



基于公钥密码体制的网络认证技术

庞松涛

(浪潮集团, 北京 100142)

摘要:网络认证技术是“互联网+”行动计划应用推广的关键安全保障,基于公钥密码体制的数字签名已经成为身份与信息认证的主要手段,而数字签名有赖于认证中心(CA)及其基础设施(PKI)。目前,认证中心依然存在身份认证不能互信互认、投入高、安全控制及运维难度大等问题。提出一种在不降低安全程度的情况下,缩短公钥密码长度,实现公钥可视化的技术,这种技术可以不再完全依赖第三方的认证机构,是去除认证中心当前存在问题的一种有效途径。

关键词:数字签名;身份认证中心;可视化公钥

中图分类号:TP393

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2016072

Network authentication technology based on public key system

PANG Songtao

Inspur Group Co., Ltd., Beijing 100142, China

Abstract: Network authentication technology is the key to the application of internet plus security. The digital signature which depends on the certificate authority (CA) and PKI based on public key system is the main method for identity and message authentication. However, over the years, there are still many problems for the development of CA. The digital signature is not mutual trust and mutual recognition over the application granted by different CA. Moreover, it costs a lot to construct and maintain CA. In order to solve the above problems, one of ways for the improvement is to shorten the length of public key under the condition of not reducing the degree of security. In this way, the public key can be widely recognized under the regulations instead of the third party certification. The application of this public key technology will be an effective way to remove the existing problems of the CA.

Key words: digital signature, authentication center, visual public key

1 引言

在“互联网+”应用发展中,大量传统线下业务未来将逐步转成线上业务,为此,经济有效地为“互联网+”业务应用提供安全可靠、便捷的网络认证^[1]具有十分重要的意义。

在传统经济活动中,可以用签字、盖章来确认身份,而

在互联网虚拟世界中,目前被认为安全可靠的方式是通过数字签名^[2]来保障信息在传输过程中不被篡改和抵赖,并实现身份认证,限制非法用户访问网络资源。数字签名与书面文件签名有相同之处,数字签名可用来防止电子信息因易被修改而有人作伪、冒用别人名义发送信息、发出(收到)信件后又加以否认等情况发生。数字签名已经被广泛

用于银行的信用卡系统、电子商务系统、电子邮件以及其他需要验证、核对信息真伪的系统中。

数字签名主要是利用公钥密码技术和密码算法生成一系列符号及代码,组成电子密码进行签名,代替书写签名和印章。这种签名方法在可信 PKI (public key infrastructure, 公钥基础设施) 进行认证^[3,4], PKI 提供数据单元的密码变换,并能使接收者判断数据来源及对数据进行验证。PKI 的核心执行机构是电子认证服务提供者,通称为认证中心(certificate authority, CA)。

多年来,CA 一直承担类似网络工商局的职责,为个人、企事业单位和政府机构签发数字证书,保证了网络通信双方身份的真实、有效。但是,基于目前 CA 工作机制的网络信息身份认证发展依然困难^[5-6],身份认证各自为政,不能互信互认,网上不同应用需要由不同的 CA 颁发证书(好比每个人需要多张由不同机构颁发的身份认证证件),而且不同的认证中心还可能造成重复的 PKI 建设。显然,以上种种问题难以适应未来“互联网+”应用的高速发展。为此,本文提出利用一种可视化公钥技术,可以有效解决目前 CA 存在的短板,并且可以安全、经济、可靠、便捷、有效地实现数字签名的互信互认,对于中国“互联网+”的发展具有十分重要的现实意义。

2 基于 CA 认证技术存在的问题

当前网络认证技术完全依赖于认证中心,目前我国已有几百家大型认证中心,但大都不具备合法身份。一些行业建成了自己的一套 CA 体系,如中国金融认证中心(CFCA)、中国电信 CA 安全认证系统(CTCA)等;还有一些地区建立了区域性的 CA 体系,如北京数字证书认证中心(BJCA)、上海电子商务认证中心(SHECA)等。许多 CA 没有进行严格身份确认和验证就随意发放证书,难以保证其权威性和公正性,或存在明显的地域性和行业性,根本没有达到面向全社会的第三方认证机构的基本要求,也不利于日后更加良性地发展。目前,我国 CA 体系主要存在以下几个问题。

- 在技术层面上,参与部门很多,标准不统一,这导致交叉认证过程中出现“各自为政”的局面。这种缺乏统一标准的态势必将造成多种技术标准共存的局面,这也是目前我国众多 CA 各方割据、难以互通的一个主要原因。
- 在资金支持上,CA 建设要求达到相当标准的硬件

环境,在建设初期就需要投入大量的资金,而且在 CA 运行之后,还需要解决用户规模、用户信任、保险赔付以及保障中心长期运行的资金等一系列问题。

- 在管理上,有的地方政府把 CA 认证看成一种行政管理的手段,使认证中心的建设走上了计划经济时期条块分割和地方保护主义的老路,这与信息社会的开放性和跨地域性背道而驰。
- 在法规上,相关法律还不够健全,目前行业的混乱与相关法律和行业性规范尚未形成有很大关系,缺乏法律约束,盲目地信任某一个 CA,而不是通过一定的管理办法保证 CA 是可信的。
- 在市场运作上,存在严重的同质竞争。由于并不存在完全的不可替代性,这种竞争的结果是各家认证中心都需要通过价格战占领市场,而过于低廉的费用,不但不能够保证基本的服务,其权威性也会受到质疑。CA 企业没有动力去开发新的市场,整个行业就处于一种混乱、无序的状态。

总之,当前的数字签名所依赖的 CA 还存在种种问题,不同 CA 之间不能互认,CA 建设仍处于一种无序状态,重复建设的现象还比较严重,CA 的布局不太合理,发展不平衡,不同 CA 相互之间不协调,甚至在纵横之间产生冲突的现象还存在。这些信任“孤岛”的存在,给无边界环境下电子商务的开展带来了很大不便,给电子商务的发展也制造了障碍,因为电子商务是跨地区、跨省市、跨国界发展的。随着“互联网+”的发展需求,建立一个互认的机制将是“互联网+”推动的一个巨大挑战。

3 网络认证改进策略

公钥密码体制利用一对互相匹配的密钥进行加密、解密,每个用户拥有一把仅为本人所掌握的私钥,用它进行解密和签名;同时拥有一把公钥并可以对外公开,用于加密和验证签名。事实上,CA 的核心作用是确保公钥可信,并保证接收方通过可信公钥对发送方的信息可靠性进行验证。

现有的 CA 必须作为权威的、可信赖的、公正的第三方机构,专门负责发放并管理所有参与网上交易的实体所需的数字证书,对密钥进行有效的管理,颁发证书证明密钥的有效性,并将公开密钥同某一个实体(消费者、商户、银行)联系在一起。

显然,如果统一了认证中心,那么就不会出现上述的



各自为政等问题,建立大集中的 CA 虽然有利于认证的统一,但庞大的集中的 PKI 中心必然严重影响信息化应用的灵活性,安全风险巨大,无论在技术和管理上都难以实现;而分布式 CA 管理带来的问题就是现在的管理分隔,也在一定程度上影响信息化应用的发展。

另一种可选的方法是公钥可视化,使公钥像人名或身份证号码一样可以被识别,这样公钥就可以不用复杂的 CA 进行公证,那么,传统复杂的 PKI 就可以被极大简化甚至可以消除,大集中的 CA 也不用建立,更谈不上 CA 大集中的网络风险,从而可以保证公钥的互认互通,极大方便电子商务的身份统一认证,进一步还可以把公钥纳入现实管理体制,那么第 2 节提到的各种认证体系问题就可以迎刃而解。下面以信息认证过程为例说明网络认证的改进策略。

典型的基于 CA 的数字签名验证的过程如图 1 所示。

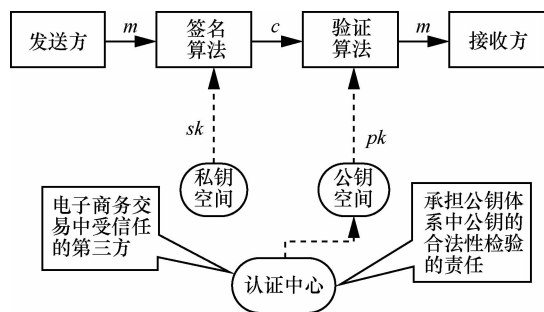


图 1 基于 CA 的数字签名验证过程

其中, m 是发送信息, c 是加密信息, sk 是私钥, pk 是公钥。

改进后的数字签名验证的过程如图 2 所示。

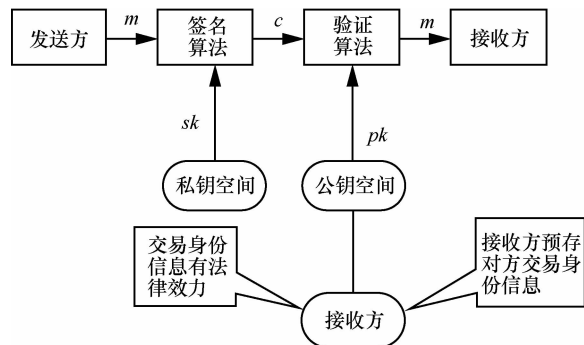


图 2 不依赖 CA 的数字签名验证过程

从以上数字签名流程可以看出,一旦公钥可视化,数字签名就很接近写在纸上的普通的物理签名,纳入现有实体管理也十分方便,从而也就可以不依赖现有的复杂的认

证中心。

4 基于短公钥的网络认证算法实现

公钥可视化的关键是可以对公钥编码^[7-10],典型的公钥加密算法有 RSA、DSA、ECC 等。RSA 算法是基于大整数素因子分解的困难性,可采用 2 048 bit 的安全密钥;DSA 算法是基于整数有限域离散对数难题,其安全性与 RSA 相似,公钥长度是 512~1 024 bit;ECC 椭圆曲线是由韦尔斯特拉斯(Weierstrass)方程所确定的平面曲线,与 RSA 相比,160 bit ECC 与 1 024 bit RSA、DSA 有相同的安全强度。显然,对于上千比特的公钥,难以对其编码,也就无法实现公钥可视化,这种公钥必须由计算机识别验证,故此公钥离不开第三方专业认证机构验证,也就是无法脱离目前的 CA 认证机制。但是,一旦公钥长度缩短到可视化,那么公钥就可以不依赖于第三方公证,从而摆脱 CA 的约束也就成为可能。

为了简化 CA 管理,国际上有人研究提出著名的基于身份的加密体制(identity-based encryption, IBE)^[11,12]方法,该方法提出使用姓名、身份证及 E-mail 等大家熟悉的用户标识作为公钥,免去了对公钥证书的依赖。这种方法在公钥简化上与本文有相同之处,但是,由于其公钥是事先确定而不是随机产生的,其安全认证有赖于私钥的统一管理,所以,该方法虽然简化了公钥管理,但私钥管理又带来严峻的安全问题,总体安全问题依然较大。近年来,有密码算法专家提出了基于阴阳环的公钥密码算法,该算法在不影响安全程度的前提下,可以缩短随机公钥长度,不仅可以摆脱对 CA 的依赖,而且安全程度明显优于 IBE。众所周知,RSA 是依赖于整数分解问题^[13,14](integer factorization problem, IFP),而基于阴阳环的公钥密码算法是采用代数数分解^[15](algebraic integer factorization, AIP),分解一个代数数,同时也分解它的范数,通过分解范数来分解一个代数数,需要解一个或多个高维丢番图方程,其难度远比分解整数难度大,所以基于阴阳环的公钥密码算法远比 RSA 复杂。使用基于阴阳环的公钥密码算法的一个显著特点是超短公钥,在同目前其他方法同样的安全程度上,其公钥长度压缩到 50~60 bit。基于阴阳环的公钥密码核心算法要点如下。

(1) 密码生成

- 建立阴阳环 $(\hat{R}, +, \cdot)$, $\hat{\theta}$ 与 $\hat{\Gamma}$ 为 $\hat{R}$ 的阴阳子集, $\hat{\theta}$ 的参数保密, $\hat{\Gamma}$ 的参数公开;

- 在 $\hat{R}$ 上定义一个范数,取值为整数;
- 随机选取 $\hat{K} \subset \hat{\Theta}$ 作为私钥;
- 选择 $\hat{P} = \{\hat{\alpha}\hat{\beta}, \hat{\alpha}, \hat{\beta} \in \hat{K}\} \subset \hat{I}$ 作为公钥。

(2)加密算法

- 把信息映射为 $\hat{m} \in \hat{I}$;
- 随机选取 $\hat{x} \in \hat{I}$,其中 $\hat{I} = \{\hat{\alpha}\hat{\beta}, \hat{\alpha} \in \hat{I}, \hat{\beta} \in \hat{P}\} \subset \hat{I}$;
- 计算 $\hat{z} = \hat{x} + \hat{m} \in \hat{I}$ 作为密码。

(3)解密算法

在特定条件下,可通过求解 $\min_{\hat{x} \in \hat{I}} \|\hat{z} - \hat{x}\|$ 来获得 $\hat{x}$ 和 $\hat{m}$,进而还原信息明文。

对于 50~60 bit 的公钥,如果从 GB2312 中选取 4 096 个中文对其编码,编码也就 5 个汉字。也就是说,采用基于阴阳环的公钥密码算法,其公钥也就 5 个汉字。显然,这种编码非常容易辨别,也就是可视化,而且这 5 个汉字还可以保证公钥的唯一性,因为每个汉字有 4 096 种选择,5 个汉字可以形成多于 11 亿亿个编码。

综上所述,采用短公钥技术,可以实现公钥的可视化。从而可以使公钥不需要第三方的公证,实现公钥的互信互认,这种方案是公钥机制非常有意义的选择,也是未来公钥技术发展的可行方向之一。

5 实验与结论

基于阴阳环的公钥密码算法是采用代数数分解,算法难度远高于现有的 RSA、DSA,由于其加密原理涉及密码学的深入知识,本文从应用角度不作深入探讨,但是,能够实现公钥可视化必然是公钥技术创新及突破发展。以下针对基于阴阳环公钥技术的可应用性,也就是密钥的响应性能进行测试。

表 1 给出的测试数据是在一台 PC 上获得的,其中第一列给出的是私钥对于 RSA 的折合长度 N ,单位为 bit;其余

各列给出的分别是密钥生成(genKey)、签名(sign)、签名验证(verify)、加密(encrypt)和解密(decrypt)算法的平均耗时,单位为 ms。根据表 1 中的数据绘制的算法性能曲线(相对于 N)如图 3 所示。从表 1 和图 3 中可以看出,即使 N 增大到 64 KB(65 536 bit),各算法的速度依然在可接受的范围内。

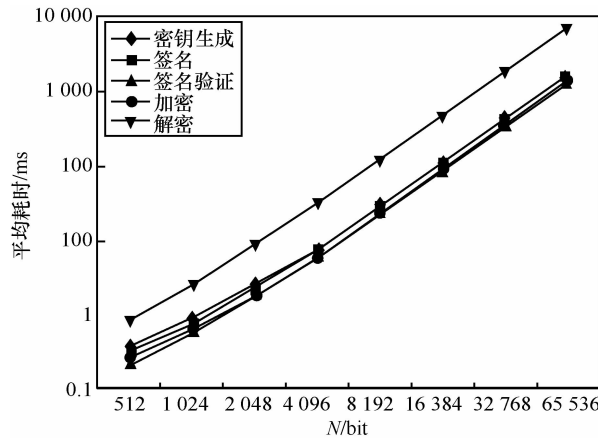


图 3 基于阴阳环的公钥密码技术实现技术性能

6 结束语

数字签名技术是网上交易、电子商务的重要环节。CA 为数字签名提供了认证和管理保障,但由于 CA “各自为政”,造成数字签名互信互认依然困难,而且数字签名的认证与管理保障体系的投入建设费用很高,《电子政务服务管理办法》规定,电子认证服务机构必须具备独立企业法人资格,人员不得少于 30 人,资金不低于 3 000 万元。这些问题对于“互联网+”行动计划的发展推动都有一定的影响。所以发展改善现有 CA 机制非常必要,笔者认为,缩短公钥长度,实现公钥编码化并纳入现有管理体制,可以解决现有 CA 存在的问题,有效实现数字签名的互信互认,同时大大节省 CA 开销,是未来网络认证技术发展的一种不错的发展方向。

表 1 基于阴阳环的公钥密码技术实现原型测试数据

长度 N/bit	密钥生成平均耗时/ms	签名平均耗时/ms	签名验证平均耗时/ms	加密平均耗时/ms	解密平均耗时/ms
512	0.37	0.31	0.21	0.26	0.9
1 024	0.87	0.75	0.56	0.61	2.46
2 048	2.45	2.21	1.76	1.75	8.28
4 096	7.12	7.57	6.12	5.92	30.34
8 192	27.34	28.15	23	21	113.12
16 384	104.56	109.29	88.04	79.95	445.5
32 768	395.29	428.39	355.48	320.53	1 766.29
65 536	1 608.85	1 682.18	1 363.45	1 229.76	6 994.45



参考文献:

- [1] 吕金刚, 王永杰, 鲜明. 计算机网络信息安全技术分析[J]. 中国新通信, 2006(15): 21-25.
LV J G, WANG Y J, XIAN M. Analyzing on techniques of computer network information security [J]. China New Telecommunications, 2006(15): 21-25.
- [2] ATREYA M. 数字签名[M]. 北京: 清华大学出版社, 2003: 161-170.
ATREYA M. Digital Signature[M]. Beijing: Tsinghua University Press, 2003: 161-170.
- [3] 肖凌, 李之棠. 公开密钥基础设施(PKI)结构[J]. 计算机工程与应用, 2002(10): 137-139.
XIAO L, LI Z T. Architecture of PKI[J]. Computer Engineering & Applications, 2002(10): 137-139.
- [4] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京: 电子工业出版社, 2008: 216-229.
GUAN Z S. Publication Key Infrastructure PKI and the Applications [M]. Beijing: Publishing House of Electronics Industry, 2008: 216-229.
- [5] 张锐, 莫平. PKI/CA 技术在电子政务安全体系建设中的应用研究[J]. 中国信息安全, 2014(7): 30-32.
ZHANG R, MO P. Application research of PKI/CA technology in e-government security system construction [J]. Computer Security, 2014(7): 30-32.
- [6] 赵可. PKI/CA 技术在电子政务信息安全领域的运用探索[J]. 科技传播, 2014(4): 116-123.
ZHAO K. Application exploration of PKI/CA technology in the field of e-government information security [J]. Public Communication of Science & Technology, 2014(4): 116-123.
- [7] 卢开澄. 计算机密码学 [M]. 北京: 清华大学出版社, 2003: 216-221.
LU K C. Cryptography [M]. Beijing: Tsinghua University Press, 2003: 216-221.
- [8] 曾福庚. 公钥密码学的研究与发展[J]. 科技信息, 2010(18): 11.
ZENG F G. Research and development of public key cryptography[J]. Science and Technology Information, 2010(18): 11.
- [9] WASHINGTON W T L C. 密码学概论 [M]. 许鹏文, 邹红霞, 李勇奇, 译. 北京: 人民邮电出版社, 2004: 153-162.
WASHINGTON W T L C. Introduction to Cryptography with Coding[M]. Translated by XU P W, ZOU H X, LI Y Q. Beijing: Posts and Telecom Press, 2004: 153-162.
- [10] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]//International Conference on the Theory and Application of Cryptographic Techniques, May 14-18, 2000, Bruges, Belgium. Berlin: Springer Berlin Heidelberg, 2000: 139-155.
- [11] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//CRYPTO 84. Berlin: Springer Berlin Heidelberg, 1985: 47-53.
- [12] BONEH D, FRANKLIN M. Identity based Encryption from the Weil pairing [C]//The 21st Annual International Cryptology Conference, August 19-23, 2001, Santa Barbara, California, USA. Berlin: Springer Berlin Heidelberg, 2001: 213-229.
- [13] 胡云. RSA 算法研究与实现 [D]. 北京: 北京邮电大学, 2010: 168-175.
HU Y. Research and implementation of RSA algorithm [D]. Beijing: Beijing University of Posts and Telecommunications, 2010: 168-175.
- [14] KMIOKA T, SHIMIZU A. The examination of the security of SAS one-time password authentication [R]. IEICE Technical Report, 2001: 156-161.
- [15] NEUKIRCH J. Algebraic Number Theory [M]. Berlin: Springer Berlin Heidelberg, 1999: 267-298.

[作者简介]



庞松涛(1972-),男,浪潮集团副总裁,中国电机工程学会电力信息化专委会委员。历任卡西欧浪潮电子有限公司通信事业部副部长,山东浪潮商用系统有限公司市场部部长,浪潮电子信息产业股份有限公司西南大区总经理、西北大区总经理,浪潮电子信息产业股份有限公司市场推进部总经理、渠道发展部总经理、市场管理部总经理等职。主要从事云计算、服务器及行业管理工作。