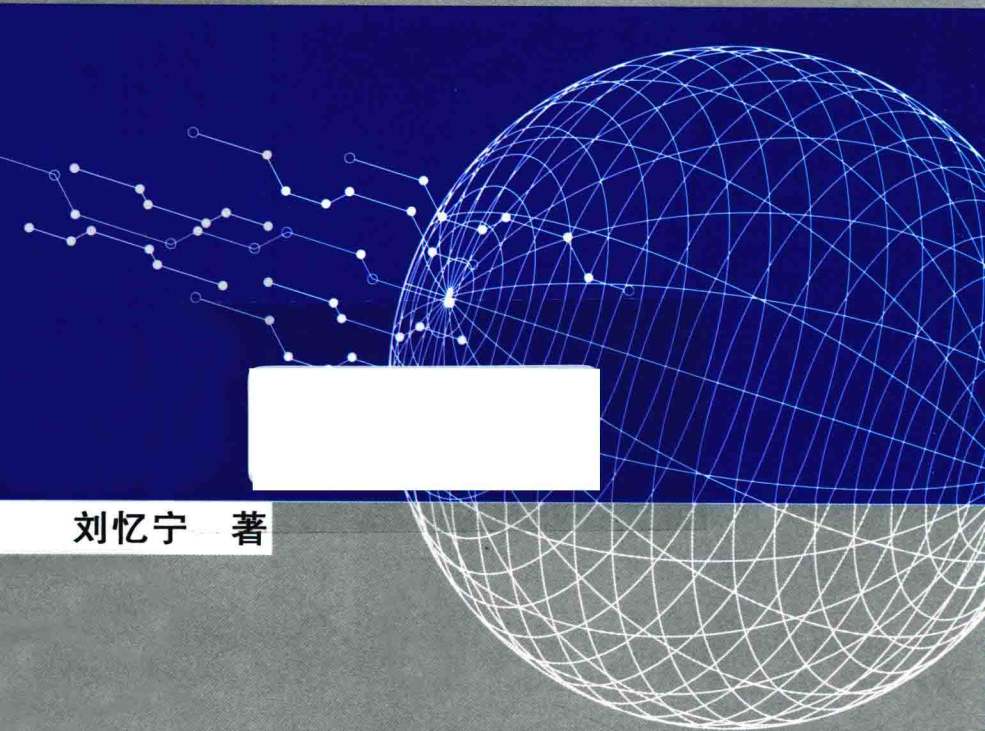
基于秘密分享的信息安全协议



刘忆宁 著

西安电子科技大学出版社
http://www.xduph.com

基于秘密分享的信息安全协议

刘忆宁　著

西安电子科技大学出版社

图书在版编目(CIP)数据

基于秘密分享的信息安全协议/刘忆宁著. —西安：西安电子科技大学出版社，2015.6

ISBN 978-7-5606-3698-6

Ⅰ. ① 基… Ⅱ. ① 刘… Ⅲ. ① 信息安全—通信协议 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2015)第 105386 号

策　划　陈婷

责任编辑　陈婷　马琼

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　邮　　编　710071

网　　址　www.xduph.com　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西天意印务有限责任公司

版　　次　2015 年 6 月第 1 版　2015 年 6 月第 1 次印刷

开　　本　850 毫米×1168 毫米　1/32　印张 3.25

字　　数　62 千字

印　　数　1～1000 册

定　　价　10.00 元

ISBN 978-7-5606-3698-6/TP

XDUP 3990001-1

＊＊＊如有印装问题可调换＊＊＊

内 容 简 介

本书主要介绍基于秘密分享的信息安全协议。本书研究的安全协议包括：安全群组通信、微支付协议、电子彩票协议、互联网彩票协议、电子投票协议以及智能电网中的轻量级通信协议等。书中部分章节的内容已经过同行的严格审查，部分内容曾发表在 IEEE Transactions on Computers，Security and Communication Networks，International Journal of Communication Systems 等期刊，部分章节的内容未曾公开发表过。

本书适合通信及信息安全、应用数学等专业高年级本科生和低年级研究生使用。

作者简介：

刘忆宁，男，1973年11月生，博士，副教授。

1995年毕业于解放军信息工程学院应用数学系，分配至61726部队从事信息安全研究工作。2002年转业，先后在中国地质大学(武汉)、桂林电子科技大学从事信息安全教学科研工作，其间于2003年在华中科技大学获得计算机软件与理论硕士学位，2007年在湖北大学获得基础数学博士学位。

近年来，主要研究基于秘密分享的信息安全协议，包括：群组通信安全协议、电子投票协议以及智能电网中的安全通信协议等，部分成果发表于IEEE Transactions on Computers, Security and Communication Networks, International Journal of Communication Systems, International Journal of Computer Mathematics等SCI期刊。

本专著由国家自然科学基金(61363069)、广西自然科学基金(2014GXNSFAA118364)、广西高等学校高水平创新团队及卓越学者计划、桂林电子科技大学创新团队资助出版。

前　言

近年来，随着网络技术的发展，网络数据的安全性遭受到了严重的威胁。为了保障数据的安全性和可靠性，提高信息系统的效率，信息安全协议相关领域的研究工作得到了前所未有的重视，这既是机遇又是挑战。

信息安全协议对于保障信息系统的安全高效运行具有重要的作用。不同的信息系统对于安全的需求程度也不尽相同，有的协议希望实现具有信息理论意义上的安全性，比如电子投票协议；有的对效率性要求更高，比如微支付协议，即使安全性保障的程度有所降低，但如果能换取更低的通信、存储及计算负担，则也可接受，也更能符合现实的需求；又比如，在电子彩票协议中，则希望能保障所有方同等作用的参与，并且以技术手段实现参与者的可追踪性的验证，从而阻止可能的合谋攻击行为；再比如智能电网协议中，需要考虑双向通信的不均衡问题，即用户端向调度者持续发送实时数据(称为高频数据)，而调度者则根据实时数据向用户端发送调度指令(显然调度指令的频次要远少于前者，被称为低频数据)。在信息系统的运行中，如何保证数据的高效安全传输，是值得研究的内容。

为了实现信息系统的安全性，本书以 Shamir 的秘密分享为基础，设计了一系列的安全协议。以 Shamir 秘密分享为基础的原因主要有两点：一是简单高效，二是具有信息理论意义上的安

全性。

本人一直都从事密码分析与破译、信息安全教学与科研等方面的工作，积累了一定的经验，也有过不少关于失败的切身体会。本书的内容，是对过去数年研究工作的小结，部分内容已经得到业内同行的认可，也有部分内容是最新的研究成果。回头看，还是觉得受益颇多，惟愿与志同者分享。

值本书出版之际，感谢各位前辈，尤其是美国密苏里大学韩亮(Lein Harn)教授、台湾逢甲大学张真诚(Chin chen Chang)教授、澳大利亚卧龙岗大学穆怡(Yi Mu)教授，对本人研究工作的悉心指点与提携，也感谢各位业内同行的关心与支持。

限于时间和篇幅，书中若有不妥之处，恳请同行和读者给予批评和指正。

著　者

2015 年 3 月

目　录

第1章 引 言

随着互联网技术的发展，大量的敏感信息通过各种网络进行传输。同时，由于网络的开放性，使得互联网上存在大量的攻击行为。在享用互联网便利性的同时，实现信息的安全保护，是一项重要的研究内容。除了制订完善的规章制度，做好物理防护措施外，使用密码学相关知识实现技术层面的安全防护，也是有价值的工作。

面对各种攻击行为，如非法访问、信息泄露、篡改、毁坏等，信息系统致力于实现机密性、完整性、可靠性、认证性等目标。机密性指防止未经授权的用户用非常规手段获取相关信息；完整性指非法用户不能随意篡改传输的数据，如果完整性受到破坏，信息的合法接收者可以检测得到；可靠性指用于存储、处理数据的系统具有一定的抗干扰破坏的能力，数据的传输系统在受到一定程度的干扰甚至破坏时，也能够正常地运行；而认证性通常用来保证参与信息接收及传送的个体是被授权的。

由于信息系统的使用遍及各个行业，使得一些网络系统对协议的安全性提出了更为独特的要求。比如，在基于移动终端的网络系统中，通常会要求移动终端执行的运算是轻量级的。另外，

考虑到通信传输对于移动终端的电量消耗较大，移动终端的通信传输负担也应该尽量小。而在基于互联网的彩票协议中，公平性的要求更为显著，通常会要求协议的所有参与者能够验证结果的公平性，即可以实现协议的可追踪性，这对协议的设计是一个挑战。再比如，对于电子投票协议来说，仅实现计算意义上的安全性是不够的，还应该实现信息理论意义上的安全性。这是因为，在关系政治大局的选举活动中，投票的内容要求长期保密，而计算安全性有可能随着敌手计算能力的增强而影响已有选票内容的安全性。而且电子投票协议通常还要求满足两个看似矛盾的安全目标：在保证投票者可验证性的同时，又要保证投票者无法向他人证明自己的选票内容，即抗胁迫性。除了一些物理措施外，为了实现这些安全目标，通常使用密码技术，如加解密、数据签名以及散列函数等来保证系统的安全性。

信息安全协议通常是一系列的规范和流程，规定先做什么再做什么，每一个步骤使用不同的密码技术来实施，也可以说，安全协议是针对特定使用环境、基于密码算法的操作规范。密码算法的安全并不一定保证安全协议的安全，除了使用方法的不规范之外，协议本身的漏洞也是较为常见的。这种现象有点类似于广为使用的操作系统，只有在广泛使用中才能发现较多的安全漏洞，并及时给予修正。通信系统中的安全协议对于保证通信传输的安全具有重要的作用。通常情况下，密钥建立协议、身份认证协议、消息认证码以及各种应用层的安全协议，都被广泛地研究和应用。

本书研究了基于 Shamir 的秘密分享的安全协议，包括群组

通信中的密钥分发协议、微支付协议、可追踪的电子彩票协议、可抵抗侧信道攻击的电子投票协议以及面向智能电网的轻量级通信协议。选用 Shamir 的秘密分享作为安全协议的基础，是基于它的两个特点：信息理论意义上的安全性和轻量级的计算复杂度。

图 1.1 给出了本书研究的基础、拟实现的安全目标以及具体的安全协议。

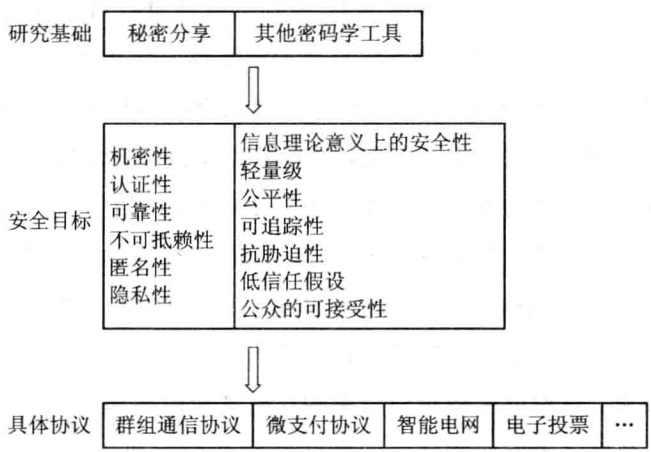


图 1.1　本书研究内容框架

本书具体内容安排如下：

第 2 章介绍了与本书研究内容直接相关的密码学知识，包括 Shamir 秘密分享理论、基于离散对数的 Pedersen 承诺、基于 Pedersen 的零知识证明以及可验证随机数构造等内容。

第 3 章首先介绍了 2010 年 Lein Harn 等人设计的群组通信中的密钥分发协议，指出其不能抵抗内部人攻击，并给出了攻击

的实例；然后给出了改进的群组通信中的密钥分发协议，该协议可抵抗来自内部或外部的人为攻击，即群组通信成员可以恢复出会话密钥但无法得知其他成员与密钥管理中心的长期秘密，群组之外的成员既无法得到群组的会话密钥，也无法得知合法群组成员与密钥管理中心的共享秘密。

第 4 章首先介绍了 Micali 和 Rivest 的基于概率抽取的微支付协议，并指出了其不适用于移动互联网环境的原因。为了使微支付协议在满足移动终端的前提下(即具有轻量级)，同时也满足可验证的公平性以及保障协议成员的隐私性，本书设计出了改良版的轻量级微支付协议，其中概率抽取的算法由所有参与者发挥同等的影响力，共同生成结果，保障了协议的可验证公平性。

第 5 章首先分析了张真诚等人给出的互联网上的电子彩票协议，指出其不能抵抗发行机构和彩票购买者之间的合谋攻击，而这容易破坏协议的公平性。具体而言，即彩票的发行机构可以预先设定中奖结果，并与最后一名彩票购买者合谋，保证该购买者总是获奖，这对电子彩票协议来说，是致命的缺陷。与第 4 章类似，可验证公平性的实现是本章研究结果的主要贡献与创新点，其有效地阻止了发行机构与恶意购买者之间的合谋攻击。

第 6 章借鉴穆怡教授茫然传输协议的设计思想，设计了基于拉格朗日插值多项式以及盲签名的电子彩票协议。协议的主要特点是保障彩票的购买者可追踪自己的参与是否被融入了中奖数字的生成，从而避免各种合谋攻击的可能。

第 7 章主要研究基于 Bingo Voting 的电子投票协议。针对 Bingo Voting 不能抵抗来自恶意投票者侧信道攻击的缺陷，本书

给出了相应的改进方案，使投票者不具有比旁观者更多的信息量，以阻止侧信道攻击。

第8章设计了轻量级且可认证的通信方案，以保证智能电网中实时采集的数据和指挥中心的指令能够安全地双向传输。与其他论文中的结果相比，此方案的存储复杂度和通信负担大幅降低，最高降幅达到70%以上，这对于保障协议的实际可用性具有重要意义。

第2章 密码学基础

本章介绍理论安全(无条件安全)与计算安全、Shamir 的秘密分享协议、Pedersen 承诺、以秘密分享和承诺技术为基础的可验证随机数、盲签名以及茫然传输协议，这些是本书安全协议设计的基础。另外，本章还将介绍基于 Pedersen 承诺的零知识证明。

2.1 理论安全与计算安全

信息安全协议的设计目标可分为两类：无条件安全(理论安全)与计算安全。

假设攻击者有无限的计算能力，仍然无法攻破一个密码系统，则称这个密码系统是无条件安全，也称为理论安全。无条件安全不依赖任何困难性假设，其安全性不随着计算机技术的发展而受到影响。“一次一密”是典型的理论安全，其安全性依靠真随机数的生成。

但“一次一密”之类的理论安全，由于其成本很高，使得使用范围受到限制，所以在现实中，使用更多的是计算安全。计算安

全通常依赖某一个困难性假设，即在现有的计算条件下，攻击者无法在短时间内破解该密码系统。这些困难性假设通常是一些复杂的数学难题，如大整数分解、离散对数等。

通常情况下，计算安全就足以满足大多数的安全性需求。但在某些情况下，如电子投票协议，由于其结果不仅影响当下，而且有可能影响未来几十年的发展，因此电子投票协议仅满足计算安全是不够的。

2.2 Shamir 秘密分享

Shamir 在 1979 年给出了秘密分享理论。将秘密 s 分成 n 份，分别是 s_1，…，s_n，满足以下两个要求：

(1) 有 t 个或 t 个以上的秘密片断，可以很容易地恢复出秘密 s；

(2) 少于 t 个片断，不能得到 s 的任何信息。

Shamir 秘密分享协议也称为(t, n) 秘密分享协议，具有信息理论意义上的安全性。

基于拉格朗日插值公式，Shamir 的秘密分享协议包括两个算法：秘密分割算法和秘密恢复算法[1]。

假设有 n 个用户 U_1，…，U_n 和一个可信任的执行机构 D，则

秘密分割算法：D 任选一个多项式 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$，其中常数项等于秘密 s，即 $s=a_0=f(0)$，所有的系数 a_0，a_1，…，a_{t-1} 属于有限域 F_p，其中 p 是安全素数。D 计算所有的秘密片断 $s_i=f(i)(i=1, \cdots, n)$，并将 s_i 安全分发给 U_i。

秘密恢复算法：通过任意的$\{i_1, \cdots, i_t\} \subseteq \{1, 2, \cdots, n\}$，可恢复出多项式 $f(x)$，将 $x=0$ 代入 $f(x)$，可得 $s = f(0) = \sum_{i \in A} s_i \left(\prod_{j \in A-\{i\}} \frac{x_j}{x_j - x_i} \right)$。

2.3 Pedersen 承诺

Pedersen 承诺在信息安全协议中有广泛的应用，可同时实现数据的发布性与数据的隐私性，即在保持一个数值秘密的情况下，将数据发送给他人。结合下例阐述承诺协议。

假设 Alice 和 Bob 用抛币的方式来解决一个争端，如果他们在同一个位置用面对面的方式，那么过程就很简单：

(1) Alice 先押结果，即正面或反面；

(2) Bob 抛硬币；

(3) 如果与之前 Alice 所押的相同，则 Alice 获胜，否则 Bob 获胜。

如果 Alice 和 Bob 不在同一个位置，则上述方法就不再适用。需要在上述过程中加入承诺步骤，以保证协议的公平性。过程如下：

(1) Alice 先押结果，并将该结果做承诺(密封)发给 Bob；

(2) Bob 抛币并公布结果；

(3) Alice 打开承诺，即将之前的密封打开；

(4) 如果 Alice 打开的承诺与 Bob 公布的一致，则 Alice 胜。

Pedersen 承诺分为两个阶段：

(1) Alice 将一个数 s 承诺后发送给 Bob，除了 Alice，其他人