# 1 原协议回顾

## 1.1 参数列表

协议中的指数运算都是在环 $Z_P$ 中进行，其他运算都是在素数 $P$ 阶乘法群 $G$ 中进行。原协议参数如表 1 所示。

**表 1 原协议参数**

Tab.1 Parameters of original protocals

| 符号 | 含义 |
|---|---|
| $A$，$S$ | 用户 $A$ 和服务器 $S$ |
| $H$ | 抗碰撞的单向哈希函数 |
| $\pi$ | 用户口令 |
| $\mathrm{ID}_A$ | 用户 $A$ 的身份 |
| $g$ | 阶为素数 $P$ 的群 $G$ 的生成元 |
| $V$ | 服务器保存的验证信息，$V=g^u=g^{H(A,S,\pi)}$，$\upsilon=H(A,S,\pi)$ |

## 1.2 协议过程

1) $A$ 选择 $\alpha\in_R Z_P^*$，计算：$X_A=g^a\oplus V$，然后将 $\mathrm{ID}_A$ 和 $X_A$ 发送给 $S$.

2) 收到 $A$ 发送过来的消息后，$S$ 从自己保存的口令文件中取出 $A$ 的验证信息，同时选取 $b\in_R Z_P^*$，计算 $X_S=V^b\oplus V$，将计算的 $X_S$ 发送给 $A$，然后计算：$K_S=(X_A\oplus V)^b=g^{ab}$，$V'_A=H(A,X_S,K_S)$，$V_S=(S,X_A,K_S)$.

3) 收到 $S$ 发送过来的 $X_S$ 后，$A$ 计算：$K_A=(X_S\oplus V)^{aH(A,S,\pi)^{-1}}=g^{ab}$，$V_A=H(A,X_S,K_A)$，将 $V_A$ 发送给 $B$，然后计算：$V'_S=H(S,X_A,K_A)$.

4) 收到 $A$ 发送过来 $V_A$ 后，$S$ 验证 $V_A=V'_A$，如果相等，$S$ 确信 $K_A$ 得到证实，然后将 $V_S$ 发送给 $A$.

5) 收到 $S$ 发送 $V_S$ 后，$A$ 验证 $V_S=V'_S$，如果相等，则 $A$ 确信 $K_S$ 得到证实。

6) 从而双方得到共同的会话密钥 $K=H(K_A)=H(K_S)=H(g^{ab})$.

文献[7]声称该协议能够抵抗服务器泄露攻击，即攻击者窃取到了存储在服务器上的口令文件，也不能够利用该文件中的信息来冒充相应的用户与服务器进行通信。

# 2 对协议的攻击性分析

文献[8]对上文提到的协议给出一个服务器泄露攻击的情形，分析了受到这种攻击的原因，然后给出一种改进的协议。

假设攻击者 $E$ 获取了服务器 $S$ 的口令文件，通过分析从中取得了服务器 $S$ 对 $A$ 身份进行验证的信息。$E$ 的目标是冒充 $A$ 与 $S$ 进行通信，试图获取共同的会话密钥，攻击过程如下：

1) $E$ 选择 $a\in_R Z_P^*$，计算 $X_A=V^a\oplus V$，将 $\mathrm{ID}_A$ 和 $X_A$ 发送给 $S$，企图伪装成 $A$ 与 $S$ 进行通信。

2) 收到 $A$ 发送过来的消息后，$S$ 从自己保存的口令文件中取出 $A$ 的验证信息，同时选取 $b\in_R Z_P^*$，计算 $X_S=V^b\oplus V$，将计算的 $X_S$ 发送给 $A$，然后计算：$K_S=(X_A\oplus V)^b=V^{ab}$，$V'_A=H(A,X_S,K_S)$，$V_S=H(S,X_A,K_S)$.

3) 收到 S 发送过来的 $X_S$ 后，$A$ 计算：$K_A=(X_S\oplus V)^a=V^{ab}$，$V_A=(A,X_S,K_A)$，将 $V_A$ 发送给 $B$，然后计算：$V'_S=H(S,X_A,K_A)$.

4) 协议 4)，5) 和正确的协议过程一样，只是最后双方得到的会话密钥都是 $K=H(K_A)=H(K_S)=H(V^{ab})$.

经过上述过程后，攻击者 $E$ 成功地伪装成 $A$ 与服务器共同获得会话密钥 $H(V^{ab})$，而服务器却错误地认为 $E$ 就是 $A$，从而遭受了服务器泄露攻击。通过对上述过程的分析，该协议不能抵抗服务器泄

露攻击是因为攻击者 $E$ 可以首先计算 $X_A$，从而将双方的会话密钥局限在一个特定的形式中，所有攻击者在以后的通信过程中，仅仅利用服务器泄露的验证信息 $V$，而不需要知道用户 $A$ 的口令 $\pi$ 就可以冒充 $A$ 同服务器建立共同的会话密钥 $H(V^{ab})$.

## 3 改进的口令认证密钥交换协议

上述协议之所以会遭受服务器泄露攻击，是因为服务器 $S$ 对用户 $A$ 的验证被攻击者 $E$ 限定在了一个特定的公式当中，所以当攻击者从服务器得到了验证信息 $V$ 之后，就能够躲避服务器 $S$ 对其的身份认证，从而能够得到双方的会话密钥。如果服务器在第 2 步提供一个额外的身份认证就可以打破由于攻击者首先计算 $X_A$ 所造成的验证信息局限性问题。以此为突破口，这里在第 2 步增加了一个扩充验证元信息 $[a+H(V^b)]$，服务器在第 2 步将扩充验证元信息发送给用户，就能够加强用户的身份认证，从而有效地防止了服务器泄露攻击。

$H$，$H_0$，$H_1$ 是抗碰撞单向哈希函数，协议过程如下：

1) $A$ 选择 $a\in_R Z_P^*$，计算：$X_A=g^a\oplus V$，然后将 $\mathrm{ID}_A$ 和 $X_A$ 发送给 $S$.

2) 收到 $A$ 发送过来的消息后，$S$ 从自己保存的口令文件中取出 $A$ 的验证信息，同时选取 $b\in_R Z_P^*$，计算 $c=g^b$；$X_S=g[a+H_0(V^b)]^b\oplus V$，将计算的 $c$，$X_S$ 发送给 $A$，然后计算：$K_S=(X_A\oplus V)^b=g^{ab}$，$V'_A=H_1(A, X_S, K_S)$，$V_S=H_1(S, X_A, K_S)$.

3) 收到 $S$ 发送过来的 $c$，$X_S$ 后，$A$ 计算：$V^b=c^v$，$K_A=(X_S\oplus V)^{[a+H_0(c^v)]^{-1}}=g^{ab}$，$V_A=H_1(A, X_S, K_A)$，将 $V_A$ 发送给 $B$，然后计算：$V'_S=H_1(S, X_A, K_A)$.

4) 收到 $A$ 发送过来 $V_A$ 后，$S$ 验证 $V_A=V'_A$，如果相等，$S$ 确信 $K_A$ 得到证实，然后将 $V_S$ 发送给 $A$.

5) 收到 $S$ 发送 $V_S$ 后，$A$ 验证 $V_S=V'_S$，如果相等，则 $A$ 确信 $K_S$ 得到证实。

6) 从而双方得到共同的会话密钥 $K=H_1(K_A)=H_1(K_S)=H_1(g^{ab})$.

改进的协议在第 2 步服务器收到 $\mathrm{ID}_A$ 和 $X_A$ 之后，计算 $X_S$ 的值修改为 $X_S=g^{[a+H_0(V^b)]^b}\oplus V$，增加了 $a+H_0(V^b)$ 这个扩充验证元，如果用户真的是 $A$ 则能够利用 $v=H(A, S, \pi)$ 和 $c$ 计算得到 $[a+H_0(V^b)]^{-1}$，在 3) 就可计算得出 $g^{ab}$，如果得不到 $g^{ab}$，则第 4 步就无法通过 $S$ 的验证，从而协议停止。假设攻击者 $E$ 冒充 $A$ 与服务器进行通信，$E$ 已经取得了验证信息 $V$，由于大素数困难性问题的存在，$E$ 无法通过 $c$ 得到 $b$ 的值，而要通过第 4) 步的验证必须通过 $v=H(A, S, \pi)$ 和 $c$ 才能得到 $V^b$，所有即使攻击 $E$ 得到了服务器的验证信息 $V$ 也无法得到会话密钥，从而有效地防止了服务器泄露攻击。

## 4 效率和安全性分析

### 4.1 效率分析

从通信开销、存储开销和计算开销分析协议的效率。新协议在通信开销方面和原协议相同，都需要 6 个步骤，需要交互 5 次才能得到会话密钥。存储开销方面比原协议多了对单向哈希函数 $H_0$，$H_1$ 的存储，基本不影响效率。在计算开销方面，新协议多了 4 次乘法运算，效率方面比原协议有所降低，但是这样的计算耗费不大，而且与原协议相比能够得到更高的安全性能。

### 4.2 安全性分析

安全性分析如下：

1) 可抵抗离线字典攻击。攻击者要得到双方共同的会话密钥就必须得到服务器 $S$ 随机选择的数字 $b$，由于大素数求解困难性问题，攻击者无法通过 $c=g^b$ 求得 $b$，因此也就无法得到 $H_1(g^{ab})$.

2) 抵抗服务器泄露攻击。假设攻击 $E$ 取得了服务器 $S$ 对用户的验证信息 $V$，由于大素数求解困难性问题，$E$ 无法通过 $c$ 求得 $b$ 的值，要通过 4) 的验证就必须通过 $v=H(A, S, \pi)$ 和 $c$ 才能得到 $V^b$，得

不到 $b$ 也就无法通过验证，也就得不到会话密钥 $H_1(g^{ab})$，有效地防止了服务器泄露攻击。

3）提供前向安全性。基于 PAKE 协议的前向安全性指的是即使攻击者获得一个或者多个合法用户的口令也不影响以前用该口令建立的会话密钥的安全性。因为该协议的会话密钥为 $H_1(g^{ab})$，而每次通信时都随机地选取 $a$ 和 $b$，所有攻击者无法根据现在的会话密钥来猜测以前的会话密钥，从而很好地提供了前向安全性。

## 5 结论

对一个两方 PAKE 协议所受的服务器泄露攻击作了分析，提出了一个改进的 PAKE 协议，改进的协议和原协议的步骤相同（6 步），仅仅在第 2 和第 3 步多出了 4 次乘法运算，而这样的操作耗费不大，与原协议相比，改进后的协议能够抵抗服务器泄露攻击，抗离线字典攻击，且具有很好的前向安全性。

**[参考文献] (References)**

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

[2] 谭示崇，张宁，王育民. 新的口令认证密钥协商协议[J]. 电子科技大学学报，2008，37 (1)：17-19.
TAN S C, ZHANG N, WANG Y M. A new password-based authenticated key agreement protocol[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(1): 17-19. (in Chinese)

[3] 李光松，韩文报. 不需加密的三方口令认证密钥交换协议[J]. 信息工程大学学报，2005，6 (1)：1-3.
LI G S, HAN W B. Three-party pssword authentication key exchange without encryption[J]. Journal of Information Engineering University, 2005, 6(1): 1-3. (in Chinese)

[4] 胡学先，刘文芬. 对两个三方口令认证密钥交换协议的分析[J]. 信息工程大学学报，2010 ，11 (1)：104-107.
HU X X, LIU W F. Cryptanalysis of two three-party password-based authentication key exchange protocols[J]. Journal of Information Engineering University, 2010 , 11(1) : 104-107. (in Chinese)

[5] 曹琛，高宇航. 改进的三方口令认证密钥交换协议[J]. 计算机工程与应用，2010，46 (16)：88-91.
CAO C, GAO Y H. Improved three-party password-authenticated key exchange protocol[J]. Computer Engineering and Applications, 2010, 46(16): 88-91. (in Chinese)

[6] 柯芳芳，唐西林，章启恒. 对一个口令认证的可攻击性分析及改进[J]. 计算机工程，2010，36 (7)：142-144.
KE F F, TANG X L, ZHANG Q H. Attack analysis and improvement of password authentication protocol[J]. Computer Engineering, 2010, 36(7): 142-144. (in Chinese)

[7] LEE S W, KIM W H, KIM H S, et al. Efficient password-based authenticated key agreement protocol[C]// Computational Science and Its Applications-ICCSA2004. Italy: Springer-Verlag, 2004: 617-626.

[8] SHIM K A, SEO S H. Security analysis of password-authenticated key agreement protocol[C]//Proceeding of 4th International Conference on Cryptology and Network Security-CANS2005. Xiamen: Springer-Verlag, 2005: 49-58.