3Q－2

階層構造における鍵管理法

関口　絵美子，中村　秀紀，岡田　謙一，松下　温

（慶応義塾大学　理工学部）

１．はじめに

現代の社会には、政府機関、企業等、多くの組織上の階層構造が見られる。その中で、上司は部下達が持つ情報を知る事ができるが、部下は上司から監視されるだけで、上司達が持つ情報を通常知る事はできない。現在、階層構造専用の暗号方式はなく、個別通信の暗号方式を拡張しているにすぎないが、ユーザが保持する鍵の数が多い等、鍵管理の面で問題があった。そこで本論文では、階層構造をしたネットワークでの暗号通信に用いる、鍵の新しい管理方法について述べる。

２．階層鍵生成方式

鍵は、漏洩、紛失等が起これば、盗聴される危険性があるので、鍵管理は暗号の中で非常に重要である。鍵の安全保管の１つの方法として、分割保管がある。ここで提案する階層鍵生成方式はラグランジュ補間多項式[1]に基づいて、鍵を分割保管する方法である。

次のような任意の(t-1)次多項式を与える。

$$h(x)=(a_0+a_1x+\cdots+a_{t-1}x^{t-1}) \pmod p$$

（ただしｐは大きな素数）…(1)

(1)式で表される曲線上に点をばらまき、それをピースＤと名付ける。

$$D_i=h(x_i) \quad (i=1,2,\cdots) \quad \cdots(2)$$

（ただし、$x_1<x_2<\cdots$）

ピースｎ個（ｎ＜ｔ）を任意に選び出し、座標上のそれらｎ点をつないでできる(n-1)次の曲線g(x)が、ラグランジュ補間多項式より次のように求まる。

$$g(x)=\sum_{s=1}^{n} D_s \prod_{\substack{j=1\\ j\neq s}}^{n} \frac{x-x_j}{x_s-x_j} \pmod p \quad \cdots(3)$$

定数値g(0)の値を暗号化、復号化の時に用いる鍵Ｋとする（fig.１）。

$$K=g(0)=\sum_{s=1}^{n} D_s \prod_{\substack{j=1\\ j\neq s}}^{n} \frac{x_j}{x_j-x_s} \pmod p \quad \cdots(4)$$

fig.１のK_{123}を使ってかけた暗号文は、ピースD_1、D_2、D_3を持つユーザだけが読め、２つしかピースを持たないユーザには読めない。

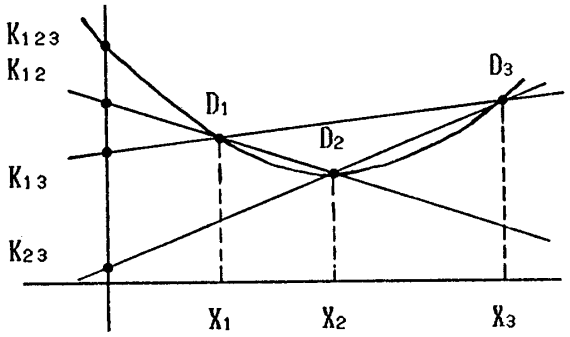

fig.１　ラグランジュ補間方式

これを階層構造に応用するには、ユーザが持つピースの種類と数を階層ごとに変えて、例えばfig.２のようにすればよいのである。ユーザU_1は、部下U_2、U_3、U_4がかけた暗号文は全て読めるが、ユーザU_2、U_3、U_4は　上司U_1の暗号文は読めないことになる。

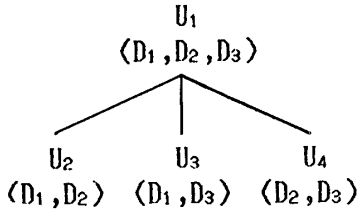

fig.２　階層構造

３．ピースの配布方法

fig.２のような階層構造にするには、どのようにピースを各ユーザに配布すればよいのかを述べる。

ピースは必ず２個の組み合わせを最小単位とする。ピース１個では、そのピース自体が鍵となり、安全性が低くなるからである。

階層構造の基本単位、２層の場合を考える。最下層でのピース２個の組合わせを効率良く使い、第２層の人が所持するピース数をなるべく少なくすることを考えると、枝の数ｋは

$$k={}_mC_2 \quad (m=3,4,\cdots) \quad \cdots(5)$$

とすればよいことになる。

ｋは、ユーザが適用する階層構造の形態の特徴（段数が多いのか、或は段数は少ないが下層に広がっているのか等）に合わせて決めれば、いろいろな階層構造に対応できる。

fig.３にｋ＝３の場合の例を示す。

A key management scheme in a hierarchical structure

Emiko SEKIGUCHI,Hidenori NAKAMURA,Ken-ichi OKADA,Yutaka MATSUSHITA

Keio University

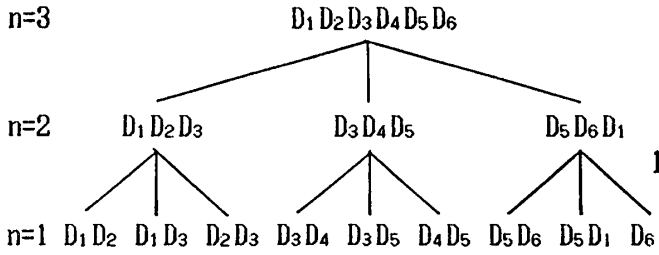

fig.3　k=3の場合の階層構造の例

4．システム概要と安全性

ピースの管理は、fig.4のように集中管理法を用いる。ピースは各ユーザが保管し、ピース番号は知ることができても、ピース自体を知ったり、直接手を加えたりできないような環境に設定する。そしてピース番号リスト（誰が何番のピースを持っているのか）をピース番号管理センターで管理する。

・上司→部下へ送信する場合

上司は、送りたい部下の中で最下層の部下が持つピース番号をセンターに問い合わせ、そのピースを用いて、鍵を生成し、暗号化する。部下達はヘッダのピース番号を見て鍵を生成し、受信した電文を復号化する。

・部下→上司へ送信する場合

部下が持っているピースは上司も持っているので、部下は自分のピースで鍵を生成し、暗号化する。受信した上司は、ヘッダのピース番号を見て鍵を生成し、電文を復号化する。

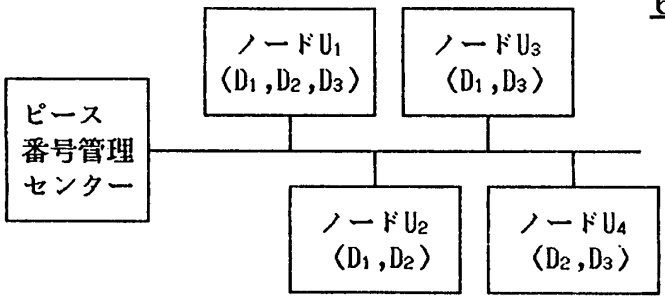

fig.4　ピース番号管理センター

同階層への通信は、階層ではなく、グループとなるのでこの方式では通信できない[2]。

この方式の安全性は、ピースの完全な秘密保管にかかってくる。鍵が生成されれば、暗号化は慣用的な方法（例えばＤＥＳ[3]）で行うので、まず安全と言ってよいだろう。ピースの中味さえわからないような環境を設定すれば、下層が共謀したり、鍵が盗まれても、わかるのはピース番号のみで、鍵を生成することはできず、被害は最小にできる。

5．評価

階層構造ネットワークにおける通信は、同報通信におけるグループ間通信に上層から下層へという方向性を持たせた特殊な例である。同報通信で最も一般的なコピー鍵方式[4]と本論文で提案する階層鍵生成方式とを、fig.3のような階層構造ネットワークに適用した場合について比較検討する。

1)鍵（ピース）所持数

コピー鍵方式の場合、自分が属するグループの数が所持する鍵の数になる。階層構造では縦割りのグループとなり、第ｎ段の人が所持する鍵の数は、

$$\frac{1}{2}\left(3^n-3\right)$$

となる。階層鍵生成方式の場合、第ｎ段の人が所持するピース数はfig.3より、

$$\begin{cases} 2 & (n=1) \\ \frac{1}{2}\left(3^{n-1}+3\right) & (n\geq 2) \end{cases}$$

で、ｎ≧２となれば、階層鍵生成方式の方が所持するものが少なく（ｎ＝３の時、鍵は１２、ピースだと６）、しかも所持しているのは鍵ではなくピースなので、安全性が高いことになる。

2)メッセージ長

共に｜暗号文｜＝｜平文｜である。

3)処理時間・伝送効率

鍵を生成する分、階層鍵生成方式の方が時間がかかるが、鍵ができてしまえば伝送効率は同程度である。

6．おわりに

この管理方式はまだ理論の段階にすぎないので、今後はこれを実際にハード化して検討する必要がある。また、この方法では認証ができないという問題がある。

参考文献

[1] Samir,A., "How to Share a Secret", Comm.ACM,Vol.22(11),pp.612-613(1979).

[2] 高木，南部，岡田，松下，"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] "Data Encryption Standard", FIPS.PUB 46,National Bureau of Standards,Washington,DC.(1977).

[4] Kent,S.J., "Security Requirement and Protocols for a Broadcast Scenario", IEEE Trans. Commun.,COM-29,6, pp.778-786(1981).