基于双线性对和 Nonce 的智能卡远程用户认证方案 *

王德松[1], 李建平[1,2]

(1. 电子科技大学 计算机科学与工程学院, 成都 610054; 2. 后勤工程学院 国际小波分析与应用研究中心, 重庆 400016)

摘 要: 远程用户认证方案是远程服务器通过不安全的网络认证远程用户身份的一种机制。根据椭圆曲线上的双线性对的优良性质,2006 年,Das 等人提出了基于双线性对的远程用户认证方案。2009 年, Goriparthi 等人指出该方案易遭受伪造攻击和重放攻击并给出了一个改进方案。然而发现 Goriparthi 等人的改进方案易遭受内部人员攻击、拒绝服务攻击和服务器哄骗攻击以及存在时钟同步问题。为了克服这些缺点,提出了基于双线性对和 Nonce 的智能卡远程用户认证方案。安全分析表明,该方案不但增强了认证系统的安全性,而且可安全地完成用户和远程系统间的交互认证。

关键词: 认证; 双线性对; 智能卡; 攻击; 安全; Nonce

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0733-04

doi:10.3969/j.issn.1001-3695.2010.02.091

Authentication scheme for remote users based on bilinear pairing and Nonce using smart cards

WANG De-song[1], LI Jian-ping[1,2]

(1. *School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 610054, *China*; 2. *International Centre for Wavelet Analysis & Applications, Logistical Engineering University, Chongqing* 400016, *China*)

Abstract: Remote user authentication scheme is a mechanism which allows a server to authenticate a remote user over insecure channel. In 2006, Das et al proposed a remote user authentication scheme using bilinear pairings according to the merits of bilinear pairing on an elliptical curve. In 2009, Goriparthi et al pointed out that Das et al's scheme is easily vulnerable to the replay attack and the forgery attack, and proposed an improved scheme. However, found out weaknesses of Goriparthi et al's scheme against the insider attack, the denial of service attack, the server spooling attack and the existing clock synchronization problem. To overcome these weaknesses, proposed a novel authentication scheme for remote users based on bilinear pairing and nonce using smart cards. The security analysis shows that the proposed scheme not only enhances the security of the authentication system but also accomplishes mutual authentication safely between the user and the remote system.

Key words: authentication; bilinear pairing; smart card; attack; security; Nonce

0 引言

随着计算机网络的普及和电子商务的蓬勃发展, 越来越多的资源和应用都是利用网络远程获取。如何确保特定的资源只能被合法、授权的用户访问和使用,即如何正确地鉴别用户的身份是保证通信网和系统数据安全的首要条件。在计算机网络中,身份认证是一种证实用户所声称的身份是否真实的技术,结合密码学技术,许多专家和学者提出了有关身份认证的有效方案。1981 年,Lamport[1] 提出了一种基于密码表的用户认证方案,其可以抵抗重放攻击。然而,当存储在主机的口令一旦遭到攻击者的修改,方案将无任何安全可言, 同时该方案的计算量非常大,实用性不强。为了改进远程认证的效率和增强其安全性,避免对密码表的所有可能的攻击,许多基于智能卡的认证方案被提出[2~10]。智能卡可以作为一种更有效的用于认证身份的个人持有物。由于智能卡具有数据处理能力,它可以进行较复杂的操作,能实现系统与持卡人之间的相互认证,用智能卡作为用户的身份标志时,采用合适的认证协议,可以使认证系统的安全性大大提高。

为了更好地抵抗重放攻击,许多基于时间戳的方案被提出[11~14]。虽然时间戳可以为任何电子文件或网上交易提供准确的时间证明,可以检验出文件或交易的内容在自己加上时间戳后是否曾被人修改过,然而,基于时间戳的方案存在严重的时钟同步问题。在文献[15]中,Needham 等人首次提出了 Nonce 概念。此后许多研究人员提出了基于 Nonce 的认证方案[16~19],解决了认证方案的时钟同步问题,但有些方案仍然存在一些缺陷,如文献[16]提出的认证方案易受到拒绝服务(DoS)攻击;文献[17]提出的认证方案易受到内部人员攻击[20];文献[18]提出的认证方案易遭受中间人攻击[21]。

收稿日期: 2009-06-03; **修回日期**: 2009-07-29 **基金项目**: 国家"863"计划资助项目(2007AA01Z423);国家自然科学基金资助项目(60703113);中国工程物理研究院重大基金资助项目(2006Z0604);四川省经贸委资助项目(2008CD00053)

作者简介:王德松(1973-),男,四川渠县人,博士研究生,主要研究方向为信息安全、身份认证、生物特征识别与认证(desong.wangg@gmail.com);李建平(1964-),男,湖南祁阳人,教授,博导,主要研究方向为小波分析、信息安全、生物特征识别与认证.

作为一种特殊映射的双线性对[22]，它是把椭圆曲线的两个元素对映射生成合适的有限域上的一个元素[23]，而且对于安全效率、密钥大小和带宽方面，椭圆曲线加密系统比整数因数分解系统和离散对数系统更加有效[24]。文献[20]利用椭圆曲线密码系统实现了用户和服务器的双向认证。在 2006 年，Das 等人[25]提出了一个基于双线性对的远程用户认证方案，但在文献[19]中，田俊峰等人指出该方案易遭受伪造攻击和拒绝服务攻击，同时在认证过程中也存在时钟同步问题。为克服这些缺点，他们利用双线性对 Nonce 概念提出了双私钥双随机数认证方案，安全高效地实现了交互认证。在 2009 年，Goriparthi 等人[26]指出了 Das 等人的方案不但存在伪造攻击，还存在重放攻击，而且还给出了一个改进方案。然而，发现 Goriparthi 等人的改进方案在认证过程中存在时钟同步问题，易遭受拒绝服务攻击和服务器伪装攻击，同时也存在内部人员攻击。

为了克服 Goriparthi 等人方案的不足，本文在智能卡方案的基础上，采用双线性对和 Nonce 概念提出了基于双线性对和 Nonce 的智能卡远程用户认证方案。该方案不但很好地解了决时钟同步问题，而且还能有效地防止内部人员攻击、拒绝服务攻击和服务器伪装攻击，更加安全地实现了交互认证。在本文的方案中借鉴了文献[18, 26]中的认证思想，并对其进行了改进，使本文的方案具有更高的安全性。

1 Goriparthi 等人的认证方案及其安全漏洞

Goriparthi 等人的认证方案包括五个阶段，即设置阶段、注册阶段、登录阶段、认证阶段和密码修改阶段。

1）设置阶段

假设 G_1 和 G_2 是两个阶为 q 的加法和乘法循环群，q 是一个大素数；假设 P 是 G_1 的生成元，$e: G_1 \times G_1 \rightarrow G_2$ 为一个双线性对，$H: \{0,1\}^* \rightarrow G_1$ 是单向加密 hash 函数，$h: \{0,1\}^* \rightarrow Z_q^*$ 是安全单向 hash 函数。远程系统 RS 选择秘密私钥 s 并计算公钥 $\text{pub}_{\text{RS}} = sP$，远程系统 RS 公布系统参数 $\{G_1, G_2, e, q, P, \text{pub}_{\text{RS}}, H, h\}$ 和保密私钥 s。

2）注册阶段

R1：用户 U_i 通过安全的通道向远程系统 RS 提交个人的 ID_i 和密码 PW_i；

R2：远程系统 RS 接收到注册请求后计算 $Re\ g_{\text{ID}_i} = sH(\text{ID}_i) + H(PW_i)$；

R3：RS 将 ID_i，$Re\ g_{\text{ID}_i}$，$H(\cdot)$，$h(\cdot)$ 存储到智能卡中并通过安全的通道将智能卡发送给用户 U_i。

3）登录阶段

L1：用户 U_i 把智能卡插入相应的终端设备中并输入个人 ID_i 和 PW_i；

L2：在验证 ID_i 的有效性后，智能卡计算

$$V_i = V(V_x, V_y) = r\text{pub}_{\text{RS}}$$

$$D\text{ID}_i = (r + h(T_U \| V_x \| V_y))(Re\ g_{\text{ID}_i} - H(PW_i))$$

其中：T_U 是当前用户系统的时间戳，r 是智能卡产生的一个随机数，$\|$ 表示字符串级联；

L3：U_i 向 RS 发送登录请求信息 $\{\text{ID}_i, D\text{ID}_i, V_i, T_U\}$。

4）认证阶段

假设 RS 在 T_{RS} 接收到认证请求信息 $\{\text{ID}_i, D\text{ID}_i, V_i, T_U\}$，则 RS 执行如下的操作：

A1：RS 检查是否 $T_{\text{RS}} - T_U \leqslant \Delta T$ 成立，这里 ΔT 表示因为传输延迟所期望的有效时间间隔，T_{RS} 为远程系统 RS 端当前的时间戳，如果不成立，则拒绝服务，否则转第 A2 步；

A2：验证是否

$$e(D\text{ID}_i, P) \stackrel{?}{=} e(H(\text{ID}_i), V_i + h(N_1 \| V_x \| V_y)\text{pub}_{\text{RS}})$$

如果成立则接收登录请求，否则拒绝请求。

5）密码修改阶段

P1：用户 U_i 把智能卡插入相应的终端设备中并输入个人 ID_i 和 PW_i；

P2：智能卡对用户产生一个警告信息；

P3：验证用户输入的 ID_i 与智能卡中储存的 ID_i 是否匹配，如果匹配，则立刻要求用户输入新的 PW_i^*；

P4：智能卡计算

$$Re\ g_{\text{ID}_i}{}^* = R_e\ g_{\text{ID}_i} - H(PW_i) + H(PW_i^*)$$

并用 $Re\ g_{\text{ID}_i}{}^*$ 替换先前储存在智能卡上的 $Re\ g_{\text{ID}_i}$。

虽然 Goriparthi 等人[20]的远程认证方案比较有效，但它很容易受到内部人员攻击、拒绝服务攻击、服务器伪装攻击，同时还存在时钟同步问题。

1）内部人员攻击　由于 Goriparthi 等人方案中，用户 U_i 的密码 PW_i 对 RS 是透明的，当用户使用相同的口令登录其他服务器时，RS 的内部人员就可假冒 U_i 接入其他服务器。

2）拒绝服务攻击　由于该方案中是利用时间戳来保证一个认证请求信息的有效性，利用该特性，攻击者可拦截登录阶段的认证请求信息 $\{\text{ID}_i, D\text{ID}_i, V_i, T_U\}$，并延迟一段时间后再重新向 RS 传送该信息，当延迟超过一定的时间，T_U 就不能通过 RS 的有效性检查，从而使得 RS 不能为用户提供连续有效的服务。若攻击者截获登录请求信息 $\{\text{ID}_i, D\text{ID}_i, V_i, T_U\}$ 后，只需选取合适的 T_U^* 或者修改时间 T_U 至足够大，构造出 $T_{\text{RS}} - T_U \leqslant \Delta T$，就可以向远程系统发送信息 $\{\text{ID}_i, D\text{ID}_i, V_i, T_U^*\}$，仿冒用户 U_i 登录远程系统，并能通过远程系统认证阶段的第 A1 步检验，致使远程系统忙于认证阶段的第 A2 步中的计算和检验，从而形成对 RS 的拒绝服务攻击。另外，当网络发生阻塞时，也会发生以上的拒绝服务。

3）服务器伪装攻击　由于 Goriparthi 等人的方案只执行单边认证即只有客户端身份验证，而用户却不知道 RS 的真实性，攻击者可以设置一个假的服务器来熟练操作用户的数据。如果假定 Goriparthi 等人的方案被部署于电子银行或者电子商务，客户也希望验证远程实体。然而，在 Goriparthi 等人的方案中，认证只是单向认证，客户没有认证服务器的真实性，因此，客户不能相信远程系统是真实的服务实体。导致 Goriparthi 等人的方案很容易受到假的服务器伪装攻击。下面具体说明如何实现服务器伪装攻击。

假设 Eric 是一个在用户和服务器之间的攻击者。当用户通过不安全的通信通道发送认证请求信息 $C = \{\text{ID}_i, D\text{ID}_i, V_i, T_U\}$ 时，Eric 也能得到它，此时 Eric 通过假扮服务器哄骗用户 U_i。Eric 通过下面的操作来扮演假的服务器和发送伪造互认证信息：

S1：Eric 通过不安全的通信通道得到登录认证信息 $C = \{\text{ID}_i, D\text{ID}, V_i, T_U\}$ 后，计算 $C_1 = h(V_i \| T_E)$，T_E 是当前 Eric 的时间戳。

S2：Eric 向用户 U_i 发送互认证信息 $\{C_1, T_E\}$。

S3：用户 U_i 收到信息 $\{C_1, T_E\}$ 后，验证时间戳的有效性，如果无效，则拒绝互认证并终止操作；否则计算 $C_1^* = h(V_i \| T_E)$，并验证是否 $C_1^* \stackrel{?}{=} C_1$，如果成立则相信 Eric 是真正的服务器。然而 Eric 却是一个攻击者，此时 Eric 就成功地实现了服务器伪装攻击。

4)时钟同步问题　由于 Goriparthi 等人认证协议采用了时间戳,就要求网络内需要有全局时钟服务器和相应的时钟同步协议。由上面的分析可看出,Goriparthi 等人的方案中的漏洞有一部分是由于时间戳引起的,基于时间戳的认证协议不仅引入了较多的安全风险,而且要在全网实现时间同步,这在实施上是非常困难的。

2　本文提出的认证方案

本文设计的认证方案也包括五个阶段,即设置阶段、注册阶段、登录阶段、认证阶段和密码修改阶段。

1)设置阶段

假设 G_1 和 G_2 是两个阶为 q 的加法和乘法循环群,q 是一个大素数;假设 P 是 G_1 的生成元,$e:G_1\times G_1\to G_2$ 为一个双线性对,$H:\{0,1\}^*\to G_1$ 是单向加密 hash 函数,$h:\{0,1\}^*\to Z_q^*$ 是安全单向 hash 函数。远程系统 RS 选择秘密私钥 s 并计算公钥 $\mathrm{pub}_{RS}=sP$,远程系统公布系统参数 $\{G_1,G_2,e,q,P,\mathrm{pub}_{RS},H,h\}$ 和保密私钥 s。

2)注册阶段

R1:用户 U_i 通过安全的通信通道向远程系统 RS 提交个人的 ID_i 和 $H(PW_i\oplus R)$,这里 PW_i 是用户的密码,R 是一个 64 bit 的随机数;

R2:远程系统 RS 接收到注册请求后,搜索用户 ID 存储表(表 1),检验是否已存在该 ID_i,如果存在,则返回要求用户 U_i 重新选择 ID_i;否则计算

$$Re\ g_{\mathrm{ID}_i}=sH(\mathrm{ID}_i)+H(PW_i\oplus R)$$

其中:s 为远程系统 RS 密钥,$\oplus$表示按位异或运算,并保存 ID_i 到 ID 存储表;

R3:RS 将 ID_i,$Re\ g_{\mathrm{ID}_i}$,$H(\cdot\ )$,$h(\cdot\ )$存储到智能卡中并通过安全的途径将智能卡发送给用户 U_i;

R4:在用户收到智能卡后,向智能卡输入 R,此时智能卡中存储的参数是 $\{\mathrm{ID}_i,Re\ g_{\mathrm{ID}_i},H(\cdot\ ),h(\cdot\ ),R\}$。

3)登录阶段

L1:用户 U_i 把智能卡插入相应的终端设备中并输入个人 ID_i 和 PW_i;

L2:在智能卡验证 ID_i 和 PW_i 的有效性后,智能卡产生两个随机数 Nonce[15~19](Nonce means used only once,即只用一次)r 和 N_1,并计算

$$V_i=V(V_x,V_y)=r\mathrm{pub}_{RS}$$

$$D\mathrm{ID}_i=(r+h(N_1\|V_x\|V_y))(Re\ g_{\mathrm{ID}_i}-H(PW_i\oplus R));$$

L3:用户 U_i 向远程系统 RS 发送登录请求信息 $C=\{\mathrm{ID}_i,D\mathrm{ID}_i,V_i,N_1\}$。

4) 认证阶段

为了讨论方便,先给出如下新鲜标记定义。

定义 1　新鲜标记[19]。对于从用户发来信息中由用户 ID 和随机数 N 组成的 $\{\mathrm{ID}_i,N_1\}$,如果是首次出现则认为是新鲜的,可被接收的,否则认为是不新鲜的,拒绝服务。

远程系统 RS 接收到用户认证请求信息 $\{\mathrm{ID}_i,D\mathrm{ID}_i,V_i,T_U\}$ 后,RS 执行如下的操作:

A1:远程系统将为 ID_i 设置一个计数器和时间戳,用于计算该 ID_i 的出现频率。检查会话状态表(表 2),看 ID_i 是否已在会话状态,如果是则拒绝登录,如果否则检查 ID 存储表,看是否已存在该 ID_i,如果不存在,则拒绝为该用户服务;同时,检查用户 ID_i 的出现频率值,如果该值大于某一经验阈值,则认为非法用户正尝试非法登录或对远程系统进行攻击,删除 ID_i 或隔离审查;否则,转第 A2 步。

A2:验证是否

$$e(D\mathrm{ID}_i,P)\stackrel{?}{=}e(H(\mathrm{ID}_i),V_i+h(N_1\|V_x\|V_y)\mathrm{pub}_{RS})$$

如果不成立则拒绝请求,否则接收登录请求;

A3:远程系统 RS 产生一个随机数 Nonce N_2,计算 $C_2=N_2sH(\mathrm{ID}_i)$,并向用户发送互认证信息 $\{C_2,N_2\}$;

A4:用户收到来自 RS 的信息后,计算

$$C_2^*=N_2(Re\ g_{\mathrm{ID}_i}-H(PW_i'\oplus R))$$

其中 PW_i' 是用户的密码;

A5:验证是否 $C_2^*\stackrel{?}{=}C_2$,若成立,则用户通过了对 RS 的认证,否则用户终止任何操作。

5)密码修改阶段

本认证方案也支持用户对密码进行修改,以避免密码猜测攻击或设置更易记忆的密码,而且这一操作不需要远程系统协助,降低了远程系统的负担,减少了更改密码协议所需的通信消耗,也使得密码修改过程的安全性得以保证。密码修改的具体过程如下:

P1:用户 U_i 把智能卡插入相应的终端设备中并输入个人 ID_i 和 PW_i;

P2:智能卡对用户产生一个警告信息;

P3:智能卡验证用户 ID_i 和 PW_i 的有效性,并在验证通过后提示用户输入新的 PW_i^*;

P4:智能卡计算

$$Re\ g_{\mathrm{ID}_i}^*=Re\ g_{\mathrm{ID}_i}-H(PW_i\oplus R)+H(PW_i^*\oplus R)$$

并用 $Re\ g_{\mathrm{ID}_i}^*$ 替代先前储存在智能卡上的 $Re\ g_{\mathrm{ID}_i}$,这样就成功地修改了用户的密码口令。

表1　ID存储表

用户序列号	ID
1	ID_1
2	ID_2
⋮	⋮
i	ID_i
⋮	⋮

表2　会话状态表

会话ID	随机数N	RS时间T
ID_1	N_1	T_1
ID_3	N_3	T_3
ID_5	N_5	T_5
⋮	⋮	⋮
ID_i	N_i	T_i
⋮	⋮	⋮

3　安全性分析

以下的安全性分析是在单向无碰撞 hash 函数和计算离散对数问题的困难性[19]的前提下进行的。分析表明,本文提出的认证方案具有更好的安全性,因为它可以有效地克服内部人员攻击、拒绝服务攻击和服务器伪装攻击。

1)可以防止内部人员攻击　本方案中,用户首先选了一个 64 bit 的随机数 R 后计算 $H(PW_i\oplus R)$,然后发送 $H(PW_i\oplus R)$给 RS,因此远程系统只知道 $H(PW_i\oplus R)$,而且 R 的熵是非常大的,因而能冒充用户 U_i 的口令为 PW_i 去登录其他服务器的概率就很小。

2)可以防止重放攻击　由于 Nonce 变量 N_1 和 N_2 是由智能卡和远程系统独立产生,且在每次会话时 N_1 和 N_2 的值都是截然不同的,攻击者没有机会来成功实现重放攻击。假设攻击者截获登录阶段的第 A3 步中的登录请求认证信息 $\{\mathrm{ID}_i,D\mathrm{ID}_i,V_i,N_1\}$,并假冒用户 U_i 向 RS 重新发送 $\{\mathrm{ID}_i,D\mathrm{ID}_i,V_i,N_1\}$给远程系统,但此时的$\langle\mathrm{ID}_i,N_1\rangle$已在会话状态表中,因而无法通过 RS 的认证,这样远程系统就有效地防止了重放攻击。

3)可以防止拒绝服务攻击　由于在认证过程中设置了会话状态表,可通过检验 ID_i 出现的频率值和$\langle\mathrm{ID}_i,N_1\rangle$对的新鲜

标记来有效防止拒绝服务攻击。本方案认证请求信息的有效性与时间因子无关,因而不会产生与 Goriparthi 等人的认证方案类似的拒绝服务攻击。

4)可以防止猜测攻击 假设攻击者截获了认证信息$\{ID_i, DID_i, V_i, N_1\}$和$\{C_2, N_2\}$,由于这些信息中不包括用户密码的任何信息,攻击者不可能计算出用户的密码 PW_i;同样,根据单向无碰撞 hash 函数的性质和计算离散对数问题的困难性,攻击者也是极其困难地从截获的认证信息$\{ID_i, DID_i, V_i, N_1\}$和$\{C_2, N_2\}$中得到远程系统的密钥 s,这样就有效地防止了猜测攻击。

5)可以防止服务器伪装攻击 在本方案中,用户首先在注册阶段认证服务器的真实性;其次由于攻击者不知道远程系统的密钥 s,无法计算 $C_2 = N_2 sH(ID_i)$,从而无法正确产生互认证信息$\{C_2, N_2\}$来实现互认证,因此可以有效地防止服务器伪装攻击。

6)可以防止伪造攻击 如果攻击者不知道用户的密码口令 PW_i、远程系统的密钥 s,要构造出有效的 $Re\ g_{ID_i} = sH(ID_i) + H(PW_i \oplus R)$,其难度相当于求解离散对数问题;如果攻击者截获 $ID_i, DID_i, V_i, N_1, C_2, N_2$ 信息,从这些信息中攻击者仍然不能计算出 PW_i 和 s,这也是属于离散对数问题的难解性;如果攻击者改变其中的信息发送到远程系统,远程系统将在认证阶段的第 A2 步检验出来;如果不改变信息,直接发送到远程系统,这属于重放攻击,根据前面的分析也能防止。攻击者不能构造有效的 DID_i、V_i、$Re\ g_{ID_i}$,从而本方案能有效地防止伪造攻击。

4 安全性比较

本文提出的认证方案与 Goriparthi 等人和 Das 等人的认证方案的安全性比较如表 3 所示。从表 3 中可看出,本文提出的认证方案具有更高的安全性。

表3 三种认证方案的安全性比较

安全属性	本文所提认证方案	Goriparthi等人认证方案	Das等人认证方案
内部人员攻击	否	是	是
重放攻击	否	否	是
拒绝服务攻击	否	是	是
猜测攻击	否	否	是
服务器伪装	否	是	是
伪造攻击	否	否	是
双向认证	是	否	否

5 结束语

本文提出的基于双线性对和 Nonce 的智能卡远程用户认证方案是在智能卡方案的基础上,采用双线性对与 Nonce 概念相结合的方法,正确有效地实现了用户与远程系统的交互认证。该方案不但满足了 Goriparthi 等人的认证方案的优点,而且还能有效地防止内部人员攻击、拒绝服务攻击、猜测攻击和服务器哄骗攻击,同时还很好地解决了时钟同步问题。

参考文献:

[1] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24(11): 770-772.

[2] SHIMIZU A, HORIOKA T, INAGAKI H. A password authentication method for contents communication on the Internet[J]. IEICE Trans on Communications, 1998, E81-B(8): 1666-1673.

[3] FAN C L, CHAN Y C, ZHANG Zhi-kai. Robust remote authentication scheme with smart cards[J]. Computers & Security, 2005, 24(8): 619-628.

[4] JUANG W S. Efficient password authenticated key agreement using smart card[J]. Computer & Security, 2004, 23: 167-173.

[5] KU Wei-chi, CHEN Shuai-min. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Trans on Consumer Electronics, 2004, 50(1): 204-207.

[6] LEE C C, LI Li-hua, HWANG M S. A remote user authentication scheme using hash functions [J]. ACM SIGOPS Operating Systems Review, 2002, 36(4): 23-29.

[7] PEYRAVIAN M, ZUNIC N. Methods for protecting password transmission[J]. Computers & Security, 2000, 19(5): 466-469.

[8] WEN H A, LEE T F, HWANG T. Provably secure three-party password-based authenticated key exchange protocol using Weil pairing[J]. IEE Proceedings of Communications, 2005, 152(2): 138-143.

[9] 邱慧敏, 杨义先, 胡正名. 一种新的基于智能卡的双向身份认证方案设计[J]. 计算机应用研究, 2005, 22(12): 103-105.

[10] 薛素静, 孔梦荣. 基于单向哈希函数的远程口令认证方案[J]. 计算机应用研究, 2008, 25(2): 512-515.

[11] CHIEN H Y, JAN J K, TSENG Y M. An efficient and practical solution to remote authentication: smart card [J]. Computers & Security, 2002, 21(4): 372-375.

[12] JUANG W S. Efficient password authenticated key agreement using smart cards[J]. Computers & Security, 2004, 23(2): 167-173.

[13] SUN H M. An efficient remote user authentication scheme using smart cards[J]. IEEE Trans on Consumer Electronics, 2000, 46(4): 958-961.

[14] WANG Bin, LI Zheng-quan. A forward-secure user authentication scheme with smart cards[J]. International Journal of Network Security, 2006, 3(2): 108-111.

[15] NEEDHAM R M, SCHROEDER M D. Using encryption for authentication in large networks of computer[J]. Communication of the ACM, 1978, 21(12): 993-998.

[16] LEE S W, KIM H S, YOO K Y. Efficient nonce-based remote user authentication scheme using smart cards[J]. Applied Mathematics and Computation, 2005, 167(1): 355-361.

[17] FAN C I, CHAN Y C, ZHANG Zhi-kai. Robust remote authentication scheme with smart cards[J]. Computers & Security, 2005, 24(8): 619-628.

[18] LIU Jia-yong, ZHOU An-min, GAO Min-xu. A new mutual authentication scheme based on Nonce and smart cards[J]. Computer Communications, 2008, 31(10): 2205-2209.

[19] 田俊峰, 焦洪强, 李宁,等. 双私钥双随机数认证方案[J]. 计算机研究与发展,2008, 45(5): 779-785.

[20] JUANG W S, CHEN S T, LIAW H T. Robust and efficient password-authenticated key agreement using smart cards[J]. IEEE Trans on Industrial Electronics, 2008, 55(6): 2551-2556.

[21] SUN Da-zhi, HUAI Jin-peng, SUN Ji-zhou, *et al*. Cryptanalysis of a mutual authentication scheme based on nonce and smartcards[J]. Computer Communications, 2009, 32(6): 1015-1017.

[22] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computing, 2003, 32(3): 585-615.

[23] BARRETO P S L M, KIM H Y, LYNN B, *et al*. Efficient algorithms for pairing-based cryptosystems[C]//Proc of the 22nd Annual International Cryptology Conference on Advances in Cryptology. 2002: 354-369.

[24] LAUTER K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless Communications, 2004, 11(1): 62-66.

[25] DAS M, SAXENA A, GULATI V, *et al*. A Novel remote user authentication scheme using bilinear pairings[J]. Computers & Security, 2006, 25(3): 184-189.

[26] GORIPARTHI T, DAS M L, SAXENA A. An improved bilinear pairing based remote user authentication scheme[J]. Computer Standards & Interfaces, 2009, 31: 181-185.