数字电视中的一种新的身份认证方案

张方国,廖 平,王育民
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 数字化技术的发展,使得视频广播也进入了数字时代.在数字电视中,由于安全上的要求,Smart 卡与数字机顶盒之间要进行零知识身份认证.本文基于椭圆曲线数字签名算法(ECDSA),首次提出了一个新的不泄露签字的认证方案,并应用于数字电视中,同时分析了它的安全性与有效性.

关键词: 数字机顶盒; 身份认证; 椭圆曲线数字签名算法; Smart 卡
中图分类号: TN941.3 **文献标识码**: A **文章编号**: 0372-2112 (2001) 07-0927-03

A New Identity Authentication Scheme in DTV

ZHANG Fang-guo, LIAO Ping, WANG Yu-min
(P. O. Box119 Key Lab. on ISN, Xidian Univ., Xi'an, Shanxi 710071, China)

Abstract: With the development of digital tehnology, video broadcast has come into digital age. In DTV, it needs zero-knowledge identity authentication between the smart card and the digital Set-Top-Box because of the scurity requirement. This paper presents a new authentication scheme that will not leak the signature based on ECDSA, and applies it in DTV, and at the same time we analyze its security and efficiency.

Key words: digital set-top-box; identity authentication; ECDSA; Smart cards

1 引言

随着数字化技术的发展,电信,电视,数据传输进入数字化时代.数字化时代的特征之一就是数字视频广播(DVB)的实施,包括数字卫星视频广播(DVB-S),数字地面视频广播(DVB-T),及数字有线视频广播(DVB-C).而最终的用户端数字接收设备将会是数字电视(DTV).在传统的模拟电视向数字电视转变的过程中的过渡解决方案是数字机顶盒,而数字电视传输中需要解决的一个安全问题就主要集中在数字机顶盒与 Smart 卡之间交互式身份认证.目前在机顶盒与 Smart 卡的认证中大都采用 RSA 数字签名与 GQ 零知识认证技术相结合的方案,由于 RSA 的密钥长,为达到安全性要求,至少需要 1024 比特.这对于像 Smart 卡这类需要较短密钥的产品是极不相称的.由 Koblitz[1]和 Miller[2]开创性的工作,使得被数学家研究了一百多年的椭圆曲线在密码领域中得以发挥重要作用.由于椭圆曲线密码体制独特的优越性,使得这一密码体制更适合于 Smart 卡这样的密码产品.在本文中,基于椭圆曲线数字签名算法(ECDSA)首次得出了一个新的不泄露签字的认证方案,并分析了它的效率和安全性.

本文内容组织安排如下:在第二节中简单介绍了数字机顶盒与 Smart 卡及其在数字电视中的作用;第三节介绍了现有的数字机顶盒与 Smart 卡之间的交互式身份认证方案(GQ 认证体制);第四节描述了基于椭圆曲线提出的认证方案;在第五节中对提出的认证方案的安全性和有效性进行了分析;最后一节是结束语.

2 机顶盒与 Smart 卡简介

由于目前世界上大量现有模拟电视接收设备不可能全部被弃用更新,因而在由模拟电视机向数字电视机转换过程中,需要有过渡期的解决方案,即配置可使模拟电视接收机接收数字信息的数字机顶盒,简称 STB(Set-Top-Box)或 DSTB(Digital-Top-Box).数字机顶盒具有较强的数字信息处理能力,在技术上包含了数字电视的解调、译码、解密等许多核心技术,既支持现有的模拟电视业务,又兼备未来的数字视频业务.图 1 是机顶盒的一般结构图[3].

Smart 卡存有用户的 ID 和可信赖中心的签字.数字机顶盒与 Smart 卡的交互式身份认证,是数字视频广播服务安全性问题的关键技术之一.机顶盒对 Smart 卡的认证保证了当前使用的卡是经过可信赖中心授权的"合法"卡,否则机顶盒将拒绝提供部分或全部视频服务;Smart 卡对机顶盒的认证保证了机顶盒是经过可信赖中心授权的"合法"机顶盒,否则 Smart 卡将拒绝机顶盒对卡进行敏感数据的读写,如:从卡中存取初始控制字或持卡人的私人信息等.在认证中,由于安全上的需要,我们不希望机顶盒得到 Smart 卡的由可信赖中心给的签名(即不希望传输和在机顶盒中存储这个签名),同时

收稿日期:2000-04-03;修回日期:2000-09-20
基金项目:国家自然科学基金(No.19931010)

又要让机顶盒相信 Smar 才是的确有可信赖中心给的合法签名.

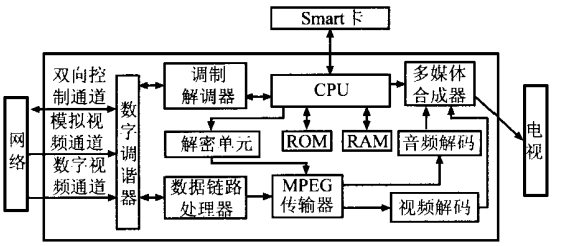

图 1 数字机顶盒的一般结构图

3 机顶盒与 Smart 卡间现有的认证方案

机顶盒的研究中,数字机顶盒与 Smart 卡的交互式身份认证,是数字视频广播服务安全性问题的关键技术之一,目前大都采用 Guillou-Quisquater 身份认证体制,简称 GQ 体制[4]. 该体制是基于 RSA 密码体制的零知识证明协议,需要三方参与,三次传送实现. 可信赖第三方 T 先选定 RSA 体制的秘密参数 p 和 q,生成大整数模 $n = p \cdot q$;公钥指数为 e,满足: $GCD(\Phi, e) = 1$, $\Phi = (p - 1)(q - 1)$;计算出秘密指数 $d = e^{-1} \bmod \Phi$,公开 (e, n). 各用户选定自己的参数,用户 A 的唯一性身份 I_A,通过 Hash 函数计算: $J_A = H(I_A)$, $1 < J_A < n$, $(J_A, \Phi) = 1$. T 向 A 分配秘密数 $S_A = (J_A)^{-d} \bmod n$.

用户 B 认证用户 A 的单轮协议为:

(1) A 选择随机数 r, $1 \leq r \leq n - 1$,计算 $x = r^e \bmod n$, A 将 (I_A, x) 送给 B;

(2) B 选择随机数 u 作为提问, $1 \leq u \leq e$,并将提问送给 A;

(3) A 计算 $y = r \cdot S_A^u \bmod n$,将 y 送给 B;

(4) B 收到 y 后,从 I_A 计算 $J_A = H(I_A)$,及 $J_A^u \cdot y^e \bmod n$. 若结果不为零且等于 x,则 B 认可 A 这一轮的证明;否则拒绝.

此协议可执行 t 轮,只有每一轮的验证均被接受时 B 才接受 A 的身份证明.

由于 RSA 密码体制中密钥长度与资源有限的灵巧卡间的矛盾,基于 RSA 密码体制的安全方案在 Smart 卡上的应用受到限制,特别是 1999 年 8 月 22 日,CWI(在荷兰的一个数学和计算机科学的国家研究学会)的 Herman te Riele 宣告成功的分解出了 512-bit RSA 模的素因子,这就需要更安全更适用于 Smart 卡的密码体制来替代 RSA.

4 本文的认证方案

4.1 Smart 卡上签名生成

在数字电视系统中,用户所持有的 Smart 卡中要有可信赖中心的签字,这里一般指电视台. 在本文的方案中,采用椭圆曲线数字签名(ECDSA)技术,为了以后的零知识身份认证,对它进行了适当修正.

对所用的 ECDSA 采用如下参数(有关椭圆曲线密码体制的介绍可参见[5]): $D = (p, a, b, G, n)$, (d, Q), SHA - 1. 其中: p 是有限域的元素个数; $a, b \in GP(p)$,定义 $GF(p)$ 上的椭圆曲线; $y^2 = x^3 + ax + b \quad p > 3$; $G = (x_G, y_G)$ 是 $E(GF(p))$ 中的一个点, $ord(G) = n$; n 是 $\#E(GF(p))$ 的一个大素因子, $n > 2^{160}$ 且 $n > 4\sqrt{q}$; $d \in_R Z_n^*$ 是签名私钥, $Q = dG$ 是签名验证公钥; SHI - 1: $\{0,1\}^* \rightarrow \{0,1\}^{160}$ 是一个单向 Hash 函数,它可以是 FIPS 180 - 1(联邦信息处理标准)中的 Hash 算法.

将 $D = (q, a, b, G, n)$, Q, SHA - 1 公开, d 保密.

用户到电视台购买 Smart 卡,电视台在 Smart 卡中签字,下面是利用修正的 ECDSA 签字过程:

签名生成 电视台利用上面的参数对消息 m 进行签名(这里的一般包含用户 ID 和购买时间,即 $m = (ID \| time)$;

(1) 随机或伪随机地选择一个整数 $k \in_R Z_n^*$;

(2) 计算 $R = kG = (x_1, y_1)$, $r = x_1 \bmod n$,如果 $r = 0$,则返回到 1;

(3) 计算 $e = \text{SHA} - 1(m)$;

(4) 计算 $s = k(e + dr)^{-1} \bmod n$,如果 $s = 0$,返回到 1;

(R, s) 是 A 对消息 m 的签名. 这个签名的关键是 s,在后面将看到,即使公开了 R,也无法伪造出一个合法的 s.

签名验证

(1) 计算 $r = R_x(R) \bmod n$, $R_x(R)$ 表示取 R 的 x 坐标;

(2) 验证 r, s 是 $[1, n - 1]$ 中的整数;

(3) 计算 $e = SHA\text{-}1(m)$;

(4) 计算 $X = seG + srQ$,当且仅当 $X = R$ 时接受这个签名.

4.2 认证方案

用户在收看电视时,首先要进行 Smart 卡与机盒之间的相互认证. 在 Smart 卡向机顶盒证明它是合法用户时,只须向机顶盒提交 ID(即 m),同时向它证明自己有电视台的合法签名,但不把签字提交给机顶盒. 因为如果提交签字,则在传输过程中会被非法用户截获,从而可以冒充合法用户收看节目. 下面是本文设计的基于椭圆曲线的不泄露签字的认证方案.

Smart 卡首先向机顶盒发送 m 和 R,机顶盒计算 $SHA - 1(m)\, G + R_x(R)\, Q = P$,并将 P 发给 Smart 卡; Smart 卡向机顶盒证明它知道 s,使得 $sP = R$,但不向机顶盒泄露 s,即 $SKLOG\{s : sP = R\}(m)$ (关于离散对数的知识签名证明)[6]

Smart 卡 机顶盒

$\xrightarrow{R, m}$ 计算 $SHA - 1(m) + R_x(R) = P$

$t \in_R Z_n$, $T = tP$ $\xleftarrow{P}$

$c = SHA - 1(R_x(P) \| R_x(R) \| R_x(T) \| m)$

$a = t - cs \bmod n$ $\xrightarrow{(a, c)}$ 验证

$c \overset{?}{=} SHA - 1(R_x(P) \| R_x(R)_x(aP + cR) \| m)$

机顶盒验证等式成立,则认为 Smart 卡有电视台的合法签名.

5 方案分析

对基于离散对数的数字签名的证明,即 A 想向 B 证明自己有可信赖中心的签名,但又不泄露这个签名,实际上就是要向 B 证明自己所有的签名满足一个关系式. 而一般基于离散对数的数字签名,象 ElGamal 或 DSA 等,这个关系式是一个

关于签字的既有指数形式又有多项式形式的表达式,用零知识证明这样一个表达式是很困难.

为了实现基于 ECDSA 的零知识身份认证,我们将签字一部分 R 发送给机顶盒. 虽然给出了 R,但因为 $s = k(e + dr)^{-1} \bmod n$,所以除了电视台,任何人都不可能伪造出 s. 而且 Smart 卡也不可能伪造出一个 (R', s'),使得提交 R 后,在后面的零知识证明中能蒙混过关,这是由 ECDSA 的安全性所决定的. 事实上,可以证明下面的结论:

命题 1　Smart 卡证明 $SKLOG\{s: sP = R\}(m)$ 与零知识证明数字鉴名是等价的.

证明　首先,如果 Smart 卡知道 (R, s),使得 $sP = R$ 成立.

其次,如果 Smart 卡知道 s',使得 $s'P = R$ 成立,这里 $P = SHA-1(m)G + R_x(R)Q$,则 $s'(SHA-1(m)G + s'R_x(R)Q = s'R_x(R)Q = s'eG + s'rdG = R = kG$,从而

$s'e + s'rd = k \bmod n$,即

$s' = k(e + rd)^{-1} (\bmod n) = s$.　□

此外,由于 160 比特的椭圆曲线密码体制的安全强度等效于 1024 比特的 RSA 密码体制,所以本方案在效率上要远优于原来的基于 RSA 的方案. 对于椭圆曲线密码体制的实现,国内外许多公司在科研单位都在做. 表 1 是比利时的 COSIC 对 ECDSA 和 RSA 及 DSA 实现记录对照表(EC 域的大小是 191 比特,RSA 和 DSA 的模的大小是 1024 比特,RSA 的公开指数是 3,所有时间都是毫秒)[2]

表 1

	ECDSA $GF(p)$	RSA	DSA
密钥生成	5.5	1s	22.7
签名	6.3	43.3	23.6
验证	26	0.65	28.3

6　结束语

模拟电视即将消亡,数字电视的推行是必然的趋势. 数字机顶盒与 Smart 卡的交互式身份认证是数字视频广播服务安全性问题的关键技术之一. 在本文中,基于椭圆曲线数字签名算法(ECDSA)首次提出了一个新的不泄露签字的认证方案,并分析了它的效率和安全性. 本方案无论在安全性能上还是在实现效率上都优于原来的基于 RSA 的认证方案,我们深信本方案将获得广泛的应用.

参考文献:

[1] N Koblitz. Elliptic curve curve cryptosystems [J]. Mathematics of Computation. ,1987 ,48 ,(177) :203 - 209.

[2] V S Miller. Use of elliptic curve in cryptograpphy [A]. In Advances in Cryptology-CRYPTO '85 (Santa Barbara ,Calif. ,1985) [C] ,Spring-Verlag ,LNCS 218 ,1986 :417 - 426.

[3] Hyun-Ho Jeon ,et al ,Transmission of System Information and Additional Service Data for Digital HDTV Broadcasting [J]. IEEE Trans. on Broadcasting ,1998 ,44(1) :87 - 93.

[4] L C Guillou ,J J Quisquater. A practical zero-knowledge protocol fitted to security micorprocessor minimizing both transmission and memory [A]. Advances in Cryptology-EUROCRYPT '88 [C] , Springer Verlag ,LNCS 330 ,1988 :123 - 128.

[5] IEEE P1363. Standard Specifications for Public-Key Cryptography [S]. ballot draft , 1999. Drafts available at http://grouper.ieee.org/groups/13163/index.html.

[6] C P Schnorr. Efficient signature generation by smart cards [J]. Journal of Cryptology ,1991 ,4(3) :161 - 174.

[7] E D Win ,S Mister ,B Preneel ,M Wiener. On the performance of signature schemes based on elliptic curves [A]. in J. P. Buher ,editor , Algorithmic Number Theory , Proceedings Third Intern. Symp. [C] , ANTS-III , Springer-Verlag , LNCS1432 , 1998 : 621 - 638.

作者简介:

张方国　男. 1972 年 12 月生于山东省淄博市,博士研究生. 1996 年在烟台师范学院数学系获得理学学士学位,1999 年在上海同济大学应用数学系获得理学硕士学位,现在西安电子科技大学通信工程学院攻读密码学博士学位,研究兴趣是电子商务和椭圆曲线密码体制及其推广.

廖　平　男. 1973 年 8 月出生,1995 年在西安电子科技大学电子工程学院获工学学士学位,2000 年在该校通信工程学院获工学硕士学位,现在大唐电信有限公司北京研发中心工作.

王育民　男. 生于 1936 年,教授,IEEE 高级会员,博士生导师,长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究.