带有基于 RSA 签名的接入控制的不经意传输协议

赵春明 葛建华 李新国
(西安电子科技大学 通信工程学院 西安 710071)

摘 要 该文在 RSA 签名及关于数据串的不经意传输的基础上提出了一种增强的不经意传输协议，解决了一种不经意传输的接入控制问题。除了具备一般不经意传输协议的特征外，该方案具有如下特点：只有持有权威机构发放的签字的接收者才能打开密文而且发送者不能确定接收者是否持有签字，即不能确定接受者的身份。在 DDH 假设和随机预言模型下该方案具有可证明的安全性。该方案使用标准 RSA 签名及 Elgamal 加密。

关键词 Elgamal 加密，接入控制，不经意传输，RSA 签名，决策性 Diffie-Hellman 假设
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2006)08-1501-03

Oblivious Transfer Protocol with RSA-Based Access Control

Zhao Chun-ming Ge Jian-hua Li Xin-guo
(*School of Telecommunications Engineering, Xidian University, Xi'an* 710071, *China*)

Abstract Based on RSA signature and (string) oblivious transfer, an oblivious transfer protocol is proposed which solved the access control problem for an oblivious transfer protocol. The protocol proposed has the property: the only receiver who has the signature issued by the central authority can open the message which he chose; the sender can not decide whether the receiver has the signature or not. That is the identity of the receiver can not be confirmed after the protocol. Under the Decisional Diffie-Hellman(DDH) assumption the proposed scheme has provable security. The proposed scheme employs the standard RSA signature and Elgamal encryption.

Key words Elgamal encryption, Access control, Oblivious transfer, RSA(Rivest Shamir Adleman) signature, Decisional Diffie-Hellman (DDH) assumption

1 引言

不经意传输协议首先由Rabin[1]提出，随后又出现多种不同的形式，这类协议在密码学和电子商务协议设计中有着广泛的应用。简单地说，不经意传输协议能够使参与协议的双方以一种不经意的方式传送消息。协议有两个参与者，即消息接收者与消息发送者。发送者持有若干个消息，接收者选择其中一个(或几个)。协议执行完以后，接收者只能得到他所选择的消息而不能得到其余消息；发送者不能确定接收者选择的是哪些消息。与匿名的协议相比较，不经意传输协议提供给协议参与者较弱的隐私保护，但由于避免了零知识证明，这种协议效率较高。在已有的不经意传输协议中对于接收者的接入控制问题还没有专门的研究，而此问题对于电子商务协议的实际应用又是十分必要的。比如，电子购物、多媒体视频点播等只有被授权的用户才能得到相应的消息，同时用户所具有的某一级别的授权等身份信息属于用户的隐私应得到保护。

一般而言，在分布式系统中，数字证书的交换被普遍地用来实现鉴别和授权。在交换证书的过程中，采用自动信任协商的方法来调节敏感的信息流。文献[2]提出了一种基于数字签名的接入控制方案，该方案克服了传统接入控制方案不能很好处理循环相依策略的缺陷。此方案可以简单地描述如下：数字证书的内容(包括持有者的身份、证书序列号、持有者的权限、证书的有效期、签字算法、授权机构等)及授权者的公钥信息对参与协议双方公开，而授权者对证书的签字只有接收者知道对发送者保密；接收者和发送者执行联合计算，发送者发送一个密文，只有持有签字的接收者才能打开密文而且发送者不能确定接收者是否持有签字。也就是执行完协议后，发送者不能把证书的内容与发送者相联系。

本文采用这一思想提出了带有基于RSA签名[3]的接入控制的不经意传输协议，该协议除了具备一般不经意传输的特征外，还具有只有持有签字的接收者才能打开他所选中的某一消息而且发送者不能确定接收者是否持有签字的特征。因此该协议中不仅接收者的选择而且接收者是否持有签字发送者不能确定。

2 协议的基础

2.1 1-out-of-*n* 不经意传输协议

Tobias 在文献[4]中提出了一种对于数据串的有效的1-out-of-*n*不经意传输协议。简述如下：

系统参数：g 是阶为 q 的循环群 G 的生成元。$g^{b_1}, g^{b_2}, \cdots, g^{b_n}$ 公开。

接收者的输入：R 秘密选择 $\delta \in \{1 \cdots n\}$，Elgamal密钥对

2004-12-06 收到, 2005-04-28改回
国家自然科学基金重点项目(60332030)资助课题

$\left(x, h=g^x\right)$。

发送者 S 的输入： $m_1, m_2, \cdots, m_n \in G$。

(1) R 把 $C=\left(g^{b_\delta} h^r, g^r\right)$ 发送给 S，这里 $r \in_R Z_q$ (表示 r 是 Z_q 中的一个随机数)。

(2) S 检查是否有 $c_1^q=1$， $c_2^q=1$；计算 $C'=\left(c_1^a g^k h^l, c_2^a g^l\right)$， $a,k,l \in_R Z_q$ 及 $E_i=m_i g^{ab_i+k}$； S 发送 C'， E_i 给 R。

(3) R 计算 $g^{ab_\delta+k}=c_1' c_2'^{-x}$，再打开密文 $m_\delta=E_\delta g^{-ab_\delta-k}$。

2.2 决策性Diffie-Hellman(DDH)假设

首先介绍计算性不可分辨的概念。称两个概率总体 $\{X_n\}$ 与 $\{Y_n\}$ 是计算性不可分辨的，如果对于任何一个概率多项式时间图灵分辨器(PPTM) D、任何一个多项式 $p(n)$ 及充分大的 n，

$$\left|\Pr\left[D(X_n)=1\right]-\Pr\left[D(Y_n)=1\right]\right|<1/p(n)。$$

由于对于 D 来说，X_n 与 Y_n 看起来相同，如果 D 不能由 X_n 计算出某一信息，它由 Y_n 也不能；反之亦然。

决策性 Diffie-Hellman(DDH)假设 设 g 是一个随机选择的阶为 q 的生成元，$a,b,c \in_R Z_q$，以下两个概率总体是计算性不可区分的： $Y_1=\left(g, g^a, g^b, g^{ab}\right)$ 与 $Y_2=\left(g, g^a, g^b, g^c\right)$。

3 基于 RSA 签名的对于一种不经意传输的接入控制方案

为了构造有效的不经意传输的接入控制，需要对RSA数字签名系统作适当的修正。本文使用了文献[5]所提出的对RSA数字签名系统添加的初始化阶段。

系统参数 消息 M 是接收者 R 的数字证书的内容，它含有接收者 R 的身份号， R 的权限，证书的有效期等信息，但不包含对 M 的签字。 N 是两个大素数的乘积，并且有 $N=p'q'=(2p+1)(2q+1)$， p， q 也是大素数。在 Z_N^* 中随机地取一数 $\bar{g}$。令 $g=\bar{g}^2 \bmod N$，那么 $\langle g\rangle$ 是一个阶为 pq 的循环群(g 的阶以很大的概率是 pq)，记为 G。群 G 的阶 pq 保密，但 pq 的 bit 长 l_G 公开。协议中随机的指数取自于 $\{0,1\}^{tl_G+1}$，这里 t 是一个大于 1 的安全参数。$H:\{0,1\}^* \to G$ 是一个安全的 Hash 函数。整数 $e\ (>2)$ 是系统的公钥。整数 d 满足: $ed=1 \bmod pq$， d 是系统的密钥，只有证书发放机构 CA 知道。证书发放机构对消息 M 的签字是 $\sigma=H(M)^d \bmod N$，只有 CA 和 R 知道而对发送者 S 保密。 M， H， e， N， g 为参与协议的各方所知。 $m_i\ (1\le i\le n)$ 是待发送的消息只有 S 知道。

(1) R 选择 $x \in \{0,1\}^{tl_G+1}$，计算 $h=g^x$ 并公开(以下若无特别声明群乘法运算均在 Z_N^* 中)； R 发送 $C=(C_1,C_2)=\left(\sigma g^{b_\delta} h^r, g^r\right)$ 给 S， r 是 $\{0,1\}^{tl_G+1}$ 中的一个随机数简记为 $\left(r \in_R \{0,1\}^{tl_G+1}\right)$。

(2) S 计算 $C_1'=C_1^{ea} H(M)^{-a} g^k h^l$， $C_2'=C_2^{ea} g^l$， $E_i=m_i g^{eab_i+k}\ (1\le i\le n)$， $k,l \in_R \{0,1\}^{\tau l_G+1}$， $C'=\left(C_1', C_2'\right)$. S 把 $\left(C', E_i\right)$ 发送给 R。

(3) R 计算 $g^{eab_\delta+k}=C_1'\left(C_2'\right)^{-x}$， $m_\delta=E_\delta g^{-eab_\delta-k}$。

若消息 m_i 的长度超过 Z_N^* 中的群元素的长度，(2)中的加密 E_i 可采用以 g^{eab_i+k} 为密钥的对称加密。

方案的正确性 接收者 R 发送的消息 C 是对 σg^{b_δ} 的以 h 为公钥的Elgamal加密[6]。根据Elgamal加密的同态性， C' 是对 $\left(\sigma g^{b_\delta}\right)^{ea} g^k H(M)^{-a}$ 的以 h 为公钥的Elgamal加密。 接收者 R 若持有签字就能由 C' 解密出 $g^{eab_\delta+k}$ 从而得到消息 m_δ。

方案的有效性 与文献[4]中的协议相比较，本方案通信量不变，计算量略有增加。接收者 R 只需增加一个模乘法运算(此计算负担可忽略)；发送者需增加一个低指数(指数是 e)的模幂运算(此计算负担可忽略)及一个模逆运算。

4 安全性分析

接收者 R 发送的密文 C 是对消息 σg^{b_δ} 的以 h 为公钥的Elgamal加密，由Elgamal加密的语义安全性[7]可知，在DDH假设成立的条件下，接收者是否持有签名及接收者的选择 b_δ 是安全的。

在DDH假设成立的条件下发送者是安全的，即接收者不能得到他没有选择的消息，此结论可采用文献[4]中的安全性分析的方法得到，在此省略。

以下证明在RSA签名安全及DDH假设成立的条件下，不持有签字的攻击者在执行完协议后不能得到任何消息 $m_i\ (1\le i\le n)$。

定理 在DDH假设成立的条件下，不持有签字的接收者在执行完协议后不能得到任何消息。

证明 通过对理想实现的一个模拟来证明安全性。构造一个提取器来提取接收者的密钥。这样模拟器就可以解密接收者在协议第一阶段发送给发送者的消息。

(1) 模拟器选择随机数 $a,k,l \in_R \{0,1\}^{tl_G+1}$。

(2) 模拟器计算 $C'=\left(c^{ea} H(M)^{-a} g^k, g^l\right)$。

(3) 对于 $1\le i\le n$ 模拟器选择 $E_i \in_R G$。

以下证明在DDH假设下真实的协议与模拟协议不可区分。

假设存在一个不持有签名的攻击者 $\mathcal{A}$ 能够区分真实的协议和模拟的协议。在模拟协议中除 E_i 而外接收者所有其余观察值与真实协议一致。在真实协议中 E_i 的形式为 $E_i=m_i g^{eab_i+k}\ (1\le i\le n)$，而在模拟的协议中 E_i 为随机选取。

定义 $n+1$ 个分布 $\mathcal{D}_0,\cdots,\mathcal{D}_n$： 模拟攻击者计算 C 并选择 $C' \in_R G^2$。假设 $c=g^y$ 是 C 中的被加密的明文，模拟器选择 $a \in_R \{0,1\}^{tl_G+1}$，那么存在一个值 $k \in \{0,1\}^{tl_G+1}$ 使得 C' 是 $g^{yea+k} H(M)^{-a}$ 的Elgamal加密(模拟器不知道 k)。在分布 $\mathcal{D}_j$ 中元素 $E_i\ (1\le i\le j)$ 设为 $m_i g^{eab_i+\hat{k}}$，这里 $\hat{k} \in_R \{0,1\}^{tl_G+1}$。 E_i 的其余值随机地取自于 G。注意到在分布 $\mathcal{D}_0$ 中所有的 E_i 都是随机取值，也就是 $\mathcal{D}_0$ 出现在模拟协议中。

首先证明在DDH假设下 $\mathcal{D}_0$ 与 $\mathcal{D}_n$ 是计算性不可分辨的。假设存在一个攻击算法 $\mathcal{A}$ 可以区分 $\mathcal{D}_0$ 与 $\mathcal{D}_n$，那么存在一个指数 μ 算法 $\mathcal{A}$ 也可以区分 $\mathcal{D}_\mu$ 与 $\mathcal{D}_{\mu+1}$ $(1\le\mu\le n-1)$。利用算法 $\mathcal{A}$ 构造一个算法 $\mathcal{A}^*$ 能够区分 $\left(g,g^{ea},g^b,g^{eab}\right)$ 与 $\left(g,g^{ea},g^b,g^r\right)$，这里 a，b，r 是随机数。设 $\left(g,g^a,g^b,\bar{g}\right)$ 是一个DDH问题的实例。算法 $\mathcal{A}^*$ 如下:

(1) 选择 $m_1,m_2,\cdots,m_n\in G$，其分布与真实协议相同;

(2) 随机地选择 $1<\tau\le n$ (τ 代表指数的分布);

(3) 随机地选择 b_i $(1\le i\le n)$，输出 $g^{b_1},\cdots,g^{b_{\tau-1}}$，$g^b$，$g^{b_{\tau+1}},\cdots,g^{b_n}$；

(4) 像 $\mathcal{A}$ 一样计算 C。C 是 g^y 的Elgamal加密;

(5) 选择 $a,k,l\in_R\{0,1\}^{tl_G+1}$，设 $C'=\left(g^{eay+k}H(M)^{-a}h^l,\ g^l\right)$;

(6) 设 $E_i=m_ig^{eab_i+k}$ $(1<i<\tau)$;

(7) 设 $E_\tau=m_\tau\bar{g}g^k$;

(8) 选择 $E_i\in_R G$ $(\tau<i\le n)$;

(9) 与 m_i 一起的其余的输出与算法 $\mathcal{A}$ 的输入相同。

在真实协议中 $C_2=g^r$ 转换为 $C_2'=g^{ear+l}$，l 用来随机化密文。没有此随机值 l 以上的模拟器不能工作。因为模拟器仅仅知道 g^{ea} 和 g^r 而不知道 a 和 r，这样它不能计算 g^{ear}。

如果 $\bar{g}=g^{eab}$，那么所构造的分布与 $\mathcal{D}_\tau$ 相同，否则与 $\mathcal{D}_{\tau-1}$ 相同。因此有

$$\left|\Pr\left(\mathcal{A}^*\left(g,g^{ea},g^b,g^{eab}\right)\right)-\Pr\left(\mathcal{A}^*\left(g,g^{ea},g^b,g^r\right)\right)\right|>\frac{1}{np(n')}$$

因子 n 与 τ 的选择有关。以上的不等式与DDH假设矛盾。

这就证明了在DDH假设下 $\mathcal{D}_0$ 与 D_n 是计算性不可分辨的。以下只需证明在DDH假设下算法 $\mathcal{A}$ 不能区分 D_n 与 $\mathcal{D}$，这里 $\mathcal{D}$ 是执行完真实协议的分布。在真实协议中 $k=\hat{k}$，而在模拟协议中 k 与 $\hat{k}$ 不同。$c=g^y$ 是接收者发送的消息的明文。由 C' 算法 $\mathcal{A}$ 得到 $g^{yea+k}H(M)^{-a}$ 计算 $g^{yea+k}H(M)^{-a}\cdot(E_i)^{-1}m_i$，算法 $\mathcal{A}$ 由分布 $\mathcal{D}$ 得到 $\left(g^{e(y-b_i)}/H(M)\right)^a$，而由分布 $\mathcal{D}_n$ 得到 $\left(g^{e(y-b_i)}/H(M)\right)^a g^{k-\hat{k}}$。$\mathcal{A}$ 能够区分 $\mathcal{D}_n$ 与 $\mathcal{D}$ 当且仅当它在给定 g，g^a，$g^{e(y-b_i)}/H(M)$ 时能够区分 $\left(g^{e(y-b_i)}/H(M)\right)^a$ 与一个随机元素。这与DDH假设矛盾。

因此，在DDH假设下真实协议与模拟协议不可区分。不持有签字的接收者不能得到任何消息。　　证毕

与已有方案的比较　与已有的基于数据串的不经意传输协议[4]相比，本方案通信量不变，计算量略有增加，但本协议有机地结合了基于证书授权的接入控制功能；同时发送方不能确定接收方是否持有签字(授权证书)，保护了接收方的隐私。

5　结束语

本文对于不经意传输提出了基于证书的接入控制方案，该方案中发送者不能确定接收者的身份，这种接入控制是不经意的。本方案使用RSA签名，系统建立后协议不需要第三方参与，参与协议的双方不需要陷门信息。本方案基于证书授权，扩展了RSA数字证书的用途，同时保护了证书持有者的隐私。本方案与文献[4]中的方案相比，通信量相同计算代价略高，而增加了对于接收者的接入控制功能。这种接入控制基于标准的RSA签名，因此本方案有助于不经意传输协议的实用化。本方案采用Elgamal公钥加密，由于加密的同态性，可以容易的推广到价格不同的不经意传输协议[8]的情形。本方案具有可证明的安全性。

参 考 文 献

[1] Rabin M. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard Univ., 1981.

[2] Li Ninghui, Du Wenliang, Boneh Dan. Oblivious signature-based envelope[A]. In Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003)[C], Boston, Massachusetts, ACM Press, New York, July 2003：182−189.

[3] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public key cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120–126.

[4] Tobias Christian. Practical oblivious transfer protocols. [A]. 5th International Workshop on Information Hiding(IH 2002)[C]. Springer Verlag, LNCS 2578，Noordwijkerhout, The Netherlands, October 2002：415−426.

[5] Ateniese G. Verifiable encryption of digital signatures and applications[J]. *ACM Transactions on Information and System Security*, 2004，7(1): 1−20.

[6] ElGamal T. A Public key cryptosystem and a signature scheme based on discrete logarithms[J]. *IEEE Trans. Information Theory*, 1985, 31(4): 469−472.

[7] Tsiounis Y, Yung M. On the security of ElGamal-based encryption[A]. Proc. of PKC '98[C]. Springer Verlag, LNCS 1431, Yokohama, Japan, 1998: 117−134.

[8] Aiello B, Ishai Y, Reingold O. Priced oblivious transfer: How to sell digital goods[A]. Proc. Advances in Cryptology (Eurocrypt'01)[C]. Springer Verlag, LNCS 2045, Innsbruck, Austria, 2001: 119−135.

赵春明：　男，1967年生，博士生，研究方向为密码学与信息安全.

葛建华：　男，1961年生，教授，博士生导师，研究方向为数字多媒体技术、信息论、密码学与信息安全.

李新国：　男，1976年生，博士生，研究方向为密码学与信息安全.