一种任意数量托管代理的密钥托管方案

谢冬青[1,2],张大方[1],李 超[3],冷 健[1]
(1. 湖南大学计算机科学系,长沙 410082;2. 中国科学院软件研究所计算机科学开放实验室,北京 100080;
3. 国防科技大学理学院数学与系统工程系,长沙 410073)

摘 要: 已有的密钥托管方案都要求恢复密钥的托管方数量相等,本文提出一种新的密钥托管方案,在恢复会话密钥时,可以是任意指定的托管方数量,托管方成员增加、减少、更换时,无需更改已托管的密钥碎片,密钥分拆和密钥恢复运算量各不超过 $4n+1$ 次 RSA 运算. n 为托管代理总数.

关键词: 密钥托管; 协议; 门限方案
中图分类号: TN918.4 **文献标识码**: A **文章编号**: 0372-2112 (2001) 02-0172-03

A Key Escrow Scheme for Escrow Agency of Arbitrary Number

XIE Dong-qing[1], ZHANG Da-fan[1], LI Chao[2], LENG Jian[3]
(1. *Dept. of Computer Science, Hunan University, Changsha* 410082, *China*;
2. *Laboratory of Computer Science, Institute of Software, The Chinese Academic of Science, Beijing* 100080, *China*;
3. *Dept of Mathematics and System Engineering, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: The known key escrow scheme requires equal number in key recover escrow side. This paper proposes a new key escrow scheme. In recovering session key, any assigned number of escrow side is allowable. When increasing, reducing and changing the member of escrow side, it is not necessary to modify the storing key part, and no more than $4n+1$ (n is positive integer) RSA operations are needed respectively for key split or key recover.

Key words: key escrow; protocol; threshold scheme

1 引言

现代保密通信追求的目标是任何时间、任何地点、任何人之间的通信,但是政府却希望有能力对某些特殊用户之间的保密通信实施监听,以防止犯罪,或者协助调查犯罪事实. 据此,美国政府推出了密钥托管加密标准 EES[1] (Escrow Encryption Standard),推荐了防篡改的密码芯片 CLIPPER,其中提供的密码算法是 SKIPJACK[2],密钥长度为 80bit,能抗差分攻击,安全性高,但密钥生成的每 5 轮后会重复使用相同的密钥,且 F 函数使用了 4 个 Feistel 结构,对芯片速度有较大影响. 密钥托管的核心思想是提供强密码算法实现用户的保密通信,并使得合法授权的法律执行部门利用密钥托管机构提供的信息,恢复出会话密钥,从而对通信实施监听. 目前已有多种密钥托管方案,大都基于 Shamir (n, k) 门限思想[3~6],法律执行机构行使监听权时,每一次恢复密钥的托管代理成员数量相等. 文[7]为了防止法律执行机构大规模地恢复用户密钥,设计了部分密钥托管体制,达到了延缓恢复时间的目的,但是它要求所有托管代理共同参与,即是 Shamir (n, n) 门限方案.

公开密钥密码体制通信前无需交换密钥,安全性好,而实现速度较慢,因此实际的安全系统大多采用公开密钥密码体制来交换会话密钥,采用对称加密体制(如 Triple-DES, IDEA)来加密信息本身. 会话密钥或者依每一次连接而改变,或者依每一个消息而变化,而公开密钥密码体制的公开钥和私钥相对固定. 本文利用更一般的密钥共享思想[8],给出一种密钥托管方案,允许数目灵活的托管代理,实施对用户私钥的托管,当托管方成员增加、减少、更换时,无需更改已托管的密钥碎片. 法律执行机构利用托管恢复的私钥来恢复会话密钥,从而实施通信监听.

2 方案描述

定义 1:密钥 k 的托管体制是一个五元组$\langle E, A, k, P, X\rangle$,其中 E 是法律执行部门,A 是必须将私钥托管的用户,简称托管者,P 是托管方集合,其某一些子集合作可以恢复 A 的密钥 k,k 是托管的密钥.

此处将法律授权部门与法律执行部门合并称为法律执行部门.

定义 2:称 $X\subset P$ 是能行恢复集,如果 X 中成员合作能恢复密钥 k.

收稿日期:2000-01-17;修回日期:2000-03-29
基金项目:国家自然科学基金(No. 69973016);东南大学移动通信国家重点实验室资助项目

若要求所有能行恢复集成员数相同,即退化为 Shamir(n, k)门限方案.

定义 3:设分配给托管方 $P=\{P_1, P_2, \cdots, P_n\}$的子数据是 $S=\{s_1, s_2, \cdots, s_n\}$,称 s_i 是 k 的碎片或影子.

2.1 系统初始化

记托管用户 A 的公开钥为 N_A, e_A,私钥为 d_A,记 P 是托管代理集合 $P=\{P_1, P_2, \cdots, P_n\}$, P_i 都有 RSA 公开钥 N_i, e_i,私钥 d_i,他们由法律执行机构,记为 E,有 RSA 公开钥 N_E, e_E,私钥 d_E,委托托管某一秘密 k,使对于法律授权的 $X_1, X_2, \cdots, X_l \subset P, X_j$ 中成员合作能恢复 $k, j=1,2,\cdots,l$, X_j 称为能行恢复集,而任何 $A \subset P, A \notin \{X_j \mid j=1,2,\cdots,l\}$ 不能恢复 k. 注意这里并不要求$|X_1|=|X_2|=\cdots\cdots=|X_l|$.

2.2 私钥托管

(1) 托管者 A 随机选取整数 $s_1, s_2, \cdots, s_n$,将 $t_i=((s_i \| req_i)^{e_i} \bmod N_i)^{d_A} \bmod N_A$ 通过公开信道传给 $P_i, i=1,2,\cdots,n$. 其中 req_i 是 A 向第 i 个托管代理的托管请求,$\|$ 表示连接(此处,也可以将 t_i 看成 k 的碎片,即托管代理 P_i 共享 t_i).

(2) P_i 计算 $w_i=((t_i^{d_i}) \bmod N_i)^{e_A} \bmod N_A$,恢复出 s_i 和 req_i 以确认 P_i 收到密钥碎片 t_i.

(3) P_i 向托管用户 A 发回确认信息.

(4) 对于 P 中每个能行恢复集 X, A 随机选取生成元 g_X,并计算 $f(g_X^{\sum_{i\in X} s_i})$,其中 $\sum_{i\in z} s_i$ 表示行恢复集 z 中各成员的 s_i 求和,令

$$T_X = k - f\left(g_X^{\sum_{i\in X} s_i}\right).$$

(5) 将 (X, g_X, T_X) 公告.

2.3 私钥恢复

不妨记 $X=\{P_{i_1}, P_{i_2}, \cdots, P_{i_r}\}$, $r=|X|$

(1) P_{ij} 恢复 $S_{i_j}, S_{i_j}=((t_{i_j})^{d_{i_j}} \bmod N_{i_j})^{e_A} \bmod N_A, j=1,2,\cdots,r$

(2) P_{ij} 计算 $g_X^{s_{i_j}}$ 将 $v_{ij}=(g_X^{s_{i_j}})^{e_E} \bmod N_E$ 传给法律执行部门 E. $j=1,2,\cdots,r$.

(3) E 计算 $(v_{i_j})^{d_E} \bmod N_E = \left(\left(g_X^{s_{i_j}}\right)^{e_E} \bmod N_E\right)^{d_E} \bmod N_E = g_X^{s_{i_j}}, j=1,2,\cdots,r$. 再计算 $\prod_{j=1}^{r} g_X^{s_{i_j}} = g_x^h$,其中 $h=\sum_{j=1}^{r} s_{i_j}$.

(4) 法律执行部门从公告板上查出能行恢复集 X 对应的 g_X 及 T_X,并计算 $k=T_X+f(g_X^h)$.

2.4 用户通信

用户之间的通信不因密钥托管而改变.

2.5 监听过程

(1) 法律执行机构向能行恢复集 X 中各成员在公开信道上传送加密了的监听命令信息 m, m 包含了监听对象的身份号和公开钥号,即 $m=\{req \| ID \| PK\}$, req 表示监听命令, ID 表示监听对象的身份号, PK 表示监听对象的公开钥号.

$$u_i=((m^{d_E}) \bmod N_E)^{e_i} \bmod N_i$$

(2) 能行恢复集 X 中各成员解密监听命令信息,验证法律执行机构的监听命令

$$m=((u_i^{d_i}) \bmod N_i)^{e_N} \bmod N_E$$

若不成功,终止.

(3) 进入私钥恢复阶段,利用私钥恢复会话密钥,然后实施监听.

3 方案性能分析

3.1 效率分析

本文将 RSA 加密运算和解密运算统一称为 RSA 运算,记 $s=\max\{s_i \mid i=1,2,\cdots,n\}$.

定理 1　密钥托管方案中私钥分拆和私钥恢复各需 $4n+1$ 次 RSA 运算.

证　私钥分拆:私钥分拆的步骤 1、2 各需 $2n$ 次 RSA 运算,共 $4n$ 次 RSA 运算,步骤 4 需计算 $g_X^{\sum_{i\in X} s_i}$,需 $2\log(\sum_{i\in X} s_i) \le 2\log(ns)$ 次 $\log g_x$ 位整数乘法,计算 $f\left(g_X^{\sum_{i\in X} s_i}\right)$, f 可取 RSA 函数,相当于一次 RSA 运算. 故私钥分拆共需 $4n+1$ 次 RSA 运算.

私钥恢复:步骤 1 需 $2r$ 次 RSA 运算,步骤 2 需 r 次 RSA 运算,$4r\log s$ 次 $\log g_x$ 位整数乘法,步骤 3 需 r 次 RSA 运算,计算 $\prod_{j=1}^{r} g_X^{s_{i_j}}$,总比特运算量

$$\begin{aligned}&=\log s_{i_1}\log^2 g_X + (\log s_{i_2}\log^2 g_X + s_{i_1}s_{i_2}\log^2 g_X) + (\log s_{i_2}\log^2 g_X + (s_{i_1}+s_{i_2})s_{i_3}\log^2 g_X) + \cdots + (\log s_{i_r}\log^2 g_X + (s_{i_1}+s_{i_2}+\cdots+s_{i_{r-1}})s_{i_r}\log^2 g_X) \le r\log s\log^2 g_X + \log^2 g_X(s_{i_1}s_{i_2} + (s_{i_1}+s_{i_2})s_{i_3} + \cdots + (s_{i_1}+s_{i_2}+\cdots+s_{i_{r-1}})s_{i_r}) \le r\log s\log^2 g_X + \log^2 g_X(s^2+2s^2+\cdots+(r-1)s^2) = \log^2 g_X(r\log s + s^2 r(r-1)/2)\end{aligned}$$

注意到 $r=|X|$,运算量为 $O(|X|^2) \approx O(n^2)$,步骤 4 相当于一次 RSA 运算,故私钥恢复阶段共需 $4r+1 \le 4n+1$ 次 RSA 运算和 $O(n^2)$ 次整数乘法. 由于此处 RSA 处理的是托管的密钥,而密钥长度都相当有限,因此,可采用高强度的 RSA 算法,如 1024 位.

3.2 能行恢复集成员变化时方案容易适应:当能行恢复集 X 中的成员增加、减少或更换时,无需对已经托管的密钥碎片进行更新,只需将公告板上的 T_X 修改即可. 方案对能行恢复集成员数没有限制,可以从 1 个到所有的托管成员.

3.3 托管的确认:由于密钥托管方案带有托管者自签名,一方面能防止对托管机构的冒充,另一方面由于托管者将托管请求和密钥碎片级连以后,一起用托管方的公钥加密,传递给托管方,只有托管方能够恢复,使托管方确信已得到密钥碎片,保证了托管方的权益.

3.4 可跟踪托管机构的逃脱

托管者对托管机构的逃脱是指托管者将无意义的碎片交给托管方 P 保管,这可以通过事后各成员间合作能否得到私钥 k 来验证.

4 结束语

除了用于政府机构的监听以外,密钥托管能够帮助恢复属于他人的密钥,这些人或许已经离开了公司,或许遗忘了密钥. 安全应用系统应当能够提供密钥托管功能. 本文给出的密钥托管方案,允许恢复密钥时托管代理数量不一定相同,即 n 个托管代理中,对任意指定的托管代理集合,不论其数量多少,只要规定他们是能行恢复集就可以恢复,突破了 Shamir 共享密钥方案中恢复者成员数均为 k 的限定. 此外,托管成员

发生变化时,无需更换托管方的密钥碎片.

参考文献:

[1] National Institute for Standards and Technology. Escrow Encryption Standard [S]. Federal Information Processing Standards Publication 185, U. S. Dept of Commerce, 1994.

[2] SKIPJACK and KEA Algorithm Specifications, (Version 2.0) [DB/OL]. May 1998, Available at the National of Standards and Technology's web page, http://csrc.nist.gov/encryption/skipjack-kea.htm.

[3] D Denning, D. Branstad. A taxonomy for key escrow encryption system [J]. Comm. of the ACM, 1996, 39(3): 34 - 40.

[4] A. Shamir. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612 - 613.

[5] 孙晓蓉,刘建伟,王育民. 移动通信中的密钥托管方案 [J]. 电子学报,1999,27(4):137 - 139.

[6] 宋荣功,詹榜华,胡正名. 基于多层次可验证共享协议的密钥托管方案 [J]. 电子学报,1999,27(6):136 - 137.

[7] 陈伟东,翟起滨. 一种新的公开可验证的部分密钥托管体制 [J]. 通信学报,1999,20(11):25 - 30.

[8] M. Ito, A Saito and T Nishizeki. Secret sharing scheme realizing general access structure [A]. Proc IEEE Globecom'87 [C], 1987: 99 - 102.

作者简介:

谢冬青 1965 年生,副教授. 1985 年获西安电子科技大学应用数学系理学学士学位,1988 年获西安电子科技大学计算机系工学硕士学位,1999 年获湖南大学应用数学系理学博士学位. 1988 年起在湖南大学计算机系任教. 发表学术论文四十余篇. 现主要从事信息安全领域的教学、科研工作.

张大方 1959 年生,博士,教授. 主要从事容错计算、网络测试等领域的教学与科研工作,主持国家自然科学基金项目和国家 863 计划项目 3 项,发表学术论文 100 余篇. 现任中国计算机学会容错计算专委会委员兼测试与诊断学组副组长,全国计算机继续教育研究会副理事长,IEEE 会员,全国高等学校计算机教育研究会理事,湖南省政协常委.

第六届固态和集成电路技术国际会议(ICSICT—2001)征文通告

2001 年 10 月 22～25 日,上海

第六届固态和集成电路技术国际会议(ICSICT—2001)将于 2001 年 10 月 22～25 日在上海贵都国际大饭店召开. 这次会议由中国电子学会(CIE)主办,并得到 IEEE 电子器件分会、国家自然科学基金委、上海市科委、IEEE 北京分会等国内外学术单位协助和支持.

征文内容

1. 集成电路制造和工艺集成

逻辑电路、模拟电路、射频电路以及数模混合电路、存储器(DRAM、SRAM, Flash/EEPROM, FRAM …)、片上系统(SoC)、可编程逻辑器件(FPGA)、智能功率集成 IC、SOI-IC 等集成电路的工艺集成、生产制造和分析表征.

2. 超大规模集成电路工艺技术

离子注入,隔离,超薄栅氧化层以及高 K 栅介质材料,金属栅,金属硅化物,源漏形成技术,光刻和腐蚀,多层布线,低 K 介质材料,先进金属化和扩散阻挡层,化学机械抛光以及与 CMOS、双极和 BICMOS 等有关的其它 VLSI 工艺.

3. 新器件结构,器件物理,建模以及 TCAD

纳米器件和新器件结构,SiGe/Si 异质结器件,单电子器件,量子器件,超导器件,器件以及工艺建模和模拟.

4. 器件特性表征,可靠性和失效分析

工艺引入的缺陷(热电子、等离子体损伤等),器件以及互连的可靠性,测试结构,硅片级可靠性、器件和材料表征,新器件和先进互连线的失效机制,缺陷减少技术,清洗及污染控制技术,失效分析技术.

5. 封装技术

封装有关技术和材料,多芯片模块,直接芯片焊接,芯片倒装技术,与 Cu/低 K 互连有关的封装问题,电源调配,光子器件封装.

6. 化合物半导体和高频器件

III-V, II-VI 和其它化合物半导体的生长和制造工艺,宽带半导体(GaN、SiC 等),III-V 异质结双极型晶体管和场效应管,半导体激光器和探测器,光电子器件和集成电路,用于高速宽带通讯的半导体和固态器件.

7. 薄膜材料及器件

非晶 Si,薄膜晶体管 AMLCD 集成电路,平板显示器,其它薄膜材料和器件,有机半导体薄膜材料和器件.

8. 微电子机械系统

微机械加工和微制造技术,传感器,探测器,执行器,微电子机械和微光电机械系统技术和应用.

有关投稿的进一步信息可按以下地址联系:

上海复旦大学电子工程系李炳宗教授

邮编:200433 E-mail: bzli@fudan.ac.cn

电话:021-65643768 传真:021-65648267

第六届(2001 年)ICSICTG 国际会议程序委员会