改进的具有 PFS 特性的口令认证密钥协商方案

汪定[1]，马春光[1]，翁臣[2]，贾春福[2]

（1. 哈尔滨工程大学计算机科学与技术学院，黑龙江 哈尔滨 150001；
2. 南开大学信息技术科学学院，天津 300071）

摘要：身份认证和密钥协商是确保信息系统安全的重要手段，基于智能卡的口令认证密钥协商协议由于实用性较强而成为近期研究热点. 讨论了 Hao 等新近提出的具有完备前向安全性（Perfect Forward Secrecy, PFS）的基于智能卡的远程用户口令认证密钥协商方案，指出该方案无法实现所声称的在非抗窜扰智能卡假设下抗离线口令猜测攻击，对密钥泄露仿冒攻击是脆弱的，并且存在时钟同步问题，不适于分布式网络应用. 给出一个改进方案，用随机数代替时间戳来实现消息的新鲜性，对其进行了安全性和效率分析. 分析结果表明，改进方案弥补了原方案的安全缺陷，保持了较高的效率，适于分布式网络应用环境.

关键词：身份认证；智能卡；口令猜测攻击；密钥泄露仿冒攻击

中图分类号：TP309.08　　**文献标识码：A**

Improved Password-based Key Agreement Scheme with Perfect Forward Secrecy

WANG Ding[1]，MA Chun-guang[1]，WENG Chen[2]，JIA Chun-fu[2]

(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, Heilongjiang, China;
2. College of Information Technology Science, Nankai University, Tianjin 30071, China)

Abstract: With identity authentication and key agreement becoming an essential mechanism to ensure robust system security in distributed networks, smartcard-based remote user password authentication protocols have been studied intensively for their great practicality. This paper points out that a recent smartcard-based password authentication scheme with Perfect Forward Secrecy (PFS) proposed by Hao et al. cannot achieve the claimed security and reports its following flaws: 1) It is vulnerable to offline password guessing attack and key compromise impersonation attack; 2) It has the problems of no poor repairability and time-synchronization. As our main contribution, an improved scheme is presented and analyzed, the analysis shows that our new scheme eliminates the defects of Hao et al.'s scheme while keeping the merit of high performance, suitable for applications in distributed networks.

Key words: Authentication; Smart card; Offline password guessing attack; Key compromise impersonation attack

0　引言

随着电子商务和电子政务的快速发展，在远程用户和服务器之间进行身份认证，是确保分布式网络环境中信息系统安全的重要手段. 在众多的身份认证方式中，基于口令的认证最为简单、方便，且应用最广泛. 但这种身份认证系统中用户常为了方便记忆而选择低信息熵的弱口令，极易遭到离线口令猜测攻击——攻击者通过截获合法用户与服务器间的一些认证交互消息，离线地对口令进行猜测和验证，而不需要用户或服务器的参与. 这种攻击是口令密钥协商协议面临的最严重安全威胁[1]. 关于弱口令、强口令的具体含义详见文献[2]，文献[3]是关于口令密钥协商方案的一个经典综述.

为提高身份认证的安全性和有效性，1993 年 Chang 等[4]首次采用智能卡与口令相结合的技术来设计远程用户身份认证方案，实现双因子认证，即用户只有同时拥有智能卡和知道相应的口令才能认证成功. 随后大量的基于智能卡的远程用户口令认证方案被提出[5-7]，但是这些方案都假设智能卡内敏感信息是安全的，攻击者无法获取. 这个假设在采用了抗窜扰技术的特殊智能卡环境下是成立的，而对于普通智能卡则难以实现. 文献[8-10]的研究表明，普通智能卡内秘密参数信息可通过能耗分析或旁路信息泄露等边信道攻

收稿日期：2012-04-28

基金项目：国家自然科学基金(61073042;61170241)；博士后科研人员落户黑龙江科研启动资助金项目(LBH-Q10141)；北京邮电大学网络与交换技术国家重点实验室开放课题(SKLNST-2009-1-10)

作者简介：汪　定 (1985-)，男，硕士研究生，研究方向为密码学与信息安全. E-mail: wangdingg@mail.nankai.edu.cn
马春光（1974-）,男，教授，博士生导师，研究方向为密码与网络安全. E-mail: chunguangma@hrbeu.edu.cn

击技术而被提取出来. 一旦攻击者获取智能卡内秘密参数信息，可以猜测用户口令，然后利用该用户与远程服务器在公开信道上传输的认证信息来验证猜测的口令的正确性，这些方案便面临着离线口令猜测攻击、仿冒攻击等安全威胁.为应对该问题，近年来出现了一些新的增强型方案[11-13]，但都随后被发现存在这样或那样的安全漏洞[14-17].

2007 年 Wang 等[11]针对文献[5]中方案存在离线口令猜测攻击和仿冒攻击等安全缺陷，提出了一个基于 Hash 函数的高效的远程用户口令认证方案，并宣称他们的改进方案能够防御已知的各种攻击. 随后，Chen 等[15]分析发现 Wang 等方案无法抵抗仿冒攻击和平行会话攻击，然后针对这些安全缺陷提出了改进方案，并声称改进方案适合安全需求较高的应用. 2011 年，Hao 等[16]指出，Chen 等提出的改进方案在非抗窜扰智能卡假设下对离线口令猜测攻击仍然是脆弱的，且未实现前向安全性，然后在 Chen 等方案基础上提出了一个基于 Diffie-Hellman 密钥交换技术的增强型方案. Hao 等宣称他们的增强型方案继承了 Chen 等方案的优点，在非抗窜扰智能卡假设下能够抵御离线口令猜测攻击等众多安全威胁，且实现了完备前向安全性，适于分布式网络环境应用.

但本文分析发现，Hao 等方案[16]仍然存在严重安全缺陷，该方案无法实现所声称的抗离线口令猜测攻击，对密钥泄露仿冒攻击是脆弱的，可修复性较差，且存在时间同步问题，不适合分布式网络环境；然后在保持 Hao 等方案高效、具有 PFS 特性等优势的基础上，给出一个改进方案；最后，详细分析了改进方案的安全性和效率.

1 Hao 等方案简要回顾

Hao 等方案[16]包含四个阶段，即注册阶段、登录阶段、认证阶段和口令更新阶段，方案中所使用的符号及其含义如表 1 所示.

表 1 符号定义

符号	含义	符号	含义
U_i	用户 i	T_H	Hash 运算时间复杂度
S	服务器	T_E	模冥乘运算时间复杂度
ID_i	用户 i 的标识符	$h(\cdot)$	安全散列函数
PW_i	用户的 i 口令	$h_k(\cdot)$	带密钥 k 的安全散列函数
x	服务器主密钥	$\oplus$	按位异或运算
e,d	服务器公钥，私钥	$\|\|$	比特连接运算
$\mathcal{D}$	用户口令空间	$A\rightarrow B:M$	将消息 M 通过普通信道由 A 传送到 B
T_X	异或运算时间复杂度	$A\Rightarrow B:M$	将消息 M 通过安全信道由 A 传送到 B

1.1 注册阶段

R1. 用户 U_i 选择用户名 ID_i 和口令 PW_i，生成随机数 b，并计算 $h(b\oplus PW_i)$.

R2. $U_i\Rightarrow S:\{ID_i, h(b\oplus PW_i)\}$.

R3. 服务器 S 产生 3 个公开参数 p, q, g，其中 p 和 q 是大素数，且 $q\,|\,p-1$，g 是乘法群 $\mathbb{Z}_p^*$ 中阶为 q 的生成元. 然后 S 计算 $P=h(ID_i\oplus x)$，$R=P\oplus h(b\oplus PW_i)$，最后将$\{p, q, g, R, h(\bullet)\ h_k(\bullet)\}$写入智能卡.

R4. $S\Rightarrow U_i$:智能卡.

R5. U_i 将 b 写入智能卡.

1.2 登陆阶段

L1. 用户 U_i 插入智能卡读卡器，输入 ID_i 和 PW_i.

L2. 智能卡生成一个临时交互号 r 和随机数 $r_u\in[1, q-1]$，计算 $R_u=g^{r_u} \bmod p$；然后读取当前时间戳 T_u，计算：

$$P=R\oplus h(b\oplus PW_i),$$

$$C_0=h(ID_i\oplus P)\oplus R_u,$$

$$C_1=P\oplus h(r\oplus b),\quad C_2=h_P(h(r\oplus b)\,\|\,T_u\,\|\,R_u).$$

L3. $U_i \rightarrow S$:{ID_i, C_0, C_1, C_2, T_u}.

1.3 认证阶段

V1. 服务器 S 在时间 T_s 接收到来自 U_i 的认证请求后，检查 ID_i 和 T_u 的有效性，若 ID_i 或 T_u 无效，或者 $T_s - T_u > \Delta T$，或者 $T_s = T_u$，则拒绝登录请求.

V2. S 计算 $P = h(ID_i \oplus x)$，$R_u' = h(ID_i \oplus P) \oplus C_0$，$C_1' = C_1 \oplus P$ 和 $C_2' = h_P(C_1' \| T_u \| R_u)$，然后验证 $C_2' = C_2$ 是否成立. 如果不成立，则 S 拒绝 U_i 的登录请求；否则，S 产生随机数 $r_s \in [1, q-1]$，计算：

$R_s = g^{r_s} \bmod p$，

$W_s = (R_u')^{r_s} \bmod p$，

$K_s = h(W_s \| C_1')$，

$C_3 = h_P((C_1' \oplus T_s) \| P \| R_s)$，

$C_4 = h(ID_i \| P) \oplus R_s$

V3. $S \rightarrow U_i$:{ T_s, C_3, C_4}.

V4. U_i 首先检查 T_s 的有效性，然后计算 $R_s' = C_4 \oplus h(ID_i \| P)$ 和 $C_3' = h_P((h(r \oplus b) \oplus T_s) \| P \| R_s')$，并验证 $C_3' = C_3$ 是否成立. 如果成立，则 U_i 计算 $W_u = (R_s')^{r_u} \bmod p$ 和 $K_u = h(W_u \| h(r \oplus b))$. $K_u = K_s$ 作为 U_i 和 S 间协商的会话密钥, 认证完成.

1.4 口令更新阶段

C1. 执行 2.2 节和 2.3 节的登录阶段和认证阶段，完成双向身份认证.

C2. 智能卡提示用户输入新口令，待用户输入所选择的新口令 PW_i^{new} 后，智能卡计算 $R^{new} = P \oplus h(b \oplus PW_i) \oplus h(b \oplus PW_i^{new})$，并用 R^{new} 替换 R.

2 对 Hao 等方案的安全性分析

攻击者模型. 对于基于智能卡的口令认证密钥协议，传统的攻击者模型一直沿用经典的 Dolev-Yao 模型，即攻击者可以任意监听、截获、插入、修改、阻断流经公开信道中的消息. 近年来，随着边信道攻击技术[8-10]研究的进展，攻击者还可以分析出智能卡内的秘密参数信息. 2012 年，Wang 在文献[17]中首次讨论了存在恶意读卡器的情形，认为攻击者可通过恶意读卡器增加新的能力——获取用户输入的口令，并指出现实中下述两个假设仍然是合理的：1）攻击者无法在合法用户使用恶意读卡器的同时分析出智能卡内秘密参数信息；2）应排除“攻击者先通过恶意读卡器获取用户输入的口令，然后窃取用户智能卡以分析出智能卡内秘密参数信息”这一平凡攻击情形.

安全目标. 文献[3]中列出了理想的口令认证协议应当满足的 9 项安全需求，包括实现双向认证和 PFS，以及能够抵抗口令猜测攻击、DoS 攻击、仿冒攻击、重放攻击、平行会话攻击、窃取验证项攻击和智能卡丢失攻击. 文献[18]指出，除实现上述 9 项安全需求外，认证密钥协商协议还应能够抵抗已知密钥攻击、密钥泄露仿冒攻击和未知密钥共享攻击. Hao 等方案[16]声称能够抵抗离线口令猜测攻，但本文研究发现该方案无法实现这一基本安全目标，并且对密钥泄露仿冒攻击是脆弱的. 此外，Hao 等方案可修复性较差，且存在时间同步问题.

2.1 离线口令猜测攻击

离线口令猜测攻击是基于口令的认证协议面临的最大安全威胁，一个适于实际应用的口令认证方案应能够防御该威胁[19]. 而我们分析发现 Hao 等方案仍无法实现这一安全目标.

由于用户 U_i 的口令 PW_i 由其自主选择，为了方便记忆，PW_i 往往是弱口令[2]. 攻击者通过能耗分析或旁路信息泄露等边信道攻击技术[8-10]，可获得 U_i 的智能卡内秘密参数 R 和 b. 如果攻击者还从公开信道上截获了此前用户 U_i 与服务器 S 间的某次认证请求消息{ID_i, C_0, C_1, C_2, T_u}，可实施离线口令猜测攻击，具体攻击流程如下：

1） 攻击者猜测 U_i 的口令为 PW_i^*；

2） 计算： $P^* = R \oplus h(b \oplus PW_i^*)$，

$R_u^* = C_0 \oplus h(ID_i \oplus P^*)$，

$M = h^*(r \oplus b) = C_1 \oplus P^*$，

$C_2^* = h_{P^*}(h(M) \| T_u \| R_u^*)$；

3） 验证 $C_2^* = C_2$ 是否成立. 如果等式成立，则 PW_i^* 猜测正确；否则转 1）.

用 $|\mathcal{D}|$ 表示用户口令空间大小，上述流程的时间复杂度为 $\mathcal{O}(|\mathcal{D}| * (5T_X + 4T_H))$. 在实际中，$|\mathcal{D}|$ 一般非常有限[23]，攻击能够在多项式时间内完成.

上述攻击能够成功的根本原因在于，用户 U_i 的登录消息 C_0、C_1 和 C_2 之间的隐含关系 $C_2 = h_p(h(C_1 \oplus P) \| T_u \| C_0 \oplus h(ID_i \oplus P))$ 成为了攻击者验证所猜测口令是否正确的验证关系. 一旦攻击者获得 PW_i，利用已获取到的智能卡内秘密参数 R 和 b，便可计算出核心安全参数 $P = R \oplus h(b \oplus PW_i)$. 此后，攻击者可以任意仿冒 U_i 登录服务器 S，或者仿冒服务器 S 对来自 U_i 的认证信息进行响应.

2.2 密钥泄露仿冒攻击

对于带会话密钥协商的认证协议，能抵抗密钥泄露仿冒攻击是一个重要安全属性[18]. 该安全属性关注的是，当通信实体 A 的长期私钥泄露后，攻击者显然能够成功冒充 A 与协议的其它参与者进行通信，然而这一密钥泄露应不能使得攻击者反过来向 A 冒充为其他合法通信实体 B ($B \neq A$).

在 Hao 等方案中，假设服务器 S 的长期私钥 x 泄露. 攻击者可计算出用户 U_i 的核心安全参数 $P = h(ID_i \oplus x)$，其中 ID_i 从公开信道获取. 攻击者计算出 U_i 的核心安全参数 P 后，即使无法得到 U_i 的智能卡，仍可以随时发起用户仿冒攻击：

1） 攻击者选取随机数 X, $r_m \in [1, q-1]$，读取当前时间戳 T_m，计算：

$R_m = g^{r_m} \bmod p$

$C_0 = h(ID_i \oplus P) \oplus R_m$，

$C_1 = P \oplus X$，

$C_2 = h_P(X \| T_m \| R_u)$.

2） 攻击者向服务器发送{ID_i, C_0, C_1, C_2, T_m}.

3） 当收到服务器的响应消息{ T_s, C_3, C_4}后，攻击者计算: $R_s' = C_4 \oplus h(ID_i \| P)$，

$W_u = (R_s')^{r_u} \bmod p$，

$K_u = h(W_u \| X)$.

当服务器 S 收到来自 U_i（实际上是攻击者）的登录消息{ID_i, C_0, C_1, C_2, T_m }后，显然 ID_i 和 T_m 的合法性检查将顺利通过；由于攻击者计算 C_0, C_1, 和 C_2 时使用的参数 $P = h(ID_i \oplus x)$，与 S 计算 R_u' 和 C_1' 时使用的 P 的值完全相同，S 计算出的 C_2' 将与收到的 C_2 相等. 因此 S 将接受 U_i（实际上是攻击者）的登录请求，并响应{ T_s, C_3, C_4}. 攻击者在收到 S 的响应后，在上述步骤 3）中成功计算会话密钥 K_u, 针对 U_i 的仿冒攻击完成.

通过上述攻击流程可看出，当服务器 S 的长期私钥 x 后，即使无法得到 U_i 的智能卡，攻击者仍可在 $\mathcal{O}(2T_E + 5T_X + 4T_H)$ 时间内成功仿冒 U_i.

2.3 不可修复性问题

当攻击者通过 2.1 节中的攻击方法获取用户 U_i 的口令 PW_i 后，或者如 2.2 节所述当服务器 S 的长期私钥 x 泄露后，攻击者可成功计算出 U_i 的核心安全参数 $P = R \oplus h(b \oplus PW_i) = h(ID_i \oplus x)$，然后可如 2.2 节所述成功仿冒 U_i 登录 S.

现在的问题是，当用户 U_i 发现自己的核心安全参数 P 泄露后却无能为力，即使通过更新口令也不能修复或解决该问题，因为 P 的值与用户口令无关. 另一方面，由于 P 的值只与用户 U_i 身份标识 ID_i 和服务器 S 的长期私钥 x 相关，若要更新 P 的值，必须更换 ID_i 或 x. 然而这样做对用户和服务器来讲都是不合理的：1）服务器长期私钥 x 参与了系统所有用户安全参数的计算，仅因为一个用户的安全问题而更换 x，代价十分昂贵；2）用户通常在许多应用系统中采用相同的身份标识 ID，且很多情况下，应用系统将用户 ID

与用户身份绑定，更改用户身份标识 ID 不切实际. 因此，该方案存在可修复性问题.

2.4 时间同步问题

在分布式网络中进行时间同步，需要部署额外的时间同步机制或基础设施，代价昂贵；而且由于网络拓扑结构的动态性，基于中央控制的同步机制难以实现，而基于分散式同步机制的精确性与理想情况相差甚远[20-21]. 另一方面，现实网络中的时延具有不确定性，基于时间戳机制的协议仍然可能遭受重放攻击[22]. 因此，基于时间戳机制来提供消息新鲜性以抵抗重放攻击的协议不适合分布式网络环境. Wang等方案[11]、Chen等方案[15]和 Hao 等方案[16]均采用时戳机制来提供消息的新鲜性，因此这些方案均存在时间同步问题.

综上所述， Hao 等方案存在时间同步问题，未实现所宣称的“适合分布式网络环境应用”.

3 改进方案

本节在保持 Hao 等方案具有 PFS 等优势的基础上，根据节 2 中的安全性分析，提出一个改进方案，其先进性主要体现在以下三点：1）采用“加盐”思想[23]来抵抗离线口令猜测攻击，未增加计算复杂度；2）通过在用户 U_i 的智能卡和服务器间共享一个随机数 N_i，一并解决可修复性和密钥泄露仿冒攻击问题；3）采用随机数机制代替时间戳机制来提供消息的新鲜性，解决时间同步难题.

改进方案分为注册阶段、登录阶段、认证阶段、口令更新阶段和重注册阶段. 其中，重注册阶段用以实现系统可修复性，符号含义如表 1.

3.1 注册阶段

R1. 用户 U_i 选择用户名 ID_i 和口令 PW_i，生成随机数 b，并计算 $h(b \oplus PW_i)$.

R2. $U_i \Rightarrow S:\{ID_i, h(b \oplus PW_i)\}$.

R3. 服务器 S 产生 3 个公开参数 p, q, g，其中 p 和 q 是大素数，且 q 整除（ $p-1$），g 是乘法群 $\mathbb{Z}_p^*$ 中阶为 q 的生成元. 然后 S 计算 $P = h(ID_i \oplus N_i \oplus x)$， $R = P \oplus h(b \oplus PW_i)$. 其中， N_i 是 S 产生的与 ID_i 对应的随机数. S 在后台数据库中增加一个新的条目（ID_i, N_i ），并将{ $p, q, g, N_i, R, h(\bullet)$ $h_k(\bullet)$ }写入智能卡.

R4. $S \Rightarrow U_i$:智能卡.

R5. U_i 将 b 写入智能卡.

3.2 登陆阶段

L1. 用户 U_i 插入智能卡读卡器，输入 ID_i 和 PW_i.

L2. 智能卡生成一个随机数 $r_u \in [1, q-1]$，计算：

$$R_u = g^{r_u} \bmod p,$$
$$P = R \oplus h(b \oplus PW_i),$$
$$C_1 = h(ID_i \oplus P) \oplus R_u.$$

L3. $U_i \rightarrow S:\{ID_i, C_1\}$.

3.3 认证阶段

V1. 服务器 S 接收到来自 U_i 的认证请求后，检查 ID_i 的有效性，若 ID_i 无效，则拒绝登录请求.

V2. S 从后台数据库查找与 ID_i 对应的 N_i, 计算 $P = h(ID_i \oplus N_i \oplus x)$ 和 $R_u' = h(ID_i \oplus P) \oplus C_1$.然后产生随机数 $r_s \in [1, q-1]$，计算：

$$R_s = g^{r_s} \bmod p,$$
$$W_s = (R_u')^{r_s} \bmod p,$$
$$K_s = h(ID_i \| N_i \| R_u' \| R_s \| W_s),$$
$$C_2 = h(ID_i \| N_i \| R_s \| K_s).$$

V3. $S \rightarrow U_i:\{R_s, C_2\}$.

V4. U_i 收到 S 的响应后，计算：

$W_s' = (R_s)^{r_u} \bmod p$，

$K_u = h(ID_i \| N_i \| R_u \| R_s \| W_s')$，

$C_2' = h(ID_i \| N_i \| R_s \| K_u)$.

接着，用户 U_i 验证 $C_2' = C_2$ 是否成立. 如果不成立，则 U_i 结束会话；否则，U_i 计算 $C_3 = h(R_u \| R_s \| ID_i \| N_i \| K_u)$.

V5. $U_i \rightarrow S$:{ C_3 }.

V6. S 计算 $C_3' = h(R_u' \| R_s \| ID_i \| N_i \| K_s)$，并验证 $C_3' = C_3$ 是否成立. 如果成立，则 U_i 和 S 完成双向认证并成功协商会话密钥 $SK = K_u = K_s$.

3.4 口令更新阶段

C1. 执行 3.2 节和 3.3 节的登录阶段和认证阶段，完成双向身份认证.

C2. 智能卡提示用户输入新口令，待用户输入新口令 PW_i^{new} 后，智能卡计算 $R^{new} = P \oplus h(b \oplus PW_i) \oplus h(b \oplus PW_i^{new})$，并用 R^{new} 替换 R.

3.5 重注册阶段

当智能卡丢失，或者发现参数 P 泄露、口令 PW_i 被破解时，用户 U_i 使用原用户名 ID_i 和新口令 PW_i^{new} 到服务器重新注册，服务器为 U_i 产生一个新的随机数 N_i'，具体过程与注册阶段相同.

4 改进方案的分析

由于改进方案采用随机数机制代替时间戳机制来提供消息的新鲜性，不存在时间同步难题. 安全性和效率是衡量基于口令认证方案优劣的两个最重要指标[3]，下面分别从这两方面进行分析.

4.1 安全性分析

由于改进方案基于 Hao 等方案，继承了 Hao 等的方案所具有的安全性，例如实现双向认证和完备前向安全性，抵抗重放攻击、仿冒攻击、拒绝服务攻击等，在这一部分我们仅对增强的安全特性进行分析.

4.1.1 抵抗离线口令猜测攻击

假设攻击者 $\mathcal{A}$ 通过能耗分析或旁路信息泄露等边信道攻击技术[9-10]，获得了 U_i 的智能卡内秘密参数 N_i, R 和 b. 假设 $\mathcal{A}$ 还截获了{ID_i, C_1 }、{ R_s, C_2}和{C_3 }. 在认证过程中，只有参数 P 中包含 PW_i 的信息，与攻击 Hao 等方案一样，$\mathcal{A}$ 必须首先猜测口令为 PW_i^*，然后计算 $P^* = R \oplus h(b \oplus PW_i^*)$，再通过某种途径验证所计算的 P^* 的正确性来检验所猜测的 PW_i^* 的正确性.

由于随机数 $r_u \in [1, q-1]$，故 $R_u = g^{r_u} \bmod p$ 也是一个随机数，取值范围为 $[1, p-1]$. C_1 是 $h(ID_i \oplus P)$ 与随机数 R_u 进行异或运算的结果，故通过这种“加盐”操作将 $\mathcal{A}$ 的口令猜测空间大小由 $|\mathcal{D}|$ 增大到 p，使 $\mathcal{A}$ 仅由 C_1 来猜测口令不可行；C_2 是 R_u、K_s 与 ID_i 等进行 Hash 运算后的结果，由于 R_u 的参与，将 $\mathcal{A}$ 的口令猜测空间大小由 $|\mathcal{D}|$ 增大到 $|\mathrm{Hash}|$，其中 $|\mathrm{Hash}|$ 表示 Hash 运算的象空间，这样使 $\mathcal{A}$ 仅由 C_2 来猜测口令不可行；同 C_2 一样，C_3 也是由 R_u、$K_s = K_u$ 与 ID_i 等进行 Hash 运算后的结果，由于 R_u 的参与，这样使 $\mathcal{A}$ 仅由 C_3 来猜测口令也不可行.

另一方面，由于安全 Hash 函数的假设，C_2 与 C_3 之间不存在相互关系，C_1 与 C_2、C_1 与 C_3 之间的关系分别如下：

$C_2 = h(ID_i \| N_i \| R_s \| (C_1 \oplus h(ID_i \| P))^{r_s} \bmod p)$，

$C_3 = h(C_1 \oplus h(ID_i \| P) \| R_s \| ID_i \| N_i \| (C_1 \oplus h(ID_i \| P))^{r_u} \bmod p)$. 由此不难推出：$\mathcal{A}$ 利用 C_1 与 C_2、C_1 与 C_3、C_2 与 C_3 之间的关联关系进行离线口令猜测攻击，其口令猜测空间大小为 $\min\{|\mathrm{Hash}|, q\}$.

综上所述，$\mathcal{A}$ 的口令猜测空间大小为

$$|PW_i^*| = \min\{p, q, |\mathrm{Hash}|\}$$

即改进方案通过“加盐”操作将攻击者 $\mathcal{A}$ 的口令猜测空间大小 $|PW_i^*|$ 由 $|\mathcal{D}|$ 扩展到 $\min\{p, q, |\mathrm{Hash}|\}$，如当 Hash

函数取 SHA-1 时，$|PW_i^*| \geq 2^{160}$. 因此，改进方案可以抵御离线口令猜测攻击.

4.1.2 抵抗密钥泄露仿冒攻击

假设服务器S的长期私钥x泄露. 因为攻击者$\mathcal{A}$不知道N_i的值，$\mathcal{A}$将无法计算出用户U_i的安全参数$P=h(ID_i \oplus N_i \oplus x)$. 因此，$\mathcal{A}$无法仿冒用户$U_i$来欺骗服务器$S$. 另一方面，假设用户$U_i$的口令泄露. 同样由于攻击者$\mathcal{A}$不知道$N_i$的值，$\mathcal{A}$将无法计算出用户$U_i$的安全参数$P=h(ID_i \oplus N_i \oplus x)$. 因此，$\mathcal{A}$无法仿冒服务器$S$来欺骗用户$U_i$.

综上可得，改进方案可抗密钥泄露仿冒攻击.

4.1.3 可修复性

当智能卡丢失，或者发现参数P泄露、口令PW_i被破解时，用户U_i可使用原用户名ID_i和新口令PW_i^{new}到服务器重新注册，即运行3.5节的重注册阶段. 因此，改进方案实现了可修复性.

4.2 效率分析

根据计算复杂性理论，远程用户双向认证方案的效率主要取决于交互的轮数、通信量、计算量和存储量. 通信量主要指传输的信息量；计算量主要取决于模幂乘运算T_E、模逆运算T_I、Hash运算T_H，其中$T_E \approx T_I \approx 600T_H$[24]，其余的计算量如“$\oplus$”、“$||$”可忽略；存储量主要指用户端所需要的静态存储空间. 考虑到注册往往是事先完成的，并且用户注册的频率要远远低于用户登录认证的频率，因此方案的效率主要取决于登录阶段和认证阶段. 不失一般性，假设Hash函数，典型的如SHA-1，其散列值为160 bit，系统生成的随机数、时间戳为160 bit，用户ID和口令PW长度为128 bit，p, q和g长度均为1024 bit. 几个针 Wang 等方案[11]的改进方案效率比较如表2所示.

由表 2 对比可知：改进方案和 Chung 等方案为了克服分布式网络中时间同步问题，采用随机数机制来提供消息的新鲜性，需要 3 次交互；改进方案各效率指标均优于 Chung 等方案和 Hao 等方案；为实现 PFS，改进方案基于 Diffie-Hellman 密钥交换技术，相较 Tsai 等方案仅在服务器端增加了一次模幂乘运算和 896 bit 的存储量，对于资源相对充足的服务器来说是可以承受的. 综合来看，改进方案的实用性相较 Hao 等方案、Chung 等方案和 Tsai 等方案大大提高，更适合于分布式网络应用环境.

表 2　相关远程用户口令认证方案的性能比较

方案	交互次数	计算量		通信量/bit		存储量/bit	可修复性	PFS
		用户端	服务器	用户端	服务器			
Hao 等方案[16]	2 *	$2T_E+7T_H$	$2T_E+6T_H$	1632	1344	3392	否	是
Chung 等方案[12]	3	$2T_E+T_I+6T_H$	$3T_E+T_I+6T_H$	2336	1344	3392+ **	是	是
Tsai 等方案[13]	2 *	$2T_E+5T_H$	T_E+5T_H	1504	288	3232	是	否***
改进方案	3	$2T_E+5T_H$	$2T_E+4T_H$	1312	1184	3552	是	是

注：* Hao 等方案和 Tsai 等方案基于时间戳机制，其余两个方案基于随机数机制；

** Chung 等方案的智能卡中除了存储 3232 bit 的数据外，还存储了一个长度未定的随机字符串.

*** 文献[14]指出 Tsai 等方案无法实现完备前向安全性（PFS）.

5 结 论

确保密码协议的安全性是一个公开难题，对已有认证协议的分析旨在为协议的设计提供更好的参考和借鉴. 本文首先分析了 Hao 等方案的安全性，指出该方案无法实现所宣称的抗离线口令猜测攻击，对密钥泄露仿冒攻击是脆弱的，且存在不可修复性和时间同步问题，不适于分布式网络应用；然后在保持 Hao 等方案高效等优势的基础上，给出了一个改进方案. 安全性分析表明，改进方案弥补了 Hao 等方案的安全缺陷，能够实现理想口令认证协议应当满足的 9 项主要安全需求；效率分析表明，改进方案在克服 Hao 等方案缺陷的同时保持了高效性，不需要时间同步机制，更适合于分布式网络应用环境.

需要指出的是，改进方案的简要安全性分析仍然是基于启发式的，利用可证明安全理论对改进方案安全性进行严格的形式化证明具有重要意义. 但正如文献[17]指出的，在基于智能卡的口令认证协议领域目前尚没有一个公认合理的攻击者模型，因而也就缺乏形式化证明的基础. 因此，对攻击者模型的研究将是我们下一步工作重点.

参考文献:

[1] 冯登国, 陈伟东. 基于口令的安全协议的模块化设计与分析[J]. 中国科学(E辑), 2007, 37(2):223–237.

[2] 秦小龙, 杨义先. 强口令认证协议的组合攻击[J]. 电子学报, 2003, 31(7):1043–1045.

[3] TSAI C S, LEE C C, HWANG M S. Password Authentication Schemes: Current Status and Key Issues[J]. International Journal of Network Security, 2006, 3(2):101–115.

[4] CHANG C C, WU T C. Remote password authentication with smart cards[J]. IEE Proceedings-E Computers and Digital Techniques, 1993, 138(3):165–168.

[5] KU W C, CHEN S M. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 204–207.

[6] WANG Y Y, LIU J Y, XIAO F X, et al. A more efficient and secure dynamic ID-based remote user authentication scheme[J]. Computer Communications, 2009, 32(4): 583–585.

[7] Khan M K, Kim S K, Alghathbar K. Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme’[J]. Computer Communications, 2011, 34(3): 305-309.

[8] KOCHER P, JAFFE J, JUN B. Differential Power Analysis[C]//Proceedings of Advances in Cryptology- CRYPTO’99, California, USA, August 15–19, Springer-Verlag, 1999: 388–397.

[9] MESSERGES T S, DABBISH E A, SLOAN R H. Examining Smart-Card Security under the Threat of Power Analysis Attacks[J]. IEEE Transactions on Computers, 2002, 51(5): 541–552.

[10] MANGARD S, OSWALD E, STANDEXT F X. One for all-all for one: unifying standard differential power analysis attacks[J]. IET Information Security, 2011, 5(2):100–110.

[11] Wang X M, Zhang W F, Zhang J S, Khan M K. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards[J]. Computer Standards and Interfaces, 2007, 29(5): 507–512.

[12] CHUNG H R, KU W C, TSAUR M J. Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environ- ments[J]. Computer Standards & Interfaces, 2009, 31(4): 863–868.

[13] TSAI J L, WU T C, TSAI K Y. New dynamic ID authentication scheme using smart cards[J]. International Journal of Communication Systems, 2010, 23(12): 1449–1462.

[14] WU Shuhua, ZHU Yuefei, PU Qiong. Robust smart-cards-based user authentication scheme with user anonymity[J]. Security and Communication Networks, 2012, 5(2):236–248.

[15] ChEN T H, HSIANG H C, SHIH W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Generation Computer Systems, 2011, 27(4): 377–380.

[16] 郝卓，俞能海. 一个具有完备前向安全性的基于口令认证密钥协商方案[J]. 中国科学技术大学学报，2011, 41(7):589–593.

[17] WANG Y G. Password Protected Smart Card and Memory Stick Authentication Against Off-line Dictionary Attacks[C]//Proceedings of the 27th IFIP International Information Security and Privacy Conference, Heraklion, Greece, Jun 4–6, Springer- Verlag, 2005: 546–566.

[18] KRAWCZYK H. HMQV: A high-performance secure Diffie-Hellman protocol[C]. Advances in Cryptology- CRYPTO’05, California, USA, August 14–18, 2005: 546–566.

[19] MA Chunguang, WANG Ding, ZHANG Qiming. Cryptanalysis and Improvement of Sood et al.'s Dynamic ID-based Authentication Scheme[C]// Proceedings of ICDCIT’12, LNCS 7154, Springer- Verlag, 2012: 141–152.

[20] BALDONI R, CORSARO A, QUERZONI L. Coupling- based internal clock synchronization for large-scale dynamic distributed systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(5): 607–619.

[21] HAN J, JEONG D K. A practical implementation of IEEE 1588-2008 transparent clock for distributed measure- ment and control systems[J]. IEEE Transactions on Instrumentation and Measurement, 2010, 59(2): 433–439.

[22] GONG L. A security risk of depending on synchronized clocks. ACM Operating System Review[J]. 1992, 26(1): 49–53.

[23] 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, California, IEEE, 1992: 72–84.

[24] FERGUSON N, SCHNEIER B, KOHNO T. Cryptography Engineering: Design Principles and Practical Applications[M]. New York: John Wiley & Sons, 2010: 326–344.