分类号：_____ 密级：_____

UDC：_____ 编号：_____

工学硕士学位论文

基于智能卡的远程用户口令认证协议研究

硕士研究生：汪　定

指 导 教 师：马春光 教授

学科、专业：计算机系统结构

论文主审人：王慧强 教授

哈尔滨工程大学

2013 年 3 月

分类号：_____ 密级：_____

UDC：_____ 编号：_____

工学硕士学位论文

基于智能卡的远程用户口令认证协议研究

硕士研究生：汪　定

指导教师：马春光 教授

学位级别：工学硕士

学科、专业：计算机系统结构

所在单位：计算机科学与技术学院

论文提交日期：2012 年 12 月

论文答辩日期：2013 年 3 月

学位授予单位：哈尔滨工程大学

Classified Index:
U.D.C:

A Dissertation for the Degree of M. Eng

Research on Password-based Remote User Authentication Schemes Using Smart-cards

Candidate:	Wang Ding
Supervisor:	Prof. Ma Chunguang
Academic Degree Applied for:	Master of Engineering
Specialty:	Computer Architecture
Date of Submission:	Dec., 2012
Date of Oral Examination:	Mar., 2013
University:	Harbin Engineering University

哈尔滨工程大学
学位论文原创性声明

本人郑重声明：本论文的所有工作，是在导师的指导下，由作者本人独立完成的。有关观点、方法、数据和文献的引用已在文中指出，并与参考文献相对应。除文中已注明引用的内容外，本论文不包含任何其他个人或集体已经公开发表的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者（签字）：

日期：　　年　月　日

哈尔滨工程大学
学位论文授权使用声明

本人完全了解学校保护知识产权的有关规定，即研究生在校攻读学位期间论文工作的知识产权属于哈尔滨工程大学。哈尔滨工程大学有权保留并向国家有关部门或机构送交论文的复印件。本人允许哈尔滨工程大学将论文的部分或全部内容编入有关数据库进行检索，可采用影印、缩印或扫描等复制手段保存和汇编本学位论文，可以公布论文的全部内容。同时本人保证毕业后结合学位论文研究课题再撰写的论文一律注明作者第一署名单位为哈尔滨工程大学。涉密学位论文待解密后适用本声明。

本论文（□在授予学位后即可　□在授予学位12个月后　□解密后）由哈尔滨工程大学送交有关部门进行保存、汇编等。

作者（签字）：　　导师（签字）：

日期：　　年　月　日　　年　月　日

摘　要

随着电子商务、电子医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基本手段。基于智能卡的远程用户口令认证协议由于安全性高，便携性好，简单易用，在业界获得了广泛的应用。经过近二十年的研究和发展，这种认证协议在安全性和功能特性方面逐渐趋于完善，但它们都基于一个共同假设——智能卡内秘密信息无法为攻击者获取。近年来边信道攻击技术研究结果表明，攻击者可通过逆向工程、能耗分析、计时攻击等手段分析出普通智能卡内秘密参数，使传统协议所基于的安全假设不再成立。相应地，设计基于非抗窜扰智能卡的远程用户口令认证协议自 2006 年来成为轻量级安全协议领域的一个研究热点。

设计安全高效的基于非抗窜扰智能卡的远程用户口令认证协议是一个巨大的挑战：一方面需要综合考虑众多的安全目标和理想特性，另一方面智能卡本身又是一种资源受限设备。近几年来虽然有一些基于非抗窜扰智能卡的增强型协议被提出，但都随后被指出存在这样或那样的安全漏洞和性能缺陷。存在这一问题的根本原因在于，以往研究要么关注于某个安全目标或理想特性的实现，要么在对先前协议进行攻击分析后只给出简单的漏洞修补，缺乏系统性和原理性的研究。针对这一现状，本文以基于非抗窜扰智能卡的远程用户口令认证协议为主线，从协议的评价指标、分析和设计原则，以及新协议的设计方面展开了研究，主要完成了以下四方面工作：

1）分析了近期三个较为典型的基于智能卡的远程用户口令认证协议。分析了 Xie 等学者在 2010 年设计的基于 RSA 的口令认证协议，指出其无法实现所声称的抗重放攻击，并且对密钥泄露仿冒攻击是脆弱的；分析了 Hao 等学者于 2011 年提出的具有前向安全性的口令认证密钥协商方案，指出其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，并且存在时钟同步问题；分析了 Hsieh 等学者在 2012 年设计的仅使用 Hash 函数的高效口令认证协议，指出其无法实现所声称的抗离线口令猜测攻击，对内部人员攻击是脆弱的，并且存在用户友好性差、不适于移动应用等问题。

2）梳理了基于智能卡的远程用户口令认证协议评价指标间的相互关系，提出了三个协议设计原则。首次证明了在非窜扰智能卡假设下，采用公钥技术是实现协议可抗离线口令猜测攻击的必要条件；首次证明了在服务器端无敏感验证表项情形下，服务器（至少）进行两次模幂运算（或点乘运算）是实现前向安全性的必要条件；首次深入分析了“抗智能卡丢失攻击”这一安全目标和“口令本地自由更新”这一理想属性间存在的矛盾，提出“模糊验证因子”技术来较好地平衡这一对矛盾。

3）设计了一个基于 RSA 适于资源受限环境的远程用户口令认证协议。Fang 等方案为了克服资源受限这一难题，仅采用了对称密码操作（Hash 函数），这一策略违反了本文给出的“公钥技术原则”，无法抵抗离线口令猜测攻击；利用 RSA 加密和解密操作运

算量的非对称性，设计了一个安全高效的方案，并且完成了启发式安全性分析，与已有协议相比，新方案在客户端性能方面具有显著优势,适于移动应用环境。

4）设计了一个随机预言机模型（ROM）下可证明安全的“理想协议”。基于计算Diffie-Hellman（CDH）困难性假设，设计了一个能够满足所有安全目标和实现所有相关理想属性的协议，并且在 ROM 下完成了紧归约的形式化安全证明，进而回答了Madhusudhan 和 Mittal 2012 年初在 Journal of Network and Computer Applications 上提出的公开问题。此外，协议中首次提出“模糊验证因子”的概念，较好地解决了以往此类协议无法同时实现抗智能卡丢失攻击和支持口令本地自由更新这一难题。

关键词：口令认证协议；智能卡；非抗窜扰；离线口令猜测攻击；随机预言机模型

Abstract

With the rapid development of e-commerce, e-health as well as e-government, user authentication has become an essential mechanism to assure the distributed systems' security and privacy from malicious adversaries. Owing to its high level of security, portability, simplicity and cryptographic properties, smart card based password authentication has been widely adopted in various applications. After twenty years of intensive research, the security requirements and desirable properties that such schemes can support gradually tend to be ideal. A common feature among most of the previous schemes is that, the smart card is assumed to be tamper-resistant, i.e., the sensitive parameters stored in the smart card cannot be extracted. However, recent research results have shown that the secret information stored in the smart card could be extracted by some means, such as monitoring the power consumption, reverse engineering or analyzing the leaked information, which invalidates the basic assumption that the traditional schemes are based on. Consequently, the design of a secure and efficient scheme based on the non-tamper resistance assumption of the smart cards has been a hot topic in the domain of lightweight cryptographic protocols since 2006.

Unfortunately, under this new assumption, how to design a secure and efficient smart card based password authentication scheme is really a big challenge. On the one hand, there are various security requirements and desirable features that a practical scheme should satisfy; on the other hand, the smart card itself is resource-constrained and computationally intensive operations are not suitable for such environments. Although there are a number of schemes using non-tamper resistant smart cards proposed in recent years, all of them have been found severely flawed shortly after they were first put forward. The main reason of such dilemma is that, previous researchers either only focus on the realization of some security requirements or admired properties, or just present an enhancement after cryptanalysis of a problematic scheme, no systematic work or rationale is given. To alleviate this situation, in this thesis, taking the password authentication schemes using non-tamper resistant smart cards as the main line, we focus on the evaluation criteria, the analysis and design principles, as well as the design of new schemes. And our contributions are as follows:

1) Three recently proposed smart-card-based password authentication schemes are investigated. Firstly, we cryptanalyze the RSA-based scheme proposed by Xie et al. in 2010, and find it vulnerable to replay attack and key compromise impersonation attack. Secondly, the password-based authentication key exchange protocol presented by Hao et al. in 2011 is analyzed, and we find it susceptible to offline password guessing attack and key compromise impersonation attack. In addition, it is subject to the clock synchronization problem. Thirdly, Hsieh et al.'s scheme is scrutinized. This scheme only employs lightweight cryptographic

primitives such as Hash function and XOR operations, and thus it is very efficient. Unfortunately, we point out that it cannot withstand offline password guessing attack and insider attack. Moreover, it is not repairable and not well-suited to mobile environments.

2) The relationships among the evaluation criteria are examined. To the best of our knowledge, we are the first to put forward three general principles for smart card based password authentication: (i) public-key techniques are indispensable to resist against offline password guessing attack and to preserve user anonymity under the non-tamper resistance assumption of the smart cards; (ii) at least two exponentiation (respectively elliptic curve point multiplication) operations conducted on the server side are necessary for achieving forward secrecy; and (iii) there is an unavoidable trade-off when fulfilling the goals of local password update and resistance to smart card loss attack.

3) A novel RSA-based password authentication scheme using smart cards for resource-constrained environments is proposed. Before giving our new scheme, we investigate the scheme proposed by Fang et al. in 2011. For the sake of efficiency, Fang et al.'s scheme only involves symmetric cryptographic primitives (such as Hash function), which violates the "public key principle" and it is inherently unable to resist against offline password guessing attack. Accordingly, based on the observation that the computation cost of RSA encryption and the corresponding decryption is quite asymmetric, we advance a secure and efficient scheme and its security is analyzed by heuristics. In comparison with related schemes, our scheme is superior in the efficiency at the client side and thus is more suitable for mobile environments.

4) An "ideal scheme" proved secure in the random oracle model is proposed. Based on the intractability of CDH problem, we put forward a provably secure scheme that can satisfy all the security requirements and provide all the desirable properties, which highly indicates the settlement of an open problem raised by Madhusudhan and Mittal in Journal of Network and Computer Applications in early 2012. Besides, in this scheme, we propose the concept of "fuzzy verifier" which well resolves the problem that no previous scheme can achieve the goals of local password update and resistance to smart card loss attack at the same time.

Key words: Password authentication protocol; Smart card; Non-tamper resistant; Offline password guessing attack; Random oracle model

目　　录

第 1 章 绪论

1.1 研究背景及意义

随着电子商务、电子医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。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]：1）基于用户所知，比如口令、PINs、私钥等；2）基于用户所有，比如智能卡、USB-Key、加密卡等；3）基于用户生物特征，比如指纹、虹膜、掌形等。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，如英文单词，电话号码，或简单的字母数字串，这种低信息熵的口令极易遭到离线口令猜测攻击，这是口令认证协议面临的最严重安全威胁。研究发现,一台普通 PC 机在几分钟内可以 25%的成功概率对用户口令进行离线字典攻击[2]。

为抵御这种针对低信息熵口令的离线字典攻击，一种自然的解决方案是，在用户和认证服务器之间共享一个高信息熵的长期密钥。而在实际应用中,由于高信息熵的密钥不便于记忆,所以它通常被存放在特殊的移动存储设备中。这种存储设备的特殊性在于，不仅能够存储密钥信息,还需要能够执行相关的密码操作运算,即其上不仅有 RAM 和 I/O 模块，还嵌有微处理器，一般称之为智能卡[3,4]。在这种情况下，协议的安全性又完全取决于智能卡的安全性。如果合法用户智能卡丢失，攻击者可利用该智能卡内存储的秘密信息（如共享密钥）仿冒合法用户成功进行登录认证。

为提高身份认证的安全性和有效性，1993 年 Chang 等首次采用智能卡与口令相结合的技术来实现对远程用户身份的认证，随后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[5-13]。这些方案的基本架构如图 1.1 所示。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。近年来随着边信道攻击技术研究的不断进展，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击技术而被提取出来[14-17]。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，然后利用在公开信道上截获的认证信息来验证所猜测口令的正确性，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。为此，近年来出现了一些新的增强型方案[18-32]，但大多都随后被发现存在这样或那样的安全漏洞[33-38]。

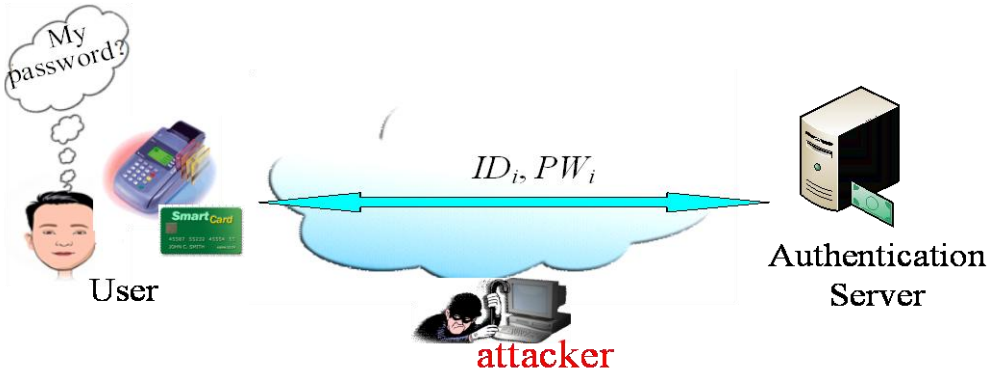

图 1.1 基于智能卡的远程用户口令认证协议基本架构

另一方面，随着无线移动网络的迅速发展，大量智能移动终端被广泛应用于无线移动网络，移动商务服务和应用获得了巨大的发展。由于信道的开放性和用户的移动性，无线网络面临着相较有线网络更多的安全威胁，比如这类应用需在阻止非法用户获取服务资源的同时，防止合法用户滥用服务资源。为解决这些问题，首要的就是对移动终端用户进行身份认证。但是，智能移动终端的存储空间、电池能量和运算能力受限，基于传统公钥技术的认证协议显然不能够适应这种资源受限环境。新兴的公钥技术——椭圆曲线密码系统[39]（Elliptic Curve Cryptography, ECC）具备良好的密码学特性，能用较短的密钥实现传统公钥技术（如 RSA，Elgamal）同等的安全性[40, 41]，ECC 更适合应用于资源受限的移动环境中。近一两年来，出现了一些基于 ECC 的远程用户认证方案[42-48]，这些方案大多采用了双线性对技术，而双线性运算是一种计算强度很大的密码操作，抵消了采用 ECC 所带来的效率优势[49]。剩下的几个方案，也都随后被指出是不安全的[30, 37, 50-56]。本文作者注意到，由于 RSA 加密和解密运算量的非对称性，RSA 密码体制比其它公钥密码体制（包括 ECC），更适合于非对称应用环境，但这方面的相关研究却很少。RSA 密码体制中，加密指数 e 的取值一般比较小，比如一个推荐取值为 $2^{16}+1$[57]。根据文献[58-62]的研究结果，当 $e=2^{16}+1$ 时，在 1024bit 安全强度下，RSA 加密时间只是 ECC 下点乘运算时间的一半。远程用户认证协议[1]的实际应用环境是一种典型的非对称环境，其中客户端智能卡的计算能力非常有限，而认证服务器的计算能力相对强大。因此，设计基于 RSA 密码体制的远程用户口令认证协议具有重要的实用价值。

当前所提出的众多方案之所以被发现存在这样或那样的安全缺陷，被指出与其所宣称的安全性相矛盾，一个重要原因是这些方案的安全性证明是基于启发式的[63]。由于启发式证明很难考虑所有的攻击场景，即使一些方案至今尚未发现安全缺陷，但其安全性的可信度仍然值得怀疑，很多著名的认证协议（包括国际标准）中的安全缺陷是在几十

[1] 文中“方案”和“协议”表达完全相同的概念。

年后才被研究者发现。虽然有少数协议[19, 25, 30, 51]完成了形式化证明，但由于形式化证明技术的复杂性和密码系统安全目标的复杂性，其中一些被指出证明过程有误，另一些因计算复杂度过高而缺乏实用性[37, 64-67]。因此，可证明安全的远程用户认证协议也是值得研究的一个方向。

1.2 国内外研究现状

自1993年Chang等[68]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之后，基于智能卡的远程用户口令认证方案的研究逐渐成为安全协议领域的热点之一。由于基于智能卡的远程用户口令认证技术是现实应用最广、理论研究最多的双因子认证技术，它也常被直接称为双因子认证。目前，众多国内外的IT巨头、IT研究机构和著名大学都积极开展对基于智能卡的远程用户口令认证协议的研究，如微软、IBM、贝尔实验室、剑桥大学、麻省理工学院、加利福尼亚大学洛杉矶分校、上海交通大学、北京邮电大学、西安电子科技大学、浙江大学、电子科技大学等等。近年来，新的基于智能卡的远程用户认证方案频频亮相知名国际会议如IEEE S&P、IPCCC、APWeb、ISCC、EUC等，国内外期刊如IEEE Trans.系列、Computer &Security、Computer Standard & Interfaces、Computer Communications、International journal of communication systems、电子学报、电子与信息学报等更是反映了这一研究领域的活跃情况。目前对基于智能卡的远程用户口令认证协议的分类还没有一个统一的标准，但大体上可分为以下四类：

1） 依据协议是否使用公钥技术，可分为基于公钥的远程用户口令认证协议和基于对称密码体制的远程用户口令认证协议；

2） 依据协议的安全性证明是否使用了形式化方法，可分为可证安全的远程用户口令认证协议和启发式安全的远程用户口令认证协议；

3） 依据协议是否实现了匿名性，可分为基于动态ID的远程用户口令认证协议和非动态ID的远程用户口令认证协议；

4） 依据协议是否实现了前向安全性，可分为具备前向安全性的远程用户口令认证协议和未实现前向安全性的远程用户口令认证协议。

1.2.1 远程用户认证协议评价指标的研究现状

在支持弱口令的环境中，一个天然缺陷就是口令空间受限，可以被攻击者穷举。进而，攻击者有两种方式来确认正确的口令：一是借助在线字典攻击；二是借助离线字典攻击。由于前者不可避免，而后者不需要与合法用户交互，攻击者可以在本地进行，是基于口令的协议面临的最大安全威胁[54]。对于前者，攻击者通过与合法用户的一次交互，不可避免地可验证一个所猜测的口令，因此对于一个理想的口令协议，该攻击应是攻击者获取用户口令的最好途径。

如文献[38, 69]所指出，设计安全高效的远程用户口令认证协议是信息安全研究领域的一个挑战。一个适于应用的方案不仅需要考虑安全性，还要综合考虑理想属性和效率这两个方面。这三项评价标准的任一缺位都会使方案出现重大缺陷，难于适应实际应用。但是，除了效率评价应主要包括计算量、通信量、存储量三方面取得共识外，对安全性和功能属性的具体评价内容至今尚没有统一的认识[18, 37, 69, 70]。本文在文献[18, 36-38, 69, 70]研究基础上总结了一个理想的认证协议所应实现的如表 1.1 所示 *S1~S12* 共 12 个安全目标，如表 1.2 所示 *U1~U10* 共 10 个理想属性。Tsai 等在 2006 年所指出，当时还不存在全部实现 *S1~S10* 和 *U1~U5* 的高效方案；Madhusudhan 和 Mittal[69]在 2012 年指出，全部实现 *S1~S9* 和 *U1~U8* 的高效方案仍然尚未面世。近几年虽然出现了大量的方案，但多数情况下，作者只对方案中实现了的安全目标和理想属性进行对比和阐述，而对未实现的安全性或理想属性避而不谈，如[13, 25, 31, 36, 38, 71]。剩下一部分情况是，作者首先定义一个“好的方案”所应实现的安全性和可用性（或功能）目标，然后提出方案并论证其满足“好的方案”的所有要求，如[18, 30, 37, 38, 51]。这里存在的问题是，大家对“好的方案”的标准没有统一认识，各行其是。文献[30, 51]中“好的方案”标准中没有 *S10~S12*，而文献[72, 73]明确指出 *S10~S12* 是支持密钥协商的密码协议应实现的重要属性；文献[18, 74]给出的评价“好的方案”标准中无理想属性 *U4~U10*，而文献[37, 42, 69]明确指出它们是理想方案应具备的属性。

表 1.1 远程用户口令认证协议的安全目标

安全目标	描述
S1	抗离线口令猜测攻击
S2	抗窃取验证项攻击
S3	抗仿冒攻击
S4	抗智能卡丢失攻击
S5	抗重放攻击
S6	抗平行会话攻击
S7	抗拒绝服务攻击
S8	抗内部人员攻击
S9	抗反射攻击
S10	抗未知密钥共享攻击
S11	抗已知密钥攻击
S12	抗密钥泄露仿冒攻击

表 1.2 远程用户口令认证协议理想属性

功能特性	描述
U1	服务器端无验证表项
U2	口令本地自由更新
U3	双向认证
U4	前向安全性
U5	口令错误输入及时检测
U6	智能卡撤销
U7	密钥协商
U8	用户匿名性
U9	可修复性
U10	无时钟同步

对“好的方案”标准认识的混乱引起了作者的思考，初步发现，在安全的 12 个具体评价指标和理想属性的 10 个具体评价指标之间，有的是相互促进的，有的需要进行平衡，还有一些之间存在本质性矛盾，不可共存。比如作者发现，*S1* 和 *U2*、*U5* 之间需要平衡，否则必然会顾此失彼；实现 *U2* 而未实现 *U5*，则 *S4* 将无法满足。这些具体评价指标之间的关系直接影响到协议的设计策略，梳理这个评价指标间的关系是设计出满足上述所有目标和特性的理想协议的基本前提，但尚未有系统性的研究。另外，如何实

现各个安全目标和理想属性，尽作者所知，目前也没有给出任何相关的理论原则，导致同样的错误一再重复[75]。比如，自 2006 年以来很多学者[9, 12, 27, 31, 35, 76, 77]试图在非抗窜扰智能卡假设下，仅基于对称密码原语（如对称加密算法，Hash 函数，异或运算）来设计可抗离线口令猜测攻击的远程用户认证协议，如作者在第二章将要证明的，这种尝试（协议设计策略）从原理上讲是不可行的。

1.2.2 基于非抗窜扰智能卡的远程用户认证协议研究现状

最初，人们普遍认为智能卡是抗窜扰设备，即其内存储的敏感信息无法为攻击者所获取。但是近年来对边信道攻击技术的研究表明，可通过能量分析攻击[14, 15, 78]、计时攻击[16]、逆向工程[78, 79]等手段获取普通智能卡内秘密信息。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，这些基于智能卡的方案便面临着离线口令猜测攻击、仿冒攻击等安全威胁。2004年 Ku等人[80]首次注意到了该问题，并设计一个了基于非抗窜扰智能卡的协议。不幸的是，在该协议提出不久，Yoon和Yoo[6]发现它易遭平行会话攻击，即无法实现安全目标*S6*,于是提出了一个改进方案。2007年Wang[8]等发现Yoon和Yoo的方案也存在安全缺陷，无法实现安全目标*S1*、*S3*和*S7*，并给出了改进方案。2009年，Chung等[81]分析发现Wang等方案在非抗窜扰智能卡假设下无法抵抗高线口令猜测攻击，对仿冒攻击是脆弱的，且存在无法实现前向安全性，可修复较差等问题，即无法满足评价指标*S1, S3,U4, U9*。为克服这些缺陷，Chung等给出了一个基于离散对数难解性的改进方案。2011年方恩博[35]等分析发现，Wang等方案无法实现目标*S1*、*S3*和*U6*，并指出Chung等针对Wang等的改进方案需要在客户端进行大指数模幂乘运算，在资源受限的智能卡环境具有局限性，于是提出了仅基于Hash函数的改进方案。不久前，本文作者发现，Fang等方案仍然无法实现所宣称的*S1*、*S6*和*S11*，相应的安全性分析和改进方案在第三章中给出。与文献[35]同时，Chen等[12]也发现了[8]中方案的上述缺陷并提出改进方案。2012年，Wang和Ma[82]分析发现，在非抗窜扰智能卡的假设下，文献[12]的改进方案无法实现目标*S1*、*S7*、*S9*、*S10*和*U9*[82]。

在Ku等指出一个实用的方案应基于非抗窜扰智能卡假设的同时，2004年Das等[83]发现，已往方案中用户的ID在网络中直接传输，存在泄露用户隐私的风险，开创性地提出了一个可以实现匿名性的方案。随后，Chien-Chen[7]指出Das等的方案实际上无法实现用户匿名性，因为在认证消息中包含一个与用户直接相关的固定参数。2009年Wang等[9]针对Das等方案无法实现匿名性的缺陷，仅基于Hash函数给出了一个改进方案。不幸的是，Wang等的方案仍然无法实现匿名性，且存在众多安全漏洞，难以抵抗仿冒攻击、离线口令猜测攻击、智能卡丢失攻击和拒绝服务器攻击[13, 25, 31]。Sood、Khan和Wen-Li等学者分别给出了改进方案，但这些方案和原方案一样，都尝试仅用非公钥技术来实现

用户匿名性和抵抗离线口令猜测攻击。2012年，Ma等[75]基于1998年Halevi和Krawczyk[84]的工作，成功证明在非抗窜扰智能卡假设下，公钥技术对于抗离线口令猜测攻击是不可或缺的。同年，Wang和Ma[85]根据他们在基于智能卡的口令认证协议分析方面的经验，推断：在非抗窜扰智能卡假设下，公钥技术对于实现用户匿名性是不可或缺的。

从图1.2中可以看出，在基于非抗窜扰智能卡的口令认证协议研究历史中，主要有三条研究路线：

1） 以2004 Ku等[80]为代表的第一条路线。该路线关注于协议的安全性，提出了众多试图抵抗各类潜在攻击的方案，也对一些理想特性进行了探讨，如前向安全性、可修复性等（但不包括匿名性），多数方案仅基于非公钥技术；

2） 以2004Das[83]为代表的第二条路线。该条路线重点关注于实现协议的匿名性，提出的方案很高效但大多存在各种安全缺陷，绝大多数方案仅基于非公钥技术；

3） 以2009Xu等[19]为代表的第三条路线，该路线也是主要关注协议的安全性，致力于设计能够抵抗所有潜在攻击的强健方案，但与前两条不同，基于这条研究路线的协议一般采用公钥技术，如基于离散对数难解问题或大数因子分解问题。

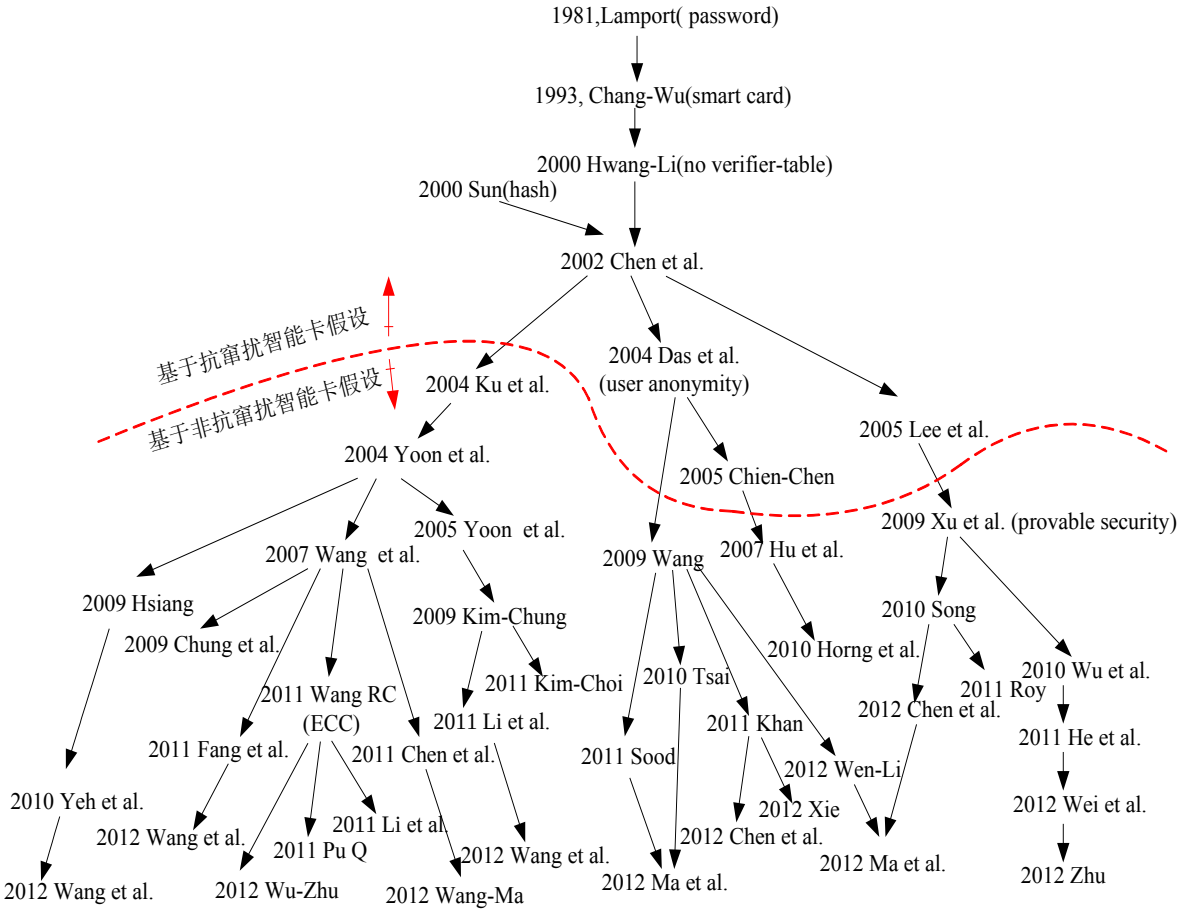

图1.2 一个“攻击—改进—攻击”的历史长河

依据表1.1中的安全目标和表1.2中的理性特性，对上述三条研究轨迹中的7个典型协议进行了分析，评估结果如表1.3。从表1.3中可看出，虽然基于智能卡的口令认证协议已有将近20年的研究历史，对基于非抗窜扰智能卡的协议的研究从2004年也已经开始，但目前仍没有一个协议能够抵抗如表1.1中所列的12个潜在攻击[69, 86]。一个实用的协议应是一个实现安全性、理想属性和性能的合理平衡的协议[72]，如果连基本攻击(如表1.1)都无法抵抗，实现再多的理想特性也没有实际价值。因此，在非抗窜扰智能卡假设下，设计一个安全高效的远程用户口令认证协议仍是一个值得深入研究的课题。

表 1.3 典型远程用户口令认证协议评价指标满足情况总结

	Xu et al. [19]	Song [10]	Tsai et al. [25]	Chen et al.[12]	Kim et al. [71]	Xie [87]	Wang et al. [88]
抗离线口令猜测攻击（*S1*）	✓	×	✓	×	✓	✓	✓
抗验证项窃取攻击（*S2*）	✓	✓	✓	✓	✓	✓	✓
抗仿冒攻击（*S3*）	×†	✓	✓	✓	✓	✓	✓
抗智能卡丢失攻击（*S4*）	×	×	✓	×	✓	×	×
抗重放攻击（*S5*）	✓	✓	✓	✓	✓	✓	✓
抗平行会话攻击（*S6*）	✓	✓	✓	✓	✓	✓	✓
抗拒绝服务攻击（*S7*）	✓	✓	×	✓	×†††	✓	✓
抗内部人员攻击（*S8*）	×	×	✓	✓	✓	✓	✓
抗反射攻击(*S9*)	✓	✓	✓	✓	✓	✓	✓
抗未知密钥共享攻击（*S10*）	✓	✓	✓	✓	✓	✓	✓
抗已知密钥攻击（*S11*）	✓	✓	✓	×	✓	✓	✓
抗密钥泄露仿冒攻击（*S12*）	×	✓	✓	×	✓	×	×
服务器端无验证表项（*U1*）	×	×	✓	✓	✓	✓	✓
口令本地自由更新（*U2*）	×	×	✓	✓	×	✓	✓
双向认证（*U3*）	×	×	✓	✓	×	✓	✓
前向安全性（*U4*）	×	×	×††	×	×	✓	✓
口令错误输入及时检测（*U5*）	×	×	×	✓	×	×	✓
智能卡撤销（*U6*）	×	×	✓	✓	✓	×	✓
密钥协商（*U7*）	×	×	✓	✓	✓	✓	✓
用户匿名性（*U8*）	×	×	✓	×	×	✓	✓
可修复性（*U9*）	×	×	×	×	×	×	×
时钟同步（*U10*）	×	×	×	×	×	✓	×

注：† Xu等方案在2010年被Song指出无法抵抗用户仿冒攻击[10]；†† Tsai等方案在2012年被Wu等指出无法实现前向安全性[37]；††† 本文发现Kim等方案在口令更新阶段的最后一次交互缺乏数据完整性保护，易遭DoS攻击。

1.2.3 可证明安全的远程用户认证协议研究现状

由于启发式证明很难考虑所有的攻击场景，即使一些方案至今尚未发现安全缺陷，但其安全性的可信度仍然缺乏足够支撑，很多著名的认证协议（包括国际标准）中的安全缺陷是在几十年后才被研究者发现[63]。形式化证明方法正是为应对这一难题而提出来的，它采用数学方法构造安全证明过程，以说明待论证的协议实现了声称的安全目标。这一证明过程的基本模式为[89]：首先确定协议的安全目标；然后根据攻击者的能力构建

一个形式的攻击者模型，通过该模型定义协议的参与者以及参与者之间的互信关系、协议的安全参数和协议的通信环境等；基于以上形式化的模型去分析协议，“归约”论断是基本工具；最后指出挫败方案或协议的唯一方法就是破译或解决相关“极微本原”，如数学公开难题或如某个基础密码算法。形式化方法分为三类[90]：

1）基于信息论的方法。在这种证明方法中，一般假设攻击者有无限的计算能力和计算资源。因此，信息论安全的协议也常常被称为是无条件安全的协议；

2）基于符号的方法。这种方法利用一些特定的语法规则定义安全模型。典型的有串空间理论[91]、SVO逻辑[92]和BAN逻辑[93]。

3）基于计算复杂性的方法。与基于信息论的方法相比，基于计算复杂性的方法对攻击者的计算资源和计算能力进行某种“合理的限制”。实际上，这更符合现实情况：如果攻击者攻击某协议的代价比获得的秘密信息的价值还高的话，这对攻击者来说是没有意义的。这种证明方法的基本思想是：将协议*A*的安全性归约到另一个问题*P*的难解性上，如果*P*的难解性被公认为是成立的话，那么协议*A*的安全性被攻破就会导致问题*P*的有效解决；然而，问题*P*是公开难题，因此协议*A*的安全性不会被攻破。这种方法是目前大多数人认为的最可靠的安全性论证手段，人们也通常把采用这种方法论证安全性的协议称为可证明安全的协议。

在远程用户口令认证协议研究领域，通常采用的形式化方法主要是后两种。其中采用逻辑类方法（如BAN逻辑）证明过程中，一个重要的步骤就是将协议的一般说明转化为可被逻辑系统所理解的方式，也称为理想化处理。然而，逻辑类方法没有为理想化方法提供形式化转化方法，这使得协议的理想化的正确（一致性）与否十分依赖于分析者的经验和直觉。BAN逻辑最大问题是不够完备，只能分析安全协议的认证属性不能分析保密属性，这使得BAN逻辑面临尴尬的局面：如果BAN逻辑证明一个协议是安全的，结果不一定令人信服；如果BAN证明一个协议是不安全的，那么这个协议一定存在缺陷。因此，不奇怪的是，一些方案（如[25, 50, 94-96]）即使采用BAN逻辑方法进行了安全性证明，但仍然被发现存在众多安全缺陷，无法达到所声称的安全目标。相比之下，基于计算复杂性的证明方法是对适于应用的协议目前所能达到的最有效的安全证明方法[97]。

口令认证密钥协商协议中使用最为普遍的可证安全模型是随机预言机（Random Oracle Model, ROM）模型[98]和标准模型。由于标准模型下的协议通常计算量比较高，不适合资源受限的智能卡环境[99]，因此选择ROM模型对基于智能卡的口令认证协议进行形式化证明是一种更为可行的方案。虽然有少数协议完成了在ROM模型下的形式化证明，但由于形式化证明技术的复杂性和密码系统安全目标的复杂性，其中一些被指出证明过程有误，另一些因协议缺乏对基本理想属性的支持而失去实用性。

2009年Xu等人[19]提出了一个ROM下可证安全的远程用户认证协议，声称协议能够抵抗各种潜在攻击。2010年，Song[10]发现Xu等人的方案无法实现所宣称的抗用户仿冒攻

击，本文作者进一步分析出现该矛盾的根本原因，发现Xu等方案证明过程中的攻击游戏5（Game 5）中计算Diffie-Hellman难解性（Computational Diffie-Hellman，CDH）归约不成立。2011年Wang RC等[51]针对2006年Mangipudi等的SIKA方案[100]需要大量模幂运算的缺陷，提出了一个在ROM下安全的基于ECC的方案。不久前，Pu等[66]指出Wang等方案[51]因可信中心需要维护所有用户证书列表而缺乏可扩展性，不适合在分布式网络中应用，并给出了改进方案。本文作者发现，Pu等的改进方案[66]不能抵抗已知临时会话信息攻击，未实现可撤销性，且口令更新阶段存在DoS攻击。2012年，Wu等[37]也针对Wang等方案[51]的缺陷提出了改进方案，本文作者发现尽管他们的改进方案非常高效，但口令更新阶段仍存在DoS攻击，并且协议中使用了代价高昂的MaptoPoint运算[101-103]。因此，如何设计出ROM下可证安全的且能实现表1.1中12项安全目标的高效方案将是一件富有挑战性并非常有意义的工作。

1.3 研究内容

随着信息化进程的深入推进和移动设备的广泛应用，基于智能卡的远程口令认证协议因在高效性、安全性和用户友好性方面具有独特的优势，在远程用户身份鉴别领域必将有着广泛应用前景。但是当前此类协议的研究中还存在着评价标准不统一、依赖抗窜扰设备和安全性缺乏严格形式化证明等问题，对这几方面问题的研究有着重要的理论意义和重大现实需求。本课题关注的是，在非抗窜扰智能卡的弱假设情况下（实际上，由于边信道攻击研究的不断进展[14, 15, 17, 104]，这个假设正逐渐成为现实），如何设计安全高效的远程用户口令认证协议，并在随机预言机模型下完成协议的安全性证明，实现可证安全性。本课题的研究工作主要体现在以下几个方面：

（1） 协议评价指标的研究

首先，通过对近期三个典型协议进行分析，指出其中的安全漏洞和功能缺陷，揭示远程用户口令认证设计中存在的挑战和难题。然后，从安全性、理想属性和效率这三个维度出发，在对各维度的构成元素进行准确刻划的基础上，研究各维度内部构成元素之间、不同维度构成元素之间的相互关系，为评价协议的优劣和避免协议设计失误提供参考。最后，提出并证明了实现一些关键指标的设计原则，并通过相关典型案例来检验所提出设计原则的有效性，为设计安全高效的协议提供指导性建议。

（2） 基于非抗窜扰智能卡的远程用户认证协协议研究

在非抗窜扰智能卡假设下，设计远程用户口令认证协议，实现与抗窜扰智能卡假设下同等的安全性和同样的理想属性，需要引入公钥密码技术，如何确保协议的高效性就就成为协议设计的关键。在移动应用中，移动终端设备的计算能力、带宽和存储资源受限，而服务器的资源相对充足，在这种非对称环境中，协议需要重点关注用户端的效率。

针对 RSA 具有加密指数一般远小于解密指数的特性，设计基于 RSA 的适于移动运用的远程用户口令认证协议，并完成效率和安全性分析。

（3） 可证明安全的远程用户认证协议研究

可证明安全是一个密码协议具有可信性和吸引力的重要因素。ROM 模型下可证安全的协议相比标准模型下可证安全的协议具有更高的实用性。对攻击者能力进行建模，基于修正的随机预言机 ROM 模型，对设计的认证协议进行严格的形式化安全性分析，将攻击者对协议的有效攻击归约到对 NP 问题的解决。

1.4 研究成果

针对上述三方面研究内容，本文取得了以下四方面成果：

1）对近期三个较为典型的基于智能卡的远程用户口令认证协议进行了安全性分析和理想属性分析。分析了 Xie 等学者在 2010 年设计的基于 RSA 的口令认证协议，指出其无法实现所声称的抗重放攻击，并且无法实现前向安全性；分析了 Hao 等学者于 2011 年提出的具有前向安全性的口令认证密钥协商方案，指出其无法实现所声称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；分析了 Hsieng 等学者在 2012 年设计的仅使用 Hash 函数和异或运算的高效的口令认证协议，指出其无法实现所无法实现所声称的抗离线口令猜测攻击，对内部人员攻击是脆弱的，并且存在用户友好性差、不适于移动应用等问题。

2）针对基于智能卡的远程用户口令认证协议的评价指标相关研究严重不足的问题，依据作者对近年来 100 余个此类协议的分析经验，梳理了各指标间的相互关系，提出了三条协议设计原则。并且，首次证明了在非抗窜扰智能卡假设下，采用公钥技术是实现协议可抗离线口令猜测攻击的必要条件；首次证明了在服务器端无敏感验证表项情形下，服务器（至少）进行两次模幂运算（或点乘运算）是实现前向安全性的必要条件。

3）讨论了 Fang 等 2011 年提出的一个适于受限资源环境的远程用户认证协议，指出该协议存在安全性问题和功能缺陷，不适于实际应用；利用 RSA 公钥技术的加密和解密运算量非对称特性，设计了一个适于受限资源环境的远程用户认证协议。与已有相关基于公钥技术的协议相比，该协议在客户端的性能具有显著优势。

4）基于离散对数难解性(DLP)问题，设计了一个能够满足所有安全目标和实现所有相关理想属性的协议，并且在随机预言机模型（ROM）下完成了形式化安全证明。协议中首次提出“模糊验证因子”的概念，解决了以往此类协议无法同时实现抗离线口令猜测攻击和支持口令本地自由更新这一难题，进而回答了 Madhusudhan 和 Mittal 2012 年初在 Journal of Network and Computer Apllications 上提出的公开问题。

1.5 论文结构

论文后续章节内容安排如下：

第 2 章是基础知识部分，给出了基于智能卡的远程用户口令认证协议的攻击者能力模型，总结了此类协议理想中应实现的安全目标，并简要介绍了后续章节中用到的相关密码学组件和计算复杂性假设。

第 3 章主要研究协议评价指标，通过对近期三个典型协议进行分析，指出远程用户口令认证设计中存在的挑战和难题，进一步梳理了各具体评价指标间的相互关系，并提出了四个协议设计原则。

第 4 章研究基于 RSA 的远程用户口令认证协议，分析了 2011 年 Fang 等提出的一个适于资源受限环境下应用的协议，指出该协议无法实现所宣称的安全目标，不适于资源受限环境，并提出了一种新的基于 RSA 的适于资源受限环境的远程用户认证协议。

第 5 章研究 ROM 模型下可证安全的远程用户口令认证协议，通过赋予敌手最强攻击能力，在修正的 BR93 模型下提出了一种可证明安全的远程用户口令认证协议，安全性和理想属性分析表明，所提出的协议实现了理想中所有的安全目标和理想属性，并且与已有协议相比，保持了较高的效率，解决了 Madhusudhan 和 Mittal 2012 年初提出的公开问题。

最后是本文的结束语部分，对全文进行总结，并指出本研究中的不足和下一步值得研究的问题。

第 2 章 基本知识

本章主要介绍基于智能卡的远程用户认证协议所需基础理论和背景材料，主要包括攻击者模型、安全目标、基本密码学组件、计算复杂性理论和随机预言机模型。本章共分四节，其中第一节简要介绍密码协议的通用设计原则；合理的攻击者模型和明确的安全目标是分析和设计任何协议的基石，因此第二节将给出相关攻击者能力模型和协议应实现的安全目标；第三节列举一些本文中使用到的基本密码学组件；第四节给出本文中涉及到的计算复杂性假设；第五节介绍可证明安全的基础知识；最后一节小结本章。

2.1 密码协议设计基本原则

在协议设计过程中，一方面要求协议具有足够的强健性以抵抗各种潜在的攻击，这通常导致协议的较高的复杂性；另一方面，高效性是其能否真正应用于现实网络环境的关键衡量指标，效率越高的协议往往意味着更大的应用可能。因此，设计一个实现安全性、功能性和高效合理平衡的协议并非易事，人们在实践中总结了下面的一些基本的设计原则[90, 105]：

- **明确的攻击者能力限定。**一个协议在这个攻击者模型中是安全的，在另外一个攻击者模型中很有可能不再安全，因此协议的安全性只能相对于特定的攻击者模型而言。一个攻击者模型与另一个攻击者模型的区别正是在于对攻击者能力的明确限定，即规定攻击者能做什么，不能做什么，因此它与特定的应用环境密切相关。在给定的应用环境下，一个合理的攻击者模型应是赋予了攻击者最强的攻击能力，除了那些能轻易使攻击者攻破任何此类协议的能力。
- **明确的安全目标定义。** 在协议设计之初，应首先确定协议的应用环境，根据应用环境确定攻击者能力模型和安全需求，然后制定安全目标。明确的攻击者能力定义和安全目标是确保协议设计满足既定要求的前提条件，也是在保证协议安全的基础上尽可能提高协议效率的基本手段。如果一个协议限定了明确的攻击者能力，列出了明确的安全目标，然后协议确实达到了这些预期目标，那么该协议在该攻击者模型下就是安全的。即使密码分析者后来发现了预期安全目标之外的安全缺陷，也不应否认协议自身的安全性，因为协议设计之初已明确显示没有考虑这一攻击情形。因为攻击手段层出不穷，这种设计的局限性是合理的，协议设计者应做的是把这种局限性降低到最低。当然，如果协议设计者为了避免密码协议分析者的攻击而主动放弃协议必须实现的基本安全属性，其所设计的协议也就是过时的、不合时宜的，失去基本的创新价值。
- **尽量避免对时间戳的使用。** 在早期的很多密码协议设计中，人们多采用时间戳

来提供消息的新鲜性，比如著名的 Kerberos 认证系统[106]。这种时间戳机制需要系统维持一个时间服务器来同步时间，以便各参与者对其它实体的身份认证和消息新鲜性验证的请求。一方面，这种机制需要部署额外的时间同步机制或基础设施，代价昂贵；在分布式网络中，如 Internet，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[107, 108]。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[109]。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大规模分布式网络环境。但需要注意的是，使用时间戳机制的协议通常比使用随机数机制的协议需要更少的交互轮数，从这个意义上来讲，前者可能更高效，因此在一些带宽较高、时延较小的专用网络中，时戳机制有自己的优势。因此，建议在设计安全协议时依据应用环境，尽可能采用随机数机制代替时间戳机制来实现消息的新鲜性。

- **尽量避免较高的计算复杂度和冗余的消息。**在密码协议构造过程中，为使协议高效轻便，应要求协议尽量避免计算量密集的运算，应构造尽可能简短的消息。这样做不仅降低了消息泄露导致口令、秘密协议参数、会话密钥等敏感信息被攻击者分析出来的风险，也提高了协议的效率和适应能力，以期协议既适用于数据处理和传输能力比较强的环境中，也适用于智能卡、USB-Key、移动设备等计算资源和带宽等资源受限的环境。
- **不要天然假设所收到的消息具有某种特定的格式。**在密码分析中，有一种特殊的攻击叫归因于类型攻击[110]，专门利用协议设计者对接收者所收到消息的格式的天然假设。因此，除非消息接收者能够检测所接收消息的格式，否则不要假设所接收的消息具有某种特定格式[105]。

2.2 攻击者模型和安全目标

明确的攻击者能力定义和安全目标是确保协议设计满足既定要求的前提条件，也是在保证协议安全的基础上尽可能提高协议效率的基本手段。基于智能卡的远程用户口令认证协议通常应用于安全需要较高的场合，比如电子商务、电子政务和电子医务[111]，这要求此类协议应具有足够的强健性。一个适于应用的协议应对攻击者能力进行合理假设，在攻击者能力假设基础上能够抵抗各种现有已知攻击。

2.2.1 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[112]，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研究的进展[14, 15, 17, 104]，攻击者还可以分析出智

能卡内的秘密参数信息。

2012 年，Wang[113]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，因为攻击者无法在用户的监视下进行边信道攻击；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。

为了实现用户友好性，现实中一般允许用户自己选择口令 PW，而用户通常为了记忆方便而选取具有低信息熵的“弱口令”，故用户口令间 $\mathcal{D}_{pw}$ 一般非常有限，如 $|\mathcal{D}_{pw}| \le 10^6$ [2, 114-116]。用户的身份 ID 通常也是由用户自行选取，且在很多时候遵循一定的格式，因此用户的身份标识空间 $\mathcal{D}_{id}$ 与口令 $\mathcal{D}_{pw}$ 一样是非常有限的。这也就意味着，攻击者在多项式时间内穷举 $\mathcal{D}_{id} \times \mathcal{D}_{pw}$ 内的所有元素。此外，用户的身份标识长期保持不变（与之对比的是，用户口令应定期更换），攻击者若获取用户智能卡，可以或多或少知道一个用户身份信息。因此，假设主动攻击者可以获取用户身份标识 ID 是合理的。

现实中，用户的会话密钥可能因各种原因（意外公开、敌手入侵）而泄露，尤其是在一些协议中可能会规定将过期会话密钥公开。并且，现实中，对过期会话密钥的保护常常存在各种问题。因此，一个现实的假设是，攻击者可以获取过期会话。给攻击者增加此能力，利于下一节中评估抗已知密钥攻击这一安全目标。

最后，为了评估协议在最终失效事件发生（服务器的长期私钥泄露）后的强健性，此时假设攻击者可获取服务器的长期私钥或窃取服务器中存储的敏感验证表项，但二者不能同时成立，否则为平凡攻击。

现将攻击者 $\mathcal{A}$ 的能力总结如表 2.1 所示。

表 2.1 攻击者拥有的能力

能力	含义
C-00	$\mathcal{A}$ 可以穷举 $\mathcal{D}_{id} \times \mathcal{D}_{pw}$ 中的所有元素
C-01	$\mathcal{A}$ 可以（通过主动攻击）获取用户的 ID
C-1	$\mathcal{A}$ 可以监听、截获、插入、修改、阻断流经公开信道中的消息
C-2	$\mathcal{A}$ 可以 (i) 获知用户口令 PW; (ii) 分析出用户智能卡内秘密参数，但二者不能同时成立，否则为平凡攻击
C-3	$\mathcal{A}$ 可以获知过期的会话密钥
C-4	$\mathcal{A}$ 可以(i) 获知服务器的长期私钥; (ii)窃取服务器中存储的敏感验证表项，但二者不能同时成立，否则为平凡攻击。此能力仅用于评估系统终极失效时的强健性

2.2.2 协议安全目标

基于智能卡的远程用户口令认证协议本质是双因子认证协议，即用户只有同时拥有

智能卡和相应的口令才能登录成功。一方面，用户的口令一般为弱口令，易被攻击者猜测；另一方面，如前文所述，边信道攻击的进展也给此类协议的设计带来了巨大的挑战。因此，设计一个安全的此类协议具有巨大的挑战性。此外，随着信息化进程的推进和网络通信技术的发展，攻击者的计算能力显著增强，攻击手段持续更新。由于攻击者计算能力的提高和攻击手段的不断更新，谁也无法预知新的攻击将何时出现，会对协议的安全性造成什么样的影响。但是，在协议设计中还是希望协议能够抵抗尽可能多的已知各类攻击，实现以下的安全目标[69, 70, 74]（如表 1.1 所示）：

（1） 抗离线口令猜测攻击(*S1*)

根据攻击者能力模型中的 C-00，攻击者 $\mathcal{A}$ 可以穷举用户的口令空间，但关键是要求敌手无法验证所猜测口令的正确性。换句话说，如果 $\mathcal{A}$ 通过窃听协议中传输的消息（C-1）或者通过分析出受害用户智能卡内的秘密参数（C-2(ii)）找到口令的一个验证等式，则可离线地反复对口令进行猜测并验证，直到找到正确的口令为止。由于该攻击过程不需要服务器参与，因此 $\mathcal{A}$ 的该攻击行为不会被服务器察觉。抵抗离线猜测攻击是任何口令协议都应满足的基本安全需求[117]，这也是口令认证协议面临的最大安全威胁[116]。

（2） 抗窃取验证项攻击(*S2*)

根据攻击者能力模型中的 C-4 (ii)，攻击者 $\mathcal{A}$ 可窃取服务器中存储的用户敏感验证表项（如果存在的话）。本安全目标要求，即使 $\mathcal{A}$ 获取了服务器中存储的用户敏感验证表项，系统的安全性仍然不会受到影响。近来的一个趋势是，设计在服务器端无须存储敏感验证表项的协议，这将大大降低系统的负担，并且天然满足本安全目标。

（3） 抗仿冒攻击(*S3*)

根据攻击者能力模型中的 C-1，攻击者 $\mathcal{A}$ 可以通过插入、篡改公开信道中传输的消息来仿冒合法用户登录；根据攻击者能力模型中的 C-2(ii)，攻击者可通过分析出自己智能卡内的秘密参数，然后构造消息仿冒其它合法用户登录，如 2010 年 Song[10]针对 2009Xu 等方案[19]的用户仿冒攻击。本安全目标要求，在没有合法用户智能卡的情形下，任何其它用户应不能仿冒合法用户登录成功。

另一方面，根据攻击者能力模型中的 C-1，攻击者 $\mathcal{A}$ 可以通过插入、篡改公开信道中传输的消息来仿冒服务器；根据攻击者能力模型中的 C-2(ii)，攻击者可通过分析出自己智能卡内的秘密参数，然后构造消息仿冒服务器对合法用户的登录请求进行响应。本安全目标要求，在没有服务器私钥和服务器中存储的秘密验证表项的情形下，任何其它用户应不能仿冒服务器对合法用户的登录请求进行响应。

（4） 抗智能卡丢失攻击(*S4*)

当用户的智能卡丢失或被盗而被攻击者 $\mathcal{A}$ 获得后，$\mathcal{A}$ 可能尝试更改用户的口令或仿冒合法用户登录。本安全目标要求攻击者的这些企图不能成功。

（5） 抗重放攻击(*S5*)

攻击者 $\mathcal{A}$ 可能会试图在信道中插入此前截获的消息来到达仿冒攻击的目的，如 3.1.2 中本文作者针对 Xie 等方案的重放攻击。如果攻击成功，常常能够使协议违反其认证用户的安全性目标．攻击者重放的消息可能是合法用户在某个过去的时刻发送的，也可能来自于和被攻击会话同时运行的其他会话。该安全目标要求 $\mathcal{A}$ 对消息的简单重放应不威胁协议的安全性。

（6） 抗平行会话攻击(*S6*)

在攻击者 $\mathcal{A}$ 的特意安排下，协议的一个或两个实例并发运行，并发的多个运行使得 $\mathcal{A}$ 能够从一个运行中得到另外某个运行中困难的答案。如果协议没有能够提供机制以区分不同会话中的消息，而使得 $\mathcal{A}$ 可以将其它会话中的消息不被察觉地用于给定的会话，那么这种攻击就能够成功。

（7） 抗拒绝服务攻击(*S7*)

若拒绝服务攻击针对单个用户，可使用户的认证过程无法正确完成，除非重新到服务器进行注册；该攻击也可以针对所有（或部分）用户，即针对服务器，使用服务器不能正常为用户的请求服务。该攻击可以给用户带来不便，但不能仿冒用户。

（8） 抗内部人员攻击(*S8*)

由于用户通常使用一个口令登录多个应用系统，如果用户的口令被某个认证服务器的内部人员获知，则该内部人员有可能使用该口令仿冒用户登录其它应用系统。该安全目标要求，口令应不能被服务器知道，或者不能经过简单的攻击得到，如离线猜测攻击。

（9） 抗反射攻击(*S9)*

反射攻击可以看作是重放攻击的一种变体，其中 $\mathcal{A}$ 将一个消息重新发送给消息的发送方。在满足一定条件的情况下，比如消息发送方预期的回复刚好与发送的消息格式相同或对称，发送方可能错误地将这一条自己发送的消息当成响应方的正确回复并且最终完成会话，而实际上另一个用户可能根本没有在线。

（10） 抗未知密钥共享攻击(*S10*)

对远程用户口令认证协议而言，还可能存在如下攻击方式：攻击者 $\mathcal{A}$ 成功使用户 B 认为他和用户 A 完成了会话，但是实际上 B 是和 $l \neq A$ 完成的会话。此时，$\mathcal{A}$ 可能得不到最终的会话密钥，但是却成功地破坏了认证协议的认证性。例如，用户 B 认为他和用户 C 完成了会话，但是实际上是和 $\mathcal{A}$ 完成的会话，并且用户 B 和 C 都是诚实的。

（11） 抗已知密钥攻击(*S11*)

即使此前的会话密钥泄露，当前会话的安全性仍不受影响，即攻击者 $\mathcal{A}$ 仍然不能区分当前会话的真实密钥和一个从密钥空间中选择的随机数。

（12） 抗密钥泄露仿冒攻击(*S12*)

通信方 B 的长期私钥泄露后，攻击者 $\mathcal{A}$ 可以很容易地冒充 B 欺骗通信的另一方，但是希望能够将长期私钥泄露带来的危害降到最低，要求 $\mathcal{A}$ 拿到 B 的长期私钥不能反

向冒充通信另一方来欺骗 B。

2.3 基本密码学组件

本小节简要介绍在后文的协议设计和安全性证明中用到的一些密码学相关组件。

2.3.1 密码体制

密码体制，也称为密码系统[110]（Cryptosystem）或密码方案（Scheme），它指一个密码算法、相关参数及其使用方法的总和。

定义 2.1 一个密码体制是一个五元组（M, C, K, E, D），其中 M 表示明文空间，C 表示密文空间，K 表示密钥空间，E 表示加密算法，D 表示解密算法。其中，每个密钥 $k \in K$ 均由加密密钥 k_e 和解密密钥 k_d 和组成，即 $k = <k_e, k_d>$。

设 $m \in M$ 是一个明文，$k = <k_e, k_d> \in K$ 是一个密钥，则

$$c = E_{k_e}(m) \in C$$

$$m = D_{k_d}(c) \in M$$

显然，在一个密码体制中对任意的 $m \in M$，都应有

$$D_{k_d}(E_{k_e}(m)) = m$$

成立。

一个安全的密码体制应至少满足的必要条件：

（1）有效密钥空间 K 足够大，穷举搜索计算上不可行；

（2）在已知明文 m 和加密密钥 k_e 时，计算密文 $c = E_{k_e}(m)$ 可在多项式时间内完成；

（3）在已知密文 c 和解密密钥 k_d 时，求解明文 $m = D_{k_d}(c)$ 可在多项式时间内完成，在 k_d 未知时，由密文 c 计算明文 m 是困难的。

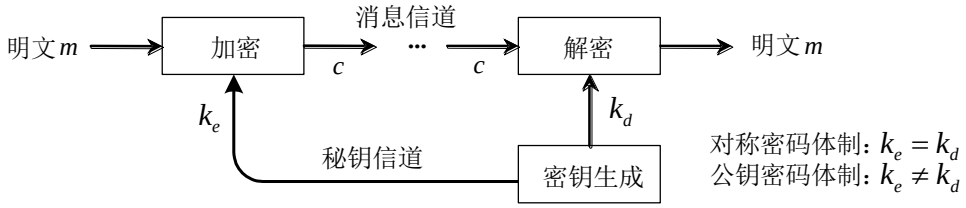

图 2.1 密码体制

密码体制从原理上可分为对称密码体制和非对称密码体制。如果一个密钥密码体制的加密密钥 k_e 与解密密钥 k_d 相同，或由其中一个容易推出另一个，则称其为对称密码体制（Symmetric Cryptosystem）；否则，称其为非对称密码体制（Asymmetric Cryptosystem）。图 2.1 给出了密码体制模型。

对称密码体制的安全性主要取决于密钥的安全性，与算法的保密无关，即由密文和加解密算法不能得到明文。因此，对称密码体制中的核心问题是密钥管理问题，即密钥全生命周期中的产生、分配、使用、存储、销毁等。如果密钥管理存在问题，即使算法

强度足够，也无法确保系统的安全性。其中，密钥的分配又是密钥管理的关键，它包括密钥传递和密钥交换两种方式。其中密钥传递可通过安全信道也可通过离线方式进行，这种方式不方便而且成本高，而密钥交换恰好可弥补这种不足。密钥交换的目标是在非安全信道中通过交互协商出加密密钥，这正是下面将要介绍的非对称密码体制的重要功能之一。常见的对称密码算法有 DES、AES、IDEA、RC 系列、Safer++等。

在非对称密码体制中，由加密密钥 k_e 计算解密密钥 k_e 是困难的（多项式时间内不可行），这种密码体制又称为公钥密码体制（Public-key Cryptosystem, PKC），由 Diffie 和 Hellmen 于 1976 年首次提出。在 PKC 中，用户拥有一对密钥（k_e, k_d），也称之为公私钥对。其中，加密密钥 k_e 可以公开，称为公钥（Public key），可以通过认证中心（Authentication Authority, CA）进行注册公布，或者可由系统任意参与者根据该用户的公开信息多项式时间内计算出来；对应的解密密钥则是秘密的，称为私钥（Private key），除用户自己，其它任何人不能由 k_e 或其它公开信息计算得到。PKC 主要基于 NP 难解性问题，将加密和解密能力分开，因而可以实现：①一个用户可通过对方的公钥向系统中的多个用户发送加密消息；②一个用户的加密消息可由其它多个用户解读。前者可用于公开信道中实现保密通信，而后者可用于实现对用户的认证。常见的公钥密码算法有 RSA、Elgamal、Rabin、MH 背包算法等。

对称密码体制和公钥密码体制均能提供机密性，但对称密码的效率更高，因此它常用于数据量较大的保密通信中，而公钥密码常用于数字签名、密钥协商、实体认证等。

2.3.2 Hash 函数

Hash 函数是一个从消息空间到像空间的不可逆映射，也称为散列函数、哈希函数、杂凑函数等。Hash 函数是一种具有压缩特性的单向函数，它可以将任意长度的输入经过变换得到固定长度的输出，其像通常称为散列值（Hash Value）、消息摘要（Message Digest）或数字指纹（Digital Fingerprint）。我们设 $H:\{0,1\}^* \to \{0,1\}^n$ 为一输出长度为 n 的 Hash 函数，则它满足以下条件：

（1）能够应用于任意长度的消息，且产生定长的输出。

（2）对任意给定的消息 x，计算 $H(x)$是容易的，用硬件和软件均可实现。

（3）对于任意给定的消息 z，寻找 x，使得 $H(x) = z$ 是不可行的。

（4）对于任意给定的消息 x，寻找 y，使得 $y \neq x$ 且 $H(x) = H(y)$ 是计算上不可行的。

（5）寻找 (x, y)，使得 $x \neq y$ 且 $H(x) = H(y)$ 是计算上不可行的。

性质（1）中的“任意”是指在实际中存在的，“定长的输出”是 Hash 函数的基本特性，性质（2）值指 Hash 函数的可用性，性质（3）、（4）、（5）则是 Hash 函数为满足不同应用而需具备的安全特性。

性质（3）称为单向性（One-way），也称为抗原像性（Pre-image Resistance），是 Hash

函数的基本性质，它可以防止由消息的散列值逆向求出消息，这个性质是满足性质（4）和（5）的必要条件。如果 Hash 函数不满足单向性，那么寻找碰撞不再是困难的。

性质（4）和（5）是指 Hash 函数应具有抗碰撞性。性质（4）称为抗弱碰撞性（Weakly Collision-free），也称为抗第二原像性（Second Pre-image Resistance），它可以防止对 Hash 函数的伪造，即将一个消息的散列值伪造成另一个消息的散列值在计算上是不可行的；性质（5）称为抗强碰撞性（Strongly Collision-free），它可以防止对 Hash 函数实施生日攻击。抗强碰撞性的 Hash 函数比抗弱碰撞性的 Hash 函数的安全性更高，即满足抗强碰撞的 Hash 函数肯定满足抗弱碰撞性，反之不成立。

常见的 Hash 函数有 MD5、SHA-1、SHA-256、RIPEMD-160 等。

2.3.3 MAC 算法

认证可分为实体认证和消息认证两种。实体认证用来验证实体的身份，消息认证用来验证消息的真实性。消息认证有两个作用，一是验证信息来源的真实性，一般称为信息源认证；另一个是验证消息的完整性，即消息在传输和存储过程中没有篡改、伪造等。消息认证码（MAC，Message Authentication Code）是一种认证技术，是指消息被一密钥控制的公开函数作用后产生的、用于认证符的、固定长度的数值，也称为密码校验和。认证码与通信中的检错码不同，检错码用来检测由于通信缺陷而导致消息发生的错误，而认证码是用来防止攻击者恶意篡改或伪造消息。例如，发送方 *A* 和接受方 *B* 共享一个密钥 *K*，若 *A* 向 *B* 发送消息 *M*，则 *A* 计算

$$MAC = C_K(M)$$

其中 $C_K(\cdot)$是密钥控制的公开函数，称为认证函数，*MAC* 是 *M* 的消息认证码，称为 MAC 值。*A* 将原始消息 *M* 和 *MAC* 一起发送给 *B*。*B* 对收到的消息 *M′*用同样的密钥进行相同认证函数的计算，得出新的 *MAC′*，并将接收到的 *MAC* 与其计算出的 *MAC′*进行比较。如果仅收发双方知道密钥 *K*，且 *B* 计算得到的 *MAC′*与接收到的 *MAC* 一致，则：

（1）接收方可以相信发送方发来的消息未被篡改。因为攻击者不知道密钥，所以不能够在篡改消息后相应地篡改 MAC 值，而如果仅篡改消息，则接收方计算的新 MAC 值将与收到的 MAC 值不同。

（2）接收方可以相信发送方不是冒充的。因为除收发双方外再无其他人知道密钥，因此第三方不能产生正确的消息和 MAC 值。

MAC 函数与加密算法类似，不同之处为 MAC 函数不必是可逆的，另外，输出的结果也有区别，MAC 函数输出的 MAC 值是定长的，而加密算法输出的程度与明文程度有关。因此，MAC 函数的设计比加密算法更为灵活。近年来，人们越来越多地利用 Hash 函数来设计 MAC 算法，这是因为：

（1）Hash 函数（如 MD5、SHA-1）的软件实现快于分组密码（如 DES）的软件实

现。

（2）Hash 函数的库代码来源广泛。

（3）Hash 函数没有出口限制，而分组密码即使用于 MAC 也有出口限制。

但是，Hash 函数并不是专为 MAC 而设计的，且 Hash 函数不使用密钥，所以它不能直接用做 MAC。目前已提出许多基于 Hash 的消息认证算法，其中 HMAC（RFC 2104）是实际应用中使用最多的方案，已作为 FIPS198 被公布，其中广泛使用的安全协议 SSL（Secure Socket Layer）就是用 HMAC 来实现消息认证功能。

2.4 计算复杂性理论

基于计算复杂性的可证明安全方法在证明协议的安全性时，常用到下面的基本概念，我们给出严格的定义[118]：

定义 2.2　对于两个函数 $f(x)$和 $g(x)$，若存在一个正常数 k 和一个正整数 x_k，满足对所有 $x > x_k$，都有 $0 \leqslant f(x) \leqslant kg(x)$，则我们说 $f(x) = O(g(x))$。

定义 2.3（可忽略函数）　称函数 $f(x)$是可忽略的，则对于任意多项式 $p(\cdot)$，总存在一个自然数 $k \in \mathbb{N}$，使得对于所有 $x > k$，$f(x) < \frac{1}{p(x)}$。

定义 2.4（不可忽略函数）　若 $f(x)$不是可忽略函数，则 $f(x)$是不可忽略函数。

定义 2.5（多项式时间算法）设一个算法的输入长度为 n，如果在最坏情况下，该算法的运行时间是$O(n^k)$的一个函数，其中 k 为常数，那么称该算法为多项式时间算法。反之，若一个算法的运行时间不能够被这样界定，那么我们称它为一个非多项式时间算法。

定义 2.6（计算不可区分）：称两个概率总体 $X = \{X_n\}_{n\in\mathbb{N}}$ 和 $Y = \{Y_n\}_{n\in\mathbb{N}}$ 是计算不可区分的，如果对于任意的概率多项式时间算法 $\mathcal{M}$，以及任意的正多项式 $g(n)$，都存在 $k \in \mathbb{N}$ 使得 $n > k$ 时，满足

$$|\Pr[\mathcal{M}(X_n, 1^n) = 1] - \Pr[\mathcal{M}(Y_n, 1^n) = 1]| \leq \frac{1}{g(n)}$$

定义 2.7（生日悖论）：一个 k 个人的房间，则有人的生日相同的概率为

$$p = 1 - (1 - \frac{1}{365})^{\frac{k(k-1)}{2}}$$

若令 $p = \frac{1}{2}$，则 $k \approx 22.49$，这种现象称为生日悖论。将这种现象一般化，令 $E(n,k)$ 表示将 k 个小球随机掷向 n 个篮子时，至少有两个小球落入一个篮子的事件概率，则

$$E(n,k) = 1 - (1 - \frac{1}{n})(1 - \frac{2}{n}) \cdots (1 - \frac{k-1}{n}),$$

进一步可得

$$1 - e^{\frac{-k(k-1)}{2n}} \leq E(n,k) \leq \frac{k(k-1)}{2n}$$

定义 2.8（离散对数问题(DLP: Discrete Logarithm Problem)）：　令$<\mathbb{G}, \cdot>$表示一个阶为 q 的群，g 表示它的生成元。离散对数问题是：给定一个元素 $y \in_R \mathbb{G}$，计算整数 $x \in \mathcal{Z}_q$，使得 $y = g^x \bmod q$。

定义 2.9（计算 Diffie-Hellman 问题(CDHP: Computational Diffie-Hellman Problem)): 令$<\mathbb{G},\cdot>$表示一个阶为q的群，g表示它的生成元。计算 Diffie-Hellman 问题是：给定三元组$<g, g^a, g^b>$ (其中，随机元素$a, b \in_R \mathcal{Z}_q$)，计算g^{ab}。

定义 2.10（因子分解问题(IFP: Integer Factorong Problem)): 给定一个奇合数$N \in \mathbb{N}$，计算整数$x \in \mathbb{N}$，使得$x \mid N$。

2.5 随机预言机模型

如何设计一个面向具体应用的密码协议，同时平衡可证明安全性和实用性，成为密码协议设计中的重要问题。人们很难接受一个安全但效率非常低下的协议，因此一个低效率的方案与不安全的方案一样，都无法在实际中广泛使用。随机预言机模型一经提出，便成为了平衡密码方案可证安全性和实用性的重要途径[99]。许多广泛应用的密码方案都是在随机预言机模型下可证安全的，如公钥加密（Public Key Encryption）方案 RSA-OAEP，数字签名（Digital Signature）方案 PSS。

随机预言机模型在构建可证安全密码协议时，主要思想在于哈希函数首先被考虑为随机函数－－随机预言机。在协议开始设计的时候，系统中的各个角色共享随机预言机完成操作。当协议设计完成之后，再用实际的哈希函数将此随机预言机替换掉[110]。

定义 2.11 (随机预言机): 哈希函数$H:\{0,1\}^* \rightarrow \{0,1\}^n$ 如果满足以下性质：

- 均匀性：预言机H的输出在$\{0,1\}^n$上均匀分布；
- 确定性：对于相同的输入，预言机H的输出值必定是相同的；
- 有效性：给定一个输入串x，$H(x)$的计算可以在关于x的长度规模的低阶多项式（理想情况是线性的）时间内完成。

称其为随机预言机。

定义 2.12 (随机预言机模型（Random Oracle Model, ROM): 在证明密码协议的安全性时，如果利用随机预言机的上述性质，那么这样的证明模型称为随机预言机模型[101]。

在 ROM 下，通常将整个证明过程形象化为一个仿真游戏（Game），如图 2.2 所示。证明的主要思想是：如果仿真游戏以不可忽略的概率取胜，那么协议所基于的困难性问题（典型的如 CDHP, DLP, IFP）被攻击者解决的概率不可忽略，这与实际中该已知困难问题的难解性相矛盾，因而该攻击者在现实中是不存在的，协议在 ROM 模型下是安全的[99,110]。在基于 ROM 的证明中，除了随机预言机(Random Oracle)之外，还定义了一个特殊的代理，称之为模拟器（Simulator, 简称 Simon），它以规定的某种方式模拟每个参与者（包括攻击者 Malice）的随机预言行为。每当 Malice 产生一个随机预言查询，Malice 实际上不知情地将该查询递交给 Simon， Simon 应遵循查询顺序并且及时返回查询结果，这一过程被称之为训练（Trainning）。在仿真游戏的结尾，模拟器给出预先选择的

挑战（Challenge），如果 Malice 成功解决挑战，那么意味着 Malice 在仿真游戏中取胜。因为预先选择的 Challenge 包含有模拟器可用来解决协议所基于的困难问题的知识（Knowledge），若 Malice 成功解决挑战，那么模拟器可成功解决该困难问题，显然这是与实际情况相矛盾的，证明完成。

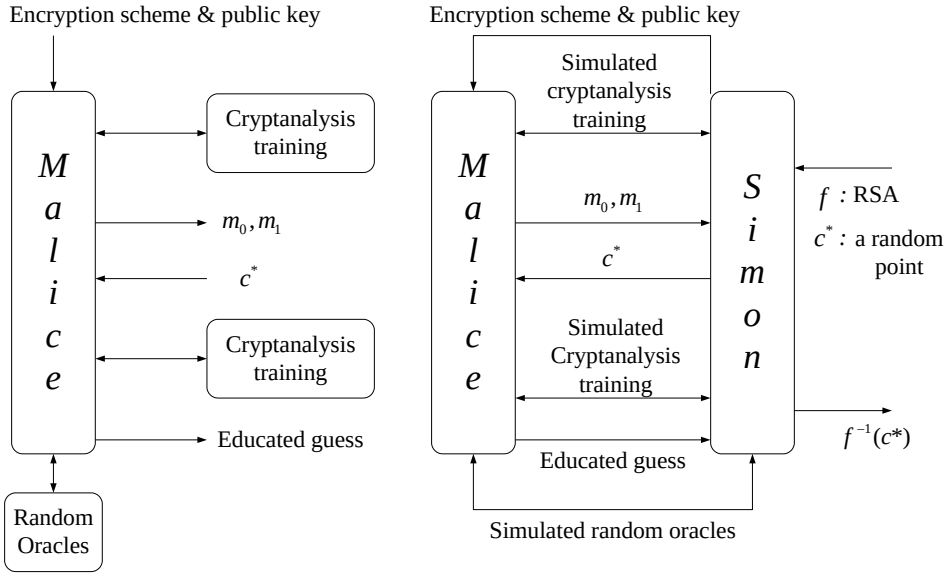

图2.2 ROM下的仿真游戏过程

2.5 本章小结

本章主要介绍了论文所基于的基础理论和预备知识。首先总结了密码协议设计所应遵循的基本准则；然后总结了基于智能卡的远程用户口令认证协议中的攻击者能力模型以及协议所应实现的安全目标；接着介绍了基本密码学组件和计算复杂性理论；最后，简要描述了随机预言机 ROM 安全模型。

第 3 章 远程用户认证协议评价指标研究

本章首先通过对近期三个典型协议进行分析，指出其中的安全漏洞和功能缺陷，揭示远程用户口令认证设计中存在的挑战和难题。然后，从安全性、理想属性和效率这三个维度出发，在对各维度的构成元素进行准确刻划的基础上，研究各维度内部构成元素之间、不同维度构成元素之间的相互关系，为评价协议的优劣和避免协议设计失误提供参考。最后，提出三个重要指标的设计原则，并通过相关典型案例来检验所提出设计原则的有效性，为设计安全高效的协议提供指导性建议。

3.1 对近期三个典型协议的分析

远程用户认证协议可分为基于公钥技术和基于对称密码技术两类，而基于公钥技术的协议又可以分为基于 RSA 和基于 Diffie-Hellman 两类。本节分析近期三个典型方案：Xie 等方案[33]、Hao 等方案[34]和 Hsieh 等方案[77]。其中， Xie 等方案基于 RSA 公钥技术，Hao 等方案基于 Diffie-Hellman 技术，Hsieh 等方案基于对称密码技术。

本节所使用的符号及其含义如表 3.1 所示。

表 3.1 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

3.1.1 对 Xie 等方案的分析

3.1.1.1 Xie 等方案的回顾

2009 年 Park 等[119]提出了一个基于智能卡和大数因子分解难解性的远程用户口令认证方案，宣称他们的方案是第一个能抵抗离线口令猜测攻击的基于非窜扰智能卡的口令认证方案，而且具有不需要存储口令表、传输和计算量小、没有时间戳等优点。Park 等方案的核心设计思想是，即使攻击者获得智能卡中的秘密参数信息，但攻击者无法验证所猜测口令的正确性，进而也就抵御了口令猜测攻击。2010 年，Xie 等[33]分析发现 Park 等提出的方案实际上无法抵抗伪造攻击和离线口令猜测攻击，然后提出了改进方案。谢琪等改进方案包括随机数和时间戳两种机制，并主要以随机数机制为例进行了分析。由于这两种机制类似，因此本文也只以随机数机制为例进行分析。谢琪等方案包含三个阶

段，即注册阶段、登录阶段和认证阶段，方案中所使用的符号及其含义如表 3.1 所示。

（1）注册阶段

R1. 用户 U_i 选择 ID_i 和 PW_i，通过安全信道发给远程服务器 *RS*。

R2. 服务器 S 产生大素数 p 和 q，计算 $n=pq$；选取 e 计算 d，满足 $ed=1 \mod(p\text{-}1)(q\text{-}1)$；计算 $S_i=h(ID_i \| PW_i)\oplus h(d \oplus ID_i)$；将$\{n, e, g, ID_i, S_i, h(\cdot)\}$写入智能卡，然后将智能卡通过安全信道发往 U_i。同时，S 为每个用户建立认证请求数据表 $List\_u_i$，初始为空。

（2）登录阶段

L1. 用户 U_i 输入口令 PW_i，智能卡产生随机数 N_1，计算：

$$B_i=(S_i \oplus h(ID_i \| PW_i)\oplus h(N_1) \| N_1)^e \bmod n.$$

然后把 $msg1=(ID_i, B_i)$发往服务器 S。

（3）认证阶段

V1. 服务器 S 收到来自 U_i 的 ID_i 和 B_i 后，检查 $List\_u_i$，如果 $B_i \in List\_u_i$，则终止协议；否则将 B_i 写入 $List\_u_i$ 中。计算 $B_i^d \bmod n$，读取前 128 位设为V_i，后 128 位为 N_1'，计算 $V_i'=h(d \oplus ID_i)\oplus h(N_1')$，验证$V_i$ 与V_i' 是否相等。若不等，则 S 拒绝U_i 的登录，选取随机数 M，计算$C_1=h(M)$，这是为了让U_i 无法感知登录是否成功；若相等，则服务器 S 接受U_i 的登录，计算:

$$C_1=h((N_1+1) \| (h(d \oplus ID_i)+2)^d \bmod n,$$

然后 S 将 $msg2=C_1$ 发往 U_i。

V2. U_i 收到来自 S 的消息 C_1 后，计算 $C_1^e \bmod n$，并比较

$$C_1^e \bmod n=h((N_1+1) \| (S_i \oplus h(ID_i \| PW_i)+2)),$$

是否相等，如果不等则终止协议，否则认证成功。

3.1.1.2 Xie 等方案的安全性分析

谢琪等宣称所提出的改进方案可以抵抗重放攻击，但本文分析发现，该方案不能抵抗重放攻击、内部人员攻击和密钥泄露仿冒攻击。

(1) 重放攻击

分析发现 Park 等方案[119]无法抵抗重放攻击，但谢琪等没有意识到该安全缺陷，他们所提出的方案继承了这一缺陷，下面给出攻击方法。

在用户 U_i 的第 k $(k \geq 1)$次登录过程中，攻击者把 U_i 发给远程服务器 S 的消息 $msg1=(ID_i, B_i)$篡改为 $msg1'=(ID_i, B_i')$，则服务器 S 收到 $msg1'$ 后必将通不过验证，S 向 U_i 发送 $C_1=h(M)$。用户 U_i 在收到 C_1 也将通不过验证，确定此次认证失败。实际上，攻击者将 $msg1=(ID_i, B_i)$篡改为 $msg1'=(ID_i', B_i)$ 亦可实现此目的，这里仅以篡改 B_i 为例。

现在，由于 B_i 未曾达到远程服务器 S，因此 $B_i \notin List\_u_i$，攻击者即使不知道用户的口令 PW_i，仍可重放 $msg1=(ID_i, B_i)$，$msg1$ 将顺利通过谢琪等方案设计的重放攻击检测机制，进而通过远程服务器 S 的验证，攻击成功。

（2）内部人员攻击

现实生活中，用户常为了方便而在多个不同的系统（帐户）中使用相同的口令[114]。如果用户将口令以明文或其它容易被恢复出来的方式在注册时提交给服务器，则服务器端的恶意内部人员可利用用户的口令仿冒登录其它服务系统[120]。在 Xie 等方案中，用户直接将口令以明文的方式向服务器提交。因此，Xie 等方案无法抵抗内部人员攻击。

（3）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[72]。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 Xie 等方案中，如果服务器的长期私钥 d 因偶然泄露或被窃取，则攻击者可截获并解密用户 U_i 发往远程服务器 S 的 B_i，获得 N_1，计算 $h(N_1)$，进而计算出 $S_i \oplus h(ID_i \| PW_i) = V_i \oplus h(N_1)$。然后攻击者选取随机数 N_1'，公钥 e 又是公开的，因此可计算：

$$B_i' = (S_i \oplus h(ID_i \| PW_i) \oplus h(N_1') \| N_1')^e \bmod n,$$

然后把 $msg1=(ID_i, B_i')$发往 S。显然 B_i'能够通过服务器 S 的验证，冒充合法用户成功。

3.1.2 对 Hao 等方案的分析

2007 年 Wang 等[8]针对文献[80]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[12]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[34]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[34]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。

3.1.2.1 Hao 等方案的回顾

Hao 等方案[34]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 3.1 所示。

(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 $q \mid p-1$，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。

(2) 登录阶段

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

(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。

(4) 口令更新阶段

C1. 执行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。

3.1.2.2 Hao 等方案的安全性分析

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。

（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[116]。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。攻击者通过能耗分析或旁路信息泄露等边信道攻击技术[14, 15, 78]，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[114-116]，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）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[72]。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。

（3）不可修复性问题

当攻击者通过上文中的攻击方法获取用户 U_i 的口令 PW_i 后，或者当服务器 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。

（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[107, 108]。 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[109]。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[8]、Chen等方案[12]和Hao等方案[34]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”。

3.1.3 对 Hsieh 等方案的分析

由于智能卡是资源受限设备，因此一个协议对资源的需求越低，越具有实用性。自 2000 年 Sun 等[121]首次尝试仅基于 Hash 函数来设计安全高效的远程用户口令认证协议以来，随后大量的此类协议[6, 83, 122-124]被提出。这个协议都假设智能卡的抗窜扰的，即智能卡内秘密信息不能被攻击者分析出来，但 Kocher 等[14]和 Messerges 等[15]的研究表明，普通智能卡内参数信息可通过能耗分析或旁路信息泄露等边信道攻击技术被攻击者分析出来。2004 年，Ku 等[120]首次注意到了这个问题，提出了第一个基于非抗窜扰智能卡的远程用户口令认证协议，该协议仅使用了 Hash 函数，没有公钥密码操作，十分高效。不幸的是，200 年 Yoon 等[6]指出 Ku 等方案无法抵抗平行会话攻击，并且口令更新过程存在不安全因素。此后，众多学者试图在非抗窜扰智能卡上实现高效的仅基于 Hash 函数的远程用户口令认证协议[6, 8, 9, 12, 13, 20, 21, 31, 125]。但是，这些协议在提出不久都被发现存在这样或那样的安全问题。2012 年，Hsieh 等[77]针对文献[21]中的协议存在离线口令猜测攻击和仿冒攻击等安全缺陷，提出了一个仅基于 Hash 函数的改进方案，声称改进方案是安全高效的。但是本文分析发现，Hsieh 等方案无法实现所声称的抗离线口令猜测攻击，对内部人员攻击是脆弱的，无法实现前向安全性，并且存在用户友好性差、不适于移动应用等问题。

3.1.3.1 Hsieh 等方案的回顾

Hsieh 等方案[77]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 3.1 所示。

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

R3. 服务器 S 在数据库中为 U_i 产生一个数据表项，保存 $n=0$。然后 S 计算 $EID = h(ID_i \| i)$，$P = h(EID \oplus x)$，$R = P \oplus h(b \oplus PW_i)$ 和 $V = h(h(PW_i) \oplus h(x))$。最后将 $\{R, h(\cdot)\}$ 写入智能卡，将 $\{V\}$ 写入与 ID_i 对应的表项。

R4. $S \Rightarrow U_i$:智能卡。

R5. U_i 将 b 写入智能卡。

(2) 登录阶段

L1. 用户 U_i 插入智能卡读卡器，输入 ID_i 和 PW_i。

L2. 智能卡读取当前时间戳 T_u，计算：

$$C_1 = P \oplus h(b \oplus PW_i),\quad C_2 = h(C_1 \oplus T_u)。$$

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

(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 $T_s - T_u \le 0$，则拒绝登录请求。

V2. S 计算 $C_2' = h(h(EID \oplus x) \oplus T_u)$，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 $C_3 = h(h(EID \oplus x) \oplus h(T_s))$。

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

V4. U_i 首先检查 T_s 的有效性，然后计算 $C_3' = h(C_1 \oplus h(T_s))$，并验证 $C_3' = C_3$ 是否成立。如果成立，则 U_i 成功认证服务器 S，认证完成。

(4) 口令更新阶段

该阶段用户需要通过安全信道与服务器进行交互，由于该阶段与后面的讨论无关，故不在这里详述，读者可参见文献[77]。

3.1.2.2 Hsieh 等方案的安全性分析

Hsieh 等[77]指出，在 Hsiang-Shi 方案[21]中，一旦用户分析出智能卡内秘密参数信息，就无法抵抗离线口令猜测攻，然后专门针对该缺陷提出了改进方案。但本文研究发现该方案仍无法实现这一基本安全目标，对内部人员攻击是脆弱的，并且存在用户友好性差、时间同步问题。

（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[116]。而我们分析发现 Hsieh 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。攻击者通过能耗分析或旁路信息泄露等边信道攻击技术[14, 15, 78]，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_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：$P^* = R \oplus h(b \oplus PW_i^*)$，

$$C_2^* = h(C_1^* \oplus T_u) = h(P^* \oplus T_u)$$；

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）。

用 $|\mathcal{D}|$ 表示用户口令空间大小，上述流程的时间复杂度为 $\mathcal{O}(|\mathcal{D}| * (3T_X + 2T_H))$。在实际中，$|\mathcal{D}|$ 一般非常有限[114-116]，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_2 $(= h(P \oplus T_u))$ 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）内部人员攻击

现实生活中，用户常为了方便而在多个不同的系统（帐户）中使用相同的口令[114]。如果用户将口令以明文或其它容易被恢复出来的方式在注册时提交给服务器，则服务器端的恶意内部人员可利用用户的口令仿冒登录其它服务系统[120]。在Hsieh等方案中，用户将口令的Hash值$h(PW_i)$向S提交。因此，服务器端的恶意内部人员可恢复出用户口令

1）攻击者猜测 U_i 的口令为 PW_i^*；

2）验证 $h(PW_i^*)=h(PW_i)$，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，$|\mathcal{D}|$一般非常有限[114-116]，攻击能够在多项式时间内完成。

（3）用户友好性差问题

在口令协议中，为确保口令的安全性，用户应不定期的更新口令。是否支持用户本地自由更新口令是衡量一个协议是否具有用户友好性的一个重要指标[74]。在 Hsieh 等方案的口令更新阶段，用户需要通过安全信道与服务器端交互。一方面，用户不能本地更新口令；另一方面，需要通过安全信道，这在现实中会给用户带来很多不便。因此，Hsieh 等方案中的口令更新阶段存在用户友好性差的问题。

（4）时间同步问题

在无线或移动网络中，系统的时延具有较大的波动性，基于时间戳机制的协议仍然可能遭受重放攻击[109]。另一方面，在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[107, 108]。因此，如Islam 等[42]所指出的，时戳机制不适于移动应用。

3.2 协议评价指标内在关系研究

虽然有大量的文献[5, 8, 13, 126-131]对已往协议的安全性（表 1.1 中的 *S1~S12*）、理想属性（表 1.2 中的 *U1~U10*）和性能进行分析，但有关这些评价指标内部构成元素之间、评价指标之间的关系研究较少。除了效率评价应主要包括计算量、通信量、存储量三方面取得共识外，对安全性和理想属性的具体评价内容至今尚没有统一的认识[18]。产生这种混乱局面的一个重要因素就是对这些评价指标定义不清；另一个重要因素就是这些评价指标间的关系十分复杂，有的之间互相包含，有的之间互斥，还有的之间共生。举个例子，Ku 等方案[80]在服务器端需要为用户 U_i 保存一个非敏感数据表项$\{ID_i, n_i\}$不违背“无验证表项”这一理想特性，因为$\{ID_i, n_i\}$不像口令表项，如$\{ID_i, h(PW_i)\}$那样敏感，即使被攻击者获取也不会对系统安全性造成危害（如果服务器端可以确保$\{ID_i, n_i\}$的完整性的话）；Wang 等[8]认为在服务器端为用户 U_i 保存一个非敏感数据表项，如$\{ID_i, n_i\}$，仍然违背了“无验证表项”这一理想特性，因为服务器仍然需要增加额外的维护、查询

负担，以及完整性保护措施；Chung 等指出，如果为了实现“无验证表项”这一理想特性，不在服务器保存一些用户相关参数，如$\{ID_i, n_i\}$，协议将无法实现“可修复性”这一理想特性，这里需要 “安全性—性能”的平衡；Wang 等分析发现，如果不在服务器保存一些用户相关参数，如$\{ID_i, n_i\}$，协议将无法实现“抗密钥泄露仿冒攻击”这一安全目标。为此，我们首先对安全性和理想属性这两个评价指标的具体内容，也就是 *S1~S12* 和 *U1~U10* 进行清晰的定义，然后再梳理它们之间的关系。

3.2.1 安全性具体评价指标的定义

有关安全性这一评价指标的具体内容 *S1~S12* 的定义详见节 2.2.2。

3.2.2 理想属性具体评价指标的定义

（1）服务器端无验证表项[86]（*U1*）

服务器端无须保存敏感数据表项。这里的“敏感”相对该表项内容被攻击者获取后造成的危害而言：如果表项是“敏感”的，攻击者获取后将多项式时间内恢复出用户口令或直接仿冒用户登录，典型的“敏感”表项如明文口令或口令的派生值 $h(PW_i)$；如果表项是“非敏感”的，攻击者除了可以破坏表项的完整性，获取该表项内容对攻击者破坏系统安全性没有任何帮助[81, 86]，典型的“非敏感”表项如$\{ID_i, T_{reg}\}$，其中 T_{reg} 表示用户的注册时间。实现该属性有两种方式：1）在服务器端不保存任何数据表项，如 Wang 等方案[8]；2）在服务器端仅保存非敏感数据表项，如 Chung 等方案[81]。我们称实现方式 1 的协议具有“*U1*-强”属性，实现方式 2 的协议具有“*U1*-弱”属性。

（2）口令本地自由更新[18]（*U2*）

用户可以在本地更新口令，自由选择，并且无须与服务器端进行交互。注意 *U2* 与“口令自由更新”[69]这一说法的区别：后者虽然支持用户自由选择所要更新的口令，但口令更新这一过程需要与服务器进行交互。实现该属性也有两种方式：1）协议不仅支持用户本地更新口令，而且会检查用户所输入旧口令的合法性，如 Kim 等方案[20]；2）协议支持用户本地更新口令，但不检查用户所输入旧口令的合法性，如 Yang 等方案[18]我们称实现方式 1 的协议具有“*U2*-强”属性，实现方式 2 的协议具有“*U2*-弱”属性。

（3）双向认证[69]（*U3*）

不仅服务器能够证实用户的合法性，而且用户也能够证实服务器的身份。提供强双向认证可抵抗仿冒攻击（中间人攻击）。用户到服务器的认证和服务器到用户的认证的简单组合常常并不意味着双向认证[132]。

（4）前向安全性[69]（*U4*）

即使服务器的长期秘钥泄露，此前协商的会话密钥的安全性不受影响。该属性是为了评价系统终极失效（服务器的长期私钥泄露）后的强健性。

（5）口令错误输入及时检测[8, 69]（*U5*）

在登录阶段，如果用户不小心输入错误口令，协议能够及时提示用户口令输入错误，而不是将错误的登录请求信息继续发往服务器，通过服务器对用户登录的拒绝来判断口令输入的失误。

（6）智能卡撤销[30, 69, 82]（*U6*）

在用户智能卡丢失的情况下，用户丢失的智能卡的有效性能够被服务器撤销，以防攻击者滥用该卡。

（7）密钥协商[70]（*U7*）

协议支持在认证过程中协商一个用于后续数据通信的会话密钥。该会话密钥只能够被通信的双方获知，对任何其它方来说与同等长度的随机值不可区分。

（8）用户匿名性[69, 70]（*U8*）

该属性关乎用户的隐私。用户匿名性有两个层次：一是攻击者无法获知用户的身份标识 *ID*，即 Sender anonymity; 二是攻击者无法分辩出两个会话是否由同一个用户参与的，即 Sener un-traceability。容易看出，第二个层次更高级，对用户的隐私保护得更彻底。绝大多数协议中所说的匿名性指的是实现了第二个层次的的匿名性。一些仅实现了第一个层次，即 Sender anonymity，的协议中[31, 133]，攻击者仍可以跟踪用户的行动，对用户的隐私构成威胁。

（9）可修复性[30, 81]（*U9*）

该属性关心的是，当用户的智能卡丢失或核心参数泄露，用户需要重新注册时，用户是否仍可以使用原来的用户名。在很多情况下，用户的用户名是唯一确定的或不便更换的。如果协议支持在用户重注册时使用原来的用户名，且系统的安全性不受影响，则称该协议具有可修复性；否则，称该协议的修复性较差。

（10）无时钟同步[30, 42]（*U10*）

如节 3.1.2 所述，在分布式网络中，如 Internet，进行时钟同步代价高昂，且由于网络拥堵的不确定性带来时延的不可预测性，不适于使用时戳机制来提供消息的新鲜性。

3. 2. 3 评价指标间关系的梳理

3.2.3.1 安全性评价指标内部元素间关系

在已往研究中，*S1~S10* 这 10 个安全目标是基于智能卡远程用户认证口令认证协议的基本安全目标，几乎所有的（双因子认证）协议都试图满足这些目标，这些目标间彼此独立；*S10~S12* 这三个安全目标是认证密钥协商协议[72, 73]关注的对象，这些目标间彼此独立。在文献[134]中，作者首次注意到，因为双因子认证协议中通常都协商了会话密钥，*S10~S12* 这三个安全目标也应是双因子认证协议中重要的安全需求。基于作者对近期 100 余个相关协议的分析经验，*S1~S12* 这 12 个安全目标间可能不彼此独立，但也不

属于共生、互斥或包含关系。其中，非共生、非包含关系比较明显，是否存在互斥关系还有待考证。幸运的是，文献[82]中提出了一个安全高效的、能够满足 *S1~S12* 的远程用户口令认证协议，这表明 *S1~S12* 这些安全目标间不是互斥的。

3.2.3.2 理想属性评价指标内部元素间关系

如文献[69]在 2012 年初所指出的，当前还不存在能够满足 *U1~U10* 这 10 个理想属性的协议。作者分析发现，产生这种现象的一个重要因素就是，已往研究中很少关注这些属性内部间的关系。举个例子，如何实现 *U1* 直接影响着 *U6* 和 *U9* 的满足与否：如果协议在服务器端不为用户存储任何表项（即实现 *U1*-强），则 *U1* 显然满足，但 *U6* 和 *U9* 必将无法满足；如果协议在服务器端仅存储非敏感表项（即实现 *U1*-弱），则 *U1* 满足，同时 *U6* 和 *U9* 也将容易满足。如果不注意到这个关系，必然会顾此失彼。

对于 *U2*，有一个需要注意的地方是，如果协议实现了“口令本地自由安全更新”（即实现 *U2*-强），则协议将容易实现 *U5*；如果协议仅实现了“口令本地自由更新”而不能实现“口令本地自由安全更新”（即实现 *U2*-弱），则协议无法实现 *U5*。

对于 *U3~U10*，它们与其它理想属性间彼此独立。此论断可通过实例进行论证。比如，2012 年 Wu 等[37]提出的基于 ECC 的匿名认证方案可实现除 *U5* 外的所有理想属性，这就表明 *U5* 与其它理想属性间是彼此独立的。 可通过同样的证明方法来完成剩余部分，这里不再赘述。

3.2.3.3 理想属性评价指标与安全性评价指标间关系

一个协议如能实现越多的安全目标，满足越多的理想属性，则这个协议适于实际应用的可能性就越大。但是，安全性评价指标各元素与理想属性评价指标各元素间存在着如表 3.2 所示复杂的关系，如互斥关系、包含关系等。

（1）*U1*-强与 *S1~S12* 间关系

协议实现“*U1*-强”表示服务器端不存储有关用户的任何表项信息，攻击者无法发起“窃取验证项攻击”；服务器和客户端不需要在认证过程中维护同步信息，攻击者无法发起“拒绝服务攻击”；一旦攻击者获取服务器长期私钥，攻击者可采取完全与服务器构造验证用户认证信息相同的方式来伪造用户登录信息，发起“密钥泄露仿冒攻击”。

（2）*U1*-弱与 *S1~S12* 间关系

协议实现“*U1*-弱”表示服务器端仅存储与用户相关的非敏感表项信息，攻击者无法发起“窃取验证项攻击”；服务器和客户端不需要在认证过程中维护同步信息，攻击者无法发起“拒绝服务攻击”；即使攻击者获取服务器长期私钥，由于攻击者不知道服务器内存储的用户信息，无法采取与服务器构造验证用户认证信息相同的方式来伪造用户登录信息，即不能发起“密钥泄露仿冒攻击。”

（3）*U2*-强与 *S1~S12* 间关系

协议实现“*U2*-强”表示客户端支持口令的“本地自由安全更新”，那么意味着用户

的智能卡内必须存储口令验证参数，用以验证旧口令的合法性。如果攻击者窃取（或拾到）了用户智能卡，分析出智能卡内口令验证参数，则该口令验证参数正好为攻击者提供了一个验证所猜测口令正确与否的对比目标，协议必将遭受“离线口令猜测攻击”。

（4）*U2*-弱与 *S1~S12* 间关系

协议实现“*U2*-弱”表示客户端支持口令的“本地自由更新”，但不支持“安全更新”。如果攻击者获得了接触用户智能卡的临时机会，可随意更新用户的口令，致使智能卡内参数信息发生改变，而合法用户只知道所持有的旧口令。即使攻击者将智能卡还给用户，用户无法输入正确的新口令，智能卡不能构造正确的登录信息，造成“智能卡丢失攻击”。

（5）*U3* 与 *S1~S12* 间关系

协议实现“双向认证”表示攻击者无法仿冒用户欺骗服务器，也无法仿冒服务器欺骗用户。 “仿冒攻击”、“平行会话攻击”、“未知密钥共享攻击”都会违背协议的双向认证性。因此，如果一个协议实现了双向认证性，则必然满足 *S3, S6, S9* 和 *S10*。

表 3.2 理想属性评价指标与安全性评价指标间关系

	S1	*S2*	*S3*	*S4*	*S5*	*S6*	*S7*	*S8*	*S9*	*S10*	*S11*	*S12*
U1-强	*	共生	*	*	*	*	共生	*	*	*	*	互斥
U1-弱	*	共生	*	*	*	*	共生	*	*	*	*	共生
U2-强	互斥	*	*	*	*	*	*	*	*	*	*	*
U2-弱	*	*	*	互斥	*	*	*	*	*	*	*	*
U3	*	*	包含	*	*	包含	*	*	包含	包含	*	*
U4	*	*	*	*	*	*	*	*	*	*	*	*
U5	*	*	*	*	*	*	*	*	*	*	*	*
U6	*	*	*	*	*	*	*	*	*	*	*	共生
U7	*	*	*	*	*	*	*	*	*	*	*	*
U8	*	*	*	*	*	*	*	*	*	*	*	*
U9	*	*	*	*	*	*	*	*	*	*	*	共生
U10	*	*	*	*	*	*	*	*	*	*	*	*

注：　†“*”表示独立关系或关系未知；

††“U_i 与 S_j 共生”表示如果 U_i 或 S_j 中有一个成立，则 U_i 和 S_j 都成立；

†††“U_i 与 S_j 互斥”表示如果 U_i 或 S_j 中有一个成立，则另一个必不成立；

††††“U_i 包含 S_j”表示如果 U_i 成立，则 S_j 必成立。

（6）*U6* 与 *S1~S12* 间关系

协议支持“智能卡撤销”表示用户智能卡过期或丢失后，服务器可使该失效智能卡无法继续登录成功。这就意味着服务器端需要保存用户（或用户智能卡）相关参数信息。协议正好可利用这些用户相关参数信息来实现“抗密钥泄露仿冒攻击”。文献[81, 86, 135]中的协议正是采用了这个策略。

（7）*U9* 与 *S1~S12* 间关系

协议具有“可修复性”表明用户智能卡丢失或发现核心安全参数泄露后，用户可用原来的用户名 ID 重新注册。这与（6）中的情况类似，服务器端需要保存除用户的身份标识 ID 外的其它相关参数。协议正好可利用这些用户相关参数信息来实现“抗密钥泄露仿冒攻击”。文献[81, 86, 135]中的协议均采用了这个策略。

3.3 协议设计的三个原则

自 1993 年 Chang 和 Wu 首次提出基于智能卡的远程用户口令认证协议以来，数以百计的协议被提出，并且有大量的文献[5, 8, 13, 127-131]讨论已往协议的安全缺陷，但是对此类协议设计原则的相关研究却很少，导致了同样的根本性错误一再重复。举个例子，自 2006 年以来很多学者试图在非抗窜扰智能卡假设下，仅基于对称密码原语（如对称加密算法，Hash 函数，异或运算）来设计可抗离线口令猜测攻击的远程用户认证协议，近期的如[12, 27, 31, 35, 76, 77]。这些协议都随后被发现无法抵抗离线口令猜测攻击，但立即又有新的企图采用“更巧妙设计”的仅基于对称密码原语的改进方案被提出。正如下面将证明的，无论协议构造如何“巧妙”，这种设计策略在本质上是不可行的。

3.3.1 公钥技术原则

作者分析 100 余个近期提出的协议，发现所有基于非抗窜扰智能卡、未采用公钥技术的协议都无法抵抗离线口令猜测攻击。换句话说，所有那些基于非抗窜扰智能卡假设，仅基于对称密码技术却声称能够抵抗离线口令猜测攻击的协议都是无法实现所宣称安全的，最近的典型例子如[12, 13, 31]。

接下来将证明这绝非偶然。在非抗窜扰智能卡假设下，智能卡内秘密参数可被攻击者分析出来。不难看出的是，一旦攻击者获取用户的智能卡，分析出智能卡内参数后，双因子协议便退化为一个单因子协议（仅基于口令）。在文献[72]中，Halevi 和 Krawczyk 已经证明，在分布式计算攻击模型下（即 Dolev-Yao 模型[112]），未采用公钥技术的口令认证协议（即传统的基于口令的单因子认证协议）无法抵抗离线口令猜测攻击的概率等同于“$\boldsymbol{P \neq NP}$”的概率。基于这一论断，我们可以得出：在非抗窜扰智能卡假设下，未采用公钥技术的远程用户口令认证协议（即双因子认证协议）无法抵抗离线口令猜测攻击的概率等同于“$\boldsymbol{P \neq NP}$”的概率。根据这一原则，可以很容易发现，所有仅基于对称密码技术的远程用户口令认证协议（如[9, 12, 27, 31, 35, 76, 77, 136]）都无法抵抗离线口令猜测攻击。现在，对策已经很明显：采用公钥技术来防御离线口令猜测攻击。

3.3.2 前向安全性原则

前向安全性关注的是会话密钥对长期密钥（对称或非对称）的依赖性，它是评价密

钥协商协议优劣的重要指标之一[137]。更确切地说，一个能实现前向安全性的协议所提供的保证是，即使一方或多方的长期私钥泄露，系统此前协商的会话密钥的安全性仍然不受影响。自然地，绝大多数协议试图实现该属性，但现实情况是很多协议都失败了，最近的典型例子如[10, 25, 138]。这些协议都声称能够实现前向安全性，结果却大相径庭。尽作者所知，基于智能卡的口令认证领域，目前还没有关于前向安全性实现原则的研究，因此同样的错误一再重复也不足为奇。

通常情况下，会话密钥由用户相关信息（如身份标识 ID）和会话相关信息（如 Diffie-Hellman 临时值 g^x）两部分信息计算而来，这也就意味着会话密钥的机密性决定于这两部分信息的机密性。一个广泛接受的策略是，为防止内部人员攻击（*S8*）和验证项篡改攻击(*S7*)，在服务器端不应保存用户相关敏感参数，因而近期几乎所有的协议都没有在服务器端保存用户相关敏感参数。再者，如果攻击者获取了服务器的长期私钥，则 $\mathcal{A}$ 可采用与服务器完全相同的办法计算与所有与会话密钥相关的用户相关信息。这也就意味着，当 $\mathcal{A}$ 获取了服务器的长期私钥后，会话密钥的机密性仅仅取决于会话相关信息的机密性。现在，我们可以在密钥协商协议这个更广的范围内讨论前向安全性的实现原则这个问题。

在文献[137]中，Park 等首次研究了密钥协商协议中前向安全性的实现原则。他们提出了实现前向安全性的两个原型：一个基于传统的 Diffie-Hellman 密钥交换技术，另一个基于服务器所选择的随机数的机密性。Park 等进一步推断，前向安全性只能由这种原型来实现。我们发现，在这两种原型中，服务器端都至少需要两次模幂运算或椭圆曲线下的点乘运算。读者可参见文献[137]了解更多的相关细节。基于 Park 等的工作，不难推出：1）实现前向安全性，公钥技术不可或缺（因为在服务器端需要进行模幂或点乘运算），这解释了文献[12, 13]中协议失败的原因；2）实现前向安全性，至少需要在服务器端进行两次模幂或点乘运算，这解释了文献[10, 25, 71, 138]中协议失败的原因。需要注意的是，上述两条推断可合二为一：至少在服务器端进行两次模幂或点乘运算是实现前向安全性的必要条件。

3.3.3 安全性-可用性平衡原则

2004 年，Yoon 等[6]指出 Ku 等[80]提出的协议虽然支持口令本地自由更新，但无法实现安全更新（即实现了“*U2*-弱”），然后提出了一个改进方案：在智能卡中增加一个口令验证因子 $V = h(EID \oplus x)$，实现“*U2*-强”。不幸的是，Hsiang 和 Shih 指出 Yoon 等的改进方案无法抵抗离线口令猜测攻击：攻击者分析出 $R = V \oplus h(b \oplus PW_i)$、$V$ 和 b，通过 $V = ? R \oplus h(b \oplus PW_i^*)$ 来验证所猜测的口令 PW_i^* 的正确性。2007 年，Nam 等[130]指出 Lee 等[139]提出的协议的口令更新阶段存在类似安全性缺陷：该协议虽然支持口令本地更新，但在更新口令过程中不检测旧口令的正确性，一旦攻击获取用户的智能卡，可以任意更

新用户的口令，完成 DoS 攻击。Nam 等进一步指出，对这种缺陷的修补是十分微妙的：如果要实现口令本地自由安全更新（即实现 “*U2*-强”），需要在智能卡内存储口令验证因子，设为 V，而这个验证因子 V 又带来了新的安全隐患。如果攻击者临时获取了用户的智能卡，通过能耗和计时攻击等边信道攻击技术分析出了 V，可发起离线口令猜测攻击。Nam 等虽然注意到了实现“*U2*-强”的微妙性，但却没有给出一个解决方案。

近来，绝大多数协议要么实现“*U2*-弱”(如[13, 18, 25, 37, 74, 140])，要么不支持“*U2*”（如[19, 81, 141, 142]），而那些试图实现“*U2*-强”的协议（如[8, 12, 26, 27, 31, 125]）都随后被发现无法抵抗离线口令猜测攻击。在文献[86]中作者发现，可用性属性“*U2*”和安全性目标“*S4*”间存在不可避免的平衡，采用“模糊验证因子”是一个较好的平衡办法。例如在 Yoon 等[6]的改进方案中令 $R=V\oplus h((b\oplus PW_i)\bmod 256)$，即使攻击者分析出了 R、V 和 b，因为 R 是模糊验证因子（模糊因子为 $\frac{1}{256}$），攻击者仅可以排除 $\frac{1}{256}$ 的潜在口令，无法确切地验证所猜测口令的正确性。采用这种平衡办法，实现了口令本地自由更新，以大于 $\frac{996}{1000}$ 的概率实现了口令的安全更新，且有效抵抗了离线口令猜测攻击。

3.4 本章小结

确保密码协议的安全性是一个公开难题，对已有协议的分析旨在为新协议的设计提供更好的参考和借鉴。本章首先分析了近期三个典型方案，指出其中的安全缺陷；然后研究了基于智能卡的远程用户口令认证协议中理想属性评价指标和安全性评价指标间的内部关系，尽作者所知，在该领域是首次进行这方面的研究；最后，为避免同样的失误一再重复，作者基于对已往 100 余个协议的分析经验，提出了设计此类协议应遵循的三个通用原则。

第 4 章 改进的适于受限资源环境的远程用户认证方案

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。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[74]。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[9, 12, 13, 83]。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[14, 15, 17]。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[8, 25, 30]，但都随后被指出存在这样或那样的安全缺陷[37, 81, 143]。

2007 年 Wang 等[8]针对文献[80]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[81]分析发现 Wang 等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[35]针对 Wang 等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 等方案[35]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。

表 4.1 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

4.1 Fang等方案简要回顾

Fang 等方案[35]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 4.1 所示。

4.1.1 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 产生随机数 N_i，计算 $k = h(ID_i \oplus x \oplus N_i)$，$R = k \oplus h(b \oplus PW_i)$，然后将{$R$，$h(\bullet)$，$h_k(\bullet)$}写入智能卡，并在后台数据库中保存新条目$\{ID_i, N_i\}$。

R4. $S \Rightarrow U_i$: 智能卡。

R5. U_i 将 b 写入智能卡。

4.1.2 登陆阶段

L1. 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

L2. 智能卡计算 $k = R \oplus h(b \oplus PW_i)$，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 $C_2 = h_k(h^2(r \oplus b) \oplus T_u)$。

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

4.1.3 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 $T_s - T_u > \Delta T$，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。

V2. S 计算 $k = h(ID_i \oplus x \oplus N_i)$，$C_1' = C_1 \oplus k$ 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 $C_3 = h_k(C_1' \oplus T_s)$。

V3. $S \rightarrow U_i:\{C_3, T_s\}$。

V4. 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 $SK = h(r \oplus b)$，认证完成。

4.1.4 口令更新阶段

C1. 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

C2. 智能卡产生随机数 r_c，读取当前时间戳 T_u，计算 $k = R \oplus h(b \oplus PW_i)$，$m_1 = k \oplus r_c$ 和 $m_2 = h_k(h(r_c) \oplus T_u)$。

C3. $U_i \rightarrow S:\{ID_i, m_1, m_2, T_u\}$。

C4. 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。

C5. S 计算 $k=h(ID_i\oplus x\oplus N_i)$，$m_1'=m_1\oplus k$ 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。

C6. S 产生随机数 N_i^{new},计算 $k_{new}=h(ID_i\oplus x\oplus N_i^{new}),m_3=k\oplus k_{new}$ 和 $m_4=h_k(h(k_{new})\oplus T_s)$。

C7. $S\rightarrow U_i$:{ m_3, m_4, T_s}。

C8. 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 $m_3'=C_3$ 是否成立。如果成立，则 U_i 选择新口令 PW_i^{new}，计算 $m_5=h_{m_3'}(m_4)$ 和 $R_{new}=k_{new}\oplus h(b\oplus PW_i^{new})$，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 $m_5'=h_{k_{new}}(m_4)$，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。

4.2 Fang等方案安全性分析

文献[70]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 等方案[15]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。

4.2.1 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，一个实用的口令认证方案应能够防御该威胁[30]。而我们分析发现 Fang 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[144]。攻击者通过能耗分析或旁路信息泄露等边信道攻击技术[14, 15, 17]，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_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 $k^*=R\oplus h(b\oplus PW_i^*)$，$M=h^*(r\oplus b)=C_1\oplus k^*$ 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 $k=R\oplus h(b\oplus PW_i)$。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，Halevi 和 Krawczyk 在文献[84]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。

4.2.2 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[72]。该安全属性关注的是，某次会话中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 $SK_j = h(r \oplus b)$ 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 $k = C_1^j \oplus SK_j$。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 $SK_t = k \oplus C_1^t$，其中 C_1^t 从公开信道截获。因此，Fang 等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 $\{ID_i,\ C_1',\ C_2',\ T_u\}$ 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。

4.2.3 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 $\{ID_i, m_3^j, m_4^j, T_s^j\}$，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[145]。

4.2.4 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 PW_i^{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 PW_i^{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 PW_i^{new}；登录失败，则服务器端未完成参数更新，新口令 PW_i^{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[81]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；只有在出现用户口令 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[81]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。

4.3 改进方案

本节在保持 Fang 等方案优势的基础上，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[72]；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 4.1 所示。

4.3.1 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 $ed=1 \bmod (p-1)(q-1)$。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 $h(b \oplus PW_i)$。

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

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

R4. $S \Rightarrow U_i$: 智能卡。

R5. U_i 将 b 写入智能卡。

4.3.2 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 $k = R \oplus h(b \oplus PW_i)$，$C_1 = k \oplus h(r \| T_u \| ID_i)$ 和 $C_2 = r^e \bmod n$。

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

4.3.3 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 $k' = C_1 \oplus h(r \| T_u \| ID_i)$，并从后台数据中读取与 ID_i 对应的 N_i。

V2. S 计算 $k'' = h(ID_i \oplus d \oplus N_i)$，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 $C_3 = h_{k'}(ID_i \| r \| T_s)$。

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'= $h_k(ID_i \| r \| T_s)$ 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 $SK = h(ID_i \| T_s \| T_u \| r)$，认证完成。

4.3.4 口令更新阶段

C1. 运行登录阶段 *L1~L3* 和认证阶段 *V1~V2*。

C2. S 计算 $m_3 = h_{k'}(r \| T_s \| ID_i)$。

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'= $h_k(r \| T_s \| ID_i)$ 并验证 $m_3' = m_3$ 是否成立。如果成立，则 U_i 输入新口令 PW_i^{new}，计算 $R_{new} = k \oplus h(b \oplus PW_i^{new})$，然后用 R_{new} 替换 R。

4.3.5 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 PW_i^{new} 到服务器重新注册，具体过程与注册阶段相同。

4.4 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[70]，下面分别从这两

个方面进行分析。

4.4.1 安全性分析

由于改进方案基于 Fang 等方案，继承了 Fang 等的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。

4.4.1.1 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[14, 15, 17]，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，服务器与用户的交互信息是经过安全信道传输的，攻击者非法监听、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 $k^* = R \oplus h(b \oplus PW_i^*)$，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 $\{ID_i, C_1, C_2, T_u\}$ 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_1 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。

4.4.1.2 已知密钥攻击

Fang 等方案易遭已知密钥攻击的根本原因在于，会话密钥 $SK = h(r \oplus b)$ 是登录消息 $C_1 = k \oplus h(r \oplus b)$ 的直接构成部分，SK 和 k 之间具体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 $k = C_1 \oplus h(r \oplus b) = C_1 \oplus SK$。

在改进方案中，双方协商的会话密钥 $SK = h(ID_i \| T_s \| T_u \| r)$ 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[72]，能够抵抗已知密钥攻击。

4.4.1.3 平行会话攻击

由于 C_1 保证了 $msg1=\{ID_i, C_1, C_2, T_u\}$ 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_s 或 T_u。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。

4.4.1.4 用户友好性

Fang 等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 4.2 总结了 Fang 等方案、Wang 等方案、Chung 等方案和本文所提出改进方案的安全性质。由表 4.2 可知，改进方案弥补了 Fang 等方案的安全缺陷，实现了文献[70]所列出的口令认证协议相关的 9 项主要安全目标。

表 4.2　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 等方案[11]	是	否	是	否	是	否	是	是	否
Chung 等方案[14]	是	是	是	是	是	是	是	是	是
Fang 等方案[35]	是	是	是	否	是	是	否	是	否
本文改进方案	是	是	是	是	是	是	是	是	是

4.4.2 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 $T_e \approx 600T_h$ [146]，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、用户 *ID* 和口令 *PW* 长度为 128 bit，服务器产生的大素数 *n* 和私钥 *d* 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 $2^{16}+1$ [110]。因此，不妨设公钥 *e* 的长度为 32 bit，则 $T_{se} \approx \frac{32}{1024} \cdot T_e \approx 20T_h$。基于开源标准密码库 MIRCAL[147]，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 4.3 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。四个相关方案的效率比较如表 4.4 所示。

表 4.3　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 4.4　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 等方案[8]	2	$5T_h$	$3T_h$	576	288	448	否	好
Chung 等方案[81]	3	$2T_e+6T_h$	$2T_e+6T_h$	1472	1184	3232+ *	是	好
Fang 等方案[15]	2	$5T_h$	$4T_h$	576	288	288	是	差
本文改进方案	2	$T_{se}+4T_h$	T_e+4T_h	1440	288	1216	是	好

注：*Chung 等方案[14]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

Chung 等方案采用随机数机制来提供消息的新鲜性，需要 3 轮交互，其它三种方案均采用时间戳机制，两轮交互即可。改进方案为了克服 Fang 等方案和 Wang 等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-4KSc 33MHz 嵌入式处理为例[148]，当模数 n 长为 1024bit 时，一次普通指数模幂乘运算耗时 320ms，而一次小指数模幂乘运算仅需要 2.28ms。文献[149, 150]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 4.3 和表 4.4 对比可知：改进方案和 Chung 等方案为了克服 Fang 等方案和 Wang 等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 等方案同等的安全性，但其各效率指标均优于 Chung 等方案。因此，改进方案保持了 Fang 等方案的高效性和 Chung 等方案的安全性，更适合于对安全需求较高的资源受限应用环境。

4.5 本章小结

本章首先分析了 Fang 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，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 等方案。综合来看，改进方案的实用性相较 Fang 等方案、Wang 等方案和 Chung 等方案大大提高，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 等方案和 Chung 等方案一样，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。

第 5 章 可证明安全的远程用户口令认证协议

第四章提出的基于 RSA 的远程用户认证协议是作者已发表论文[151]，该协议虽然能够抵抗已知的各种攻击，但仍存在两方面局限性：1、协议的安全性分析仍然是启发式的，缺乏严格的形式化证明；2 协议不支持用户口令的本地更新，即未实现理想属性 *U2*。为应对以上问题，本章基于离散对数难解性提出一种可证安全的远程用户口令认证协议，该协议在 2.2.1 节所给出的攻击者模型下能够实现 *S1~S12* 这 12 个安全目标，并且支持 *U1~U10* 这 10 个理想属性，进而解决了 Madhusudhan 和 Mittal[69]于 2012 年初在 Journal of Network and Computer Applications 上提出的公开难题。

与作者此前在文献[88]中提出的协议相比，本章所提出的协议主要贡献在于：协议能够在 2.2.1 节所给出的攻击者模型下实现 *S1~S12* 这 12 个安全目标，而文献[88]中的协议在 C-00 假设下（详见第 2 章中的表 2.1）无法抵抗离线口令猜测攻击。

设计可证明安全的远程用户口令认证协议是一件非常具有挑战性的事情[153]。少数几个协议（如[19, 25, 27, 30, 50]）给出了形式化证明，但随后都被发现存在这样或那样的安全缺陷。一个宣称可证明安全，而随后又被发现不安全（存在安全漏洞），产生这种矛盾现象有两方面原因：一方面由于证明过程的复杂性和证明方法的技巧性，形式化证明极易出错[154]；另一方面，一些形式化证明方法存在不完善性，导致证明安全的协议不一定安全，证明不安全的协议一定不安全，典型的如文献[25, 50]中采用的 BAN 逻辑无法保障协议的机密性。如节 1.2.3 所述，在众多的形式化方法中，随机预言机模型（ROM）下可证明安全性具有较高的可信性，并且绝大多数实用的可证安全的协议都给出了 ROM 下的证明[99]。因此，本章只关注 ROM 模型。

2009 年，Xu 等[19]给出了第一个 ROM 下可证明安全的协议。遗憾的是，2010 年 Song[10]发现一旦攻击者获取智能卡内秘密信息，Xu 等的协议便无法抵抗用户仿冒攻击，也就意味着无法实现基本目标——双向认证。Song 给出了改进方案，但也立即被发现无法抵抗离线口令猜测攻击[127]。一方面 Xu 等方案给出了形式化证明，另一方面又存在严重安全缺陷，产生这种矛盾现象的根本原因是什么？到底是由于形式化方法本身的缺陷，还是由于形式化证明过程的失误导致这一矛盾？对于这一问题，尚未有相关研究。

本章首先研究 Xu 等方案的形式化证明过程失误之处，然后提出一个可满足所有 *S1~S12* 安全目标和 *U1~U10* 理想属性的“理想协议”，并给出详细的 ROM 模型下形式化归约证明。效率分析表明，所提出的协议在实现安全性的同时保持了较高的效率。

5.1 Xu等方案形式化证明失误分析

本节首先回顾 Xu 等方案[19]和 Song[10]指出的仿冒攻击，然后指出 Xu 等方案形式化

证明过程中存在的失误之处。

5.1.1 Xu 等方案简要回顾

Xu 等方案[19]包含 3 个阶段，即注册阶段、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 5.1 所示。

表 5.1 符号定义

符号	含义	符号	含义
U_i	用户 i	p,q	两个大素数，且满足 $p=2q+1$
S	服务器	g	循环群 $\mathbb{Z}_q^*$ 中的生成元
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
$h(\cdot)$	安全散列函数	$A\Rightarrow B:M$	将消息 M 通过安全信道由 A 传送到 B

5.1.1.1 注册阶段

R1. 用户 U_i 选择用户名 ID_i 和口令 PW_i。

R2. $U_i \Rightarrow S:\{ID_i, PW_i\}$。

R3. 服务器 S 计算 $B = h(ID_i)^x + h(PW_i) \bmod p$，然后将 $\{ID_i, B, p, q, h(\cdot)\}$ 写入智能

R4. $S \Rightarrow U_i$:智能卡。

5.1.1.2 认证阶段

V1. 用户 U_i 插入智能卡，输入 ID_i 和 PW_i。

V2. 智能卡产生随机数 $w \in \mathbb{Z}_q^*$，读取当前时间戳 T，计算 $B' = (B - h(PW_i))^w \bmod p$，$W = h(ID_i)^w \bmod p$ 和 $C = h(T \| B' \| W \| ID_i)$。

V3. $U_i \rightarrow S:\{ID_i, C, W, T\}$。

V4. 服务器 S 在时间 T' 接收到来自 U_i 的认证请求后，检查 ID_i 和 T 的有效性，若 ID_i 或 T 无效，或者 $T' - T > \Delta T$，则拒绝登录请求。

V5. S 计算 $B'' = W^x \bmod p$，然后验证 $h(T \| B'' \| W \| ID_i)$ 和 C 是否相等。如果不相等，则 S 拒绝 U_i 的登录请求；否则，S 计算选择随机数 $m \in \mathbb{Z}_q^*$，读取当前时间戳 T''，计算 $M = h(ID_i)^m \bmod p$ 和 $C' = h(M \| B'' \| T'' \| ID_i)$

V6. $S \rightarrow U_i$:$\{ID_i, C', M, T''\}$。

V7. U_i 检查 T'' 的有效性，然后验证 $h(M \| B' \| T'' \| ID_i)$ 是否与 C_3 相等。如果相等，则 U_i 和 S 间共享会话密钥 $SK = h(ID_i \| M \| W \| M^w)$，认证完成。

5.1.1.3 口令更新阶段

C1. 执行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 $B^{new} = B - h(PW_i) + h(PW_i^{new})$，并用 B^{new} 替换 B。

5.1.2 针对 Xu 等方案的用户仿冒攻击

文献[19]中明确假设攻击者可以通过边信道攻击获取用户智能卡内秘密参数信息，并且宣称，即使攻击者获取这些信息，仍不会破坏协议安全性。实际上，正如 Song 所指出的一样，Xu 等方案[19]对用户仿冒攻击是脆弱的。恶意内部攻击者$U_{\mathcal{A}}$通过能耗分析或旁路信息泄露等边信道攻击技术[14, 15, 78]，可获得其自身拥有的智能卡内秘密参数 B 和 p,可仿冒任意用户（甚至不存在用户）登录服务器，具体攻击流程如下：

1）计算 $h(ID_{\mathcal{A}})^x = B - h(PW_{\mathcal{A}})$，因为$U_{\mathcal{A}}$知道自己的智能卡对应的口令 $PW_{\mathcal{A}}$；

2）选取随机数 $w \in \mathbb{Z}_q^*$，任意选择将要仿冒的用户U_r，计算 $B' = (h(ID_{\mathcal{A}})^x)^w \bmod p$，$W = h(ID_r)^w \bmod p$ 和 $C = h(T \| B' \| W \| ID_r)$。其中，若$U_{\mathcal{A}}$不知道受害用户$U_r$的身份标识 ID_r，则 ID_r 可任意选择，只要符合系统中对身份标识的定义规则即可（如符合一定的格式）。

3）$U_{\mathcal{A}} \rightarrow S:\{ID_r, C, W, T\}$。

4）收到来自服务器 S 的响应后，计算会话密钥 $SK = h(ID_r \| M \| W \| M^w)$。

在服务器收到来自上述步骤 3）中的登录请求后，由于 ID_r 和 T 的构造符合要求，并且 $B' = (h(ID_{\mathcal{A}})^x)^w \bmod p = (h(ID_{\mathcal{A}})^w)^x \bmod p = B'$，必然接收来自$U_r$的请求（实际上为$U_{\mathcal{A}}$），并向$U_{\mathcal{A}}$返回响应。

上述攻击危害性体现在两方面：1）$U_{\mathcal{A}}$不仅能够欺骗服务器成功登录，而且能够计算会话密钥 SK; 2）$U_{\mathcal{A}}$可以仿冒任意用户，甚至是系统中不存在用户，这严重违背了认证的完备性。

5.1.3 Xu 等协议形式化证明失误的研究

尽管 Xu 等协议的缺陷已被众多学者指出，但对形式化证明中的根本失误之处却少有研究，以致后续的不少改进方案（如文献[10, 24]）仍然存在几乎相同的缺陷。因此，下面作者首次对其中的证明失误之处进行分析。

Xu 等采用 ROM 模型对所提出的协议进行了形式化证明，核心思想是通过设计一系列仿真实验($\mathsf{Exp}_1, \mathsf{Exp}_2, \cdots, \mathsf{Exp}_5$)，将攻击者 $\mathcal{A}$ 对协议的成功攻击归约到对 CDH 问题的有效解决。在初始实验 Exp_1 中，预言机模拟的是 $\mathcal{A}$ 攻击实际协议，在后续的实验中逐步修改预言机的回答方式，使 $\mathcal{A}$ 在相邻两个实验中成功概率的差值是一个忽略的值，用 $\mathsf{Pr}[\mathsf{Exp}_i]$表示攻击者在实验 Exp_i 中(i=1,2,⋯,5)成功的概率。

在实验 Exp_1 中，预言机按协议的描述回答攻击者的查询，故 $\mathsf{Pr}[\mathsf{Exp}_1] = 0$；

在实验 Exp_2 中，若遇到某个$\{ID_i, C, W\}$或$\{ID_i, C', M\}$与先前会话中的对应项相同，则终止该会话，故 $\mathsf{Pr}[\mathsf{Exp}_2] \le \frac{(q_{exe}+q_{send})^2+{q_h}^2}{2p}$；

在实验 Exp_3 中，若攻击者成功猜测出 C 或C'，则终止该会话，故 $\mathsf{Pr}[\mathsf{Exp}_3] \le \frac{q_{send}}{p}$；

在实验 Exp_4 中，采用私有 Hash 函数 $h'(\cdot)$ 代替 $h(\cdot)$ 来计算会话密钥 SK，即令会话钥

$SK = h'(ID_r \| M \| W)$。显然 SK 与 $h(\cdot)$、K_U 或 K_S 无关。Exp_4 和 Exp_3 的唯一区别在于：攻击者 $\mathcal{A}$ 对 $ID_r \| M \| W \| K_U$ 或 $ID_r \| M \| W \| K_S$ 查询 $h(\cdot)$。Xu 等将这两个查询归纳为对 $ID_r \| M \| W \| \mathrm{CDH}(M,W)$ 的查询，进而将攻击者的成功查询优势归约为已知 $M = h(ID_r)^m, W = h(ID_r)^w$，求解 $\mathrm{CDH}(M,W) = h(ID_r)^{mw}$ 的优势。因此，$\Pr[\mathsf{Exp}_4] \le \Pr[\mathrm{AskH}_4]$；又由于 SK 由私有 Hash 函数 $h'(\cdot)$ 计算而得，攻击者成功的优势 $\Pr[\mathrm{Succ}_4] = \frac{1}{2}$。

在实验 Exp_5 中，利用 DH 问题的随机自归约特性，求得 $\Pr[\mathrm{AskH}_4] = \Pr[\mathsf{AskH}_5] \le \frac{q_{send}}{|\mathcal{D}|} + q_h \mathsf{Adv}^{\mathsf{CDH}}_{\mathbb{G}}(t + (q_{send} + q_{exe} + q_h)\cdot \mathcal{T}_{\mathbb{G}})$。证明完成。

Xu 等上述证明的失误之处在于，实验 Exp_4 中，将攻击者 $\mathcal{A}$ 对 $ID_r \| M \| W \| \mathrm{CDH}(M,W)$ 的查询优势归约为已知 $M = h(ID_r)^m$, $W = h(ID_r)^w$，求解 $\mathrm{CDH}(M,W) = h(ID_r)^{mw}$ 的优势。这一归约是 Xu 等证明过程的关键点，但实际上，这一归约是不成立的。Xu 等没有考虑到内部攻击者的情形。

内部攻击者 $\mathcal{A}$ 拥有自己的智能卡，一方面，$\mathcal{A}$ 可计算出 $h(ID_{\mathcal{A}})^x = B - h(PW_{\mathcal{A}})$，然后自行选择随机数 $w \in \mathbb{Z}_q^*$，任意选择将要仿冒的用户 U_r，计算 $B' = (h(ID_{\mathcal{A}})^x)^w \bmod p$，仿冒 U_r 向服务器 S 发送登录请求 $\{ID_r, C, W, T\}$；另一方面，$\mathcal{A}$ 在收到来自服务器 $M = h(ID_r)^m \bmod p$ 后，由于随机数 $w \in \mathbb{Z}_q^*$ 由其自己选择，故可轻易计算 $M^w = h(ID_r)^{mw} \bmod p$。

由上面分析不难看出，正确的归约应为：将攻击者 $\mathcal{A}$ 对 $ID_r \| M \| W \| \mathrm{CDH}(M,W)$ 的查询优势归约为，已知 $M = h(ID_r)^m$、随机数 w 和受害用户身份标识 ID_r，计算 $\mathrm{CDH}(M, W) = h(ID_r)^{mw}$ 的优势。显然，攻击者的成功优势 $\Pr[\mathrm{Succ}_4] = 1$。

5.2 ROM下可证明安全的新方案描述

本节在文献[88]中协议和对 Xu 等协议分析（更详尽讨论见[152]）的基础上，提出一种新的基于离散对数难解性的可证安全的远程用户口令认证协议，该协议在 2.2.1 节所给出的攻击者模型下能够实现 *S1~S12* 这 12 个安全目标，并且支持 *U1~U10* 这 10 个理想属性。新方案包含 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 5.1 所示。

5.2.1 注册阶段

协议定义于阶为 q 的素阶群 $\mathbb{G} = \langle g \rangle$ 上，其中 q 的长度为 $\mathcal{L} > 2^{512}$，g 为 $\mathbb{G}$ 的生成元。p 也是一个素数，$q \mid p-1$。Hash 函数 $\mathcal{H}_i(\cdot): \{0,1\}^* \to \{0,1\}^{l_i}$ (i=0, 1, 2, 3)，其中 $l_i \ge 2^{160}$。定义一个中等大小的整数 n（$2^8 \le n < 2^{16}$）来决定（ID, PW）池的容量，（$x, y=g^x$）分别表示服务器 S 的私钥和公钥。

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. $U_i \Rightarrow S$:$\{ID_i, \mathcal{H}_0(b \oplus PW_i)\}$。

R3. 服务器 S 检查 U_i 是否是已注册用户。如果是 U_i 的初次注册，则服务器 S 在后台数据库中为 U_i 产生一个新的条目（ID_i, T_{reg}），其中 T_{reg} 表示 U_i 注册时的时间戳；否则服务器 S 仅更新 T_{reg} 的值。接着，S 计算 $N_i = \mathcal{H}_0(b \oplus PW_i) \oplus \mathcal{H}_0(x \| ID_i \| T_{reg})$，$A_i = \mathcal{H}_0((\mathcal{H}_0(b \oplus PW_i) \oplus \mathcal{H}_0(ID_i)) \bmod n)$。

R4. S 将{ A_i，N_i，p，q，y，n，$\mathcal{H}_0(\cdot)$，$\mathcal{H}_1(\cdot)$，$\mathcal{H}_2(\cdot)$，$\mathcal{H}_3(\cdot)$ }写入智能卡。

R5. $S \Rightarrow U_i$: 智能卡。

R6. U_i 将 b 写入智能卡。

5.2.2 登陆阶段

L1. 用户 U_i 插入智能卡，输入 ID_i^* 和 PW_i^*。

L2. 智能卡计算 $A_i^* = \mathcal{H}_0((\mathcal{H}_0(b \oplus PW_i^*) \oplus \mathcal{H}_0(ID_i^*)) \bmod n)$，验证 A_i^* 是否与智能卡中存储的 A_i 相等。若不相等，则拒绝；否则意味着以 $\frac{n-1}{n}$（$\geq \frac{999}{1000}$，当 $n = 2^{10}$）的概率有 $ID_i^* = ID_i$，$PW_i^* = PW_i$。

L3. 智能卡产生随机数 u，计算 $C_1 = g^u \bmod p, Y_1 = y^u \bmod p$，$k = N_i \oplus \mathcal{H}_0(b \| PW_i)$，$CID_i = ID_i \oplus \mathcal{H}_0(C_1 \| Y_1)$，$M_i = \mathcal{H}_0(Y_1 \| k \| CID_i)$。

L4. $U_i \rightarrow S$:{ C_1, CID_i, M_i }。

5.2.3 认证阶段

V2. 服务器 S 计算 $Y_1 = C_1^x \bmod p$，$ID_i = CID_i \oplus \mathcal{H}_0(C_1 \| Y_1)$，并检查 ID_i 的有效性，若 ID_i 无效则拒绝登录请求；否则，S 根据 ID_i，从后台数据中读取与 ID_i 对应的 N_i。

V3. S 计算 $k = \mathcal{H}_0(x \| ID_i \| T_{reg})$，$M_i^* = \mathcal{H}_0(Y_1 \| k \| CID_i)$，然后验证 $M_i^* = M_i$ 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 v，计算 $C_2 = g^v \bmod p$，$C_3 = \mathcal{H}_1(ID_i \| ID_S \| Y_1 \| C_2 \| k \| K_S)$。

V4. $S \rightarrow U_i$:{ C_2, C_3 }。

V5. 智能卡计算 $K_U = (C_2)^u \bmod p$，$C_3^* = \mathcal{H}_1(ID_i \| ID_S \| Y_1 \| C_2 \| k \| K_U)$，并验证 $C_3^* = C_3$ 是否成立。如果成立，则 U_i 继续计算 $C_4 = \mathcal{H}_2(ID_i \| ID_S \| Y_1 \| C_2 \| k \| K_U)$。

V6. $U_i \rightarrow S$:{ C_4}。

V7. 服务器计算 $C_4^* = \mathcal{H}_2(ID_i \| ID_S \| Y_1 \| C_2 \| k \| K_U)$，并验证 $C_4^* = C_4$ 是否成立。如果成立，则 U_i 和 S 间共享会话密钥 $SK = \mathcal{H}_3(ID_i \| ID_S \| Y_1 \| C_2 \| k \| K_U)$，认证完成。

5.2.4 口令更新阶段

C1. 用户 U_i 插入智能卡，输入 ID_i^* 和 PW_i^*。

C2. 卡计算 $A_i^* = \mathcal{H}_0((\mathcal{H}_0(b \oplus PW_i^*) \oplus \mathcal{H}_0(ID_i^*)) \bmod n)$，验证 A_i^* 是否与智能卡中存储的 A_i 相等。若不相等，则拒绝；否则意味着以 $\frac{n-1}{n}$（$\geq \frac{999}{1000}$，当 $n = 2^{10}$）的概率有 $ID_i^* = ID_i$，$PW_i^* = PW_i$。

C3. 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 $N_i^{new}=N_i\oplus h(b\oplus PW_i)\oplus h(b\oplus PW_i^{new})$ 和 $A_i^{new}=\mathcal{H}_0((\mathcal{H}_0(b\oplus PW_i^{new})\oplus\mathcal{H}_0(ID_i))\bmod n)$，并用 N_i^{new} 替换 N_i，A_i^{new} 替换 A_i。

设计思想：为同时实现理想属性 U_2 和安全目标 S_4，在口令更新过程中对旧口令真实性的验证是必要的。因此，除了 N_i，还需要额外的与口令相关的安全参数存储在智能卡中，这就会带来新的安全威胁，如离线口令猜测攻击和仿冒攻击等[10, 31]。比如，若令 $A_i=\mathcal{H}_0(PW_i\oplus\mathcal{H}_0(ID_i))$ 存储在智能卡中。在用户每次更新口令过程中，用户需要输入身份标识 ID_i^* 和旧口令 PW_i^*，然后验证 $A_i^*=\mathcal{H}_0(PW_i^*\oplus\mathcal{H}_0(ID_i^*))$ 是否与存储的 A_i 相等。不难发现，攻击者分析出智能卡内的 A_i 和 b 后，则可离线搜索出正确的（*ID, PW*）对。然而，如果令 $A_i^*=\mathcal{H}_0((\mathcal{H}_0(b\oplus PW_i^*)\oplus\mathcal{H}_0(ID_i^*))\bmod n)$，则

1）$\mathcal{A}$ 即使分析出智能卡内的 A_i 和 b，且已知受害用户的身份标识 ID_i，$\mathcal{A}$ 只能排除掉 $(1-\frac{1}{n})|\mathcal{D}|$ 个口令，还剩下 $\frac{|\mathcal{D}|}{n}$ 个潜在口令。而对于这剩余的 $\frac{|\mathcal{D}|}{n}$ 个潜在口令，$\mathcal{A}$ 只能通过在线口令猜测攻击来逐一排除。

2）在口令更新过程中，对于用户输入的身份标识 ID_i 和旧口令 PW_i^*，如果计算出的 A_i^* 与存储的 A_i 相等，则意味着以 $\frac{n-1}{n}$（$\geq\frac{999}{1000}$，当 $n=2^{10}$）的概率有 $ID_i^*=ID_i$，$PW_i^*=PW_i$，也就表明用户的错误输入通过验证的可能小于 $\frac{1}{1000}$。

由上可知，通过 A_i^* 这种新型的验证因子，新方案能够较好的平衡 *U2* 和 *S4*。根据节 3.3.3，这种可用性和安全性间的平衡是不可避免的。我们称这种新型的验证因子为“模糊验证因子”。文中仅以模 *n* 运算为例来说明“模糊验证因子”，实际上也可定义特殊的 Hash 函数来实现，如令 $A_i^*=\bar{\mathcal{H}}(\mathcal{H}_0(PW_i^*)\oplus\mathcal{H}_0(ID_i^*))$，其中 $\bar{\mathcal{H}}:\{0,1\}^*\rightarrow\{0,1\}^8$。

为实现理想属性 U_4，采用 Diffie-Hellman 密钥交换技术来实现完备前向安全性；为实现理想属性 U_6，在服务器端为每个用户保存一个条目(ID_i, T_{reg})用户撤销智能卡时只需要更新 T_{reg}，而不用更换身份标识 ID_i；另一方面，这样也没有违背 U_1；为实现理想属性 U_8，用户的身份标识 ID_i 被动态变化的随机身份标识 CID_i 中；为实现理想属性 U_{10}，采用随机数机制而非时戳机制来提供消息的新鲜性。

5.3 ROM下形式化安全证明

本节我们首先为基于智能卡的远程用户口令认证协议定义一个形式化安全模型，然后证明上节中提出的新方案在 ROM 模型和 CDHP 困难性假设下是安全的。特别地，新方案能够实现前向安全性、已知密钥攻击和密钥泄露仿冒攻击。

5. 3. 1 形式化安全模型

本节简要回顾 Bellare 等在文献[101]中定义的基于口令密钥协商协议的形式化安全模型，通过查询预言机来模拟攻击者的能力。但是，本文不直接采用原始模型，而是采

用 Bresson 等[155]优化后的改进模型，并进行一些相应的调整，使它能够反应基于智能卡的远程用户口令认证协议的特殊安全需求。

参与者。协议$\mathcal{P}$中的参与者为服务器S和用户U。每个参与者被模拟成一组预言机，每个预言机（也称实例）可独立，甚至并发执行协议$\mathcal{P}$。将服务器和用户的实例分别设为S^j和U^i，可统一表示为I^k，$i,j,k\in\mathbb{Z}$。

根据 5.2 节中描述，服务器拥有一个公私钥对(g^x,x)，用户拥有口令，其中口令从服从均匀分布的空间$\mathcal{D}$中取样。[2] 此外，当用户U向服务器S注册时，S向U颁发一个内置有安全参数$\{N_i,A_i\}$的智能卡。

查询。攻击者$\mathcal{A}$与协议$\mathcal{P}$中的参与者I间的交互通过预言机查询来实现，以此来模拟现实中攻击者的能力。赋予$\mathcal{A}$的查询类型主要有：

—Execute(U^i,S^j): 这个查询模拟攻击者的被动攻击（侦听）的能力，输出为协议正常运行情况下的交互信息；

—Send(I,m): 这个查询模拟攻击者的主动攻击，$\mathcal{A}$向实例I发送消息m，I根据协议$\mathcal{P}$向$\mathcal{A}$返回处理m所产生的相应的信息。其中，Send(I,Start)发起一个会话；

—Test(I): 这个查询不是模拟攻击者的攻击能力，而是用来定义会话密钥的语义安全性，只运行一次，且只对“新鲜”的会话有效。如果实例I尚无会话密钥，返回$\perp$。否则，随机选择一个比特c，如果c=1，向$\mathcal{A}$返回会话密钥sk；如果c=0，向$\mathcal{A}$返回一个等长的随机串；

—Reveal(I): 这个查询模拟会话密钥的滥用（对应表 1 中的 C-3）。如果实例I确实拥有会话密钥，且I和其伙伴没有被执行 Test 查询，则返回sk；否则，返回$\perp$。

—Corrupt(I, a): 这个查询模拟攻击者的腐化能力（对应表 1 中的 C-2 和 C-4）。注意$\mathcal{A}$确实可以窃取/获得用户的两个认证因子中的一个（不能两个同时获取）：

- 如果$a=1$，则输出U^i的口令PW_i；
- 如果$a=2$，则输出U^i的智能卡中参数$\{N_i,\ A_i,\ b\}$；
- 如果$a=3$，则输出服务器S的私钥x。

不难看出，上述几个查询确实能够模拟如表 2.1 中所示的攻击者的攻击能力。

伙伴关系。我们基于会话标识符 sid 来定义伙伴关系。让U^i和S^j为两个实例，如果下述条件满足，则为一对伙伴：①这两个实例均已接受；②这两个实例拥有相同的会话标识符sid；③实例U^i的伙伴标识符pid=S^j,实例S^j的伙伴标识符pid=U^i。一般地，我们令sid为U^i或S^j所有按顺序接受或发送的消息的连接。

新鲜性。新鲜性的概念用来描述这样一个直观事实：会话密钥不能轻易被攻击者所获知。如果一个实例I满足下述条件，则认为I是新鲜的：① I已接受且计算出会话密

[2] 这里假设$\mathcal{D}$服从均匀分布仅为了便于表示的需要，其实不管$\mathcal{D}$服从何种分布，只要将概率$\frac{\lambda}{|\mathcal{D}|}$替换为前$\lambda$个可能性最大的口令的概率之和即可。

钥；② I 和它的伙伴这两个实例都未被执行 Reveal 查询；③自协议运行开始，对相应的用户至多执行一种 Corrupt 查询，且未对服务器执行 Corrupt 查询。

完备性。如果U^i和S^j这两个实例互为伙伴关系且均已接受，则它们拥有相同的会话密钥，即 $sk_U^i = sk_S^j$。

认证。认证协议的一个基本目标就是防止攻击者仿冒用户U或服务器S。用$\mathrm{Adv}_{\mathcal{P}}^{\mathrm{Auth}}$表示攻击者$\mathcal{A}$成功仿冒用户$U$（或服务器$S$）的优势，也就是说，服务器$S$（或用户$U$）计算出了会话密钥，但这个会话并不是和意定中的用户U（或服务器S）共享。

语义安全性。带会话密钥协商的认证协议另一个关注目标就是语义安全性。在协议$\mathcal{P}$的一次运行中，$\mathcal{A}$可以执行多项式次 Execute、Send、Reveal、Corrupt 查询和对新鲜实例的一次 Test 查询。在游戏结束时，$\mathcal{A}$输出对 Test 查询中涉及的比特c的猜测c'。如果$c'=c$，我们说$\mathcal{A}$取得游戏的胜利，并将此事件定义为Succ。相应地，$\mathcal{A}$破坏协议$\mathcal{P}$的语义安全性的优势为

$$\mathrm{Adv}_{\mathcal{P}}^{\mathrm{ake}}(\mathcal{A}) = 2\Pr[\mathrm{Succ}] - 1 = 2\Pr[c' = c] - 1$$

其中，概率空间定义在攻击者所有的掷币和所有的实例之上。如果在安全参数ℓ下，任一多项式攻击者成功的优势都是可忽略的，则说协议$\mathcal{P}$是语义安全的。

5.3.2 安全性证明

本小节给出新方案在 ROM 模型下的安全证明，主要基于节 2.4 中的 CDH 假设。为了便于我们对协议的模拟，对原方案进行稍微的调整，即 5.2.1 节 R3 中的“如果是 U_i 的初次注册，则服务器 S 在后台数据库中为 U_i 产生一个新的条目（ID_i, T_{reg}）……”修改为“如果是 U_i 的初次注册，则服务器 S 在后台数据库中为 U_i 产生一个新的条目（ID_i, T_{reg}，$P_i(=h(b\oplus PW_i))$）……”。需要指出的是，这样的调整只是为了证明的需要，对协议的安全性不会造成实质影响。

定理 5.1 （语义安全）设$\mathbb{G}=<g>$为表示群，口令空间$\mathcal{D}$均匀分布，$\mathcal{P}$为 5.2 节中的协议，攻击者$\mathcal{A}$在多项式时间t内最多进行q_{send}次 Send 查询、q_{exe}次 Execute 查询、q_h次随机预言机查询，则攻破$\mathcal{P}$的语义安全的优势为

$$\begin{aligned}\mathrm{Adv}_{\mathcal{P}}^{\mathrm{ake}}(\mathcal{A}) &= 2\Pr[\mathrm{Succ}_8] - 1 + 2(\Pr[\mathrm{Succ}_8] - \Pr[\mathrm{Succ}_0]) \\ &\le \frac{2q_{send}}{|\mathcal{D}|} + 12q_h\mathrm{Adv}_{\mathcal{P},\mathbb{G}}^{\mathrm{cdh}}(t + (q_{send} + q_{exe} + 1)\cdot\mathcal{T}_e) \\ &\quad + \frac{q_h^2 + 6q_{send}}{2^l} + \frac{(q_{send}+q_{exe})^2}{p}\end{aligned}$$

其中$\mathcal{T}_e$表示群$\mathbb{G}$中模幂（或 ECC 的点乘）运算的时间，$l=\max\{l_i\}$，$i=1,2,3,4$。

证明：令$\mathcal{A}$为试图破坏协议语义安全性的攻击者。证明的主要思想是，利用$\mathcal{A}$来构建破坏密码原语的攻击者，如果$\mathcal{A}$成功破坏协议的语义安全性，则至少一个密码原语被攻破。我们定义一系列的仿真游戏（Game_0, Game_1, Game_2, ……, Game_8），在所有的游戏中，预言机按照协议的描述处理查询。其中，Game_0对应真实的协议攻击，在后续

的游戏中逐步修改预言机的回答方式，以致于在 Game_8 中 $\mathcal{A}$ 没有任何优势。在每个游戏 Game_n（$n=0,\ 1,\ 2,\cdots\cdots,8$）中，我们定义下述事件：

Succ_n：$\mathcal{A}$ 成功猜测 Test 查询中的测试比特 c；

$\mathsf{AskPara}_n$：$\mathcal{A}$ 通过对 $x\|ID_i\|T_{reg}$ 或 $b\|PW_i$ 查询 $\mathcal{H}_0$，从而成功计算出核心安全参数 k；

$\mathsf{AskAuth}_n$：$\mathcal{A}$ 成功计算出核心安全参数 k，并且对 $ID_i\|ID_S\|Y_1\|C_2\|k\|K$ 查询 $\mathcal{H}_1$ 或 $\mathcal{H}_2$，其中 $K=K_U$ 或 K_S；

AskH_n：$\mathcal{A}$ 对 $ID_i\|ID_S\|Y_1\|C_2\|k\|K$ 查询 $\mathcal{H}_i$（$i=1,2,3$），其中 $K=K_U$ 或 K_S；

Game_0：该游戏对应 ROM 下的真实攻击，根据定义有

$$\mathsf{Adv}_{\mathcal{P}}^{\mathsf{ake}}(\mathcal{A})=2\Pr[\mathsf{Succ}_0]-1 \tag{5-1}$$

Game_1：本游戏中，我们正常模拟所有的 Hash 查询 $\mathcal{H}_i$ 以及将在 Game_7 中出现的 $\mathcal{H}_i'$（$i=0,1,2,3$），但维护一个 Hash 查询结果列表 $\Lambda_{\mathcal{H}}$（和 $\Lambda_{\mathcal{A}}$，该列表记录由 $\mathcal{A}$ 所直接实施的 Hash 查询）。对于其它查询，保持与真实协议攻击不变。不难看出，

$$\Pr[\mathsf{Succ}_1]-\Pr[\mathsf{Succ}_0]=0 \tag{5-2}$$

Game_2：为便于分析，本游戏中我们去掉一些不太可能发生的碰撞：

—通信消息（$(C_1, CID_i,\ M_i)$，(C_2, C_3)，C_4）的碰撞，需要指出的是，这些产生这些通信消息的参与方中至少有一个是诚实实体，故 C_1 和 C_2 中至少有一个随机分布的；

—Hash 输出的碰撞；

根据生日悖论原理，可得

$$\Pr[\mathsf{Succ}_2]-\Pr[\mathsf{Succ}_1]\le\frac{(q_{send}+q_{exe})^2}{2p}+\frac{q_h^2}{2^{l+1}} \tag{5-3}$$

Game_3：本游戏中，如果 $\mathcal{A}$ 幸运地猜测到认证元 M_i、C_3 或 C_4，则终止协议的执行。由于 Hash 输出碰撞的可能性在 Game_2 中已排除，因此除非合法认证元（由 $\mathcal{A}$ 产生）被拒绝，Game_3 和 Game_2 是不可区分的，

$$\Pr[\mathsf{Succ}_3]-\Pr[\mathsf{Succ}_2]\le\frac{q_{send}}{2^l} \tag{5-4}$$

Game_4：本游戏中，如果 $\mathcal{A}$ 幸运地猜测到核心安全参数 k，则终止协议的执行。由于合法认证元 M_i、C_3 或 C_4 碰撞的可能性在 Game_2 中已排除，因此除非由 $\mathcal{A}$ 自行产生的合法认证元被拒绝，Game_4 和 Game_3 是不可区分的，

$$\Pr[\mathsf{Succ}_4]-\Pr[\mathsf{Succ}_3]\le\frac{q_{send}}{2^l} \tag{5-5}$$

Game_5：本游戏中，如果 $\mathcal{A}$ 正确地计算出核心安全参数 k，且成功地仿冒用户或服务器，则终止协议的执行。在事件 $\mathsf{AskPara}_5$ 不发生的情况下，Game_5 和 Game_4 是不可区分的，可得

$$\Pr[\mathsf{Succ}_5]-\Pr[\mathsf{Succ}_4]\le\Pr[\mathsf{AskPara}_5] \tag{5-6}$$

Game_6：本游戏中，如果 $\mathcal{A}$ 正确地计算出认证元 C_3 或 C_4，则终止协议的执行。在

事件 $\mathsf{AskAuth}_6$ 不发生的情况下，Game_6 和 Game_5 是不可区分的，可得

$$\begin{aligned}&\Pr[\mathsf{Succ}_6]-\Pr[\mathsf{Succ}_5]\le\Pr[\mathsf{AskAuth}_6]\\&\Pr[\mathsf{AskPara}_6]-\Pr[\mathsf{AskPara}_5]\le\Pr[\mathsf{AskAuth}_6]\end{aligned}\tag{5-7}$$

Game_7：本游戏中，我们用私有的 Hash 函数 $\mathcal{H}_i'$ 来代替 $\mathcal{H}_i$（$i=1,2,3$），即有

$$\begin{aligned}C_3&=\mathcal{H}_1'(ID_i\|ID_S\|Y_1\|C_1\|k)\\C_4&=\mathcal{H}_2'(ID_i\|ID_S\|Y_1\|C_2)\\SK&=\mathcal{H}_3'(ID_i\|ID_S\|Y_1\|C_2)\end{aligned}$$

这样，C_3 、C_4 和 SK 完全独立于核心安全参数 k、K_U 和 K_S。在事件 AskH_7 不发生的情况下，Game_7 和 Game_6 是不可区分的，可得

$$\begin{aligned}&\Pr[\mathsf{Succ}_7]-\Pr[\mathsf{Succ}_6]\le\Pr[\mathsf{AskH}_7]\\&\Pr[\mathsf{AskPara}_7]-\Pr[\mathsf{AskPara}_6]\le\Pr[\mathsf{AskH}_7]\\&\Pr[\mathsf{AskAuth}_7]-\Pr[\mathsf{AskAuth}_6]\le\Pr[\mathsf{AskH}_7]\end{aligned}\tag{5-8}$$

引理 5.1 在游戏 Game_7 中，事件 Succ_7 和 $\mathsf{AskPara}_7$ 发生的概率约束如下：

$$\begin{aligned}&\Pr[\mathsf{Succ}_7]=\tfrac{1}{2}\\&\Pr[\mathsf{AskPara}_7]\le\tfrac{q_{send}}{|\mathcal{D}|}+\tfrac{q_{send}}{2^l}\end{aligned}\tag{5-9}$$

证明：在游戏 Game_7 中，会话密钥由私有的 Hash 函数 $\mathcal{H}_3'$ 计算而来，完全独立于 $\mathcal{A}$ 的攻击能力，因此 $\Pr[\mathsf{Succ}_6]=\frac{1}{2}$。

让我们用 $R(U)$ 表示用户实例接收到的通信消息（C_2, C_3）的集合，用 $R(S)$ 表示服务器实例接收到的通信消息（C_4）的集合。由于我们在 Game_4 中已经去除了 $\mathcal{A}$ 幸运地猜测到核心安全参数 k 的情形，$\mathcal{A}$ 可以通过 $\mathsf{Corrupt}(I=U^i,\ 1)$和 $\mathsf{Corrupt}(I=U^i,\ 2)$这两个查询的帮助来计算 k，这两个不同情况的概率分别记为 $\Pr[\mathsf{AskPara}_7\mathsf{WithCorr}_1]$和 $\Pr[\mathsf{AskPara}_7\mathsf{WithCorr}_2]$。我们在 Game_2 中已去除了通信消息碰撞的可能性，从信息论的角度，则有

$$\begin{aligned}&\Pr[\mathsf{AskPara}_7\mathsf{WithCorr}_1]\le\tfrac{q_{send}}{2^l}\\&\Pr[\mathsf{AskPara}_7\mathsf{WithCorr}_2]=\Pr[\exists C_3\in R(U),\ (1,ID_i\|ID_S\|Y_1\|C_2\|k\|*,C_3)\in\Lambda_{\mathcal{A}}]\\&\qquad+\exists C_4\in R(S),\ (0,\ *,\ P_i)\in\Lambda_{\mathcal{A}}]\\&\qquad\le\tfrac{\#R(U)+\#R(S)}{|\mathcal{D}|}=\tfrac{q_{send}}{|\mathcal{D}|}\end{aligned}\tag{5-10}$$

Game_8：本游戏中，利用 Diffi-Hellman 问题的自归约特性：任给一个随机 CDH 实例 $(A,\ B)$，取随机数 $u,v\in_R\mathbb{Z}_q^*$，计算 $C_1=A^u,C_2=B^v$，则可得 $\mathrm{CDH}(C_1,C_2)=\mathrm{CDH}(A^u,B^v)=\mathrm{CDH}(A,B)^{uv}$。需要注意的是，$\mathsf{AskH}_8$ 表示 $\mathcal{A}$ 对 $ID_i\|ID_S\|Y_1\|C_2\|k\|\mathrm{CDH}(C_1,C_2)$ 查询 $\mathcal{H}_i$（$i=1,2,3$），根据定义有

$$\Pr[\mathsf{AskH}_8]=\Pr[\mathsf{AskH}_7]\tag{5-11}$$

通过随机在 $\Lambda_{\mathcal{A}}$ 列表中选取，可有 $\frac{1}{q_h}$ 的概率得到 $\mathrm{CDH}(C_1,C_2)$，进而可计算出 $\mathrm{CDH}(A,B)=\mathrm{CDH}(C_1,C_2)^{\frac{1}{uv}}$，得

$$\Pr[\mathsf{AskH}_8]\le q_h\mathsf{Adv}_{\mathcal{P},\mathbb{G}}^{\mathsf{cdh}}(t')\tag{5-12}$$

其中，$t' \le t + (q_{send} + q_{exe} + 1) \cdot \mathcal{T}_e$，$\mathcal{T}_e$表示群$\mathbb{G}$中模幂（或 ECC 的点乘）运算的时间。

综上所述，通过关系(5-1) ～(5-5)可得

$$\Pr[\mathsf{Succ}_4] - \Pr[\mathsf{Succ}_0] \le \frac{2q_{send}}{2^l} + \frac{(q_{send}+q_{exe})^2}{2p} + \frac{q_h^2}{2^{l+1}}$$

通过关系(5-6) ～(5-9)可得

$$\Pr[\mathsf{Succ}_7] - \Pr[\mathsf{Succ}_4] \le \Pr[\mathsf{AskPara}_5] + \Pr[\mathsf{AskAuth}_6] + \Pr[\mathsf{AskH}_7]$$

根据定义有　　$\Pr[\mathsf{AskAuth}_6] \le \Pr[\mathsf{AskH}_6]$

综合得

$$\begin{aligned}\mathsf{Adv}_{\mathcal{P}}^{\mathsf{ake}}(\mathcal{A}) &= 2\Pr[\mathsf{Succ}_8] - 1 + 2(\Pr[\mathsf{Succ}_8] - \Pr[\mathsf{Succ}_0]) \\ &= \frac{2q_{send}}{|\mathcal{D}|} + 12q_h\mathsf{Adv}_{\mathcal{P},\mathbb{G}}^{\mathsf{cdh}}(t + (q_{send} + q_{exe} + 1)\cdot\mathcal{T}_e) \\ &\quad + \frac{q_h^2 + 6q_{send}}{2^l} + \frac{(q_{send}+q_{exe})^2}{p}\end{aligned}$$

定理 5.2 （认证性）设$\mathbb{G} = < g >$为表示群，口令空间$\mathcal{D}$均匀分布，$\mathcal{P}$为 5.2 节中的协议，攻击者$\mathcal{A}$在多项式时间t内最多进行q_{send}次 Send 查询、q_{exe}次 Execute 查询、q_h次随机预言机查询，则攻破$\mathcal{P}$的双向认证性的优势为

$$\begin{aligned}\mathsf{Adv}_{\mathcal{P},\mathbb{G}}^{\mathsf{auth}}(\mathcal{A}) &\le \frac{q_{send}}{|\mathcal{D}|} + 5q_h\mathsf{Adv}_{\mathcal{P},\mathbb{G}}^{\mathsf{cdh}}(t + (q_{send} + q_{exe} + 1)\cdot\mathcal{T}_e) \\ &\quad + \frac{q_h^2 + 6q_{send}}{2^{l+1}} + \frac{(q_{send}+q_{exe})^2}{2p}\end{aligned}$$

其中$\mathcal{T}_e$表示群$\mathbb{G}$中模幂（或 ECC 的点乘）运算的时间，$l = \max\{l_i\}$，$i = 1,2,3,4$。

证明：令$\mathcal{A}$为试图破坏协议双向认证性的攻击者。证明的主要思想和过程与定义 1 类似。我们再定义一个事件：

Auth_n：$\mathcal{A}$在游戏Game_n（$n = 0, 1, 2, \cdots\cdots, 8$）中功计算出认证元$C_3$或$C_4$；

根据定义，有$\mathsf{Adv}_{\mathcal{P},\mathbb{G}}^{\mathsf{auth}}(\mathcal{A}) = \Pr[\mathsf{Auth}_0]$

然后，我们采用与证明定理 1 完全相同的一系列的仿真游戏（Game_0, Game_1, Game_2, ……, Game_8）即可得到上述结论，这里不再赘述。

5.4 性能分析

本节中，通过与文献[19, 81, 87, 88, 141]中的方案进行对比来评估节 5.2 中新方案的优劣。之所以选择这些方案作为比较对象，是因为它们是少数的几个支持完备前向安全性的协议。根据表 1.1 和 1.2 中的标准对这些方案进行评估，结果如表 5.2 和 5.3 所示。

表 5.2 相关远程用户口令认证方案的性能比较

	新方案	Wang 等方案[88]	Xie 方案[87]	Horng 等方案[141]	Chung 等方案[81]	Xu 等方案[19]
计算量	$6T_E + 14T_H$	$6T_E + 12T_H$	$8T_E + 7T_H$	$7T_E + 4T_S + 8T_H$	$4T_E + 2T_I + 12T_H$	$6T_E + 8T_H$
通信量	2560 bits	2560 bits	3328 bits	2432 bits	2560 bits	2816 bits
存储量	3488 bits	3456 bits	1280 bits	3328 bits	3200 bits	3200 bits

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、对称加/解密运算T_S和 Hash 运算T_H，其中$T_E \approx T_I > T_S >> T_H$ [146]，其余的

计算量如“⊕”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 函数散列值为 128 bit，系统生成的随机数、用户 *ID* 和口令 *PW* 长度为 128 bit，服务器产生的大素数 p 和 q 长度均为 1024 bit，系统安全参数 n 的长度为 32 bit。

在新方案中，智能卡内存储$\{b, N_i, A_i, y, n, g\}$，故存储开销为 3456(=32+3*128 +3*1024) bits; 通信量为登录和认证过程中传送的消息量 2332(=3*128 +2*1024）bits；登录和认证过程中，服务器端和客户端的计算量总和为 $6T_E$+$14T_H$。由表 5.2 可知，新方案的效率优于 Horng 等方案[141]和 Xie 方案[87]，与 Xu 等方案[19]、Wang 等方案[88]和 Chung 等方案[81]大致相同。

表 5.3 总结了新方案和几个参照方案的评价指标满足情况。新方案可实现所有 *S1~S12* 安全目标和 *U1~U10* 理想属性，达到文献[69]中所给出的“理想协议”的要求。新方案和 Chung 等方案具有相同的安全性，但后者无法实现 *U2*、*U5* 和 *U8*；其余几个方案都存在这样或那样的安全缺陷，在理想属性的支持方面也不尽如人意。

表 5.3 相关远程用户口令认证方案的评价指标满足情况

方案	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10
新方案	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
Wang 等[88]	是	是	是	否	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是	是	否	是
Xie[148]	是	是	是	否	是	是	是	是	是	是	是	否	是	是	是	是	否	否	是	是	否	是
Horng 等[141]	是	是	是	是	是	是	是	是	是	是	是	否	是	否	是	是	否	是	是	是	否	是
Chung 等[81]	是	是	是	是	是	是	是	是	是	是	是	是	是	否	是	是	否	是	是	否	是	是
Xu 等方案[19]	是	是	否	否	是	是	是	否	是	是	是	否	是	否	是	是	否	是	是	否	否	否

5.5 本章小结

本章首先通过分析 Xu 等方案的形式化证明过程中存在的失误，揭示了可证明安全中的难题和挑战。然后通过采用“模糊验证因子”技术，基于 CDH 困难性假设，给出了一个“理想协议”，并在 ROM 模型下给出了紧归约的安全性证明。最后，通过与同类方案进行对比，显示了新方案的先进性。尽作者所知，新方案是第一个能够实现所有 *S1~S12* 安全目标和 *U1~U10* 理想属性，解决了文献[69]中提出的公开问题。

结　论

基于智能卡的口令认证由于安全性高、便携性好、简单易用，而成为应用最为广泛的双因子认证技术。传统的此类协议一般假设智能卡内秘密信息是安全的，但随着近期边信道攻击技术的不断进展，普通智能卡内秘密信息可通过能耗分析、计时攻击和逆向工程等手段被攻击者获取。因此，研究在非抗窜扰智能卡假设下实现安全高效的远程用户口令认证协议具有重要的理论和现实意义。

本文围绕基于非抗窜扰智能卡的远程用户口令认证协议的评价指标和协议的设计、分析展开研究。通过对已有最新典型协议的分析，指出其安全漏洞和功能缺陷，梳理协议评价指标间内在关系，提出协议设计原则。基于大因子分解困难问题，设计了一个安全高效的适于移动用户的远程用户口令认证协议，并完成了启发式分析；基于离散对数难解性问题，设计了一个能够满足所有安全目标和实现所有相关理想属性的协议，并且在随机预言机模型下完成了形式化安全证明。主要取得了以下四方面成果：

1）分析了近期三个典型的方案，即 Xie 等方案、Hao 等方案和 Hsieh 等方案。其中 Xie 等方案基于 RSA 公钥技术，指出其无法抵抗基本的重放攻击；Hao 等方案和 Hsieh 等方案基于仅基于对称密码操作（Hash 函数），指出它们均无法实现所宣称的抵抗离线口令猜测攻击。这三个方案都给出了启发式的安全性分析，并声称是安全的，我们的启发式攻击结果表明，启发式的安全性分析严重依赖分析者的协议攻击经验，极易出错，借助于可证明安全技术来确保协议的安全性是更好的选择。

2）针对基于智能卡的远程用户口令认证协议的评价指标相关研究严重不足的问题，依据作者对近年来 100 余个此类协议的分析经验，梳理了各指标间的相互关系，提出了三条协议设计原则。首次证明了在非抗窜扰智能卡假设下，采用公钥技术是实现协议可抗离线口令猜测攻击的必要条件；首次证明了在服务器端无敏感验证表项情形下，服务器（至少）进行两次模幂运算（或点乘运算）是实现前向安全性的必要条件。

3）利用 RSA 公钥技术的加密和解密运算的非对称特性，设计了一个适于受限资源环境的远程用户口令认证协议。与已有相关协议相比，新协议在保持安全性的同时，在客户端性能方面具有显著优势。

4）基于 CDH 困难性假设，设计了一个 ROM 下可证安全的“理想协议”。可证明安全理论是保障协议安全性的有效手段，ROM 下可证安全的协议往往能够较好地对安全性和效率进行平衡，故更适于资源受限的智能卡环境。与已有相关协议对比结果表明，新协议在保持较高效率的同时，实现了所有相关安全目标和理想属性，解决了 Madhusudhan 和 Mittal 于 2012 年初提出的公开问题。

由于学习时间和技术水平等方面的因素，本论文只是致力解决了基于智能卡的口令认证研究领域中的几个问题。单就协议评价指标这一研究内容来说，我们也只是根据密

码分析经验给出了各评价指标间的关系，而对这些关系的正确性与否没有给出具体的例证。若实现这一点，将是一件十分有意义的事情，可能写出比本文还厚的另一份论文。除此，我们认为以下内容也是值得进一步研究的：

1）设计 ROM 下可证明安全的基于 RSA 的远程用户口令认证协议。尽作者所知，近期虽然有若干基于 RSA 的协议被提出，但这些协议都仅仅给出了启发式分析。鉴于 RSA 加密和解密操作运算量的非对称性，在资源受限环境下具有独特的优势，设计可证安全的此类协议是我们下一步的工作。

2）设计基于多服务器架构的远程用户口令认证协议。若采用本文所研究的这些方案，对于每个应用系统，用户都需要记住相应的 ID 和口令。随着信息化进程的推进，大量的信息系统被建设，用户需要维护（记忆）大量的（ID，口令）对，这将给用户带来很大的负担和潜在安全隐患。为此，基于多服务器架构的协议具有重要应用前景，但这方面研究刚刚开始起步，是一个非常值得研究的方向。

3）针对特定应用场合，比如异构传感网环境下实时数据获取访问控制中的认证问题，卫星通信中的用户接入认证问题，无线融合网络漫游环境下的接入认证问题等，来设计安全高效的特种双因子认证协议，也将会是未来非常出色的工作。

参考文献

[1] O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication[J]. Proceedings of the IEEE, 2003,91(12):2021-2040P

[2] Klein D V. Foiling the cracker: A survey of, and improvements to, password security[C]. Proceedings of the 2nd USENIX Security Workshop, Anaheim, CA, USA. Berkeley, CA, USA: USENIX Association, 1990: 5−14P

[3] Rossudowski A M, Venter H S, Eloff J, et al. A security privacy aware architecture and protocol for a single smart card used for multiple services[J]. Computers & Security, 2010,29(4):393-409P

[4] Wikipedia. Smart Cards[EB/OL]. [Sep 20th, 2012]. http://en.wikipedia.org/wiki/Smart_card.

[5] Hsu C L. Security of two remote user authentication schemes using smart cards[J]. Consumer Electronics, IEEE Transactions on, 2003,49(4):1196-1198P

[6] Yoon E J, Ryu E K, Yoo K Y. Further improvement of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 612-614P

[7] Chien H Y, Chen C H. A remote authentication scheme preserving user anonymity[C]. Proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA 2005), Taipei, Taiwan, 2005. Washington, DC, USA, IEEE Computer Society, 2005:245-248 P

[8] Wang X, Zhang W, Zhang J, et al. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards[J]. Computer Standards &Interfaces, 2007,29(5):507-512P

[9] Wang Y, Liu J, Xiao F, et al. A more efficient and secure dynamic ID-based remote user authentication scheme[J]. Computer communications, 2009,32(4):583-585P

[10] Song R. Advanced smart card based password authentication protocol[J]. Computer Standards & Interfaces, 2010,32(5):321-325P

[11] Chen Y, Huang C H, Others. Comments on five smart card based password authentication protocols[J]. International Journal of Computer Science and Information Security, 2010, 8(2):16-20P

[12] Chen T H, Hsiang H C, 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):377-380P

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

[14] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. Proceedings of 19th Annual International Cryptology Conference, California, USA, August 15–19, 1999. Berlin: Springer, 1999:388-397P

[15] 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 P

[16] Gu K, Wu L, Li X, et al. Design and Implementation of an Electromagnetic Analysis System for Smart Cards[C]. Proceedings of 2011 Seventh International Conference on Computational Intelligence and Security (CIS 2011), Hainan, China. Washington, DC, USA, IEEE Computer Society, 2011: 653-656 P

[17] Kasper T, Oswald D, Paar C. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation[J]. RFID. Security and Privacy, 2012:61-77P

[18] Yang G, Wong D S, Wang H, et al. Two-factor mutual authentication based on smart cards and passwords[J]. Journal of Computer and System Sciences, 2008,74(7):1160-1172P

[19] Xu J, Zhu W T, Feng D G. An improved smart card based password authentication scheme with provable security[J]. Computer Standards & Interfaces, 2009,31(4):723-728P

[20] Kim S K, Chung M G. More secure remote user authentication scheme[J]. Computer Communications, 2009,32(6):1018-1021P

[21] Hsiang H C, Shih W K. Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards[J]. Computer Communications, 2009,32(4):649-652P

[22] Sood S K, Sarje A K, Singh K. An improvement of Hsiang-Shih's authentication scheme using smart cards[C]. Proceedings of the International Conference and Workshop on Emerging Trends in Technology, Mumbai, India , February 26 - 27, 2010. New York, USA, ACM Press, 2010:19-25P

[23] Sood S K, Sarje A K, Singh K. An improvement of Liao et al.'s authentication scheme using smart cards[C]. Porceedings of 2010 IEEE 2nd International Advance Computing Conference (IACC 2010), Patiala, India February 19-20, 2010. Washington, DC, USA, IEEE Computer Society, 2010: 240-245P

[24] Sood S K, Sarje A K, Singh K. An improvement of Xu et al.'s authentication scheme using smart cards[C]. Proceedings of the Third Annual ACM Bangalore Conference, New York, USA, ACM Press, 2010:15-22P

[25] 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):1449-1462P

[26] Sood S, Sarje A, Singh K. Secure dynamic identity-based remote user authentication scheme[C]. Proceedings of the 6th International Conference on Distributed Computing and Internet Technology (ICDCIT 2010), Lecture Notes in Computer Science, Vol. 5966, Springer-Verlag, 2010: 224-235P

[27] Yeh K H, Su C, Lo N W, et al. Two robust remote user authentication protocols using smart cards[J]. Journal of Systems and Software, 2010,83(12):2556-2565P

[28] Tsai J L. Weaknesses and Improvement of Hsu-Chuang's User Identification Scheme[J]. Information Technology and Control, 2010,39(1):48-50P

[29] Li C T, Lee C C, Liu C J, et al. A robust remote user authentication scheme against smart card security breach[C]. Proceedings of 25th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec 2011), Richmond, VA, USA, July 11-13, 2011. Berlin: Springer, 2011:231-238P

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

[31] Sood S K. Secure Dynamic Identity-Based Authentication Scheme Using Smart Cards[J]. Information Security Journal: A Global Perspective, 2011,20(2):67-77P

[32] Ratanahirwal R, Sanjay Sonwanshi S. An Efficient and Secure ID-based Remote User Authentication Scheme using Smart Card[J]. International Journal of Applied Information Systems, 2012,1(6):35-41P

[33] 谢琪, 陈德人, 于秀源. Park 等远程用户认证协议的分析与改进[J]. 系统工程理论与实践, 2010(10):1877-1882 页

[34] 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(7):589-593 页

[35] 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(5):140-145 页

[36] Ma C G, Wang D, Zhang Q M. Cryptanalysis and Improvement of Sood et al.'s Dynamic ID-Based Authentication Scheme[C]. Proceedings of the 8th International Conference on Distributed Computing and Internet Technology (ICDCIT 2012), Bhubaneswar, India, February 2-4, 2012. Berlin: Springer-Verlag, LNCS, Vol.7514, 2012:141-152P

[37] Wu S, Zhu Y, Pu Q. Robust smart-cards-based user authentication scheme with user anonymity[J]. Security and Communication Networks, 2012,5(2):236-248P

[38] Ma C G, Wang D, Zhao P, et al. A New Dynamic ID-Based Remote User Authentication Scheme with Forward Secrecy[C]. Proceedings of the 14th Asia-Pacific Web Conference (APWeb 2012 Workshops), Kunming, China, April 11-13. Berlin: Springer, 2012: 199-211P

[39] Hankerson D R, Vanstone S A, Menezes A J. Guide to elliptic curve cryptography[M]. Springer-Verlag, New York Inc, 2004: 74-101P

[40] Chabanne H, Tibouchi M. Securing E-passports with elliptic curves[J]. IEEE Security & Privacy, 2011,9(2):75-78P

[41] Lauter K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless Communications, 2004,11(1):62-67P

[42] Islam S H, Biswas G P. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystemon [J]. The Journal of Systems and Software, 2012, 84(11):1892-1898P

[43] Yoon E J, Yoo K Y. Three Attacks on Jia et al.‟ s Remote User Authentication Scheme using Bilinear Pairings and ECC[J]. World Academy of Science, Engineering and Technology, 2011,60(1): 621-626P

[44] Toan T, Minh-Triet T, Anh-Duc D. Improvement of the More Efficient and Secure ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC[C]. Proceedings of AINA 2012, Fukuoka, Japan. Washington, DC, USA, IEEE Computer Society, 2012: 698-703P

[45] He D, Chen J, Hu J. An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security[J]. Information Fusion, 2012,13(3):223-230P

[46] Islam S, Biswas G. Design of improved password authentication and update scheme based on elliptic curve cryptography[J]. Mathematical and Computer Modelling, 2012, Doi:10.1016/j.mcm.2011.07.01

[47] Yang J, Chang C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]. Computers & Security, 2009,28(3–4):138-143P

[48] Toan-Thinh T, Minh-Triet T, Anh-Duc D. Improvement of the More Efficient and Secure ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC[C]. Proceedings of AINA 2012. Washington, DC, USA, IEEE Computer Society, 2012: 698-703P

[49] Yang J H, Chang C C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]. Computers & security, 2009,28(3-4):138-143P

[50] Wang R C, Juang W S, Lei C L. A simple and efficient key exchange scheme against the smart card loss problem[J]. Emerging Directions in Embedded and Ubiquitous Computing, 2007:728-744P

[51] Wang R C, Juang W S, Lei C L. Provably secure and efficient identification and key agreement protocol with user anonymity[J]. Journal of Computer and System Sciences, 2011,77(4):790-798P

[52] Hafizul Islam S K, Biswas G P. Comments on ID-Based Client Authentication with Key Agreement Protocol on ECC for Mobile Client-Server Environment[C]. Proceedings of Advances in Computing and Communications 2011. Berlin: Springer, 2011:628-635P

[53] Wang D, Ma C. Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC [J]. Information Fusion, 2013, Doi: http://dx.doi.org/10.1016/j.inffus.2012.12.002

[54] 薛锋, 汪定, 王立萍, 马春光. 对两个基于智能卡的口令认证协议的安全性分析[J]. 计算机应用, 2012,32(7):2007-2009 页

[55] Ding Wang, Chunguang Ma, Sendong Zhao, Changli Zhou. Breaking a Robust Remote User

Authentication Scheme using Smart Cards. Proceedings of the 9th IFIP International Conference on Network and Parallel Computing (NPC 2012). Berlin: Springer-Verlag, 2012: 110–118P

[56] Wang D, Ma C, Shi L, et al. On the Security of an Improved Password Authentication Scheme Based on ECC[C].Proceedings of ICICA 2012, Chende, China, Sep 14-16. Berlin: Springer, 2012: 181-188P

[57] Mao W. Modern Cryptography: Theory and Practice[M]. New York: Prentice Hall, 2004: 23-65P

[58] Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences, 2010,180(15):2895-2903P

[59] Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[J]. Cryptographic Hardware and Embedded Systems-CHES 2004, 2004:925-943P

[60] Scott M A C N. Implementing Cryptographic Pairings on Smartcard[C]. Proceedings of CHES 2006 , Yokohama, Japan, October 10-13. Berlin: Springer-Verlag, 2006: 134-147P

[61] Wang H, Li Q. Efficient implementation of public key cryptosystems on mote sensors[C]. Proceedings of ICICS 2006, Raleigh, NC, USA, December 4-7. Berlin: Springer-Verlag, 2006:519-528 P

[62] Bertoni G M, Chen L, Fragneto P, et al. Computing tate pairing on smartcards[J]. White Paper, STMicroelectronics, 2005:1-13P

[63] Zhao J, Gu D. Provably secure authenticated key exchange protocol under the CDH assumption[J]. Journal of Systems and Software, 2010,83(11):2297-2304P

[64] Chang Y F, Chang P Y. An Improved User Authentication and Key Agreement Scheme Providing User Anonymity[J].JOURNAL OF ELECTRONIC SCIENCE AND TECHNOLOGY, 2011,9(4):352-358 P

[65] Li C T. Secure smart card based password authentication scheme with user anonymity[J]. Information Technology And Control, 2011,40(2):157-162P

[66] Pu Q, Wang J, Zhao R. Strong authentication scheme for telecare medicine information systems[J]. Journal of Medical Systems, 2011:1-11P

[67] Tseng Y M. On the security of an efficient two-pass key agreement protocol[J]. Computer Standards & Interfaces, 2004,26(4):371-374P

[68] Chang C C, Wu T C. Remote password authentication with smart cards[J]. IEE Proceedings-E Computers and Digital Techniques, 1991,138:165-168P

[69] Madhusudhan R, Mittal R C. Dynamic ID-based remote user password authentication schemes using smart cards: A review[J]. Journal of Network and Computer Applications, 2012,35(4):1235-1248.

[70] 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.

[71] Kim J Y, Choi H K, Copeland J A. Further Improved Remote User Authentication Scheme[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011,94(6): 1426-1433P

[72] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol[C]. Proceedings of CRYPTO 2005, California, USA, August 14-18. Berlin: Springer-Verlag, 2005:546-566P

[73] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis[C]. Crytography and Coding, UK, December 17–19. Berlin: Springer-B1997:30-45P

[74] Liao I E, Lee C C, Hwang M S. A password authentication scheme over insecure networks[J]. Journal of Computer and System Sciences, 2006,72(4):727-740P

[75] Ma C, Wang D, Zhao S. Security flaws in two improved remote user authenti- cation schemes using smart cards[J]. International Journal of Communication Systems, 2012, doi: 10.1002/dac.2468

[76] Chen T H, Chen Y C, Shih W K, et al. An efficient anonymous authentication protocol for mobile

pay-TV[J]. Journal of Network and Computer Applications, 2011,34(4):1131-1137P

[77] Hsieh W, Leu J. Exploiting hash functions to intensify the remote user authentication scheme[J]. Computers & Security, 2012,31(6):791-798P

[78] Mangard S, Oswald E, Popp T. Power analysis attacks: Revealing the secrets of smart cards[M]. Springer-Verlag, New York Inc, 2007: 107-153P

[79] Mangard S, Oswald E, Standaert F X. One for all?? all for one: unifying standard differential power analysis attacks[J]. IET Information Security, 2011,5(2):100-110P

[80] 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):204-207P

[81] 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 environments[J]. Computer Standards & Interfaces, 2009,31(4):863-868P

[82] WANG D, MA C. Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards[J]. The Journal of China Universities of Posts and Telecommunications, 2012, 19(5):104-114P

[83] Das M L, Saxena A, Gulati V P. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Consumer Electronics, 2004,50(2):629-631P

[84] Halevi S, Krawczyk H. Public key cryptogrphy and password protocols[J]. ACM Transactions on Information and System Security,2(3):230-268P

[85] Wang D, Ma C. On the (in)security of some smart-card-based password authentication schemes for WSN [R].IACR Cryptology ePrint Archive 2012/581, 2012, http://eprint.iacr.org/2012/581.pdf

[86] Wang D, Ma C. Robust Smart Card based Password Authentication Scheme against Smart Card Security Breach[R]. IACR Cryptology ePrint Archive 2012/439, http://eprint.iacr.org/2012/439.pdf

[87] Xie Q. Dynamic id-based password authentication protocol with strong security against smart card lost attacks[J]. Proceedings of ICWCA 2011, Sanya, China, August 1-3. Berlin: Springer, 2012:412-418 P

[88] Wang D, Ma C, Wu P. Secure password-based remote user authentication scheme with non-tamper resistant smart cards[C].Proceedings of DBSec 2012, Paris, France. Berlin: Springer, 2012:114-121P

[89] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005(10):1743-1756 页

[90] 赵建杰. 认证密钥协商协议的分析与设计[D]. 上海交通大学博士学位论文, 2011: 2-10 页

[91] Thayer F J, Abrega F, Herzog J C, et al. Strand spaces: proving security protocols correct[J]. Journal of Computer Security, 1999,7(2):191-230P

[92] Syverson P F, van Oorschot P C. On unifying some cryptographic protocol logics[C]. Proceedings of IEEE S&P 1994, Okland, CA, USA. IEEE Computer Society, 1994: 14-28P

[93] Burrows M, Abadi M, Needham R. A logic of authentication [J]. ACM Transactions on Computer Systems, 1990,8(1):18-36P

[94] Vaidya B, Makrakis D, Mouftah H. Two-factor mutual authentication with key agreement in wireless sensor networks[J]. Security and Communication Networks, 2012, DOI: 10.1002/sec.517

[95] Kumar P, Lee S G, Lee H J. E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks[J]. Sensors, 2012,12(2):1625-1647P

[96] Yoo S G, Park K Y, Kim J. A Security-Performance-Balanced User Authentication Scheme for Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2012, doi:10.1155/2012/382810

[97] Choo K K, Boyd C, Hitchcock Y. Errors in computational complexity proofs for protocols[C]. Proceedings of ASIACRYPT 2005, Chennai, India, December 4-8. Berlin: Springer, 2005:624-643P

[98] Bellare M, Rogaway P. Entity authentication and key distribution[C]. Proceedings of CRYPTO'93, California, USA August 22–26. Berlin: Springer, 1994:232-249P

[99] 龚征. 随机预言机模型下可证明安全性关键问题研究[D]. 上海交通大学博士论文, 2008: 1-17 页

[100] Mangipudi K,Katti R. A secure identification and key agreement protocol with user anonymity (SIKA)[J]. Computers & Security, 2006,25(6):420-425P

[101] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C]. Proceedings of ACM CCS 2003, Fairfax, VA, USA. New York,USA, ACM Press: 62-73P

[102] Smart N P, Vercauteren F. On computable isomorphisms in efficient asymmetric pairing-based systems[J]. Discrete Applied Mathematics, 2007,155(4):538-547P

[103] He D, Chen J, Hu J. An ID-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunications, 2011,66(11):657-662P

[104] Mangard S, Oswald E, Popp T. Power analysis attacks: Revealing the secrets of smart cards[M]. Springer, 2007: 78-112P

[105] Hao F. On robust key agreement based on public key authentication[J]. Security and Communication Networks, 2012, DOI: 10.1002/sec.550

[106] Neuman C C, Ts'O T. Kerberos: An authentication service for computer networks[J]. Communications Magazine, IEEE, 1994,32(9):33-38P

[107] Baldoni R, Corsaro A, Querzoni L, et al. Coupling-based internal clock synchronization for large-scale dynamic distributed systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2010,21(5):607-619P

[108] Han J, Jeong D K. A practical implementation of IEEE 1588-2008 transparent clock for distributed measurement and control systems[J]. IEEE Transactions on Instrumentation and Measurement, 2010,59(2):433-439P

[109] Gong L. A security risk of depending on synchronized clocks[J]. ACM SIGOPS Operating Systems Review, 1992,26(1):49-53P

[110] Mao W. Modern cryptography: theory and practice[M]. Publisher: Prentice Hall PTR, Copyright: Hewlett Packard, 2004:515-551P

[111] Wu Z Y, Lee Y C, Lai F, et al. A secure authentication scheme for telecare medicine information systems[J]. Journal of medical systems, 2012:1-7P

[112] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983,29(2):198-208P

[113] Wang Y. Password protected smart card and memory stick authentication against off-line dictionary attacks[C]. Proceedings of SEC 2012, Heraklion, Crete, Greece. Berlin, Springer, 2012:489-500P

[114] Florencio D, Herley C. A large-scale study of web password habits[C]. Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada. New York, ACM Press: 657-666P

[115] Dell'Amico M, Michiardi P, Roudier Y. Password strength: an empirical analysis[C]. Proceedings of INFOCOM 2010 , San Diego, CA. Washington, DC, USA, IEEE Computer Society, 2010:1-9P

[116] Wu T. A real-world analysis of Kerberos password security[C]. Proceedings of the 1999 ISOC Network and Distributed System Security Symposium, San Diego, CA, USA. ISOC, 1999:1-14P

[117] 魏福山. 网关口令认证密钥交换协议的安全模型与设计研究[D]. 解放军信息工程大学博士学位论文, 2011:7-15 页

[118] Goldreich O. Foundations of Cryptography[M]. England: Cambridge University Press, 2003: 21-39P

[119] Park J H, Lee J S, Chang J H. An efficient remote user authentication scheme secure against the off-line password guessing attack by power analysis[C]. Proceedings of ICACT 2009, Phoenix Park, Korea, 2009. Washington, DC, USA, IEEE Computer Society, 2009: 1289-1292P

[120] 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): 204-207P

[121] Sun H M. An efficient remote use authentication scheme using smart cards[J]. IEEE Transactions on Consumer Electronics, 2000,46(4):958-961P

[122] Chien H Y, Jan J K, Tseng Y M. An efficient and practical solution to remote authentication: smart card[J]. Computers & Security, 2002, 21(4):372-375P

[123] Yoon E J, Ryu E K, Yoo K Y. An improvement of Hwang–Lee–Tang's simple remote user authentication scheme[J]. Computers & Security, 2005,24(1):50-56P

[124] Hwang M S, Lee C C, Tang Y L. A simple remote user authentication scheme[J]. Mathematical and Computer Modelling, 2002,36(1):103-107P

[125] Sood S K, Sarje A K, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture[J]. Journal of Network and Computer Applications, 2011,34(2):609-618P

[126] Kai H, Qingyu O, Xiaoping W, et al. Cryptanalysis of a remote user authentication scheme using smart cards [C]. Proceedings of WiCom 2009, Beijing, China, September 24-26. Washington, DC, USA, IEEE Computer Society, 2009:1-4P

[127] Roy S, Das A K, Li Y. Cryptanalysis and security enhancement of an advanced authentication scheme using smart cards, and a key agreement scheme for two-party communication. Proceedings of IEEE IPCCC 2011, Orlando, FL. Washington, DC, USA, IEEE Computer Society, 2011:1-7P

[128] Sun D Z, Huai J P, Sun J Z, et al. Cryptanalysis of a mutual authentication scheme based on nonce and smart cards[J]. Computer Communications, 2009,32(6):1015-1017P

[129] Xiang T, Wong K, Liao X. Cryptanalysis of a password authentication scheme over insecure networks[J]. Journal of Computer and system Sciences, 2008,74(5):657-661P

[130] Junghyun N, Seungjoo K, Dongho W. Security analysis of a nonce-based user authentication scheme using smart cards[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007,90(1):299-302P

[131] Ku W C, Tsai H C, Chen S M. Two simple attacks on Lin-Shen-Hwang's strong-password authentication protocol[J]. ACM SIGOPS Operating Systems Review, 2003,37(4):26-31P

[132] 汪定, 马春光, 翁臣, 等. 强健安全网络中的中间人攻击研究[J]. 计算机应用, 2012(1):42-44 页

[133] Juang W S, Chen S T, Liaw H T. Robust and efficient password-authenticated key agreement using smart cards[J]. IEEE Transactions on Industrial Electronics, 2008,55(6):2551-2556P

[134] Wang D, Ma C, Zhao S, et al. Breaking a Robust Remote User Authentication Scheme using Smart Cards[C]. Proceedings of 9th IFIP International Conference on Network and Parallel Computing (NPC 2012), Gwangju, Korea. Berlin: Springer-Verlag, 2012: 110-118P

[135] Li X, Zhang Y. A simple and robust anonymous two-factor authenticated key exchange protocol[J]. Security and Communication Networks, 2012, DOI: 10.1002/sec.605

[136] 汪定, 薛锋, 王立萍, 等. 改进的具有 PFS 特性的口令认证密钥协商方案[J]. 山东大学学报(理学版), 2012,47(9):19-25 页

[137] Park D G, Boyd C, Moon S J. Forward secrecy and its application to future mobile communications

security[C]. Proceedings of PKC 2000, Melbourne, Australia. Berlin: Springer, 2000:433-445P

[138] Chen B L, Kuo W C, Wuu L C. Robust smart-card-based remote user password authentication scheme[J]. International Journal of Communication Systems, 2012, DOI: 10.1002/dac.2368

[139] Lee S W, Kim H S, Yoo K Y. Efficient nonce-based remote user authentication scheme using smart cards[J]. Applied Mathematics and Computation, 2005,167(1):355-361P

[140] Wen F, Li X. An improved dynamic ID-based remote user authentication with key agreement scheme[J]. Computers & Electrical Engineering, 2011, 38(2): 381-387P

[141] Horng W B, Lee C P, Peng J W. A secure remote authentication scheme preserving user anonymity with non-tamper resistant smart cards[J]. WSEAS Transactions on Information Science and Applications, 2010,7(5):619-628P

[142] Li X, Qiu W, Zheng D, et al. Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards[J]. IEEE Transactions on Industrial Electronics, 2010,57(2): 793-800P

[143] Wang D, Ma C G, Zhang Q M. Secure Password-based Remote User Authentication Scheme against Smart Cards Loss attack. Journal of Networks, 2013, 8(1):148-155P

[144] 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 页

[145] Diffie W, Oorschot P C, Wiener M J. Authentication and authenticated key exchanges[J]. Designs, Codes and Cryptography, 1992,2(2):107-125P

[146] Ferguson N, Schneier B, Kohno T. Cryptography Engineering: Design Principles and Practical Applications[M]. John Wiley & Sons, 2012: 134-149P

[147] Scott M. MIRACL Library[EB/OL]. [Feb 2, 2012]. http://www. shamus.ie/index.php?page=home.

[148] Großschädl J, Kamendje G A. Architectural enhancements for Montgomery multiplication on embedded RISC processor [C]. Proceedings of ACNS 2003, Kunming, China, October 16-19. Berlin: Springer, 2003:418-434P

[149] Wong D S, Fuentes H H, Chan A H. The performance measurement of cryptographic primitives on palm devices[C]. Proceedings of 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, Dec 10-14. Washington, DC, USA, IEEE Computer Society, 2001: 92-101P

[150] 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):128-143P

[151] 汪定, 马春光, 翁臣, 等. 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[J].电子与信息学报, 2012,34(10):2520-2526 页

[152] 汪定, 马春光, 孟彦, 等. 可证明安全的高效远程用户认证协议[J]. 计算机研究与发展, 2013, (已投稿)

[153] He D, Ma M, Zhang Y, et al. A strong user authentication scheme with smart cards for wireless communications[J]. Computer Communications, 2011,34(3):367-374P

[154] Menezes A. Another look at provable security[J]. Journal of Cryptology, 2007, 20(1):3-37P

[155] Bresson E, Chevassut O, Pointcheval D. New security results on encrypted key exchange[C]. Proceedings of 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004. Berlin: Springer, 2004:145-158P

攻读硕士学位期间发表的论文和取得的科研成果

已发表论文

[1] **Ding Wang**, Chunguang Ma. Cryptanalysis of a Remote User Authentication Scheme for Mobile Client-Server Environment with Provable Security based on ECC. **Information Fusion**, 2013, Doi: http://dx.doi.org/10.1016/j.inffus.2012.12.002 (**SCI/EI, IF=1.467**)

[2] Chunguang Ma, **Ding Wang**, Sendong Zhao. Security flaws in two improved remote user authentication schemes using smart cards. **International Journal of Communication Systems**, 2012, Doi: http://dx.doi.org/10.1002/dac.2468 (**SCI/EI, IF=0.406**)

[3] **Ding Wang**, Chunguang Ma. Cryptanalysis and security enhancement of a remote user authentication scheme. **The Journal of China Universities of Posts and Telecommunications**, 2012, 19(5):104-114, Doi: http://dx.doi.org/10.1016/S1005-8885(11)60307-5 **(EI)**

[4] **Ding Wang**, Chunguang Ma, Qiming Zhang, et al. Secure Password-based Remote User Authentication Scheme against Smart Cards Loss attack. **Journal of Networks**, 2013, 8(1):148-155. **(EI)**

[5] **Ding Wang**, Chunguang Ma, Sendong Zhao, Changli Zhou. Breaking a Robust Remote User Authentication Scheme using Smart Cards. Proceedings of the 9th IFIP International Conference on Network and Parallel Computing (**NPC 2012**), Gwangju, Korea, Sep 6-8, **Lecture Notes in Computer Science**, vol.7351, pp. 110–118. Berlin: Springer-Verlag, 2012. **(**acceptance rate: 38/136 **≈ 27.9%** , **full paper, EI, CCF Rank C**)

[6] **Ding Wang**, Chunguang Ma, Deli Gu, Zhenshan Cui. Cryptanalysis of Two Dynamic ID-based Remote User Authentication Schemes for Multi-Server Architecture. Proceedings of the 6th International Conference on Network and System Security (**NSS 2012**), Wuyishan, China, Nov 21-23, **Lecture Notes in Computer Science,** Vol.7645, pp. 462–475. Berlin: Springer-Verlag, 2012. **(**acceptance rate: 39/173 **≈ 22.5%** , **full paper, EI**)

[7] **Ding Wang**, Chunguang Ma, Peng Wu. Secure password-based remote user authentication scheme with non-tamper resistant smart cards. Proceedings of the 26th Annual IFIP Conference on Data and Applications Security and Privacy (**DBSec 2012**), Paris, France, July 13-16, **Lecture Notes in Computer Science**, vol.7371, pp.114–121. Berlin: Springer-Verlag, 2012 **(**acceptance rate: 23/49 **≈ 46.9%** , **short paper, EI**)

[8] **Ding Wang,** Ying Mei, Chunguang Ma, Zhenshan Cui. Comments on an Advanced Dynamic ID-based Authentication Scheme for Cloud Computing. Proceedings of International Conference on Web Information Systems and Mining (**WISM 2012**), Chengdu, China, October 26–28, **Lecture Notes in Computer Science,** vol.7529, pp.246–253. Berlin: Springer-Verlag, 2012. **(**acceptance rate: 87/418 **≈ 20.8%** , **full paper, EI**)

［9］ **Ding Wang**, Chunguang Ma, Lan Shi, Yu-Heng Wang: On the Security of an Improved Password Authentication Scheme Based on ECC. Proceedings of the Third International Conference Information Computing and Applications (**ICICA 2012**), Chende, China, **Lecture Notes in Computer Science**, vol.7473, pp. 181-188. Berlin: Springer-Verlag, 2012. **(**recommened for publication in LNCS rate: 100/1089 **≈ 9.18%** , **full paper, EI**)

［10］ Chun-guang Ma, **Ding Wang**, Qi-ming Zhang. Cryptanalysis and Improvement of Sood et al.'s Dynamic ID-based Authentication Scheme. Proceedings of the 8th International Conference on Distributed Computing and Internet Technology (**ICDCIT 2012**), Bhubaneswar, India, February 2-4, **Lecture Notes in Computer Science**, vol. 7154, pp. 141–152. Berlin: Springer-Verlag, 2012. **(**acceptance rate: 17/89 **≈ 19.1%** , **full paper, EI**)

［11］ Chun-guang Ma, **Ding Wang**, Ping Zhao, et al.. A new dynamic ID-based remote user authentication scheme with forward secrecy. Proceedings of the 14th Asia-Pacific Web Conference (**APWeb 2012 Workshops**), Kunming, China, April 11-13, **Lecture Notes in Computer Science**, vol. 7234, pp. 199–211.Berlin:Springer-Verlag, 2012. **(**acceptance rate:28/68 **≈ 41.1%** ,**EI, full paper, CCF Rank C**)

［12］ Sendong Zhao, **Ding Wang**, Sicheng Zhao, et al.. Cookie-Proxy: A Solution to Prevent SSLStrip Attack. The 14th International Conference on Information and Communications Security (**ICICS 2012**), Hongkong, China, **Lecture Notes in Computer Science**, vol. 7618, pp. 365–372. Berlin: Springer-Verlag, 2012. **(**acceptance rate: 49/101 **≈ 48.5%** , **EI, Short paper, CCF Rank C**)

［13］ **汪定**，马春光，翁臣，贾春福．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．**电子与信息学报**，2012, 34(10): 2520-2526 **(EI)**

［14］ **汪定**，薛锋，王立萍，马春光．改进的具有 PFS 特性的口令认证密钥协商方案．**山东大学学报(**理学版**)**, 47(9): 19-25 **(中文核心)**

［15］ **汪定**，马春光，张启明．一种强口令认证协议的攻击与改进．**计算机科学**, 2012, 39(6): 72-76 **(中文核心)**

［16］ **汪定**，马春光，翁臣，贾春福．强健安全网络中间人攻击研究.**计算机应用**,2012, 32(1):42-44,65 **(中文核心)**

［17］ 马春光，**汪定**，张启明．广域涉密信息系统域间授权研究．**保密科学技术**, 2011,3(11): 50-52

［18］ 薛锋，**汪定**，王立萍,马春光．对两个基于智能卡的远程用户口令认证协议的安全性分析．**计算机应用**, 2012, 32(7): 221-224 **(中文核心)**

软件著作权

[1] 马春光，**汪定**，翁臣，张启明．无线校园网接入认证系统客户端软件．国家版权局，2011，**授权编号: 2011SR097595**.

致　谢

依稀记得第一次到哈尔滨的那个下午，在哈站前广场，我和一个素不相识的同学拼上了一辆出租，车上聊起来才知道我们将去同一个地方。他叫李东立，本科山东大学，考清华失利后调剂到哈尔滨工程大学。由于志趣相投，我们很快就成了好朋友。铁杆朋友从一个到两个，再到现在的五个，各有所长，我称之为“工程五虎”，都是调剂到这里。转眼间大家就要各奔东西，离开这个度过了人生美好、充实、难忘三年的地方。

东立回清华攻博，森栋到哈工大攻博，海涛去了百度，启明提前毕业进入腾讯，我也正准备去北大攻博。付出终有回报，拼搏的三年，终于到了收获的季节。还记得为了参加 CCNIS 2011 并顺便回郑州的母校解放军信息工程大学看看，连续 20 天加班加点赶出了自己的第一篇学术论文；还记得 2011 年底回母校南开看望贾老师和同学的时候，抓住偶然机遇学会了 Latex 排版软件，不仅革命了自己的论文排版手段，还教会了身边一大批同学；还记得第一篇 EI 等待 15 个月的煎熬和然后收到拒稿通知的难受；还记得第一篇 SCI 被三个审稿人一致“Accept as it is”时的激动；还记得 2012 年 9 月被评为“校十大学术之星”时的释然……。论文完成之际，幻想中的兴奋变成了感激和怀念。

首先要感谢的是我的导师马春光教授。相比其它名校，诚然身边可能少了一些大师和“牛人”，甚至在硬件方面也有劣势，但这里勤奋拼搏的干劲、大气开放的视野、勇争一流的士气和追求卓越的精神丝毫未减！作为马老师“以学生为本”育人理念的见证者和受益者，硕士期间我曾多次受全额资助外出参加 AsiaCrypt、NSS 和 APWeb 等国际著名学术会议，得以有机会与名校同学同台竞技、与学术大家近距离交流，得以找寻差距、激发思维和增长见识。马老师不但教会了我如何做学术，也指引着我如何走人生。尤其感谢马老师对自由探索的支持，对学生想法的尊重和对失败的宽容。如果说能取得一点小小的成果，都是马老师悉心栽培的结果。马老师前瞻的思维，敏锐的眼光，自由的学术思想，高效的做事风格，严谨的治学态度，都使学生受益终身。

在工程的两年多时间里，亲眼见证了 NSR 的成长和壮大，身为这样一个宽松而不失奋进，自由而不失严谨的集体而感到自豪。感谢戴膺赞师兄，楚振江师兄，刘帅师姐，王九如师兄，钟晓睿师姐和周长利师兄，能够沿着你们走过的足迹继续前行十分荣幸；感谢谷德丽同学和张启明同学，能和你们经常在一个战壕里，感受团队作战的力量，倍感珍惜；感谢赵平同学，高训兵同学和肖亮同学，你们各有的长人之处常是我学习的榜样；感谢崔振山师弟、石岚师妹和杨文文师妹在我学习上的合作和帮助；感谢付韬师弟、李迎涛师弟和史晓倩师妹，你们思维敏捷，充满活力，你们蓬勃的朝气也时常感染着我。

感谢南开信息安全系的贾春福老师，难忘本科时您逐字逐句帮我改第一篇论文的情形，难忘您对我们“踏实做人，扎实做事”的谆谆教诲。美丽的南开我的家，毕业五年来每年我都会回去看看，看望恩师和同学们。感谢电院的郭渊博老师，虽在您的直接指

导下只有半年多时间，但您的长者风范，一直以来对后辈的关心和指点，使学生常怀感激，您的为人处世给我留下了深刻印象，更是学生人生道路上学习的楷模。衷心感谢网络实验室王慧强老师、郭方方老师和冯光升老师润物于无声的关心和支持！特别感谢自动化学院李金教授和丛望教授在我硕士求学期间给予的关心和帮助！

感谢都柏林城市大学的 Michael Scott 教授、北卡罗莱纳-夏洛特分校的 Wang Yongge 教授、武汉大学的何德彪副教授和沙特阿拉伯国王大学 M.K. Khan 副教授，与您们的交流和讨论使我对研究方向有了更准确的把握和更开阔的视野！感谢南开大学的李经纬博士、解放军信息工程大学的吴树华和魏福山博士在学术论文投稿方面的交流和帮助！感谢我的学术论文编排修改支援团队，虽然我们分布在不同的实验室，不同的院系，不同的大学，甚至远隔重洋，但地理的距离并没有影响我们体验协同作战的愉快。没有你们，我的很多想法不可能在这么短的时间内变成铅字，出现在 Google Scholar!

感谢局机关的丛局长、覃局长，您们恩师般的关心和培养是我不断奋进的动力，今后不管在哪里，在什么岗位上，我都会牢记您们的指示，立足本职，扎实工作，不给您丢人；感谢局机关的参谋们，您们精于业务，善于处事，是我学习的榜样；感谢单位的院首长、葛部长、张主任、薛参谋和张教导员，感谢您们兄长般的关怀和为我营造的良好的学习大后方，为我提供的难得继续学习机遇，难忘军旅生涯第一步您们的指引。

最后，深深感谢我的父母，您们默默的支持是我勇于面对一切困难的动力。您们勤劳的一生，是为后代无私奉献的一生，您们平凡而伟大，小时候作文中虽常这样写，但至今天才真正理解了它，我为而是您们的儿子而骄傲！感谢小妹汪云，你活泼可爱，懂事乖巧，很荣幸我们不是独生子女~ 感谢所有亲人，你们一直以来的支持和理解是我毕生不断前行的力量源泉！