新しいグループ指向鍵管理方式

3Q－1

高木　和幸，南部　峰秀，岡田　謙一，松下　温

慶應義塾大学　理工学部

１．はじめに

昨今，ＬＡＮや衛星通信を利用したネットワークなど、同報機能を備えるネットワークが注目されている[1]。このようなネットワーク上で秘密通信を行なう場合においては暗号が用いられる。現在、最もよく用いられている同報暗号通信方式はコピー鍵方式[2]であるが、この方式は通信性能が優れている反面、ユーザの保持する鍵の数、鍵配布の煩雑さ、グループ構造の変化に対する柔軟さなど鍵管理の面に問題があった。そこで我々は、この問題を解決するために、１つの共通な鍵より複数の鍵を生成するＧＣＫ（Generating Copy Key）方式を用いた、グループの構造変化に柔軟に対応できるグループ指向鍵管理方式を提案する。

２．ＧＣＫ方式

２．１ コピー鍵方式の概要とその問題点[3],[4]

コピー鍵方式は、従来の個別暗号通信を単純に同報通信に拡張したものであり、グループに属するユーザは、コピー鍵と呼ばれるそのグループ間通信専用の鍵を保持し、その鍵によって暗号化、復号化の処理を行なう。この方式では、１つの平文を１種類の鍵で暗号化するので、同報暗号文のデータ長は、平文のデータ長と等しくなる。また暗号化の処理は、平文のデータ長に依存し、グループのメンバー数には無関係である。しかし、各ユーザは自分の属するグループの数だけ鍵を管理する必要があり、また、鍵を更新する場合や、グループ構造が変化した場合に、新しい鍵の配布が煩雑であった。

２．２ ＧＣＫ方式における鍵の生成法

我々の提案する方式では、以下のようにして、ある鍵Ｋを入力の一つとして実際の通信に用いる鍵Ｋ'を生成する。

$$K' = f(K, I) \qquad (1)$$

ここで、関数ｆは、ＫとＩによりＫ'を生成する一方向関数または暗号化関数である。さらに異なるＫ、Ｉに対して異なるＫ'が生成できるように、Ｋ空間からＫ'空間への変換は、１対１対応もしくは著しい退化がないことが必要である。また、Ｉは鍵を生成するための情報（ＩＫＧ: Information for Key Generation）であり、関数ｆを暗号化関数とみなした場合の暗号鍵に相当するものとなる。

複数のＩＫＧ、$I_1, I_2, \cdots, I_1$により鍵を生成する場合は、次のように関数ｆを多重に用いる。

$$K' = f(\cdots f(f(K, I_1), I_2), \cdots, I_1) \qquad (2)$$

上記のような鍵の生成法を用いることにより、１個の鍵とＩＫＧにより複数の鍵を生成することができる。１個の鍵とｎ個のＩＫＧより生成される鍵の総数は、ｎ個のＩＫＧから$1 \leqq r \leqq n$をみたすｒ個を選ぶ組み合わせの総数に等しいので、次式のようになる。

$$\sum_{r=1}^{n} {}_nC_r = 2^n - 1 \qquad (3)$$

よって、ユーザは１個の鍵とｎ個のＩＫＧを管理することによって、合計2^n個の鍵を管理することができる。

２．３ ＩＫＧの分配法

多くのグループが形成され、各ユーザは、複数のグループに属しているようなネットワークを考える。同報通信は、グループ内のメンバーで行われる。ネットワーク上にｎ人のユーザが存在する場合、ＩＫＧを次のように分配する。まず、ｎ個のＩＫＧ（$I_1, I_2, \cdots, I_n$）を用意し、ｎ－１個づつの互いに異なる組み合わせに分ける。各ユーザは、共通な鍵K_0と前述のように分けられたｎ－１個のＩＫＧの組み合わせの１つを保持する。ここで、ユーザU_iとU_jが共通に持つＩＫＧを考えると、そのようなＩＫＧはｎ－２個存在し、この組み合わせは、ｉ，ｊによって一意に決まる。メンバー数ｍのグループでは、メンバーであるユーザが共通に持つＩＫＧはｎ－ｍ個であり、メンバー以外のユーザはこれらの共通するＩＫＧの全てを持ってはいない。図１にｎ＝５の例を示すが、グループ$\{U_1, U_3, U_4\}$のメンバーであるU_1，U_3，U_4はI_1，I_4を共通に保持するが、メンバーでないU_2，U_5は、それらのいずれか１個しか持っていない。

	I_1	I_2	I_3	I_4	I_5	K_0
＊U_1	●	○	○	●		○
U_2	○	○	○		○	○
＊U_3	●	○		●	○	○
＊U_4	●		○	●	○	○
U_5		○	○	○	○	○

＊：グループ$\{U_1, U_3, U_4\}$のメンバー
○：分配されているＩＫＧ，または共通キー
●：グループ内で共通のＩＫＧ

図１　ＩＫＧの分配法（ｎ＝５の場合の例）

このようなグループのメンバーが共通に持つＩＫＧを用いて共通の鍵K_0より生成した鍵をそのグループの鍵として使用すれば、グループ内での秘密同報通信が可能となる。なお、全ユーザが共通に持つＩＫＧは存在しないため、全同報を行うためには、K_0をそのまま鍵として使用する。また、暗号文にはどのＩＫＧを用いて、暗号に用いた鍵Ｋ'を生成したかわかるように、ＩＫＧを管理する通し番号ｉが、通信文のヘッダーに付加される。

図１におけるグループ$\{U_1, U_3, U_4\}$のグループ鍵K_{134}の生成法の例を次に挙げる。I_1とI_4が共通のＩＫＧであるので（４）式のようになる。

$$K_{134} = f(f(K_0, I_1), I_4) \qquad (4)$$

以上の説明のように、我々が提案するＧＣＫ方式を用いることによって、ｎ人のユーザがネットワーク上に存在する環境で、各ユーザは、１個の共通鍵K_0とｎ－１個のＩＫＧを管理するだけで、１対１通信も含むあらゆるグループ内同報通信を行うことができる。

A new method of keys management for group oriented structure
Kazuyuki TAKAGI, Mineki NANBU, Kenichi OKADA, Yutaka MATSUSHITA
Keio University

3．評価

3．1 鍵の安全性

ここでの鍵の安全性とは、全探索などによりある鍵が露見した場合に、他の鍵が安全であるかどうかを示す。これについては、2．2で述べたように鍵を生成するための関数fには、一方向関数が用いられるために、たとえ攻撃者がある鍵K'を手にいれても、同時にIKGも入手することができなければ、その鍵K'を生成した鍵K、あるいはその鍵より生成され得る鍵K"を知ることは不可能である。さらには、2個以上の鍵を手にいれたとしても、それらの鍵を生成するために用いられたIKGを推測することも容易ではない。安全性について唯一つ注意しなければならないのは正規ユーザの共謀による攻撃である。2．3で示したIKGの分配方法では、正規ユーザが2人以上共謀することによって、共通鍵K_0と全てのIKGを入手することができ、その結果全ての鍵を生成できることになる。よって、このような可能性を考慮するならば、IKGは正規ユーザにも直接ふれることができないような環境にする必要がある。

3．2 鍵管理

ネットワークの利用形態としてグループ通信だけでの利用ということは希であり、一般には個別通信とグループ内同報通信の両形態で利用される。よって、以下の鍵管理は個別通信をサポートしたグループ内同報通信について評価することにする。

（1）保持鍵数

GCK方式では、個別通信はメンバー数2のグループ内同報通信として扱われる。鍵生成のための関数fを暗号関数とすると、IKGは暗号化の鍵に相当するものになる。よって、1個の鍵とn－1個のIKGを保持することはn個の鍵を保持することと同様である。

一方、従来のコピー鍵方式では、α個のグループ（ただし、$0 \leq \alpha \leq 2^{n-1}-n-2$）に属するユーザが保持しなければならない鍵の数は、個別通信もサポートする場合にはn＋α－1個となる。よって、$\alpha \geq 2$となるとき、GCK方式の方が保持鍵数は少なくなる。

（2）鍵の更新について

安全性の面から考え、鍵の更新は頻繁に行わなければならない。従来のコピー鍵方式では、グループごとに鍵が存在するため、鍵更新時の鍵の配送が煩雑であった。しかし、GCK方式では、共通鍵を更新すれば、全ての鍵を更新することになるので、鍵の更新は非常に簡単である。

（3）グループ構造の変化に対する柔軟性

ネットワークにおいて、グループのメンバー数が増減したり、新しいグループが構成されることは良くあることである。従来のコピー鍵方式では、それらのグループ構造の変化に対して新しい鍵を配送するなどの必要があり、柔軟に対処することができなかったが、GCK方式ではこのような必要は全くなく、1個の共通鍵とn－1個のIKGによって全てのグループ内通信が可能である。

3．3 通信性能

（1）暗号文のデータ長

GCK方式では、暗号化の処理法は従来のコピー鍵方式と同じであるから、両方式とも一度に処理される暗号文のデータ長は、暗号化の鍵のデータ長と等しくなる。

（2）処理時間

メッセージMを暗号化、または復号化する際の処理時間をGCK方式とコピー鍵方式において比較してみる。両方式とも暗号化処理にはDES[5]で代表される慣用暗号系を用いるものとし、また、GCK方式の関数fにもその暗号系を使用するものとする。ここで、

$$M = k \cdot |K| \qquad (5)$$

（$|K|$：1度に処理されるブロック長、
または、鍵Kのビット長，
k：ブロック数　）

とし、それぞれの方式の鍵の処理時間を演算回数で表すとすると、コピー鍵方式の演算回数V_cは既知のように

$$V_c = 3 \cdot k \cdot \log|K| \qquad (6)$$

となる。一方、GCK方式では演算回数V_gは、

$$V_g = 3 \cdot k \cdot \log|K| + 3 \cdot b \cdot \log|IKG|$$
$$= 3 \cdot (k+b) \cdot \log|K| \qquad (7)$$

ただし、b：多重度（＝n－m）
$|IKG|$：IKGのビット長

となり、V_cと比較して、鍵生成のための処理時間が余分にかかることになる。しかし、一般の通信ではk》bであることを考えると、鍵生成のための処理時間は無視できる程度のものだと考えられる。

4．まとめ

我々は、将来普及するであろう同報機能を持ったネットワークに注目し、同報通信での秘密保護対策として実用化されているコピー鍵方式を発展させ、同方式で問題となっていた鍵管理の面を改良したGCK方式を提案した。この方式は、共通鍵からIKGを用いて複数の鍵を生成するもので、以下のような利点を持つ。

（1）グループの構造変化に対して非常に柔軟に対処できる。

（2）各ユーザは、1個の共通鍵とn－1個のIKGを保持するだけで、全てのグループ内同報通信が行える。

（3）鍵更新は、共通鍵を変更するだけでよい。

（4）通信性能は、従来のコピー鍵方式と同程度である。

今後の課題は、正規ユーザの共謀による攻撃に対する、容易な対処法を確立することであろう。

参考文献

[1] 関口,中村,岡田,松下,:"階層構造における鍵管理法",情報処理学会第40回大会,(1990).

[2] S.J.Kent,:"Security requirements and protocols for a broadcast scenario",IEEE Trans. Commun., COM-29, 6, pp.778-786,(1981).

[3] 小山　謙二,:"マスター鍵による同報通信の暗号方式",信学会(D),J65-D-9,pp1151-1158,(1982).

[4] 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,(IN87-8),(1987).

[5] "Data Encryption Standard",FIPS PUB 46,National Bureau of Standards,Washington,D.C., (Jan. 1977).