基于口令的认证密钥协商协议的安全分析与改进

舒剑[1,2]，许春香[1]

(1. 电子科技大学 计算机科学与工程学院，四川 成都 611731；2. 江西财经大学 电子商务系，江西 南昌 330013)

摘 要：对基于口令的标准模型下可证明安全的认证密钥协商协议进行安全分析，指出该协议易受反射攻击。同时给出了一个改进方案，该方案不仅弥补了原方案的缺陷，而且改善了协议的性能。最后，基于 DDH 假设，在标准模型下证明了协议的安全性。结果表明，改进后的协议还具有完美前向安全特性。

关键词：基于口令；反射攻击；标准模型；可证安全

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2010)03-0051-06

Analysis and improvement of a password-based authenticated key exchange protocol

SHU Jian[1,2], XU Chun-xiang[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;

2. Department of Electronic Commercial, University of Jiangxi Financial Economics, Nanchan 330013, China)

Abstract: The security of a recently proposed password-based authenticated key exchange protocol was analyzed. Although it was provably secure in the standard model, it was vulnerable to reflection attacks. A modify scheme was proposed, which eliminated the defect of original scheme and improved the efficiency of the protocol. The security of the proposed scheme had been proven in the standard model under DDH assumption. The results show that it provides perfect forward secrecy.

Key words: password-based; reflection attacks; standard model; provably secure

1 引言

认证密钥协商协议是让用户在开放网络通过交互，建立一个共享的会话密钥，从而实现开放网络中的安全通信。较早的认证密钥协商协议是通信双方借助持有的高熵秘密（如数字签名的私钥)生成会话密钥，然后使用会话密钥进行加密或认证。但是这些高熵秘密不便于保存和记忆，有时还需要可信第三方的参与。让用户共享一个低熵的口令而生成高熵的会话密钥在实际环境中有广泛的应用，但这方面的研究相对较少。由于口令具有长度短的特性，攻击者可能在离线状态下进行穷举字典攻击。

Bellovin 和 Merritt[1]首先提出能抵抗字典攻击的基于口令的两方密钥协商协议，随后许多相关工作[2~9]对如何利用口令生成会话密钥进行了研究。文献[1~9]都是在随机预言模型下证明协议的安全性。随机预言模型自从 1993 年被 Bellare 和 Rogaway[10]提出以来，在密码学的可证安全领域得到广泛的应用。然而，随机预言模型下的安全并不代表真实世界的安全，因为它依赖现实世界无法实现的随机预言假设。另一方面，不需要随机预言假设的证明（即在标准模型下的证明）就能够清楚地说明，除非其

收稿日期：2009-04-17；**修回日期**：2010-01-15

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2009AA012415）

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (2009AA012415)

所基于的底层数学难题被破解，否则一个可证安全的方案不可能被攻破。因此，在标准模型下设计基于口令的认证协议更具有实际意义。

基于 Cramer-Shoup[11]提出的 CCA2(chosen ciphertext attack-2)安全的公钥加密体制，Katz, Ostovsky 和 Yung[12]首先提出了一种标准模型下可证安全的基于口令认证密钥协商协议。Gennaro 和 Lindell[13]给出了 KOY 协议的抽象框架。他们的协议计算复杂度很高，并且协议只能实现单向认证。为降低计算复杂度和实现双向认证，Jiang 和 Gong[14]提出了一种改进的标准模型下基于口令认证密钥协商协议。

通过引入伪随机函数集和通信双方均使用 ElGamal 加密方案，殷胤等[15]提出了高效的基于口令认证密钥协商协议，该协议极大降低了计算复杂度。但是，协议对发起方(客户)要进行 2 次认证，并且要求服务器方拥有私钥，因而该协议不适合只共享相同口令的双方进行密钥协商。另外，由于通信双方均使用 ElGamal 加密方案并且协议设计不合理，笔者发现该协议不能抵抗反射攻击或变型的反射攻击。

本文提出一种新的基于口令认证密钥协商协议。协议的发起方和响应方均使用 ElGamal 加密方案。与文献[15]协议相比，计算机复杂度相当并且不需要响应方拥有私钥。新协议实现了双向认证，并在标准模型下基于 DDH 假设给出了安全性证明。

2 背景知识

2.1 DDH(decisional Diffie-Hellman)假设

设大素数 p,q 满足 $q|(p-1)$，且 G_q 是乘法群 Z_p^* 的一个阶为 q 的子群，g 是群 G_q 的一个生成元，称群 G_q 满足 DDH 假设，如果对于任意 $x,y\in Z_q$，给定 g^x,g^y,任何概率多项式时间算法 D 都不能区分 (g,g^x,g^y,g^{xy}) 和 (g,g^x,g^y,r)，r 是一个随机数，即 $Adv_{g,G}^{\mathrm{ddh}}(D)=|\mathrm{pr}[D(g,g^x,g^y,g^{xy})=1]-\mathrm{pr}[D(g,g^x,g^y,r)=1]|<\varepsilon(n)$。其中 $\varepsilon(\cdot)$ 是一个可忽略函数; $Adv_{g,G}^{\mathrm{ddh}}=\max_D(Adv_{g,G}^{\mathrm{ddh}}(D))$ 表示对所有攻击者 D，$Adv_{g,G}^{\mathrm{ddh}}(D)$ 可能取得的最大值。

2.2 伪随机函数集

一个函数集 $F=\{F_n\}_{n\in N}$ 是伪随机的，如果对于每个概率多项式算法 M 和所有足够大的 n，满足 $Adv^F(M)=|\mathrm{pr}[M^{F_n}(1^n)=1]-\mathrm{pr}[M^{H_n}(1^n)=1]|<\varepsilon(n)$。其中：$H=\{H_n\}_{n\in N}$ 是一个均匀分布的函数集；$\varepsilon(\cdot)$ 是一个可忽略的函数；$Adv^F=\max_M\{Adv^F(M)\}$ 表示对所有多项式算法 M，$Adv^F(M)$ 可能取得的最大值。

2.3 形式化安全模型

本节简要回顾 Bellare 等在文献[5]中定义的基于口令密钥协商协议的形式化安全模型。模型包括一个协议参与者集合 U，每个参与者被模拟为一组预言机。参与者拥有一个共同的口令，预言机 $\prod_{I,J}^n$ 指参与者 I 与 J 的第 n 个实例。模型中还包括一个主动攻击者(用 A 表示)，它被定义为一个概率多项式时间图灵机。模型将攻击者的能力抽象为对若干个预言机的查询，并且这些查询可以是无序和自适应的。

定义 1 会话标识符(SID)：预言机 $\prod_{I,J}^n$ 发送和接收的所有消息的串联。

定义 2 搭档预言机(PID)：若 2 个预言机在同意(accept)状态时有相同的会话标识符 SID, 则称 2 个预言机互为搭档。

Execute 查询：这种查询模拟被动攻击。攻击者 A 通过查询 execute($\prod_{I,J}^n,\prod_{J,I}^s$)获得搭档预言机 $\prod_{I,J}^n$ 和 $\prod_{J,I}^s$ 执行过程中的所有交互信息。

Send 查询：这种查询模拟主动攻击。攻击者 A 向预言机 $\prod_{I,J}^n$ 发送伪造消息，若预言机收到的消息为空(null)，表示攻击者让预言机发起一个新的会话。查询返回消息为接收到假冒消息后，预言机按照协议规则的回复。

Reveal 查询：这种查询模拟预言机 $\prod_{I,J}^n$ 的会话密钥泄漏，返回值为 sk_i。如果预言机还不是“已接受”(accepted)，则返回一个符号 $\perp$ 表示终止。执行了 reveal 查询的实例状态是打开的(opened)。

Corrupt 查询：这种查询模拟前向安全性。要求被询问的预言机返回它拥有的长期私钥(口令)。回答过 corrupt 查询的预言机的状态称为“已腐化”(corrupted)。

Test 查询：这种查询描述协议的语义安全性。它只能运行一次，并且只能对一个“新鲜”的预言机进行。当攻击者 A 进行 Test 查询时，协议随机选择一个比特 $b\in\{0,1\}$,如果 $b=0$，则返回 sk_i，否则，返回一个随机数 r，攻击者根据返回值以及利用其他查询获得的信息，猜测 b 的值为 b'。

如果在 Test 查询中，攻击者成功猜对 b 的值，则称攻击者成功。定义攻击者 A 的成功概率为 $\mathrm{pr}[S]$。

$$\mathrm{pr}[S]=\mathrm{pr}[b=b'],\ \ Adv_{g,G}^{\mathrm{pake}}=2\mathrm{pr}[S]-1$$

定义 $Adv_{g,G}^{\mathrm{pake}}$ 为所有攻击者 A 可能取到的 $Adv_{g,G}^{\mathrm{pake}}(A)$ 的最大值，则称协议是安全的，如果 $Adv_{g,G}^{\mathrm{pake}}<O(q_s/N)+\varepsilon$。其中：$q_s$ 表示 Send 查询的次数；N 表示所有口令的总数；ε 是一个可忽略函数；$O(q_s/N)$ 保证每次 Send 查询，攻击者 A 最多排除常数个可能的口令。

定义 3　新鲜预言机：预言机 $\prod_{I,J}^{n}$ 在同意状态下是未打开的，其搭档预言机也未打开，并且其搭档预言机没有被腐化，则预言机 $\prod_{I,J}^{n}$ 是新鲜的。

3　殷胤等人的协议及其攻击

本节对殷胤等[15]提出的高效的基于口令认证密钥协商协议进行分析。协议描述如图 1 所示。其中 p,q 是大素数且满足 $q|(p-1)$；G_q 是乘法群 Z_P^* 的阶为 q 的子群；g,h 是 G_q 的 2 个生成元；u 是服务器拥有的私钥；F 是一个伪随机函数集；f 是从口令空间到 Z_P 的映射；pw 是客户和服务器共享的口令。

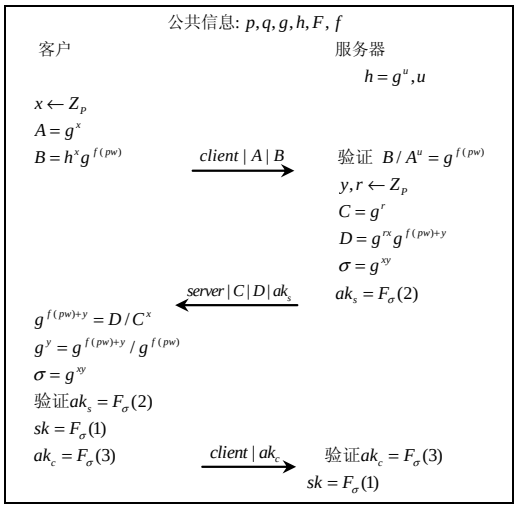

图 1　标准模型下可证安全的 EKE 协议

协议双方均使用 ElGamal 加密机制。由于 ElGamal 加密机制具有抵抗 CPA(chosen plaintext attack)特性，被动攻击无法获得任何有效信息。

假设攻击者伪装成服务器。由于客户发送的信息 $B=h^x g^{f(pw)}=g^{ux}g^{f(pw)}$ 和服务器发送的信息 $D=g^{rx}g^{f(pw)+y}$ 相似，攻击者可伪装成服务器实施变形的反射攻击。攻击过程如下。

攻击者截取客户发送的有效信息 $A=g^x\,|\,B=g^{ux}g^{f(pw)}$，它随机选择一个数 $r\in Z_P$，发送信息 $C=h=g^u\,|\,D=B*g^r=g^{ux}g^{f(pw)+r}$。客户按协议规则求出 $\sigma=g^{xr}$。由于攻击者知道 $A=g^x$ 和 $r\in Z_P$，也能算出 $\sigma=g^{xr}$。

在上面的攻击中，攻击者发动有效攻击时消息 C 必须为 $h=g^u$。即使对协议作一定的修改，使客户对消息 C 进行验证，如果 $C=h$，则终止协议。攻击者仍可以利用消息的自规约特性，伪装成服务器实施有效攻击。攻击过程如下。

攻击者截取客户发送的有效信息 $A=g^x\,|\,B=g^{ux}g^{f(pw)}$，它随机选择 2 个数 $r,v\in Z_P$，发送信息 $C=h*g^v=g^{u+v}\,|\,D=B*A^v*g^r=g^{(u+v)x}\,g^{f(pw)+r}$。客户按协议规则求出 $\sigma=g^{xr}$。由于攻击者知道 $A=g^x$ 和 $r\in Z_P$，也能算出 $\sigma=g^{xr}$，同样发生有效攻击。

4　新的基于口令认证密钥协商协议

本节提出一种新的标准模型下基于口令认证密钥协商协议，协议描述如图 2 所示。p,q 是大素数且满足 $q|(p-1)$；G_q 是乘法群 Z_P^* 的阶为 q 的子群；g,h 是 G_q 的 2 个生成元；F 是一个伪随机函数集；pw 是客户和服务器共享的口令。

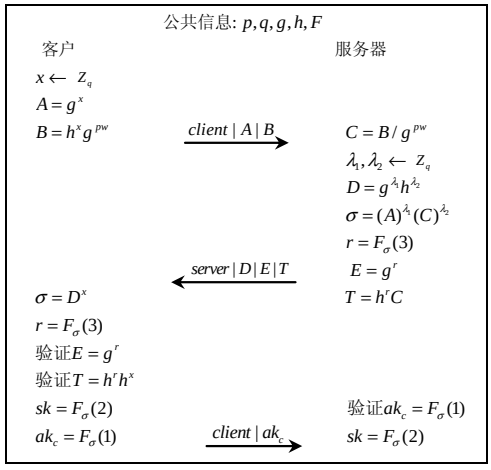

图 2　标准模型下可证安全的基于口令认证密钥协商协议

协议发起方和响应方均采用 ElGamal 加密机制。新协议与文献[15]协议相比，计算复杂度相当并且不需要对协议的发起方进行 2 次认证。由于协议响应方不需要保存私钥，该协议也适用于共享相同口令的 2 个客户进行密钥协商。

5 协议的安全性证明

证明方法是把协议执行看作仿真器与攻击者之间的游戏。仿真器选择 2 个大素数 p,q 且满足 $q|(p-1)$，然后选择 $g \leftarrow G_q, u \leftarrow Z_q$ 和一个伪随机函数 F 并计算 $h=g^u$。随后公布公钥参数 p,q,g,h,F 并像实际协议一样给通信实体分配口令。

本文设计一系列的实验($\Gamma_0,\Gamma_1,\cdots$)，在所有的实验中，预言机按协议的描述回答攻击者的查询。实验 Γ_0 模拟的是攻击者攻击实际协议，以后的实验中逐步修改预言机的回答方式，使攻击者在 2 个相邻实验中成功概率的差值可以忽略。$\mathrm{pr}[S_i]$ 表示攻击者在实验 Γ_t 中成功的概率。

定理 1 Γ 是图 2 描述的协议；N 表示所有可能的口令；F 是 $\{0,1\}^{l(n)} \to \{0,1\}^n$ ($n=\mathrm{lb}q$)的伪随机函数集；p,q 是大素数且满足 $q|(p-1)$；G_q 是乘法群 Z_P^* 的阶为 q 的子群；g,h 是 G_q 的生成元；$q_\mathrm{e},q_\mathrm{s},q_\mathrm{r}$ 分别表示攻击者进行 Execute 查询、Send 查询、Reveal 查询的次数。则，

$$Adv_{\Gamma,A}^{\mathrm{pake}} \leqslant 4q_\mathrm{s}/N + 4(q_\mathrm{e}+q_\mathrm{s})Adv_{g,G}^{\mathrm{ddh}} + 2(q_\mathrm{e}+q_\mathrm{s})Adv^F + 2\min(q_\mathrm{e},q_\mathrm{r})Adv^F + 2\min(q_\mathrm{s},q_\mathrm{r})Adv^F$$

实验 Γ_0：这是实际协议攻击实验。事件 S_0 表示攻击者成功猜出 Test 查询中预言机所使用的比特 b，则可以得到：

$$Adv_{\Gamma,A}^{\mathrm{pake}} = 2\mathrm{pr}[S_0]-1$$

实验 Γ_1：在实验 Γ_1 中，当攻击者进行 Execute 查询时，用随机数 r 替代消息 B。基于 DDH 假设，运用混合证明(hybrid arguments)技巧，可得：

$$|\mathrm{pr}[S_1]-\mathrm{pr}[S_0]| \leqslant q_\mathrm{e}Adv_{g,G}^{\mathrm{ddh}}$$

实验 Γ_2：Γ_2 与 Γ_1 的区别在于攻击者进行 Execute 查询时，ak_c, r 替换为不同的随机数。

注意，在 Γ_1 中，消息 $A|B$ 不再是 g^{pw} 的 ElGamal 加密。不失一般性，消息可为 $A=g^x|B=h^xg^{pc}$ ($pc \neq pw$)。服务器计算 $=D^xg^{(pc-pw)\lambda_2}$ $\sigma=(A)^{\lambda_1}(C)^{\lambda_2}$ $=(g^x)^{\lambda_1}(h^xg^{pc-pw})^{\lambda_2}$。由于 λ_2 的随机性和独立性，σ 在 G_q 中也是随机均匀的。利用伪随机函数集定义，运用混合证明技巧，可得：

$$|\mathrm{pr}[S_2]-\mathrm{pr}[S_1]| \leqslant q_\mathrm{e}Adv^F$$

实验 Γ_3：在实验 Γ_3 中，攻击者进行 Execute 查询时，用随机数 r 替代 sk。

与实验 Γ_2 中的分析类似，得出 σ 是随机均匀的。如果攻击者不进行 Reveal 查询，则在 Γ_3 和 Γ_2 中获得的信息是相同的。在 Γ_2 中，攻击者得到 sk 就等价于对伪随机函数集 F_n 进行了一次查询；而在 Γ_3 中，攻击者得到 r 就等价于对均匀分布函数集 H_n 进行了一次查询。根据伪随机函数集的定义，没有算法可以有效区分伪随机函数集和均匀分布函数集，所以，

$$|\mathrm{pr}[S_3]-\mathrm{pr}[S_2]| \leqslant \min(q_\mathrm{e},q_\mathrm{r})Adv^F$$

实验 Γ_4：Γ_4 与 Γ_3 的区别是，当攻击者进行 Execute 查询时，C 替换为随机数，即 T 替换为随机数。运用混合证明技巧，可得：

$$|\mathrm{pr}[S_4]-\mathrm{pr}[S_3]| \leqslant q_\mathrm{e}Adv_{g,G}^{\mathrm{ddh}}$$

实验 Γ_5：下面开始考虑 Send 查询。当攻击者进行 Send($server|D|E|T$)查询时，仿真器按如下方式验证：仿真器验证 $B/g^{pw}=T/E^u$ (因为仿真器知道 u 的值)。如果验证通过，则判定攻击者成功，否则终止协议。攻击者除非猜对了口令的值，才能通过验证。

$$|\mathrm{pr}[S_5]-\mathrm{pr}[S_4]| \leqslant q_\mathrm{s}/N$$

实验 Γ_6：Γ_6 与 Γ_5 的区别是当攻击者进行 Send($*,null$)查询时，用随机数 r 替代消息 B。

为了使攻击者的视角保持一致性，需要处理其他的预言机查询。Send($client|A|B$) 和 Send($client|ak_c$)查询保持不变。由于此时消息 $A|B$ 不存在让协议正常执行的 x，Send($server|D|E|T$)查询修改如下。

1) 如果查询消息是预言机产生的，仿真器不进行验证，用 Send($client|A|B$)查询中的 σ 计算 $ak_c=F_\sigma(1)$，然后输出 ak_c 并计算 $sk=F_\sigma(2)$。当 B 为随机数时，如果消息 $A|B$ 是 g^{pw} 的 ElGamal 加密(极小概率)，2 个匹配预言机计算的 σ 值是相等的。仿真器的仿真实验是完美的。

2) 如果查询消息是攻击者产生的，仿真器按实验 Γ_5 给出响应。如果攻击者有一定的优势获得会话密钥，则可以利用混合证明技巧，直接归约为解决 DDH 问题。

$$|\mathrm{pr}[S_6]-\mathrm{pr}[S_5]| \leqslant q_\mathrm{s}Adv_{g,G}^{\mathrm{ddh}}$$

实验 Γ_7：当攻击者进行 Send($client|A|B$)查询时，如果 $B=A^ug^{pw}$ (仿真器知道 u)，则判定攻击者成功，并终止协议。

由于攻击者之前通过 Execute 查询和 Send 查询得到的消息 $A|B$ 不是 g^{pw} 的 ElGamal 加密(B 是随机数)。攻击者成功是因为猜对了口令的值，可得：

$$|\mathrm{pr}[S_7]-\mathrm{pr}[S_6]|\leqslant q_s/N$$

实验 Γ_8： Γ_8 与 Γ_7 的区别是，当攻击者进行 Send($client|A|B$)查询时， σ 替换为随机数 r 。

在 Γ_8 中，说明攻击者没有在 Send($client|A|B$) 查询时成功(否则攻击者已经在 Γ_7 中成功，协议已终止)。这时，消息 $A|B$ 不是 g^{pw} 的 ElGamal 加密。与实验 Γ_2 的分析类似， σ 是随机均匀分布的。则，

$$\mathrm{pr}[S_8]=\mathrm{pr}[S_7]$$

实验 Γ_9：Γ_9 与 Γ_8 的区别在于攻击者进行 Send 查询时， ak_c,r 替换为不同的随机数。

由于消息 $A|B$ 不是 g^{pw} 的 ElGamal 加密， σ 是随机均匀分布的。利用伪随机函数的定义，运用混合证明技巧，可得：

$$|\mathrm{pr}[S_9]-\mathrm{pr}[S_8]|\leqslant q_s Adv^F$$

实验 Γ_{10}：攻击者进行 Send 查询时， sk 替换为随机数。

与实验 Γ_9 中的分析类似，得出 σ 是随机均匀的。如果攻击者不进行 Reveal 查询，则在 Γ_{10} 和 Γ_9 中获得的信息是相同的。所以，

$$|\mathrm{pr}[S_{10}]-\mathrm{pr}[S_9]|\leqslant \min(q_s,q_r)Adv^F$$

实验 Γ_{11}： Γ_{11} 与 Γ_{10} 的区别在于攻击者进行 Send($client|A|B$)查询时，消息 T 替换为随机数。基于 DDH 假设，运用混合证明技巧，可得：

$$|\mathrm{pr}[S_{11}]-\mathrm{pr}[S_{10}]|\leqslant q_s Adv^{\mathrm{ddh}}_{g,G}$$

在 Γ_{11} 中，由于攻击者无法获得关于 pw 的任何信息(与 pw 相关的信息 B,T 替换为随机数后，攻击者感觉不到任何变化)，从而无法获得 σ 的任何信息，说明在 Test 查询中，攻击者无法区分 sk 和随机数。

$$\mathrm{pr}[S_{11}]=1/2$$

综合以上实验中的结果，可以得出定理 1。

定理 1 表明，攻击者成功的概率依赖于它每次进行 Send 查询时对口令的猜测，而与 Execute 查询和 Reveal 查询无关。如果攻击者某个时刻通过 Corrupt 查询获得了长期私钥(双方共享的口令)，它通过以前被动窃听的会话信息得到许多三元对 (g^x,h^x,D)，攻击者无法计算 D^x ，其困难等价于 CDH 问题。攻击者无法获得 σ 的任何信息，说明协议具备完美前向安全。

6　协议的性能分析

本节给出新协议与其他标准模型下的协议比较（见表 1），新协议能抵御主动攻击，且计算复杂度较小(新协议直接计算 g^{pw}，而不是 $g^{f(pw)}$，由于 pw 较短，可以忽略以 pw 为指数的运算)。在通信效率方面，3 种协议都要进行 3 轮通信而实现显式双向认证，并且新协议与其他 2 种协议占用的带宽相同。

表 1　　新协议与其他协议的比较

协议	文献[14]	文献[15]	新协议
通信轮数	3	3	3
生成元	2	2	2
指数运算	18	11	11
拥有私钥	无	有	无
抵御攻击	主动攻击	被动攻击	主动攻击

7　结束语

本文基于 ElGamal 加密机制和伪随机函数集，在标准模型下设计了可证安全的基于口令密钥协商协议。与其他标准模型下基于口令的认证协议相比，新协议的通信效率与其他协议相当，并具有较小的计算复杂度。新协议实现了显式双向认证，并基于 DDH 假设，给出了协议的“紧规约”证明，从而真正证明了协议的安全性。

参考文献：

[1] BELLOVIN S, MERRITT M. Encrypted key exchange: password-based protocol secure against dictionary attacks[A]. Proceedings of the 1992 Conference IEEE Computer Society Symp on Research in Security and Privacy[C]. Oakland: IEEE Computer Society, 1992. 72-84.

[2] BELLOVIN S, MERRITT M. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise[A]. Proceedings of the 1st ACM Conference on Computer and Communication Security[C]. New York, 1993.244-250.

[3] JABLON D P. Extended password key exchange protocols immune to dictionary attacks[A]. Proceedings of the WETICE'97 Workshop on Enterprise Security[C]. Cambridge: IEEE Computer Society, 1997. 248-255.

[4] WU T D. The secure remote password protocol[A]. Proceedings of the Network and Distributed System Security Symp NDSS 1998[C]. San

Diego, Internet Society, 1998.232-245.

[5] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[A]. Proceedings of the Advance Eurocrypt 2000[C]. Berlin: Springer-Verlag, 2000.139-155.

[6] ABDALLA M, CHEVASSUT O, POINTCHEVAL D. One-time verifier-based encrypted key exchange[A]. Proceedings of Public Key Cryptography-PKC 2005[C]. Berlin: Springer-Verlag, 2005.47-64.

[7] ABDALLA M, POINTCHEVAL D. Simple password-based encrypted key exchange protocols[A]. Proceedings of CT-RSA 2005[C]. Berlin: Springer-Verlag, 2005.191-208.

[8] FENG D G, XU J. A new client-to-client password-authenticated key agreement protocol[A]. Proceedings of IWCC 2009[C]. Berlin: Springer-Verlag, 2009.63-76.

[9] HUANG H F. A simple three-party password-based key exchange protocol[J]. Int J Commun Syst, 2009, 22(4): 857-862.

[10] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[A]. Proceedings of the First ACM Conference on Computer and Communication Security[C]. New York, 1993.62-73.

[11] CRAMER R, SHOUP V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[A]. Proceedings of the Advance in Cryptology-CRYPTO 1998[C]. Berlin: Springer-Verlag, 1998. 13-25.

[12] KATZ J, OSTROVSKY R, YUNG M. Efficient password- authentication key exchange using human-memorable passwords[A]. Proceedings of the Advances in Cryptology-EUROCRYPT 2001[C]. Berlin: Springer-Verlag, 2001.475-494.

[13] GENNARO R, LINDELL Y. A framework for password-based authenticated key exchange[A]. Proceedings of the Advances in Cryptology-EUROCRYPT 2003[C]. Berlin: Springer-Verlag, 2003.524-543.

[14] JIANG S Q, GONG G. Password based key exchange with mutual authentication[A]. Proceedings of Cryptography-SAC 2004[C]. Berlin: Springer-Verlag, 2004.267-279.

[15] 殷胤, 李宝. 标准模型下可证安全的加密密钥协商协议[J]. 软件学报, 2007, 18(2): 422-429.
YIN Y, LI B. Provable secure encrypted key exchange protocol under standard model[J]. Journal of Software, 2007, 18(2): 422-429.

作者简介：

舒剑（1972-），男，江西南昌人，电子科技大学博士生，主要研究方向为密码学与信息安全。

许春香（1965-），女，湖南宁乡人，博士，电子科技大学教授、博士生导师，主要研究方向为密码学与信息安全。