

一种新型匿名认证方案的研究

刘东升^{1,2}, 田 浩¹, 林玉铃¹

(1 浙江工商大学 计算机与信息工程学院, 浙江 杭州 310018; 2 浙江工商大学 现代商贸研究中心, 浙江 杭州 310012)

摘 要: 为了克服现有可信平台认证方法的缺陷, 提出了一种基于单项累加器的新型可信平台匿名认证方案, 并构造了具体方法. 新方案利用环签名技术的匿名性实现直接匿名认证, 同时运用单向累加器技术将环签名成员信息累加, 使得签名环长度固定, 不会随着环规模增大而增大. 验证时, 有效降低了 hash 计算和加密、解密运算的次数, 提高了认证的效率. 通过与典型的环签名方案的比较, 表明该方法所需的空間复杂度和时间复杂度更小, 并弥补了传统环签名方案签名长度随环规模增大而增加的缺点, 在保证安全性的前提下具有较高的实现效率.

关键词: 可信计算; 匿名认证; 单向累加器; 环签名

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2011)05-0157-05

Research on a New Anonymous Authentication

LIU Dong-sheng^{1,2}, TIAN Hao¹, LIN Yu-ling¹

(1 College of Computer Science & Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China;

2 Center for Studies of Modern Business, Zhejiang Gongshang University, Hangzhou 310018, China)

Abstract: Aimed at overcoming the limitations of current authentications on trusted platform, this dissertation puts forward an improved method based on one-way accumulator, and constructs its solution in detail. New solution introduces ring signature to protect client's privacy with ring signature's anonymity, what's more, the ring length is fixed by the one-way accumulator which accumulates all the members' information so that the ring won't be too large with considerable members. During validation, the efficiency is promoted for the diminishment of the hash-compute times, encrypt-compute times and decrypt-compute times. Compared to existing ways of authentication, it indicates that new solution has lower time complexity and space complexity. At the same time, new solution guarantees anonymity and effectiveness, in addition to it makes up traditional ring-signature's weakness mentioned above; it has high efficiency on the premise of security.

Key words: trusted computing; anonymous authentication; one-way accumulator; ring signature

1 引言

可信计算技术提供了一套全新的信息安全解决方案. 可信平台的推动组织 TCG (Trusted Computing Group) 给出了实现的具体思路: 首先建立起一个可信度量根 CRTM (Core Root of Trust for Measurement), 在此基础上逐级认证, 从硬件平台扩展到操作系统, 进一步到各种应用软件, 最终扩展到整个计算机系统, 从而确保整个计算机系统的可

信^[1]. 远程证明 (Remote Attestation) 是可信计算的基本特征之一. 可信计算可以通过远程证明这一机制, 实现对接入终端的安全性检验. 根据 TCG 的规范文档^[2], 服务端通过检测远程计算机平台的完整性实现证明从而确定信任. 但服务端在进行安全检测时, 终端必须提供平台的各种配置信息, 侵犯了终端的隐私. TCG 出于这一点的考虑, 引入了身份验证密钥 (Attestation Identity Keys) 来保护可信平台模块的签名密钥 Endorsement Key, 从而隐藏平台的身份信息. AIK 的引入保护了可信平台内部的

收稿日期: 2010-07-16; 修回日期: 2010-08-20

基金项目: 国家自然科学基金项目 (71071140); 浙江省自然科学基金项目 (Y1090617); 浙江科技计划项目 (2009C13052)

EK 身份安全,但还是没有考虑平台配置信息的隐私暴露问题.近年来,保护计算平台的隐私信息得到了广泛的关注.

文中指出了现有解决方案及其不足之处,在详细分析了环签名方案流程和单向累加器特点等基础上,提出一种基于单向累加器的环签名可信平台匿名认证方法,该方案在引入环签名解决可信平台远程认证的隐私保护之上,还利用单向累加器技术克服了环签名方案的瓶颈问题:传统环签名方案的效率往往随着环规模的增大而下降.首先简述整个可信平台远程证明的现状及其存在问题,随后介绍了新方案的相关理论基础.接着详细阐述了基于单向累加器的环签名可信平台匿名认证方法并在第四节详细的证明了其安全性和有效性.第五节总结全文,并提出后续的研究方向.

2 现有方案

2.1 可信第三方机制

针对远程证明隐私保护问题,TCG 在公布的 1.1 版本中采用了基于可信第三方的模型(Trusted Third Party,即 Privacy CA)来避免平台的身份信息泄露. Privacy CA 知道所有合法 TPM 的 EK 公钥,当一个 TPM(Trusted Platform Module)需要向另一方证明自己的可信性与真实性时,就产生 AIK 的密钥对,并将之发送给 Privacy CA,用 EK 认证这个公钥.因为 Privacy CA 是掌握所有合法 TPM 的公钥的,它就从自己的密钥列表中检查是否有需要的 EK,如果找到了,就在 AIK 上发放证书并用 EK 加密,只有拥有了 EK 私钥的 TPM 才能解密该证书,TPM 就以通过这个证书给验证方证明自己.

TPP 模型的缺点显而易见:

(1) 难以避免恶意攻击者发起的拒绝服务攻击.出于安全角度考虑,TPM 每次需要证明自己身份时,都不得不重新向 Privacy CA 发起 AIK 认证申请.因此,Privacy CA 不能拒绝短时间内的连续认证请求,而如果有攻击者连续发送大量垃圾 AIK 证书申请时,就会造成 Privacy CA 无法正常工作.

(2) Privacy CA 的角色没有合适的一方能够扮演.对于用户来说,Privacy CA 不能有服务提供商运营,否则个人隐私难以得到保证;对于服务提供商而言,Privacy CA 不能由用户运行,否则合法身份不能得到认证.

2.2 直接匿名认证方案

DAA(Direct Anonymous Attestation)认证方

案是 TCG 在其公布的 1.2 规范中采用的方法,它基于了 Camenisch-Lysyanskaya 签名机制,吸收了群签名、身份托管等技术的优点,在实现验证用户身份的同时,又保护了用户隐私^[3],其根本思想是运用了零知识证明(Zero Knowledge Proof).在零知识证明中,一个人无需揭开某个秘密也可以向其他人证明自己知道这个秘密,其数学理论基础是基于离散对数的困难性和同余类的问题.

DAA 方案包括如下步骤:

(1) DAA 发行商公布其公钥 n, a, b, d , 其中 n 是 RSA 算法的模数, x 为信息上的签名. 满足:

$$c^e = a^x b^d \mod n$$

(2) TPM 签署公钥 $DAA = a^x \mod n, x$ 是 TPM 的密钥;

(3) 取随机数 S' , 计算 $c' = c b^{S'} \mod n$, 将 c' 发送给验证方;

(4) 验证者计算 $S + eS' = s''$, 并代入 $d = c'^e a^{-x} b^{-s''} \mod n$, 如果等式成立, 则说明 TPM 掌握 c, e, s'' 的内容, 即请求方存在可信平台, 是安全的.

DAA 很好的满足了可信计算的认证要求以及用户信息的保密要求,但由于其计算过程相当复杂,有大量的模幂运算,并且涉及到很多远超 1024 位的大数运算,TPM 资源有限,计算能力有限,一般只能支持最高到 1024×1024 的计算.即使采用一些加速签名或解密的算法,如 CRT(Chinese Remainder Theorem),也依然很难将大数全部降到 1024 位以下,因此就目前的技术水平来看,在 TPM 硬件芯片没有突破发展的情况下,DAA 几乎难以实现.而与此同时,环签名技术在密码学界掀起研究热潮,鉴于环签名技术能高效的实现匿名签名,可信计算领域的专家学者开始尝试将环签名技术应用到远程证明中,并取得了一定的研究成果,然而环签名的效率随着环规模增大而降低的问题却始终存在.

3 新方案

3.1 相关理论基础

3.1.1 单项累加器技术

定义:安全的单向累加器函数是一个有限的函数集合 $h_k: X_k * Y_k = Z_k$, 满足:

① 计算有效性:存在多项式 P , 对每一个给定的整数 K , 对于所有的 $x \in X_k$ 以及所有的 $y \in Y_k$, $h_k(x, y)$ 是在时间 $P(k)$ 内可计算的.

② 单向性:不存在一个多项式 P , 对于任意给定的 $(x, y) \in X_k \times Y_k$, 使得存在一个概率多项式时间

算法 A_k , 能够满足 $h_k(x, y) = h_k(x', y')$, $x' \in X_k$ 且 $x' \neq x$ 成立的概率小于 $1/P(k)$.

③ 准交换性: 对于所有 $x \in X_k, y_1, y_2 \in Y_k$, 有 $h_k(h_k(x, y_1), y_2) = h_k(h_k(x, y_2), y_1)$ 成立.

单向累加器允许一组数据按照不同的顺序累加计算而仍然得到相同的结果, 其安全性保证了找到 $h_k(x, y) = h_k(x', y')$ 是困难的, 它的这些特性可以起到数字签名的作用. Benaloh 和 Mare 在文献[4]中提出了一个单项累加器的具体构造方案, 并且证明了该单项累加器在强 RSA Assumption 下是安全的, 定义为 $h(x, y) = e_n(x, y) = x^y \bmod n$; $e_n: QR_n \times Z_n^* \rightarrow QR_n$, p, q 为两个大素数, 满足 $(p-1)/2$ 和 $(q-1)/2$ 均为大素数, $n = pq$.

3.1.2 环签名技术

环签名是一种新型的签名者模糊(Singer-ambiguous)的无条件数字签名方案, 由 Rivest 等人在 2001 年的亚密会上提出的, 鉴于签名中的参数根据一定的规则首尾相连, 故将这种签名形象的称为环签名^[5]. 在环签名方案中, 不需要其他用户真正参与, 而只需得到其他成员的公钥形成签名环即可, 因此签名人可以自己指定匿名范围, 并且被指定的用户都不必同意或知晓. 签名者将自己的身份信息隐藏在签名环中, 并且提供签名环的公钥以证明自己属于签名环成员.

从环签名被提出到现在, 吸引了世界范围内各国学者的注意力. 2002 年, Masayuki Abe 等人提出了使用不同签名方案产生公钥来构造 1-out-of- n 签名. Fangguo Zhang 等人将给予身份的密码体制和双线性对用于构造基于身份的环签名方案. Emmanuel Bresson 等人提出了门限环签名的概念. Noni Naor 提出了可否认的环签名认证方案. 2003 年, Willy Susilo 等人在文献[6-8]的基础上提出了非交互的可否认认证方案. Javier Herranz 等人提出了源于环签名方案安全性证明的分成引理. Fangguo Zhang 等人引入代理签名, 提出了代理环签名的概念. Duncan S. Wong 等人提出了另一种构造环签名的方案: Ree-Solomn code 构造法, 并给出了相应的门限方案. 2004 年 Joseph K. Liu 与 Patrick P. Tsang 等人详细讨论了签名人身份的关联问题. Tony K. Chan 等人提出了盲环签名的概念. 接下来的几年里, 门限环签名方案得到了进一步研究, Joseph K. Liu 针对密钥泄露问题首次提出了前向安全的环签名和密钥封装的环签名方案. 在世界各国学者的潜心研究下, 环签名方案得到了长足

的发展. 但环签名一直局限在传统签名应用如电子现金系统, 电子支票系统等方面, 而环签名的诸多特性恰恰满足了匿名认证的相关要求, 针对环签名在匿名认证领域的研究也开始成为学者关注的对象.

根据 Rivest 等人的描述, 签名环完整的描述性定义如下^[5]:

签名环(Ring-Sign): m 为待签名消息, 用户 A_s 想要建立一个签名环, 他先选择加入的成员 $A_1, \dots, A_n$, 并执行一个概率算法构建一个集合 $L = \{P_i\}$, 每一个 P_i 与 y_i 有关, sk_s 为签名者的私钥.

确定对称密钥 $k: k = h(m)$.

初始化: 签名者选择初始值 $v \in_R \{0, 1\}^b$.

确定 $x_i (i = 1, 2, \dots, n, i \neq s)$: 签名者为环内其他成员随即的选择 $x_i \in_R \{0, 1\}^b$, 并计算 $y_i = g_i(x_i)$.

求解 y_s : 代入环方程 $c_{k,v}(y_1, \dots, y_n) = v$ 中求解出 y_s , 此时就可以得到环签名 $\sigma = \{v, L, y_1, \dots, y_n\}$

环验证(Ring-Verify): 计算输入 $y_i = g(x_i)$, $i = 1, 2, \dots, n$, 验证计算 $k = h(m)$, 然后将消息 m 和签名 σ 以及环中各个成员的公钥, 如果合法就输出"True", 否则输出"False".

3.2 方案细节

新方案在改进现有环签名方案的基础上引入了单项累加器技术, 提出一种基于单项累加器的新型环签名匿名认证方案, 共分为三个阶段: 初始化阶段、签名阶段、交互验证阶段.

初始化阶段和签名阶段完成整个匿名身份验证的准备工作 and 签名过程, 如图 1 所示.

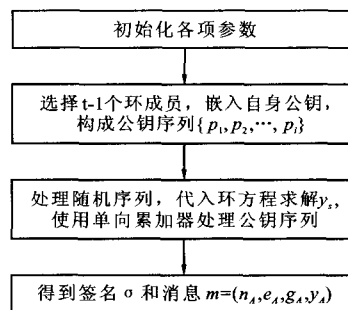


图 1 初始化和签名阶段

在完成消息签名之后, 进入交互阶段完成匿名身份认证, 通过终端与服务器之间的三次数据交换, 直接完成认证, 其主要流程如图 2 所示.

3.2.1 初始化阶段

设存在两个可信平台 A, B , A 需要向 B 提供认证. 算法以 RSA Assumption 为前提, 可信平台 A 选择两个互异的大素数 PR_1, PR_2 . $n_A = PR_1 PR_2$, e_A

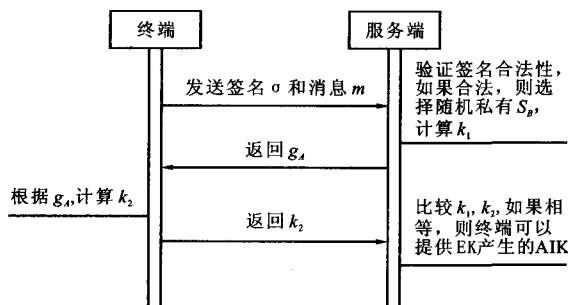


图2 交互验证阶段

$= (PR_1 - 1)(PR_2 - 1)$, 公共参数 g_A 为 $Z_{n_A}^*$ 的高阶元, 同时选择公私钥对 (e_A, d_A) . H 为安全单向累加器, 有随机序列 $x_1, x_2, \dots, x_{s-1}, x_{s+1}, \dots, x_t$; h, hv 以及 hs 均为抗碰撞散列函数.

3.2.2 签名阶段

平台 A 此时随即选择 $t-1$ 个其他可信平台的公钥信息, 并将自身嵌入其中形成环, 构建环签名, 然后将自身的 TMP 信息签名, 发送给另一个可信平台. 具体步骤如下:

步骤 1: 可信平台 A 选择 $t-1$ 个可信平台公钥, 与自身的公钥 p_i 构成序列 $\{p_1, p_2, \dots, p_t\}$;

步骤 2: 令 $h = \{0, 1\}^* \rightarrow \{0, 1\}^l, l = rd, r$ 为指定散列化后的比特数, d 为第 3 步中的块长. 计算 $y_i = h(x_i), i \neq s$, 得 $y_1, y_2, \dots, y_{s-1}, y_{s+1}, \dots, y_t$;

步骤 3: 将 y_i 按每 d 位一组, 共划分为 r 组, 得 $y_{i1}, y_{i2}, \dots, y_{ir}$, 逐个计算 $y_{ij} = (y_{ij} \oplus \{0, 0\}^d) \oplus 1 : 0$, $\oplus$ 为逐比特异或运算, 重新计算 y_i 的值则有 $y_i = y_{i1} * 2^{r-1} + y_{i2} * 2^{r-2} + \dots + y_{ir} * 2^0 = \sum_{j=1}^r y_{ij} * 2^{r-j}$, 此时获得散列后位长为 r 的序列 $y_1, y_2, \dots, y_{s-1}, y_{s+1}, \dots, y_t$;

步骤 4: 选择初始值 v , 环签名 $\sigma = H(H(p_1, H(\dots), p_t))$, 环方程沿用 Rivest 在文献[5]中提出的方程 $C_{k,v}(y_1, y_2, \dots, y_t) = E_k(y_t \oplus E_k(y_{t-1} \oplus E_k(\dots \oplus E_k(y_1 \oplus v) \dots))) = v$. E_k 为对称加密算法, $k = hs(m, p_1, p_2, \dots, p_t)$. 根据环方程, 利用 E_k 的对称解密算法 D_k 可以得到 y_s , 同时求得 $x_s = h^{-1}(y_s)$;

步骤 5: 可信平台 A 由 EK 生成一个 AIK, 记为 δ , 并选择一个私有信息 s_A , 计算 $y_A = (g_A^{s_A} - hs(\delta, y_1, y_2, \dots, y_t))^{d_A} \bmod n_A$. 签名的信息 $m = (n_A, e_A, g_A, y_A)$;

步骤 6: 可信平台 A 发送签名 σ 和信息 $m = (n_A, e_A, g_A, y_A)$ 到平台 B, 开始交互验证.

3.2.3 交互验证阶段

可信平台 B 在接收到平台 A 发送的消息和签名

之后, 旋即展开交互式验证:

① 验证签名的合法性, 若签名非法, 则拒绝请求, 反之进行下一步操作;

② 随机选择私有信息 s_B , 并计算 $k_1 = hv(y_A^{e_A} + hs(\delta, y_1, y_2, \dots, y_t))^{s_B}$, 同时返回 $g_A^{s_B}$;

③ 可信平台 A 在接收到 B 的返回信息之后, 计算 $k_2 = hv((g_A^{s_B})^{e_A})$ 并返回结果给 B;

④ 平台 B 接收 A 返回的 k_2 , 考察 $k_2 = k_1$, 如果成立, 则表明平台 A 拥有 TMP 的密钥, 反之则判定平台 A 无法提供由 TMP 平台 EK 产生的身份认证密钥.

4 性能分析

4.1 便捷性分析

本方案继承了标准环签名方案拥有的优点, 签名发起人只需获取环内所有成员的公钥信息即可构建签名环, 无需环成员同意或协助, 亦无需管理员角色维护整个系统, 环中的组织结构自由. 相对于可信第三方认证机制而言, 本方案无需第三方认证机构存在, 实现了终端与服务端的直接认证. 相对于直接匿名认证而言, 本方案无需进行大规模的模幂运算, 使得在现有可信平台计算能力的基础上能够相对便捷的加以实现. 同时, 得利于单向累加器技术的引入, 本方案可以在环成员个数变化的情况下使环签名的长度为定值, 不仅提高了签名效率, 也提高了方案的便捷性.

4.2 安全性证明

4.2.1 正确性:

考察验证阶段, 有

$$k_1 = hv((y_A^{e_A} + hs(\delta, y_1, y_2, \dots, y_t))^{s_B})$$

$$y_A = (g_A^{s_A} - hs(\delta, y_1, y_2, \dots, y_t))^{d_A} \bmod n_A$$

则可以得到

$$k_1 = hv((y_A^{e_A} + hs(\delta, y_1, y_2, \dots, y_t))^{s_B}) = hv((g_A^{s_A})^{s_B}) = hv((g_A^{s_B})^{e_A}) = k_2$$

证毕.

4.2.2 匿名性

在环签名的生成过程中, 因为 $x_1, x_2, \dots, x_{s-1}, x_{s+1}, \dots, x_t$ 序列是随机选择的, 因而 $y_i = h(x_i), i \neq s$, 得到得 $y_1, y_2, \dots, y_{s-1}, y_{s+1}, \dots, y_t$ 也是随机的, 由于签名环内的任意一个成员都可以生成这样的签名, 因此除签名发起人之外, 任何人都无法确定真正的签名者. 就算存在攻击者非法获取了所有环内成员的私钥信息, 也依然难以确定签名人, 其理论概率

不超过 $\frac{1}{n}$,这里的 n 为环内成员的个数.

4.2.3 不可伪造性

通过反证法证明. 假设有一个攻击者成功攻破了新签名方案,也就是攻击者获得了签名者的 AIK 信息,也就是攻击者利用签名消息 $m = (n_A, e_A, g_A, y_A)$ 计算并得出了 $\delta = hs^{-1}(g_A^{\delta_A} - y_A^{\delta_A})$,那么攻击者也就了解了解 e_A, n_A 这两个大素数,这与前提条件,即 RSA Assumption 矛盾,因此假设不成立,不可伪造性得证.

4.3 有效性分析

签名高效性. 环签名中方案的匿名性与环成员的个数成正比,但传统的签名方案在环成员群体增大时效率显著降低,本方案引入单向累加器技术使得签名长度固定并且较小,相对于传统签名方案,效率明显提升. 表 1 为本方案与普通环签名方案的计算复杂度分析比较. 包括幂指运算(PE Operation)、散列运算(Hash Operation)、加密解密运算(ED Operation).

表 1 新方案与普通环签名方案的比较

方案名称	阶段	运算次数		
		PE	Hash	ED
普通环签名	签名	0	t^2	t
	验证	0	t	t
新方案	签名	2	$t+1$	t
	验证	2	1	0

从表 1 看出通过引入单向累加器技术使新方案在签名环节将计算复杂度由 $O(n^2)$ 下降到 $O(n)$,加密、解密操作也相应减少. 虽然在签名和验证环节多了幂指运算,但由于计算次数是常数,不会随着环规模改变而影响方案效率. 可以看出,新方案的效率得到了较大的提高.

5 结束语

基于单向累加器的新型可信平台匿名认证机制通过引入单向累加器技术有效的解决了传统方案中环签名效率随环规模增大而降低的问题,提出了一个基于 RSA 假设的新型环签名方案. 实现了可信计算中的匿名认证过程,继承了环签名的长处,吸收了

单向累加器技术的优点. 在保证方案安全性的前提下,具有较高的执行效率. 然而,由于签名发起是无条件的,并且具有匿名性,签名人可以诬陷其他非真实的签名人;另外,由于环成员系任选,方案对于选择群公钥攻击无法抵抗;此外安全抗碰撞散列函数的构建,也成为影响签名方案效率的重要因素,这些问题都是今后面临的挑战.

参考文献:

[1] 徐明迪,张焕国,严飞. 基于标记变迁系统的可信计算平台信任链测试[J]. 计算机学报,2009,32(4):635-645.

[2] Trusted Computing Group. TCG specification architecture overview [Z]. Specification 11. 4[S]. Oregan, USA: TCG, 2007.

[3] 刘吉强,赵佳,赵勇. 可信计算中远程自动匿名证明的研究[J]. 计算机学报,2009,32(7):1304-1310.

[4] Benaloh J, Mare M. One-way accumulators a decentralized alternative to digital signature[C]// EuRocrypt'93 Lofthus, Norway: Computer Science, 1993: 274-285.

[5] Rivest, Shamir A, Tauman Y. How to leak a secret [C]//Advance in Cryptology: ASIACRYPT 2001, Lecture Notes in Computer Science 2248. Bedm: Spdngeg 2001:552-565.

[6] Zhang F G, Kim K. ID-based blind signature and ring signature from pairings[C]// Proc ASIACRYPT'02. Berlin Heidelberg: Springer-Verlag, 2002:533-547.

[7] Bresson E, Stern J, Szydlo M. Threshold ring signatures and applications to ad-hoc groups[C]// Proc CRYPTO'02. Santa Bardara, CA, USA:Springer-Verlag, 2002:465-480.

[8] Naor M. Deniable ring authentication[C]// Proceedings of the 22nd international Advances in Cryptology - Crypto'02. Springer-Verlag, 2002:481-498.

作者简介:

刘东升 男,(1974-),博士,副教授. 研究方向为电子商务、智能信息处理.

田 浩 男,(1989-),本科生. 研究方向为信息安全、可信计算.

林玉玲 女,(1989-),本科生. 研究方向为信息安全、数据挖掘.