# 隐藏认证的有条件不经意传输

赵春明，葛建华，李新国

(西安电子科技大学 综合业务网理论与关键技术国家重点实验室，陕西 西安 710071)

**摘要**：在不经意属性证书和隐藏证书的基础上提出了隐藏认证的有条件不经意传输，利用双线性对构造了一个具体方案，解决了不经意属性证书可能暴露接收者的某些敏感信息的问题. 该方案有如下特点：只有持有特定属性证书的接收者才能打开与其属性值相对应的消息，而接收者不需要向发送者提供任何证书. 发送者不能确定接收者是否能够打开消息也不能确定接受者打开的是哪个消息.

**关键词**：不经意属性证书；双线性对；有条件不经意传输；隐藏证书

**中图分类号**：TP309 **文献标识码**：A **文章编号**：1001-2400(2006)06-0849-04

# Hidden authentication conditional oblivious transfer

*ZHAO Chun-ming*, *GE Jian-hua*, *LI Xin-guo*

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

**Abstract**: Hidden authentication conditional oblivious transfer based on oblivious attribute credentials (OACerts) and hidden credentials is proposed and a scheme based on bilinear pairing for implementing the idea is constructed which solves the problem that OACerts may exposure some sensitive information of the receiver. The scheme proposed has the property that only the receiver who has the required attribute credentials can open the message corresponding to its attribute value and that the receiver need not provide to the sender any credentials. The sender can not decide whether or not the receiver can open the messages and which message he can open.

**Key Words**: oblivious attribute credentials; bilinear pairing; conditional oblivious transfer; hidden credentials

不经意传输[1,2]是密码学中一种基本构件，这类协议在密码学和协议设计中有着广泛的应用[1~3]. 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. 有条件不经意传输[4,5]是服务需求方(接收者)向服务提供方(发送者)传送其秘密数值的有关信息，若接收者的数值大于发送者预先设定的数值则可打开发送者提供的第一个密文；否则，接收者可打开第二个密文. 在此过程中，发送者不能确定接收者打开的是哪一个. 实际的信息系统中接收者的输入需要得到权威机构(CA)认证，而发送者的访问策略也可以公开. 例如在信任管理和基于证书的访问控制系统[6]中，控制决策基于接收者的属性特征. 由于属性特征的敏感性，为保护接收者的隐私，Li 等提出不经意属性证书[7]，由权威机构对属性的数值构造一个 Pedersen 承诺[8]，然后签署该承诺，产生该承诺的数字证书. 接收者得到可打开承诺的秘密信息及数字证书. 接收者在请求提供服务时必须把某个属性值的承诺及其数字证书传递给发送者. 发送者验证此证书，然后利用上述承诺并依照自己的访问控制策略产生对要发送消息的密文. 接收者使用可打开承诺的秘密信息来打开密文.

Li 的方案[7]中，接收者必须提供对承诺的标准数字证书，这就暴露了接收者的某些敏感信息. 比如，接收者的会员资格属性证书，发送者由承诺及证书即可判断接收者属于哪一类的会员，尽管发送者不知道其是这一类中的哪一种.

利用隐藏证书[9]和 Li 等提出的将承诺及打开承诺的秘密分拆的方法[7]，笔者构造了隐藏认证的有条件

收稿日期：2006-01-21

基金项目：国家自然科学基金资助项目(60332030)

作者简介：赵春明(1967-)，男，西安电子科技大学博士研究生.

不经意传输(HACOT). 发送者的访问策略是:若接收者的经过认证的属性值大于或等于某一指定值则收到第一个消息;若此属性值小于指定值则收到第二个消息. 而在此过程中发送者既不能确定接收者是否能够得到消息也不能确定得到哪一个消息. 这也解决了文献[9]提出的一个公开问题,如何利用隐藏证书实现比较属性数值的访问控制策略.

## 1 协议的基础

(1) 双线性对及有关安全性假设[10] 设 $G_1$ 和 $G_2$ 是两个阶为大素数 $q$ 的循环群. $\hat{e}:G_1\times G_1\to G_2$ 是一个满足以下条件的双线性映射.

① 双线性 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ 对于任何 $P,Q\in G_1$ 与 $a,b\in Z$ 成立.

② 非退化性 存在 $P,Q\in G_1$ 使 $\hat{e}(P,Q)\neq 1$.

③ 可计算性 存在有效算法,对于 $P,Q\in G_1$ 可计算 $\hat{e}(P,Q)$.

对于以上定义有以下难解问题作为安全假设:

① 离散对数问题 设 $P,Q\in G_1$,寻找一个整数 $n$ 使得 $P=nQ$.

② 计算性 Diffie-Hellman(CDH)问题 对于任意的 $a,b\in Z_q$,假设一个三元组 $P,aP,bP\in G_1$,寻找 $abP$.

③ 双线性 Diffie-Hellman (BDH)问题 $a,b,c\in Z_q$,假设一个三元组 $aP,bP,cP\in G_1$,寻找 $\hat{e}(P,P)^{abc}$.

一般地,取 $q$ 为 160 比特的素数可保证上述安全假设成立[10].

(2) 隐藏证书 隐藏证书方案[9]是发送者加密一个消息,只有持有满足发送者访问策略证书的接收者才可解密. 接收者可以非交互式地解密消息而发送者不必知道接收者是否持有证书.

隐藏证书方案有以下 4 个函数:CA_Create(),CA_Issue($N,A$),$\mathrm{HC_E}(M,N,P)$及 $\mathrm{HC_D}(C,C')$,其功能依次是建立一个 CA 产生其私钥、公钥对并公布此公钥,产生对假名为 $N$ 的用户属性 $A$ 的证书,根据对用户必须具备的属性特征的访问策略 $P$ 加密消息 $M$,使用证书 $C'$ 解密密文 $C$.

文献[9]使用双线性对在 BDH 假设下构造了隐藏证书的具体实现方案.

## 2 隐藏认证的有条件不经意传输(HACOT)

### 2.1 HACOT 概述

隐藏认证的有条件不经意传输使得接收者的经过认证的属性值(认证该值的承诺)大于或等于发送者的某限定值时则收到第一个消息;若此属性值小于指定值则收到第二个消息. 而在此过程中发送者既不能确定接收者是否能够得到消息也不能确定得到哪一个消息. HACOT 协议有以下 5 个阶段:

系统建立 CA 产生用于 Pedersen 承诺[8]及发放隐藏证书的公开参数.

产生承诺及证书 $R$ 通过安全信道将属性值及用来识别用户的假名($N$)发送给 CA. CA 产生对此属性值的承诺并签署该承诺. CA 将用来打开承诺的秘密信息和对承诺的签名通过安全信道发送给 $R$.

初始化 $S$ 公开其访问策略. $S$ 选定一个限定范围的某确定值,若 $R$ 的被 CA 承诺(该承诺值必须获得 CA 认证)的属性值大于或等于限定值则得到第一个消息,否则得到第二个消息.

信息交互 $R$ 根据 $S$ 的访问策略将自己属性值的承诺分拆,并将其及 $N$ 发送给 $S$. $S$ 由收到的信息并根据系统公钥和访问策略对自己的消息加密. $S$ 将密文发送给 $R$.

打开密文 $S$ 用自己的秘密信息打开相应于其属性值的密文.

### 2.2 HACOT 的实现方案

系统建立 CA 产生系统公开参数 $P_0=<q,G_1,G_2,P,Q,\hat{e},l,s,H_1,H_2,H_3,H_4,E,D>$,$q$ 是一个大素数,$G_1,G_2$ 是阶为 $q$ 的群. $\hat{e}$ 是 $G_1\times G_1$ 到 $G_2$ 的非退化双线性对. $P,Q$ 是 $G_1$ 的两个生成元,$Q$ 对于 $P$ 的离散对数保密. 系统的公钥是 $P_{\mathrm{PUB}}=s_{\mathrm{CA}}P$,相应的私钥是 $s_{\mathrm{CA}}$. $l$ 满足 $2^l<q/2$,$V=[0,\cdots,2^l-1]$ 表示某一属性的数值 $a$ 的取值范围,用来识别用户 $R$ 的假名 $N\in\{0,1\}^{l'}$. $H_1,H_2,H_3,H_4$ 是如下的 hash 函数 $H_1:[0,\cdots,2^l-$

$1]\times G_1\to G_1$, $H_2:G_2\to\{0,1\}^s$, $H_3:G_1\to\{0,1\}^s$, $H_4:\{0,1\}^{(l+1)s}\to\{0,1\}^s$. $E,D$ 是密钥空间为 $\{0,1\}^s$ 的对称加密与解密算法.

**产生承诺及证书**　$R$ 选择一个整数 $a\in V$. $R$ 将 $N$ 和 $a$ 秘密地发送给 CA. CA 随机选取 $r\in Z_q^*$, 计算对于属性数值 $a$ 的 Pedersen 承诺 $C=aQ+rP$, $s=s_{CA}H_1(N,C)$. CA 把 $s,r$ 秘密地发送给 $R$.

**初始化**　$S$ 持有消息 $M_0,M_1\in\{0,1\}^*$. $S$ 选定 $a_0\in V$, 公开访问控制策略, 若 $a\geqslant a_0$, 则可得到 $M_0$, 若 $a<a_0$ 则可得到 $M_1$.

**信息交互**

(1) $R$ 随机选取 $r_1,\cdots,r_{l-1}\leftarrow Z_q^*$. 若 $a\geqslant a_0$, 置 $d=a-a_0$, $r_0=r-\sum_{i=1}^{l-1}2^ir_i \bmod q$; 若 $a<a_0$ (即 $a\leqslant a_0-1$), 置 $d=(a_0-1)-a$, $r_0=-r-\sum_{i=1}^{l-1}2^ir_i \bmod q$. 设 $d_0,\cdots,d_{l-1}$ 为 $d$ 的二进表示, 即 $d=d_02^0+d_12^1+\cdots+d_{l-1}2^{l-1}$. 对于 $0\leqslant i\leqslant l-1$ 计算 $C_i=d_iQ+r_iP$. $R$ 把 $<N,C_0,\cdots,C_{l-1}>$ 发送给 $S$.

(2) 收到 $C_0,\cdots,C_{l-1}$ 后 $S$ 随机选取 $y\leftarrow Z_q^*$, 计算 $U=yP$, $V=\sum_{i=0}^{l-1}2^iC_i$, $T_0=H_1(N,V+a_0Q)$, $\bar{k}_0=H_2(\hat{e}(P_{pub},T_0)^y)$, $T_1=H_1(N,(a_0-1)Q-V)$, $\bar{k}_1=H_2(\hat{e}(P_{pub},T_1)^y)$. 对于 $0\leqslant i\leqslant l-1$, $S$ 随机选取 $k_i\in\{0,1\}^s$, 计算 $h_i^0=yC_i$, $h_i^1=y(C_i-Q)$, $c_i^0=H_3(h_i^0)\oplus k_i$, $c_i^1=H_3(h_i^1)\oplus k_i$. 计算 $K_0=H_4(\bar{k}_0\parallel k_0\parallel\cdots\parallel k_{l-1})$, $K_1=H_4(\bar{k}_1\parallel k_0\parallel\cdots\parallel k_{l-1}$, $c_0=E_{K_0}(M_0)$, $c_1=E_{K_1}(M_1)$. $S$ 把 $<U,c_0^0,c_0^1,\cdots,c_{l-1}^0,c_{l-1}^1,c_0,c_1>$ 发送给 $R$.

**打开密文**　$R$ 收到 $<U,c_0^0,c_0^1,\cdots,c_{l-1}^0,c_{l-1}^1,c_0,c_1>$ 以后, 若持有属性证书而且 $a\geqslant a_0$, 则 $d=d_02^0+d_12^1+\cdots+d_{l-1}2^{l-1}$, $d_i\in\{0,1\}$, $V+a_0Q=C$. $R$ 可以计算 $\bar{k}_0'=H_2(\hat{e}(U,s))$, 对于 $0\leqslant i\leqslant l-1$ 计算 $h_i'=r_iU$, 得到 $k_i'=H_3(h_i')\oplus c_i^{d_i}$, 然后计算 $K_0'=H_4(\bar{k}_0'\parallel k_0'\parallel\cdots\parallel k_{l-1}')$, 用它解密 $c_0$ 得到消息 $M_0$; 若持有属性证书而且 $a<a_0$, 则 $d=d_02^0+d_12^1+\cdots+d_{l-1}2^{l-1}$, $d_i\in\{0,1\}$, $(a_0-1)Q-V=C$. $R$ 可以计算 $\bar{k}_1'=H_2(\hat{e}(U,s))$, 对于 $0\leqslant i\leqslant l-1$ 计算 $h_i'=r_iU$, 得到 $k_i'=H(h_i')\oplus c_i^{d_i}$, 然后计算 $K_1'=H_4(\bar{k}_1'\parallel k_0'\parallel\cdots\parallel k_{l-1}')$, 用它解密 $c_1$ 得到消息 $M_1$.

**协议说明**: 为了实现隐藏认证, $S$ 在信息交互阶段第(2)步加密明文时只需根据系统公钥和访问策略增加计算 $\bar{k}_0$ 和 $\bar{k}_1$, 在 Li 的方案[7]中 $S$ 也必须验证对于承诺的签名, 同时为了保证实现访问策略还要验证两个等式, 而本方案实现了认证与访问策略的一体化. 由于 $R$ 根据 $yP$ 和自己的秘密信息就能计算出解密密钥, 与 Li 的方案[7]相比较, 本方案实现认证功能只需要 $R$ 增加计算一个双线性对, 但本方案减少了通信负担(R 不用传送 CA 对承诺的签名及承诺本身).

## 3　安全性分析

(1) 首先, 假设一个模拟的接收者 $R'$ 知道承诺 $C$ 却不能打开, $R'$ 可以随机选 $d',d_1,\cdots,d_{l-1}\leftarrow Z_q^*$, $r',r_1,\cdots,r_{l-1}\leftarrow Z_q^*$, 置 $d_0=d'-\sum_{i=1}^{l-1}2^id_i \bmod q$, $r_0=r'-\sum_{i=1}^{l-1}2^ir_i \bmod q$, 对于 $1\leqslant i\leqslant l-1$ 计算 $C_i'=d_iQ+r_iP$, $C_0'=C+(d_0-d'-a_0)Q+(r_0-r')P$ $a\geqslant a_0$ 或者 $C_0'=(d_0-d'+a_0-1)Q+(r_0-r')P-C$, $(a<a_0)$. 显然以上构造的 $C_0',\cdots,C_{l-1}'$ 满足 $\sum_{i=0}^{l-1}2^iC_i'=C-a_0Q$ $(a\geqslant a_0)$ 或者 $\sum_{i=0}^{l-1}2^iC_i'=(a_0-1)Q-C$ $(a<a_0)$. $C_0',\cdots,C_{l-1}'$ 与协议信息交互阶段第(1)步 $R$ 所计算的 $C_0,\cdots,C_{l-1}$ 无条件地(信息论意义)不可分辨. 由 $R$ 发送的消息 $C_0,\cdots,C_{l-1}$, $S$ 不能判断 $R$ 是否可以打开承诺 $C$. 由于隐藏证书的特点 $R$ 并没有传送证书中的签名 $s$ 的任何信息. $S$ 不能判断 $R$ 是否持有承诺 $C$ 的签名. 这也就是 $R$ 是否持有某类属性证书对 $S$ 是不可区分的. 由此 $S$ 也不可判断 $R$ 是否可以打开密文. 其次, 由于 $S$ 预先不知道 $C$, $S$ 不能判断 $(a_0-1)Q-\sum_{i=0}^{l-1}2^iC_i=C$ 与 $\sum_{i=0}^{l-1}2^iC_i+a_0Q=C$ 何者成立. 这也就是 $S$ 不知道 $R$ 将得到的是哪一个消息.

Li 的方案[7]中只分析了 $R$ 可打开承诺时 $a\geqslant a_0$ 与 $a<a_0$ 两种情形下所传送消息的不可分辨性; 笔者在此分析了 $R$ 可打开承诺与不能打开承诺两种情形下所传送消息的不可分辨性. 这是一种更强的不经意性.

(2) 根据离散对数假设 $R$ 由收到的 $yP, yr_1P, yr_0P, \cdots, yr_{r-1}P$ 不可能计算出 $y$. 由随机问答器模型 $H_1(N,C)$ 视为 $G_1$ 中的随机元素,根据 BDH 假设若不知 $s_{CA}H(N,C)$ 即证书中的签名,由 $yP, s_{CA}P, H(N,C)$ 计算 $\hat{e}(s_{CA}P, H(N,C))^y$ 是不可能的. 所以若不持有 $H_1(N,C)$ 的签名,$R$ 不可能计算出 $\bar{k}$,进而不能得到 $K$,$R$ 就不可能打开任何一个密文. 安全性依赖于对系统公钥的信任.

(3) 由于属性值 $a$ 的取值范围限定,$R$ 不能同时把 $a-a_0$ 与 $(a_0-1)-a$ 表示成 $l$ bit 的二进制数,所以在协议信息交互阶段第(1)步 $R$ 只可计算出满足条件 $(a_0-1)Q-\sum_{i=0}^{l-1}2^iC_i=C$ 或 $\sum_{i=0}^{l-1}2^iC_i+a_0Q=C$ 二者之一的 $C_0, \cdots, C_{l-1}$. 持有证书的接收者 $R$ 不可能得到两个消息.

## 4 与相关方案的比较

与 Li 的方案[7]相比较,笔者所提出的方案中 $S$ 不需要预先知道 CA 对承诺的签名及承诺本身. 这样 $S$ 既不能确定 $R$ 是否具有该类属性特征(即 $R$ 可否打开密文),又不能确定 $R$ 的属性值的范围(即 $R$ 能打开哪一个密文),本方案具有更强的不经意性. 与强有条件的不经意传输[5] 比较,本方案中 $R$ 要打开密文必须持有 CA 对承诺的签名. 具有隐藏的认证性,但是 $S$ 的访问控制策略是公开的. 设计具有隐藏认证特征而且发方的访问策略不公开的有条件不经意传输协议仍是一个公开的问题.

## 5 结 束 语

提出了隐藏认证的有条件不经意传输,利用双线性对构造了一个具体方案,分析了该方案具有的不经意性和对发送者的安全保护. 该方案实现了对于有条件不经意传输中用户秘密输入的隐藏认证,同时服务提供者不能确定用户是否持有证书,解决了不经意属性证书方案中可能泄露用户属性特征的部分信息及用隐藏证书实现比较属性数值的访问控制策略问题.

参考文献:

[1] Tzeng W. Efficient 1-out-of- n Oblivious Transfer Schemes with Universal Usable Parameters [J]. IEEE Trans on Computers, 2004, 53(2): 232-240.

[2] Naor M, Pinkas B. Efficient Oblivious Transfer Protocols [A]. Proceedings of SODA 2001, SIAM Symposium on Discrete Algorithms[C]. New York: ACM, 2001. 448-457.

[3] Zhao Chunming, Ge Jianhua, Li Xinguo. RSA-based Enhanced Oblivious Transfer Protocol[J]. Journal of Xidian University, 2005, 32(4): 562-565.

[4] Crescenzo G, Ostrovsky R, Rajagopalan S. Conditional Oblivious Transfer and Time-released Encryption[A]. Proc. CRYPTO'99 ( Lecture Notes in Computer Science): Vol 1592[C]. Berlin: Springer-Verlag, 1999. 74-89.

[5] Blake I, Kolesnikov V. Strong Conditional Oblivious Transfer and Computing on Intervals[A]. ASIACRYPT 2004 ( Lecture Notes in Computer Science): Vol 3329[C]. Berlin: Springer-Verlag, 2004. 515-529.

[6] Li N, John C, William H. Design of a Role-based Trust Management Framework[A]. Proceedings of the 2002 IEEE Symposium on Security and Privacy[C]. Los Alamitos: IEEE Computer Society Press, 2002. 114-130.

[7] Li J, Li N. OACerts: Oblivious Attribute Certificates[A]. Applied Cryptography and Network Security (ACNS 2005 Lecture Notes in Computer Science): Vol 3531[C]. Berlin : Springer -Veralg, 2005. 178-206.

[8] Pedersen T. Non-interactive and Information-theoretic Secure Verifiable Secret Sharing[A]. Advances in Cryptology (CRYPTO'91, Volume 576 of Lecture Notes in Computer Science): Vol 576[C]. Berlin: Springer -Veralg, 1991. 129-140.

[9] Bradshaw R, Holt J, Seamons K. Concealing Complex Policies with Hidden Credentials[A]. Eleventh ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2004. 146-157.

[10] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[A]. Proceedings of Crypto 2001 (Lecture Notes in Computer Science): Vol 2139[C]. Berlin: Springer-Verlag, 2001. 213-229

(编辑: 高西全)