Research on Real-Name Identity Authentication Architecture Based on Combined Symmetric Key

LIU Tong, JIANG Jiya

Beijing Municipal Institute of Science and Technology Information, Beijing, China

e-mail: *liutong@bjstinfo.com.cn, jiang_jiya@sohu.com*

Abstract: A large-scale real-name authentication architecture and key management protocol based on combined symmetric key algorithm are proposed. With the CSK algorithm and smart card technology, the authentication process can be finished in the chips, and the management of large-scale keys can be simplified to the management of small-scale key seeds. The security of the proposed architecture is analyzed and the experimental results are shown. It is obvious that the abilities of large-scale identity authentication and management are improved while the building cost is reduced evidently with the application of the proposed architecture. It is an applicable solution for real-name authentication network.

Keywords: combined symmetric key; key management; mutual-authentication; real-name authentication

基于组合对称密钥的网络实名制身份认证体系研究

刘彤，蒋继娅

北京市科学技术情报研究所，北京，中国，100044

e-mail: liutong@bjstinfo.com.cn, jiang_jiya@sohu.com

【摘　要】提出了一种基于组合对称密钥（CSK，Combined Symmetric Key）的网络实名制身份认证体系架构与密钥管理协议。通过组合式动态密钥产生算法和智能卡技术，实现芯片级的安全认证过程。对大规模密钥的管理简化为对小规模密钥种子的管理。提出的基于“主—从”认证中心模式的认证体系架构能够高效率地支持大规模用户的并发认证。对该认证系统的安全性进行了分析，并给出了性能测试数据。该系统的实施与应用，能够以较低的建设成本实现对大规模用户身份的识别以及管理，为我国网络实名制的研制提供了一个可行的解决方案。

【关键词】组合对称密钥；密钥管理；双向身份认证；网络实名制

1 引言

在虚拟网络社会里，网络用户没有切实证明自己身份的凭证，因此身份盗用、冒名顶替的情况屡有发生[1]。近几年网络应用蓬勃发展，随着网上办公系统、交易系统、信息服务系统的日益增多，对信息安全保障的需求也在日益增长。在互联网上实施网络实名制管理将成为一种必然的技术解决方案。

目前学术界对网络实名制的研究，主要集中在法理基础、可行性、公共政策分析等理论层面，对于其核心技术层面的研究和讨论尚不多见[2][3]。网络实名制对系统和协议的安全性、认证效率、管理用户量和并发量提出了更高的要求。要实现网络实名制，需要在保证认证协议安全的前提下，解决规模化认证和低成本认证体系的难题。

韩国自 2002 年起率先实行网络实名制，要求用户提供其真实姓名和身份证号码进行实名注册，实际上仍是基于“口令”（含静态“口令”）的身份认证。由于此技术方法是对用户的真实姓名和身份证号码等静态信息进行认证，虽然建设和维护成本不高，但在网络传递过程中易被截获并冒名顶替，因此安全性较低。

近年来，以密码技术为基础的网络身份认证产品由于其高安全性而得到了迅速发展。在当前应用较多的 PKI 公钥设施体系中，认证过程需要庞大的证书数据库在线对比认证，每 1000 多用户就要建立一级 CA 及一套数据库存放证书和密钥，数据库在线对比认证效率低、速度慢，管理用户量小。若要实现网络实名制下的规模化认证，需要多个 CA 认证中心之间交叉

基金项目：北京市科技新星计划（2006B35）

Foundation Item：Beijing Science and Technology New Star Plan（2006B35）

认证，而多级 CA 存在着可信度降低、认证效率下降等问题，其建立和维护成本都较高。为替代 PKI 提出的 IBE 技术虽然取消了建立第三方 CA 认证中心，降低了建设 CA 认证中心的成本，仍没有从根本上解决效率低、管理用户量小、运营维护成本高的问题[4][5]。我国学者南相浩教授提出的 CPK (Combined Public Key) 标识认证系统采用组合映射算法实现认证和密钥管理，为上述问题的解决提出了有益的尝试[5]。

对大规模网络用户的身份认证和海量密钥的管理是实现网络实名制的关键所在[6]。本文提出了一种基于组合对称密钥（CSK，Combined Symmetric Key）的网络实名制身份认证体系架构，对大规模密钥的管理简化为对小规模的密钥种子的管理。通过组合式动态密钥产生算法和智能卡技术，实现芯片级的安全认证过程。该认证系统的实施与应用可以提高网络系统对网络实名制要求下大规模用户身份的识别以及管理能力，是一种安全有效的认证管理体制。

2 组合对称密钥算法（CSK 算法）

组合对称密钥核心思想是给定小规模的密钥种子集合，在时间戳与随机数的参与下，通过某种映射关系将集合中的密钥进行组合计算，得到大规模的密钥集合。对大规模密钥的管理可以简化为对小规模的密钥种子的管理，从而解决了密钥管理的规模性问题[7]。

组合密钥算法需要以下列几点为基础：

(1) 确保每个用户的密钥基不一样。

(2) 由相同的密钥生成基，不同的随机数计算得到的实体密钥不同。

(3) 由不同的密钥生成基，相同的随机数计算得到的实体密钥不同。

(4) 密钥生成基的数据量有限，但由其组合计算可以到几乎无限数量的实体密钥。

组合对称密钥生成过程如下：

(1) 首先生成用户密钥种子矩阵 $K_{M\times N}$，其中 $M=148, N=16$，作为密钥的基。

$$K_{M\times N}=\begin{bmatrix} A_{10\times 16} \\ B_{12\times 16} \\ C_{31\times 16} \\ D_{24\times 16} \\ E_{60\times 16} \\ Z_{11\times 16} \end{bmatrix} \tag{1}$$

其中 $A_{10\times 16}$ 为“年”密钥种子群，$B_{12\times 16}$ 为“月”密钥种子群，$C_{31\times 16}$ 为“日”密钥种子群，$D_{24\times 16}$ 为“时”密钥种子群，$E_{60\times 16}$ 为“分”密钥种子群，$Z_{11\times 16}$ 附加密钥种子群。

(2) 根据时间戳（year 年 month 月 day 日 hour 时 minute 分）在 $K_{M\times N}$ 中进行选择相应的年、月、日、时、分密钥种子组，与附加密钥种子群组合，构成密钥种子矩阵 $K'_{16\times 16}$。

$$K'_{16\times 16}=\begin{bmatrix} A'_{year,m} \\ B'_{month,m} \\ C'_{day,m} \\ D'_{hour,m} \\ E'_{\mathrm{minute},m} \\ Z_{11\times 16} \end{bmatrix} \tag{2}$$

其中 $0\le m\le 15$。生成随机数序列 R_i（$0\le i\le 15, 0\le R_i\le 15$）作为偏移量，从 $K'_{16\times 16}$ 中选择相应元素，最终得到密钥种子矩阵 $K''_{1\times 16}$。

下面举例说明密钥种子矩阵 $K''_{1\times 16}$ 的产生过程。用户密钥种子矩阵 $K_{M\times N}$ 的行与列分别由时间戳和随机数序列进行控制。假设时间戳为“2009-07-06 10:21:15”，则“年”密钥种子群中的第 9 行被选中（假设起始时间为 2000 年），“月”密钥种子群中的第 7 行、“日”密钥种子群中的第 6 行、“时”密钥种子群中的第 10 行、“分”密钥种子群中的第 21 行依次被选中。这些被选中的行向量与附加密钥种子群 $Z_{11\times 16}$ 相组合，构成密钥种子矩阵 $K'_{16\times 16}$。然后根据随机数序列进行进一步选取。假设随机数序列为“EFA06CB125348D97”，则 $K'_{16\times 16}$ 矩阵中的 $A_{9,14}$、$B_{7,15}$、$Z_{0,13}$、….$Z_{11,7}$ 依次被选中，组合得到密钥种子矩阵 $K''_{1\times 16}$。

(1) 将 $K''_{1\times 16}$ 按行的顺序串联起来，形成字符串 KeySeed，与随机数序列 R_i 一起经过加密运算 $Em(\bullet)$，产生了此次的实体密钥 key,

$$key = Em(\mathrm{KeySeed} \parallel \mathrm{R_i}) \tag{3}$$

由算法看出，每一次密钥产生过程都是根据时间戳和随机码从用户密钥种子矩阵中进行选择，由于时间戳和随机码不会重复，因此每一次计算得到的实体密钥都不同。只要给定用户密钥种子矩阵和映射关系就可以计算出每一次的实体密钥。采用 2-3K 字节的“密钥种子”就能产生大量的密钥，密钥在的变化量为 2^{128}。因此，对大规模密钥的管理简化为对小规模的密钥种子的管理。

978-1-935068-06-8 © 2009 SciRes.

3 系统实现

在常见的双向身份认证系统中，认证服务器端需要利用一个与终端共享的秘密信息进行双向身份认证。这里存在以下两个问题：秘密信息在网络上进行传输本身存在着安全隐患；认证服务端与终端之间必须预建一个安全通道用于传输秘密信息[8]。为了解决这个问题，本文将用户的身份标识信息和该用户对应的密钥种子矩阵按照 COS（片内操作系统）规定的格式存放在该用户持有的智能卡中。在服务器端，这些信息存放在认证数据库中。这种预先部署知识的密钥分发方案既不需要在认证服务端和终端之间预建立安全通道，又能够安全地实现认证服务端和终端之间的双向认证[9][10]。

3.1 系统认证协议说明

表 1 为文中用到的符号说明。

Table 1. Signal definitions

表 1. 符号说明

符号	含义
IDa	用户 a 的身份标识（如身份证号）
IDb	认证服务器 b 的身份标识
Na	用户 a 产生的随机数，即 16 个取值在 0～15 之间的数字
Nb	认证服务器 b 产生的随机数，即 16 个取值在 0～15 之间的数字
Na*	认证服务器 b 接收到的用户 a 发送的随机数
Nb*	用户 a 接收到的认证服务器 b 发送的随机数
Ta	用户 a 产生的时间戳
Tb	认证服务器 b 产生的时间戳
Ta*	认证服务器 b 接收到的用户 a 发送的时间戳
Tb*	用户 a 接收到的认证服务器 b 发送的时间戳
Keya	保存在用户持有的 USB Key 中的用户 a 对应的密钥种子矩阵
Keya*	保存在认证服务器 b 中用户 a 对应的密钥种子矩阵，与该用户所持 USB Key 中存储的密钥种子矩阵相同
Em[M]	用密钥 m 对信息 M 进行加密
Dm[M]	用密钥 m 对信息 M 进行解密
f(M)	对信息 M 进行 f 运算(f 为双方约定的数字运算)
‖	字符串连接操作
A- B: M	从 A 向 B 发送信息 M
Comp(M1,M2)	比较信息 M1 和 M2 是否相同

3.2 认证流程

认证流程如图 1 所示。

Step 1. $A \rightarrow B : IDa$ 。

客户端计算机从用户所持的智能卡中读取该用户的用户号，发送给认证服务器。

Step 2. $B \rightarrow A : Tb \,\|\, Nb \,\|\, Em(f(Tb, Nb, Keya^*))$

服务器创建会话，认证系统验证用户号是否合法，如果合法则根据用户号从数据库中取出该用户对应的密钥种子矩阵 Keya*，并获取服务器系统时间戳 Tb，生成随机数 Nb，按照规则 f 从 Keya*中进行组合选取，生成 8 字节的身份认证信息，与 Nb 一起通过分组加密算法 $Em(\bullet)$ 生成 16 字节的服务器端认证码 SL1，与 Tb、Nb 一起组成服务器端认证参数发送给客户端。

Step3. $Comp(Em(f(Tb,Nb,Keya^*)),\ Em(f(Tb^*,Nb^*,Keya)))$，

$A \rightarrow B : Tb^* \,\|\, Na \,\|\, Em(f(Tb^*, Na, Keya))$

客户端接到服务器端认证参数后，根据 Tb*、Nb*以及加密算法 $Em(\bullet)$ 在用户的 USB 智能卡内再次生成认证码 SL2，与 SL1 比较，如果相同，则说明服务器是可信的。否则中断认证过程。在客户端确认服务器可信的情况下，客户端产生一串随机数 Na，与 Tb*一起在智能卡内产生客户端认证码 CL1，与 Na、Tb*一起组成客户端认证参数发送给服务器。

Step 4. $Comp(Em(f(Tb^*,Nb^*,Keya)),\ Em(f(Tb,Na^*,Keya^*)))$

服务器收到客户端认证参数后，通过会话标识符和时间戳判断本次会话是否仍是与客户端最初建立的那个会话（防止重放攻击）。如果不是，则中断认证过程。如果是，服务器则根据 Tb 和 Na*再次生成认证码 CL2，与 CL1 进行比较，二者若完全相同，则该用户为合法用户，登录成功；否则拒绝该用户登录。

本系统中，用户身份标识及其对应的密钥种子都存放在客户端 USB Key 中，这样，用户得到了系统分配的 USB Key 后，就相应地得到了自己所对应的密钥种子矩阵，从而解决了重要信息的分发问题。认证过程中使用的 $f(\ )$运算和 $Em(\ )$运算是固化在硬件上的，客户端的加密运算完全是在 USB Key 内这样一个安全封闭的环境中完成，实现了芯片级认证。系统采用实时组合、随机生成的方法产生用户认证码，即每一次认证都是根据时间戳和随机码从密钥种子矩阵中进行选择，并通过分组密码算法生成 16 字节的认证码，因此认证码是严格意义上的一次一变，攻击者无法预

测和跟踪认证码的生成规律，从而有效抵抗 sniffer（网络嗅探）攻击。

3.3 基于“主—从”认证中心模式的认证体系架构

基于“主—从”认证中心模式的认证体系架构如图 2 所示，认证中心的认证服务器端使用标准的 PCI

接口，与一块或多块加密卡结合（也可与加密机相连）。服务器端的认证运算就在加密卡或加密机等加密设备

中进行。WEB 服务器作为系统的主认证服务器，接收到认证请求后，和从认证服务器之间直接建立 Socket 通道，将客户端发送的认证参数分配给从认证服务器。主认证服务器（Web 服务器）对从认证服务器进行轮循发送控制。认证合格后，从认证服务器将认证结果返回到 Web 服务器，关闭 Socket。用户将被

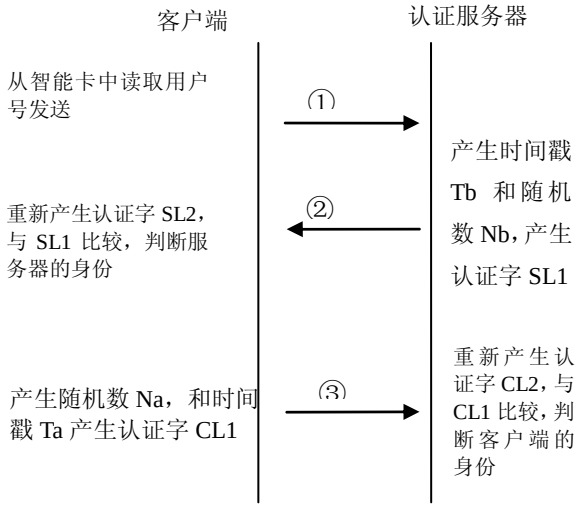

Figure 1. CSK-Based dynamic bi-directional authentication flow
图 1. 基于 CSK 的动态双向身份认证流程

Table 2. The concurrent authentication experiment result
表 2 系统并发认证测试数据

认证中心设备	1000 用户平均响应时间/秒	2000 用户平均响应时间/秒	5000 用户平均响应时间/秒	10000 用户平均响应时间/秒
1 台认证服务器,1 块加密卡	1.08	2.09	5.18	10.38
2 台认证服务器,各 1 块加密卡	0.91	1.81	4.39	8.83
3 台认证服务器,各 1 块加密卡	0.87	1.83	4.31	8.91
1 台认证服务器, 2 块加密卡	0.91	1.78	4.44	8.89
2 台认证服务器,各 2 块加密卡	0.84	1.65	4.20	8.63

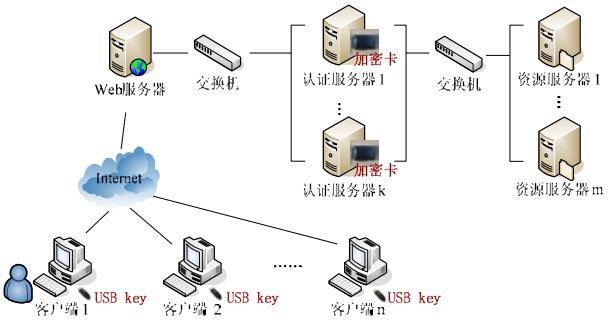

Figure 2. The master-slave authentication center model-based authentication architecture
图 2. 基于“主—从”认证中心模式的认证体系架构

允许按照相应权限访问资源服务器。实验表明：由于组合对称密钥计算量小，并且对称密码算法加密速度快，是非对称密码算法加密速度的 10 倍以上，并且在加密设备内部进行的运算速度快，这种“主—从”认证中心模式的认证体系架构能够高效率地支持大规模用户的并发认证。

为加强对重放攻击和等待重放攻击的抵御能力，系统不仅使用了挑战/应答的握手方式，还通过会话标识符和时间戳判断认证时的会话是否为服务器与客户端通过握手建立的会话。在服务器端还建有日志系统，对用户登录系统的情况进行统计、分析和管理，对同一网络用户多次使用过期的或相同的时间戳和随机码进行跟踪，发出警告并断开连接。另外，客户机向网络 Web 服务器发送身份认证请求时，在 Web 服务器端设置会话保持时间，若超过会话保持时间，用户需要重新向网络服务器端发出登录请求，从而可以防止黑客用截获到的认证口令对服务器进行攻击。

4 系统性能测试

本系统的测试在局域网环境下进行，运行平台为

978-1-935068-06-8 © 2009 SciRes.

IBM X3850 服务器，CPU2.4G，内存 4G，硬盘 146G。《中国国家应用软件产品质量监督检验中心》对采用本方案建立认证中心的性能进行了测试，获得了不同用户量并发认证所用的总认证时间，数据如表 2 所示。测试结果表明，系统运行稳定，在大用户量并发访问时响应时间比较理想。与传统基于证书的 CA 技术相比，本系统在认证效率、可管理用户量等方面均有 10 倍左右的提高，而在建设成本和维护成本方面有着显著的下降，如表 2 所示。

5 总结与展望

本文提出了一种基于组合对称密钥（CSK，Combined Symmetric Key）的网络实名制身份认证体系架构，对大规模密钥的管理简化为对小规模的密钥种子的管理。通过组合式动态密钥产生算法和智能卡技术，实现芯片级的安全认证过程。实验表明：由于组合对称密钥计算量小，并且芯片级的安全认证速度快，本文提出的“主—从”认证中心模式的认证体系架构能够高效率地支持大规模用户的并发认证。通过该认证系统的实施与应用，能够以较低的建设成本实现对大规模用户身份的识别以及管理能力，是一种安全有效的认证管理体制。具有以下 3 个创新点：

(1) 软硬件协同的身份认证。用户密钥种子集中生成并封装到硬件载体中。通过客户端和服务器端芯片内 CSK 算法生成一次一变的认证密钥，在芯片内部实现认证和对比过程，仅将结果发送到外部设备，保证了算法及密钥的安全性。

(2) 规模化的密钥管理方案。每个用户建立 M 行 N 列（M=148，N =16）密钥种子矩阵。利用时间戳和随机数共同作用的控制函数，从种子矩阵中选取参数并生成密钥。采用 2.6K 字节的“密钥种子”就能满足一位用户的认证需求，密钥的变化量为 2^{128}，将大规模密钥的存储和管理转化为对种子矩阵的存储和管理。

(3) 支持大规模用户并发认证请求的“主—从”认证中心模式的认证体系架构。主认证服务器负责认证请求的分配，从认证服务器配有加密卡（插入服务器中）或加密机，负责校验认证参数。

目前，我国正处在网络实名制的论证与核心技术的关键阶段。要实现网络实名制，必须在网络认证架构安全的前提下，解决规模化认证和低成本的难题。本文所提出的大规模认证体系架构与密钥管理方案为其提供了一个可行的解决方案。

References (参考文献)

[1] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C [M], US: John Wiley & Sons Press. 2000.16-20.

[2] LIU Dazhi, Analysis on Network Real Name System from the Perspective of Public Policy—Also on Internet Management Concept [J], Journal of Chongqing Institute of Technology (Social Science Edition). 2007, 21(8), P40-43.
刘大志.网络实名制的公共政策分析——兼论互联网的管理理念[J], 重庆工学院学报（社会科学版）,2007,21(8),P40-43.

[3] Zhang Huan, Yang Lin, Identity homologous Relation: the Legal Basis for the Real Name System for E-registration[J], Social science journal of colleges of Shanxi, Vol. 21 No.4, P97-100.
张欢,杨霖, 身份映射关系:网络实名制的法理基础[J], 山西高等学校社会科学学报.21 卷第 4 期, P97-100.

[4] Zhou Jiafa, Ma Tao, Li Yifa, Comparison and analysis of PKI、CPK and IBC [J], Journal of Information Engineering University, Vol.6 No. 3, P26-31.
周加法, 马涛, 李益发, PKI、CPK、IBE 性能浅析[J].信息工程大学学报,2005,3(6), P26-31.

[5] Denf Huifang, Deng Wen, Tian Wenchun, Zheng Dongxi, Design and implementation of CPK identity based on authentication system [J], Computer Engineering and Design, Vol.29 No.19, P4920-4922.
邓辉舫,邓文,田文春,郑东曦, CPK标识认证系统的设计及实现[J], 计算机工程与设计,Vol.29 No.19, P4920-4922.

[6] Hu Xiangyi, Zhao Guifen. A CSK-based Solution for Person Authentication [A]. In: The Seventh Wuhan International Conference on E-Business: Unlocking the Full Potential of Global Technology [C]. Wuhan, 2008, P244-249.

[7] Tang Wen, Nan Xianghao, Chen Zhong, Elliptic Curve Cryptography-based Combined Public Key Technique [J], Computer Engineering and Applications, 2003(11), P1-3.
唐文，南相浩，陈钟.基于椭圆曲线密码系统的组合公钥技术[J].计算机工程与应用，2003(11),P1-3. http://www. ietf. org/rfc/rfc3281.txt[EB/OL], 2002.

[8] Qing Sihan, Twenty years development of security protocols research, Journal of Software, 2003, 14(10), P1740-1752.
卿斯汉,安全协议 20 年研究进展[J],软件学报,2003,14(10), P1740－1752.

[9] Zhang Rui, Jiang Hua, Yang Yatao, P2PSIP authenticated key agreement scheme based on SGC-PKE [J], Journal of Beijing Elrctronin Science and Technology Institute, Vol. 16 No.4, P49-55.
张睿，蒋华，杨亚涛.一种基于 SGC-PKE 的 P2PSIP 可认证密钥协商方案[J],北京电子学院学报,2008(3), P49-55.