软件密钥托管加密系统研究

宋荣功,杨义先,胡正名
(北京邮电大学信息安全中心 126 信箱,北京 100876)

摘 要: 本文基于 RSA 公钥体制提出了一个不依赖物理设备的软件密钥托管加密方案. 新方案不仅具有抗窜扰特性,而且克服了以前方案中的缺点,并同时能对消息的源和宿进行追踪.

关键词: RSA 公钥体制; 密钥托管加密系统; 软件密钥托管加密系统
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2000) 08-0132-03

On the Software Key Escrow System

SONG Rong-gong, YANG Yi-xian, HU Zheng-ming
(*Beijing University of Post and Telecommunication, Beijing* 100876, *China*)

Abstract: Based on RSA public key encryption system, a new software key escrow system is proposed. This new system provides not only effectually anti-flaw in other software key escrow systems, but also satisfies tracing message's sender and receiver, and satisfies other escrow characteristics. So the new approach is established for the software key escrow encryption system.

Key words: RSA public key encryption system; key escrow encryption system; software key escrow encryption system

1 引言

美国政府在 1993 年 4 月公布了托管加密标准 EES[1],其目的在于在确保合法用户保密通信的同时,保证政府能对犯罪分子的保密通信进行有效监听. 托管加密技术已成为密码学界的一个研究热点. 有人从硬件方案[2,3],也有人从软件方案[4,5]出发,对不依赖于防窜扰设备的软件方案以及追踪消息源和宿的方法进行研究.

软件密钥托管加密技术必须解决两个最关键的问题,其一是系统的非规避性问题,其二是消息源和宿的追踪问题. 这两个特性由硬件实现时,由于依赖于抗窜扰特性的物理设备而使得其实现非常容易,但由软件实现时难度非常大.

目前提出的真正不依赖防窜扰设备的软件密钥托管加密方案只有两个. 第一个是 1995 年由 Desmedt 提出[5],但不久就被击破[6];第二个方案是 1997 年由 Boyd 提出[7]. 但是 Boyd 的方案只能对消息的宿进行追踪,而无法对消息的源进行追踪. 本文基于 RSA 公钥体 ,设计了一个新的软件密钥托管加密方案. 该方案能满足密钥托管的所有最基本条件:系统非规避性、消息源和宿的可追踪性、监听对象受限性以及监听时间受限性.

2 新软件密钥托管加密系统的设计

2.1 新软件密钥托管加密系统的简单描述

在新设计的软件密钥托管加密系统中,用户采用对称密码体制来加密消息 M,会话密钥 k 是用 RSA 公钥密码体制来加密传递. 密码系统中有一个证书中心(CA),负责颁发通信用户的公钥证书;有两个密钥托管代理机构(T_1 和 T_2),负责托管用户的 RSA 部分私钥;有一个法律授权机构负责监听授权和存储用户的部分私钥;有一个监听机构负责实施用户通信的监听.

2.2 新软件密钥托管协议的设计

在新的软件密钥托管加密系统中. 用户首先向 KMC 注册申请公钥证书. KMC 随机选取两个大素数 p 和 q(一般为 512bit),利用下面托管协议生成用户的 RSA 私钥和公钥证书,并实施对用户的 RSA 私钥进行托管. 其中假设系统中证书中心的 RSA 公钥、私钥和模分别为 K_{CAP}、K_{CAS}和 N_{CA};代理 1 的 RSA 公钥、私钥和模分别为 K_{TIP}、K_{TIS}和 N_{Ti};代理 2 的 RSA 公钥、私钥和模分别为 K_{T2P}、K_{T2S}和 N_{T2};法律授权机构的 RSA 公钥、私钥和模分别为 K_{OP}、K_{OS}和 N_O.

第一步 用户 A 随机选取 $K_{AS} \in Z^+$(一般小于 1000bit),然后用 CA 的公钥加密,并将自己的身份证明和密文 $K_{AS}^{K_{CAP}} \bmod N_A$ 出示给 CA.

第二步 CA 验证完用户 A 的身份后,为用户 A 产生一个身份号 ID_A,并解出明文 K_{AS}. 然后随机选取两个大素数 p 和 q(大约 512bit),计算 $\phi(N_A) = (p-1)(q-1)$,并随机选取 $K_{AO} \in Z^+$(一般小于 1000bit),计算 $K_A \equiv K_{AS}K_{AO} \bmod \phi(N_A)$,并检查 K_A 与 $\phi(N_A)$ 是否互素. 若不互素则重选 K_{AO}. (由于 p 和 q 是大素数,所以重选很少几次就行了). 然后用法律授权机

收稿日期:1999-04-21;修回日期:1999-11-20
基金项目:国家自然科学基金重大项目资助(No. 69772035, No. 69882002);重点基础研究发展规划项目(No. G1999035805)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

构的公钥对 K_{AO}加密,得到 $A_O \equiv K_{AO}^{K_{OP}} \bmod N_O$. 然后将 K_{AS}随机地分为两部分 K_{AS1}和 K_{AS2},使得 $K_{AS} \equiv K_{AS1} + K_{AS2} \bmod \phi(N_A)$,并分别用代理 1 和代理 2 的公钥加密,得到 $A_{T1} \equiv K_{AS1}^{K_{T1P}} \bmod N_{T1}$和 $A_{T2} \equiv K_{AS2}^{K_{T2P}} \bmod N_{T2}$. 最后计算签名 $S_{CAT1} = Sig_{CA}(h(ID_A, Time, A_{T1}, N_A))$、$S_{CAT2} = Sig_{CA}(h(ID_A, Time, A_{T2}, N_A))$和 $S_{CAO} = Sig_{CA}(h(ID_A, Time, A_O, N_A))$,并将 $(ID_A, Time, A_{T1}, N_A, S_{CAT1})$、$(ID_A, Time, A_{T2}, N_A, S_{CAT2})$和 $(ID_A, Time, A_O, N_A, S_{CAO})$分别传送给托管代理 1、托管代理 2 和法律授权机构.

第三步　托管代理 1 和托管代理 2 收到 $(ID_A, Time, A_{T1}, N_A, S_{CAT1})$、$(ID_A, Time, A_{T2}, N_A, S_{CAT2})$后,分别验证签名和时间的有效性. 如果通过验证,则分别计算签名 $S_{T1CA} = Sig_{T1}(h(ID_A, ID_{T1}, Time))$和 $S_{T2CA} = Sig_{T2}(h(ID_A, ID_{T2}, Time))$,并将 $(ID_A, ID_{T1}, Time, S_{T1CA})$和 $(ID_A, ID_{T2}, Time, S_{T2CA})$分别传送给 CA.

第四步　法律授权机构收到 $(ID_A, Time, A_O, N_A, S_{CAO})$后,验证签名和时间的有效性. 如果通过验证,则分别计算签名 $S_{OCA} = Sig_O(h(ID_A, ID_O, Time))$,并将 $(ID_A, ID_O, Time, S_{OCA})$传送给 CA.

第五步　CA 验证完 $(ID_A, ID_{T1}, Time, S_{T1CA})$、$(ID_A, ID_{T2}, Time, S_{T2CA})$和 $(ID_A, ID_O, Time, S_{OCA})$的有效性,计算 K_{AP}使得 $K_{AP}K_A \equiv 1 \bmod \phi(N_A)$,并计算签名 $S_{CAA} = Sig_{CA}(h(ID_A, K_{AP}, N_A, Time, \cdots))$,最后颁发用户 A 的公钥证书 $C(A) = (ID_A, K_{AP}, N_A, Time, \cdots, S_{CAA})$. 否则,则告知用户 A 注册失败.

新软件密钥托管加密系统中用户的密钥托管过程如图 1 所示.

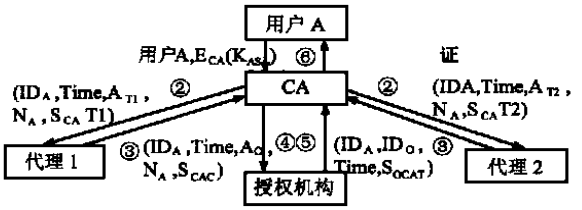


图 1　新软件密钥托管加密系统中用户的密钥托管过程

2.3　新软件密钥托管加密系统的通信过程

新软件密钥托管加密系统的通信过程由三部分组成:发送方的操作过程、接收方的操作过程和授权机构的操作过程.

2.3.1　发送方的操作过程　当用户 A 欲向用户 B 发送秘密消息 M 时,用户 A 首先随机选取会话密钥 K,并用传统加密算法将消息 M 加密,得到密文 $C \equiv E(K, M)$;然后他要用授权机构的公钥 K_{OP}把他和用户 B 的身份以及时间戳加密,得到密文 $C_{AO} \equiv (ID_A, ID_B, Time)^{K_{OP}} \bmod N_O$,并用 B 的公钥 K_{BP}将会话密钥加密,得到 $C_{BK} \equiv K^{K_{BP}} \bmod N_B$,用 hash 函数计算 $H = h(ID_A, ID_B, Time, C_{BK})$,并用他自己的部分私钥 K_{AS}对 C_{BK}和 H 签名,得到 $S_{AO} \equiv (C_{BK}, H)^{K_{AS}} \bmod N_A$;最后将 (C_{AO}, S_{AO}, C)传送给用户 B 或直接传送给授权机构. 因为用户 B 只有部分私钥,而另一部分私钥被授权机构掌握且也是随机的大数,即用户 B 企图搜索出被授权机构掌握的部分私钥在计算上是不可能的,所以他只有先将 (C_{AO}, S_{AO})或 (C_{AO}, S_{AO}, C)传送给授权机构.

2.3.2　授权机构的操作过程　授权机构按下列固定程序进行操作:

①首先计算 $(C_{AO})^{K_{OS}} \bmod N_O$,从而解密出 $(ID_A, ID_B, Time)$;然后用 A 的公钥 K_{AP}和授权机构拥有的用户 A 的另一部分私钥 K_{AO}计算 $(S_{AO})^{K_{AP}K_{AO}} \bmod N_A$,从而解密出 C_{BK}和 H;最后计算 $H' = h(ID_A, ID_B, Time, C_{BK})$,并验证 $H = H'$? 若通过验证则转到 ②,否则停止计算.

②授权机构用 B 的公钥 K_{BP}和他所拥有的 B 的另一部分私钥 K_{BO}对 $(ID_A, ID_B, Time)$重新加密,得到 $C_{OB} \equiv (ID_A, ID_B, Time)^{K_{BP}K_{BO}}(C_{BK})^{K_{BO}} \bmod N_B$,然后用 K_{BO}继续对 C_{BK}加密,得到 $C_{AB} \equiv (C_{BK})^{K_{BO}} \bmod N_B$,并计算 $H = h(ID_A, ID_B, Time, C_{AB})$;最后授权机构用他自己的私钥 K_{OS}对 C_{AB}和 H 加密,得到 $S_{OB} \equiv (C_{AB}, H)^{K_{OS}} \bmod N_B$,并将 (C_{OB}, S_{OB})或 (C_{OB}, S_{OB}, C)传送给用户 B.

2.3.3　接收方的操作过程　用户 B 收到授权机构发送的 (C_{OB}, S_{OB})或 (C_{OB}, S_{OB}, C)后,首先用他自己的部分私钥 K_{BS}对 C_{OB}解密,得到 $(ID_A, ID_B, Time) \equiv (C_{OB})^{K_{BS}} \bmod N_B$,同时用授权机构的公钥 K_{OP}解密 S_{OB},得到 $(C_{AB}, H) \equiv (S_{OB})^{K_{OP}} \bmod N_O$;然后验证 $H = h(ID_A, ID_B, Time, C_{AB})$? 若通过验证,则用他的部分私钥 K_{BS}对 C_{AB}解密,得到会话密钥 $K \equiv (C_{AB})^{K_{BS}} \bmod N_B$;最后再用 K 解密 C,得到明文 $M = D(K, C)$. 从而完成整个通信.

新软件密钥托管加密系统的整个通信过程如图 2 所示.

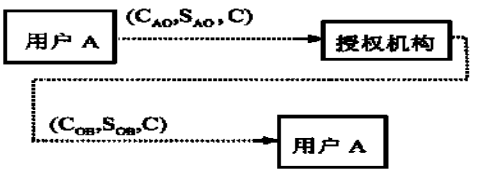


图 2　新软件密钥托管加密系统的通信过程

2.4　新软件密钥托管加密系统的监听过程

新软件密钥托管加密系统可进行有效期内一次性在线式监听和永久性离线式监听两种方式对用户实施监听,监听过程如下.

2.4.1　有效期内在线式监听　(a) 监听机构获取法律授权部门的有效期内在线式监听证书后,将证书和监听到的 (C_{AO}, S_{AO}, C)出示给授权机构. (b) 授权机构按照第三部分的操作过程将计算出的 $(ID_A, ID_B, Time, C_{AB})$进行签名后交给监听机构. (c) 监听机构将 $(ID_A, ID_B, Time, C_{AB}, S_{OAB})$和监听证书分别出示给委托代理 1 和委托代理 2. (d) 委托代理 1 和委托代理 2 验证其有效性后,分别用他们所托管的 B 的部分私钥 K_{BS1}和 K_{BS2}对 C_{AB}进行加密,得到 $C_1 \equiv (C_{AB})^{K_{BS1}} \bmod N_B$ 和 $C_2 \equiv (C_{AB})^{K_{BS2}} \bmod N_B$,并将 C_1 和 C_2 分别传送给监听机构. (e) 监听机构收到 C_1 和 C_2 后,计算

$$C_1 C_2 \equiv (C_{AB})^{K_{BS1}} (C_{AB})^{K_{BS2}} \bmod N_B \equiv (C_{AB})^{K_{BS1}+K_{BS2}} \bmod N_B$$
$$\equiv (C_{AB})^{K_{BS}} \bmod N_B \equiv K^{K_{BP}K_{BO}K_{BS}} \bmod N_B \equiv K^{K_{BP}K_B} \bmod N_B$$
$$\equiv K \bmod N_B$$

恢复出 A 和 B 通信的会话密钥,最后通过计算 $M = D(K, C)$

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

解出明文,从而实现对 A 与 B 通信的监听.

2.4.2 永久性离线式监听 *(a)* 监听机构获取法律授权部门的永久性离线式监听证书后,将证书分别出示给委托代理 1 和委托代理 2. *(b)* 委托代理 1 和委托代理 2 验证其有效性后,分别他们所托管的 B 的部分私钥 K_{BS1} 和 K_{BS2} 交给监听机构. *(c)* 监听机构收到 K_{BS1} 和 K_{BS2} 后,对任何时间监听到的 (C_{OB}, S_{OB}, C) 进行计算,首先计算

$$(C_{OB})^{K_{BS1}+K_{BS2}} \bmod N_B \equiv (C_{OB})^{K_{BS}} \bmod N_B \equiv (ID_A, ID_B, Time) \bmod N_B$$

同时用授权机构的公钥 K_{OP} 解密 S_{OB},得到 $(C_{AB}, H) \equiv (S_{OB})^{K_{OP}} \bmod N_O$;然后验证 $H = h(ID_A, ID_B, Time, C_{AB})$? 若通过验证,则用 K_{BS1} 和 K_{BS2} 对 C_{AB} 解密,得到

$$(C_{AB})^{K_{BS1}+K_{BS2}} \bmod N_B \equiv (C_{AB})^{K_{BS}} \bmod N_B \equiv \equiv K^{K_{BP}K_{BO}K_{BS}} \bmod N_B \equiv K^{K_{BP}K_B} \bmod N_B \equiv K \bmod N_B$$

恢复出 A 和 B 通信的会话密钥,最后通过计算 $M = D(K, C)$ 解出明文,从而实现对 A 与 B 通信的永久性监听.

新软件密钥托管加密系统的监听过程如图 3 所示.

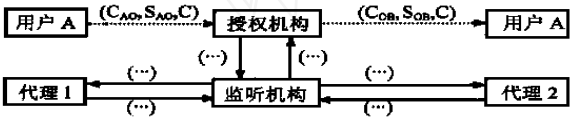


图 3 新软件密钥托管加密系统的监听过程

3 新软件密钥托管加密系统的安全性分析

(1) 新软件密钥托管加密系统具有系统非规避特性. 由于欲利用该保密系统进行通信的用户 A 和 B,在进行会话密钥的传递时,用户 A 和 B 只拥有相对于他们的公钥和部分私钥,而另一部分私钥为授权机构所拥有,所以接收方 B 要想解密出 A 用 B 的公钥加密的会话密钥的密文,则必须首先使该密文经过授权机构的预处理,否则接收方是无法解密出会话密钥 K 的.

(2) 新软件密钥托管加密系统可有效的对消息源和宿进行追踪. 由于在新系统中,授权机构是按照一个固定程序进行操作的,他首先用他的私钥 K_{OS} 计算 $(C_{AO})^{K_{OS}} \bmod N_O$,解密出 $(ID_A, ID_B, Time)$,从而找到发送者 A 和接收者 B. 一方面若发送方 A 企图用假身份代替 ID_A,则由于用户 A 没有用户 C 的部分私钥,因而他无法用 C 的部分私钥对 C_{BK} 和 H 进行签名,因此当授权机构用 C 的公钥 K_{CP} 和授权机构拥有的用户 C 的另一部分私钥 K_{CO} 计算 $(S_{AO})^{K_{CP}K_{CO}} \bmod N_A$ 后,经过验证 H 的值会发现这一假象,从而停止任何操作,所以发送者企图用假身份代替他自己是行不通的. 另一方面,若发送方 A 企图用假身份代替 ID_B,则由于授权机构在验证完 H 的值后,要用他拥有的 C 的另一部分私钥对 C_{BK} 进行加密,而用户 B 又不拥有 C 的部分私钥,所以他无法解密出会话密钥 K,即发送者企图用假身份代替 ID_B 也是行不通的.

(3) 新软件密钥托管加密系统具有监听时间受限特性. 当监听机构得到有效期内一次性在线式监听证书时,它只能把有效期内得到 $(ID_A, ID_B, Time, C_{AB}, S_{OAB})$ 交给托管代理,并从托管代理提供的信息中求出该次通信所用的会话密钥 K,从而实施监听,但无法求出用户 B 的 RSA 部分私钥 K_{BS}. 由 RSA 公钥密码体制本身的特点,可知它不能求出其它次通信所使用的会话密钥 K,因此只能进行该次通信的监听,从而防止了监听机构滥用权力的现象. 当监听机构得到永久性离线式监听证书时,则它可利用托管代理提供的信息求出用户 B 的 RSA 部分私钥 K_{BS},从而对用户 B 进行永久性监听,保证监听的有效性.

(4) 新软件密钥托管加密系统具有监听对象受限特性. 由监听过程和授权机构的操作可知授权机构完全有能力限制监听机构对两个特定用户之间的通信进行监听,以及用户 A 与任何其他人之间的通信或任何其他人与用户 B 之间的通信进行监听.

(5) 新软件密钥托管加密系统可保证每个托管代理所托管的用户部分私钥碎片的真实性以及授权机构所拥有的用户部分私钥的有效性. 由于用户的公钥是由证书中心控制产生的,并且证书中心要验证完 $(ID_A, ID_{T1}, Time, S_{T1CA})$、$(ID_A, ID_{T2}, Time, S_{T2CA})$ 和 $(ID_A, ID_O, Time, S_{OCA})$ 的有效性后,才能颁发用户 A 的公钥证书 $C(A) = (ID_A, K_{AP}, N_A, Time, \cdots, S_{CAA})$,从而保证了每个托管代理和授权机构都已得到用户的正确的部分私钥.

作者简介:

宋荣功 1999 年毕业于北京邮电大学,获密码学博士学位. 到目前为止,他已经在国内外发表论文 20 余篇. 目前主要从事密码设计,密钥托管,网络安全和信息安全等方面的应用基础研究和工程开发工作.

杨义先 1961 年生. 北京邮电大学信息安全中心主任,教授,博士导师,全国政协委员. 到目前为止,他已经在国内外发表论文 300 余篇,出版学术专著数部. 他主要从事网络安全,信息安全,现代密码学,数字信号处理,电子商务等方面的基础研究,应用基础研究和产品开发.

参考文献:

[1] NIST. Escrowed Encryption Standard (EES). FIPS PUB (Federal Information Processing Standards Publication) 185, U. S. Dept. of Commerce, February 9, 1994.

[2] He J and Dawson E. A new key escrow cryptosystem [A]. In Cryptography: Policy and Algorithms [M], LNCS 1029, Berlin: Spinger-Verlag, 1995, 105 - 114.

[3] Frankel Y and Yung M. Escrow encryption systems visited: attacks, analysis and design [A]. Advances in Cryptology-CRYPTO '95, LNCS963, Berlin: Springer-Verlag [M], 1995: 222 - 235.

[4] Dawson E and He J. Another aproach to software key escrow encryption. information security and privacy [A], LNCS 1172, Berlin: Springer-Verlag, 1996: 87 - 95.

[5] Desmedt Y. Securing tracablity of ciphertexts ——towards a secure software key escrow system [A]. Advances in Cryptology-EUROCRYPT '95, LNCS921, Berlin: Springer-Verlag [M], 1995: 147 - 157.

(下转第 131 页)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

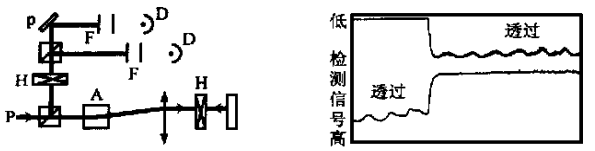


图 4　(a) 测量驱动器输出频率时间响应的声光晶体双通过装置;A:AOM　P:偏振分束器　H:四分之一波片　F:F-P 腔　D:光电二极管. (b) 通过比较频率跳变时两个 F-P 腔的透过信号,可以测量驱动器输出频率的时间响应

团转变以进一步冷却原子的过程一般为毫秒量级,在此过程中频率变化不超过十几个自然线宽(以铯为例,其 $6P^{3/2}$ 线宽为 5.2MHz).从这些方面看,所做声光晶体驱动器已完全满足要求,我们有关激光冷却实验也表明了驱动器的实用性[3].

参考文献:

[1] J. Dalibard, C. Cohen-tannoudji. Opt. Soc. Am. B6, 1989: 2023.

[2] A. Yariv, P. Yeh. Optical Waves In Crystals [C]. John Wiley & Sons, Inc. 1984.

[3] Hou Jidong, Li Yimin, Yang Donghai, Wang Yiqiu, CHIN. PHYS. LETT. 1998, 15(6): 413.

[4] Hou Jidong, Li Yimin, Yang Donghai, Wang Yiqiu. ACTA PHYSICA SINICA, 1998, 7(12): 881

作者简介:



侯继东　1991 年西安交通大学毕业,1994 年西安光机所获硕士学位. 1998 年北京大学电子学系获博士学位. 从 1996 年起至今一直从事激光冷却和囚禁原子的工作.



杨东海　1969 年毕业于北京大学,1985 年在美国纽约州立大学石溪分校物理系获博士学位. 现任北京大学电子学系教授,博士生导师,全国计量测试学会时间频率委员会委员,全国时间频率计量技术委员会委员. 他一直从事量子电子学领域的课题研究,如氦原子的超精细分裂精密测量、铷原子高激发态的斯塔克效应、激光减速、原子频标、激光冷却与超冷原子、激光光谱等研究工作. 目前主要研究方向是光抽运铯原子频标、激光冷却、超冷原子、原子激光等.

(上接第 134 页)

[6] Knudsen L R and Pedersen T P. On the difficulty of software key escrow [A]. Advances in Cryptology-EUROCRYPT '96 [M], Berlin: Springer-Verlag, 1996: 237 - 244.

[7] Boyd C. Enforcing Traceability in software. international conference of information and communication security [A], ICICIS '97 [M], LNCS 1334, Berlin: Springer-Verlag, 1997: 398 - 408.

[8] Simmons G J. Contemporary Cryptology [J]. IEEE Press, Inc. 1992: 441 - 497.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net