第10卷 第1期 华东交通大学学报 Vol. 10 No. 1
1993年 3月 Journal of East China Jiaotong University Mar. 1993

# 一种大规模计算机安全网络的密钥管理规程

## ——分群式密钥管理系统

杨列亮 聂 涛

（电气工程系） （北方交通大学）

**摘 要**

任何一种用密钥控制的加密，都存在着密钥管理问题。在具有很强的密码算法的时候，保密系统的安全性主要取决于对密钥的管理。因此在计算机安全网中，设立一种好的密钥管理规程是至关重要的。本文讨论一种可能的密钥管理方式，可以支持大规模计算机安全网之间的通信。

**关键词**：加密；解密；密钥管理；通信会期

## 1 概 述

分群式密钥管理系统是将大规模计算机安全网络进行分割，形成一个由较小的计算机网络组成的安全网。设整个安全网络为一个群，较小的计算机网络称为它的子群。在子群里的计算机按IBM规程进行保密通信。而且所有子群里的计算机集中于一台叫做中继计算机的计算机。中继计算机又叫中继站。它负责和别的中继站建立联系，为子群里的计算机选择一条和别的计算机相连的通路。每个子群设立一个中继站。基本结构如图1所示。其中H代表主机。

在这种分割成子群的情况下，每个子群里的任何一台主机只要存储2N（设子群里共有N台主机）个二级通信钥。而不必考虑非本子群主机的情况。主机——主机之间通过公开算法建立联系。

## 2 主要密码操作

- 在主机主控钥下加密：

  EMK：{Key} $\longrightarrow E_{KM_0}$ (Key)

- 加密数据：

  ECPH：{$E_{KM_0}$ (KS)，data} $\longrightarrow E_{KS}$ (data)

本文于1992年5月20日收到

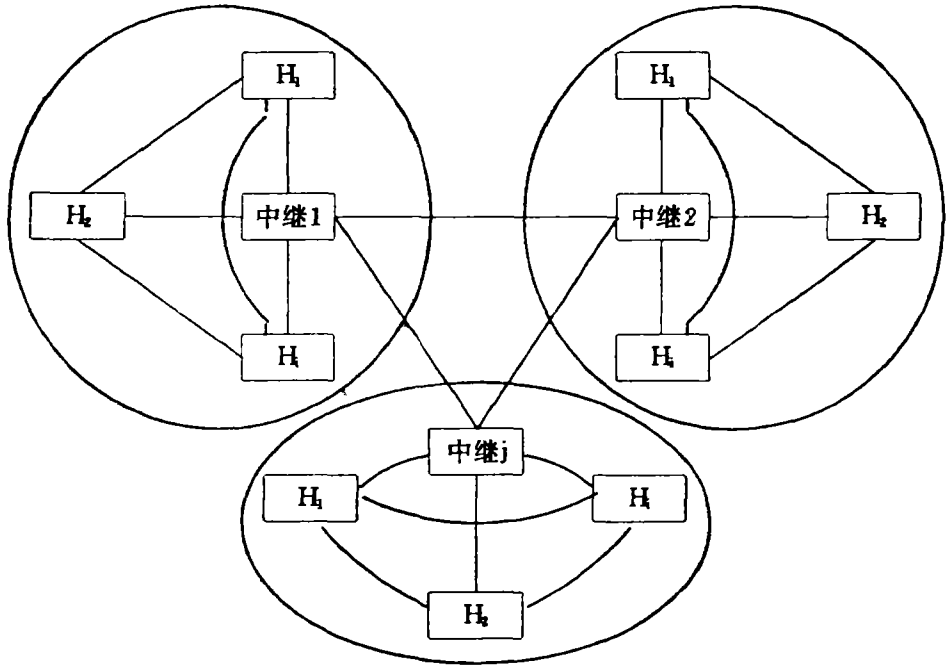


图1 分群式密钥管理系统的基本结构

·解密数据：

DCPH：$\{E_{KM0}(KS), E_{KS}(data)\} \longrightarrow data$

·脱密后再加密：

RFMK：$\{E_{KM1}(KMT), E_{KM0}(KS)\} \longrightarrow E_{KMT}(KS)$

·回到主密钥再加密：

RTMK：$\{E_{KM2}(KNC_i), E_{KNC_{ij}}(KS)\} \longrightarrow E_{KM0}(KS)$

本文中由于存在着公开密钥算法与DES（数据加密标准）算法之间的转换，故定义另外两个密码操作：

·转换操作1：

EXMK1：$\{E_{KM0}(x)\} \longrightarrow E_{KM1}((X^e \cdot ID)^r \bmod n)$

·转换操作2：

EXMK2：$\{E_{KM0}(x)\} \longrightarrow E_{KM2}((X^e \cdot ID)^r \bmod n)$

上述两个转换操作中，EXMK1是主叫方操作（发信方操作）；EXMK2是被叫方操作（受信方操作）。这两个操作在密码设施里实现的情况如图2所示：

## 3 系统算法选择与密钥分配

为了减少可信任节点的设置，而且使会期密钥尽量少地进行密码操作，本文提出一种方案，使中继站只负责控制建立主机——主机之间的联系。由于不同子群里的主机——主机之间不存在二级通信钥。必须建立一种方案使得主机——主机之间建立会期而又不影响其安全

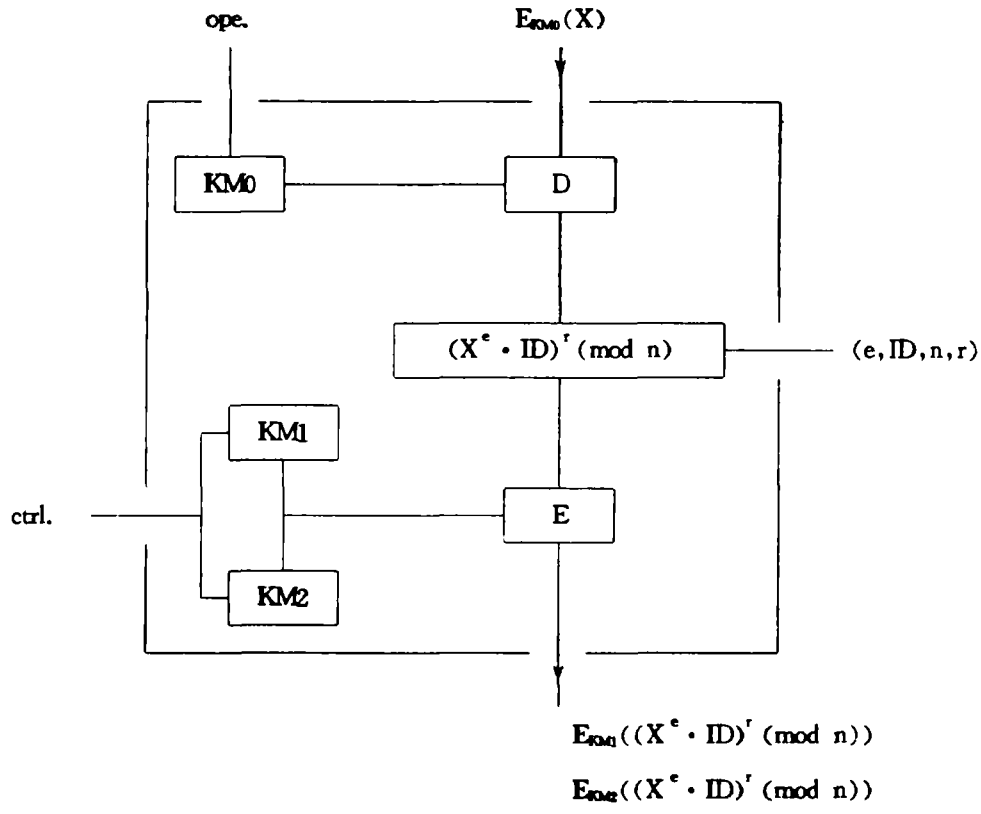


图2　EXMK1，EXMK2操作的密码设施

强度。本方案采用在每台主机里设置公开算法，而终端和中继站里只设置 DES 算法。终端里只设置DES 算法，这样选择的原因是由于公开算法便于验证对方的身份，而 DES 算法计算速度快，便于数据处理。

分群式密钥管理系统采用分散与集中相结合的方式，除主机主控钥 KM0 以明码形式存储在主机里的密码设施里之外，其它任何密钥不得以明码形式存储和传输。在各个子群里，由于它们采用 IBM 规程进行通信会期，所以每台主机必须按 IBM 规程的密钥分配方案进行密钥分配。每个终端存储有终端主控钥(KMT)。这个密钥用于将主机送来的会期密钥变成明码，以便和别的终端建立会期。所有的终端主密钥在自己的主机里以 $E_{KM1}$ (KMT) 方式存储。每台主机必须存储有和所在子群里的主机建立会期的二级通信钥。另外，主机里存储有进行公开密钥密码算法的 n，g，e（意义见 4）。中继站里的主机主控钥以明码形式存储在密码设施里，同时也存储有和子群里主机及别的中继站进行通信的二级通信钥。中继站里存储有所在子群中所有主机的身份标志。它们在系统中的分配情况详见图 3。

在这个系统中，每台主机具有自己的身份和所在子群的特性，记作 $IDH_{ij}$。而每个终端具有自己的身份和所在主机的标志，记作 $IDT_{ijk}$。这些标志可以根据码字的设置来实现。

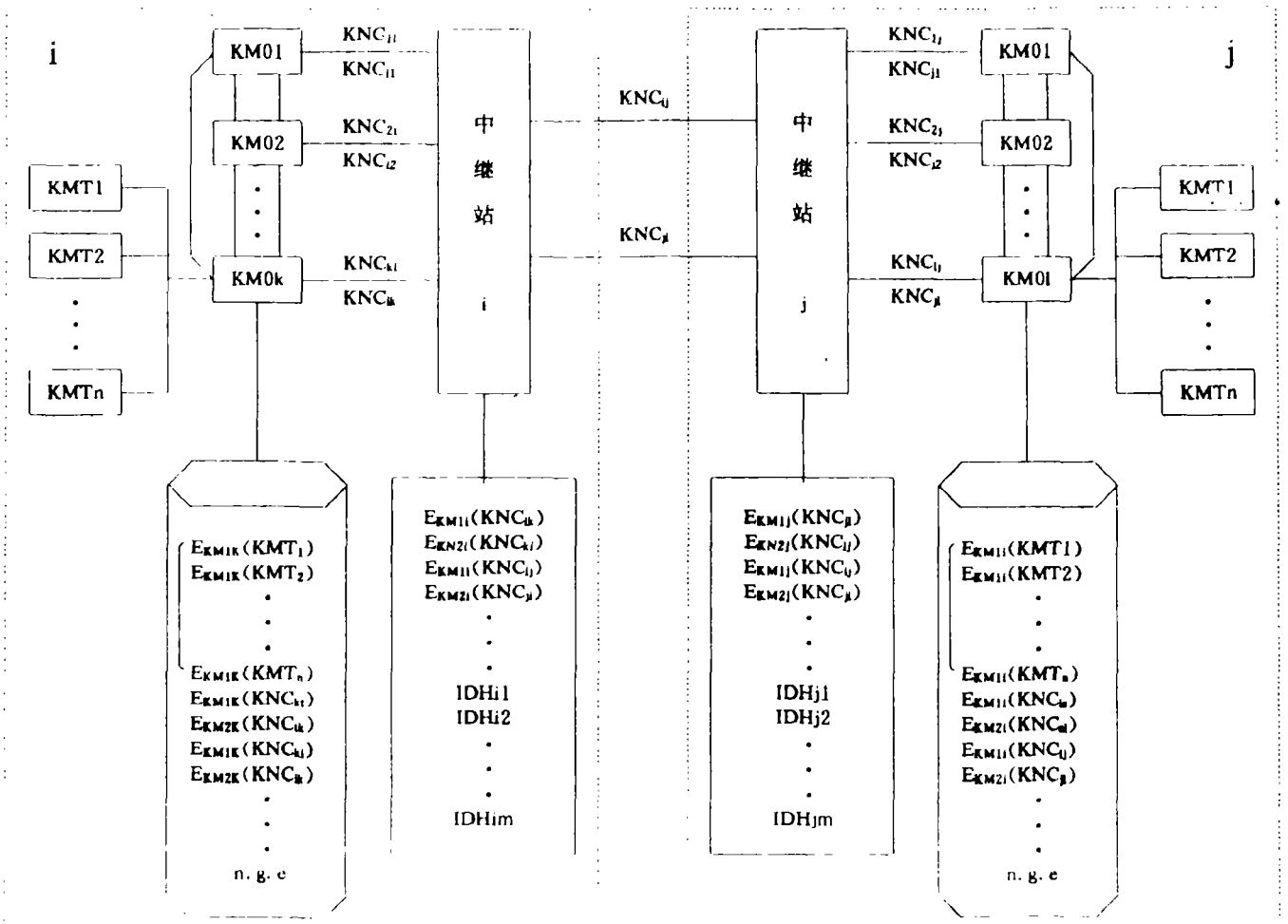


图3 i,j子群的密钥分配原理图

## 4 主机间公开算法的设置

主机里的公开算法根据下面原则设置：

1. 由系统安装人员（或专门人员）选择两个大素数 p 和 q，n=p·q。并确定素数 e 和整数 d，使它们满足：

$$e \cdot d(mod(p-1)(q-1)) \equiv 1 \qquad (e,d < n) \tag{1}$$

另外再选择一整数 g，g 是 GF（p）和 GF（q）中的本原元。对于用户 i，其身份标志为 $ID_i$，专门人员计算

$$S_i = ID_i^{-d}(modn) \qquad (i = 1,2,\cdots) \tag{2}$$

并将（n，g，e，$s_i$）通过秘密形式传送给主机 i。其中 $S_i$ 只有主机 i 知道，而 n，g，e 都是公开的，每台主机都存有它。d 对于任何用户都是保密的。当整个系统安装好后，消去 d。

由等式（1）和（2）可推知：

$$Si^e \cdot ID_i(modn) \equiv 1 \tag{3}$$

在通信阶段，当用户 A 和用户 B 想建立会期时，用户 A 产生一随机数 $r_i$，用户 B 产生一随机数 $r_j$。用户 A 和用户 B 分别进行下面计算：

$$X_A = S_A \cdot g^{r_i} \quad (modn) \tag{4}$$

$$X_B = S_B \cdot g^{r_i} \quad (modn) \tag{5}$$

然后用户 A 将 $X_A$ 传送给用户 B，同时用户 B 将 $X_B$ 传送给用户 A。这样用户 A 和用户 B 之间的通信会期密钥可以按如下方式产生：

$$WK_A = (X_B^e \cdot ID_B)^{r_i} \qquad (modn) \tag{6}$$

$$WK_B = (X_A^e \cdot ID_A)^{r_i} \qquad (modn) \tag{7}$$

下面证明 $WK_A = WK_B$。

将（4）、（5）两式分别代入（6）、（7）两式得：

$$WK_A = ((S_B \cdot g^{r_j})^e \cdot ID_B)^{r_i} \qquad (modn)$$

$$WK_B = ((S_A \cdot g^{r_j})^e \cdot ID_A)^{r_i} \qquad (modn)$$

所以：

$$WK_A = g^{er_ir_j}(S_B^e \cdot ID_B)^{r_i}$$

$$= g^{er_ir_j} \qquad (modn)$$

$$WK_B = g^{er_ir_j}(S_A^e \cdot ID_A)^{r_j}$$

$$= g^{er_ir_j} \qquad (modn)$$

故 $WK_A = WK_B$ (modn)

在分群式密钥管理系统中，就是利用 $WK_A$，$WK_B$ 在两台主机间传送密钥的。在这个系统中，只有主机 A 和主机 B 能产生这两个加密钥，其它任何节点即便知道 $X_A$、$X_B$ 也无法算出 $WK_A$ 和 $WK_B$。从上面建立的过程还可以知道主机 A 和主机 B 能彼此确定对方的身份。

## 5 通信安全会期建立过程协议

为了叙述方便，设所有计算机组成的网络被分成 M 个子群；每个子群里有 m 台主机；每

台主机有n个终端。设i子群里有一终端要求和j子群里的另一终端建立会期，会期密钥为KS，在这里抽出i、j子群，示意它们的密钥分配，来说明建立会期的过程。密钥分配图如图3所示。

每一子群里所有主机的身份标志存储在中继站里。如果第i子群中的k主机的t终端（记作$KMT_{ikt}$）要求和j子群中第l主机的s终端（记作$KMT_{jls}$）建立会期。设终端的身份标志分别为$IDT_{kt}$，$IDT_{ls}$，主机的标志分别为$IDH_{ik}$，$IDH_{jl}$。建立会期的过程如下：

(1) 一旦主机k收到它的一个终端t要求建立会期的请求，在主机$KMO_{ik}$处产生一伪随机数（RN），定义：

$$(RN) = E_{KMO_{ik}}(KS)$$

终端送入主机的信息有自己的身份标志，被呼叫终端的标志和被呼叫终端所在主机的标志。

(2) 主机k进行RFMK操作：

$$RFMK: \{E_{KMO_{ik}}(KS),\ E_{KMI_{ik}}(KMT_t)\} \rightarrow E_{KMT_t}(KS)$$

并将它送往请求会期的终端t。

(3) 在终端t处进行解密操作：

$$DMK: \{KMT_t,\ E_{KMT_t}(KS)\} \rightarrow KS,$$

KS用于建立会期。

(4) 主机k对被请求终端所在主机的身份标志进行鉴别，如果发现两终端是同一子群里的两个终端，则它们之间采用IBM规程帮助建立会期（参考[1]）。否则，如果发现双方非同一子群，则主机k要求出中继。主机k将对方子群j及主机l的标志告诉中继站i。中继站i和中继站j共同作用，使主机k和主机l相连。

(5) 一旦主机k和主机l连接好后，主机k产生一随机数$r_k$，计算：

$$X_k = S_k \cdot g^{r_k} \quad (mod n)$$

同时主机l也产生一随机数$r_l$，计算：

$$X_l = S_l \cdot g^{r_l} \quad (mod n)$$

为了将$X_k$送给主机l，$X_l$送给主机k，需要进行一系列操作。这里仅就$X_k$从主机k至主机l作详细介绍。而$x_l$由主机l至主机k的情况类同。

1° $EMK: \{X_k\} \rightarrow E_{KM0k}(X_k)$

2° $RFMK: \{E_{KM0_{ik}}(X_k),\ E_{KM1_{ik}}(KNC_{ki})\} \rightarrow E_{KNC_{ki}}(X_k)$ 主机k将$E_{KNC_{ki}}(X_k)$送给中继站i。

3° $RTMK: \{E_{KM2_{ij}}(KNC_{ki}),\ E_{KNC_{ki}}(X_k)\} \rightarrow E_{KM0_{ij}}(X_k)$

4° $RFMK: \{E_{KM0_{ij}}(X_k),\ E_{KM1_{ij}}(KNC_{ij})\} \rightarrow E_{KNC_{ij}}(X_k)$ 中继站i将$E_{KNC_{ij}}(X_k)$送给中继站j。

5° $RTMK: \{E_{KM2_{ij}}(KNC_{ij}),\ E_{KNC_{ij}}(X_k)\} \rightarrow E_{KM0_{ij}}(X_k)$

6° $RFMK: \{E_{KM0_{ij}}(X_k),\ E_{KM1_{ij}}(KNC_{jl})\} \rightarrow E_{KNC_{jl}}(X_k)$

(6) 当主机收到$E_{KM0_{ik}}(X_l)$，主机l收到$E_{KM0_{il}}(X_k)$时，进行以下操作。

主机k操作：

$$EXMK1: \{E_{KM0_{ik}}(X_l)\} \rightarrow E_{KM1_{ik}}(WK_k)$$

其中$WK_k = (X_l^{s_j} \cdot IDH_{jl})^{r_k} \mod n$

RFMK：$\{E_{KM1_k}(WK_k)，E_{KM0_k}(KS)\}\rightarrow E_{WK_k}(KS)$

主机 k 将 $E_{WK_k}(KS)$ 送给主机 l，当主机 l 收到 $E_{WK_k}(KS)$ 时，进行以下操作：

EXMK2：$\{E_{KM0_l}(X_k)\}\rightarrow E_{KM2_l}(WK_l)$

其中 $WK_l=(X_l^s\cdot IDH_{ik})^{r_l}\ \ modn$

RTMK：$\{E_{KM2_l}(WK_l)，E_{WK_k}(KS)\}\rightarrow E_{KM0_l}(KS)$

(7) 在主机 l 处进行以下操作：

RFMK：$\{E_{KM0_l}(KS)，E_{KM1_l}(KMT_s)\}\rightarrow E_{KMT_s}(KS)$；主机 l 将 $E_{KMT_s}(KS)$ 送给终端 S。

(8) 在终端 s 处进行解密操作：

DMK：$\{KMT_s，E_{KMT_s}(KS)\}\rightarrow KS$

至此，会期密钥由主机 k 送至被要求会期的终端 s。因此，i 子群 k 主机的 t 终端就可以利用会期密钥 KS 和 j 子群 l 主机的 s 终端进行保密通信会期。

## 6 系统安全性分析

分群式密钥管理系统的各个子群中采用 IBM 规程进行通信会期；而且当会期建立完毕后，公开密钥密码算法不参与任何会期，采用的加密算法是数据加密标准 (DES)。这样系统具有 IBM 规程的一切优点。

分群式密钥管理系统中，在主机里引入了基于身份的公开算法。使这种通信规程具有以下优点：

(1) 主机——主机之间可以相互鉴别对方的身份。鉴别的过程在 $WK_i$，$WK_j$ 时就已经建立，不需要额外的鉴别手段。由于 $S_i$ 和 $r_i$ 只有主机 i 知道，而 $S_j$，$r_j$ 只有主机 j 知道。假设主机 i 想和主机 j 进行连接时，有一主机 k 想冒称主机 j 和主机 i 建立通信会期。由上面会期过程可知首先它必须同自己所在子群的中继站合作才能有效地和主机 i 相连。但是即使它收到了中继站送给它的 $X_i$，并且可以获得 $E_{KM0_k}(X_i)$，它也不能有效地和主机 i 建立会期通信会期。因为：

在主机 i 处：$WK_i=(X_k^s\cdot ID_j)^{r_j}\ \ (modn)$

在主机 k 处：$WK_k=(X_i^s\cdot ID_i)^{r_k}\ \ (modn)$

显然，由于 $WK_i=(X_k^s\cdot ID_j)^{r_i}\ (modn)$ 中 $X_j$，变为 $X_k$，所以 $WK_i\neq WK_k$。因此不能在主机 i 和冒称者之间建立会期。同样任何别的主机也不能冒称主机 i 和主机 j 建立有效会期。由于任何别的主机不知道 $S_i$，它不能算出 $X_i$。

故 $(X_j^s\cdot ID_j)^{r_k}\ (modn)\neq(X_k^s\cdot ID_i)^{r_j}\ (modn)$

(其中 $r_k$ 为伪装者产生的随机数，$X_k$ 为伪装者计算的结果)。

(2) 任何别的节点即使知道 $X_i$，$X_j$ 也不能推知主机 i 和主机 j 的会期密钥 $WK_i$，$WK_j$。因为任何别的节点不能从 $X_i=S_i\cdot g^{r_i}\ (modn)$，$X_j=S_j\cdot g^{r_j}\ (modn)$ 中推出 $r_i$，$r_j$。

(3) 中继站中引入 DES 算法，使得 X 以 $E_{KNC}(X)$ 形式传送给主机。在主机的密码设施之外，X 不会以明码形式出现。因此主机 i 不能在密码设施之外产生二级通信钥 WK。

(4) EXMK1，EXMK2 都是在密码设施里进行的，主机 i 和主机 j 不能确知 $WK_i$，$WK_j$。

由上可见，任何密钥都不会以明码形式在密码设施之外出现。

## 7 结 论

分群式密钥管理系统在主机中引入了基于身份的公开密钥算法。有效地克服了IBM规程在大规模安全网中不利于身份鉴别，存储密钥太多的不足。它的安全性与IBM规程一样强。在大规模安全网中具有较好的应用价值。

### 参 考 文 献

[1] 卡尔H. 梅尔，司蒂芬·马脱耶斯·密码学：计算机数据安全的一个新领域·北京：国防工业出版社，1988

[2]Eiji Okamoto. Key Distribution Systems Based On Identification Information. Advance in Cryptology crypto' 87.

[3] Lein Harn and Thomas Keisie. Authenticated Group Key Distribution Scheme for A Large Distributed Network. IEEE Symposium on Security and Privacy, 1989.

# A Key Management Scheme for a Large Computer Safety Network

## ——The Grouped Key Management System

Yang Lie Liang Nie Tao

**ABSTRACT**

In this paper, a key management scheme for establishing end-to-end encrypted communication in a large distributed computer network is discussed. This Scheme is easy to manage, fast in encryption and powerful in secrecy. At the same time, this scheme makes it possible for users to identify each other easily.

**Key words**: Encryption; Decryption; Key Management; Communication Session