基于智能卡的组播内容保护与支付系统

李新国[①②] 葛建华[①] 赵春明[①]
[①](西安电子科技大学 ISN国家重点实验室 西安 710071)
[②](解放军洛阳外国语学院 数学教研室 洛阳 471003)

摘 要 内容保护问题是实现数字内容网上交易的关键问题。传统的组播密钥管理都假设所有合法组用户可以知道组密钥，这种假设对于商业组播是不现实的。该文设计的组播内容保护和支付系统假设智能卡是安全的，所有攻击者包括持卡人都无法获知智能卡中的私钥和组密钥。系统使用最近提出基于身份加密方案，从而避免了公钥证书的使用。系统可以保证数字内容的安全传输，同时具有用户身份认证、内容认证和密钥管理方面的简单性，系统还支持用户的匿名消费。

关键词 组播密钥管理，数字内容保护，智能卡，支付
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2006)08-1497-04

Smartcard-Based System for Multicast Content Protection and Payment

Li Xin-guo[①②] Ge Jian-hua[①] Zhao Chun-ming[①]
[①](*National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an* 710071, *China*)
[②](*Dept. of Mathematics, PLA Foreign Language Institute, Luoyang* 471003, *China*)

Abstract Content protection is the key issue to perform digital content transactions on the web. It is impractical for commercial multicast assuming that all group members know the group key in traditional multicast key management schemes. The proposed design for multicast content protection and payment system is based on the secure smartcard assumption under which both attackers and card holder are not able to obtain the private key and group key stored in the smartcard. Identity-based encryption scheme is introduced in the system to avoid using public key certificates. The system can guarantee the secrecy of content transmission with other features like simplicity for identification, content authentication, key management and anonymity for payments.

Key words Multicast key management, Digital content protection, Smartcard, Payment

1 引言

随着网络带宽的增加，通过因特网传输有高带宽要求的多媒体数字内容已经成为可能。IP 组播则是以最有效的带宽利用方式将同一数据发送给多个组用户，IP 组播技术的日渐成熟使之成为数字内容网上传输的首选技术。在传输问题解决之后，版权保护问题就成为实现数字内容网上交易的关键。本文考虑如何将数字音视频内容通过 IP 组播的方式安全地分发给组用户，同时保证从事数字内容组播的商家获得来自用户的支付。所设计的系统适用于通过 IP 网络提供数字内容服务的商家。为了便于描述，将面向的用户限定为具有宽带连接的数字电视机顶盒，传输和接收方式是流媒体，用户端对数据不做存储。支付模式限定为 PPV (Pay Per View)，也就是用户选定单个节目，然后付费并收看，相对于包月支付模式。

在数字版权保护DRM (Digital Rights Management)领域，为了保证数字内容在传输过程中不被截获，必须对内容进行加密，然后将解密密钥传给合法用户。尽管合法用户可以使用解密密钥解密内容，但是绝对不允许用户读取解密密钥；否则，合法用户就可以将解密密钥公开，这样任何有解密密钥的不合法用户就变成了合法用户，版权所有者利益也将遭受损失。可以肯定地说，唯一解决版权保护问题中这一矛盾的办法就是在用户端配置一个安全部件用来阻止用户对解密密钥等信息的读取。安全部件可以是一个特别设计的软件，如微软的Media Player 10[1]；也可以是智能卡之类的硬件。我们选择智能卡作为系统的安全部件，首先是因为当前的智能卡安全特性足以满足系统的需求，其次是智能卡为系统功能的实现和应用扩展提供了更大的空间。本文的内容保护方案只是对数字内容的网上传输提供保护，数字内容在用户端的拷贝控制等安全措施可以认为是另外一个独立的问题[2]，在本文中不做讨论。

2004-11-24 收到，2005-10-31 改回
国家自然科学基金重点项目（60332030，60496316）资助课题

2 系统模型

整个系统的模型可以认为是 3 个相对独立的模型的关联。依次是公钥基础设施 PKI 模型，支付模型和内容保护模型。

2.1 PKI 模型

系统不使用传统的PKI模型，如X.509。而是使用最近提

出的由基于身份的公钥密码体制IBE (Identity-Based Encryption)所搭建起来的PKI[3]，称之为IBE-PKI。IBE-PKI中的可信第 3 方对应于系统中的可信发卡机构。可信发卡机构为每张智能卡生成一个公私钥对：(PK,SK)，并将其存放在智能卡中。注意IBE并没有使用传统的公钥证书，不使用公钥证书也是IBE体制设计的主要动机。在有一个可信发卡机构、商家出售数字内容这样一个相对封闭的应用环境中，使用由IBE-PKI建立的信任体系是合理的。IBE-PKI的优势充分体现在第 4 节的用户身份认证和匿名消费协议当中。

2.2 支付模型

支付模型中有 4 个主体：发卡机构，银行，商家，用户。完整的支付活动需要 3 个协议：发卡机构和用户之间的发卡协议，用户和商家之间的支付协议，以及银行内部的结算协议。

发卡协议：用户通过零售点购买一张发卡机构的智能卡(可以是预付费的)，卡中有一个唯一标识该卡身份的公私钥对。

支付协议：用户/智能卡对所购买商品的名称、价格、商家名称等信息用私钥签名，并将签名和智能卡公钥反馈给银行；银行验证数字签名的合法性和用户帐户的状态；银行将支付完成信息传给商家；商家将商品送达用户手中。

结算协议：银行从用户帐户将消费的金额扣除，并转移到商家的帐户。

2.3 系统假设

系统假设银行和发卡机构是两个可信任的机构，也假设智能卡是一个交易各方都信任的安全部件。关于可信任机构的假设是显而易见的，否则这两个机构将面临信任危机和破产。对智能卡的安全假设是：智能卡不能将其私钥等信息让外界知道，包括用户本人！只有发卡机构知道智能卡的私钥，而可信的发卡机构不会冒着倒闭的风险泄露它们。所以要满足智能卡安全假设，主要工作应该是在智能卡的物理制造方面：智能卡可以参与一定的加解密运算，但任何攻击者试图获取卡的私有信息的操作都是不可行的。有几个理由可以说明该假设的合理性：一方面，这类可信的智能卡已经在数字电视等商业领域获得应用[4]；另一方面，最新的研究成果和技术也证明这种合理性[5,6]；第三，我们可以通过审计措施追踪智能卡的行为，一旦发现问题，可以将某张智能卡吊销。

其它假设主要是算法的安全性假设，如超奇异椭圆曲线上的计算性Diffie-Hellman问题[3]。

2.4 系统参考模型

系统中有 4 个主体：发卡机构，从事数字内容组播的商家，银行和用户。每个用户需要购买一张智能卡。商品实际上加密数字内容的密钥。在下面的叙述中，除非特别指明，我们对智能卡和用户不做区分。图 1 中尽管没有标出发卡机构，但该机构在系统运行时，必须负责智能卡的吊销问题，并将当前的吊销列表及时传给银行。

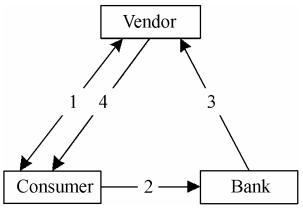

图 1 系统参考模型

Fig.1 System reference model

3 系统运行过程

在消费数字内容之前，假设用户已经拥有了一张智能卡，并且通过一定的方式往该智能卡帐户中注入一定量的钱数，这是系统运行的前提条件。如图 1 和图 2 所示，系统运行过程如下：

(1)用户通过智能卡向某个从事数字内容组播的商家发出消费请求[7]，并下载消费清单。清单中有商家的身份信息，所要消费的数字内容的标识，价格信息等。同时将智能卡的公钥 PK 传给商家。商家等待来自银行的支付确认信息。

(2)智能卡将消费清单用自己的私钥签名[8]，并传给银行。

(3)银行首先查看用户智能卡的公钥 PK 是否出现在由发卡机构公布的吊销列表中，然后验证签名的正确性。如果 PK 没有被吊销，智能卡的签名也是正确的，并且用户帐户中的钱数可以支付本次消费，此时银行向商家发送一个支付完成消息。同时将用户帐户的消费金额转到商家帐户。

(4)商家收到来自银行的支付完成信息后，使用用户智能卡的公钥加密用于加密数字内容的密钥 DK，并将密文传给智能卡。商家用对称密钥 DK 加密数字内容，并将加密的内容通过IP组播路由协议[9]传给各个用户。

(5)智能卡使用内部的私钥 SK 解密出 DK，从而进一步使用 DK 解密出数字内容。接下来用户可以消费数字内容。

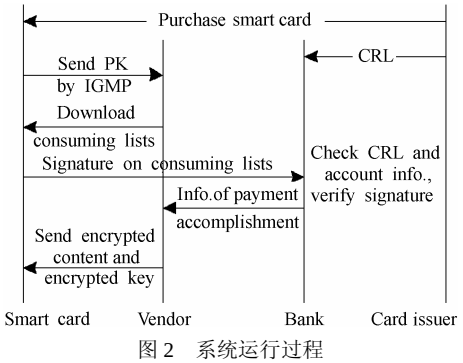

图 2 系统运行过程

Fig.2 System running process

4 系统主要组件的设计与分析

4.1 密钥管理

系统主要涉及两个密钥的管理问题。一个是智能卡的公私钥对，另一个是组密钥。两者在管理上的安全合理性除了来自相应的密码算法，更主要是来自本文的关于智能卡的安全假设。

智能卡公私钥对有发卡机构生成。公钥可以是任意的 $\mathrm{ID}\in\{0,1\}^*$，为了便于管理，可以定义为由发卡机构统一分配的序列号。在智能卡吊销时，只须公开这个序列号即可。智能卡的私钥是 $d_{\mathrm{ID}}=s\cdot Q_{\mathrm{ID}}$，其中 $Q_{\mathrm{ID}}=H_1(\mathrm{ID})$，$s$ 是发卡机构的系统主密钥，H_1 是一个将智能卡序列号映射到群元素的 Hash 函数。私钥 d_{ID} 存储在卡的安全区域，任何攻击者包括用户本人也不可以读取。

组播数据加密密钥 DK 是对称密码密钥，可以认为是和解密密钥相同，称为组密钥。组密钥 DK 由从事数字内容组播的商家生成用于加密传输数字内容。当获得用户支付以后，商家使用用户智能卡的公钥 ID 将组密钥加密后，传给智能卡。智能卡在其安全运算环境中用私钥 d_{ID} 解密出 DK，并将 DK 存储在安全区域内。接下来用户可以使用 DK 解密数字内容。

在解密组密钥和解密数字内容的过程中，与智能卡私钥一样，组密钥 DK 对用户来说是透明的、不可见的。这是本文中的组播密钥管理方法和传统的组播密钥管理方法的根本不同之处。传统的组播密钥管理方案[10-12]都假设组中的所有用户可以获知组密钥的内容。在这样的假设下，当一个新用户加入组和一个老用户离开组时，都必须更新组密钥以保证前向和后向安全性，密钥管理方法比较复杂，尤其不适用于多个组用户的场合。我们认为传统的组播密钥管理假设在商业组播中是不可行的，我们不能保证合法组用户在得到组密钥之后不会将其传给不合法的用户。在本文基于智能卡的安全假设下，组密钥管理变得相当简单，甚至可以说是不用管理。这是因为所有用户都不知道组密钥的内容，当用户加入和离开组时，没有前向和后向安全问题，无须更新组密钥。

4.1.1 吊销问题　前文我们假设了智能卡的安全性。如果智能卡是安全的，那么任何攻击者都得不到智能卡的私钥 d_{ID} 和组密钥 DK。然而我们不能排除私钥泄露情况的发生，在这种情况下，系统必须有必要的机制将各方面的损失降到最低。

第一种可能是某张卡的私钥泄漏给了攻击者。那么攻击者可以用该私钥签名消费清单，从而盗用用户账户中的金钱。这是用户所不期望的。在用户购买智能卡后，对智能卡设置一个用户身份标识码PIN[5]可以在一定程度上延缓攻击。更完整的解决办法是：一旦用户发现智能卡丢失或者被损坏，就及时向发卡机构报告。发卡机构将该卡的序列号公布在吊销列表中，当银行验证智能卡的数字签名时，就会阻止消费行为的继续进行，从而保护用户的利益。

另一种更具破坏性的攻击者如果知道了智能卡的私钥 d_{ID}，就可以解密出组密钥 DK。进一步该攻击者可以将组密钥传递给那些没有银行账户的不合法用户使用，这样数字内容保护的全部努力就都完全失效了。技术上，一方面可以设计更安全的智能卡来阻止这种攻击[5]，也可以通过定期更新组密钥(比如一分钟更新一次)的办法来增加攻击难度；另一方面，将从网络中组播路由器那里获得的数字内容所流向的目的地信息和发卡机构的智能卡销售记录加以综合，可以大致推断出一些不合法的用户；最后，数字水印技术[13]可以帮助商家追踪到盗版者。使用法律手段让盗版者为其行为负责也是必不可少的数字内容保护手段。

4.2 身份认证和内容认证

用户登录数字内容网站时无须进行身份认证；银行在验证用户对消费清单的数字签名时，也无须验证用户的身份。银行只是简单地查找吊销列表并确认该用户的智能卡序列号没有出现在吊销列表中，接下来银行可以利用用户提供的序列号对签名进行验证。可以认为银行对用户智能卡的身份认证是隐含的认证，因为能以出示给银行的序列号进行合法签名的个体必然拥有该序列号对应的私钥。与传统的使用公钥证书的 PKI 相比，注意到我们这里没有了对公钥证书的验证。减少了一次公钥证书验证过程正是 IBE-PKI 的优势，也使整个系统的反应速度得以提高。

内容认证对于像即时的股市行情这样的数字内容是至关重要的。用户除了要认证组播商家的合法性之外，还要认证商家所提供的数字内容的完整性和合法性。在多对多的组播环境中，每个组用户都可以向其它组成员发送消息，要认证每个用户的消息是非常困难的[10, 12]。在我们的系统中，一个组中只有一个成员即商家可以发送数字内容，对商家数字内容的认证可以通过先认证商家的组密钥，再认证每个数据包来实现。具体过程如下，商家在发给用户的组密钥中添加对该密钥的数字签名，然后在每个加密的数字内容数据包中添加对整个数据包的消息认证码MAC；用户可以先认证组密钥的合法性，进而利用组密钥计算出每个数据包的MAC值来验证内容的完整性和合法性。

4.3 匿名消费

在系统的运行过程中，商家收到用户的智能卡序列号和来自银行的支付完成信息后，要用该序列号加密组密钥传给用户。当同一用户使用同一序列号在该商家购买多次数字内容之后，商家显然可以将该用户的消费行为归入同一序列号下。为了保护用户消费隐私权，在 IBE-PKI 上，系统实现这一功能是简单的。

用户每次登录到一个数字内容组播商家之后，不提供其智能卡的真正序列号 ID，而是随机地取一个盲化因子 $t\in Z_q^*$，并将 $Q'=t\cdot H_1(\mathrm{ID})$ 提供给商家。商家在得到支付之后，使用用户提供的盲化的序列号信息 Q' 加密组密钥 DK 传给用户。

加解密过程：商家随机地取 $r\in Z_q^*$，计算关于组密钥 DK 的密文：$C=(r\cdot P,\mathrm{DK}\oplus H_1(g_{\mathrm{ID}}^r))$，其中 $g_{\mathrm{ID}}=\bar{e}(Q',P_{\mathrm{pub}})$。用户智能卡收到密文 $C=(U,V)$ 后用自己的私钥 d_{ID} 解密得到组密钥：$\mathrm{DK}=V\oplus H_1(\bar{e}(t\cdot d_{\mathrm{ID}},U))$。加解密的一致性是由下

式保证：

$$\overline{e}(Q', P_{\text{pub}})^r = \overline{e}(r\cdot Q', s\cdot P) = \overline{e}(s\cdot t\cdot H_1(\text{ID}), r\cdot P)$$
$$= \overline{e}(t\cdot d_{\text{ID}}, r\cdot P) = \overline{e}(t\cdot d_{\text{ID}}, U)$$

以上实现了用户的消费行为对商家的匿名性。需要注意的是，用户提供给银行的序列号必须是智能卡真正的序列号，也就是说用户的消费行为对银行来说不是匿名的。

5 结束语

采用 IP 组播技术在 Internet 上传输数字内容是一种非常有前景的互联网应用之一。为了保证组播内容的安全性，传统的组播密钥管理方案都假设每个合法组用户都知道了组密钥，并在该假设的基础上讨论如何将对组密钥获知限定在合法用户的范围之内。对于数字内容的商业组播来说，这个假设是不现实的，我们不能假设每个合法组用户都不会将组密钥泄漏给不合法的用户。本文假设所使用的智能卡是安全的：攻击者和持卡人都无法获知智能卡的私钥。在此假设下，我们设计了一个完整的数字内容安全组播和支付系统。由于假设了智能卡的安全性并且使用了 IBE-PKI 信任模型和算法，系统中的密钥管理、身份认证、内容认证和匿名消费都是简单有效的。

参 考 文 献

[1] MicroSoft Media Player. www.microsoft.com.

[2] DTCP Specification Version 1.3. www.dtcp.com.

[3] Boneh D, Franklin M. Identity based encryption from Weil pairing. CRYPTO 2001, Berlin: Springer-Verlag, 2001: 213−229.

[4] Tu F K, Laih C S, Tung H H. On key distribution management for conditional access system on pay-TV system. *IEEE Transactions on Consumer Electronics*, 1999, 45(1): 151−158.

[5] Gennaro R, Lysyanskaya A, Malkin T, Micali S, Rabin T. Algorithmic Tamper-Proof (ATP) security: Theoretical foundations for security against hardware tampering. TCC 2004, LNCS 2951, Berlin, Heidelberg, Springer-Verlag 2004: 258−277.

[6] Schneier B, Shostack A. Breaking up is hard to do: Modeling security threats for smart cards. USENIX Workshop on Smart Card Technology, Chicago, USENIX Press, 1999: 175−185.

[7] Fenner W. Internet Group Management Protocol Version 2, RFC 2236, IETF, 1997.

[8] Hess F. Efficient identity based signature schemes based on pairings. Selected Areas in Cryptography 9th Annual International Workshop, London, Springer-Verlag, SAC 2002, LNCS 2595: 310−324.

[9] Ballardie T, Francis P, Crowcroft J. Core based trees: An architecture for scalable inter-domain multicast routing. In proc. ACM SIGCOMM, ACM, San Francisco, 1993: 85−95.

[10] Mittra S. Iolus: A framework for scalable secure multicasting. In Proc. ACM SIGCOMM, Cannes, France, 1997: 277−288.

[11] Canetti R, Garay J, Pinkas B. Multicast security: A taxonomy and some efficient constructions. In Proc. INFOCOM'99, New York, 1999, V. 2: 708−716.

[12] Wong C K, Gouda M, Lam S S. Secure group communications using key graphs. *IEEE/ACM Transactions on Networking*, 2000, 8(1): 16−30.

[13] Swanson M D, Kobayashi M, Tewfik A H. Multimedia data embedding and watermarking techniques, Proc. IEEE, 1998, 86(6): 1064−1087.

李新国： 男，1976 年生，博士生，研究方向为 PKI、DRM、安全组通信.

葛建华： 男，1961 年生，教授，博士生导师，主要研究方向包括：数字电视、通信系统、信号处理、信息安全等.