可信 DRM 中直接匿名认证的应用研究

岳宝玲,张功萱,李 晨,贺定龙

(南京理工大学计算机科学与工程学院,江苏 南京 210094)

[**摘要**] 数字版权管理(DRM)技术一直致力于数字内容的保护,特别是防止售后非法使用. 而所依靠的密码学保护措施很容易被攻击和破解. 为了在硬件方面加入保护,可信 DRM 引入了 TPM 安全芯片,借助 TPM 在身份认证、许可授权等方面加强保护. 为了解决身份认证时用户隐私泄露的问题,可信 DRM 采用了直接匿名认证协议. 在此基础上提出了基于零知识认证和 ElGamal 算法的双随机数签名的改进方案,并介绍了该方案在可信 DRM 中是如何应用的. 最后经过分析得出该方案在安全性和匿名性方面都有所提高.

[**关键词**] DRM,可信 DRM,TPM,零知识认证,ElGamal 算法

[**中图分类号**]TP393 [**文献标志码**]A [**文章编号**]1001-4616(2014)01-0112-05

Application of Direct Anonymous Attestation in Trusted DRM

Yue Baoling, Zhang Gongxuan, Li Chen, He Dinglong

(Department of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: Digital Rights Management (DRM) is a technology to protect digital contents from illegal usages after sale. DRM depends on soft cryptography protection, which is a weak protection against hackers. Trusted DRM applied TPM security chip to improve protection in terms of hardware for authentication, licensing and other aspects. To overcome the problem of user privacy, trusted DRM used direct anonymous authentication protocol. On this basis, this article proposed an improved protocol based on zero-knowledge proof and ElGamal signature algorithm of double random numbers, and then described its application in trusted DRM. The proposed technique could improve security and anonymity in DRM.

Key words: DRM, trusted DRM, TPM, zero-knowledge proof, ElGamal algorithm

随着互联网技术的快速普及,人们生活中使用的数字产品越来越多,如最新上映的电影、最流行的音乐歌曲、最专业的电子书籍等. 生产者和销售者可以通过这些数字产品的版权获得利益. 但是随着盗版业越来越猖獗,那些盗版者利用复制、修改等手段疯狂地窃取内容来传播甚至贩卖,这些非法的行为严重地危害了数字产品作者的利益. 因此人们迫切地需要一种技术来改变这一现状.

在这一背景下,数字版权管理(Digital Right Management, DRM)技术便应运而生. 文献[1]对 DRM 做如下定义:DRM 是对有形和无形资产所有版权使用形式的描述、标识、交易、保护、监视和跟踪,也包括对版权所有者之间的关系的管理. 在目前大部分的 DRM 系统中,绝大多数的攻击发生在客户端. 不仅因为客户端承担数字内容解密、权限验证这两方面的责任,同时也因为采用的传统加密或者数字水印技术很脆弱,很容易被攻破. 因此,在硬件方面加强保护就显得尤为重要. 可信 DRM 加入了硬件保护,利用可信平台模块 TPM 来增加安全性. TPM 通常嵌入在计算机主板上,具有物理防篡改、密码安全运算等特点,内部集成了随机数产生器、密码协处理器等一系列安全模块.

与此同时,由身份认证带来的用户隐私问题也引起了社会广泛关注. 目前,生活中使用最广泛的身份认证方式是“用户名/密码”登录方式,这种方式虽然操作简单便于记忆,但是很容易被破解,容易被不法之徒获取到用户隐秘信息. 因此,对用户进行身份认证的同时保护用户隐私十分重要. 可信 DRM 利用 TPM 进行匿名认证,这样使得身份认证不仅更加隐秘安全,也更加高效.

收稿日期:2013-10-20.

基金项目:国家自然科学基金(61272420).

通讯联系人:岳宝玲,硕士研究生,研究方向:Web Services 和信息安全. E-mail:756291527@qq.com

1 预备知识

1.1 DRM 系统组成

目前,国内外不同领域已经推出了不同的 DRM 系统,比较出色的是:国外的 eBook DRM 系统:Microsoft DAS、Adobe Content Server;针对流媒体的 DRM 有 IBM 的 EMMS 和 Microsoft Windows Media DRM;国内电子文档 DRM 有方正 Apabi Office DRM;按照保护措施可以将它们分为两类:一类是加大复制难度,如加入数字水印;另一类是将数字内容加密. 虽然用户可以复制数字内容,但是数字内容必须通过专门的许可证才能使用. 而许可证通常与机器硬件信息绑定,彼此一一对应,不同的机器使用不同的许可证.

典型的 DRM 系统[2]中由 3 个主要部分组成:许可证服务器、内容服务器和客户端,如图 1 所示.

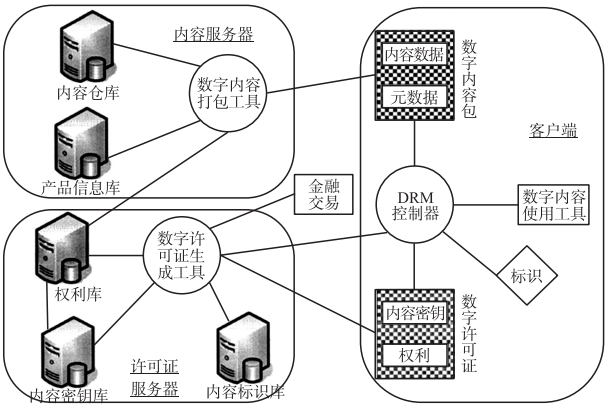

图 1 典型 DRM 系统的体系结构

Fig. 1 The architecture of typical DRM system

(1)内容服务器包括内容仓库、产品信息库和 DRM 打包工具. 内容仓库负责存放数字内容,产品信息库负责存放内容信息. 内容服务器主要有两大功能:一是将数字内容加密后与内容标识元数据一起打包封装;二是负责生成数字内容的使用权利,将密钥和权限信息发给许可证服务器.

(2)许可证服务器包括权利库、内容密钥库、用户身份标识库和 DRM 许可证生成工具. 许可证服务器的主要功能是在收到用户申请后对用户身份进行认证,并在认证成功后为其颁发数字许可证. 数字许可证是由权利描述语言描述的,包括数字内容的使用权利和许可证颁发者的信息. 数字内容的使用权利可以具体到怎样的权限使用范围、多少次的使用、多久的使用时长等一系列用户很关心的问题. 许可证服务器的另一优势是结合金融交易,负责根据用户使用情况进行收费.

(3)客户端包含 DRM 控制器和数字内容使用工具. 客户端的主要功能是向许可证服务器申请数字许可证,获得许可证后才允许用户在许可证规定的权限内使用数字内容.

本文主要研究和分析了许可证服务器中使用的身份认证协议,并就其不足和应用进行了探讨.

1.2 可信身份认证

无论哪个领域的 DRM 系统中,身份认证都占有很重要的部分. 试想一个系统中最基本的用户身份都无法得到确认保护,整个系统将是一片混乱. 最早期身份认证应用的场景是在战争中同一方的士兵交接的时候要互报暗号,防止敌人乔装入侵. 这一身份认证方式得到了大家的认同,越来越多的人在不同的场景中应用. 因此身份认证迅速地发展起来. 认证的方式早已经不是单一的口令交换,指纹、声音、图形识别等技术开始在身份验证中发挥特殊作用. 近几年,国内外的学者对身份认证进行了深刻的研究与讨论. 国外的 Kaoru Kurosawa 等人最早提出了基于 ID 的身份认证方案(ID-based Identification,IBI),Liu Chenglian 等[3]人在身份认证方面使用了神经网络的知识. Debiao HE 等[4]人又提出了基于智能卡的多服务器身份认证方案,王尚平等[5]人利用了双线性映射原理实现了签名隐藏.

可信计算组织 TCG 为了防止用户身份泄密,引入了芯片 TPM 来增强保护. 即使攻击者获取了客户端用户的信息,但是仍然不能够知道与之相关的 TPM 信息,这样在验证的时候终将识别出伪造的身份. 目前可信计算组织提供了两种身份认证的技术:隐私 CA 协议(Privacy Certification Authority)[6]和直接匿名认证协议(Direct Anonymous Attestation,DAA)[7]. 在隐私 CA 协议中,每次认证都需要 CA 的参与,这使得效率低下. 并且因为 CA 知道所有 TPM 的 EK 公钥,假如 CA 和认证方串通,认证方就可以掌握所有 TPM,安全和隐私方面存在着很大的风险. 为了解决隐私 CA 协议中的问题,TCG 发布了直接匿名认证协议. 直接匿名认证协议利用零知识证明和 CL 签名技术来实现用户间的身份认证,没有使用 CA,因此不存在隐私 CA 协议中效率低的问题. 具体协议流程如图 2 所示.

直接匿名认证协议的认证方案大体如下:

(1)初始化(Setup)阶段:TPM 产生初始化信息 f,将 f 拆分为 f_0 和 f_1.

(2)加入(Join)阶段:TPM 将一些信息以及 EK 公钥发送给证书发布方. 证书发布方收到后首先检验 EK 公钥是否正确合法,然后利用零知识证明检验 TPM 的秘密信息是否正确合法. 上述条件都正确合法后,许可证服务器为 TPM 颁发 DAA 证书.

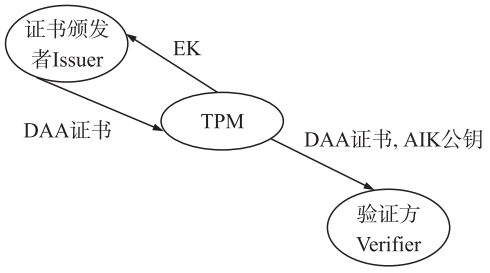

图 2　DAA 协议流程示意图

Fig. 2　DAA protocol flow diagram

(3)签名(Sign)阶段:TPM 首先利用零知识证明向验证方 Verifier 证明自己拥有 DAA 证书;其次用秘密信息和 DAA 证书对自身产生的 AIK 公钥进行签名,最后将签名后的结果发送给验证方 Verifier.

(4)验证(Verification)阶段:验证方 Verifier 验证正确性,若验证通过,则验证方相信 TPM 拥有 DAA 证书并且相信用户身份合法.

直接匿名认证也存在着一些缺点和问题:首先,匿名性不够强. DAA 认证方案中的 N_v 是通过参数 ζ 计算出来. 假如参数 ζ 是随机生成的,那么 N_v 也是随机的. 但如果参数 ζ 也是通过某种固定计算得出的,N_v 因此固定. 这种情况下匿名程度大大降低. 其次,无法跨域认证. DAA 认证方案仅限于 1 个域内使用,不适合于不同协议签署方与协议验证方之间的匿名认证.

2　直接匿名认证协议的改进

DRM 系统使用的协议可以归纳为 4 种:内容加密协议、身份认证协议、许可授权协议和业务计费协议. 从上文的 DRM 基本架构知识可以知道,许可证服务器参与着身份认证、许可证授权和业务计费 3 个方面,可见责任之重,意义之大. 本文重点阐述 DRM 中采用的身份认证协议:直接匿名认证方案. 在详细分析了直接匿名认证的流程和缺点后,本文提出并应用了直接匿名认证的改进方案. 该方案在认证阶段仍然采取了零知识证明,签名阶段采用的是基于 ElGamal 算法的双随机数签名.

2.1　零知识证明认证

Goldwasser 等人在 20 世纪 80 年代提出来了零知识证明(zero-knowledge proof)[8]. 主要思想是在证明者 Peggy 不提供自己的秘密信息情况下,验证者 Victor 相信证明者 Peggy 的确拥有这个信息.

零知识证明满足下面 3 个特性:

(1)确定性:证明者 Peggy 无法欺骗验证者 Victor,如果 Peggy 进行了欺骗,则 Victor 接受秘密信息的概率非常小.

(2)完备性:验证者 Victor 无法欺骗证明者 Peggy,如果 Peggy 拥有了秘密信息,则 Peggy 让 Victor 以非常大的概率几乎完全相信他能证明.

(3)零知识性:验证者 Victor 除了相信证明者 Peggy 拥有秘密信息外,无法再获得额外的任何信息.

本文将 Fiat-Shamir 零知识身份认证协议进行简化(如图 3 所示),可信第三方随机选取两个大素数 p、q,根据 $n=pq$ 计算出 n,n 向外界公开,p 和 q 并不公开. 证明者 Peggy 随机选择一个数 s 满足 $s>1$ 且 $s<n-1$,并计算 $v=s^2 \bmod n$,v 是公钥,s 是私钥.

(1)证明者 Peggy 随机选取 r 满足 $r<n$,计算 $x=r^2 \bmod n$,将 x 发送给验证者 Victor.

(2)验证者 Victor 将随机位 b 发送给证明者 Peggy,b 只能是 0 或 1.

(3)证明者 Peggy 根据 $y=rs^b \bmod n$ 计算出 y,将 y

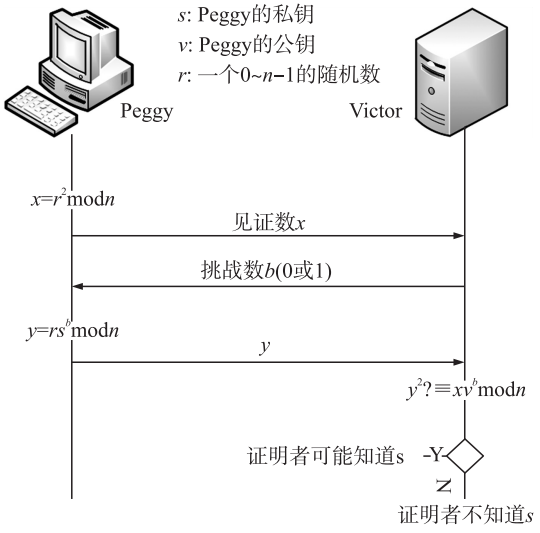

图 3　Fiat-Shamir 零知识身份认证协议

Fig. 3　Fiat-Shamir zero-knowledge authentication protocol

送给验证者 Victor;

(4)验证者 Victor 检验 $y^2 \equiv xv^b \bmod n$,如果正确则认为证明者 Peggy 可能知道秘密信息.

重复步骤 1 ~4 多次,次数越多,可信度越高,直至验证者 Victor 完全相信证明者 Peggy 拥有秘密信息.

2.2 基于 ElGamal 算法的双随机数签名

1985 年 ELGamal 提出了 ELGamal 数字签名算法[9],其安全性是基于数学上有限域内离散对数求解的难题,其签名方案如下:

设 p 为有限域 GF(p)上的一个大素数,集合 $Z_p=\{0,1,2,\cdots,p\}$,子集 $Z_p^*=\{0,1,2\cdots\cdots,p-1\}$,取 $g\in Z_p^*$ 满足 $\gcd(g,p)=1$. 在密钥集定义中:$x\in Z_p^*$,$K=\{(p,g,x,y):y\equiv g^x \bmod p\}$. 公开密钥为 p,g,y,私钥为 x.

用户 A 首先对消息 m 签名,然后发送给验证方 B,具体的步骤如下:

(1)用户 A 随机选取 k 满足 $k\in Z_p^*$ 且 $\gcd(k,p-1)=1$.

(2)计算 $r\equiv g^k \bmod p$.

(3)求解同余方程 $m\equiv(xr+ks)\bmod(p-1)$中的 s,即 $s\equiv(m-xr)k^{-1}\bmod(p-1)$.

用户 A 对消息 m 的签名是(r,s). 用户 A 将(m,r,s)发送给验证方 B. B 收到(m,r,s)后,验证方程 $g^m\equiv y^r r^s \bmod p$ 是否成立. 若成立,证明签名真实有效;否则,拒绝.

可见在传统 ElGamal 签名方案中只采用了 1 个随机数 k,如果这个随机数被攻击者窃取,则整个 ElGamal 算法都失去了意义. 为了增加签名方案的安全性,本文采用了双随机数签名法. 俩个随机数同时被窃取的几率远远小于 1 个随机数泄露的概率. 除了随机数 k 外,再选取个与 k 互异的随机数 t,满足 $t\in Z_p^*$,且 $\gcd(t,p-1)=1$. 计算 $\lambda\equiv g^t \bmod p$. 同余方程相应地变为 $m\equiv(xr+k\lambda+ts)\bmod(p-1)$,验证方程也变为 $g^m\equiv y^r r^\lambda \lambda^s \bmod p$.

用户 A 对消息 m 的签名是(r,λ,s). 用户 A 将(m,r,λ,s)发送给验证方 B. B 收到签名后,验证方程 $g^m\equiv y^r r^\lambda \lambda^s \bmod p$ 是否成立. 若成立,证明签名真实有效;否则,拒绝. 总结全部签名方程如下:

$$y\equiv g^x \bmod p,$$
$$r\equiv g^k \bmod p,$$
$$\lambda\equiv g^t \bmod p,$$
$$m\equiv(xr+k\lambda+ts)\bmod(p-1).$$

验证方程 $g^m\equiv y^r r^\lambda \lambda^s \bmod p$.

具体流程如图 4 所示.

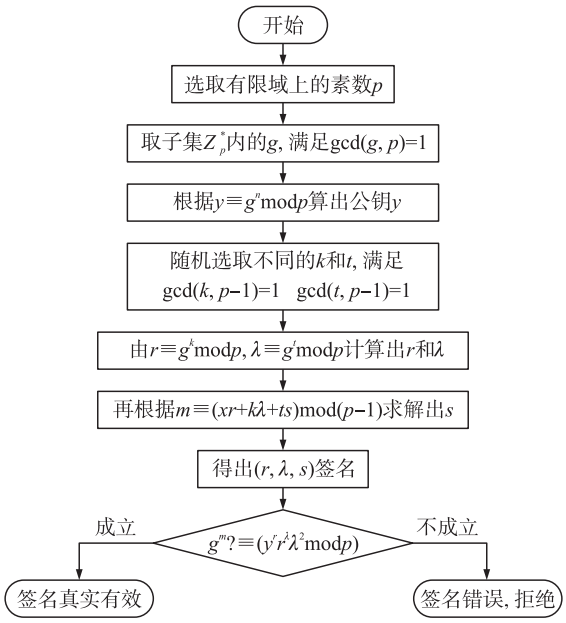

图 4 算法流程图

Fig. 4 The algorithm flowchart

3 应用及分析

在可信 DRM 系统的身份认证阶段,TPM 首先将自己的身份信息和 EK 公钥发送给许可证服务器,许可证服务器接下来检验 EK 公钥是否正确合法,然后利用零知识证明检验 TPM 的秘密信息. 着重检验 TPM 是否在已经泄漏公钥的黑名单中,如若在,说明此 TPM 不可信. 上述条件都满足后,根据上文介绍的 ELGamal 双随机数签名算法得出签名(r,λ,s),发送给 TPM. TPM 检验 $g^m\equiv y^r r^\lambda \lambda^s \bmod p$ 是否成立,若成立证明签名正确. 身份得到认证.

3.1 匿名性分析

DAA 改进方案在认证阶段依旧采用了零知识证明,在验证身份的过程中,一直没有获取具体秘密信息,极大地保护了隐私性. 与原来的直接匿名验证协议隐私性一致. 在签名阶段采用了双随机数签名算法,签名为(r,λ,s),其中 r 和 λ 是由随机数 k,t 算出的,由于选取的 k,t 不同导致签名也不同,这样很好地保

护了隐私性.

3.2 安全性分析

假设攻击者通过攻击可以窃取到私钥 x,但是想由已知求出随机数 k 和 t 是非常困难的. 因为 $m\equiv(xr+k\lambda+ts)\bmod(p-1)$,相当于求解有限域内的离散对数问题. 离散对数难题在密码学上一直被认为是安全和无解的.

假设攻击者获得了某一信息签名 r 和 λ,由于采用了双随机数,s 的验证方程由 $r^s\equiv g^m y^{-r}\bmod p$ 变为 $\lambda^s\equiv g^m y^{-r}r^{-\lambda}\bmod p$,后者多求了1次逆预算,明显更复杂困难,因此即便攻击者获得了签名 s,也只适用这一消息的签名,对于其他的消息不构成任何威胁.

双随机数签名中选取的随机数是不同的,假如每次选取的随机数相同,根据 $m\equiv(xr+k\lambda+ts)\bmod(p-1)$多式联立可以求出 t,这是极不安全的,因此每次签名采取的随机数必须不同,这样每次的签名也不同,如此不确定性也增加了安全性.

3.3 计算量与时间复杂度分析

由于本文采用的是双随机数签名,传统 ElGamal 算法中只用了1个随机数,因此,双随机数签名中关于随机数的运算会多算1次. 另外,验证方程 $g^m\equiv y^r r^{\lambda}\lambda^s\bmod p$ 计算,或者同余方程 $m\equiv(xr+k\lambda+ts)\bmod(p-1)$求解与传统算法相比可以说是变得复杂,增加了计算量.

签名增加了 $\lambda\equiv g^t\bmod p$,但是时间上不会有很大变化. 因此时间复杂度还是维持不变.

4 结论

在版权问题日益突出的今天,DRM 的出现带来了新的希望. 本文重点介绍了引入 TPM 芯片的可信数字版权管理,改变了以往密码保护不足的困境,更好地致力于数字版权的管理. 尤其在身份认证方面,详细分析了隐私 CA 方案和直接匿名认证的优缺点后,提出了直接匿名认证的改进方案,即将零知识认证和 ElGamal 的双签名结合在一起. 既有效地保护用户隐私,又能安全有效地进行身份认证,应用前景广阔,具有十分重要的意义. 最后经过分析得出改进方案在安全性,匿名性方面有所提高.

[参考文献]

[1] Zhang Zhiyong, Pei Qingqi, Ma Jianfeng, et al. Security and trust in digital rights management[J]. International Journal of Network Security, 2009, 9(3): 247-263.

[2] Jamkhedkar Pramod A, Heileman Gregory L. Digital rights management architectures[J]. Computers and Electrical Engineering, 2009, 35(2): 376-394.

[3] Liu Chenglian, Lin Chenglu, Harn Lien, et al. Security analysis of remote password authentication schemes for multi-server architecture using neural networks[J]. Advanced Science Letters, 2012, 7(1): 680-683.

[4] Debiao H E, Hao Hu. Cryptanalysis of a smartcard-based user authentication scheme for multi-server environments[J]. IEICE Transations on Communications, 2012, 95(9): 3 052-3 054.

[5] 王尚平,杨春霞,王晓峰,等. 基于双线性对的隐藏签名认证方案[J]. 电子与信息学报,2008,30(2):486-489.

[6] 李超零,周雁舟,李立新,等. 基于代理的隐私 CA 模型[J]. 信息工程大学学报,2010,11(1):113-117.

[7] 宋成,孙宇琼,彭维平,等. 改进的直接匿名认证方案[J]. 北京邮电大学学报,2011,34(3):62-65.

[8] Zhou F C, Xu J, Li H, et al. Group signature based on non-interactive zero-knowledge proofs[J]. China Communications, 2011, 8(2): 34-41.

[9] 刘怀明,魏仕民. 基于椭圆曲线的 ElGamal 型数字签名[J]. 吉林师范大学学报:自然科学版,2012,33(3):57-60.

[责任编辑:顾晓天]