基于 RSA 数字签名的增强不经意传输协议

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,陕西 西安 710071)

摘要：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,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,即不能确定接收者的身份. 在 DDH 假设和随机预言模型下具有可证明的安全性.

关键词：接入控制;Elgamal 加密;不经意的传输;RSA 签名;决策性 Diffie-Hellman 假设
中图分类号:TN918 **文献标识码**:A **文章编号**:1001-2400(2005)04-0562-04

RSA-based enhanced oblivious transfer protocol

ZHAO Chun-ming, *GE Jian-hua*, *LI Xin-guo*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: Based on the RSA signature and (string) oblivious transfer, an enhanced oblivious transfer protocol is proposed which solves the access control problem for an oblivious transfer protocol. The protocol proposed has the property that only the receiver who has the signture issued by the central authority can open the message which he choose and that the sender can not decide whether the receiver has the signature or not. That is to say, the identity of the receiver can not be confirmed after the protocol. Under the decisional Diffie-Hellman assumption the proposed scheme has provable security.

Key Words: access control; Elgamal encryption; oblivious transfer; RSA; decisional Diffie-Hellman assumption

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协议设计者中有着广泛的应用[2]. 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[3]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. 笔者采用其思想提出了基于 RSA 数字签名的一种不经意传输协议,该协议除了具备一般不经意传输的特性外,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.

1 协议的基础

1.1 1-out-of-n 不经意传输协议

Tzeng 在文献[4]中提出了一种对于数据串的 1-out-of-n 不经意传输协议. 简述如下：

系统参数：(g, h, G_q),G_q 是一个 q 阶循环群,g,h 是 G_q 的两个生成元,$\log_g^h$ 保密;发送者 S 的输入 $m_1, m_2, \cdots, m_n \in G_q$ 接收者 R 的选择 α,$1 \leqslant \alpha \leqslant n$.

收稿日期:2004-08-26
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.

(1) R 发送 $y = g^r h^\alpha, r \in_R Z_q$;

(2) S 发送 $c_i = (g^{k_i}, m_i (y/h^i)^{k_i}), k_i \in_R Z_q, 1 \leqslant i \leqslant n$;

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

1.2 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(PPTM)图灵分辨器 D、任何一个多项式 $p(n)$ 及充分大的 n, $|Pr[D(X_n) = 1] - \Pr[D(Y_n) = 1]| < 1/p(n)$. 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 的循环群的生成元,$a, b, c \in_R Z_q$,以下两个概率总体是计算性不可区分的:$Y_1 = (g, g^a, g^b, g^{ab})$ 与 $Y^2 = (g, g^a, g^b, g^c)$.

计算性 Diffie-Hellman(CDH)假设:给定 (g, g^a, g^b),不存在有效 PPTM 算法能以不可忽略的概率计算出 g^{ab}.

2 基于 RSA 数字签名的增强的不经意传输协议

为了构造有效的增强的不经意传输协议,需要对 RSA 数字签名系统作适当的修正. 本文中使用了文献[5]所提出的对 RSA 数字签名系统添加的初始化阶段.

(1) 系统建立　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 $< g >$ 是一个阶为 pq 的循环群(g 的阶以很大的概率是 pq),记为 G. h 是 G 的另一个生成元,$\log_g^h$ 保密. 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 $\{0,1\}^{\tau l_G + 1}$,这里 τ 是一个大于 1 的安全参数. $H: \{0,1\}^* \to Z_N$ 是一个安全的 Hash 函数. 整数 e (> 2) 是系统的公钥. 整数 d 满足:$ed = 1 \bmod 2pq$, 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 $\sigma = H(M)^{2d} \bmod N$($d$ 是奇数,为了实现语义安全性对 $H(M)^2$ 签字)只有 CA 和 R 知道而对发送者 S 保密. M, H, N, g, h 为参与协议的各方所知. m_i ($1 \leqslant i \leqslant n$) 是待发送的消息只有 S 知道.

(2) 信息交互　接收者 R 的选择记为 $\alpha, \alpha \in [1, \cdots, n]$. 从 $\{0,1\}^{\tau l_G + 1}$ 随机地选一数 r,为方便起见,简记为 $r \in_R \{0,1\}^{\tau l_G + 1}$. 接收者 R 在群 Z_N^* 计算(以下若无特别声明群乘法运算均在 Z_N^* 中):$y = \sigma g^r h^\alpha$,并把它发送给 S.

发送者 S 收到 y 以后,检查是否 $y \in Z_N^*$,若成立则在群 Z_N^* 计算如下:

$$c_i = \left(g^{ek_i}, m_i \left(\frac{y^e}{H(M)^2 h^{ei}}\right)^{k_i}\right), \quad k_i \in_R \{0,1\}^{\tau l_G + 1}, \quad 1 \leqslant i \leqslant n.$$

(3) 数据解密　由 $c_\alpha = (a, b)$ 接收者 R 可以在群 Z_N^* 计算如下:$m_\alpha = b/a^r$,方案的正确性:

$$b/a^r = m_\alpha \left(\frac{y^e}{H(M)^2 h^{e\alpha}}\right)^{k_\alpha} \Big/ a^r = m_\alpha \left(\frac{\sigma^e g^{er} h^{e\alpha}}{H(M)^2 h^{e\alpha}}\right)^{k_\alpha} \Big/ g^{ek_\alpha r} = m_\alpha.$$

方案的有效性:与文献[4]相比较接收者 R 只需增加一个低指数(指数是 e)模运算一个模乘法运算;发送者需增加一个低指数(指数是 e)模运算、一个模逆运算及一个模乘法运算.

方案的安全性:假设 $H(M)$ 是循环群 G 中的元素,这样可以证明方案的语义安全性. 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,该方案的安全性类似于 Elgamal 加密方案的安全性[6]. 在 DDH 问题是困难的条件下接收者 R 不能得到其余 m_i ($i \neq \alpha$) 的任何信息,假冒的接收者(不持有签字)R' 不能解密 m_α,而且他从 S 所接收到的信息 c_i ($1 \leqslant i \leqslant n$) 与随机的消息是计算性不可分辨的.

定理 1　接收者 R 的选择 α 是无条件安全的,发送者 S 从 y 中得不到 α 的任何信息.

证明　对于任意 $\alpha' \in [1, \cdots, n]$,存在 $r' \in \{0,1\}^{\tau l_G + 1}$,使得 $H(M)^{2d} g^{r'} h^{\alpha'} = H(M)^{2d} g^r h^\alpha$ 成立. 因此,即使 S 有无限的计算能力也不能得到 R 的所选 α 的任何信息.

为证明协议的安全性,需要利用在特定的群中的 DDH 假设,以下首先定义此群:

设 $g' = g^e$,那么 $< g' >$ 是一个阶为 $pq/(e, pq)$ 的循环群,记 $t = pq/(e, pq)$, $G' = < g' >$, $h' = h^e$(h' 也是 G' 的一个生成元).

定理 2　在 DDH 假设成立条件下,半可信的接收者 R(执行协议但企图得到更多的信息)不能得到其余

$m_i(1 \leqslant i \neq \alpha \leqslant n)$ 的任何信息. 也就是,即使 R 知道(r,α),对 R 来说 $e_i = (g',h',c_i)$ 与 $x = (g',h',a,b)(a, b \in_R G' \setminus \{1\})$ 也是计算性不可分辨的.

证明 首先,R 不能计算出两个对(α,r),(α',r') 使得下式成立:$H(M)^{2d} g^{\alpha} h^{r} = H(M)^{2d} g^{\alpha'} h^{r'}$,不然,$R$ 可求出$\log_g^h = (r - r')/(\alpha - \alpha')$. 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 $c_i = (g^{ek_i}, m_i g^{ek_i r} h^{ek_i(\alpha-1)}) = (g'^{k_i}, m_i g'^{k_i r} h'^{k_i(\alpha-i)})$. 设 $e_i = (g',h',c_i)$,$(1 \leqslant \alpha \neq i \leqslant n)$,以下证明 DDH 假设成立的条件下,对每个 $i \neq \alpha$,$e_i = (g',h',c_i)$ 看起来是随机的. 定义随机变量 $E_i = (g',h',g'^{k_i}, m_i g'^{k_i r} h'^{k_i(\alpha-i)})$. 这里,$k_i \in_R \{0,1\}^{\tau l_G+1}$,$g',h' \in_R G' / \{1\}$. 设 $X = (r_1,r_2,r_3,r_4)$,这里 $r_1,r_2 \in_R G'/\{1\}$,$r_3,r_4 \in_R G'$. 以下证明,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 D 作子程序的 PPTM 分辨器 D' 所区分:

输入 (g',u,v,w)(来自于 Y_1 或 Y_2);(1) 若 $u = 1$,则输出 1;(2) 随机地选取 $r \in_R \{0,1\}^{\tau l_G+1}$;(3) 若 $D(g', u,v, m_i v^r w^{\alpha-i}) = 1$,则输出 1,否则输出 0.

可以看出,如果 $(g',u,v,w) = (g',g'^{a},g'^{b},g'^{ab})$ 来自于 Y_1 且 $a \neq 0$,$(g',u,v, m_i v^r w^{\alpha-i}) = (g,h,g^b, m_i(g'^r h'^{\alpha-i}))$ 具有 E_i 中元素的形式,这里 $h' = u$. 如果$(g',u,v,w) = (g',g'^{a},g'^{b},g'^{c})$ 来自于 Y_2 且 $a \neq 0$,$(g', u,v, m_i v^r w^{\alpha-i}) = (g,h,g^b, m_i(g^{br+c(\alpha-i)})$ 均匀地分布于 $G'/\{1\} \times G'/\{1\}$ 和 $G' \times G' = X$. 因此,如果 D 能以不可忽略地占优势的概率 ε 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,r),e_i 对其也是计算性不可分辨的.

定理 3 发送者得不到接收者是否持有签名的任何信息.

证明 因为存在 $k,r' \in \{0,1\}^{\tau l_G+1}$ 使下式成立:$H(M)^{k} g^{r'} h^{\alpha} = H(M)^{2d} g^{r} h^{\alpha}$,$r \in_R \{0,1\}^{\tau l_G+1}$,$\alpha \in [1, \cdots, n]$,$d$ 是 RSA 秘密指数. 所以,接收者 R 是否拥有签名是无条件安全的.

定理 4 在 DDH 假设成立条件下偷听者不能解密 m_α,并且 $e_i = (g',h',c_i)(1 \leqslant i \leqslant n)$ 与随机的消息 $x = (g',h',a,b)(a,b \in_R G' \setminus \{1\})$ 对其是计算性不可分辨的.

证明 首先,偷听者不能解密得到 m_α,因为$(g^{ek_\alpha}, m_\alpha g^{rek_\alpha})$ 是 m_α 的 Elgamal 加密,其安全性等价于 DDH 假设. 其次,对于偷听者所得到的消息 $e_i = (g',h',c_i)(1 \leqslant \alpha \neq i \leqslant n)$ 与随机的消息 $x = (g',h',a,b)(a, b \in_R G' \setminus \{1\})$ 对其是计算性不可分辨的. 证明类似于定理 2.

定理 5 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 $(y^e / h^{ei} H(M)^2)^{k_i}(1 \leqslant i \leqslant n)$.

证明 在执行完协议以后不持有签名 $H(M)^{2d}$ 的攻击者不能由 $a = g^{ek_i}$ 及 y 计算出$(y^e / h^{ei} H(M)^2)^{k_i}$. 首先,攻击者不可能知道 $\bar{r}_i$ 使得 $g^{r_i} = y / h^i H(M)^{2d}$,否则他能知道 $H(M)^{d} = y / g^{r_i} h^i$. 进一步,假如攻击者能由 $a = g^{ek_i}$ 及 y 计算出$(y^e / h^{ei} H(M)^2)^{k_i}$,由于$(y^e / h^{ei} H(M)^2)^{k_i} = (y / h^i H(M)^{2d})^{ek_i}$,那么他能解决以下的 CDH 问题:给定 g^{ek_i} 和$y / h^i H(M)^{2d}$ 计算出$(y / h^i H(M)^{2d})^{ek_i}$.

3 在随机预言模型下的协议

系统建立阶段除增加一个 Hash 函数 H' 外与前相同.

信息交互:接收者 R 将 $y = \sigma g^r h^{\alpha}$,这里 $r \in_R \{0,1\}^{\tau l_G+1}$,发送给 S. S 发送 $a = g^{ek}$,$c_i = m_i \oplus H'((y^e / h^{ei} H(M)^2)^k, i)$ 给 R,这里$k \in_R \{0,1\}^{\tau l_G+1}$,$1 \leqslant i \leqslant n$. 数据解密:$R$ 由 $a = g^{ek}$,c_α 计算 $m_\alpha = c_\alpha \oplus H'(a^r, \alpha)$.

接收者的安全性与前述方案相同. 在随机预言模型及 DDH 假设下可以证明对于发送者的安全性,但由于篇幅所限在此省略.

4 结 论

对于不经意传输提出了基于证书的接入控制方案,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. 该方案使用标准的 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. 该方案基于证书授权,扩展了 RSA 数字证书的用途,同时保护了证书持有者的隐私. 与文献[4]中的方案相比,通信量相同计算代价略高,而功能更强. 该方案采用 Elgamal 公钥加密,由于加密的同态性,可以容

易地推广到价格不同的不经意传输协议[7]的情形. 该方案具有可证明的安全性.

参考文献：

[1] Rabin M O. How to Exchange Secrets by Oblivious Transfer[R]. Cambridge：Harvard Aiken Computation Laboratory，1981.

[2] Wang Jilin，Chen Xiaofeng，Wang Yumin. A Survey of the Studies on Secure Electronic Auction[J]. Journal of Xidian University，2003，30(2)：20-25.

[3] Li N，Du W，boneh D. Oblivious Signature-based Envelope[A]. Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing[C]. New York：ACM Press，2003. 182-189.

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

[5] Ateniese G. Verifiable Encryption of Digital Signatures and Applications[J]. ACM Transactions on Information and System Security，2004，7(1)：1-20.

[6] Tsiounis Y，Yung M. On the Security of Elgamal-based Encryption[A]. Public Key Cryptography，PKC 1998，Lecture Notes in Computer Science：Vol 1431[C]. Berlin：Springer-Verlag，1999. 117-134.

[7] Aiello B，Ishai Y，Reingold O. Priced Oblivious Transfer How to Sell Digital Goods[A]. Advances in Cryptology，Eurocrypt 2001，Lecture Notes in Computer Science：Vol 2045[C]. Berlin：Springer-Veralg，2001. 119-135.

（编辑：李维东）

（上接第 561 页）

当 IFO 试验值等于真实值，即 $g' = g$ 时，可以得到：

$$S(g,g) = \sum_{k=0}^{N/2-1} c_{k-g}\, c_{k-g}^{*} \quad . \tag{15}$$

此时，ML 和 Kim 算法的测度值相等，且有：

$$\mathrm{Re}\{S(g,g)\} = |S(g,g)| = S(g,g) \quad . \tag{16}$$

当 IFO 试验值不等于真实值，即 $g' \neq g$ 时，因为一个复数的实部总是小于其模值，即

$$\mathrm{Re}\{S(g',g)\} < |S(g',g)| \quad , \quad g' \neq g \quad . \tag{17}$$

所以，在噪声存在的情况下，当 IFO 试验值不等于真实值，即 $g' \neq g$ 时，ML 方法的 IFO 测度 $\mathrm{Re}\{S(g',g)\}$ 大于 $S(g,g)$ 的概率一定小于 Kim 方法 IFO 测度 $|S(g',g)|$ 大于 $S(g,g)$ 的概率，实际上当 g' 接近 g 时，$\mathrm{Re}\{S(g',g)\}$ 中的信噪比比 $|S(g',g)|$ 大，ML 方法的错误估计概率要小于 Kim 方法.

根据两种算法的频偏测度函数可以得到以下结论：由于频偏 $b = 2g$ 的变化只会引起频偏测度序列的循环移位，并不会改变两个频偏测度集合中元素的大小，因此，频偏 b 对两种估计算法的性能没有影响.

4　结　　论

在 Kim 算法的基础上，推导出 OFDM 系统整数倍频偏的 ML 估计算法. 两种算法都利用了频域一个 OFDM 码元中偶数数据之间的差分关系，只是频偏测度函数产生的方法不同. 通过仿真，证明在不增加算法复杂度的基础上，ML 估计算法优于传统 Kim 算法的估计性能，当信噪比 SNR = 3 dB，子载波个数 $N = 32$ 时，采用传统 Kim 算法的错误估计概率为 4.03×10^{-4}，采用 ML 估计算法错误估计概率降为 6.535×10^{-5}.

参考文献：

[1] Schmidl T M，Cox D C. Robust Frequency and Timing Synchronization for OFDM[J]. IEEE Trans on Commun，1997，45(12)：1613-1621.

[2] Kim Y H，Song I，Yoon S，et al. An Efficient Frequency Offset Estimator for OFDM System and Its Performance Characteristics[J]. IEEE Trans on Vehicular Technology，2001，45(5)：1307-1312.

[3] Chen Chen，Li Jiangdong，Han Gang，et al. ML Estimation of Integer Frequency Offset in OFDM System[J]. Journal of Xidian University，2004，31(6)：846-849.

（编辑：李维东）