

グループ指向型鍵管理に適した暗号鍵配送法

高木和幸 武藤康史 岡田謙一 松下温
慶應義塾大学

通信衛星や LAN 等の発達によりグループ同報通信という通信形態が一般化してきた。この通信環境において、秘密通信を行なう方法として暗号法によるアクセス制御を用いることが多いが、グループ構造の変化等による暗号鍵の再配達が煩雑になるという問題が存在する。本件では、これらの問題に対する一解答として、高木、中村、武藤らが提案する MCK 鍵管理方式に基づく暗号鍵の配達法を提案する。

A Group Oriented Key Distribution Method

Kazuyuki Takagi, Yasushi Mutoh
Ken-ichi Okada, Yutaka Matsushita
Keio University

3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223, Japan

Thanks to the progress of the technology for the satelite communication and local area network, a communicational form called the group broadcast communication gets much popular. In this form, a secure broadcast communication can be generally achieved by means of using encryption. But once a communicational structure ,which may sometimes called a "group", changes , a lot of encryption keys must be redistributed in order to renew the appropriate keys. In this paper, we propose a method for key distribution based on MCK method.

1. はじめに

暗号法は、データの安全性、真実性、完全性を守るために方法であるが、それに加えて情報へのアクセス制御にも利用される。これは、暗号化されたデータの復号は正しい鍵を持つ者だけしかできないということによるものである。昨今注目されている大規模な L A N や通信衛星による通信において、通信路に流されるデータの安全を守るために暗号法を用いることはとても自然なことと考えられる。

組織が存在してその組織が活動している場合にはその中においては数多くの通信が行われている。その通信はその組織自体の構造にかなり依存していると考えられ、構造自体には様々なバリエーションがあるが一般的にはそのうちの少数の基本的な構造またはそれらの組み合わせにすぎないとみなすことができる。代表的なものは、階層構造とグループ構造、および、その両方の構造的特徴を兼ね備えたものである。

そのような組織構造に多くのグループが存在し、グループ内で秘密通信を行う場合ではそのグループ内通信用の鍵を持たなければならない。また、グループの構成員が変化した場合、秘密通信を確保するために従来方式においては必ず鍵の再配達を行わなければならず煩雑であった。

このように、グループの構造が変化する場合に有効である鍵管理法が中村、高木、武藤らによって提案されている(M C K 方式)。M C K 方式では、「共通鍵」といくつかの「ピース」と呼ばれる鍵生成子の組み合わせから、多重鍵を生成する方法を採用している。ピースの組み合わせの数は、ピース自身の数よりはるかに大きいので、少数のピースから多数の鍵を生成することができる。本件では M C K 方式において最適なピースの配送方式を提案する。

2. M C K 方式 (Modified Copy Key Method)

M C K 方式においてグループのメンバーは暗号化や復号化に用いる鍵をそのままの形で保持するのではなく、鍵の代わりにひとつの「共通鍵」といくつかの鍵生成子である「ピース」を保持し、通信に用いる暗号鍵を共通鍵といいくつかのピースのセットから生成する。

2. 1 鍵生成法

M C K 方式において平文を暗号化するための通信鍵 K' は共通鍵 K とピース P によって以下のように生成される。

$$K' = f(K, P) \quad (1)$$

ここで f は適当な暗号化関数である。 P と K の独自な組から、独自な K' を生成するためには、 f は K 空間から K' 空間への 1 対 1 対応である必要がある。もしも、通信鍵を生成するために、複数個のピース $[P_1, P_2, \dots, P_i]$ が用いられるのであれば、 K' は以下のようにして生成される。

$$K' = f(\dots f(f(K, P_1) P_2), \dots, P_i) \quad (2)$$

ここで、ピース P_i は通し番号の昇順で代入される。もしも f が 1 対 1 対応であれば独自なピースの組み合わせによって独自な鍵が生成される。

3. 2 ピース分配法

まず、一つのグループにメンバーが n 人存在する場合を考える。この時に必要となるピースの総数は n 個で、fig.1 のように互いに異なる $n - 1$ 個のピースの組を各メンバーに分配する。

この方法を用いることによって、各グループのメンバーは $n - 1$ 個のピースと共通鍵を持つことで合計 n 個の鍵に対する情報を持つことになる。

	P1	P2	P3	P4	P5	Common Key
• U1		●	○	○	●	○
• U2	○		○	○	○	
• U3	○	●		○	●	○
• U4	○	●		○	●	○
• U5	○	○	○	○	●	○

• :Members of the group
○ :Distributed piece
● :Common piece

Fig.1 Group oriented piece distribution

3. 3 通信方法

通信文は、通信に必要とされるピースから生成された通信鍵を用いて暗号化される。そのときに使用したピースの通し番号は共通キーKによって暗号化され、ヘッダとして通信文の先頭に附加され、電文となる。各メンバーはヘッダを復号化し、ピース番号を知ることにより通信文が復号化可能であるかどうかを判定する。また、全グループ内への同報通信は、グループ内の全てのメンバーに共通するピースが存在しないので、通信文は全てのメンバーが持つ共通鍵Kによって暗号化される。

4. グループ指向型鍵配達法 GKD

(Group Oriented key Distribution method)

MCK方式において、鍵の配達の重要性が問題となるのは共通鍵ではなく、ピースである。各ユーザーにネットワークなどの同報機能を有する配達経路を用いてピースを配達する方法GKDを提案する。

まず、各ユーザーに個別にピースを配達する方法が考えられるが、従来の方式である配達センターを介する方法や公開鍵配達系を用いる方法においては、ピース配達者にトラフィックが集中するのでピース生成者のオーバーヘッドが大きくなるという問題点がある。

次に示すGKD方式を採用することでこの問題を改善することができる。まず、この方式では、同じピースをより多く所有しているユーザーには、そのピースの集合をブロック化して同報通信によって配達するという方法をとっている。

各ユーザーはあらかじめ公開鍵配達系に対応した秘密鍵を生成し、その秘密鍵から公開鍵を生成してピース生成者に公開しておく。その後ピース生成者は、全てのピースを生成した後でグループに所属しているユーザーのリストによってユーザーを2分割し、前半と後半の2つのサブグループに分ける。そこで、前半のグループに属しているユーザー全てに、ピース同報配達用の鍵（この鍵をブロック鍵とする）を公開鍵配達系により配達する。その後、このブロック鍵により前半のグループのユーザーが共通に所有するピースを同報する。後半のグループにも同様な方法により共通なピースを同報する。さらに、この時点で配達されていないピースのブロックについても再帰的に同じ操作を繰り返すことによって残りのブロックを効率よく同報により配達することが可能である。

この操作は対象となるユーザーのブロックにユーザーが4人以上いる場合には有効であり、4人未満の場合には個別に公開鍵配達系を用いて配達した場合との通信効率の差はないので、ユーザー×ピース マトリックスが 4×4 のブロックを最小分割単位とする。ここで通信効率は、配達するピースのサイズと配達する回数の積、即ち実質的なトラッフィックの量で比較することにする。

以下に、具体的な例をあげて説明する。

	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12
u1	x	o	o	o	o	o	x	x	x	x	x	x
u2	o	x	o	o	o	o	o	x	o	o	x	o
u3	o	o	x	o	o	o	o	o	x	o	o	o
u4	o	o	o	x	o	o	o	o	o	x	o	o
u5	o	o	o	o	x	o	o	o	o	o	x	o
u6	o	o	o	o	o	x	o	o	o	o	o	x
u7	x	x	x	x	x	x	x	o	o	o	o	o
u8	x	x	x	x	x	x	o	x	o	o	o	o
u9	o	o	o	o	o	o	o	o	x	o	o	o
u10	o	o	o	o	o	o	o	o	o	x	o	o
u11	o	o	o	o	o	o	o	o	o	o	x	o
u12	o	o	o	o	o	o	o	o	o	o	o	x

(□ □ 部分を同報)

fig.2 GKD method 1

ユーザー数が12人の場合、fig.2のようにユーザーu1からユーザーu6までのグループと、ユーザーu7からu12までのグループの2グループに分割し、それぞれにブロック鍵B1、B2を

配送する。次に、ブロック鍵B1によってピースp7からp12を同報し、ブロック鍵B2によってピースp1からp6を同報する。ここで、右上と左下に配送していないピースのブロックが残

	p7	p8	p9	p10	p11	p12
u7	x	o	o			
u8	o	x	o			
u9	o	o	x			
u10				x	o	o
u11				o	x	o
u12				o	o	x

	p1	p2	p3	p4	p5	p6
u1	x	o	o			
u2	o	x	o			
u3	o	o	x			
u4				x	o	o
u5				o	x	o
u6				o	o	x

Fig.3 GKD Method 2

さらに、この残りのブロックについても、fig.3 のようにユーザーu1からユーザーu6を2分割してブロック鍵B3,B4を配送して、それぞれピースp4,p5,p6とp1,p2,p3を同報する。もうひとつつの残りのブロックについても同様に、の用に分割して配送する。ここまで分割すると、残りのブロックについては個別に配送しても通信効率は変わらないので個別に配送する。

	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11
u1	x	o	o	o	o	o					
u2	o	x	o	o	o	o					
u3	o	o	x	o	o	o					
u4	o	o	o	x	o	o					
u5	o	o	o	o	x	o					
u6	o	o	o	o	o	x					
u7							x	o	o	o	o
u8							o	x	o	o	o
u9							o	o	x	o	o
u10							o	o	o	x	o
u11							o	o	o	o	x

(□ □ 部分を同様)

Fig.4 GKD METHOD 3

また、ユーザー数がfig.4 のように奇数になった場合でも、同報によって配送するピースをブロックによってできる残りのブロックは常に正方形となり、再帰的な操作を繰り返すことができる。

5. 通信効率の評価

ユーザー数を 2^n 人 ($n > 2$) としピースのサイズを k (bit) とすると、個別に配送する場合では、 2^n 人に對し $(2^n - 1)$ 個のピースを配送しなければならないので、全体の通信量は

$$2^n k (2^n - 1) \text{ (bit)} \quad (3)$$

となる。これに対しGKD方式による配送では、ブロック鍵の配送に要する通信量が、

$$(2^n + 2^2 * 2^{(n-1)} + 2^2 * 2^{(n-2)} + \dots + 2^{(n-3)} * 2^3) * k$$

$$= 2^n k * (n-2) \text{ (bit)} \quad (4)$$

であり、ピースの配送に要する通信量が、

$$(2 * 2^{(n-1)} + 2^2 * 2^{(n-2)} + \dots + 2^{(n-2)} * 2^2 + 2^n * 2^3) * k$$

$$= 2^n k * (n-2) + 2^n * 3k$$

$$= 2^n k * (n+1) \text{ (bit)} \quad (5)$$

であるから、これらを合わせると

$$2^n k * (2n+1) \text{ (bit)} \quad (6)$$

となる。したがって $n > 2$ のとき GKD 方式による配送方法の方が通信量が少くなり通信効率がよいことになる。また、ブロック鍵は配送のみに使用するので鍵の寿命が長く頻繁に更新を行う必要がない。仮に、前回使用したブロック鍵を続けて使用した場合のピース配送のための通信量は $2^n k * (n+1)$ (bit) となる。これはブロック鍵の配送がある場合のほぼ $1/2$ になっている。

この式はユーザー数が 2^n の形で表せるときにしか成り立たないが、他の場合について実際の計算により比較してみる。ユーザーが 100 人の場合、従来の配送方法では 99 個のピースを 100 回配送しなければならない。即ち、通信量は $9900k$ (bit) となる。一方、GKD 方式ではブロック鍵の配送が 500 回、それぞれのブロック鍵による同報配送が 600 回、個別配送が $1126k$ (bit) あるため、全部で $1216k$ (bit) となる。これから配送における通信量の比は

$$1216 / 9900 = 0.123 \quad (7)$$

となる。また、ブロック鍵の配送を除けば、GKD の配送に必要な通信量は 716 個のピースの

配送と等価になるので、通信量の比は

$$716 / 9900 = 0.072 \quad (8)$$

となる。

またここでは、ブロックの分割は2分割としているが、3分割や4分割等様々な分割方法が考えられるが、同報で配送するブロックの割合を最大にするような分割方法が通信効率を最大にするので、均等に2分割する方法が最も効率がよい。

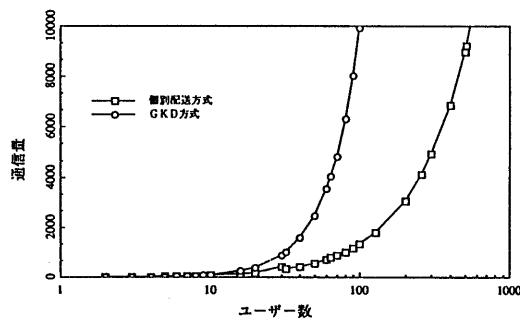


fig.5 ユーザー数の増加に伴う通信量の変化

この方法と個別にピースを配送する方法との通信効率を比較すると、fig.5に示すようにユーザー数が多くなるにつれてGKD方式では通信効率がよくなるということがわかる。

6. 結果

グループ同報秘密通信に適した鍵管理方式であるMCK方式の環境に適した、鍵生成子を同報により配送するGKD方式を提案した。この方式によりピース生成ノードの、配送によるオーバーヘッドをかなり低減できることが可能である。

今後の課題としては、共謀によるピースの露見をピースの保管法で以下に防ぐかというところであろう。

参考文献

- [1]Desmedt.Y., "Society and Group Oriented Cryptography: A New Concept", Lect Notes Comput Sci, 293, pp120-127, 1988.
- [2]高木和幸他,"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.
- [3]中村秀紀他,"ハイアラキー構造に適した鍵管理",情処件報 vol.90, No.45, 1990.
- [4]高木和幸他,"チーム指向型暗号方式",情処件報, vol.90, No.73, 1990.
- [5]中村秀紀他,"Hierarchical Group Oriented Key Management Method: HGK", Proceeding of 6th Comput Secure Appli Conf, p44-49, 1990.
- [6]高木和幸他,"Multiple Keys Generation Method for Controlling Access to information", Conf of ICCS '90, vol.1, pp212-215, 1990.
- [7]"Data Encryption Standard", FIPS PUB 46, National Buureau of Standards, Washington, D.C., 1977.
- [8]太田和夫,"効率の良い同報暗号通信", 信学技法, vol.87, No.12, pp43-48, 1987.
- [9]Shamir,A., "How to Share a Secret", Commun. ACM, Vol.22, No.11, pp.612-613, 1979.