基于椭圆曲线的隐私增强认证密钥协商协议

曹天杰,雷 红
(中国矿业大学计算机科学与技术学院,江苏徐州 221116)

摘 要: 认证密钥协商协议能够为不安全网络中的通信双方提供安全的会话密钥,但是,大多数的认证密钥协商协议并没有考虑保护用户隐私.论文关注网络服务中用户的隐私属性,特别是匿名性和可否认性,规范了增强用户隐私的认证密钥协商协议应满足的安全需求,即双向认证、密钥控制、密钥确认、会话密钥保密、已知会话密钥安全、会话密钥前向安全、用户身份匿名、用户身份前向匿名、不可关联和可否认,并基于椭圆曲线密码系统设计了一个满足安全需求的隐私增强认证密钥协商协议.

关键词: 匿名性; 可否认性; 认证密钥协商; 椭圆曲线
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2008) 02-0397-05

Privacy-Enhancing Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptosystem

CAO Tian-jie, LEI Hong
(*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu* 221116, *China*)

Abstract: Authenticated key agreement protocol is designed to provide pair of parties communicating over an insecure network with a secure session key. However, most of the existing authenticated key agreement protocols are not designed for protecting privacy. We emphasize user's privacy properties in network services, in particular we stress anonymity and deniability. We specify the desired security properties of privacy-enhancing authentication key agreement protocols, i.e. mutual authentication, key control, key confirmation, session-key confidentiality, known-key security, forward secrecy, anonymity of user, forward anonymity of user, unlinkability, deniability. Based on elliptic curve cryptosystem we also propose a protocol which satisfies all the desired security properties.

Key words: anonymity; deniability; authentication key agreement; elliptic curve

1 引言

通常采用的隐私定义是由Alan Westin给出的:"隐私是指个人、团体和机构决定自己的信息何时、如何以及在多大程度上泄漏给其他人的一种主张"[1].认证密钥协商协议能使通信双方相互认证并协商建立共享的会话密钥.Diffie-Hellman密钥交换协议广泛应用于认证密钥协商.但由于该协议不提供双向认证,存在中间人攻击[2].在现实环境中,攻击者能够拷贝、重放、更改或删除通信中的所有信息,因此,双向认证是通信的本质要求.

在认证密钥协商协议中,除了认证和密钥协商的安全需求之外,隐私需求正获得更多的关注[3~8].

匿名性是隐私的一个主要特征.在一些具体应用中,除了通信双方,用户可能不希望暴露自己的身份给第三方,如果在认证阶段明文传输用户的身份信息则暴露了用户的身份.Aydos等人设计的用于无线通信的认证密钥协商协议A-WAP首次强调了用户匿名性需求[3~5],但A-WAP协议存在缺陷,如未能提供认证性、匿名性[9,10].Mangipudi等人提出了用户匿名认证密钥协商协议UAP、用户与服务器匿名认证密钥协商协议US-AP[7],但这两个协议服务器均不能认证用户[11].Abadi和Fournet提出了私有认证的概念[6],考虑了移动实体在认证过程中保护身份的问题,设计了两个私有认证协议.该协议在发起方预先获得响应方的公钥证书的假设下,提供双向认证、密钥传输、不可否认、参与者匿名.

可否认性是隐私的另一个特征.可否认性能够使协议参与方事后否认参与了该协议.在可否认认证协议中[12],一方面消息接收方能够认证收到的消息是由预期的发送方发送的,事后,发送方能够否认曾经向接收

收稿日期: 2006-04-11; 修回日期: 2007-12-15
基金项目: 江苏省自然科学基金(No. BK2007035); 中国矿业大学科技基金(No. 0D0601624287)

方发送过该消息. 在客户-服务器系统中, 服务器能够认证消息来源于一个具体用户, 但他没有能力向第三方证明消息是由该用户生成的, 即使服务器愿意向第三方泄漏他的私钥. 例如用户在匿名公告板中发帖, 服务器需要认证用户的合法性, 但服务器没有能力向第三方提供证据证明用户的发帖行为, 这样既保护服务器不会被非法用户滥用, 又保护了合法用户的隐私.

由于服务器是提供公共服务的实体, 通常不需要匿名, 因此本文只考虑用户匿名. 为增强用户隐私, 认证密钥协商协议除了应满足认证与密钥协商的需求外, 我们增加了用户身份匿名、用户身份前向匿名、不可关联、可否认等用户隐私需求. 隐私增强的认证密钥协商协议应满足的安全需求规范如下.

(1) 双向认证: 任何使用协议的双方都应彼此认证. 即预期通信的用户和服务器双方应能相互证实对方的身份, 攻击者不能假冒一方与另一方通信. 双向认证确保通信方的消息来源于真实的发送方, 并且消息在传输中没有被攻击者篡改.

(2) 密钥控制: 任何一方不能强迫会话密钥选择为一个预先确定的值. 即通信双方对协商共享的会话密钥都有贡献, 单方不能控制密钥的选择.

(3) 密钥确认: 是指执行协议的任何一方能够确认另一方拥有了共享的会话密钥.

(4) 会话密钥保密: 除了参与通信的实体之外任何人都不能获得会话密钥.

(5) 已知会话密钥安全: 即使攻击者获得某次通信的会话密钥, 也不能根据该会话密钥来获得其他会话密钥. 即会话密钥之间具有独立性.

(6) 前向安全: 即使攻击者获得一个或多个实体的长期密钥, 也不能影响以前由该长期密钥建立的会话密钥的安全. 即会话密钥与长期密钥之间具有独立性.

(7) 用户身份匿名: 如果用户与服务器成功地建立了一个会话密钥, 则攻击者不能获得用户的身份信息. 如果攻击者攻破了一个会话密钥, 攻击者仍然不能获得该次会话的用户身份信息. 匿名性可确保除通信双方之外, 任何人都不能知道谁在和谁通信.

(8) 用户身份前向匿名: 如果攻击者攻破了一个或多个实体的长期密钥, 攻击者仍然不能获得利用该长期密钥建立会话的用户身份信息.

(9) 不可关联: 攻击者不能区分同一个用户的两次不同通信.

(10) 可否认: 预期的响应方不能向任何第三方证明消息源. 设计可否认认证协议的基础是参与的双方能够导出一个共享的秘密参数, 该秘密参数用作双方通信的密钥. 由于双方事后都能够独自得出该秘密参数, 因此双方都能够否认曾经参与该次通信.

基于椭圆曲线上离散对数问题的密码系统近年来广泛应用于无线、移动通信网络, 与其他密码系统相比, 在椭圆曲线上实现数字签名具有速度快、密钥和签名短等优点. 目前, 基于椭圆曲线离散对数问题的公钥密码已被包括在多个标准中, 如 IEEE 标准(IEEE 1363)[13]、联邦信息处理标准 FIPS 186-2 和国际标准化组织的 ISO 15946.

2 基本构造模块

系统参数选择如下: p 是一个有限域 F_p 的元素个数, 这里 p 是一大素数(长度大于 160)或 $p=2^m$, m 为正整数. a, $b\in F_p$, 定义 F_p 上的椭圆曲线: $y^2=x^3+ax+b$ 当 $p>3$, 或 $y^2+xy=x^3+ax^2+b$ 当 $p=2$. P 是 $E(F_p)$ 中阶为素数 n 的一个基点, n 为大素数. H 是安全 HASH 函数, 记号 $P.x$ 和 $P.y$ 分别表示 P 点的 x、y 坐标. 下面描述论文中利用的基本构造模块.

(1) 基于椭圆曲线的 Diffie-Hellman 密钥交换协议(ECDH)[14]

发起者 A 选择随机数 r_a 并计算 $Q_a=r_aP$, 然后将 Q_a 发送给响应者 B. B 选择随机数 r_b 并计算 $Q_b=r_bP$, 然后将 Q_b 发送给 A. A 计算 r_aQ_b, B 计算 r_bQ_a, A 和 B 生成相同的会话密钥 $K=(r_aQ_b).x=(r_bQ_a).x$.

(2) 椭圆曲线数字签名算法(ECDSA)[13]

密钥生成: 用户选择随机数 $d_a\in[2, n-2]$ 作为私钥并计算 $Q_a=d_aP$ 作为公钥.

签名: 为对消息 m 生成签名, 签名者选择随机数 $k\in[2, n-2]$, 计算 kP 和 $r=(kP).x \bmod n$, 计算 $s=k^{-1}(H(m)+d_ar) \bmod n$, 对消息 m 的签名是 (r, s).

验证: 为验证 A 对消息 m 的签名 (r, s), 验证者计算 $c=s^{-1} \bmod n$, $u_1=H(m)c \bmod n$ 和 $u_2=rc \bmod n$, 计算 $R=u_1P+u_2Q_a$ 和 $v=R.x \bmod n$; 如果 $v=r$ 则验证者接受签名.

(3) 椭圆曲线加密方案(ECES)[15]

密钥生成: 用户 A 选择随机数 $d_a\in[2, n-2]$ 作为私钥并计算 $Q_a=d_aP$ 得到相应的公钥.

加密: 用户 B 对消息点 P_m 加密, 首先查找 A 的公钥 Q_a, 选择随机数 $k\in[2, n-2]$, 计算 $P_1=kp$ 和 $P_2=P_m+kQ_a$, 发送 (P_1, P_2) 给 A.

解密: A 收到 (P_1, P_2), 计算 $P_m=P_2-d_aP_1$.

3 隐私增强的认证密钥协商协议

完整的认证密钥协商协议包括两个阶段: 初始化阶段、认证与密钥协商阶段. 论文使用 $E(k, \cdot)$、$D(k, \cdot)$ 表示对称密码加密、解密算法, 密钥为 k.

初始化阶段是一个离线过程, 见图 1. 认证中心选

择一个随机数 d_{CA} 作为签名私钥, $Q_{CA}= d_{CA}P$ 为公钥. 认证中心使用 ECDSA[14] 为通信方(用户 U/服务器 S)发行证书并规定证书有效期. 有效期到期后需要初始化, 以获得另一个有效的证书和有效期. 初始化阶段通过一个安全信道来执行. 用户 U 首先生成随机私/公钥对 (d_U, Q_U), 并把公钥 Q_U 发送给认证中心. 认证中心分配用户身份标识 I_U 和有效期 t_U, 计算 $e_U= H(Q_U.x, I_U, t_U)$ 并将生成的证书 (r_U, s_U) 和 I_U, t_U 随同自己的公钥 Q_{CA} 发送给用户 U. 用户储存 d_U, Q_U, Q_{CA}, I_U, (r_U, s_U), t_U. 服务器 S 执行类似的初始化过程并储存 d_S, Q_S, Q_{CA}, I_S, (r_S, s_S), t_S.

用户		认证中心
1. 选择$d_U \in \{2, n-2\}$		选择$k_U \in \{2, n-2\}$
2. $Q_U = d_U P$		$R_U = k_U P$
3. 发送Q_U	→	接收Q_U
4.		选择唯一的I_U和t_U
5.		$r_U = R_U.x \bmod n$, $e_U = H(Q_U.x, I_U, t_U)$
6.		$s_U = k_U^{-1}(e_U + d_{CA} r_U)$
7. 接收Q_{CA}, I_U, (r_U, s_U), t_U	←	发送Q_{CA}, I_U, (r_U, s_U), t_U
8. 储存d_U, Q_U, Q_{CA}, I_U, (r_U, s_U), t_U		

图 1　初始化阶段

在认证与密钥协商阶段, 服务器和用户进行双向认证并协商会话密钥, 见图 2. 该阶段是一个在线过程, 每当用户请求服务器服务时, 双方相互认证, 并生成一个会话密钥.

当用户发送资源访问请求后, 服务器选择随机数 $k_1, k_2 \in \{2, n-2\}$, 并把服务器公钥 Q_S、身份标识 I_S、证书 (r_S, s_S)、有效期 t_S、k_1P 和 k_2P 发送给用户, 其中 k_1P 作为临时公钥.

用户选择 k_3, k_4, 检查 t_S 的有效性, 验证服务器证书的有效性. 通过检查后, 计算对称密钥 $k_U= H(d_U Q_S.x, k_3k_2P.x)$. 使用服务器公钥 Q_S 和临时公钥 k_1P 利用 ECES[15] 加密自己的公钥 Q_U, 密文为 $k_4Q_S+ k_3k_1P+ Q_U$, 并使用对称密钥 k_U 加密自己的证书 (r_U, s_U)、身份 I_U、有效期 t_U 和 $k_1P.x$ 得到密文 C_U, 把 k_3P、k_4P、$k_4Q_S+ k_3k_1P+ Q_U$ 和 C_U 发送给服务器. 用户计算共享的会话密钥 $k_{US}= H(d_U Q_S.x, k_3k_2P.x, I_U, I_S)$.

服务器首先利用 d_S、k_1 解密 $k_4Q_S+ k_3k_1P+ Q_U$ 得到用户公钥 Q_U, 计算对称密钥 $k_S= H(d_S Q_U.x, k_2k_3P.x)$, 若双方诚实执行协议则 $k_S= k_U$, 服务器解密 C_U 检查 $k_1P.x$ 和 t_U 的有效性, 检查用户证书的有效性. 若无效则终止协议. 否则, 使用 k_S 加密 $k_3P.x$ 后得到 C_S, 并把 C_S 发送给用户. 服务器计算会话密钥 $k_{US}= H(d_S Q_U.x, k_2k_3P.x, I_U, I_S)$.

一旦收到 C_S, 用户解密 C_S 检查 $k_3P.x$ 的有效性. 若无效则终止协议.

用户		服务器
1. 选择$k_3, k_4 \in \{2, n-2\}$		选择$k_1, k_2 \in \{2, n-2\}$
2. 接收Q_S, I_S, (r_S, s_S), t_S, k_1P和k_2P	←	发送Q_S, I_S, (r_S, s_S), t_S, k_1P和k_2P
3. t_S是否有效;计算$e_S = H(Q_S.x, I_S, t_S)$		
4. $c = s_S^{-1} \bmod n$; $u_1 = ce_S \bmod n$; $u_2 = cr_S \bmod n$		
5. $R = u_1P + u_2Q_{CA}$		
6. $v = R.x$		
7. 如果$v \neq r_S$则中断		
8. 计算$k_U = H(d_U Q_S.x, k_3k_2P.x)$		
9. 发送k_3P, k_4P, $k_4Q_S + k_3k_1P + Q_U$, C_U 其中$C_U = E(k_U, (r_U, s_U), I_U, t_U, k_1P.x)$	→	接收k_3P, k_4P, $k_4Q_S + k_3k_1P + Q_U$, C_U
5. 计算$k_{US} = H(d_U Q_S.x, k_3k_2P.x, I_U, I_S)$		计算$d_S k_4P$, k_1k_3P,解密得Q_U
6.		$k_S = H(d_S Q_U.x, k_2k_3P.x)$
7.		$D(k_S, C_U)$,检查 $k_1P.x$, t_U是否有效
8.		计算$e_U = H(Q_U.x, I_U, t_U)$
9.		$c = s_U^{-1} \bmod n$; $u_1 = ce_U \bmod n$; $u_2 = cr_U \bmod n$
10.		$R = u_1P + u_2Q_{CA}$, $v = R.x$
11.		如果$v \neq r_U$则中断
12.		计算$C_S = E(k_S, k_3P.x)$
13. 接收C_S	←	发送C_S
14. $D(k_U, C_S)$,检查$k_3P.x$是否有效		计算$k_{US} = H(d_S Q_U.x, k_2k_3P.x, I_U, I_S)$

图 2　认证与密钥协商阶段

4　安全分析

本节分析所设计的协议的安全性并与其他具有隐私保护属性的协议做比较.

(1) 双向认证: 所设计的协议通过挑战– 响应实现双向认证. 服务器发送的是随机值 k_1P 和 k_2P, 用户随后用加密的用户公钥与加密的证书消息 C_U 响应. 由于只有该证书属主的用户才能用对应的私钥生成 k_U, 因此攻击者不能假冒用户生成 C_U. 服务器解密 C_U, 就可检查 $k_1P.x$ 和刚才发送的随机值是否一致, 有效期 t_U 是否有效, 用户的证书是否有效, 当检查通过, 服务器就完成了对用户的认证. 同样, 只有服务器证书属主才能用对应的私钥生成 k_S, 因此攻击者不能假冒服务器生成 C_S. 用户解密 C_S, 检查 $k_3P.x$ 和刚才发送的随机值是否一致, 有效期 t_S 是否有效, 服务器证书是否有效, 当检查通过, 用户就完成了对服务器的认证.

(2) 密钥控制: 所设计的协议使用 Diffie-Hellman 密钥交换协议协商会话密钥 $H(d_U d_S P.x, k_2k_3P.x, I_U, I_S)$, 由于 k_2 是服务器选择的, k_3 是用户选择的, 任何一方都不能单独控制会话密钥的选择, 达到了密钥协商的目的.

(3) 密钥确认: 用户加密传送自己的公钥、证书等内容, 把 k_3P、k_4P、$k_4Q_S+ k_3k_1P+ Q_U$ 和 C_U 发送给服务器. 当服务器解密 C_U 并检查通过时, 由认证性, 服务器能够确认用户有能力计算出正确的会话密钥. 同样, 当用户解密 C_S 并检查通过时, 由认证性, 用户能够确认服务器有能力计算出正确的会话密钥.

(4) 会话密钥保密: 协议使用 Diffie-Hellman

密钥交换算法协商会话密钥为 $k_{US}=H(d_Ud_SP.x, k_2k_3P.x, I_U, I_S)$. 由于协议具有双向认证性, 攻击者无法假冒用户和服务器, 因此无法计算出 $d_Ud_SP.x$、$k_2k_3P.x$, 这样除了参与通信的用户与服务器之外任何人都不能获得会话密钥.

(5) 已知会话密钥安全: 攻击者攻破一次通信的会话密钥, 无助于攻破另一次通信的会话密钥. 用户与服务器的会话密钥为 $k_{US}=H(d_Ud_SP.x, k_2k_3P.x, I_U, I_S)$. 由于两次通信使用的是不同的随机数, 这种随机数的不相关性使得攻击者即使攻破了一个会话密钥, 他也无法利用该信息攻破另一次通信的会话密钥.

(6) 前向安全: 协议使用 Diffie-Hellman 密钥交换算法协商会话密钥为 $k_{US}=H(d_Ud_SP.x, k_2k_3P.x, I_U, I_S)$. 因此攻击者即使获得用户与服务器的长期密钥 d_U、d_S, 由于无法计算 $k_2k_3P.x$, 攻击者不能计算出会话密钥.

(7) 身份匿名: 在用户与服务器执行协议的过程中, 攻击者由于没有服务器的私钥, 无法获得用户的身份(公钥). 因此, 如果用户与服务器成功地建立了一个会话密钥, 由双向认证性知道协议执行过程中不存在不被觉察的主动攻击, 而用户公钥是使用服务器的公钥 Q_S 和临时公钥 k_1P 加密的, 用户的证书是由攻击者无法计算的 $k_U=H(d_UQ_S.x, k_2k_3P.x)$ 加密的, 因此实现了用户匿名. 如果攻击者攻破会话密钥 $k_{US}=H(d_Ud_SP.x, k_2k_3P.x, I_U, I_S)$, 这无助于计算 k_1 和 $k_U=H(d_UQ_S.x, k_2k_3P.x)$, 攻击者仍然不能获得该次会话的用户身份信息.

(8) 身份前向匿名: 如果攻击者攻破了用户与服务器的长期密钥 d_U、d_S, 攻击者仍然不能获得利用该长期密钥建立会话的用户身份信息. 因为只有知道服务器的临时公钥 k_1P 对应的私钥才可解密获得用户的公钥, 只有计算出 $k_2k_3P.x$ 才可计算用于加密用户证书的对称密钥 $k_U=H(d_UQ_S.x, k_2k_3P.x)$. 由于攻击者无法计算 k_1 和 k_U, 协议具有身份前向匿名性.

(9) 不可关联: 用户公钥是使用服务器的公钥 Q_S 和临时公钥 k_1P 加密的, 用户的证书是由攻击者无法计算的 $k_U=H(d_UQ_S.x, k_2k_3P.x)$ 加密的. 两次不同通信使用的是不同的随机数 k_1、k_2、k_3, 所以, 攻击者不能确定两次通信是否来自同一个用户. 即实现了会话的不可关联性.

(10) 可否认: 服务器不能够向第三方证明与他通信的用户身份. 因为服务器能够选择 k_1, k_2, k_3, k_4, 计算 $k_S=H(d_SQ_UP.x, k_2k_3P.x)$ 和 k_3P、k_4P、$k_4Q_S+k_3k_1P+Q_U$, C_U, 其中 $C_U=E(k_S, (r_U, s_U), I_U, t_U, k_1P.x)$. 也就是说, 服务器也能够仿真用户生成同样的认证消息. 所以, 设计的的协议对用户来说是可否认的.

这里与其他具有隐私保护性质的类似协议进行比较. 文献[3~7]强调了用户匿名性, 但文献[3~5]设计的协议不满足认证性、匿名性、不可关联性、前向安全性、可否认性, 文献[7]不满足对用户的认证性, 文献[6]由于使用密钥传输和签名, 因此不提供密钥控制、前向安全性、可否认性, 另一个明显不足是需要预先获得响应方的公钥证书, 在大型分布式网络中此假设是不现实的. 文献[12]强调了可否认性, 但没考虑密钥控制、前向安全、用户匿名. 目前, 认证协议已制订出国际标准并普遍应用于工程实践, 具有匿名性、可否认性等单一的隐私属性的认证协议也已经出现[6,12], 但满足本文的增强隐私属性的认证协议还没人提出. 在我们的认证协议中, 由于采用公钥密码体制且不预先存储对方证书, 因此需要验证数字证书, 为了提供前向安全性、用户身份的前向匿名性, 需要采用 Diffie-Hellman 密钥交换, 因此带来了协议复杂, 计算量较大等不足, 用户端与服务器端各需要 8 次点乘、2 次随机数生成、3 次 HASH 运算、1 次逆运算、1 次对称密码加密与解密.

5 结论

本文规范了增强用户隐私的认证密钥协商协议应满足的安全需求, 基于椭圆曲线设计了一个增强用户隐私的认证密钥协商协议, 并对其进行了安全性分析. 所设计的协议可以有效地保护用户的隐私并可应用于电子商务.

参考文献:

[1] Westin. Privacy and Freedom[M]. New York: Atheneum, 1967. 7-7.

[2] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22: 644-654.

[3] Aydos M, Sunar B, Koc C K. An elliptic curve cryptography based authentication and key agreement protocol for wireless communication[EB/OL]. http://www.crypto.wpi.edu/Publications/Documents/ask_98_an.pdf, 1998-10-30/2007-12-14.

[4] Aydos M, Savas E, Koc C K. Implementing network security protocols based on elliptic curve cryptography[EB/OL]. http://islab.oregonstate.edu/papers/c16nsecc.pdf, 1999-05-20/2007-12-14.

[5] Aydos M, Yanik T, Koc C K. High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor[J]. IEE Proceedings on Communications, 2001, 148(5): 273-279.

[6] Abadi M, Fournet C. Private authentication[J]. Theoretical Computer Science, 2004, 322(3): 427-476.

[7] Mangipudi K, Katti R, Fu H. Authentication and key agreement protocols preserving anonymity[J]. International Journal of Network Security, 2006, 3(3): 259- 270.

[8] 陈晓峰, 王育民. 基于匿名通讯信道的安全电子投票方案[J]. 电子学报, 2003, 31(3): 390- 393.
Chen X F, Wang Y M. A secure electronic voting scheme based on anonymous communication channel[J]. Acta Electronica Sinica, 2003, 31(3): 390- 393. (in Chinese)

[9] Mangipudi K, Malneedi N, Katti R, Fu H. Attacks and solutions on Aydos-Savas-Koc's wireless authentication protocol[A]. Symposium on Security and Network Management, IEEE Global Telecommunications Conference[C]. Piscataway: Institute of Electrical and Electronics Engineers Inc, 2004. 2229- 2234.

[10] Sun H M, Hsieh B T, Tseng S M, Cryptanalysis of Aydos et al's ECC-based wireless authentication protocol[A]. IEEE International Conference on e-Technology, e-Commerce, and e-Service[C]. Piscataway: Institute of Electrical and Electronics Engineers Inc, 2004. 565- 568.

[11] 曹天杰. 隐私增强协议研究[D]. 北京: 中国科学院软件研究所, 2006.

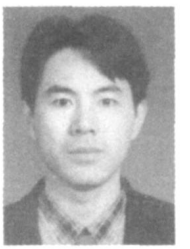
[12] Cao Tianjie, Lin Dongdai, Xue Rui. An efficient ID-based deniable authentication protocol from pairings[A]. 19th International Conference on Advanced Information Networking and Applications[C]. Piscataway: Institute of Electrical and Electronics Engineers Inc, 2005. 388- 391.

[13] P1363: Standard Specifications For Public Key Cryptography[S].

[14] Schroeppel R, et al. Fast key exchange with elliptic curve systems[A]. Advances in Cryptology[C]. Berlin: Springer-Verlag GmbH & Company KG, 1995. 43- 56.

[15] William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition[M]. Upper Saddle River: Prentice Hall, 2005. 312- 312.

作者简介:



曹天杰　男, 1967 年生于江苏徐州, 教授, 博士. 研究方向为密码学与信息安全.
E-mail: tjcao@cumt.edu.cn

雷　红　女, 1982 年生于云南曲靖, 硕士研究生. 研究方向为密码学与信息安全.