标准模型下高效的基于口令认证密钥协商协议

舒　剑[①②]　　许春香[①]
[①](电子科技大学计算机科学与工程学院　成都　610054)
[②](江西财经大学电子商务系　南昌　330013)

摘　要：基于口令的认证密钥协商协议是利用预先共享的口令协商安全性较高的密钥。现有的基于口令认证密钥协商协议大多需要较大的计算量，或者只在随机预言模型下证明了协议的安全性。该文提出了新的标准模型下基于口令密钥协商协议，协议只需要一个生成元。 与其它标准模型下的协议相比，新协议不需要 CPA 或 CCA2 安全的加密方案，因而具有计算复杂度低和协议描述简单的特点。相对于殷胤等人在“标准模型下可证安全的加密密钥协商协议”一文中提出的协议，新协议将指数运算降低了 64%。最后，基于 DDH 假设，在标准模型下证明了协议的安全性。

关键词：身份认证；基于口令；标准模型；可证安全
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)11-2716-04

Efficient Password-Based Authenticated Key Exchange Protocol under Standard Model

Shu Jian[①②]　　Xun Chun-xiang[①]
[①](*School of Computer Science and Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)
[②](*Department of Electronic Commercial*, *University of Jiangxi Financial Economics*, *Nanchan* 330013, *China*)

Abstract: The goal of password-based authenticated exchange protocol is established secure key by using pre-shared human-memorable password. Most of existing schemes either have computation burden or rely on the random oracle model. A new scheme without random oracles is proposed, which requires only one generator. Due to not using CPA or CCA2 public encryption scheme, the proposed protocol is efficient in computational cost and simple in protocol description when compared other solutions without random oracles. Specifically, this protocol reduces 64% of the exponential computations of the protocol proposed by Yin Yin *et al.* in the paper of “Provable secure encrypted key exchange protocol under standard model”. The security of the proposed scheme has been proven in the standard model under DDH assumption.

Key words: Authentication; Password-based; Standard model; Provably secure

1　引言

基于口令的密钥认证协议让用户共享一个低熵的口令而生成高熵的会话密钥。由于口令通常长度较短并便于记忆，因而完成协议所需的计算量较小。但由于口令的固有特性(长度短，随机性较差)，该类协议容易受到离线字典攻击。

Bellovin 和 Merritt[1]首先提出能抵抗字典攻击的基于口令密钥协商协议，随后许多相关工作[2–6]对如何利用口令生成会话密钥进行了研究。Bellare 等[2]提出了基于口令密钥协商的一种理论模型，本文的协议安全证明也采用了这种模型。Shao 等[5]提出了无需公共信息的基于口令认证协议。Feng 等[6]给出了设计、分析基于口令认证协议的通用框架和标准方法。文献[1–6]都是在随机预言模型下证明其安全性的。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。

Katz 等[7]首先提出了标准模型下可证安全的基于口令认证密钥协商协议。但协议计算复杂度很高，并且协议只能实现单向认证。Jiang 和 Gong[8]提出了一种改进的基于口令认证密钥协商协议。协议的发起方使用 ElGamal 加密，协议的响应方使用 CCA2 安全的公钥加密，该协议降低了计算复杂度并实现了双向认证。通过引入伪随机函数集和通信双方均使用 ElGamal 加密机制，殷胤等[9]提出了高

2008-11-25 收到，2009-04-21 改回
国家“863”计划项目(2009AA012415)资助课题

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，但要求服务器方拥有私钥。

本文提出一种新的基于口令认证密钥协商协议。协议只需要一个生成元，与其它标准模型下的协议相比，计算机复杂度最低。新协议不需要响应方拥有私钥且实现了双向认证。

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 $g^x,g^y\mathrm{Adv}_{g,G}^{\mathrm{ddh}}(D)=|\ \mathrm{pr}[D(g,g^x,g^y,g^{xy})=1]-\mathrm{pr}[D(g,g^x,g^y,r)=1]|<\varepsilon(n)$。其中 $\varepsilon(\cdot)$ 是可忽略函数。

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 $\mathrm{Adv}^F(M)=|\ \mathrm{pr}[M^{F_n}(1^n)=1]-\mathrm{pr}[M^{H_n}(1^n)=1]|<\varepsilon(n)$。其中 $\varepsilon(\cdot)$ 是可忽略函数；$H=\{H_n\}_{n\in N}$ 是一个均匀分布的函数集。

2.3 形式化安全模型

本节简要回顾 Bellare 等学者在文献[2]中定义的基于口令密钥协商协议的形式化安全模型。这一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。$\Pi_{u_i}^j$ 表示组成员 u_i 的第 j 个实例。

定义 1　会话标识符(SID)：实例 $\Pi_{u_i}^j$ 发送和接收的所有消息的串联。

定义 2　搭档实例(PID)：若两个实例在同意(accept)状态时有相同的会话标识符 SID，则称两个实例互为搭档。

模型中还包括一个主动攻击者(用 A 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。

Execute 查询：这种查询模拟被动攻击，攻击者 A 通过查询 execute($\Pi_{u_i}^j$)获得实例 $\Pi_{u_i}^j$ 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 向实例 $\Pi_{u_i}^j$ 发送伪造消息，若实例收到的消息为空，表示攻击者让实例发起一个新的会话。查询返回消息为接收到假冒消息后，实例按照协议规则的回复。

Reveal 查询：这种查询模拟实例 $\Pi_{u_i}^j$ 的会话密钥泄漏，返回值为 sk_i，如果实例的状态还不是“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。要求被询问的实例返回它拥有的长期私钥(口令)。回答过 corrupt 查询的实例的状态称为“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”的实例进行。当攻击者 A 进行 Test 查询时，实例随机选择一个比特 $b\in\{0,1\}$，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'。定义攻击者 A 成功的概率为 $\mathrm{Adv}_{g,G}^{\mathrm{pake}}=2\mathrm{pr}[b'=b]-1$。

定义 3　新鲜实例：实例 $\Pi_{u_i}^j$ 在同意(accepted)状态下是未打开的，其搭档也未打开，并且其搭档没有被腐化，则实例 $\Pi_{u_i}^j$ 是新鲜的。

3　新的基于口令认证密钥协商协议

本文提出一种高效的标准模型下基于口令认证密钥协商协议，协议描述如图 1 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 是 G_q 的生成元；F 是 $\{0,1\}^{l(n)}\to\{0,1\}^n$ 的伪随机函数集；f 是从口令空间到 G_q 的映射；pw 是客户和服务器共享的口令。

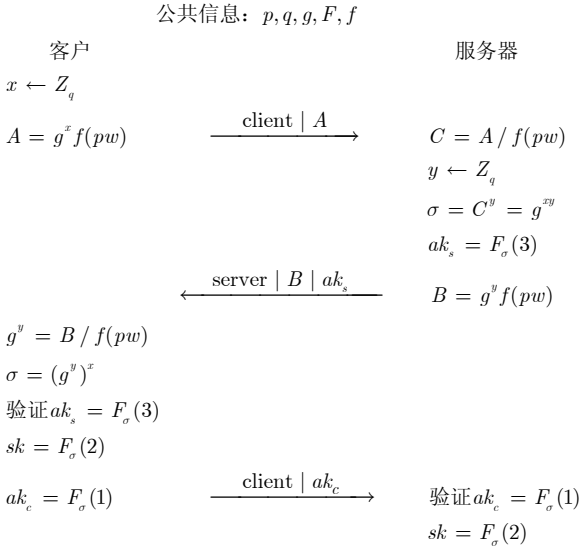

图 1　标准模型下高效的基于口令密钥协商协议

4　协议的安全性证明

证明的思想是设计一系列的实验($\Gamma_0,\Gamma_1,\cdots$)，在所有的实验中，预言机按协议的描述回答攻击者的查询。其中实验 Γ_0 模拟的是攻击者攻击实际协议。而以后的实验中逐步修改预言机的回答方式，使攻击者在两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_τ 中成功的概率。

定理 1　Γ 是图 1 描述的协议；参数如前所述；

N 表示所有可能的口令；q_e, q_s, q_r 分别表示攻击者进行 Execute 查询，Send 查询，Reveal 查询的次数。则

$$\mathrm{Adv}_{\Gamma,A}^{\mathrm{pake}} \le 4q_s / N + 2(q_e + 2q_s)\mathrm{Adv}_{g,G}^{\mathrm{ddh}} + 2(q_e + q_s)/q$$
$$+2(q_e+q_s)\mathrm{Adv}^F + q_s / 2^{n-1} + 2\min(q_e+q_s, q_r)\mathrm{Adv}^F$$

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

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

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 A。由于消息 A 本身是由一个随机数乘 $f(pw)$，攻击者感觉不到任何变化。则

$$\mathrm{pr}[S_1] = \mathrm{pr}[S_0] \tag{2}$$

实验 Γ_2：Γ_2 与 Γ_1 的区别在于攻击者对消息 B 进行 Execute 查询时，用随机数 r 替代消息 B。同实验 Γ_1 类似，可得

$$\mathrm{pr}[S_2] = \mathrm{pr}[S_1] \tag{3}$$

实验 Γ_3：在实验 Γ_3 中，攻击者进行 Execute 查询时，用随机数 r 替代消息 σ。攻击者得到信息 A, B 后，通过猜测 pw 的值，可在离线方式下得到不同的 (g^x, g^y) 对。由于 DDH 的难解性，它还是无法区分 g^{xy} 和 r。运用混合证明(hybrid arguments)技巧，可得

$$|\mathrm{pr}[S_3] - \mathrm{pr}[S_2]| \le q_e \cdot \mathrm{Adv}_{g,G}^{\mathrm{ddh}} \tag{4}$$

实验 Γ_4：Γ_4 与 Γ_3 的区别是，当攻击者进行 Execute 查询时，ak_s, ak_c 替换为随机数。

在实验 Γ_3 中，攻击者无法区分 σ 和随机数，如果攻击者可以区分 ak_s, ak_c 和随机数，则表示攻击者可以有效区分伪随机函数集和均匀分布函数集，运用混合证明技巧，可得

$$|\mathrm{pr}[S_4] - \mathrm{pr}[S_3]| \le q_e \cdot \mathrm{Adv}^F \tag{5}$$

实验 Γ_5：现在开始考虑主动攻击。Γ_5 与 Γ_4 的区别是，攻击者构造消息 A，用来进行 Send(client | A)查询。

攻击者有以下 3 种攻击方式：

(1)攻击者选择一个数 $x \in Z_q$，并猜测口令的值为 pw_c，产生消息 $A = g^x f(pw_c)$ 进行 Send 查询。攻击者成功的概率为 $q_s \cdot \mathrm{Adv}_{g,G}^{\mathrm{ddh}}$。

证明 如果攻击者 A_1 成功，则可构造一个算法 π 以相同的概率解决 DDH 问题。构造过程如下：π 收到一个 3 元组 $d = (d_1, d_2, d_3) = (g^{x_1}, g^{x_2}, g^{x_3})$，映射函数定义为 $f(pw) = d_2^{pw}$，它选择一个随机数 $r \in Z_q^*$，把 r，pw_c，f，$A = g^r (d_2)^{pw_c}$ 和 $B = d_1 (d_2)^{pw}$ 给 A_1。如果攻击者 A_1 成功，表明攻击者可以计算出 $\sigma_c = (g^r (d_2)^{pw_c - pw})^{x_1}$。$\pi$ 计算 $\sigma_s = d_1^r (d_3)^{pw_c - pw}$，如 $\sigma_c = \sigma_s$，则 π 输出 $g^{x_3} = g^{x_1 \cdot x_2}$。否则输出 $g^{x_3} \ne g^{x_1 \cdot x_2}$。

(2)重放消息。与实验 Γ_3 的证明方法类似，攻击者成功的概率为 $q_s \cdot \mathrm{Adv}_{g,G}^{\mathrm{ddh}}$。

(3)攻击者猜中口令 pw。由于在 Γ_5 中，攻击者得到的消息都与 pw 无关，所以在本次 Send 查询中，攻击者猜中 pw 的概率为 q_s / N。

$$|\mathrm{pr}[S_5] - \mathrm{pr}[S_4]| \le q_s / N + 2q_s \cdot \mathrm{Adv}_{g,G}^{\mathrm{ddh}} \tag{6}$$

实验 Γ_6：Γ_6 与 Γ_5 的区别是，当攻击者进行 Send(server | B | ak_s)查询时，按协议描述验证 ak_s 的正确性，如果验证通过，则判定攻击者成功，并终止协议。

这时攻击成功有以下 3 种方法：

(1)攻击者重放信息 server | B | ak_s。要通过验证，必须与信息 client | A 相匹配，这时攻击者成功的概率为 $(q_e + q_s)/q$。

(2)攻击者要通过验证，必须计算 σ 的值，即攻击者要选取 y 的值，除非是猜对了 pw 的值，才能得到 g^x，并求出 $\sigma = g^{xy}$，进而得到有效信息 B | ak_s。攻击者成功的概率为对 pw 的猜测，即为 q_s / N。

(3)攻击者在不知道 σ 的情况下，成功地算出 $ak_s = F_\sigma(3)$ 的值。与实验 Γ_4 的证明方法类似，攻击者成功的概率为 $q_s \cdot \mathrm{Adv}^F$。

$$|\mathrm{pr}[S_6] - \mathrm{pr}[S_5]| \le q_s / N + (q_e + q_s)/q + q_s \cdot \mathrm{Adv}^F \tag{7}$$

实验 Γ_7：Γ_7 与 Γ_6 的区别是，当攻击者进行 Send(client | ak_c)查询时，按协议描述验证 ak_c 的正确性，如果验证通过，则判定攻击者成功，并终止协议。

如果攻击者在 Γ_6 中没有成功，则所有的消息都一定是由 client 和 server 产生的，并且没有泄露任何关于 x, y 的信息，攻击者得不到任何关于 g^{xy} 的信息。由于 F 是一个 $\{0,1\}^{l(n)} \to \{0,1\}^n$ 的伪随机函数集，则攻击者猜中 $F_\sigma(1)$ 的概率为 $1/2^n$，所以

$$|\mathrm{pr}[S_7] - \mathrm{pr}[S_6]| \le q_s / 2^n \tag{8}$$

实验 Γ_8：Γ_8 与 Γ_7 的区别是，当攻击者进行 Reveal 查询时，sk 替换为随机数 r。

攻击者进行 Execute 和 Send 查询后，不进行 Reveal 查询。则攻击者在 Γ_8 和 Γ_7 中获得相同信息。在 Γ_7 中，攻击者得不到任何关于 g^{xy} 的信息。则没有算法可以有效区分伪随机函数集和随机数。运用混合证明技巧可得

$$|\mathrm{pr}[S_8] - \mathrm{pr}[S_7]| \le \min\{(q_e + q_s), q_r\} \cdot \mathrm{Adv}^F \tag{9}$$

在 Γ_8 中，由于攻击者无法获得关于 pw 的任何信息，从而无法获得 g^{xy} 的信息，除非攻击者在这之

前对实例或其搭档进行过 reveal 查询，而这是定义 3 不允许的。因此在 Test 查询中，攻击者无法区分 sk 和随机数。

$$\mathrm{pr}[S_8]=1/2 \tag{10}$$

综合以上实验中的结果式(1)–式(10)，可以得出定理 1。　　证毕

定理 1 表明基于 DDH 假设，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。即新协议可以抵御被动攻击(离线字典攻击)、主动攻击(攻击者伪装成客户或服务器以及中间人攻击)并具备已知密钥安全(某个会话密钥的泄露不会影响其它会话密钥的安全性)。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)，则它通过以前被动窃听的会话信息得到许多二元对(g^x, g^y)。但攻击者仍无法计算 $\sigma = g^{xy}$，其困难等价于 CDH 问题，说明协议具备完美前向安全。

5　协议的性能分析

本节给出新协议与其它标准模型下协议的性能比较。如表 1 所示，新协议实现了双向认证，并能抵抗主动攻击，而且计算复杂度最小。

表 1　与其它协议的比较

协议	文献[7]	文献[8]	文献[9]	本文协议
生成元	5	2	2	1
指数运算	30	18	11	4
认证	单向认证	双向认证	双向认证	双向认证
拥有私钥	无	无	有	无

6　结论

基于口令的认证密钥协商协议在实际环境中有广泛的应用。大多数解决方案在随机预言机模型下给出了安全性证明，现有的标准模型下的解决方案计算复杂度较高。本文利用伪随机函数集，在标准模型下设计了可证安全的基于口令认证密钥协商协议。新协议只需要一个生成元，具有协议描述简单，计算量小等特点。最后，基于 DDH 假设，给出了协议的安全证明。

参 考 文 献

[1] Bellovin S and Merritt M. Encrypted key exchange: password-based protocol secure against dictionary attacks[C]. Proceedings of the 1992 Conference IEEE computer society symp. on Research in security and privacy, Oakland, USA, 1992: 72–84.

[2] Bellare M, Pointcheval D, and Rogaway P. Authenticated key exchange secure against dictionary attacks[C]. Proceedings of EUROCRYPT 2000, Bruges, Belgium, LNCS 1807: 139–155.

[3] Abdalla M, Chevassut O, and Pointcheval D. One-time verifier-based encrypted key exchange[C]. Proceedings of PKC 2005, Les Diablerets, Switzerland, LNCS 3386: 47–64.

[4] Abdalla M and Pointcheval D. Simple password-based encrypted key exchange protocols[C]. Proceedings of CT-RSA 2005, San Francisco, USA, LNCS 3376: 191–208.

[5] Shao Jun, Cao Zhen fu, and Wang Li cheng. Efficient password-based authenticated key exchange without Public information[C]. Proceedings of ESORICS 2007, Dresden, Germany, LNCS 4734: 299–310.

[6] Feng Deng guo and Chen Wei dong. Modular approach to the design and analysis of password-based security protocols[J]. *Science in China Series F*, 2007, 50(3): 381–398.

[7] Katz J, Ostrovsky R, and Yung M. Efficient password-authentication key exchange using human-memorable passwords[C]. Proceedings of EUROCRYPT 2001, Innsbruck, Austria, LNCS 2045: 475–494.

[8] Jiang S Q and Gong G. Password based key exchange with mutual authentication[C]. Proceedings of SAC 2004, Nicosia, Cyprus, LNCS 3357: 267–279.

[9] 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 Yin and Li Bao. Provable secure encrypted key exchange protocol under standard model[J]. *Journal of Software*, 2007, 18(2): 422–429.

舒　剑：　男，1972 年生，博士生，研究方向为密码学与信息安全.

许春香：　女，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.