ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.2, February 2007, pp.422−429
DOI: 10.1360/jos180422

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

标准模型下可证安全的加密密钥协商协议*

殷 胤, 李 宝+

(信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

Provable Secure Encrypted Key Exchange Protocol Under Standard Model

YIN Yin, LI Bao+

(State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88258713, E-mail: lb@is.ac.cn, http://www.lois.cn

Yin Y, Li B. Provable secure encrypted key exchange protocol under standard model. *Journal of Software*, 2007,18(2):422−429. http://www.jos.org.cn/1000-9825/18/422.htm

Abstract: Encrypted key exchange protocol's goal is to establish a high secure key used for further encryption and authentication through a low secure password. Most existing encrypted key exchange protocols either lack security proofs or rely on the Random Oracle model. Compared with those protocols based on the Random Oracle model, provable secure EKE (encrypted key exchange) protocols have heavier computation burden and their descriptions are more complex, although they don't need the Random Oracle model. Through introducing server's public key and applying ElGamal encryption scheme and pseudorandom function ensemble, a provable secure encrypted key exchange protocol is designed from the protocol proposed by David P. Jablon in the paper of "Extended Password Key Exchange Protocols Immune to Dictionary Attacks", and a proof is presented. Compared with the original protocol, this protocol only needs DDH (decisional Diffie-Hellman) assumption but not ideal encryption and Random Oracle model. Compared with other provable secure encrypted key exchange protocols, because this protocol doesn't need CCA2 (chosen ciphertext attack-2) secure public encryption scheme, it can reduce the number of exponible computations and greatly simplify the protocol's description. Specifically, this protocol reduces 73% of the exponential computations of KOY protocol, and reduces 55% of the exponential computations of the protocol proposed by Jiang Shao-Quan et al. in the paper of "Password Based Key Exchange with Mutual Authentication".

Key words: encrypted key exchange; provable security; password; standard model

摘 要: 密钥加密协议的目的是利用安全性低的口令协商安全性高的密钥,进而利用密钥对以后的通信进行加密或身份认证,从而实现安全通信.现有的密钥加密协议大多缺乏安全证明,或者仅在 Random Oracle 模型下证明了协议的安全性.与 Random Oracle 模型下的协议相比,标准模型下可证安全的 EKE(encrypted key exchange)协议虽然不需要 Random Oracle 假设,但它们都对参与方的计算能力要求较高,协议规则也更为复杂.从 David P. Jablon 在"Extended Password Key Exchange Protocols Immune to Dictionary Attacks"一文中提出的协议出发,通

* Supported by the National Natural Science Foundation of China under Grant No.90304013 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z427 (国家高技术研究发展计划(863))

Received 2005-12-10; Accepted 2006-02-23

过引入服务端的公钥,并利用 ElGamal 加密和伪随机函数集,将一个 Random Oracle 模型下可证安全的 EKE 协议改进为一个标准模型下可证安全的 EKE 协议,并证明了改进后的协议仍然是安全的.与原始协议相比,改进后的协议只需要 DDH(decisional Diffie-Hellman)假设,而不需要理想加密和 Random Oracle 假设;与其他标准模型下可证安全的协议相比,改进后的协议不需要 CCA2(chosen ciphertext attack-2)安全的加密方案,从而不仅可以减少指数计算的次数,而且具有协议规则简单的优点.相对于 KOY 协议,改进后的协议将指数运算次数降低了 73%;相对于 Jiang Shao-Quan 等人在"Password Based Key Exchange with Mutual Authentication"一文中提出的协议,改进后的协议将指数运算次数降低了 55%.

关键词: 加密密钥协商;可证安全;口令;标准模型
中图法分类号: TP309 文献标识码: A

密钥协商协议的目的是在通信双方之间通过交互,建立一个共同的密钥,从而实现安全通信.一般地,研究者们都假设通信双方已经共享了一个公共的长期密钥,然后利用长期密钥生成一个短期会话密钥.在接下来的通信中,仅使用短期会话密钥进行加密或认证.但是,这些长期密钥既不便于保存,也不便于记忆.在现实情况下,人们总是倾向于记忆或使用那些安全程度较低的密钥.口令就是一种被广泛应用的低安全的密钥,它们通常长度较短,随机性较差,但却便于记忆和使用.同时应注意到,由于口令本身的弱点,如果对口令使用不当,攻击者可能发起穷举字典攻击.

为了研究如何安全地利用口令进行密钥协商,并避免穷举字典攻击,研究者们提出了加密密钥协商协议(encrypted key exchange,简称 EKE)的概念,又称为基于口令的密钥协商协议.EKE 协议最早是由 Bellovin 和 Merritt 在文献[1]中提出来的,后来,Bellovin 和其他一些研究者按照这种思路对文献[1]中的协议进行改进,并提出了一些新的 EKE 协议,如文献[2–5].2000 年,Mihir Bellare 等人在文献[6]中利用语义安全[7]的思想,提出了一种 EKE 协议的理论模型.本文使用这种理论模型来证明协议的安全性;同时,Victor Boyko 等人在文献[8]中则利用多方安全计算的思想,提出了另一种 EKE 协议的理论模型.这两种模型有各自的优点和不足.利用理论模型,研究者们提出了一系列可证安全的 EKE 协议,如文献[9–13].但除了文献[12,13]以外,其他协议都是在 Random Oracle 模型[14]下证明其安全性的.正如 Canetti 等人在文献[15]中所指出的那样:在 Random Oracle 模型下证明安全的协议,当用 Hash 函数或伪随机函数集代替 Random Oracle 时,不一定能保证协议仍然是安全的.所以,如何不利用 Random Oracle 模型而设计出可证安全的 EKE 协议非常重要,但现在这方面的研究还很少.

自从认识到 Random Oracle 模型的局限性以来,研究者们一直试图设计标准模型下(即不使用 Random Oralce)可证安全的 EKE 协议.第一个标准模型下可证安全的 EKE 协议是由 Katz,Ostrovsky 和 Yung 在 2001 年提出的 KOY 协议[13].他们的协议高度依赖于 CCA2(chosen ciphertext attack-2)安全的 Cramer-Shoup 公钥加密体制[16].Cramer-Shoup 公钥加密体制是一种计算复杂度很高的加密体制,它每加密一个明文需要进行 5 次指数运算,因此导致 KOY 协议的计算复杂度很高.

为了降低计算复杂性,Jiang 和 Gong 于 2004 年提出了一种新的 EKE 协议[12].协议发起方使用 ElGamal 加密,协议的另一方则仍然使用 Cramer-Shoup 加密(文献[12]中只提到使用一个 CCA2 安全的公钥加密,并没有指定具体使用什么加密方案.在表 1 中,我们假定使用 Cramer-Shoup 加密).由于 ElGamer 公钥加密体制每加密一个明文只需要 2 次指数运算,比 Cramer-Shoup 公钥加密体制少 3 次运算,因此降低了 KOY 协议的计算复杂度.

Table 1 Comparison with other protocols

表 **1** 与其他协议的比较

	KOY protocol[13]	Jiang's protocol[12]	New protocol
Number of exponential computations	30	18	11
Rounds of communication	3	3	3
Authentication	Unilateral authentication	Mutual authentication	Mutual authentication

利用 Cramer-Shoup 加密体制的 CCA2 的安全特性,协议可以在协商密钥的同时进行身份认证.但如果将密钥协商和身份认证分开考虑,我们可以仅使用 CPA(chosen plaintext attack)安全的 ElGamal 加密体制设计 EKE

协议.而在协议最后,通过增加 1 轮通信专门实现认证.新协议虽然极大地降低了计算复杂度,但是与 KOY 协议和 Jiang 的协议相比,需要服务器拥有公钥.

表 1 是 KOY 协议、Jiang 的协议和新协议的比较.由于 pw 很短,在计算指数运算次数时,没有考虑以 pw 作为指数的指数运算.从表 1 中可以看出,新协议分别将计算复杂度降低了 73%和 55%.另外,除了指数运算以外,KOY 协议还需要 4 次 Hash 计算和一次签名运算,Jiang 的协议需要 2 次 Hash 计算和 5 次伪随机函数集计算,而新协议只需要 2 次伪随机函数集计算.

1 背景知识

1.1 可忽略的函数

称函数 $\varepsilon(\cdot)$是一个可忽略的函数,如果对于任意多项式时间内可计算的函数 $p(\cdot)$,都存在 $N\in$N,使得任意 $n>N$ 满足$\varepsilon(n)<1/p(n)$.

1.2 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,如果对于任何 $x,y\in Z_q$,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),其中,r 是一个随机数,即

$$Adv_{g,G}^{ddh}(D)=|\Pr[D(1^n,g,g^x,g^y,g^{xy})=1]-\Pr[D(1^n,g,g^x,g^y,r)=1]|<\varepsilon(n),$$

其中:$\varepsilon(\cdot)$是一个可忽略的函数; $Adv_{g,G}^{ddh}=\max_D(Adv_{g,G}^{ddh}(D))$ 表示对所有攻击者 D,$Adv_{g,G}^{ddh}(D)$ 可能取到的最大值.

1.3 伪随机函数集

称一个函数集 $F=\{F_n\}_{n\in N}$ 是伪随机的,如果对于每个概率多项式 Oracle M 和所有足够大的 n,满足

$$Adv^F(M)=|\Pr[M^{F_n}(1^n)=1]-\Pr[M^{H_n}(1^n)=1]|<\varepsilon(n),$$

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;$Adv^F=\max_M\{Adv^F(M)\}$表示对所有的 Oracle M,$Adv^F(M)$可能取到的最大值.

2 协议描述

Bellare 在文献[6]中利用理想加密和 Random Oracle 提出了一种可证安全的 EKE 协议.从这个协议出发,将理想加密用一般的抵抗选择明文攻击的 ElGamal 加密代替,而将 Random Oracle 用伪随机函数集代替,得到一种新的标准模型下的 EKE 协议.进一步地,我们证明了这个协议仍然是安全的.

如图 1 所示为协议的描述.两个参与方 Client 和 Server 通过 EKE 协议协商公共密钥,p,q,g,h,F,f 是公开的公共参数,其中:p,q,g 满足 DDH 假设中的要求;而 h 是 Server 的 ElGamal 加密公钥;u 是相应的私钥;F 是一个伪随机函数集;f 是一个从口令空间到 Z_p 的映射;pw 是 Client 和 Server 共享的口令.

3 协议的安全性

利用文献[6]中的理论模型证明上述协议是安全的,其具体描述请参见原文.模型允许协议的多个实例并发执行,而攻击者只需获取其中任何一个实例的会话密钥.模型将攻击者的能力抽象为对若干个 Oracle 的查询.

Execute 查询:这种查询模拟被动攻击.攻击者 A 通过查询 $Execute(i)$获得协议实例 i 的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.$Send(i,0,Client,\text{null})$查询表示攻击者让 Client 发起一个新的实例 i; $Send(i,1,Server,Client|A_i|B_i)$假冒 Client 向 Server 发送消息$(Client|A_i|B_i)$;$Send(i,2,Client,Server|C_i|D_i|ak_{i,s})$查询假冒 Server 向 Client 发送消息;$Send(i,3,Server,ak_{i,c})$查询假冒 Client 向 Server 发送消息 $ak_{i,c}$.查询返回消息为接收到假冒消息后,参与方的回复.

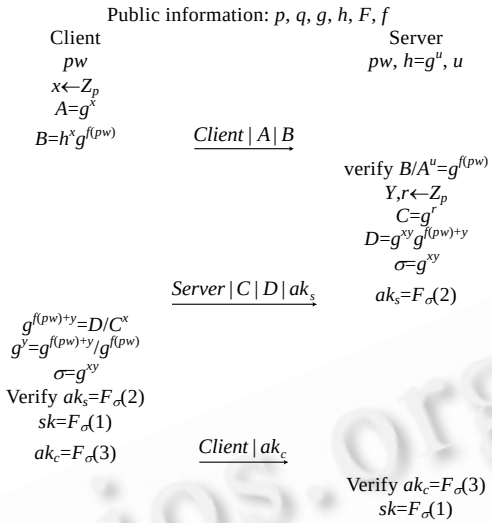

Fig.1 Provable secure EKE protocol under standard model

图 1 标准模型下可证安全的 EKE 协议

Reveal 查询:这种查询模拟某个实例 i 中会话密钥的泄漏.返回值是 sk_i.

Test 查询:这种查询刻画协议的安全性.它只能运行一次,且只能对一个没有进行过 Reveal 查询的协议实例 i 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 Pr[S].

$$\Pr[S]=\Pr[b'=b],\ Adv^{eke}_{g,h,G,F}(A)=2\Pr[S]-1.$$

定义 $Adv^{eke}_{g,h,G,F}$ 为所有攻击者 A 可能取到的 $Adv^{eke}_{g,h,G,F}(A)$ 的最大值.称协议是安全的,如果

$$Adv^{eke}_{g,h,G,F}<O(q_s/N)+\varepsilon.$$

其中:q_s 表示 Send 查询的次数;N 表示所有口令的总数;ε是一个可忽略的函数;$O(q_s/N)$保证每次 Send 查询,攻击者 A 最多排除常数个可能的口令.

定理 **1**. Γ是一个如图 1 所描述的协议;F 是一个$\{0,1\}^n\leftarrow\{0,1\}^{l(n)}$的伪随机函数集,其中 n 是安全参数;$l(\cdot)$是一个多项式时间内可计算的函数;大素数 p,q 满足 $q|(p-1)$;G_q 是乘法群 Z_p^* 的阶为 q 的子群;$g,h=g^u$ 是群 G_q 的两个生成元,其中(u,h)是 Server 用于 ElGamal 加密用的私钥、公钥对.q_e,q_s,q_r 分别表示攻击者进行 Execute 查询、Send 查询以及 Reveal 查询的次数.如果群 G_q 满足 DDH 假设,则

$$Adv^{eke}_{g,h,G,F}\le 4q_s/N+6(q_e+q_s)\cdot Adv^{ddh}_{g,G}+2(\min\{q_e,q_r\}+\min\{q_s,q_r\})\cdot Adv^{F}+$$
$$(4q_s+2q_e)/q+2(q_e+q_s)\cdot Adv^{F}+2q_s\cdot 2^{-n}.$$

其中,$Adv^{ddh}_{g,G}$ 为攻破 DDH 假设的概率,Adv^F 为攻破伪随机函数集的概率,N 为所有口令的个数.

4 协议的证明

证明的基本思想是设计一系列的 Game,$\Gamma_0,\Gamma_1,\ldots,\Gamma_{14}$.在$\Gamma_0$ 中,所有的 Oracle 都按照协议的描述回答攻击者的查询,所以攻击者在Γ_0 中的成功概率等于攻击者攻击实际协议的成功概率.而以后的 Game 逐步修改 Oracle 的回答方式,并保证攻击者在两个相邻的 Game 中成功概率的差值是可忽略的.用 S 表示攻击者成功,Pr[S_i]表示攻击者在协议Γ_i中的成功概率.

Game Γ_1:Γ_1与Γ_0的区别是,当攻击者进行Execute查询时,B为一个随机数.我们将证明攻击者不能区分真正的 B 和一个随机数的概率很大.

引理 **1**. $|\Pr[S_1]-\Pr[S_0]|\le q_e\cdot Adv^{ddh}_{g,G}$.

证明:利用 Hybrid 技巧证明引理 1.假设攻击者一共进行了 q_e 次 Execute 查询.定义协议 $\Gamma_{1,l}$ 为前 l 次 Execute 查询按照 Γ_1 执行,而以后的 Execute 查询则按照 Γ_0 执行.显然有 $\Gamma_{1,0}=\Gamma_0,\Gamma_{1,q_e}=\Gamma_1$.所以,

$$\Pr[S_1]-\Pr[S_0]=\Pr[S_{1,q_e}]-\Pr[S_{1,0}],$$

其中, $\Pr[S_{1,q_e}],\Pr[S_{1,0}]$ 分别表示攻击者在 $\Gamma_{1,q_e},\Gamma_{1,0}$ 中的成功概率.

对每个 $0\le i\le q_e$,构造可以区分 (g,g^x,g^u,g^{xu}) 和 (g,g^x,g^u,r) 的算法 D_i,其中,r 是一个随机数.

1. 算法 D_i 获得输入 (g,g^x,g^u,Z),其中,Z 可能是 g^{xu},也可能是 r;
2. 设 $h=g^u$,随机选择一个 pw 作为 Client 和 Server 的口令;
3. 当攻击者 A 查询除了 Execute 之外的 Oracle 时,按照 Γ_0 中的描述,利用 pw 回答攻击者的查询;
4. 当攻击者 A 第 $j(j<i)$ 次查询 Execute 时,随机选择 $x',r'\in Z_q$,令 $A=g^{x'},B=r'g^{f(pw)}$;
5. 当攻击者 A 第 $i+1$ 次查询 Execute 时,令 $A=g^x,B=Zg^{f(pw)}$;
6. 当攻击者 A 第 $j(j>i+1)$ 次查询 Execute 时,随机选择 $x'\in Z_q$,令 $A=g^{x'},B=h^{x'}g^{f(pw)}$;
7. 如果攻击者成功,则输出 1;否则,输出 0.

当 $Z=g^{xu}$ 时,攻击者 A 得到的信息和在协议 $\Gamma_{1,i}$ 中得到的信息相同.而当 $Z=r$ 时,攻击者 A 得到的信息和在协议 $\Gamma_{1,i+1}$ 中得到的信息相同.所以,

$$\begin{aligned}|\Pr[S_1]-\Pr[S_0]|&\le\sum_{i=0}^{q_e-1}|\Pr[S_{1,i+1}]-\Pr[S_{1,i}]|\\&=\sum_{i=0}^{q_e-1}|\Pr[D_i(g,g^x,g^u,r)=1]-\Pr[D_i(g,g^x,g^u,g^{xu})=1]|\\&\le q_e\cdot Adv^{ddh}_{g,G}.\end{aligned}$$

Game Γ_2:Γ_2 与 Γ_1 的区别是,当攻击者进行 Execute 查询时,D 为随机数.与引理 1 类似,有:

引理 **2**. $|\Pr[S_2]-\Pr[S_1]|\le q_e\cdot Adv^{ddh}_{g,G}$.

Game Γ_3:Γ_3 与 Γ_2 的区别是,当攻击者进行 Execute 查询时,σ 为随机数.由于现在 B,D 都是随机数,所以攻击者可以得到的信息只有 $A=g^x$,而没有关于 y 的任何信息.所以,有以下引理:

引理 **3**. $\Pr[S_3]=\Pr[S_2]$.

Game Γ_4:Γ_4 与 Γ_3 的区别是,当攻击者进行 Execute 查询时,sk 为随机数.

引理 **4**. $|\Pr[S_4]-\Pr[S_3]|\le\min\{q_e,q_r\}\cdot Adv^F$.

证明:攻击者进行 Execute 查询后,Client 和 Server 将 sk 替换为随机数 r.如果攻击者不再进行 Reveal 查询,他在 Γ_4 中得到的信息和在 Γ_3 中得到的信息是相同的;如果攻击者进行 Reveal 查询,则协议返回 r.因为无论在 Γ_3 中还是在 Γ_4 中,下标 σ 都是随机数,并且攻击者没有任何关于 σ 的信息,所以在 Γ_3 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_4 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,从而证明了引理 4.证明过程与引理 1 类似,也利用了 Hybrid 的技巧. □

Game Γ_5:Γ_5 与 Γ_4 的区别是,当攻击者进行 Execute 查询时,ak_s,ak_c 均为随机数.与引理 4 类似,有

引理 **5**. $|\Pr[S_5]-\Pr[S_4]|\le q_e\cdot Adv^F+q_e\cdot Adv^{ddh}_{g,G}$.

证明:Γ_4 和 Γ_5 的区别在于攻击者是否可以区分 ak_s,ak_c 和随机数.如果攻击者可以区分 ak_s,ak_c 和随机数,那么,或者攻击者获得了关于 F_σ 的下标 σ,或者攻击者可以区分伪随机函数集.定义以下事件:

Dsigma:攻击者可以区分 $\sigma=g^{xy}$ 和随机数.

Dfvalue:攻击者可以区分 ak_s,ak_c 和随机数.

所以,

$$\begin{aligned}|\Pr[S_5]-\Pr[S_4]|&\le\Pr[Dfvalue]\\&\le\Pr[Dfvalue|\neg Dsigma]+\Pr[Dsigma]\end{aligned}$$

$$\leq q_e \cdot Adv^F + q_e \cdot Adv_{g,G}^{ddh}. \quad \square$$

Game Γ_6:至此,对 Execute 查询的修改完毕.下面开始对 Send 查询进行修改.Γ_6 与 Γ_5 的区别是,当攻击者进行 $Send(i,1,Server,Client|A_i|B_i)$查询时,Send 首先检查消息$(A_i,B_i)$是否为以前攻击者通过 Oracle 查询得到的消息.如果是,则直接判定消息有效,并继续按照 Γ_5 执行;如果不是,则首先验证是否满足 $B_i / A_i^u = g^{f(pw)}$,如果通过验证则继续按照 Γ_5 执行;否则终止协议.这只是增大了攻击者成功的概率.

引理 **6**. $\Pr[S_6] \geq \Pr[S_5]$.

Game Γ_7:Γ_7 与 Γ_6 的区别是,当攻击者进行 $Send(i,0,Client,\text{null})$查询时,Send 随机选择一个 B_i.与引理 1 类似,有

引理 **7**. $|\Pr[S_7] - \Pr[S_6]| \leq q_s \cdot Adv_{g,G}^{ddh}$.

Game Γ_8:Γ_8 与 Γ_7 的区别是,当攻击者进行 $Send(i,1,Server,Client|A_i|B_i)$查询时,Send 验证是否 $B_i / A_i^u = g^{f(pw)}$.如果是,则直接判定攻击者成功;否则,按照 Γ_7 执行.

引理 **8**. $|\Pr[S_8]-\Pr[S_7]| \leq (2q_s+q_e)/q+q_s/N$.

证明:定义以下事件:

Nvalid:攻击者构造了一条新的消息$(Client|A_i|B_i)$,用来查询 $Send(i,1,Server,Client|A_i|B_i)$,并且满足

$$B_i / A_i^u = g^{f(pw)}.$$

OValid:攻击者使用一条以前通过 Oracle 查询获得的消息$(Client|A_i|B_i)$,用来查询 $Send(i,1,Server,Client|A_i|B_i)$,并且满足 $B_i / A_i^u = g^{f(pw)}$.

因为攻击者在 Γ_8 中成功,所以,或者他在 Γ_7 中也成功,或者 NValid 事件发生,或者 OValid 事件发生,所以,

$$\Pr[S_8]=\Pr[S_7 \vee NValid \vee Ovalid]$$
$$\leq \Pr[S_7]+\Pr[NValid]+\Pr[OValid].$$

根据 Γ_2 和 Γ_7 的规则,在攻击者通过 Oracle 查询获得的所有(A,B)中,B 都是随机数.因为攻击者通过 Oracle 查询获得的所有(A,B)的总个数不会超过 q_s+q_e,从而

$$\Pr[Ovalid]=(q_s+q_e)\cdot \Pr[B/A^u=g^{f(pw)}]$$
$$\leq (q_s+q_e)/q. \quad \square$$

下面计算 Nvalid 发生的概率.分两种情况加以讨论:

1) 攻击者猜中口令 pw.由于在 Γ_8 中,攻击者可以得到的所有消息都与 pw 无关,所以攻击者每次 Send 查询时猜中 pw 的概率是 q_s/N,其中,N 表示所有可能的口令的个数.
2) 攻击者没有猜中口令,但他仍然构造了一条新的满足要求的查询.这时,当攻击者选定 A 以后,B 被唯一确定下来.由于攻击者没有任何关于 pw 的信息,因此猜中这个唯一的 B 的概率为 q_s/q.

从而

$$|\Pr[S_8]-\Pr[S_7]| \leq \Pr[Ovalid]+\Pr[NValid]$$
$$\leq (2q_s+q_e)/q+q_s/N. \quad \square$$

Game Γ_9:对 $Send(i,1,Server,Client|A_i|B_i)$进行修改.接受到查询以后,随机选择 y,r,并按照协议描述计算 $C_i=g^r$,$\sigma=(A_i)^y$,$ak_s=F_\sigma(2)$.但是,并不计算 D_i,而是将 D_i 设为一个随机数.与引理 1 类似,有

引理 **9**. $|\Pr[S_9] - \Pr[S_8]| \leq q_s \cdot Adv_{g,G}^{ddh}$.

Game Γ_{10}:Γ_{10} 与 Γ_9 的区别是,当攻击者查询 $Send(i,1,Server,Client|A_i|B_i)$时,Send 随机选择一个 ak_s.

引理 **10**. $|\Pr[S_{10}]-\Pr[S_9]| \leq q_s \cdot Adv^F$.

证明:因为在引理 9 中已经将 D_i 替换为随机数,所以攻击者通过 Send 查询得不到任何关于 g^y 的信息,因此也得不到任何关于 $\sigma=g^{xy}$ 的信息.根据伪随机函数集的定义,可以证明引理 10. $\square$

Game Γ_{11}:Γ_{11} 与 Γ_{10} 的区别是,当攻击者进行 $Send(i,2,Client,Server|C_i|D_i|ak_{i,s})$查询时,如果消息是由以前的 Execute 或 Send 查询产生的,则直接判定验证 $ak_{i,s}=F_\sigma(2)$通过,继续执行协议;否则,按照协议描述验证 $ak_{i,s}$ 的正

确性,如果验证通过,则直接判定攻击者成功,并终止协议.

引理 **11**. $|\Pr[S_{11}]-\Pr[S_{10}]|\le q_s/N$.

证明:为了通过验证,攻击者必须计算出σ的值,即攻击者必须选取 y,并利用 g^x 产生 $g^{f(pw)+y}$ 的有效 ElGamal 加密.为此,攻击者必须猜测 $f(pw)$的值,所以引理 11 得证. □

Game Γ_{12}:Γ_{12} 与Γ_{11} 的区别是,当攻击者进行 $Send(i,2,Client,Server|C_i|D_i|ak_{i,s})$查询时,返回一个随机的 ak_c.与引理 10 类似,有

引理 **12**. $|\Pr[S_{12}]-\Pr[S_{11}]|\le q_s\cdot Adv^F$.

Game Γ_{13}:Γ_{13} 和Γ_{12} 的区别是,如果 ak_c 是由查询 $Send(i,2,Client,Server|C_i|D_i|ak_{i,s})$产生的,则直接通过验证,并计算 sk;否则,终止协议.

引理 **13**. $|\Pr[S_{13}]-\Pr[S_{12}]|\le q_s\cdot 2^{-n}$.

证明:如果攻击者在Γ_{11} 中仍然没有成功,则前面所有的消息都一定是 Client 和 Server 产生的,并且没有泄露任何关于 y 的信息,所以攻击者得不到任何关于 g^{xy} 的信息.由于函数 F_σ的值域内总共有 2^n 个元素,所以攻击者猜中 $F_\sigma(3)$的概率为 2^{-n}.从而可以证明引理 13. □

Game Γ_{14}:将在 Send 查询中产生的 sk 全部替换为随机数.

引理 **14**. $|\Pr[S_{13}]-\Pr[S_{12}]|\le \min\{q_s,q_r\}\cdot Adv^F$.

证明:因为在引理 13 中,攻击者已经得不到任何关于σ的信息,所以,与引理 4 类似,可以证明引理 14. □

下面计算攻击者在Γ_{14} 中的成功概率.攻击者在Γ_{14} 中成功的可能情况有:

1. 在 $Send(i,1,Server,Client|A_i|B_i)$查询中,消息$(Client|A_i|B_i)$满足 $B_i/A_i^u=g^{f(pw)}$.这时,在Γ_8 中已判定成功;
2. 在 $Send(i,2,Client,Server|C_i|D_i|ak_{i,s})$查询中,消息$(Server|C_i|D_i|ak_{i,s})$满足 $ak_{i,s}=F_\sigma(2)$.这时,在Γ_{11} 中已判定成功;
3. 在 Test 查询中,正确猜出比特 b 的值.

在 Test 查询中,因为Γ_{14} 中的 sk 是随机选取的,所以,攻击者可以正确猜中比特 b 的值的概率就是 1/2.

综合上面的所有引理,有

$$\Pr[S]=\Pr[S_0]\le 1/2+2q_s/N+(3q_e+3q_s)\cdot Adv_{g,G}^{ddh}+$$
$$(\min\{q_e,q_r\}+\min\{q_s,q_r\})\cdot Adv^F+(2q_s+q_e)/q+(q_e+q_s)\cdot Adv^F+q_s\cdot 2^{-n}.$$

5 进一步的讨论

注意到在我们的协议中,Client 和 Server 实际上都只使用了 $g^{f(pw)}$,而没有使用 pw,因此可以假设 Server 上面只存有 $g^{f(pw)}$,这样可以防止攻击者控制 Server 以后直接得到 Client 的口令.在很多实际情况下,服务器都只保存了一个可以用来验证口令的值,并没有保存用户的口令(例如 Linux 的登陆程序).但是这时,攻击者也只需要得到 $g^{f(pw)}$就可以完成协议.为了防止这种攻击,可以使用 PAK-Y 协议[17]中使用的技巧,从而得到一个加强的 EKE 协议.文献[17]在认证时使用了 Schnorr 的签名方案[18].

References:

[1] Bellovin SM, Merritt M. Encrypted key exchange: Password-Based protocols secure against dictionary attacks. In: Proc. of the 1992 IEEE Computer Society Symp. on Research in Security and Privacy. Oakland: IEEE Computer Society, 1992. 72−84.

[2] Bellovin SM, Merritt M. Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In: Denning D, ed. ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 244−250.

[3] Jablon DP. Extended password key exchange protocols immune to dictionary attacks. In: Proc. of the WETICE'97 Workshop on Enterprise Security. Cambridge: IEEE Computer Society, 1997. 248−255.

[4] Steiner M, Buhler P, Eirich T, Waidner M. Secure password-based cipher suite for TLS. ACM Trans. on Information and System Security, 2001,4(2):134−157.

[5] Wu TD. The secure remote password protocol. In: Proc. of the Network and Distributed System Security Symp. NDSS 1998. San Diego: Internet Society, 1998.

[6] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. In: Preneel B, ed. Advances in Cryptology—EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 139−155.

[7] Bellare M, Rogaway P. Entity authentication and key distribution. In: Stinson DR, ed. Advances in Cryptology—CRYPTO'93. LNCS 773, Berlin: Springer-Verlag, 1993. 232−249.

[8] Boyko V, MacKenzie PD, Patel S. Provably secure password-authenticated key exchange using diffie-hellman. In: Preneel B, ed. Advances in Cryptology—EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 156−171.

[9] Abdalla M, Chevassut O, Pointcheval D. One-Time verifier-based encrypted key exchange. In: Vaudenay S, ed. Public Key Cryptography—PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 47−64.

[10] Abdalla M, Pointcheval D. Simple password-based encrypted key exchange protocols. In: Menezes A, ed. Topics in Cryptology—CT-RSA 2005. LNCS 3376, Berlin: Springer-Verlag, 2005. 191−208.

[11] Bresson E, Chevassut O, Pointcheval D. New security results on encrypted key exchange. In: Bao F, Deng RH, Zhou JY, eds. Public Key Cryptography—PKC 2004. LNCS 2947, Berlin: Springer-Verlag, 2004. 145−158.

[12] Jiang SQ, Gong G. Password based key exchange with mutual authentication. In: Handschuh H, Hasan MA, eds. Selected Areas in Cryptography—SAC 2004. LNCS 3357, Berlin: Springer-Verlag, 2004. 267−279.

[13] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Advances in Cryptology—EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 475−494.

[14] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Denning D, ed. ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−73.

[15] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. In: Vitter J, ed. Proc. of the 30th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1998. 209−218.

[16] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Advances in Cryptology—CRYPTO'98. LNCS 1462, Berlin: Springer-Verlag, 1998. 13−25.

[17] MacKenzie P. More efficient password-authenticated key exchange. In: Naccache D, ed. Topics in Cryptology—CT-RSA 2001. LNCS 2020, Berlin: Springer-Verlag, 2001. 361−377.

[18] Schnorr CP. Efficient identification and signatures for smart cards. In: Brassard G, ed. Advances in Cryptology—CRYPTO'89. LNCS 435, Berlin: Springer-Verlag, 1990. 239−252.

殷胤(1981－),湖南娄底人,硕士,主要研究领域为密码学,安全协议.

李宝(1962－),男,博士,研究员,博士生导师,主要研究领域为密码学,安全协议.