グループに適した暗号化鍵の管理と配送システム

7Ｇ－3　武藤　康史　中村　秀紀　松下　温　岡田　謙一
慶應義塾大学

１．はじめに

最近、ネットワークのセキュリティーに対す関心が高まっている。外部の侵入者から大切なデータを守る手段としての暗号化は、通信段階で非常に有効である。その暗号法は、これまで様々な形のものが考案されてきたが、最近では暗号化に、暗号化鍵を使用するのが一般的になっている。そのために、鍵は重要な存在となるので、鍵の管理と各ユーザーへの配送の方法も重要となってくる。

また、我々がある組織の中で作業を行う場合グループを形成して行うことが多い。さらに、各ユーザーは一つのグループだけではなく、複数のグループに所属していることも多いので、そういった状況に適したシステムが必要になってくる。

そこで、我々はグループにおける通信に適し、かつ、グループ構造の変化に対しても、柔軟に対応できる鍵管理システムを提案し、同時に、そのシステムに適した鍵配送システムも提案する。

２．暗号法

現在の暗号法は、大きく分けて、秘密鍵暗号系と公開鍵暗号系の二つに分類される。ここで、その二つを概説する。

２．１　秘密鍵暗号系

慣用鍵暗号系とも言われ、暗号化鍵と復号化鍵が同じという従来からの方式である。この方式の安全性は、鍵に依存しており、通信効率が良い。代表的なものとして、アメリカのデータ暗号化規格ＤＥＳ（Data Encryption Standard）があり、安全性・通信効率の上で非常に優れているために、今後、各方面で標準化の動きがあり、本論文でも暗号アルゴリズムはＤＥＳを想定している。

２．２　公開鍵暗号系

暗号化鍵は公開にし、復号化鍵のみを秘密にするという方式であり、1976年にDiffieとHellmanがその概念を考案した。公開鍵（暗号化鍵となる）は、一方向関数によって、秘密鍵（復号化鍵となる）から生成されるので、その安全性は一方向関数に依存している。また、公開鍵暗号は認証に利用できるので、その機能が大きな注目を浴びている。しかし、通信効率が悪いという大きな欠点がある。代表的なものとしてＲＳＡ暗号がある。

３．鍵管理システム

秘密鍵暗号系における通信は、一対一であり、通信相手が増加するとそれにともなって管理する鍵の数も増加していった。最近ではグループ化が進み、グループ用の鍵も必要になってきた。しかし、それぞれ個別の鍵で暗号化しようとすると、管理する鍵の数が多すぎて、管理しきれなくなってしまう。

３．１　鍵管理

そこで我々は、こういった状況を考慮し、秘密鍵暗号系に対し、グループ化に対応できる鍵の管理システムを提案する。それぞれのユーザーは、図１のように共通鍵K0と、鍵を生成するために使われる補助情報（以後これをピースと呼ぶ）を持つ。各ユーザーは、それぞれある一つのピース以外はすべて持つことになるのだが、ここでは便宜的にユーザーUiはピースPiを持たないことにする。

	P1	P2	P3	P4	P5	K0
U1	×	○	○	○	○	○
U2	○	×	○	○	○	○
U3	○	○	×	○	○	○
U4	○	○	○	×	○	○
U5	○	○	○	○	×	○

図１．各ユーザーが持つピース

３．２　鍵の生成

実際に通信に用いる鍵の生成法を説明する。例えば、ピースPiを使って鍵を生成したい場合は、

$$K' = f(K0, Pi)$$

という一方向関数 f(Ki,Pi) によって鍵K'を生成する。複数のピースによって鍵を生成する場合は、

$$K' = f(\ldots f(f(K0,P1),P2),\ldots,Pi)$$

として鍵K'を得る。

ユーザーU1とU4とが通信する場合、それぞれ共通鍵K0とピースP2,P3,P5を持っているので、このK0,P2,P3,P5から鍵K'を生成する。ユーザーU1とU4以外に、このK0,P2,P3,P5をすべて持っているユ

Group Oriented Management and Distribution System of Encryption Key
Yasusi Mutoh, Hidenori Nakamura, Yutaka Matsusita, Kenichi Okada
Keio University

ーザーはいないので、他のユーザーはこの鍵K'を生成することはできない。また、ユーザーU2,U3,U5がグループを形成していた場合には、それぞれ共通鍵K0とピースP1,P4を持っているので、このK0,P1,P4を使って鍵K'を生成する。さらに、全員に同報通信をしたい場合は、共通鍵K0を使って通信を行えば良い。

3．3　管理する鍵の数

ユーザーがｎ人いる場合、この方式では、各ユーザーが管理する鍵（ピース）の数は、グループの数にかかわらず、共通鍵１個とピースｎ－１個の和ｎ個である。これに対し、従来の方式では、ｍ個のグループに属していれば、自分を除いたｎ－１人との鍵と、ｍ個のグループ用の鍵を合わせてｎ＋ｍ－１個となる。従って、我々の方式の方が少ないことが分かる。

4．鍵の配送

暗号の安全性を鍵に依存しているシステムでは、安全性を持続するために、ある周期で鍵を更新する必要があり、そのためには、鍵の配送ということが問題になってくる。そこで、我々の鍵管理システムに適した鍵配送システムを同時に提案する。このシステムは、同じピースを多く持つユーザーには、なるべく同報によってピースを配送しようというものである。まず、それぞれのユーザーが配送用の秘密鍵を生成し、その鍵から公開鍵のアルゴリズムによって公開鍵を生成し、公開する。鍵生成者はユーザーを半分に分け、前半と後半のそれぞれに配送用鍵S1,S2を公開鍵配送系を使って配る。

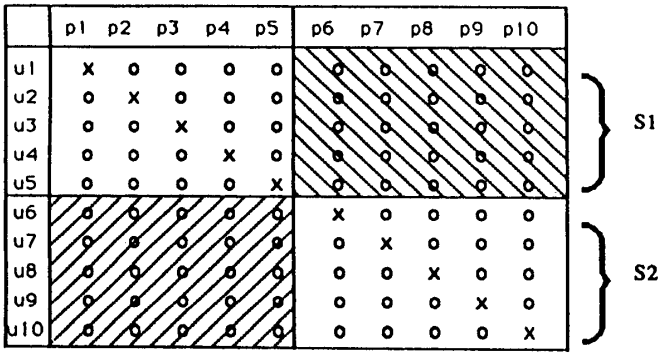

図2. 配送方法　（ ▨ ▧ 部分を同報 ）

図２の右上と左下の共通部分のピースをそれぞれこのS1,S2で同報により送る。同じ操作を残りの部分についても繰り返す。最後に分割しきれなくなったところで個々にピースを送る。配送用鍵は、配送以外には使用しないとすると、外部に知られる危険性が少ないと考えられるので、次回からの再配送の際には、この配送用鍵を使用して配送することができる。この方法で配送すると、ユーザーが６人以上であれば、すべてのピースを個々に配送する方法に比べてかなり効率が上がり、しかも安全である。ここで、図３に個々に配送した場合との通信回数の比較を示す。

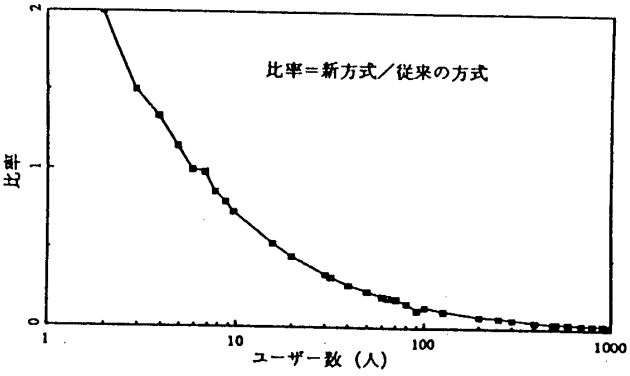

図３．配送効率

5．認証

グループ内における通信において、どのメンバーから通信文が届いたのかが判別できるように認証が必要となる。本方式において、認証は次の手順で行われる。

まず、認証用の文書Ｔｘを慣用暗号系Ｃでグループ鍵Ｋｇを用いて暗号化する。次に公開鍵暗号系Ｐの自分の秘密鍵Ｓａを用いて公開鍵暗号系で暗号化した通信文ＴＴをグループに同報する。受信したメンバーは送信者の公開鍵ＩＤａで復号化した後、Ｋｇで復号化してＴｘを得る。すなわち、

ＴＴ＝Ｐ（　Ｃ（Ｔｘ，Ｋｇ），　Ｓａ）

Ｔｘ＝Ｃ（　Ｐ（ＴＴ，ＩＤａ），Ｋｇ　）

となる。

6．おわりに

本論文では、秘密鍵暗号方式における鍵の管理システムと、それに対する鍵の配送システムを提案した。本方式の最大の利点は、ユーザーのグループ化に対して、非常に柔軟に対応できることと配送の容易さにより鍵の安全性が高まるという点である。

参考文献

[1]"Data Encryption Standard", FIPS Pub. 46, National Bureau of Standards, Washington, D. C., 1977

[2]Hidenori Nakamura, "Hierarchical Group Oriented Key Management Method", 1990

[3]高木,南部他,"新しいグループ指向鍵管理方式", 情報処理学会第40回全国大会, 1990

[4]S. J. Kent, "Security requirements and protocols for a broadcast scenario", IEEE Trans. Commun., COM-29, 6, 1981