电力智能单元传输规约安全性分析模型研究

马媛媛[1] 陈 喆[2] 汪 晨[1] 费稼轩[1] 黄秀丽[1]
(全球能源互联网研究院信息通信研究所 南京 210003)[1] (国家电网公司信息通信部运行处 北京 100031)[2]

摘 要 电力智能单元传输规约的安全性是保障智能电网中智能通信实现高速、可靠、安全的基础。为了构建适用于电力智能单元传输规约的安全性分析模型,概述了主流的协议安全性分析理论与方法。基于符号模型的形式化方法包括逻辑推理、模型检验、定理证明;基于计算模型的计算方法包括 RO 模型、BCP 模型、CK 模型以及 UC 模型;基于计算可靠性理论的方法包括映射方法、模型方法、形式化方法的计算可靠性以及计算方法的直接形式化。提出了面向智能电网领域的电力智能单元传输规约安全性分析模型,为进一步的电力智能化单元传输规约的安全性分析奠定了基础。

关键词 协议安全性分析,符号模型,计算模型,计算可靠的形式化方法,电力智能单元传输规约
中图法分类号 TP309,TM769 **文献标识码** A

Security Analysis Model of Power Intelligent Unit Transmission Protocols

MA Yuan-yuan[1] CHEN Zhe[2] WANG Chen[1] FEI Jia-xuan[1] HUANG Xiu-li[1]
(Institute of Information and Communication, Global Energy Interconnection Research Institute, Nanjing 210003, China)[1]
(Information and Communication, Start Grid Corporation of China, Beijing 100031, China)[2]

Abstract Security of communication protocols for power intelligent units is the basis of achieving high speed, reliability and security intelligent communication of smart gird. The mainstream security analysis theories and methods of protocol were reviewed for the sake of constructing security analysis model for power intelligent unit transmission protocols. The formal methods based on the symbolic theory include logic reasoning, model checking and theorem proving. The computational methods based on the theory of computational complexity include RO, BCP, CK and UC model. The methods based on the computational soundness theory include mapping based methods, model based methods, computational sound formal methods and formalization of computational methods. A security analysis model for power intelligent units transmission protocols facing the field of smart grid was proposed, which lays a foundation for the security analysis of protocols of intelligent power units.

Keywords Security analysis of protocol, Symbolic model, Computational model, Computational sound formal method, Intelligent unit transmission protocol

1 引言

智能电网已成为世界电网发展的共同趋势。其核心理念是在建立集成、高速、双向通信网络的基础上,利用先进信息通信和控制技术,提升电网智能化水平,适应可再生能源的接入、双向互动等多元化电网服务的要求,实现电网的可靠、安全、经济、高效和环境友好等目标。与传统电网相比,智能电网信息安全具有点多、面广、技术复杂等特点,信息安全风险隐患更为突出。此外,随着电网网络逐步开放、互连和共享,其遭受网络入侵的风险日益加剧。

智能化单元作为电网及其控制系统的关键组成部分,肩负着电网业务数据的采集处理、控制指令的收发与执行等重要职责。而智能单元传输规约则是智能化单元之间乃至整个电网系统之间沟通的关键纽带,基于规约,智能单元在互联网上实现消息的源与目标认证、身份认证、消息完整性、会话密钥分发、匿名通信等功能。然而,迄今为止这些规约还很少加入任何信息安全防护措施,一方面对规约机密性、完整性、可用性和可追溯性等方面分析不足;另一方面对误操作、数据篡改、通信设备故障、设备功能失效等安全威胁防护缺失。

智能单元传输规约的安全问题主要来源于自身缺陷及外在攻击。自身缺陷可分为两类:一类是设计缺陷,由设计时的不规范引发,如口令猜测缺陷、陈旧消息缺陷、并行会话缺陷等;一类是实现缺陷,在具体实现或执行过程中产生,如内存腐败、互操作性问题等。此外,外在攻击者可以阅读、修改和删除通信信息,甚至可以控制协议通信的双方。外在攻击分为被动攻击和主动攻击,被动攻击者可在线窃听并获取敏感信息,而主动攻击者可截获数据包并对其进行任意修改,甚至还可以伪装成合法主体欺骗诚实主体与其进行通信。

本文受国家电网公司项目:电网智能化单元传输规约安全分析及增强技术研究资助。
马媛媛(1978—),女,高级工程师,主要研究领域为信息安全;陈 喆(1984—),男,工程师,主要研究领域为信息通信系统安全运行管理;汪 晨(1982—),男,工程师,主要研究领域为电力信息安全;费稼轩(1984—),男,工程师,主要研究领域为电力信息安全;黄秀丽(1979—),女,工程师,主要研究领域为电力信息安全。

智能电网的实现是建立在高速、集成、实时、双向通信网络的基础之上的。智能通信网络安全性的实现依赖于其中负责通信的协议的安全性，即电力智能单元传输规约。电力智能单元传输规约的安全性是保障智能电网中智能通信实现高速、可靠、安全的基础。如果智能传输规约存在安全缺陷被攻击者利用，就会造成重大损失。因此，电力智能单元传输规约的安全性分析显得至关重要。

为了构建适用于电力智能单元传输规约的安全分析模型，进而分析和增强电力智能单元传输规约的安全性，本文概述了主流的协议安全性分析理论与方法：基于符号模型的形式化方法，包括逻辑推理、模型检验、定理证明；基于计算模型的计算方法，包括 RO 模型、BCP 模型、CK 模型以及 UC 模型；基于计算可靠性理论的方法：包括映射方法、模型方法、形式化方法的计算可靠性以及计算方法的直接形式化。在此基础上，提出了面向智能电网领域的电力智能单元传输规约安全性分析模型，为进一步的电力智能化单元传输规约的安全性分析与增强奠定了基础。

2 背景知识

2.1 智能电力自动化系统

智能电力系统是由各种设施、设备组成的电能生产和消费系统，它通过发电将自然界的能源转换为电能，经过输电和配电将电能供应给用户。整个过程包括发电、输电、变电、配电和用电。发电是指将其他形式的能量转换成电能；输电是指将电能从发电厂传输到使用电能的地区；配电是指将电能逐步传送到使用电能的用户；用电是指用户将电能转换为其他形式的能量；变电是为了便于电能的传输与使用，进行电压等级的变换。下面详细介绍变电和配电自动化系统。

2.1.1 标准变电站系统

标准变电自动化系统框架图 1 所示，系统分为 3 层：过程层、间隔层、站控层。

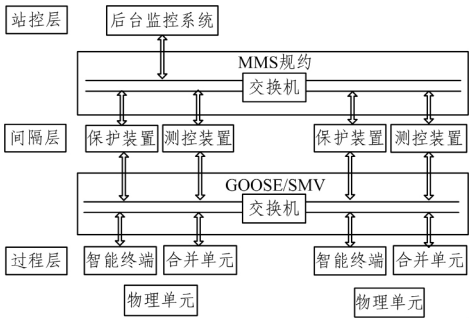

图 1 标准变电站系统框架

过程层包含由一次设备和智能组件构成的智能设备、合并单元和智能终端，其完成变电站电能分配、变换、传输及其测量、控制、保护、计量、状态监测等相关功能。间隔层设备一般指继电保护装置、测控装置、故障录波等二次设备，实现使用一个间隔的数据并且作用于该间隔一次设备的功能，即与各种远方输入/输出、智能传感器和控制器通信。站控层包含自动化系统、站域控制系统、通信系统、对时系统等子系统，实现面向全站或一个以上设备的测量和控制功能，完成数据采集和监视控制、操作闭锁以及同步相量采集、电能量采集、保护信息管理等相关功能。

2.1.2 配电自动化系统

配电自动化系统的组成如图 2 所示，包括主站系统、区域主站、配电子站、远方终端、通信网络等部分。

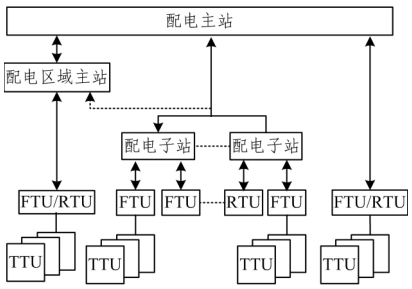

图 2 配电自动化系统框架

远方终端包括 FTU、TTU 和 RTU 等。FTU(Feeder Terminal Unit)馈线开关监控终端是装设在 10KV 断路器、负荷开关上的开关监控装置。主要作用是采集各开关所在线路的电气参数，并将这些信息向上级系统传输；监视线路的运行状况，当线路故障时及时上报，等待上级系统发来的指令进行开关开合控制，执行主站遥控命令。

TTU(Transformer Terminal Unit)是装设在配电变压器、箱变等变压器设备旁，监测变压器运行状况的终端装置。TTU 的主要作用是采集并处理配电变压器低压侧的各种电量等参数，并将这些参数向上级传输，监视变压器的运行状况，当变压器发生故障时及时上报，还可对电容器组增加本地和远程集中无功自动补偿及其他控制功能。

RTU(Remote Terminal Unit)是自动化系统的基本单元，它主要用于配电系统变压器、断路器、重合器、分段器、柱上负荷开关、环网柜、调压器和无功补偿电容器的监视及控制，与主站系统通信，提供配电系统运行及管理所需的数据，执行主站系统对远方设备发出的控制调节指令。

2.2 智能单元传输规约

智能单元传输规约是指适用于智能电力自动化系统中智能单元间的通信协议。协议[1]是指两个或两个以上的参与者采取一系列步骤以完成某项特定的任务。这个定义包含 3 层意思：1)协议至少需要两个参与实体，一个实体可以通过执行一系列的步骤来完成一项任务，但它不构成协议；2)在参与实体之间呈现为消息处理和消息交换、交替进行的一系列步骤；3)通过执行协议必须能够完成某项任务或者达成某种共识。

随着电力系统自动化技术的迅速发展和实施复杂度的不断提高，新一代面向对象的电力自动化系统标准被陆续制定，如针对变电站系统自动化的 IEC61850[83]、针对能量管理系统的 IEC61970[85] 和针对资产管理的 IEC61968[86] 等；而 IEC62351[84] 是 TC57 小组为电力系统安全运行针对有关通信协议(IEC60870-5，IEC60870-6，IEC61850，IEC61970，IEC61968 系列和 DNP3)而开发的数据和通信安全标准，以保障信息传输与交换的安全性。

典型的，如 IEC61850《变电站通信网络和系统》标准已于 2005 年 5 月全部出版完毕，目的是要实现不同厂商产品之间的互操作性；IEC60870 着重于远动设备及系统的通信传输。其内容包括：传输帧格式、传输链路规则、应用数据的一般结构、应用信息元素定义、编码和基本应用功能，可以适应电力自动化系统中各种网络配置和各种传输模式的需要；IEC61968 系列标准是为了促进支持配网管理的分布式应用软件之间的集成，提供把现有系统(包括已有系统和符合这些标准的新建系统)接口到 DMS 的一个集成框架。

2.3 智能单元传输规约的安全

通常说一个协议或者规约是安全的，指的是它对于某些性质（如机密性、认证性、完整性、不可否认性等）是满足的，对于某些特定的攻击（如窃听攻击、中间人攻击、平行会话攻击等）是可抵御的。协议的安全问题主要可分为自身的安全缺陷和外在的安全攻击。

2.3.1 自身安全缺陷

由于对协议运行环境估计不足，导致协议设计者所设计的协议存在安全漏洞进而引发攻击者对协议实施各类攻击。协议自身的缺陷分为两类：设计缺陷和实施缺陷。

文献[3]基于协议缺陷产生的原因和相应的攻击将协议安全缺陷分为 6 类，包括基本协议缺陷、口令/密钥猜测缺陷、陈旧消息缺陷、并行会话缺陷、内部协议缺陷、密码系统缺陷。

2.3.2 外在安全攻击

外在安全攻击可分为被动攻击与主动攻击。被动攻击是指攻击者不对连接中的消息进行处理，只通过窃听、流量分析等方式攻击。被动攻击难以检测，但可以防范，通过被动攻击，攻击者可以获取通信数据，造成信息外泄甚至危及敏感数据安全。

普遍被动攻击是 sniffer 攻击。sniffer 是指能解读、监视、拦截网络数据交换并且阅读数据包的程序或设备。主动攻击指攻击者对某个连接中的消息进行各种攻击，如更改、删除、延迟、复制、伪造等。典型的主动攻击方式包括阻断攻击、篡改攻击、伪造攻击、重放攻击、拒绝服务攻击等。

重放攻击是指攻击者通过窃听等方式将获得的数据包再次发给接收方，导致接收方的信息系统异常。中间人攻击是指通过第三方进行网络攻击，以达到欺骗被攻击系统、反跟踪、保护攻击者或者组织大规模攻击的目的；平行会话攻击是指在攻击者的安排下，不同轮次的协议并发运行，攻击者依靠并发运行，从一个运行中得到对另外某个运行的攻击能力；拒绝服务攻击的目的是使计算机或网络无法提供正常的服务。

2.3.3 电力领域特征安全问题

智能单元传输规约不仅面临上述安全威胁。交互的实时性和可用性等相关电力领域特征也为智能单元传输规约带来了新的安全挑战。

例如，四遥（遥测、遥信、遥控、遥调）数据是对于实时性和安全性要求较高的关键数据，但基本上没有采取加密措施。目前为了保证其安全性，通常采用网络隔离或虚拟专网（VPN）的方式。

随着智能电网的建设和发展，基于 TCP/IP 的网络通信方式将成为今后主要的电力系统通信方式。由于基于 TCP/IP 的网络本身并没有考虑安全问题，即使与 Internet 隔离，也并不能防范来自内部的攻击，电力系统数据通信安全的威胁仍然存在。

在 TCP/IP 网络通信方式下，如果电力系统的一些关键数据仍以明文的方式进行传输，将是电力系统安全稳定运行的一个重大安全隐患。任何入侵数据通信的网络者一旦对关键数据进行截获、篡改、伪造，将会造成开关误动、拒动，上传数据紊乱和整定参数的错误等，从而引发重大事故。

3 协议安全性分析理论与方法

主流的协议安全性分析理论与方法如图 3 所示，包括基于符号理论的方法、基于计算理论的方法，以及基于融合理论的方法，即基于计算可靠性理论的方法。图 4 展示了协议安全性分析 1978 年－2010 年近 30 年的发展研究脉络。

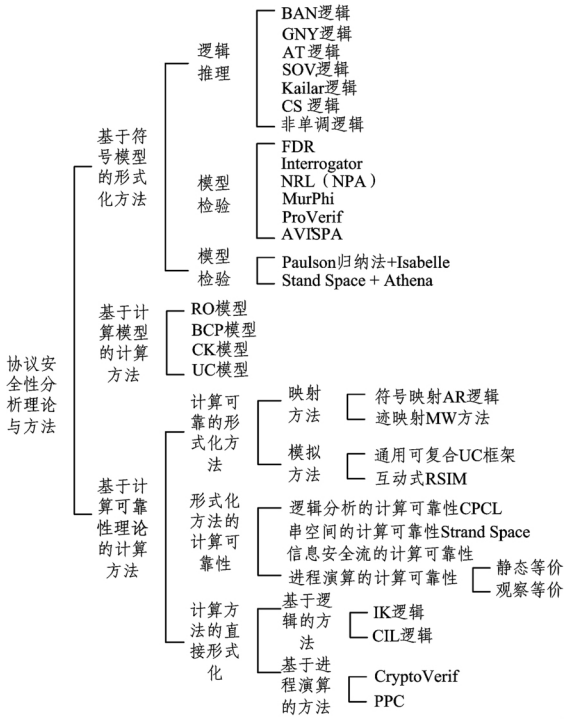

图 3 协议安全性分析理论与方法

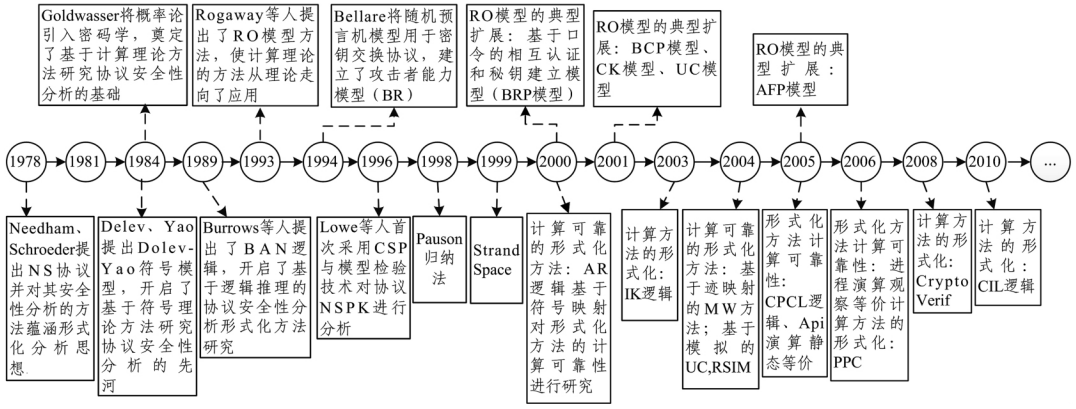

图 4 1978 年－2010 年协议安全性分析

3.1 基于符号模型的形式化方法

1978 年文献[6]对 Needham-Schroeder 协议进行了简要的安全性分析，对敌手的能力进行了一定的抽象与假设，蕴含了初步的形式化分析思想。

文献[7]明确提出安全协议的形式化分析方法，说明了协议形式化分析需要遵循的原则和对敌手能力的刻画，称为符号化模型或 Delev-Yao 模型。Dolev-Yao 模型主要包括对密码系统和敌手能力的假设：1）假设密码系统是完善的，单向函数的单向性是不可破解的；公共目录是安全的，不会被破坏；公钥是公开的，人人可得；私钥是私有的，拥有者才知道。2）敌手可发起主动攻击，即敌手可获取通过网络传播的任何消息；可作为合法用户发起会话；可截断通讯、篡改或转发任何消息。

Dolev-Yao 模型开启了密码协议形式化分析的先河，并为随后出现的协议形式化分析奠定了基础。但就自身而言，形式化分析技术具有局限性。因为协议系统不是孤立运行的，是处在某种环境之中，所以协议的形式化建模是基于对相关环境的某些假设前提下的，即只有假设成立时，证明才成立，一旦某个假设不成立，证明也就没有意义。实际中，攻击者只要违反了对系统或其环境的假设，就可成功攻击系统。另外值得一提的是，完整、明确地给出系统及其环境的假设说明是不实际的。同时，安全性是由数据完整性、机密性、消息认证和可追究性等诸多安全特性平衡组成，不同用户对不同安全属性的侧重不同，不同安全属性之间有些也不是独立的，而是相互影响，甚至是冲突的，即满足了一个特性，另一个特性就无法满足。比如电子商务协议的匿名性和可追究性就是发生冲突的两个特性。再比如，智能电力系统中对实时性和数据保密性都有要求，目前为了保证实时性，是以牺牲机密性为代价，不采取加密措施而通过 VPN 方式保护。

没有一个系统是百分之百安全的，也不可能对某一个系统的安全性给出百分之百的证明。尽管如此，协议的形式化安全分析至少可完成以下工作：界定协议安全性分析的边界，即协议系统与其所处环境的界限；更准确地描述协议的行为；更准确地定义协议的安全特性；证明协议满足其性质以及证明协议在什么条件下不能满足其相关安全特性。

基于符号模型的协议安全性方法大致可归纳为以下 4 个阶段：

（1）经验分析阶段。这一阶段的研究主要集中于对具体协议的观测、分析。

（2）逻辑推理阶段。以 Dolev-Yao 的工作为标志，BAN 类逻辑及其扩展等基于知识逻辑的有效应用，标志着研究进入了以逻辑推理方法为主体的时期。

（3）模型检测阶段。以 G. Lowe 发表其著名的论文《关于 Needham-Schroeder 公钥协议的一个攻击》为标志，各种一般用途的模型检测方法被用于协议安全性分析的研究。

（4）理论证明阶段。以 Strand space 理论及 Paulson 的归纳方法为代表，标志着进入以定理证明技术研究协议的安全性分析的发展时期。

3.1.1 逻辑推理方法

BAN[8] 逻辑是 1989 年提出的一种关于主体信仰，以及用于从已有信仰推知新的信仰的推理逻辑。该逻辑通过对认证协议的形式化分析，研究认证双方通过相互发送和接收消息，能否从最初的信仰得到协议运行最终要达到的信仰。如果在协议执行结束时，未能建立起关于诸如共享通信密钥、对方身份等信仰信息，则说明协议有安全缺陷。

BAN 逻辑成功地对 Needham-Schroeder 协议、Kerberos 协议等几个著名的协议进行了分析并发现了一些缺陷，成为密码协议形式化分析的一个里程碑[9]。然而，逻辑推理的方法抽象性较高，抽象过程会掩盖或丢失协议执行的部分状态信息，难以反映协议运行的全貌。BAN 逻辑在理想化步骤等方面存在着不足，研究人员为提高 BAN 逻辑的有效性，进行了各种不同尝试，表现为以下方面：

（1）对 BAN 逻辑自身进行扩充产生了 BAN 类逻辑，如 GNY 逻辑[10]、AT 逻辑[11]、SOV 逻辑[12]等；

（2）为具体的协议设计特定的形式化分析工具，如分析电子商务协议的 Kailar 逻辑[13]和分析与时间相关的协议的 CS 逻辑[14]等；

（3）为突破 BAN 及其类逻辑对协议主体的假设的局限性而提出 KG 逻辑[15]，以及为突破主体信仰知识的单调性而提出 Nonmonotomic 逻辑[16]。

3.1.2 模型检验方法

1996 年，Lowe 应用进程代数 CSP 和模型检验工具 FDR 分析 NSPK 协议，发现了一个 17 年来未知的漏洞[17]。Roscoe 对 CSP 和 FDR 的组合做了进一步的研究，得出模型检验技术是分析协议安全性的一种有效方法[18]的结论，激发了学者应用模型检验技术进行协议安全性分析的热情。

后续，基于模型检验方法的协议安全性分析工具相继开发。典型的有 Murϕ[19]，Maude[20]，SATMC（SAT-based Model-Checker）[21]，CL-AtSe[22]，OFMC（On-the-Fly Model-Chekcer）[23]，ProVerif[24]等。同时使用进程代数方法研究通信并发系统的理论还有 π 演算[37]，在此基础上通过引入加、解密原语将 π 演算拓展成为了协议的安全性建模分析的 Spi 演算理论[38]。

Millen 开发了通用认证协议语言 CAPSL，该语言可作为任何形式化分析工具的输入语言，如 FDR[30]，NPA[29]，Athena[27]等。生成协议系统的 CSP 描述是十分费时的，只能被熟练掌握 CSP 的人使用。协议的安全性分析编译器 Casper[31]的出现简化了这一过程。AVISPA[28]提供了一个类似于 CAPSL 的网络协议描述语言 HLPSL（High-level Protocol Specification Language），该语言基于重写转化为中间语言，可以支持 4 种模型检验工具。

3.1.3 定理证明方法

基于逻辑推理的方法不能解决秘密性，缺乏清晰的语义，难以明确指出信仰逻辑在证明什么。模型检验的方法面临状态空间爆炸问题。为此，以 Pauson 归纳证明法[25]、串空间（Strand Space）[26]为标志的定理证明技术相继提出，定理证明的方法可以通过定理证明器协助完成证明过程。

Paulson 归纳法将协议的行为表示为所有可能的迹的集合，而迹是一连串的协议通信事件。Paulson 协议模型中包含攻击者及消息丢失等情况，因此在协议执行过程中，主体并不知道消息真正的发送者，并且可能会转发一些其并不知道内容的消息。对于攻击者来说，当其获取一些私钥时，可以对消息进行加解密、伪造等。因此，攻击者可以是主动攻击者。Paulson 归纳法利用定理 Isabelle[36]证明器，通过归纳的方法来证明协议的安全属性。

Strand Space 是将协议运行的各个状态和整体的过程转

化为集合和有向图的形式进行描述，利用协议运行的特性定义集合中各个状态间的偏序关系，通过对集合中最小元的定义和证明来判断是否存在攻击节点。Strand Space 的设计具有许多优点，包括对某些数据项的属性给出了明确的语义；允许精确陈述和验证各种正确概念；可以用图示方法辅助分析证明，使之简洁直观等。Strand Space 模型中的证明要依据详细的协议行为，因此相比基于信仰逻辑类证明更具有可信性。利用 Strand Space 模型，Song 发展了一种自动检测工具 Athena[27]。此外还有 Attacks 限定法[32]、Schneider Rank Function 方法[33]、Rewritting 逼近法[34]、Invariant 方法[35]、human-readable 证明法[39]。

3.2 基于计算模型的计算方法

在基于符号模型的形式化方法发展的同一阶段，基于计算复杂性理论的安全证明方法也悄然兴起，简称基于计算模型的计算方法。该方法采用估算攻击者攻击协议的成功率以及计算代价来定义协议的安全性。它的基础是计算模型，其中消息用比特串表示，协议和攻击者被看作是随机的概率多项式时间图灵机。其基本思想是一种归约方法，即将一个复杂协议的安全性有效地归约到某一个或某几个困难问题上（如大数分解或者在椭圆曲线上求离散对数），如果协议被攻破了，那么可以推断攻击者必然是解决了相应的困难问题，但困难问题在当前的计算能力下是不可能求解的，所以协议是安全的。

Goldwasser 和 Micali 于 1984 年首次将概率论引入了密码学，奠定了可证明安全方法的理论基础[40]。1993 年，Bellare 和 Rogaway 提出了著名的随机预言（Random Oracle，RO）模型方法论[41]，最早采用可证明安全方法研究协议的安全性分析。在 RO 模型中，Hash 函数被形式化为一个预言机，生成随机值，用于协议的安全性分析的安全性归约。RO 模型的提出使可证明安全性理论由纯理论走向了实际应用。1994 年，Bellare 与 Rogaway 将随机预言机模型这种思想用于密钥交换协议，建立了攻击者能力模型（BR）[42]，并且证明了两方的实体认证和密钥交换协议。此后，很多学者不断地对 BR 模型进行拓展，出现了一系列的研究成果。如 1995 年，Bellare 和 Rogaway 提出了密钥建立了（BR95）模型[43]；2000 年，Bellare，Pointcheval 和 Rogaway 提出了基于口令的相互认证和密钥建立模型（BPR 模型）[44]；2001 年，Bresson，Chevassut 和 Pointcheval 提出了群组认证的密钥交换安全模型（BCP 模型）[45]。Bellare，Canetti 和 Krawczyk 引入了模块化的思想，通过提供可重用的模块来构造新的可证明安全的协议[47]。2001 年，Canetti 和 Krawczyk 提出了 CK 模块化的协议分析与设计模型[48]。同年，Canetti 提出了通用可组合（Universally Compassable，UC）模型[49]。2005 年，Abdalla，Fouque 和 Pointcheval 提出了基于口令的认证的密钥交换模型（AFP 模型）[46]。上述模型中应用比较广泛的是 BCP 模型[45]、CK 模型[48]和 UC 模型[49]。

3.3 基于计算可靠性理论的方法

在符号模型的形式化观点下，消息采用形式化表达式来表达，密码操作是符号化表达式空间上的抽象函数，协议通过形式化表达式来建模，对协议安全性的证明建立在符号化推理的基础上，易于自动化。在计算模型的计算方法下，消息是一个比特串，密码操作是比特串上的具体算法，协议基于敌手成功攻击的概率及计算复杂性，对协议安全性的证明必须采用人工的方法完成，容易出错。

符号模型下的安全性分析相对简洁，且易于利用机器自动验证，但缺点是抽象化的方法潜在地牺牲了计算方面的可靠性。计算模型的安全验证更严格，但是缺点在于只能够证明一个协议是正确的，而对于错误的协议往往不像形式化方法那样能够指出漏洞之所在。同时，证明正确性时往往会产生人为的错误。

为了调和两种方法，Abadi 和 Rogway 首先对形式化方法的计算可靠性进行了研究，从而使该问题成为密码协议分析领域的一个研究热点。通俗而言，密码协议形式化分析的计算可靠性是指：如果一个密码协议在形式化模型下被证明是安全的，那么它在计算模型下也是安全的。其意义在于当对密码协议的形式化分析能够保证计算可靠性时，就可以避开用复杂的计算方法进行协议分析。为了保证密码协议形式化分析的计算可靠性，人们进行了各种探索。总体可以分为基于映射的方法、基于模拟的方法、形式化方法的计算可靠性、计算方法的直接形式化 4 类[5]。

3.3.1 映射方法

2000 年，Abadi 和 Rogaway 研究被动攻击模型下消息不可区分性的计算可靠性，提出了 AR 逻辑[50]，其主要思路是通过定义消息模型，在符号化消息之间建立等价关系，然后定义一种映射关系，将符号化消息映射为计算意义下的比特串消息，最后证明形式化意义下的等价关系蕴含计算意义下的等价关系。

AR 逻辑开创了协议安全分析计算可靠性的先河。但 AR 逻辑本身过于简单，AR 逻辑是可靠的，但并不是完备的；AR 逻辑排除了循环加密；AR 逻辑中的消息仅包含了对称加密但没有涉及密码学原语；只讨论了静态消息，而未考虑动态行为；只考虑了被动攻击而未考虑主动攻击。针对这些问题，人们进行了大量的研究，并从不同角度对 AR 逻辑进行了改进。

Micciancio 和 Warinschi 指出了 AR 逻辑的计算可靠性，但不具备完备性，简单来说，在 AR 逻辑中，虽然等价性蕴含不可区分性（可靠性），但是不可区分性并不蕴含等价性（完备性），同时给出了 AR 逻辑完备性的充分条件[51]，即加密方案满足无混淆（Confusion-free）条件。2003 年，Horvitz 在文献[52]中进一步给出了完备性的充要条件，即表达式的弱秘钥认证测试。除此之外，2005 年，Bana[53] 及 Adao[54] 等的工作表明，在更一般的弱加密系统下完备性同样成立；Herzog 提出了公钥加密算法条件下的可靠性定理[55,56]，提出当公钥加密算法满足自适应选择密文攻击下的不可区分性时，形式表达式的不可区分性具有计算可靠性；Abadi 等人在文献[57]中对 AR 逻辑进行扩展，采用一种简单的编程语言对系统进描述，在讨论计算可靠性时，首先用该语言对协议进行描述，然后，将相应的程序映射为一个消息序列，并用该消息序列表示程序的运行迹，最后通过将消息序列映射到计算模型下，证明了相应的计算可靠性。文献[57]虽然只考虑了被动敌手，但它用消息序列表示协议运行迹的思路，向处理主动敌手情况迈进了一步。

适应性攻击是指敌手在攻击中使用了适应性策略，即当前获得消息的能力依赖于以前所得到的消息。为解决由适应性攻击引发的问题，2005 年，Micciancio D 在文献[58]AR 逻辑中对形式化表达式附加非循环条件的基础上进一步附加了语法限制，即将消息中密钥的使用分为两个阶段：密钥分发阶段和密钥应用阶段。在密钥分发阶段，密钥可以作为一般消息使用，而在密钥应用阶段，密钥仅被用来加密其它消息。在这种执行模式下，敌手可通过与执行环境的交互适应性改变协议的执行流程。

消息映射仅涉及到静态消息，而未涉及到动态行为，因此仅适用于被动攻击。在主动攻击模型下，敌手对通信网络有完全控制能力。从敌手角度来看，协议的每个执行流程可以形成一条执行迹，其中包含了执行流程中所有协议主体的发送和接收行为，以及这些行为之间的时序关系。

2004 年，Micciancio D 和 Warinschi B 首次提出了基于迹映射的方法[59]，简称 MW 方法，此处的迹中不仅包含了静态的消息而且包含了动态的行为，因而适用于存在主动敌手时形式化加密的计算可靠性分析。基于迹映射的方法也可称为迹映射定理，即当加密算法满足 IND-CCA2 安全性时，每条计算迹都可映射为符号迹，且这种映射关系以压倒性概率成立。该定理表明，计算模型下任意敌手行为都能用符号模型下的敌手表示。此后，研究人员从不同角度对基于迹映射的方法进行了扩展。如 Cortier V 在文献[60]中对 MW 方法在数字签名方面进行了扩展。文献[61]将 MW 方法应用于通用可复合框架，建立了通用可复合的符号化安全性分析方法。文献[62,63]通过将映射引理应用于 Hash 函数，对 MW 方法进行了扩展等。

3.3.2 模拟方法

基于模拟的方法的基本思想是定义一个理想协议，假设有一个可信方完成所有的通信和计算，从而理想化地保障安全属性的实现。当证明某个属性安全时，对于任何一个攻击实用协议的行为，模拟出一个攻击理想协议的行为。

Canetti 提出了通用可复合框架 UC，2004 年 Backes M 提出了互动式模拟(Reactive Simulatability，RSIM)方案[64]。通用可复合框架提供了一种密码协议分析的通用方法，即一个协议在独立运行情况下能实现其规范可以被推广为不管周围网络中有什么样的活动，其规范照样可以被实现。互动式模拟方案采用互动式系统描述密码协议，系统的状态用数据库来记录。针对 DY 模型可构造一种理想系统，针对计算模型可构造实际系统，然后证明存在一个模拟子，使得理想系统可模拟实际系统，从而保证计算可靠性。

3.3.3 形式化方法的计算可靠性

基于映射和基于模拟的方法大多在提出的同时就考虑了其计算可靠性。为了保持计算可靠性，它们大多注重理论上的正确性，但离实用还有一定距离。众多研究者对协议的安全性形式化分析方法进行了扩展，并证明了其计算可靠性。包括逻辑推理、进程演算、串空间、安全信息流等。

逻辑推理：2005 年，Datta A 提出的 CPCL(Computation PCL)[65]就是一种建立在协议复合逻辑(Protocol Composition Logic，PCL)[66]上的计算可靠密码协议逻辑。

进程演算：1997 年，文献[67]在 Pi 演算[68]的基础上提出了一种专门用于协议的安全性分析的 Spi 演算，用进程对密码协议进行建模。进一步的，文献[69]在 Spi 演算的基础上进行扩充，提出了一种 Api 演算，与 Spi 相比，Api 中加入了等式理论，利用等式理论可非常灵活地对各种密码原语进行建模，这使得 Api 比 Spi 更加通用。在基于 Api 的方法中，通常会用静态等价或观察等价的方式来描述协议的安全属性。静态等价与观察等价的主要区别在于前者不允许系统和观察者之间的持续交互，后者允许[70-72]。

串空间：2001 年，文献[73]中 Guttman 等人对串空间的两种处理方法进行了关联，即当一个协议在抽象模型(串空间模型)下满足其安全目标时，那么在其所定义的随机模型(Stochastic Model)下，敌手成功攻击它的概率将低于一个合适的概率。文献[74]认为文献[73]中的模型不能称为计算模型，而只能称为概率模型。因为其安全定义只是采用了概率的描述，而并没有建立在计算复杂性的基础上。但不可否认文献[73]表明了串空间下的协议正确性蕴涵了其在概率模型下的正确性。另外，2003 年，Herzog 在文献[75]中用串空间方法分析了 Diffie-Hellman 密钥交换协议，同时给出了如何在计算模型下定义并证明形式化模型下的安全性。

安全信息流：安全信息的概念是由 Denning 提出的，主要用在程序安全性分析中。程序中信息流主要指信息从一个变量向另一个变量的流动。如果一个变量的安全级别高于另一个变量的安全级别，那么禁止由前一个变量到后一个变量的信息流，满足这一规定的信息流被称为安全信息流。在形式化方法中，安全信息流通常用于无干扰性刻画，即公开输出一定不能包含任何关于秘密输入的信息。如果将密码协议看作一段程序，将协议主体的输入看作程序的输入，将协议暴露给敌手的消息看作程序的公共输出。那么，如果能够证明不存在从秘密输入到公开输出的信息流，则可以证明该程序所代表的协议能够满足秘密消息的保密性。2001 年，Laud[76]首先对计算可靠的信息流方法进行了研究，对计算安全信息流进行了定义，与无干扰性不同，此处的安全信息流是建立在计算复杂性基础上的。

3.3.4 计算方法的直接形式化

在上述方法中，通常是先给出一种形式化模型，然后再给出一种计算模型，最后表明形式化模型下的安全性蕴涵计算模型下的安全性，从而达到计算可靠的目的。近年来出现了一种新的思路，即直接对计算方法进行形式化，换言之，它是直接从计算模型入手所构造的形式化模型。

目前这类方法主要是基于逻辑的方法和基于进程演算的方法。典型的基于逻辑的方法包括 2003 年的 IK 逻辑[77]、2010 年的 CIL 逻辑[78]；典型的基于进程演算的方法包括概率多项式时间演算(Probabilistic Polynomila time Calculus，PPC)[79,80]和基于时间序列的方法[81]，如 Blanche 等人于 2008 年采用进程演算描述实验，对实验序列化进行了形式化，开发了一种计算可靠的密码协议自动验证工具 CryptoVerif[82]。

4 电力智能单元传输规约安全性分析模型

在上述主流协议安全性分析模型与方法的基础上，结合电力传输规约特征以及电力相关人员背景，提出面向智能电

网领域的智能单元传输规约安全性分析模型，如图5所示。

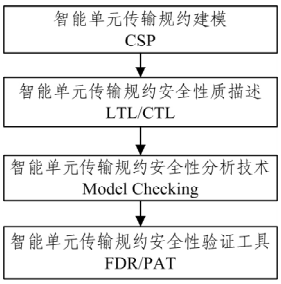

图5　电力智能单元传输规约安全性分析模型

CSP是智能单元传输规约的形式化建模语言，通信顺序进程(CSP)是著名计算机科学家C. A. R. Hoare为解决并发现象而提出的代数理论，用于网络安全协议的描述与分析。CSP具有良好的语义，可以较好地描述协议是否满足其安全属性这一问题，而且CSP对协议的描述极接近协议的本身含义，同时提供了强有力的数学理论支撑。此外，安全协议分析编译器(Complier for the Analysis of Security Protocols，Casper)的出现大大简化了生成协议系统的CSP描述工作，有利于电力工作人员的操作。

以时态逻辑公式LTL/CTL对智能电力传输规约要验证的安全属性进行刻画。线性时态逻辑(Linear Temporal Logic，LTL)和计算树逻辑(Computation Tree Logic，CTL)是应用最广泛的时态性质描述语言，可以对电力智能传输规约中要求的认证性、完整性、机密性、不可否认性等性质进行有效的刻画。

以模型检验作为智能单元传输规约的安全性分析技术。模型检验方法是针对有穷状态系统的一种自动验证方法。其基本过程是：1)将待验证的系统建模为标签迁移系统；2)系统待验证的性质用时序逻辑公式LTL/CTL刻画；3)检测刻画性质的时序逻辑公式在标记迁移系统的每一个可能的迁移路径上是否得到满足；4)自动构造标记迁移系统不满足时序逻辑公式所有可能的迁移路径。该方法相较于逻辑推理、定理证明等方法易于自动化，可以有效地找出协议存在的缺陷。

以主流的CSP模型检验工具FDR/PAT作为实施验证的工具支撑。FDR/PAT可以自动化地完成对CSP描述的协议性质验证：1)参与协议的每个主体CSP进程表示；2)最具通常意义的可与协议相互作用的攻击者也用CSP进程表示；3)检查这样的系统是否满足一些重要的安全性质，如认证性、秘密性，FDR或PAT搜索状态空间，以发现任何不安全路径是否存在；4)如果发现协议的性质是不满足，它将给出使性质不满足的路径，这条路径对应协议的一个攻击。

基于所提出的面向电力领域的智能电力传输规约分析模型，对典型的电力智能传输规约IEC61850进行了分析，实验结果表明了该模型的有效性，该方法便于电力相关人员利用该模型和方法对智能电力传输规约进行自动化的安全性分析，进而发现潜在的安全缺陷，从而提出增强措施。

结束语　电力智能单元传输规约的安全性是保障智能电网中智能通信实现高速、可靠、安全的基础。本文概述了主流的协议安全性分析理论与方法：基于符号模型的形式化方法，包括逻辑推理、模型检验、定理证明；基于计算模型的计算方法，包括RO模型、BCP模型、CK模型以及UC模型；基于计算可靠性理论的方法：包括映射方法、模型方法、形式化方法的计算可靠性以及计算方法的直接形式化。在此基础上，提出了面向智能电网领域的电力智能单元传输规约安全性分析模型，为进一步的电力智能化单元传输规约的安全性分析和增强奠定了基础。

参 考 文 献

[1] 范红. 协议的安全性分析形式化分析理论与方法[D]. 郑州：中国人民解放军信息工程大学，2003

[2] Abadi M，Needham R. Prudent engineering practice for cryptographic protocols[J]. IEEE transactions on Software Engineering，1996，22(1)：6-15

[3] Gritzalis S，Spinellis D. Cryptographic protocols over open distributed systems：A taxonomy of flaws and related protocol analysis tools[M]// Safe Comp 97. Springer London，1997：123-137

[4] Syverson P. A taxonomy of replay attacks[cryptographic protocols][C]// Proceedings of Computer Security Foundations Workshop VII，1994. IEEE，1994：187-191

[5] 雷新锋，宋书民，刘伟兵，等. 计算可靠的密码协议形式化分析综述[J]. 计算机学报，2014(5)：993-1016

[6] Needham R M，Schroeder M D. Using encryption for authentication in large networks of computers[J]. Communications of the ACM，1978，21(12)：993-999

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

[8] Burrows M，Abadi M，Needham R M. A logic of authentication[C]// Proceedings of the Twelfth ACM Symposium on Operating System Principles. 1989：1-13

[9] Grädel E. Why are modal logics so robustly decidable？[C]// Bulletin EATCS. 1999：90-103

[10] Gong L，Needham R，Yahalom R. Reasoning about belief in cryptographic protocols[C]// 1990 IEEE Computer Society Symposium on Research in Security and Privacy，1990. 1990：234-248

[11] Abadi M，Tuttle M R. A semantics for a logic of authentication[C]// Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing. ACM，1991：201-216

[12] Syverson P F，Van Oorschot P C. A unified cryptographic protocol logic[R]. Naval Research Lab Washington DC，1996

[13] Kailar R. Reasoning about accountability in protocols for electronic commerce[C]// Proceedings of Security and Privacy. IEEE，1995：236-250

[14] Coffey T，Saidha P. Logic for verifying public-key cryptographic protocols[J]. IEE Proceedings－Computers and Digital Techniques，IET，1997，144(1)：28-32

[15] Kailar R，Gligor V D. On belief evolution in authentication protocols[C]// Proceedings of Computer Security Foundations Workshop IV，1991. IEEE，1991：103-116

[16] Rubin A D，Honeyman P. Nonmonotonic cryptographic protocols[C]// Proceedings of Computer Security Foundations Workshop VII，1994. IEEE，1994：100-116

[17] Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR[M]// Tools and Algorithms for the Con-

struction and Analysis of Systems. Springer Berlin Heidelberg, 1996:147-166

[18] Roscoe A W. Proving security protocols with model checkers by data independence techniques[C]// 11th IEEE Computer Security Foundations Workshop, 1998. IEEE, 1998:84-95

[19] Mitchell J C, Mitchell M, Stern U. Automated analysis of cryptographic protocols using Murφ[C]// 1997 IEEE Symposium on Security and Privacy, 1997. IEEE, 1997:141-151

[20] Denker G, Meseguer J, Talcott C. Protocol specification and analysis in Maude[C]// Proc. of Workshop on Formal Methods and Security Protocols. 1998:25

[21] Armando A, Compagna L, Ganty P. SAT-based model-checking of security protocols using planning graph analysis[M]// FME 2003: Formal Methods. Springer Berlin Heidelberg, 2003: 875-893

[22] Chevalier Y, Vigneron L. A tool for lazy verification of security protocols[C]// 16th Annual International Conference on Automated Software Engineering (ASE 2001), 2011. IEEE, 2001: 373-376

[23] Basin D, Mödersheim S, Vigano L. An on-the-fly model-checker for security protocol analysis[M]. Springer Berlin Heidelberg, 2003

[24] Blanchet B, Abadi M, Fournet C. Automated verification of selected equivalences for security protocols[C]// 20th Annual IEEE Symposium on Logic in Computer Science, 2005. IEEE, 2005:331-340

[25] Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of Computer Security, 1998, 6(1/2): 85-128

[26] Guttman J D, Herzog J C, Fábrega F T. Strand spaces: proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2/3):191-230

[27] Song D X, Berezin S, Perrig A. Athena: a novel approach to efficient automatic security protocol analysis[J]. Journal of Computer Security, 2001, 9(1/2):47-74

[28] Armando A, Basin D, Boichut Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications[C]// Computer Aided Verification. Springer Berlin Heidelberg. 2005:281-285

[29] Meadows C. The NRL protocol analyzer: An overview[J]. The Journal of Logic Programming, 1996, 26(2):113-131

[30] Gibson-Robinson T, Armstrong P, Boulgakov A, et al. FDR3—A modern refinement checker for CSP[M]// Tools and Algorithms for the Construction and Analysis of Systems. Springer Berlin Heidelberg, 2014:187-201

[31] Lowe G. Casper: A compiler for the analysis of security protocols[C]// Proceedings of Computer Security Foundations Workshop, 1997. IEEE, 1997:18-30

[32] Stoller S D. A bound on attacks on payment protocols[C]// 16th Annual IEEE Symposium on Logic in Computer Science, 2001. IEEE, 2001:61-70

[33] Schneider S. Using CSP for protocol analysis: the Needham-Schroeder public-key protocol[M]. University of London, Royal Holloway, Department of Computer Science, 1996

[34] Boichut Y, Genet T, Jensen T, et al. Rewriting approximations for fast prototyping of static analyzers[M]// Term Rewriting and Applications. Springer Berlin Heidelberg, 2007:48-62

[35] Clarke E M, Grumberg O, Peled D. Model checking[M]. MIT Press, 1999

[36] Paulson L C. Isabelle: A generic theorem prover[M]. Springer Science & Business Media, 1994

[37] Sangiorgi D, Walker D. The pi-calculus: a Theory of Mobile Processes[M]. Cambridge University Press, 2003

[38] Abadi M, Gordon A D. A calculus for cryptographic protocols: The spi calculus[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. ACM, 1997:36-47

[39] Bolignano D. An approach to the formal verification of cryptographic protocols[C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security. ACM, 1996: 106-118

[40] Goldwasser S, Micali S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2):270-299

[41] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C]// Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993:62-73

[42] Bellare M, Rogaway P. Entity authentication and key distribution [M]// Advances in Cryptology—CRYPTO'93. Springer Berlin Heidelberg, 1994:232-249

[43] Bellare M, Rogaway P. Provably secure session key distribution: the three party case[C]// Proceedings of the twenty-seventh Annual ACM Symposium on Theory of Computing. ACM, 1995:57-66

[44] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks[M]// Advances in Cryptology—Eurocrypt 2000. Springer Berlin Heidelberg, 2000: 139-155

[45] Bresson E, Chevassut O, Pointcheval D. Provably authenticated group Diffie-Hellman key exchange—the dynamic case[M]// Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001:290-309

[46] Abdalla M, Fouque P A, Pointcheval D. Password-based authenticated key exchange in the three-party setting[M]// Public Key Cryptography-PKC 2005. Springer Berlin Heidelberg, 2005: 65-84

[47] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols [C]// Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing. ACM, 1998:419-428

[48] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[M]// Advances in Cryptology—EUROCRYPT 2001. Springer Berlin Heidelberg, 2001: 453-474

[49] Canetti R. Universally composable security: A new paradigm for cryptographic protocols[C]// 42nd IEEE Symposium on Foundations of Computer Science, 2001. IEEE, 2001:136-145

[50] Abadi M, Rogaway P. Reconciling two views of cryptography [C]// Proceedings of the IFIP International Conference on Theoretical Computer Science. 2000:3-22

[51] Micciancio D, Warinschi B. Completeness Theorems for the

Abadi-Rogaway Language of Encrypted Expressions[J]. Journal of Computer Security, 2004, 12(1): 99-129

[52] Horvitz O, Gligor V. Weak key authenticity and the computational completeness of formal encryption[M]// Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003: 530-547

[53] Bana G. Soundness and Completenss of Formal Logics of Symmetric[D]. University of Pennsylvania, 2005

[54] Adao P, Bana G, Scedrov A. Computational and information-theoretic soundness and completeness of formal encryption[C]// 18th IEEE Workshop Computer Security Foundations, 2005. IEEE, 2005: 170-184

[55] Herzog J. Computational soundness for standard assumptions of formal cryptography[D]. Massachusetts Institute of Technology, 2004

[56] Herzog J. A computational interpretation of Dolev-Yao adversaries[J]. Theoretical Computer Science, 2005, 340(1): 57-81

[57] Abadi M, Jürjens J. Formal eavesdropping and its computational interpretation[M]// Theoretical Aspects of Computer Software. Springer Berlin Heidelberg, 2001: 82-94

[58] Micciancio D, Panjwani S. Adaptive security of symbolic encryption[M]// Theory of Cryptography. Springer Berlin Heidelberg, 2005: 169-187

[59] Micciancio D, Warinschi B. Soundness of formal encryption in the presence of active adversaries[M]// Theory of Cryptography. Springer Berlin Heidelberg, 2004: 133-151

[60] Cortier V, Warinschi B. Computationally sound, automated proofs for security protocols[M]// Programming Languages and Systems. Springer Berlin Heidelberg, 2005: 157-171

[61] Canetti R, Herzog J. Universally composable symbolic security analysis[J]. Journal of Cryptology, 2011, 24(1): 83-147

[62] Cortier V, Kremer S, Küsters R, et al. Computationally sound symbolic secrecy in the presence of hash functions[M]// FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. Springer Berlin Heidelberg, 2006: 176-187

[63] Janvier R, Lakhnech Y, Mazaré L. Computational soundness of symbolic analysis for protocols using hash functions[J]. Electronic Notes in Theoretical Computer Science, 2007, 186: 121-139

[64] Backes M, Pfitzmann B, Waidner M. A general composition theorem for secure reactive systems[M]// Theory of Cryptography. Springer Berlin Heidelberg, 2004: 336-354

[65] Datta A, Derek A, Mitchell J C, et al. Probabilistic polynomial-time semantics for a protocol security logic[M]// Automata, Languages and Programming. Springer Berlin Heidelberg, 2005: 16-29

[66] Datta A, Derek A, Mitchell J C, et al. A derivation system for security protocols and its logical formalization[C]// 16th IEEE Computer Security Foundations Workshop, 2003. IEEE, 2003: 109-125

[67] Abadi M, Gordon A D. A calculus for cryptographic protocols: The spi calculus[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. ACM, 1997: 36-47

[68] Milner R, Parrow J, Walker D. A Calculus of Mobile Processes, I[J]. Information and Computation, 1992, 100(1): 1-40

[69] Abadi M, Fournet C. Mobile values, new names, and secure communication[J]. ACM SIGPLAN Notices, 2001, 36(3): 104-115

[70] Baudet M, Cortier V, Kremer S. Computationally sound implementations of equational theories against passive adversaries[M]// Automata, Languages and Programming. Springer Berlin Heidelberg, 2005: 652-663

[71] Adao P, Fournet C. Cryptographically sound implementations for communicating processes [M]// Automata, Languages and Programming. Springer Berlin Heidelberg, 2006: 83-94

[72] Comon-Lundh H, Cortier V. Computational soundness of observational equivalence[C]// Proceedings of the 15th ACM Conference on Computer and Communications Security. ACM, 2008: 109-118

[73] Guttman J D, Thayer F J, Zuck L D. The faithfulness of abstract protocol analysis: Message authentication[C]// Proceedings of the 8th ACM Conference on Computer and Communications Security. ACM, 2001: 186-195

[74] Laud P. Encryption cycles and two views of cryptography[C]// Proceedings of the 7th Nordic Workshop on Secure IT Systems (NORDSEC). 2002: 85-100

[75] Herzog J C. The Diffie-Hellman key-agreement scheme in the strand-space model[C]// 16th IEEE Computer Security Foundations Workshop, 2003. IEEE, 2003: 234-247

[76] Laud P. Semantics and program analysis of computationally secure information flow[M]// Programming Languages and Systems. Springer Berlin Heidelberg, 2001: 77-91

[77] Impagliazzo R, Kapron B M. Logics for reasoning about cryptographic constructions[C]// 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. IEEE, 2003: 372-383

[78] Barthe G, Daubignard M, Kapron B, et al. Computational indistinguishability logic[C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010: 375-386

[79] Lincoln P, Mitchell J, Mitchell M, et al. A probabilistic poly-time framework for protocol analysis[C]// Proceedings of the 5th ACM Conference on Computer and Communications Security. ACM, 1998: 112-121

[80] Mitchell J C, Ramanathan A, Scedrov A, et al. A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols[J]. Theoretical Computer Science, 2006, 353(1): 118-164

[81] Shoup V. Sequences of games: a tool for taming complexity in security proofs [J]. IACR Cryptology ePrint Archive, 2004, 2004: 332

[82] Blanchet B. A computationally sound mechanized prover for security protocols[J]. IEEE Transactions on Dependable and Secure Computing, 2008, 5(4): 193-207

[83] IEC 61850: Communication networks and system in substations, part 1 to part 10 [S]. 1999

[84] http://www.iec.ch/smartgrid/standards/

[85] **曹阳, 姚建国, 杨胜春, 等. 智能电网核心标准 IEC61970 最新进展[J]. 电力系统自动化**, 2011, 35(17): 1-4

[86] Mcmorran A W. An Introduction to IEC 61970-301 & 61968-11: The Common Information Model[D]. University of Strathclyde, 2007