素でない整数として選ぶ。

３．クライアント／サーバ・システムのセキュリティへの適用

クライアント／サーバ・システムのセキュリティ方式としてのケルベロス方式は，基本的にクライアントとサーバの手続きは一対一を想定しており，複数台のサーバと同時に通信を行うためには，サーバの台数と同じ回数の認証手続きを要する。クライアント／サーバ・システムの環境では，クライアントとサーバが一対一である場合ばかりではなく，一台のクライアントと，複数のサーバが同時に通信することが多い。ここでは，ケルベロス方式においてサーバ台数が増加したとき認証に必要となる手続きが増加するのを防ぐために，複数サーバをグループ化し（以降，サーバ・グループと記す），クライアントからサーバ・グループへの同報通信によって認証手続きを行う方法（チェイン方式マスタ鍵によるケルベロス方式）について提案を行う。

３．１　ケルベロス方式

ケルベロス方式について簡単に説明する。

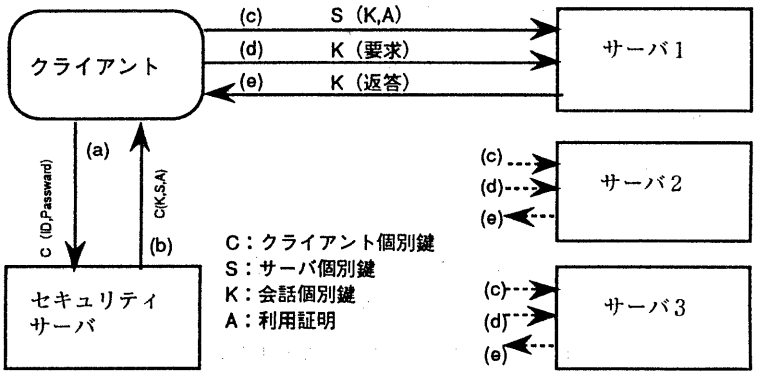


図３－１　ケルベロス認証方式

ケルベロス方式の実施手順

（a） クライアントはセキュリティサーバにクライアントの個別鍵でユーザID，パスワードを送る。
（b） セキュリティサーバは，クライアントと一つ一つのサーバとの会話のために個別会話鍵を生成する。
（c） クライアントは，サーバの個別鍵で暗号化された会話個別鍵をサーバに送る。
（d），（e） クライアントとサーバは，これ以降の通信を行うための，セキュリティ情報のやり取りを行う。
（c）～（e）はサーバの台数だけ繰り返す。
この方式で使われる暗号方式は，慣用暗号系，公開暗号系のいづれも使用することができる。

3．2　チェイン方式マスタ鍵によるケルベロス方式

従来のケルベロス方式は，基本的にクライアント－サーバ間は一対一の手続きを行っているが，チェイン方式マスタ鍵によるケルベロス方式では，チェイン方式マスタ鍵を使った同報通信による認証方式を行う。

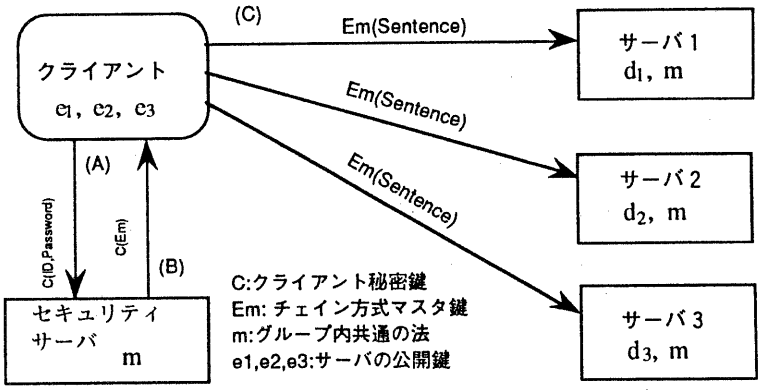


図３－２　チェイン方式マスタ鍵によるケルベロス方式

公開暗号方式であるチェイン方式マスタ鍵を使用する上で，最も少ない手順で認証を行うために，本方式では，次のような前提を設けてある。

（1） 通常のＲＳＡ暗号では，暗号化鍵と法を同時に公開するが，本方式では，暗号化鍵のみをマスタ鍵として公開する。
（2） 法mはサーバグループおよびセキュリティサーバ内のみでは公開するが，クライアントには公開しない。

これにより，複数のサーバおよびセキュリティサーバで共通の法mを用いても暗号としての安全性は保たれる。

また，本方式でチェイン方式マスタ鍵を使用する理由を以下に述べる。

（1） サーバグループ内のサーバ数が多くなた場合でも，チェイン方式を採用しているので，従来のＲＳＡ暗号のマスタ鍵よりも，一つのマスタ鍵で多くの個別鍵に対応でき，グループ内のサーバの数を容易に増やすことができる。
（2） マスタ鍵であることから，同報通信ができる。そのため認証に必要な手順を削減できる。

本方式の実施手順を図３－２にそって，以下に述べる。

（A） クライアントはセキュリティサーバにクライアントの個別鍵でユーザID，パスワードの他にクライアントからグループ化したサーバすべての個別の公開鍵をセキュリティサーバに送る。
（B） セキュリティサーバはマスタ鍵を作成し，クライアントに送り返す。
（C） クライアントは同報通信で，サーバーグループ全体にマスタ鍵Emで暗号化したセキュリティ情報を送る。サーバグループ内の各サーバは，それぞれの持つ複合化鍵 d_i とｍで複合化する。

4．従来のケルベロス方式との計算時間の比較

図４－１は従来の従来のケルベロス方式にＲＳＡ暗号を用いた場合と，本報告で提案したチェイン方式マスタ鍵によるケルベロス方式を，実際に計算機上で行った場合の比較である。前提条件として，クライアントとサーバ間で転送する平文の長さは1,000バイトである。実行はMicroSPARC (85MHz)で行った。同報通信を行っているので，サーバ台数が増加しても計算時間の増加は殆ど見られない。また，サーバ一台の場合でも，ケルベロス方式に比べ手順が簡略化されているので，計算時間は少ない。

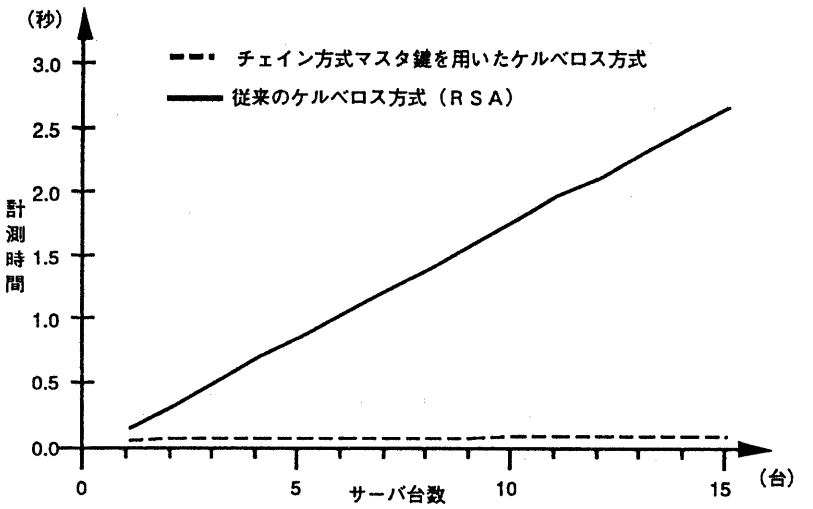


図４－１　従来のケルベロス方式との計算時間の比較

５．むすび

本報告では，クライアント／サーバ・システム環境でのサーバのグループ利用に適した新しいＲＳＡ暗号のマスタ鍵および，そのケルベロス方式への適用を行い，その有用性を示した。提案したチェイン方式のマスタ鍵は，非常に多くの個別鍵をマスタ化できるので，大規模なグループウェア・アプリケーションへの適用が可能と考えられる。引続き今後はこの面の研究を行っていきたい。

参考文献

(1) 小山謙二：" ＲＳＡ公開暗号法のマスタ鍵" ，電子通信学会論文誌（Ｄ），J65-D, No.2, pp. 163-170 , 1982.
(2) 小山謙二：" マスタ鍵による同報通信の暗号方式" ，電子通信学会論文誌（Ｄ），J65-D, No. 9, pp. 1151-1158, 1982.
(3) Renaud, P. E., "INTRODUCTION TO CLIENT/SERVER SYSTEMS", John Wiley & Sons, 1993.
(4) 高木貞治：" 初等整数論講義" ，共立出版，1931.
(5) 池野信一，小山謙二：" 現代暗号理論" ，電子情報通信学会，1986.
(6) 岡本栄司：" 暗号理論入門" ，共立出版，1993.