高效的口令基认证组密钥协商协议

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 成都 610054; 2. 江西财经大学国际经贸学院 南昌 330013)

【摘要】对认证的口令基组密钥协商协议进行安全分析，指出传送数据中的冗余导致协议的不安全。基于Burmester and Desmedt的协议，给出一种改进的协议。该协议的计算复杂度较低，通信轮数较少；该协议不但满足前向安全性、双向认证性，还能有效地抵抗中间人攻击。最后，依赖于Diffie-Hellman(CDH)假设，在随机预言机和理想密码模型下证明了协议的安全性。

关 键 词 认证； 熵； 组密钥协商； 可证安全； 公钥密码；

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.03.018

Efficient Password-Based Authenticated Group Key Exchange Protocol

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

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054;

2. School of International Trade and Economics, University of Jiangxi Financial Economics Nanchang 330013)

Abstract The security of an authenticated group key exchange is analyzed, the results show that it is insecure due to redundancy of the exchange messages. Based on the protocol of Burmester and Desmedt, an improved protocol is proposed with merits in terms of computation and communication. The improved protocol provides not only the capability of forward secrecy and mutual authentication, but also the capability against man-in-middle attack. The protocol is proven secure in the random-oracle and ideal-cipher models under the computational Diffie-Hellman(CDH) assumption.

Key words authentication; entropy; group key exchange; provable security; public key cryptography

组密钥协商协议的目的是让n(n>2)个用户在开放网络通过交互，建立一个共同的密钥，从而实现安全通信。一般地，协议借助公钥机制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，公钥机制所需计算量较大，还需要可信第三方的参与，在某些特定的场合中，如紧急救援、军事行动和Ad-hoc网络[1-2]中，由于缺少固定的安全基础设施，无法实现安全的组密钥协商。让所有用户共享一个相同的口令而生成高熵的会话密钥是很好的解决方案。由于口令的固有特性(长度短、随机性差)，如果在设计协议时口令使用不当，攻击者可能在离线状态下进行穷举字典攻击。

文献[3]首先提出基于口令的两方密钥协商协议。文献[4]提出了基于口令的两方密钥协商的一种理论模型。文献[5]和[6]也提出一种口令的两方密钥协商协议，并在随机预言机模型下给出了安全证明。文献[7]和[8]提出了在标准模型下可证安全的基于口令的两方密钥协商协议。

基于文献[9]的口令基组密钥协商协议，文献[10]提出了具有前向安全性的口令基组密钥协商协议。该协议要执行$O(n)$通讯轮数，每个用户要执行$O(n)$次模指数操作，且没有给出严格的证明。在文献[4]的基础上，文献[11]首先提出了基于口令的安全组密钥协商协议的理论模型，并在该模型下设计了可证安全的口令基组密钥协商协议。然而该协议也要线性数的通讯。基于文献[12]，文献[13]和[14]提出了可证安全的固定通讯轮数的口令基组密钥协商协议，其共同特点是通信复杂度和计算复杂度较低。但是，由于在协议设计时没有很好地处理口令以及存在冗余，攻击者可以对协议进行有效的攻击。文献[15]提出了安全的固定通信轮数的口令基组密钥协商协议，其通信复杂度和计算复杂度较高。为此，本文提出一种高效的口令基组密钥协商协议，具有

收稿日期：2007 – 12 – 22；修回日期：2008 – 10 – 25
基金项目：国家863计划(2009AA012415)
作者简介：舒 剑(1972 –)，男，博士生，主要从事密码学、信息安全方面的研究.

通信和计算复杂度低的特点，并在随机预言机模型下证明是安全的。

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 $n \in N$ 满足 $\varepsilon(n) < 1/p(n)$。

1.2 CDH(computational Diffie-Hellman)假设

设大素数 p、q 满足 $q|(p-1)$, 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_a 满足CDH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都不能计算出 g^{xy}。

2 Lee-Hwang-Lee协议及其攻击

基于文献[16]所提出的协议，文献[14]给出了一个固定通信轮数的口令基组密钥协商协议，要求所有的用户形成一个逻辑环，其中 ε 表示理想密码，H 和 H_1 是随机预言函数。协议描述如下：

第1轮：每个用户 U_i 选择一个随机数 x_i，计算 $z_i = g^{x_i}$，并广播消息 $(U_i, z_i^* = \varepsilon_{\mathrm{pw}}(z_i))$。

第2轮：每个用户 U_i 在收到相邻节点的消息后，解密得到 z_{i-1} 和 z_{i+1}，然后分别计算 $K_i = H(z_{i+1}^{x_i}) = H(g^{x_i x_{i+1}})$ 和 $K_{i-1} = H(z_{i-1}^{x_i}) = H(g^{x_{i-1} x_i})$，再计算 $W_i = K_{i-1} \oplus K_i$，然后广播消息 (U_i, W_i)。

计算会话密钥：每个用户 U_i 在收到其他 $n-1$ 个用户第2轮的消息 W_j $(1 \leqslant j \leqslant n, j \neq i)$，用户 U_i 可以计算 $K_j = H(g^{x_{j-1} x_j})$ $(1 \leqslant j \leqslant n)$。最后每个用户得到相同的会话密钥为：

$$\mathrm{sk} = H_1(H(g^{x_1 x_2}) \| H_2(H(g^{x_2 x_3}) \| \cdots \| H(g^{x_{n-1} x_n}) \| H(g^{x_n x_1}))$$

由于第2轮的明文传输中存在冗余，即 $W_1 \oplus W_2 \oplus \cdots \oplus W_{n-1} \oplus W_n = 0$，攻击者就可以利用消息冗余发动攻击。

文献[15]指出，攻击者控制了 $n-1$ 个用户(n为参与本次会话的组成员个数)，就可以发动有效的攻击。攻击者只要控制了 $\lfloor n/2 \rfloor$ 个用户，使得合法用户的左右邻居被控制，就可以发动有效的攻击。以4个用户 (U_1, U_2, U_3, U_4) 为例，攻击者控制了 U_2、U_4，攻击过程如下：

首先，攻击者让合法用户 U_1 启动两次会话。在两次会话中 U_1 分别选择两个秘密参数 x_1 和 x_1'，然后分别发送 $(U_1, z_1^* = \varepsilon_{\mathrm{pw}}(g^{x_1}))$、$(U_1, z_1'^* = \varepsilon_{\mathrm{pw}}(g^{x_1'}))$。在 U_1 发送 $(U_1, z_1^* = \varepsilon_{\mathrm{pw}}(g^{x_1}))$ 的会话中，攻击者让 U_2、U_4 分别发送 $(U_2, z_1'^* = \varepsilon_{\mathrm{pw}}(g^{x_1'}))$ 和 $(U_4, z_1'^* = \varepsilon_{\mathrm{pw}}(g^{x_1'}))$；而在 U_1 发送 $(U_1, z_1'^* = \varepsilon_{\mathrm{pw}}(g^{x_1'}))$ 的会话中，攻击者让 U_2、U_4 分别发送 $(U_2, z_1^* = \varepsilon_{\mathrm{pw}}(g^{x_1}))$ 和 $(U_4, z_1^* = \varepsilon_{\mathrm{pw}}(g^{x_1}))$。在每次会话中，合法用户左右邻居都发送相同的消息，根据协议规则，两次会话中合法用户 U_1、U_3 在第2轮发送的消息均为0。攻击者让 U_2、U_4 在两次会话中的第2轮都发送相同的值 K。

在 U_1 选择 x_1 的会话中，U_1 利用左右邻居第1轮发送的信息得到 $H(g^{x_1 x_2}) = H(g^{x_4 x_1}) = H(g^{x_1' x_1})$，在收到所有其他用户第2轮发送的信息后，$U_1$ 按如下方式计算会话密钥 sk：

$$H(g^{x_1 x_2}) = H(g^{x_1' x_1})$$

$$H(g^{x_2 x_3}) = H(g^{x_1' x_1}) \oplus W_2 = H(g^{x_1' x_1}) \oplus k$$

$$H(g^{x_3 x_4}) = H(g^{x_2 x_3}) \oplus W_3 = H(g^{x_2 x_3}) \oplus 0 = H(g^{x_1' x_1}) \oplus k$$

$$H(g^{x_4 x_1}) = H(g^{x_3 x_4}) \oplus W_4 = H(g^{x_1' x_1}) \oplus k \oplus k = H(g^{x_1' x_1})$$

U_1 把最后一步所得的值 $H(g^{x_1' x_1})$ 和第1轮后 U_1 所计算的 $H(g^{x_4 x_1})$ 比较，两者相等，则认为协议正常运行，数据没有被修改。然后计算会话密钥为：

$$\mathrm{sk} = H_1'(H(g^{x_1' x_1}) \| H(g^{x_1' x_1}) \oplus k \| H(g^{x_1' x_1}) \oplus k \| H(g^{x_1' x_1}))$$

从以上的运算过程可以看出，在另一个会话中 U_1 算出的会话密钥 $\mathrm{sk}' = \mathrm{sk}$。两次会话中，$U_1$ 计算的会话密钥相同，因而攻击者可以对 U_1 的两个实例发送Test查询，如果两次查询返回的值相同，则一定是会话密钥。

3 新的口令基认证组密钥协商协议

基于文献[12]提出的固定通信轮数的组密钥协商协议，本文提出了一种新的口令基认证组密钥协商协议。该协议基于CDH假设和理想加密机制，所有参与通信的用户形成一个逻辑环，其中 ε 和 ε' 表示理想密码；$\mathrm{ID} = \mathrm{ID}_{u_1} \| \mathrm{ID}_{u_2} \| \cdots \| \mathrm{ID}_{u_n}$；$H: \{0,1\}^* \rightarrow \{0,1\}^l$ 和 $H_1: \{0,1\}^* \rightarrow \{0,1\}^{l_1}$ 是单向哈希函数。协议描述如下：

第1轮：任意用户 U_i 随机选择两个参数 $k_i \in \{0,1\}^t$ 和 $x_i \in Z_q^*$，计算 $z_i = g^{x_i}$ 和 $z_i^* = \varepsilon_{\mathrm{pw}}(z_i + \mathrm{ID} + i)$，然后发送信息 (U_i, z_i^*) 给左右邻居，其中第 n 个用户发送 $U_n, z_i^* \| H(k_n \| 0)$。

第2轮：任意用户 U_i 收到左右邻居发送的信息后，解密得到 z_{i-1} 和 z_{i+1}，计算 $M_i^L = H(z_{i-1}^{x_i}) = H(g^{x_{i-1} x_i})$、$M_i^R = H(z_{i+1}^{x_i}) = H(g^{x_{i+1} x_i})$ 以及 $T_i = M_i^L \oplus M_i^R$ $(1 \leqslant i \leqslant n-1)$，其中，$U_n$ 计算 $T_n =$

$M_n^R \oplus k_n$，然后广播消息$(U_i, k_i \| T_i)(1 \leqslant i \leqslant n-1)$，第$n$个用户广播消息$(U_n, \varepsilon'_{\mathrm{pw}}(T_n))$。

第3轮：任意用户U_i收到其他$n-1$个用户的消息后，先解密$\varepsilon'_{\mathrm{pw}}(T_n)$得到$T_n$，计算$k_n = H(g^{x_{i-1}x_i}) \oplus T_{i-1} \cdots \oplus T_1 \oplus T_n$，接着验证$H(k_n \| 0)$是否和第1轮$U_n$发送的消息相等。如果相等，则广播认证消息$(U_i, H_1(k_1 \| k_2 \| \cdots \| k_{n-1} \| k_n \| \mathrm{ID} \| i))$。

密钥计算：任意用户U_i验证其他$n-1$个用户的认证消息，若通过，则所有的用户计算相同的会话密钥$\mathrm{sk} = H_1(k_1 \| k_2 \| \cdots \| k_{n-1} \| k_n \| \mathrm{ID} \| 0)$。

该协议与其他可证安全协议的比较如表1所示。文献[11]协议的通信轮数随用户增加呈线性增加。文献[15]的协议虽然只要4轮通信，但要求每个用户重新计算某次会话的口令，使该次会话中每个用户的口令不一样，并且还要计算并保存相邻用户的新口令(为了解密消息)，从而增加了协议的复杂度。该协议只要3轮通信和3次模指数运算(每个用户)。

表1　与其他协议的比较

	通信轮数	模指数运算(每个用户)	困难性假设
文献[11]	N	$2N$	Multiple DDH
Abdalla[15]	4	4	Parallel CDH
新协议	3	3	CDH

4　协议的证明

定理 1　Γ是本文所提出的新协议；$k_i \in_R \{0,1\}^t$；$H:\{0,1\}^* \to \{0,1\}^l$和$H_1:\{0,1\}^* \to \{0,1\}^{l_1}$是单向哈希函数，其中$l$、$l_1$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$z_p^*$的一个阶为$q$的子群，$g$是群$G_q$的一个生成元；$q_e$、$q_s$分别表示攻击者进行Execute查询、Send查询的次数；q_H、q_{H_1}、q_ε分别表示攻击者对预言机H、H_1和理想密码预言机ε的查询次数。如果群G_q满足CDH假设，则：

$$\mathrm{Adv}_{P,A}^{\mathrm{PGKE}} \leqslant \frac{q_H^2}{2^l} + \frac{q_{H_1}^2}{2^{l_1}} + \frac{q_\varepsilon^2}{\min\{(q-1), 2^t\}} + \frac{2q_s}{N} + 4q_H q_s^2 \mathrm{Adv}_{G,A}^{\mathrm{CDH}}(t)$$

证明的基本思想是设计一系列的实验$\Gamma_0 \sim \Gamma_5$。在Γ_0中，所有的预言机都按照协议的描述回答攻击者的查询，所以攻击者的成功概率等于攻击者攻击实际协议的成功概率。以后的实验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是可忽略的。$\mathrm{pr}[S_i]$表示攻击者在Γ_i实验中的成功概率。$\mathrm{Encrypt}_i$表示在实验Γ_i中攻击者A用自己生成的信息进行Send查询以猜测口令值，事件$\mathrm{Encrypt}_i$的概率衡量对字典攻击的安全性。

实验Γ_0：是现实攻击实验，可得$\mathrm{Adv}_{p,A}^{\mathrm{PGKE}} = 2\Pr[S_0] - 1$。

实验Γ_1：用列表Hlist和H_1list来模拟随机预言机H和H_1，有新的查询时，返回一个随机数。当哈希函数的输出值发生碰撞时，则直接判定攻击者成功，并终止协议。由生日悖论原理可得：

$$|\Pr[S_1] - \Pr[S_0]| \leqslant \frac{q_H^2}{2^{l+1}} + \frac{q_{H_1}^2}{2^{l_1+1}}$$

实验Γ_2：用大小为q_ε的列表Elist和列表Dlist(初始为空)来模拟加密/解密预言机。

加密：对于一个加密查询$E_k(X)$(E可以是ε或ε')，如果在Elist中存在一条记录(δ,k,X,Λ,Y)，则返回Y；否则返回大小为$|X|$的随机数Y。记录(δ,k,X,E,Y)添加到列表Elist中，其中δ=0表示查询来自模拟器，δ=1表示查询来自攻击者。

解密：对于一个解密查询$D_k(Y)$(D可以是D，或D_2，其中，D_1、D_2分别对应于ε、ε'的解密方案)，如果在Elist中存在一条记录(δ,k,X,Λ,Y)，则返回值为X；否则根据以下两种情况返回X的值：

(1) 如果$D=D_1$，返回值为$X=g^r$，其中r从Z_q中随机选出。

(2) 如果$D=D_2$，返回值为r，其中r从$\{0,1\}^t$中随机选出。

记录(k,Y,D,X)和$(0,k,X,D,Y)$分别加入列表Dlist和Elist。可以看到$D_k(Y)$在相应的加密查询之前被查询，才可能加入列表Dlist。在实验Γ_i中，当记录$(1,\mathrm{pw},X,*,Y)$出现在Elist列表中，其中Y来自Send查询，而相应的记录(pw,Y,D,X)没有出现在Dlist列表中时，$\mathrm{Encrypt}_i$事件就发生了。

从以上的模拟过程可以看出，除非分组密码的置换特性不成立，否则Γ_1和Γ_2是完全不可区分的。由于加/解密列表的最大值为q_ε，则有：

$$|\Pr[S_2] - \Pr[S_1]| \leqslant \frac{q_\varepsilon^2}{2\min\{(q-1), 2^t\}}$$

实验Γ_3：Γ_3与Γ_2的区别是$\mathrm{Encrypt}_2$事件的发生，即出现Send(U,i,Y)查询，而且记录$(1,\mathrm{pw},X,*,Y)$出现在Elist列表中，则终止协议执行：

$$|\Pr[S_3] - \Pr[S_2]| \leqslant \Pr[\mathrm{Encrypt}_2]$$

实验Γ_4：该实验与Γ_3不同之处在于，用三元组$(A=g^a, B=g^b, C=g^{ab})$嵌入到协议中。在第一轮中

除U_1和U_n随机选择c_1和$c_n \in Z_q^*$外，其他用户选择$x_2 \cdots x_{n-1} \in Z_q^*$，则$U_1$发送($U_1$, $z_1^* = \varepsilon_{\mathrm{pw}}(A^{c_1} + \mathrm{ID} + 1)$)，$U_n$发送($U_n$, $\varepsilon_{\mathrm{pw}}(B^{c_n} + \mathrm{ID} + n) \| H(k_n \| 0)$)，其他用户发送($U_i$, $z_i^* = \varepsilon_{\mathrm{pw}}(z_i + \mathrm{ID} + i)$)。在第2轮中计算$M_{n-1}^R = M_n^L = H(B^{x_{n-1}c_n})$；$M_n^R = M_1^L = H(C^{c_1 c_n})$；$M_1^R = M_2^L = H(A^{c_1 x_2})$；其他的运算和现实攻击中的情况相同。

由于c_1和c_n是随机选出的，x_i (2<i<n − 1)是随机数，而且因为CDH问题的乘法随机自归约特性，本文实验的模拟攻击和现实中的攻击是不可区分的，因而可得：

$$\Pr[S_4] = \Pr[S_3]$$

并且：

$$\Pr[\mathrm{Encrypt}_4] = \Pr[\mathrm{Encrypt}_3] = \Pr[\mathrm{Encrypt}_2] = \Pr[\mathrm{Encrypt}_1]$$

实验Γ_5：只给出二元组($A = g^a$，$B = g^b$)，而不给出$C = g^{ab}$和a、b的值。该实验与Γ_4的不同之处在于：当用户进行涉及到$M_n^R (= M_1^L)$的哈希查询时，返回值不再是$H(C^{c_1 c_n})$，而是一个从$\{0,1\}^l$中随机取得的数r。

本文定义事件AaskH为：攻击者利用自己的哈希预言查询，发现包含M_n^R哈希值的广播信息有错。

如果攻击者A能成功猜出$C^{c_1 c_n}$，并提交给哈希预言机，则攻击者可以发现包含M_n^R哈希值的不一致性。这是因为同样的哈希查询，如果发起者是攻击者，仍由随机哈希预言机回答；如果发起者是模拟器，则返回一个随机数r。因此，只要事件AaskH不发生，Γ_5和Γ_4是完全不可区分的。则有：

$$|\Pr[S_5] - \Pr[S_4]| \leqslant \Pr[\mathrm{AaskH}]$$

$$|\Pr[\mathrm{Encrypt}_5] - \Pr[\mathrm{Encrypt}_4]| \leqslant \Pr[\mathrm{AaskH}]$$

给定二元组($A = g^a$, $B = g^b$)，如果以下两个条件成立，则可以算出正确的Diffie-Hellman值$C = g^{ab}$。(1) 两个相邻用户U_1和U_n计算A^{c_1}和B^{c_n}，涉及到$M_n^R = M_1^L$的哈希值时，返回随机数，而不是进行哈希预言机查询。(2) 攻击者成功猜出$C^{c_1 c_n}$，并进行哈希查询。由以上分析可得：

$$\mathrm{Adv}_{G,A}^{\mathrm{CDH}}(t) \geqslant \frac{1}{q_{\mathrm{H}} q_{\mathrm{s}}^2} \Pr[\mathrm{AaskH}]$$

在这个实验中，攻击者A的输出值b'是完全随机的，则$\Pr[S_5] = 1/2$。

综合所有实验中所得到的不等式，可以得出：

$$|\Pr[S_0] - \frac{1}{2}| \leqslant \frac{q_{\mathrm{H}}^2}{2^{l+1}} + \frac{q_{\mathrm{H}_1}^2}{2^{h+1}} \frac{q_\varepsilon^2}{2\min\{(q-1), 2^l\}} + \Pr[\mathrm{Encrypt}_5] + 2 q_{\mathrm{H}} q_{\mathrm{s}}^2 \mathrm{Succ}_{G,A}^{\mathrm{CDH}}(t)$$

计算$\Pr[\mathrm{Encrypt}_5]$的过程如下：事件$\mathrm{Encrypt}_5$发生则表示攻击者发起了一个Send(*U*,*i*,*Y*)查询，且一条记录(1,pw,*X*,∗,*Y*)出现在Elist列表中。因为知道攻击者A最多可以进行q_{s}次Send查询，因此攻击者可以在线猜测q_{s}个口令，也就是攻击者通过猜测口令进行次q_{s}假冒攻击。另外，从攻击者角度，加密的明文和从相应的加密函数的域中取出的随机明文是不可区分的。因此，口令可以抵抗离线穷尽搜索，Execute预言机和Reveal预言机对攻击者没有任何帮助，模拟器和口令完全独立，则有：

$$\Pr[\mathrm{Encrypt}_5] \leqslant \frac{q_s}{N}$$

结合以上等式，就可得出定理1。

5 总 结

本文给出一种高效、安全的口令基组密钥协商协议。基于文献[4]提出的理论模型证明了该协议的安全性，其中的证明方法采用了文献[11]所用的证明技巧。该协议依赖于CDH假设，在随机预言机和理想密码模型下证明是安全的。

在以后的工作中，将研究在标准模型中(没有随机预言机)设计高效的口令基组密钥协商协议，同时，使协议支持成员的加入和退出也是以后研究的内容。

参 考 文 献

[1] OBRACZKA K, TSUDIK G. Pushing the limits of multicast in Ad hoc networks[C]//Proceedings of the 21th International Conference on Distributed Computing System. Washington, DC, USA: IEEE Computer Society , 2001: 719-722.

[2] ZHOU L, HASS Z J. Securing Ad hoc networks[J]. IEEE Network Magazine, 1999, 13(6): 24-30.

[3] BELLOVIN S, MERRITT M. Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise[C] //Proceedings of the 1st ACM Conference on Computer and Communication Security. New York, USA: ACM Press, 1993: 244-250.

[4] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]//Eurocrypt 2000, LNCS1807. Berlin: Springer-Verlag, 2000: 139-155.

(下转第414页)