基于数字签名的增强的不经意传输协议

赵春明 葛建华 李新国
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 该文在离散对数类数字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(Decisional Diffie-Hellman)假设和随机预言模型下该文所提协议具有可证明的安全性。

关键词 接入控制，Elgamal 加密，不经意传输，Schnorr 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(2005)02-0303-04

Signature-Based Enhanced Oblivious Transfer

Zhao Chun-ming Ge Jiang-hua Li Xin-guo
(*National Key Lab of Integrated Service Network, Xidian University, Xi'an* 710071, *China*)

Abstract Based on Schnorr (Elgamal) signature and (string) oblivious transfer, an enhanced 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.

Key words Access control, Elgamal encryption, Oblivious transfer , Schnorr signature, Decisional Diffie-Hellman(DDH) assumption.

1 引言

不经意的传输协议首先由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协议设计中有着广泛的应用。简单地说, 这种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。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。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不经意的接入控制方案, 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)及授权者的公钥等非敏感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接收者相联系. 本文采用这一思想提出了基于 Schnorr 及 Elgamal 数字签名的一种不经意的传输协议，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，即该协议是一种增强的不经意传输协议。

2004-08-03 收到，2005-02-07 收到
国家自然科学基金重点项目(60332030)资助课题

2 协议的基础

2.1 1-out-of-n 不经意传输协议

Tzeng 在文献[3]中提出了一种对于数据串的有效的1-out-of-n不经意的传输协议. 简述如下：

系统参数：(g,h,G)，G 是一个 q 阶循环群，g，h 是 G 的两个生成元，$\log_g^h$ 保密；

发送者 S 的输入：$m_1,m_2,\cdots,m_n \in G$；

接收者 R 的选择：α，$1\le\alpha\le n$。

(1) R 发送 $y=g^r h^\alpha \bmod p$ (以下群 G 中模运算符号均省略)，$r\in_R Z_q$ (r 是 R 从 Z_q 中取的一个随机数)；

(2) S 发送 $c_i=\left(g^{k_i},m_i\left(y/h^i\right)^{k_i}\right)$， $k_i\in{}_RZ_q$， $1\le i\le n$；

(3) 由 $c_\alpha=(a,b)$， R 计算 $m_\alpha=b/a^r$。

2.2 决策性Diffie-Hellman(DDH)假设

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，$a,b,c\in{}_RZ_q$，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 $Y_2=\left(g,g^a,g^b,g^c\right)$。

计算性Diffie-Hellman(CDH)假设：给定 $\left(g,g^a,g^b\right)$，不存在有效概率多项式时间图灵机(PPTM)算法能以不可忽略的概率计算出 g^{ab}。

3 基于 Schnorr 签名的对于不经意传输的接入控制方案

首先简述Schnorr签名方案[4]。系统参数：p，q 是两个大素数，$q\mid p-1$，g 是一个阶为 q 的生成元，$x\in Z_q^*$，x 是私钥，$y=g^x$ 是公钥，$H:\{0,1\}^*\to Z_q$ 是一个安全的hash函数。签名：M 是待签名的消息，签名者从 Z_q 中选择一个随机数 k (简记为 $k\in{}_RZ_q$)，然后计算 $e=H(M\|r)$，$r=g^k$，$s=k-xH(M\|r)\bmod q$。那么，数对 (e,s) 是对于消息 M 的签名。验证：签名接收者计算 $r'=g^sy^e$。当且仅当方程 $e=H(M\|r')$ 成立时，(e,s) 是对于消息 M 的有效签名。

对于不经意传输的接入控制方案:

系统建立：G 是一个 q 阶循环群，g 是 G 的一个生成元；M 是发放给接收者 R 的证书的内容. $x\in Z_q^*$，x 是系统密钥，$y=g^x$ 是公钥，(e,s) 是对于 M 的 Schnorr 签名。该签名 (e,s) 由权威机构 CA 通过秘密信道发送给 R，对外保密。系统参数 q，g 及 CA 的公钥 y 公开。

发送者 S 的输入：$m_1,m_2,\cdots,m_n\in G$，R 的证书的内容 M。

接收者 R 的输入：R 的选择 α，$1\le\alpha\le n$，M 及其签名 (e,s)。

(1) R 随机选择 $t,u\in[1\cdots2^{t_1}q]$，这里 t_1 是一个大于 1 的安全参数; 计算 $r'=g^sy^e$，$s'=s+t\bmod q$；R 把 $\left(r',s',g^uy^\alpha\right)$ 发送给 S。

(2) S 计算 $a=g^l$，$b_i=g^{v_i}$，$c_i=m_i\left(g^{s'}y^{H(M\|r')}/r'\right)^l\left(g^uy^\alpha/y^i\right)^{v_i}$，这里 $v_i,l\in{}_RZ_q/\{0\}$，$(1\le i\le n)$。S 把 $C=(a,b_i,c_i)$ 发送给 R。

(3) 由 $C=(a,b_i,c_i)$，R 打开消息 $m_\alpha=c_\alpha/a^tb_\alpha^u$。

方案的正确性：R 持有签名，$r'=g^sy^e=r$。S 发送的密文是 $c_\alpha=m_\alpha\left(g^{s+t}y^{H(M\|r)}/r\right)^l\left(g^uy^\alpha/y^\alpha\right)^{v_\alpha}=m_\alpha g^{tl}g^{uv_\alpha}$。$R$ 知道 t 和 u，他可由 a，b_α 计算出 $g^{tl}g^{uv_\alpha}$，从而解密出 m_α。

协议说明: 在协议的第一步 R 对签名 s 及选择 α 进行了部分盲化处理；在协议的第三步 S 对所有的消息 m_i $(1\le i\le n)$ 进行了两次变形的 Elgamal 加密，这种变形使得解密必须具备两个条件，即 R 持有签名且只能解密一个消息。

4 方案的安全性分析

接收者 R 是否持有签名及接收者 R 的选择 α 是无条件安全的。对于偷听者，本方案的安全性类似于Elgamal加密方案。在DDH问题是困难的条件下接收者 R 不能得到其余 m_i $(i\ne\alpha)$ 的任何信息。在CDH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密钥。

由于 t 是 R 在 $[1\cdots2^{t_1}q]$ 中随机选择的，S 只可能由 (r,s') 计算出 e，不能计算出 s，S 不能通过计算得到 (e,s) 以验证 R 是否持有签名；再者原签名 (e,s) 对 S 是保密的，S 不可能通过比较知道 R 是否持有签名。

定理1 发送者得不到接收者是否持有签名的任何信息。

证明 假设一个不持有签名的接收者 R' 发送的随机的消息是 $\left(g^{k'},t'\bmod q\right)$ (不考虑 R' 的选择 α)，这里 $k'\in_RZ_q$,$t'\in_R[1\cdots2^{t_1}q]$。只需证明 R 在协议的第一阶段发送的信息 (r,s') 与随机的信息在统计上无法区分。它们分别来自于分布族:

$$\delta^0(k,t)=\left\langle g^k\bmod p,(t+s)\bmod q\mid k\in_RZ_q,t\in_R[1...2^{t_1}q]\right\rangle$$

$$\delta^1(k',t')=\left\langle g^{k'}\bmod p,t'\bmod q\mid k'\in_RZ_q,t'\in_R[1...2^{t_1}q]\right\rangle$$

而 $\delta^0(k,t)$ 与 $\delta^1(k',t')$ 在统计上是不可区分的。

这是由于对于任何固定的 t_1，以上两个分布族都有 q^2 个点。取任何一点，两个分布族概率的差不超过 $1/2^{t_1}q^2$；总体上，两个分布族概率之差不超过 $1/2^{t_1}$，相对于 t_1 此值是可以忽略的。

因此接收者是否持有签名是无条件安全的。 证毕

定理2 接收者 R 的选择 α 是无条件安全的，发送者 S 得不到 α 的任何信息。

证明 存在 u' 及 α' 满足 $g^uy^\alpha=g^{u'}y^{\alpha'}$，所以 R 的选择 α 是无条件安全的，即使 S 有无限的计算能力也不能得到 α 的任何信息。 证毕

定理 3 在 CDH 假设成立的条件下，不持有签字的攻击者 R' 在执行完协议后不能得到任何密钥。

证明 因为 S 使用了两重 Elgamal 加密，要解密需要密钥 $\left(g^{s'}y^{H(M\|r')}/r'\right)^l$ 及 $\left(g^uy^\alpha/y^i\right)^{v_i}$。假设攻击者经过信息交互阶段以后能够计算出密钥 $\left(g^{s'}y^{H(M\|r')}/r'\right)^l$。设 $s=k'-xH(M\|r')\bmod q$，$e=H(M\|r')$ (这里 k' 满足

$g^{k'}=r'$), 那么(e,s)是对于消息M的一个Schnorr签名。接收者R'不可能知道此签名。由于R'知道s'和g^l，那么他可计算出$g^{s'l}$。由于方程$\left(g^{s'}y^{H(M\|r')}/r'\right)^l=g^{(s'-s)l}$成立, 他可根据$\left(g^{s'}y^{H(M\|r')}/r'\right)^l$和$g^{s'l}$计算出$g^{sl}$。这也就是$R'$解决了以下的CDH问题: 给定$g^s$ (由于$g^s=r'/y^{H(M\|r')}$，R'知道此值) 和g^l， 计算g^{sl}。

因此，在计算性CDH假设成立的条件下不持有对消息m的Schnorr签名的接收者不能计算出密钥。

证毕

定理4　在DDH假设成立条件下, 半可信的接收者R不能得到其余m_i $(1\le i\ne\alpha\le n)$的任何信息。也就是，即使R知道(u,α)，对R来说$E_i=(g,y,C)$ $(1\le i\ne\alpha\le n)$与随机的消息$X=(g,y,a,b)$ ($a,b\in_R G\setminus\{1\}$)也是计算性不可分辨的。

证明　首先，R不能计算出两个对(α,u)，(α',u')使得下式成立: $g^{\alpha}y^{u}=g^{\alpha'}y^{u'}$,不然，$R$可以求出$\log_g^y=\dfrac{u-u'}{\alpha-\alpha'}$。在DDH假设成立的条件下这是不可能的。因此$R$不能得到两个秘密。

其次，R接收到的消息是:

$$C=\left(g^l,g^{v_i},m_i\left(g^{s'}y^{H(M\|r)}/r\right)^l\left(g^uy^{\alpha}/y^i\right)^{v_i}\right)$$

$$=\left(g^l,g^{v_i},m_i\left(g^{l(s'-s)}\right)g^{v_iu}y^{v_i(\alpha-i)}\right)$$

虽然R可由g^l及$s'-s$计算出$g^{l(s'-s)}$，从而得到$m_ig^{v_iu}y^{v_i(\alpha-i)}$，但是只需证明对每个$i\ne\alpha$， $m_ig^{v_iu}y^{v_i(\alpha-i)}$看起来是随机的。以下予以证明：

设$E_i'=\left(g,g^u,g^{v_i},m_ig^{v_iu}y^{v_i(\alpha-i)}\right)$，$X=(r_1,r_2,r_3,r_4)$，这里$r_1,r_3\in_R G/\{1\}$，$r_2,r_4\in_R G$。只需证明，如果$E_i'$与$X$能被一个PPTM分辨器$D$所区分，那么DDH问题中的$Y_1$与$Y_2$能被以下的一个以$D$作子程序的PPTM分辨器$D'$所区分：

输入：(g,w_1,w_2,w_3)(来自于Y_1或Y_2)

(1)若$w_1=1$，则输出1；

(2)随机的选取$u\in Z_q$；

(3)若$D\left(g,w_1,w_2,m_iw_1^uw_1^{\alpha-i}\right)=1$，则输出1，否则输出0。

可以看出，如果$(g,w_1,w_2,w_3)=\left(g,g^a,g^b,g^{ab}\right)$来自于$Y_1$且$a\ne0$,

$$\left(g,w_1,w_2,m_iv^uw^{\alpha-i}\right)=\left(g,y,g^b,m_i\left(g^uy^{\alpha-i}\right)\right)$$

具有E_i'中元素的形式，这里$y=w_1$。如果$(g,w_1,w_2,w_3)=\left(g,g^a,g^b,g^{ab}\right)$来自于$Y_2$且$a\ne0$，$\left(g,w_1,w_2,m_iw_2^uw_3^{\alpha-i}\right)=\left(g,y,g^b,m_i\left(g^uy^{\alpha-i}\right)\right)$均匀地分布于$G/\{1\}\times G/\{1\}\times G\times G=X$。因此，如果$D$能以不可忽略地占优势的概率$\varepsilon$区分$E_i'$与$X$，则$D'$能以占优势的概率$\varepsilon(1-1/t)+1/t$区分$Y_1$与$Y_2$，这里$1/t$是第(1)步的概率。

在DDH假设成立的条件下，R即使知道(α,u)，E_i'对其是计算性不可分辨的，从而E_i也是。　　证毕

5　在随机预言模型下的协议

系统建立与前相同。

(1) R随机选择$t,u\in[1\cdots2^{t_1}q]$，这里τ是一个大于1的安全参数; 计算$r'=g^sy^{-e}$，$s'=s+t \bmod q$； R把$\left(r',s',g^uy^{\alpha}\right)$发送给$S$。

(2) S把$C=\left(g^l,g^v,m_i\oplus H\left(g^{s'}y^{H(M\|r')}/r'\right)^l\left(\|\left(g^uy^{\alpha}/y^i\right)^v\|i\right)\right)=(a,b,c_i)$，$(1\le i\le n)$发送给$R$，这里$l,v\in_R Z_q/\{0\}$。

(3) 由$C=(a,b,c_i)$，R打开消息$m_{\alpha}=c_{\alpha}\oplus H\left(a^t\|b^u\|i\right)$。

定理 5　在随机预言模型和CDH假设成立的条件下上述协议满足发送者和接收者的安全需求。

证明　由定理1及定理2, 接收者是否持有签字及接收者的选择α是无条件安全的。

在随机预言模型下，为得到$H\left(\left(g^{s'}y^{H(M\|r')}/r'\right)^l\|\left(g^uy^{\alpha}/y^i\right)^v\|i\right)$，询问hash函数必须知到$\left(g^{s'}y^{H(M\|r')}/r'\right)^l$及$\left(g^uy^{\alpha}/y^i\right)^v$的全部信息。由定理4，在CDH假设成立的条件下不持有签名的攻击者不能得到任何一个$\left(g^{s'}y^{H(M\|r')}/r'\right)^l$；而恶意的接收者$R$不可能计算出两个相等的值$t_1=\left(g^uy^{\alpha}/y^i\right)^v$与$t_2=\left(g^uy^{\alpha}/y^j\right)^v$，$i\ne j$；否则他可以计算$y^{v(j-i)}=t_1/t_2$。这也就是他能解决以下的CDH问题：给定$g^{(j-i)}$，$g^{(j-i)k}$，$y^{(j-i)}$计算$y^{(j-i)k}$。因此$R$不能以不可忽略的概率计算出两个密钥。

以下对于理想模型的模拟器R'输出一个与R的观察值不可分辨的概率分布：

(1) 模拟R产生$\bar{r}'$；

(2) 随机选择 $\bar{c}_i$，$1\le i\le n$；

(3) 模拟S输入$\bar{r}'$ (模拟器不知道m_is，m_is是对m_i的模拟)获得$\bar{v}$并计算$\bar{b}=g^{\bar{v}}$；

(4) 模拟R输入$\bar{a}$，$\bar{b}$及$\bar{c}_is$ ($\bar{c}_is$是对$\bar{c}_i$的模拟)询问hash函数。如果R询问$\left(\bar{a}^{(s'-s)},z,j\right)$，这里$z=\left(g^uy^{\alpha}/y^j\right)^{\bar{v}}$ ($j=\alpha$)R'把j发给可信第三方获得m_j返回$H=\bar{c}_j\oplus m_j$作为hash值$H\left(\bar{a}^{(s'-s)}\|z\|j\right)$；否则，若此hash值与以前询问的hash值

相同， R' 返回一个随机的hash值;

(5) 输出 $\left(\bar{a},\bar{r}',\bar{b},\bar{c}_1,\bar{c}_2,\cdots,\bar{c}_n\right)$。

当 R 询问 $\left(\bar{a}^{(s'-s)},z,j\right)$，这里 $z=\left(\bar{r}'/y^j\right)^{\bar{v}}$，他必须知道 $\bar{t}$，使得 $g^{\bar{t}}=\bar{r}'/y^j$。否则，他可由 $g^{\bar{t}}$ 及 $g^{\bar{v}}$ 计算 $g^{\overline{tv}}$ 这与CDH假设矛盾。因此， j 是 R 的选择。由上可知，模拟器 R' 不能以不可忽略的概率询问hash函数得到另一 $\left(\bar{a}^{(s'-s)},\left(\bar{r}'/y^i\right)^{\bar{v}},i\right)$，$i\neq j$。其余所有 $\bar{c}_i$，$i\neq j$，分布相同。R' 的输出与 R 的观察值是计算性不可分辨的。因此恶意的接收者不能得到他没有选择的消息。 证毕

6 基于Elgamal签名的增强的不经意传输

Elgamal签名方案简述如下[5]。系统参数：输入安全参数 t，输出系统参数，p 是一个大素数，g 是一个阶为 $p-1$ 的生成元，x 是私钥，$y=g^x$ 是公钥。签名:签名者选择 $k\in_R Z_{p-1}/\{0,1\}$，计算 $r=g^k$，$s=\left(\left(H(M)-xr\right)k^{-1}\bmod(p-1)\right)$。验证: 当且仅当方程 $y^r r^s=g^{H(M)}$ 成立时数对 (r,s) 是对消息 M 的有效签名。

基于 Elgamal 签名的增强的不经意传输:

系统建立：G 是一个 $p-1$ 阶循环群，g 是 G 的一个生成元；M 是发放给接收者 R 的证书的内容。$x\in Z_{p-1}^*$，x 是系统密钥，$y=g^x$ 是公钥，(r,s) 是对于 M 的 Elgamal 签名。该签名 (r,s) 由权威机构 CA 通过秘密信道发送给 R,对外保密。系统参数 p, g 及 CA 的公钥 y 公开。

发送者 S 的输入： $m_1,m_2,\cdots,m_n\in G$， R 的证书的内容 M。

接收者 R 的输入： R 的选择 α，$1\le\alpha\le n$，M 及其签名 (r,s)。

(1) R 随机选择 $t,u\in[1\cdots 2^{t_1}(p-1)]$，这里 t_1 是一个大于1的安全参数； $s'=s+t\bmod p-1$; R 把 $\left(r,s',g^u y^\alpha\right)$ 发送给 S。

(2) S 把 $C=\left(r^l,g^{v_i},m_i\left(r^{s'}y^r/g^{H(M)}\right)^l\left(g^u y^\alpha/y^i\right)^{v_i}\right)$ 发送给 R，这里 $l,v_i\in_R Z_{p-1}/\{0\}$。

(3) 由 $C=(a,b_i,c_i)$， R 打开消息 $m_\alpha=c_\alpha/a^t b_\alpha^u$。

协议说明: 由于对于 Elgamal 签名有 $r^s=g^{H(M)}y^{-r}$，所以 $\left(r^{s'}y^r/g^{H(M)}\right)^l=r^{tl}$，这样 R 与 S 能够有条件密钥协商；除此而外此协议与基于 Schnorr 签名的协议思路相同。其安全性分析从略。

7 结束语

本文利用基于签名的电子信封[2]的思想，在关于数据串的不经意传输协议[3]基础上提出了基于签名的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本文所提协议具有可证明的安全性。本文所提协议与文献[3]相比通信负担与计算量略有增加但具备了不经意的接入控制功能。

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. In Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003), Boston, Massachusetts, July 2003, New York, ACM Press, 2003: 182 – 189.

[3] Tzeng W G. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters[J]. *IEEE Trans. on Computers*, 2004, 53(2) : 232 – 240.

[4] Schnorr C. Efficient identification and signature for smart cards. In: Advances in Cryptology-Crypto'89, volume 435 of Lecture Notes in Computer Science, Berlin, Springer-Verlag, 1990: 235 – 251.

[5] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Information Theory*, 1985, 31(4): 469 – 472.

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.