一种适于受限资源环境的远程用户认证方案的分析与改进

汪 定*①③ 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 哈尔滨 150001)
②(南开大学信息技术科学学院 天津 300071)
③(解放军汽车管理学院训练部 蚌埠 233011)

摘 要：该文讨论了 Fang 等人(2011)新近提出的一个安全高效的基于智能卡的远程用户口令认证方案，指出原方案无法实现所声称的抗离线口令猜测攻击，对平行会话攻击和已知密钥攻击是脆弱的，并且存在用户口令更新友好性差问题。给出一个改进方案，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，适用于安全需求较高的资源受限应用环境。

关键词：身份认证；智能卡；离线口令猜测攻击；平行会话攻击
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2012)10-2520-07
DOI: 10.3724/SP.J.1146.2012.00376

Cryptanalysis and Improvement of a Remote User Authentication Scheme for Resource-limited Environment

Wang Ding①③ Ma Chun-guang① Weng Chen② Jia Chun-fu②
①(*College of Computer Science and Technology*, *Harbin Engineering University*, *Harbin* 150001, *China*)
②(*College of Information Technology Science*, *Nankai University, Tianjin* 300071, *China*)
③(*Department of Training*, *Automobile Management Institute of PLA*, *Bengbu* 233011, *China*)

Abstract: Recently Fang *et al.* (2011) proposed a password-based remote user authentication scheme using smart cards for resource-constrained environment, and claimed that their scheme was secure and practical. However, it is found that their scheme can not achieve the claimed security, it is vulnerable to offline password guessing attack, parallel session attack and known key attack. In addition, the password change phase of their scheme is not user-friendly and practical. Consequently, an improved scheme is presented and analyzed, the analysis shows that new scheme eliminates the defects of Fang *et al.*'s scheme while keeping the merit of high performance, suitable for resource-constrained and security-concerned application scenarios.

Key words: Authentication; Smart card; Offline password guessing attack; Parallel session attack

1 引言

随着电子商务、电子医务和电子政务的快速发展，信息系统对安全性的需求日益提高，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基本手段。为在开放信道中识别和证实远程用户身份，出现了多种身份认证技术，基本可分为 3 类：(1)基于用户所知道的秘密信息，比如口令、PINs、私钥等；(2)基于用户所持有的身份令牌，比如智能卡、加密卡、USB-key 等；(3)基于用户所具有的独特生物特征，比如掌形、指纹、笔迹等。这些身份认证技术各有优劣，但相对而言，基于口令的认证由于其简单有效、费用低廉、灵活方便，而成为应用最为广泛的一种身份认证方式。但用户常为了方便记忆而选择低信息熵的弱口令，如生日、电话号码、英文单词等，使这种身份认证系统面临一种严重安全威胁 —— 离线口令猜测攻击[1]。弱口令、强口令的具体含义详见文献[2]，文献[3]是关于口令认证协议的一个经典综述。

传统的基于口令的身份认证方案的另一缺陷是，认证服务器端需要存储口令验证表项，因而带来了众多安全隐患和管理难题[4]。为提高身份认证的安全性和有效性，大量的基于智能卡与口令相结合的双因子身份认证方案被提出[5−8]。这些方案都假设攻击者无法获取智能卡内存储的秘密参数信息，但相关研究表明，普通智能卡内敏感信息可通过能

2012-04-05 收到，2012-06-20 改回
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基金(LBH-Q10141)和北京邮电大学网络与交换技术国家重点实验室基金(SKLNST-2009-1-10)资助课题
*通信作者：汪定 wangdingg@mail.nankai.edu.cn

耗分析、旁路信息泄露或逆向工程等边信道攻击技术而被提取出来[9,10]。一旦智能卡内敏感参数信息为攻击者所获取，这些方案便面临着离线口令猜测攻击、仿冒攻击、拒绝服务攻击等安全威胁。为解决这一问题，近期提出了一些基于非抗窜扰智能卡假设的增强型方案[11–13]，但都随后被指出存在这样或那样的安全缺陷[14–17]。

2007 年 Wang 等人[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威胁。2009 年 Chung 等人[14]分析发现 Wang 等人方案仍然无法抵抗离线口令猜测攻击和仿冒攻击，然后针对这些安全缺陷提出了改进方案。但 Chung 等人改进方案的安全性基于有限域上离散对数难解性，在用户端需要进行两次大指数模幂乘运算，不适合资源受限环境应用。2011 年 Fang 等人[15]针对 Wang 等人方案的安全脆弱性和不可修复性也提出了一个改进方案，宣称他们的改进方案在保持高效性的同时，克服了原方案中的离线口令猜测攻击、仿冒攻击等众多安全缺陷，适于资源受限环境。

本文首先分析了 Fang 等人[15]方案的安全性，指出该方案无法实现所声称的抗离线口令猜测攻击，对已知密钥攻击和平行会话攻击是脆弱的，且存在用户口令更新过程友好性差问题；然后在保持 Fang 等人方案优势的基础上，提出了一个改进方案；最后，详细分析了改进方案的安全性和效率。

2　Fang等人方案简要回顾

Fang 等人[15]方案包含 4 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。

2.1 注册阶段

*R*1: 用户 U_i 选择用户名 ID_i 和 PW_i，生成随机数 b，并计算 $h(b\oplus \mathrm{PW}_i)$。

表 1 符号定义

符号	含义	符号	含义
U_i	用户 i	$h(\cdot)$	安全散列函数
S	服务器	$h_k(\cdot)$	带密钥 k 的安全散列函数
ID_i	用户 i 的标识符	$\oplus$	按位异或运算
PW_i	用户的 i 口令	$\|\|$	比特连接运算
x	服务器主密钥	$A\rightarrow B:M$	将消息 M 通过普通信道由 A 传送到 B
e,d	服务器公钥，私钥	$A\Rightarrow B:M$	将消息 M 通过安全信道由 A 传送到 B

*R*2: $U_i\Rightarrow S:\{\mathrm{ID}_i, h(b\oplus \mathrm{PW}_i)\}$。

*R*3: 服务器 S 产生随机数 N_i，计算 $k=h(\mathrm{ID}_i\oplus x\oplus N_i)$，$R=k\oplus h(b\oplus \mathrm{PW}_i)$，然后将$\{R, h(\cdot), h_k(\cdot)\}$写入智能卡，并在后台数据库中保存新条目$\{\mathrm{ID}_i, N_i\}$。

*R*4: $S\Rightarrow U_i$:智能卡。

*R*5: U_i 将 b 写入智能卡。

2.2 登陆阶段

*L*1: 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

*L*2: 智能卡计算 $k=R\oplus h(b\oplus \mathrm{PW}_i)$，产生随机数 r，读取当前时间戳 T_u，并计算 $C_1=k\oplus h(r\oplus b)$ 和 $C_2=h_k(h^2(r\oplus b)\oplus T_u)$。

*L*3: $U_i\rightarrow S:\{\mathrm{ID}_i, C_1, C_2, T_u\}$。

2.3 认证阶段

*V*1: 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 $T_s-T_u>\Delta T$，则拒绝登录请求；否则，S 根据 ID_i，从后台数据中读取与 ID_i 对应的 N_i。

*V*2: S 计算 $k=h(\mathrm{ID}_i\oplus x\oplus N_i)$，$C_1^{'}=C_1\oplus k$ 和 $C_2^{'}=h_k(h(C_1^{'})\oplus T_u)$，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 计算 $C_3=h_k(C_1^{'}\oplus T_s)$。

*V*3: $S\rightarrow U_i:\{C_3, T_s\}$。

*V*4: U_i 检查 T_s 的有效性，然后计算 $C_3^{'}=h_k(h(r\oplus b)\oplus T_s)$，并验证 $C_3^{'}=C_3$ 是否成立。如果成立，则 U_i 和 S 间共享会话密钥 $\mathrm{SK}=h(r\oplus b)$，认证完成。

2.4 口令更新阶段

*C*1: 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

*C*2: 智能卡产生随机数 r_c，读取当前时间戳 T_u，计算 $k{=}R\oplus h(b\oplus \mathrm{PW}_i)$，$m_1=k\oplus r_c$ 和 $m_2=h_k(h(r_c)\oplus T_u)$。

*C*3: $U_i\rightarrow S:\{\mathrm{ID}_i, m_1, m_2, T_u\}$。

*C*4: 服务器 S 在时间 T_s 接收到来自 U_i 的口令更新请求后，检查 ID_i 和 T_u 的有效性，若 ID_i 或 T_u 无效，或者 $T_s-T_u>\Delta T$，则拒绝口令更新请求；否则，S 根据 ID_i，从后台数据中读取与 ID_i 对应的 N_i。

*C*5: S 计算 $k=h(\mathrm{ID}_i\oplus x\oplus N_i)$，$m_1^{'}=m_1\oplus k$ 和 $m_2^{'}=h_k(h(m_1^{'})\oplus T_u)$，然后验证 $m_2^{'}=m_2$ 是否成立。如果不成立，则 S 拒绝 U_i 的口令更新请求。

*C*6: S 产生随机数 N_i^{new}，计算 $k_{\mathrm{new}}=h(\mathrm{ID}_i\oplus x\oplus N_i^{\mathrm{new}})$，$m_3=k\oplus k_{\mathrm{new}}$ 和 $m_4=h_k(h(k_{\mathrm{new}})\oplus T_s)$。

*C*7: $S\rightarrow U_i:\{m_3, m_4, T_s\}$。

*C*8: U_i 检查 T_s 的有效性，然后计算 $m_3^{'}=k\oplus m_3$ 和 $m_4^{'}=h_k(h(m_3^{'})\oplus T_s)$，并验证 $m_3^{'}=m_3$ 是否成立。如果成立，则 U_i 选择新口令 $\mathrm{PW}_i^{\mathrm{new}}$，计算 $m_5=h_{m_3^{'}}(m_4)$ 和 $R_{\mathrm{new}}=k_{\mathrm{new}}\oplus h(b\oplus \mathrm{PW}_i^{\mathrm{new}})$，将 R

在智能卡中备份，然后用 R_{new} 替换 R。

C9: $U_i \rightarrow S$:{ m_5 }。

C10: S 计算 $m_5^{'} = h_{k_{\text{new}}}(m_4)$，验证 $m_5^{'} = m_5$ 是否成立。如果不成立，则 S 拒绝 U_i 的口令更新请求；否则，S 用 N_i^{new} 替换 N_i。

3 Fang等人方案安全性分析

文献[3]中列出了理想的基于智能卡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前向安全性，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、Stolen-Verifier 攻击和智能卡丢失攻击。Fang 等人方案声称能够抵抗离线口令猜测攻击，但我们的研究发现该方案无法实现这一安全目标，并且对平行会话攻击和已知密钥攻击是脆弱的。此外，Fang 等人方案的口令更新阶段为防御 DoS(Denial of Service)攻击，在一段时期内需要用户同时记忆新旧两个口令，用户友好性较差。

3.1 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，一个实用的口令认证方案应能够防御该威胁[13]。而我们分析发现 Fang 等人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[9,10]，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{ $\text{ID}_i, C_1, C_2, T_u$ }，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 $k^* = R \oplus h(b \oplus \text{PW}_i^*)$，$M = h^*(r \oplus b) = C_1 \oplus k^*$ 和 $C_2^* = h_{k^*}(h(M) \oplus T_u)$；

(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)。

由于用户口令空间的局限性，上述流程能够在多项式时间内完成。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 $k = R \oplus h(b \oplus \text{PW}_i)$。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。

事实上，文献[18]已证明为抵抗离线口令猜测攻击，口令认证协议必须采用公钥技术，故仅基于散列函数安全性的口令认证方案不能抵抗该攻击。

3.2 已知密钥攻击

对于带会话密钥协商的认证协议，能抵抗已知密钥攻击是一个重要安全属性[19]。该安全属性关注的是，某次会话的会话密钥的泄露会不会影响到其它会话的安全性。

假设 U_i 和 S 的第 j 次会话的会话密钥 $\text{SK}_j = h(r \oplus b)$ 泄露，攻击者再根据从公开信道获取的该次登录消息 C_1^j，则可计算出秘密参数 $k = C_1^j \oplus \text{SK}_j$。攻击者获取秘密参数 k 后，可以恢复出 U_i 和 S 间任意会话 t 的会话密钥 $\text{SK}_t = k \oplus C_1^t$，其中 C_1^t 从公开信道截获。因此，Fang 等人方案不能抗已知密钥攻击。

实际上，攻击者获取秘密参数 k 后，即使无法得到 U_i 的智能卡，仍可以随时发起仿冒攻击。一方面，攻击者构造合法的登录消息{ $\text{ID}_i, C_1^{'}, C_2^{'}, T_u$ }仿冒 U_i 登录 S，其中 $C_1^{'} = k \oplus h(X)$ 和 $C_2^{'} = h_k(h^2(X) \oplus T_u)$，$X$ 随机选取，T_u 为当前时间戳；另一方面，攻击者也可构造合法的认证响应消息{ $C_3^{'}, T_s$ }假冒 S 对来自 U_i 的认证信息进行响应，其中 $C_3 = h_k(C_1^{'} \oplus T_s) = h_k((C_1 \oplus k) \oplus T_s)$，$T_s$ 为当前时间戳。

3.3 平行会话攻击

设用户 U_i 第 j 次口令更新过程的步骤 C7 中，服务器 S 向 U_i 发送响应消息{ m_3^j, m_4^j, T_s^j }。假设攻击者 $\mathcal{A}$ 截获了该消息，那么 $\mathcal{A}$ 及时发起一个同服务器 S 的新的认证会话，可成功仿冒用户 U_i，具体攻击流程如下：

(1)攻击者 $\mathcal{A}$ 向服务器 S 发送认证请求消息{ $\text{ID}_i, m_3^j, m_4^j, T_s^j$ }，其中 ID_i 也是先前从公开信道中截获的。

(2)由于 m_3^j 和 m_4^j 分别与 C_1 和 C_2 有着完全相同的结构，且 T_s^j 是有效的，服务器 S 将接受来自“用户 U_i ”的认证请求，并响应{ C_3, T_s }。

(3)攻击者 $\mathcal{A}$ 截获{ C_3, T_s }并丢弃。

上述攻击过程的步骤 2 中，服务器 S 认为认证请求来自“用户 U_i ”，而实际上该请求来自攻击者 $\mathcal{A}$，用户 U_i 并不知情，而且服务器 S 和用户 U_i 都觉察不到异常的存在。需要注意的是，攻击者 $\mathcal{A}$ 虽然成功欺骗了服务器 S，但 $\mathcal{A}$ 并不知道协商的会话密钥，因而 $\mathcal{A}$ 在认证协议完成之后不能进一步欺骗 S。虽然攻击造成的危害有限，但仍然违背了认证协议安全运行的“匹配会话”的基本原则[20]。

3.4 用户友好性较差

在口令更新阶段，如果消息{ m_5 }在网络中丢失或被恶意阻断、篡改，则服务器端将不会更新认证参数，这将导致用户端和服务器端认证参数不一致，此后用户将无法正常登录 S。为解决这一问题，Fang 等人方案要求在用 R_{new} 替换 R 前，先将 R 在智能卡中备份（设此时为时刻 T_1），以便在用户端和服务器端认证参数不一致时可用旧口令和 R 登录 S。这将导致新的问题——在一段时期内，U_i 必须同时记忆

新口令 $\mathrm{PW}_i^{\mathrm{new}}$ 和旧口令 PW_i。因为在 U_i 看来，虽然口令更新阶段已完成，但 U_i 并不知道服务器端是否也已完成参数更新，U_i 只能尝试用新口令 $\mathrm{PW}_i^{\mathrm{new}}$ 向 S 发出登录请求，依据 S 的响应来判断(设此时为时刻 T_2)：如果登录成功，则服务器端已完成参数更新，此后可使用新口令 $\mathrm{PW}_i^{\mathrm{new}}$；若登录失败，则服务器端未完成参数更新，新口令 $\mathrm{PW}_i^{\mathrm{new}}$ 无效，仍需使用旧口令 PW_i。U_i 需要在 $T_1 \sim T_2$ 这段时期内同时记忆新旧两个口令，对用户来讲这将是一个不小的负担，并且备份 R 需要额外的存储空间。

此外，在 Fang 等人方案的用户口令更新过程中，服务器端需要同步完成对秘密参数 k 的更新。依据文献[14]以及我们的分析，参数 k 在此过程的更新是不必要的，服务器 S 在用户口令的更新过程所应完成的唯一工作是对用户旧口令的认证；只有出现用户口令 PW_i 或参数 k 泄露的情况下，参数 k 的更新才是必要的。另一方面，实际应用中，用户更新口令的频率要远远高于 PW_i 或参数 k 泄露的频率。综合上述，参数 k 的更新通过重注册阶段来完成将更为合理，这也是文献[14]采用的方法。一旦发现口令 PW_i 或参数 k 泄露，用户将智能卡到服务器进行重注册，这就从根本上解决了用户口令更新过程中用户端和服务器端认证参数不一致问题。

4　改进方案

本节在保持 Fang 等人方案优势的基础上，根据第 2 节中的安全性分析，提出一个改进方案，其先进性主要体现在以下几点：(1)为抵抗离线口令猜测攻击，改进方案的安全性基于散列函数安全性和大整数分解难解性问题；(2)为抵抗已知密钥攻击，改进方案的会话密钥的构造遵循“计算独立”原则[19]；(3)为抵抗平行会话攻击，改进方案中认证消息的结构保持差异性；(4)为解决口令更新阶段用户端和服务器端认证参数不一致问题，改进方案的口令更新阶段只对用户端参数进行更新，当发现口令 PW_i、参数 k 泄露，或者智能卡丢失时，才通过重注册阶段完成对服务器端认证参数的更新。

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，其中符号含义如表 1 所示。

4.1 注册阶段

服务器 S 产生大素数 p 和 q，计算 $n=pq$；选取公钥 e，计算私钥 d，满足 $ed \equiv 1 \bmod (p-1)\cdot(q-1)$。其中 p，q 和 d 是秘密参数，n 和 e 是系统公开参数。

$R1$: 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 $h(b \oplus \mathrm{PW}_i)$。

$R2$: $U_i \Rightarrow S$:$\{\mathrm{ID}_i, h(b \oplus \mathrm{PW}_i)\}$。

$R3$: S 产生随机数 N_i，计算 $k=h(\mathrm{ID}_i \oplus d \oplus N_i)$ 和 $R=k \oplus h(b \oplus \mathrm{PW}_i)$，将$\{R, e, n, h(\cdot), h_k(\cdot)\}$写入智能卡，在后台数据库中保存$\{\mathrm{ID}_i, N_i\}$。

$R4$: $U_i \Rightarrow S$:智能卡。

$R5$: U_i 将 b 写入智能卡。

4.2 登陆阶段

$L1$: 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

$L2$: 智能卡产生随机数 r，读取当前时间戳 T_u，计算 $k=R \oplus h(b \oplus \mathrm{PW}_i)$，$C_1=k \oplus h(r \| T_u \| \mathrm{ID}_i)$ 和 $C_2=r^e \bmod n$。

$L3$. $U_i \rightarrow S$:$\{\mathrm{ID}_i, C_1, C_2, T_u\}$。

4.3 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 $T_s - T_u > \Delta T$，则拒绝认证请求；否则，S 用私钥 d 解密 C_2 得到 r，计算 $k'=C_1 \oplus h(r \| T_u \| \mathrm{ID}_i)$，并从后台数据中读取与 ID_i 对应的 N_i。

$V2$: S 计算 $k''=h(\mathrm{ID}_i \oplus d \oplus N_i)$，然后验证 $k''=k'$ 是否成立。如果不成立，则 S 拒绝 U_i 的认证请求。

$V3$: S 计算 $C_3=h_{k'}(\mathrm{ID}_i \| r \| T_s)$。

$V4$: $S \rightarrow U_i$:$\{C_3, T_s\}$。

$V5$: U_i 检查 T_s 的有效性，然后计算 $C_3'=h_k(\mathrm{ID}_i \| r \| T_s)$ 并验证 $C_3'=C_3$ 是否成立。如果成立，则 U_i 和 S 间共享会话密钥 $\mathrm{SK}=h(\mathrm{ID}_i \| T_s \| T_u \| r)$，认证完成。

4.4 口令更新阶段

$C1$: 运行登录阶段 $L1 \sim L3$ 和认证阶段 $V1 \sim V2$。

$C2$: S 计算 $m_3=h_{k'}(r \| T_s \| \mathrm{ID}_i)$。

$C3$: $S \rightarrow U_i$:$\{m_3, T_s\}$。

$C4$: U_i 检查 T_s 的有效性，然后计算 $m_3'=h_k(r \| T_s \| \mathrm{ID}_i)$ 并验证 $m_3'=m_3$ 是否成立。如果成立，则 U_i 输入新口令 $\mathrm{PW}_i^{\mathrm{new}}$，计算 $R_{\mathrm{new}}=k \oplus h(b \oplus \mathrm{PW}_i^{\mathrm{new}})$，然后用 R_{new} 替换 R。

4.5 重注册阶段

当智能卡丢失，或者发现参数 k 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 $\mathrm{PW}_i^{\mathrm{new}}$ 到服务器重新注册，具体过程与注册阶段相同。

5　改进方案的分析

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]，下面分别从这两个方面进行分析。

5.1 安全性分析

由于改进方案基于 Fang 等人方案并继承了该方案所具有的安全性，例如实现双向认证和前向安全性，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。

5.1.1 抵抗离线口令猜测攻击 假设攻击者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 R 和 b 。

用户在网络中传输的消息中不包含口令 PW_i 的明文形式，攻击者只能截获用户与服务器交互过程中的信息，发动离线猜测攻击。在注册阶段，服务器发给用户的签发信息是经过安全信道传输的，可以阻止攻击者对信息的非法截获。在登录认证阶段，只有参数 k 中包含 PW_i 的信息，与攻击 Fang 等人方案一样，攻击者首先猜测口令为 PW_i^*，然后计算 $k^* = R \oplus h(b \oplus \mathrm{PW}_i^*)$，再通过验证所计算的 k^* 的正确性来验证所猜测的 PW_i^* 的正确性。假设攻击者截获了 $\{\mathrm{ID}_i, C_1, C_2, T_u\}$ 和 $\{C_3, T_s\}$。但是由于 C_1 和 C_3 的计算式中都引入了一个随机数 r，而 r 的值只有通过服务器 S 的私钥 d 解密 C_2 才能获取，因此攻击者获取 r 的难度与分解一个大整数 n 的难度等价，我们知道后者是一个 NP 困难问题。r 的随机性和机密性确保了 C_1 和 C_3 与 PW_i 之间验证关系的机密性，使攻击者无法通过所截获的认证消息来验证所计算的 k^* 的正确性，进而攻击者也就无法验证所猜测的 PW_i^* 的正确性。因此，改进方案可以抵御离线口令猜测攻击。

5.1.2 已知密钥攻击 Fang 等人方案易遭已知密钥攻击的根本原因在于，会话密钥 $\mathrm{SK} = h(r \oplus b)$ 是登录消息 $C_1 = k \oplus h(r \oplus b)$ 的直接构成部分，SK 和 k 之间具有很好的代数运算关系：通过简单的异或运算可以由 C_1 和 SK 恢复出核心秘密参数 k，即 $k = C_1 \oplus h(r \oplus b) = C_1 \oplus \mathrm{SK}$ 。

在改进方案中，双方协商的会话密钥 $\mathrm{SK} = h(\mathrm{ID}_i \,||\, T_s \,||\, T_u \,||\, r)$ 不再是任何认证消息的直接或间接构成部分，并且在计算 SK 时通过引入临时会话参数 T_s，T_u 和 r 来实现不同会话间会话密钥的独立性。因此，改进方案遵循了会话密钥的“计算独立”原则[19]，能够抵抗已知密钥攻击。

5.1.3 平行会话攻击 由于 C_1 保证了 msg1=$\{\mathrm{ID}_i, C_1, C_2, T_u\}$ 的完整性，C_3 保证了 msg2=$\{C_3, T_s\}$ 的完整性，m_3 保证了 msg3=$\{m_3, T_s\}$ 的完整性，平行会话攻击若能成功，必须是对整个 msg1, msg2 或 msg3 的替换；另一方面，C_1, C_3 和 m_3 的结构各异，且 C_1, C_3 和 m_3 中均嵌入了时间戳 T_u 或 T_s 。因此，针对同一用户的平行会话攻击将不会成功，如针对 Fang 等人方案的平行会话攻击在本方案中不再有效。此外，C_1, C_3 和 m_3 中均嵌入了用户的身份标识符 ID_i 。因此，将 msg1, msg2 或 msg3 替换为其它用户认证流中的消息，都将通过不验证。因此，改进方案可抗平行会话攻击。

5.1.4 用户友好性 Fang 等人方案在口令更新阶段用户友好性较差的根本原因在于，用户端和服务器端均需要更新认证参数，存在二者之间认证参数不一致的可能性。当用户端和服务器端二者之间的认证参数出现不一致时，为了仍能登录服务器 S，用户在一段时期内必须同时记忆新旧两个口令。而在改进方案的口令更新阶段，不需要在服务器端更新认证参数，彻底消除了用户和服务器间认证参数不一致的可能性。并且，在用户口令 PW_i 或参数 k 泄露，或者智能卡丢失时，可通过重注册阶段来实现可修复性。因此，改进方案在不降低可修复性的同时，提高了用户友好性。

表 2 总结了 Fang 等人方案、Wang 等人方案、Chung 等人方案和本文所提出改进方案的安全性质。由表 2 可知，改进方案弥补了 Fang 等人方案的安全缺陷，实现了文献[3]所列出的口令认证协议相关的 9 项主要安全目标。

5.2 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；计算量主要取决于大指数模幂乘运算 T_e、小指数模幂乘运算 T_{se} 和 Hash 运算 T_h，其中 $T_e \approx 600T_h$ [21]，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，

表 2 相关远程用户口令认证方案的安全性比较

方案	双向认证	前向安全性	抗 DoS 攻击	抗离线口令猜测攻击	抗重放攻击	抗仿冒攻击	抗平行会话攻击	抗窃取验证项攻击	抗已知密钥攻击
Wang 等人[11]方案	是	否	是	否	是	否	是	是	否
Chung 等人[14]方案	是	是	是	是	是	是	是	是	是
Fang 等人[15]方案	是	是	是	否	是	是	否	是	否
本文改进方案	是	是	是	是	是	是	是	是	是

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、用户 ID 和口令 PW 长度为 128 bit，服务器产生的大整数 n 和公钥 e 长度均为 1024 bit。需要特别指出的是，实际应用中一般为了提高加密速度，公钥 e 通常取值较小，如 $e=3$ 或 $e=17$。在一些安全需求较高的场合，为避免小指数攻击，公钥 e 的一个推荐取值为 $2^{16}+1$ [21]。因此，不妨设公钥 e 的长度为 32 bit，则 $T_{\text{se}} \approx \frac{32}{1024} \cdot T_e \approx 20T_h$。基于开源标准密码库 MIRCAL[22]，搭建本文的实验环境：PIV 3 GHz 处理器，512 MB 内存，Linux-2.6.10 操作系统。实验中样本数为 1000，T_e，T_{se} 和 T_h 所耗费时间如表 3 所示，其中 $|n|$ 和 $|e|$ 分别表示模数 n 和指数 e 的长度，即二进制比特数。4 个相关方案的效率比较如表 4 所示。

Chung 等人方案采用随机数机制来提供消息的新鲜性，需要 3 轮交互，其它 3 种方案均采用时间戳机制，两轮交互即可。本文改进方案为了克服 Fang 等人方案和 Wang 等人方案存在的离线口令猜测攻击缺陷，引入了公钥技术，在用户端需要一次小指数模幂乘运算。以在电子护照中广泛使用的 SmartMIPS-4 KSc 33 MHz 嵌入式处理为例[23]，当模数 n 长为 1024 bit 时，一次普通指数模幂乘运算耗时 320 ms，而一次小指数模幂乘运算仅需要 2.28 ms。文献[24,25]的研究也表明，小指数模幂乘运算的计算代价比普通指数模幂乘运算低得多，在资源受限的用户端设备中，如智能卡环境，进行一两次小指数模幂乘运算是可以接受的。

由表 3 和表 4 对比可知：本文改进方案和 Chung 等人方案为了克服 Fang 等人方案和 Wang 等人方案存在的众多安全缺陷，引入了公钥技术，效率不可避免有一定的降低；改进方案提供了与 Chung 等人方案同等的安全性，但其各效率指标均优于 Chung 等人方案。因此，改进方案保持了 Fang 等人方案的高效性和 Chung 等人方案的安全性，更适合于对安全需求较高的资源受限应用环境。

6　结束语

本文首先分析了 Fang 等人方案的安全性，指出该方案无法实现所宣称的抗离线口令猜测攻击，且对已知密钥攻击和平行会话攻击是脆弱的；然后在保持 Fang 等人方案高效等优势的基础上，给出了一个改进方案，其安全性基于散列函数安全性和大整数分解难解性问题。安全性分析表明，新的改进方案弥补了 Fang 等人方案的安全缺陷，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，并且提高了用户友好性；效率分析表明，本文改进方案为抵抗离线口令猜测攻击在客户端仅增加了一次小指数模幂乘运算，各效率指标均优于具有同等安全性的 Chung 等人方案。综合来看，改进方案的实用性相较 Fang 等人方案、Wang 等人方案和 Chung 等人方案大大提高，更适合于对安全需求较高的资源受限应用环境。

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将是我们下一步的工作。此外，改进方案同 Fang 等人方案和 Chung 等人方案一样，用户口令的更新需要与服务器端进行交互，未能实现“用户口令本地自由更新”这一特性。因此，用户口令更新无需与服务器交互的、安全高效的口令认证方案，是值得进一步研究的方向。

表 3 相关密码操作运算时间(ms)

密码操作	大指数模幂运算 T_e ($\|n\|=1024, \|e\|=1024$)	小指数模幂运算 T_{se} ($\|n\|=1024, \|e\|=32$)	Hash 运算 T_h (h = SHA-1)
时间	9.057	0.273	0.026

表 4 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	用户友好性
		用户端	服务器	用户端	服务器			
Wang 等人[11]方案	2	$5T_h$	$3T_h$	576	288	448	否	好
Chung 等人[14]方案	3	$2T_e+6T_h$	$2T_e+6T_h$	1472	1184	3232+*	是	好
Fang 等人[15]方案	2	$5T_h$	$4T_h$	576	288	288	是	差
本文改进方案	2	$T_{\text{se}}+4T_h$	T_e+4T_h	1440	288	1216	是	好

注：*Chung 等人[14]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

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.
Feng Deng-guo and Chen Wei-dong. Modular approach to the design and analysis of password-based security protocols[J]. *Science in China Series E*, 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.
Qin Xiao-long and Yang Yi-xian. Composite attacks on strong- password authentication protocol[J]. *Acta Electronica Sinica*, 2003, 31(7): 1043–1045.

[3] Tsai C S, Lee C C, and 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 and 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 and 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] Song R G. Advanced smart card based password authentication protocol[J]. *Computer Standards & Interfaces*, 2010, 32(4): 321–325.

[7] Khan M K, Kim S K, and 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] Chen T H, Hsiang H C, and Shih W K. Security enhancement on an improvement on two remote user authentication schemes using smart cards[J]. *Future Generation Computer Systems*, 2011, 27(4): 377–380.

[9] Kocher P, Jaffe J, and Jun B. Differential power analysis[C]. Advances in Cryptology-CRYPTO 1999, California, USA, August 15–19, 1999, LNCS 1666: 388–397.

[10] Messerges T S, Dabbish E A, and Sloan R H. Examining smart-card security under the threat of power analysis attacks[J]. *IEEE Transactions on Computers*, 2002, 51(5): 541–552.

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

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

[13] Wang R C, Juang W S, and Lei C L. Robust authentication and key agreement scheme preserving the privacy of secret key[J]. *Computer Communications*, 2011, 34(3): 274–280.

[14] Chung H R, Ku W C, and Tsaur M J. Weaknesses and improvement of Wang *et al*.'s remote user password authentication scheme for resource-limited environments[J]. *Computer Standards & Interfaces*, 2009, 31(4): 863–868.

[15] 方恩博, 刘嘉勇, 肖丰霞. 一种适于受限资源环境的远程用户双向身份鉴别方案[J]. 四川大学学报: 工程科学版, 2011, 43(5): 140–145.
Fang En-bo, Liu Jia-yong, and Xiao Feng-xia. An efficient remote user mutual authentication scheme for resource-limited environment[J]. *Journal of Sichuan University: Engineering Science Edition*, 2011, 43(5): 140–145.

[16] Wu Shu-hua, Zhu Yue-fei, and Pu Qiong. Robust smart-cards-based user authentication scheme with user anonymity[J]. *Security and Communication Networks*, 2012, 5(2): 236–248.

[17] Ma Chun-guang, Wang Ding, and Zhang Qi-ming. Cryptanalysis and improvement of Sood *et al*.'s dynamic ID-based authentication scheme[C]. Preceedings of the 8th International Conference on Distributed Computing and Internet Technology, Bhubaneswar, India, February 2–4, Springer-Verlag, 2012, LNCS 7154: 141–152.

[18] Halevi S and Krawczyk H. Public-key cryptography and password protocols[J]. *ACM Transactions on Information and System Security*, 1999, 2(3): 230–268.

[19] Krawczyk H. HMQV: a high-performance secure Diffie-Hellman protocol[C]. Advances in Cryptology- CRYPTO 2005, California, USA, August 14–18, Springer- Verlag, 2005, LNCS 3621: 546–566.

[20] Diffie W, Oorschot P C, and Wiener M J. Authentication and authenticated key exchange[J]. *Designs, Codes and Cryptography*, 1992, 2(2): 107–125.

[21] Ferguson N, Schneier B, and Kohno T. Cryptography Engineering: Design Principles and Practical Applications[M]. New York: John Wiley & Sons, 2010: 326–344.

[22] Shamus Software Ltd. MIRACL Library[OL]. http://www.shamus.ie/index.php?page=home, 2012-02-17.

[23] Großsch dl J and Kamendje G A. Architectural enhancements for Montgomery multiplication on embedded RISC processors[C]. Proceedings of the First International Conference on Applied Cryptography and Network Security, Kunming, China, October 16–19, Springer- Verlag, 2003, LNCS 2846: 418–434.

[24] Wong D S, Fuentes H H, and Chan A H. The performance measurement of cryptographic primitives on palm devices[C]. Proceedings of the 17th Annual Computer Security Applications Conference, Washington, DC, USA, IEEE Computer Society, 2001: 92–101.

[25] Potlapally N R, Ravi S, Raghunathan A, *et al*.. A study of the energy consumption characteristics of cryptographic algorithms and security protocols[J]. *IEEE Transactions on Mobile Computing*, 2006, 5(2): 128–143.

汪 定： 男，1985年生，硕士生，研究领域为密码学与信息安全.

马春光： 男，1974年生，博士，教授，博士生导师，研究领域为密码学与信息安全.

翁 臣： 男，1986年生，硕士生，研究领域为网络与信息安全.

贾春福： 男，1967年生，博士，教授，博士生导师，研究领域为信息安全、可信计算.