

チーム指向型暗号方式

高木和幸 中村秀紀 岡田謙一 松下温
慶應義塾大学理工学部

暗号法は情報へのアクセス制御に用いることができる。これは、正しい鍵を持たないユーザは暗号化された情報を復号化できないからである。しかし、多くの人々と通信を行う場合に一人のユーザが多数の鍵を管理しなければならない。この論文では、暗号法によるアクセス制御の応用について述べる。我々は実際に作業が行われる場合の組織構造をモデル化して『チーム指向型構造』という典型的な組織構造を想定し、『ピース』と呼ばれる鍵生成子の組み合わせによる鍵の生成に基づくチーム指向型鍵管理方式（AGCK方式）を提案する。この方法は、チーム指向型構造において鍵管理の面から非常に優れていることを示す。

A Team Oriented Encryption Method

Kazuyuki Takagi, Hidenori Nakamura
Ken-ichi Okada, Yutaka Matsushita

Faculty of Science and Technology, Keio University
3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223, Japan

A cryptographic scheme can be used for controlling access to information, since any user who does not have a proper key can not decipher. But for this purpose, a user would have to manage a huge number of keys when he tries to communicate with a lot of people. The practical utilization method of access control by cryptography is discussed in this paper. We suppose a typical organization structure called the "Team Oriented Structure". After that, we propose a team oriented structure key management method (AGCK method) based on the multiple keys generated from the combination of "piece"s, which is equivalent to key generators, and describe that this method is very desirable in terms of reducing the numbers of keys required for each user in a team oriented structure structure.

1. はじめに

暗号法は、データの安全性、真実性、完全性を守るための方法であるが、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LAN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ヴァ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いふことができる。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。

そのような構造中において多くの人と秘密通信を行う立場の人は多くの鍵を持たなければならない。例えば階層構造中のより上層の人は莫大な数の鍵を管理することになる[1]。今、典型的な組織の通信における構造をチーム指向型構造とし、その構造において鍵管理の観点から非常に有効である鍵管理方式であるチーム指向型鍵管理方式（AGCK方式）を提案する。AGCK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た[2][3]。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。さらにこの方式において、ピースの数を最小にするために組織の構造に適したピースの配布法を提案する。最後に、通信効率、鍵の安全性、鍵更新の方法の面からコピー鍵方式

と比較し、AGCK方式が有効的な方法であることを示す。

2. チーム指向型構造モデル

あるグループ内においてその任意のメンバーによる様々な形態の、任意の個数構成される「チーム」というサブグループが存在するような構造を想定する。また、この構造内の任意のチームの中で行われる通信にすべてアクセスできるような非メンバーである「代表者(representative)」を想定し、代表者とメンバーによって構成される構造を「グループ」と定義する(fig.1)。

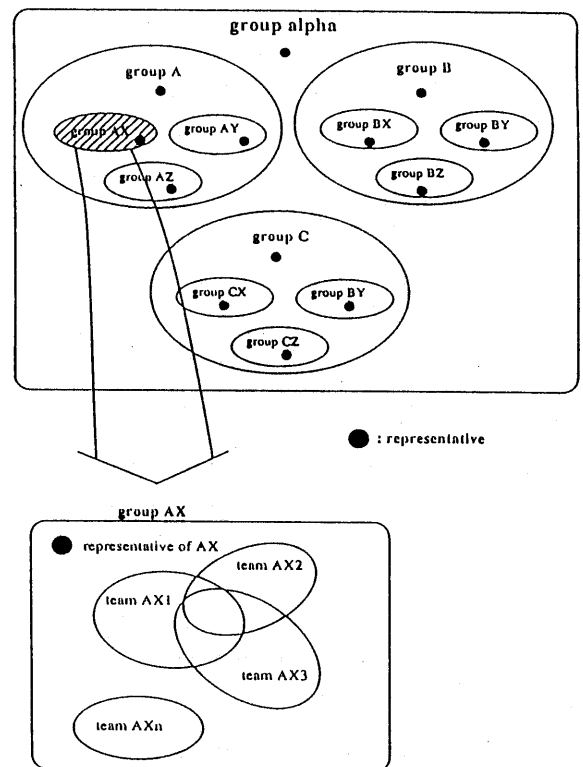


fig.1 a team oriented structure

チーム指向型構造内にはグループが複数存在し、各グループはレベルという属性値を持ち、同じレベルに存在するグループは1つのレイヤーを形成する。さらにあるレベルのレイヤーのグループの代表者は1層上層のグループのメンバーとしてグループを形成することができる。このように、チ

ーム指向型構造の全体は何層かのレイヤー構造とみなすことができる。

実際の組織において作業を行う場合、母集団に対してグループやチームを組んで作業をする人の枠はほぼ決まっているといってもよいであろう。この枠を「グループ」に対応させ、その中で組まれるグループを「チーム」に対応させているわけである。また、「代表者」はその枠内の代表者である上司やチームのリーダーに相当するわけである。

3. AGCK方式

(Advanced Generated Copy Key Method)

AGCK方式において、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「共通鍵」と鍵生成子である「ピース」を保持する。メンバーは通信に用いる通信鍵を、共通鍵とピースから生成する。

3.1 鍵生成法[2][3][4]

AGCK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 の独自の組から、独自の 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対応であれば独自のピースの組み合わせによって独自の鍵が生成される。

3.2 ピース分配法[3]

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.2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。なおそのグループの代表者にはそのグループ内で使用される全てのピースを分配する。さらに、グループが複数存在する場合は各グループは異なるピースの組を使用する。この方法は、グループのレイヤーが異なる場合にも適用される。

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ので合計 n 個の鍵に対する情報を持つことになる。また代表者については、一つ上層のレイヤーでメンバーになっている場合は、上層のレイヤーのメンバーの数を n' とすれば $n+n'-1$ 個のピースと2つの共通鍵を持ち全部で $n+n'+1$ 個の情報を、上層のレイヤーでメンバーになっていない場合は $n+1$ 個の情報を持つことになる(fig.3)。

	P_1	P_2	P_3	P_4	P_5	P_6	K
Representative	○	○	○	○	○	○	○
* M1		○	●	○	●	○	○
* M2	○		●	○	●	○	○
M3	○	○		○	○	○	○
* M4	○	○	●		●	○	○
M5	○	○	○	○		○	○
M6	○	○	○	○	○		○

Mi: Member i

Pi: Piece i

K: Common Key

*: A member of the team {m1, m2, m4}

●: A common piece for a team communication

○: A distributed piece

Fig.2 A piece distribution for a group.

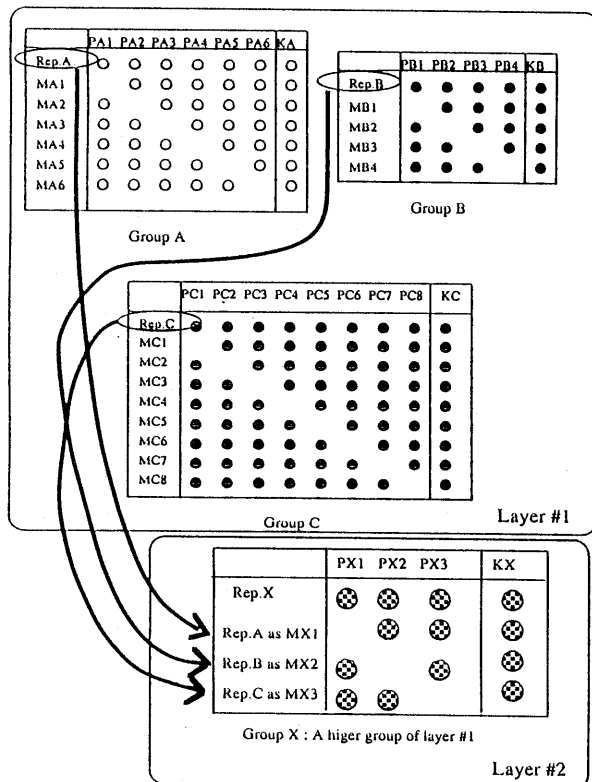


Fig.3 A team oriented piece distribution

3. 3 通信方法 [2][3][4]

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付加され、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かどうかを判定する。この構造中においては次の3つの通信形態が考えられ、それぞれにおける通信は次のように行われる。

(1) グループ同報通信

グループ同報通信は、グループ内の全てのメンバーに対する同報通信である。グループ内のメンバー全て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。

(2) チーム通信

チーム通信は何人かのメンバーで構成されるチーム内の同報通信である。チーム通信では、通信文はそのチーム内で共有されるピースと共通鍵 K によって生成される通信鍵によって暗号化される。例えば、fig.2 においてグループ内にメンバー M1, M2, M4, によって構成されるチーム内での通信は共通のピースである P3, P5, P6 と共通鍵 K によって式(3)に示されるように生成された鍵 K' を用いて行われる。

$$K' = f(f(f(K, P3), P4), P6) \quad (3)$$

(3) レイヤー間通信

あるレイヤーのメンバーとその上層のレイヤーにおけるメンバーが、下層のレイヤーの代表者を介して通信をする事ができる。これがレイヤー間通信である。下層のレイヤーのメンバーが上層のレイヤーに通信文を送る場合は、自分の持っている全てのピースを用いて生成した鍵によって通信文を暗号化して代表者に送る。代表者はヘッダにあるピース番号と宛先のアドレスにより、一度復号化した後に、上層レイヤーのピースで送り先に見合ったピースを用いて再び暗号化した後通信文を送る。上層から下層に送る場合も同様に上層のメンバーが送り先のメンバーのいるグループの代表者になっているメンバーに通信することによって可能となる。

4. 鍵の安全性

本論文では DES のような慣用暗号方式を、暗号化や復号化のために想定しており、ここでは暗号化アルゴリズム自体の安全性は考慮しないこととする [5]。また、表記 $K_{ij..n}$ は複数のピース $P_i, P_j, \dots, P_n$ と共通キー K から生成される通信鍵を表す。

4. 1 不正なメンバーからの攻撃

ピースは暗号化に直接に使用されないの

で、不正なメンバーがピースを手に入れることは困難である。そこで、不正なメンバーが複数の鍵を手に入れた場合の他の鍵の安全性が問題となる。式(2)の f は一方向関数であるので、 $K1$ も $K2$ も $K12$ から生成することは不可能である。よって一つの鍵が露見しても他の鍵の安全は保たれる [6]。

不正なメンバーが二つ以上の鍵を手に入れた場合、鍵生成に用いられたピースの通し番号からピースを手に入れることが可能である。例えば $K1$ と $K12$ が露見した場合、 $K1$ を平文とみなして $K12$ を暗号文とみなす既知平文攻撃によって、 $P2$ を手に入れることができる。しかし、この攻撃方法は全探索を必要とし、しかもピースの通し番号は共通鍵 K によって暗号化されているため容易に入手できない。従って二つ以上の鍵が露見した場合でも、他の鍵は安全である。

一方、共通鍵は頻繁に直接暗号化のために使われるので、システムの安全性を高めるためには定期的に取り替える必要がある。

4. 2 正規メンバーの攻撃

正規メンバーが自分自身のピースと通し番号を知っている場合には、ある鍵から他のピースを手に入れることが可能である。例えば $P1$ と $P2$ を持つ正規メンバが $K123$ を手にいれたとき、既知平文攻撃によって $P3$ を手に入れることが可能である。しかし、それには前述したように全探索が必要となるので、暗号文は正規メンバーの攻撃に対しても安全に保たれる。また下位メンバーが共謀して自分達の全てのピースを集めたとしても、上位メンバ間の通信を復号化することは不可能である。なぜならばレベル n メンバが上層メンバ宛ての通信文を暗号化するときには、下位レベルのメンバが保持しないレベル $n+1$ ピースを使用するからである。さらに、全てのピースを所有者にも不可視にすることによって鍵の安全性はより強化される。

5. 評価

5. 1 鍵数

A G C K方式においてピースのサイズは鍵のサイズと同様であるため、ピースの数を鍵の数とみなすことが可能である。ここでは、1つのグループにおいて、2人以上の任意の形態のチームが構成されるときに必要な鍵の総数を従来方式と比較する。グループ内にメンバーが n 人存在すると仮定すると、前述のように $n-1$ 個のピースと共通鍵が必要であるので、合計 n 個の情報が必要となる。これに対して従来方式であるコピー鍵方式をこの構造に適用した場合、

$$\sum_{r=2}^n n C_r = 2^n - 1 \quad (4)$$

$r=2$

個の情報が必要である。

5. 2 鍵の更新

システムを安全に保つために、鍵の更新が不可欠である。コピー鍵方式においては全ての鍵が更新されるが、全ての鍵の再分配には非常に手間がかかる。一方 A G C K方式においては、鍵の更新に二通りの方法が用意されている。一つは共通鍵 K だけを更新する方法である。共通鍵 K は全ての鍵生成に関わっているので、この方法を用いることによってシステム外部の人間に対して鍵を安全に保つことができ、しかも容易に実現できるために頻繁に実行することができる。ただしシステム内の人間に対しては効果がなく、共通鍵が盗まれても当然効果がなくなる。もう一つの方法は全てのピースを更新してしまう方法で、これによりシステムの外の人間及びシステム内の不正メンバに対して鍵を安全に保つことが可能である。この方法は共通鍵 K だけを更新する方法に比べると実現に手間がかかるため

に、より長期的な周期で実行するのが有効と思われる。このようにA G C K方式においては必要に応じて両者の方法を使い分けることができるということが大きなメリットとなる。

5. 2 通信効率

(1) 暗号文の長さ

コピー鍵方式とA G C K方式において、平文を暗号化するためには同じアルゴリズムが用いられるため、暗号文の長さは平文の長さと同様である。

(2) 計算回数

コピー鍵方式とA G C K方式の両方式において、平文を暗号化、復号化するためには同じ計算ステップを必要とするが、A G C K方式はピースから鍵を生成するために余分なステップを必要とする。このステップは3章1節に記述した関数 f に依存するが、鍵生成に用いられるピースのサイズは、通常通信文のサイズよりも十分に小さいので、適切な関数を用いることによって、この余分なステップ数が全体のステップ数にほとんど影響を与えないようにすることが可能である。

6. 結論

本論文で、我々はチーム指向通信のためのA G C K方式を提案した。この方式を用いることにより、現実に広く存在するような通信形態に即したアクセスコントロールが実現でき、各ユーザが管理しなければならない鍵の数を減らすことが可能である。この効果は、ユーザの数が多い状態や、グループ構造がレイヤー構造のような形態を持っているときに著しくなる。また、通信効率や鍵の安全性に関しても従来方式より有利であり、総合的にみてもA G C K方式は非常に優れていると言える。

参考文献

- [1]Desmedt,Y., "SOCIETY AND GROUP ORIENTED CRYPTOGRAPHY: A NEW CONCEPT", Lect Notes Comput Sci,293, pp120-127,1988.
- [2]関口絵美子他、"階層構造における鍵管理法" 情報処理学会第40回全国大会,1990.
- [3]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.
- [4]中村秀紀他、"ハイアラキー構造に適した鍵管理方式" 情処研報 vol.90,No45,1990.
- [5]"Data Encryption Standard",FIPS PUB 46, National Bureau of Standards, Washington,D.C.,1977.
- [6]太田和夫、"効率の良い同報暗号通信" 信学技法、Vol.87,No.12 pp.43-48,1987
- [7]Akl,S.G.and Taylor,P.D., "Cryptographic Solution to a Problem of Access Control in a Hierarchy", ACM Trans.Comput.Syst.,Vol.1, No.3, pp.239-248,Aug,1983.
- [8]Mackinnon,S.J.,Taylor,P.D.,Meijer.H.and Akl, S.G., "An Optimal Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy",IEEE Trans.Comput., Vol.C-34,No9, pp.797-802,Sept,1985.
- [9]Shamir,A., "How to Share a Secret", Commun. ACM,Vol.22,NO.11,pp.612-613, Nov,1979.