



安全协议设计与分析

第八讲：安全协议的形式化分析

李晖 网络空间安全学院



本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

形式化方法概述



➤什么是形式化方法

- 在计算机科学和软件工程领域，形式化方法是基于[数学](#)的特种技术，适合于软件和硬件系统的描述、开发和验证。

➤发展过程

- 20世纪50年代**，语法分析程序自动生成器，用于编译系统的开发
- 20世纪60年代**，为解决“软件危机”，采用数学证明程序的正确性而发展成为各种程序验证方法
- 从早期最简单的形式化方法——一阶谓词演算方法到现在的应用于不同领域、不同阶段的基于逻辑、状态机、网络、[进程代数](#)、代数等众多形式化方法
- 20世纪70年代**，形式化分析方法已经逐渐被应用于对安全协议的分析

形式化方法概述



➤ 意义

- 帮助发现其他方法不容易发现的系统描述的不一致、不明确或不完整
- 有助于增加软件开发人员对系统的理解
- 是提高软件系统、特别是安全攸关系统的安全性与可靠性的重要手段。

➤ 步骤

➤ 建模

- 为要验证的系统建立一个数学模型，用精确可靠的方式将要验证的系统抽象为数学模型来表达，从而去掉不重要的细节，便于简单有效的推理

➤ 规约

- 利用建立的数学模型将系统所要求的性质规约表述，便于形式化推导和验证

➤ 验证

- 在建立的数学模型中推理说明系统的性质是否满足。

安全协议的形式化分析方法分类



➤ 基于符号模型（或称为Dolev-Yao模型）的方法

- 符号化协议中的各元素，借助于形式化方法。

- 密码算法被看作是**完美黑盒算法**

- 不考虑算法本身可能的攻击

- **网络被敌手完全控制**

➤ 基于计算模型（或称计算方法）的方法

- 基于随机比特串的概率分布

- 将攻击者模拟为能以多项式运行的图灵机

安全协议的形式化分析方法分类



➤ 基于符号模型（或称为Dolev-Yao模型）的方法

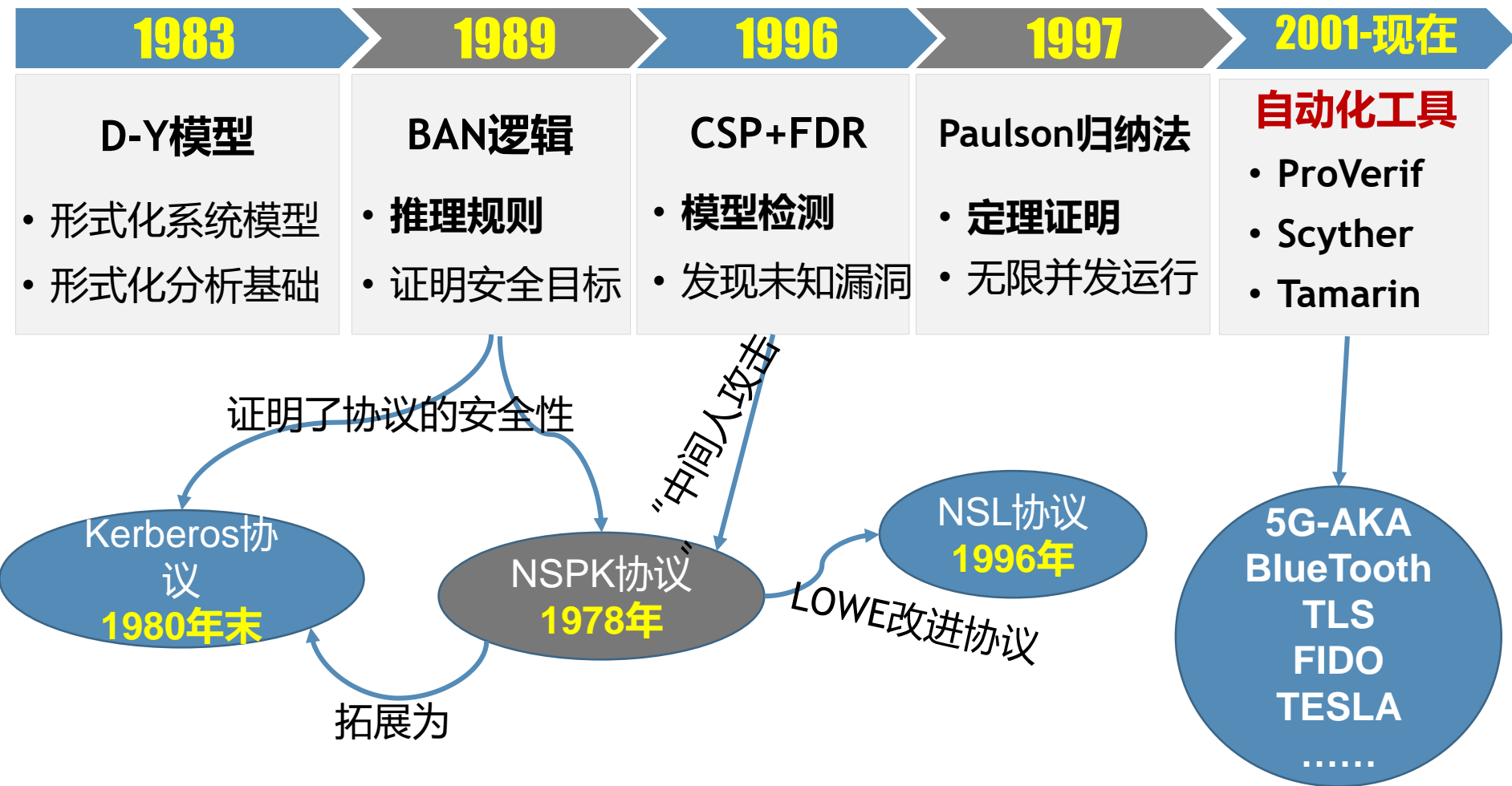
- 基于**逻辑推理**的形式化分析方法
- 基于**模型检测**的形式化分析方法
- 基于**定理证明**的形式化分析方法

➤ 基于计算模型（或称计算方法）的方法

- **密码学可证明**安全性分析方法

形式化分析方法

发展历程



本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

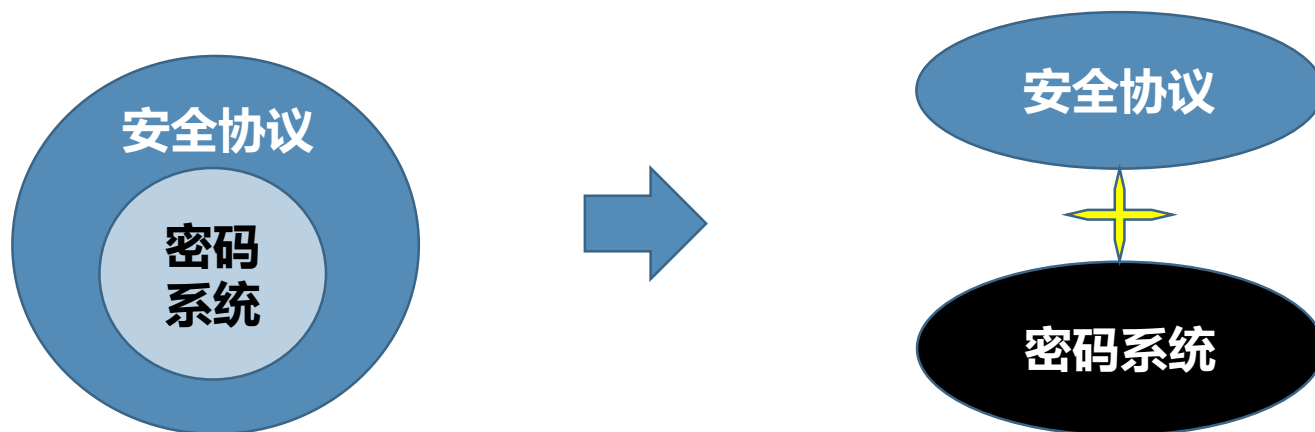
Dolev-Yao模型

➤ 由Dolev、Yao于1983年首次提出



Andrew Chi-Chih Yao

➤ 将**安全协议**本身与安全协议所采用的**密码系统**分开考虑，降低了安全协议分析问题的复杂度





➤ 密码系统模型

- 将密码系统看做是一个黑盒子，并假设采用的密码算法和密码技术是完善的；
- 主体仅在拥有了正确的解密密钥时才能进行解密，并且产生的密文必须拥有对应的明文和加密密钥。

➤ 攻击者模型

- 描述了攻击者的知识和能力



➤ 攻击者模型

- 1) 熟悉**现代密码学**，知道加解密等运算操作。
- 2) 知道**参与**协议运行的各**实体**及其**公钥**。
- 3) **拥有自己的加解密密钥**，可将窃听到的消息增加为自己的新知识。
- 4) **对网络具有完全的控制能力**，可窃听、拦截系统中传送的任何消息。
- 5) 可用他拥有的加密或解密密钥对消息进行加密或解密操作。
- 6) 可在系统中插入新的消息。
- 7) 即使不知道加密部分的内容，也可重放他所看到的任何消息。
- 8) 可以生成新的随机数等。



➤ Dolev-Yao模型的重要意义

- 1) 模型检测技术及定理证明技术均建立在此模型之上
- 2) 逻辑推理依赖于Dolev-Yao模型的黑盒假设

➤ Dolev-Yao模型的局限性

- 1) 过于理想化的假设：无法对密码系统相关缺陷进行分析
- 2) 仅仅关注协议本身的逻辑：忽略协议实现细节
- 3) 过度简化了攻击者的能力
 - 攻击者的能力可能远超过模型中所定义
 - 攻击者总能形成拒绝服务攻击（DOS）

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

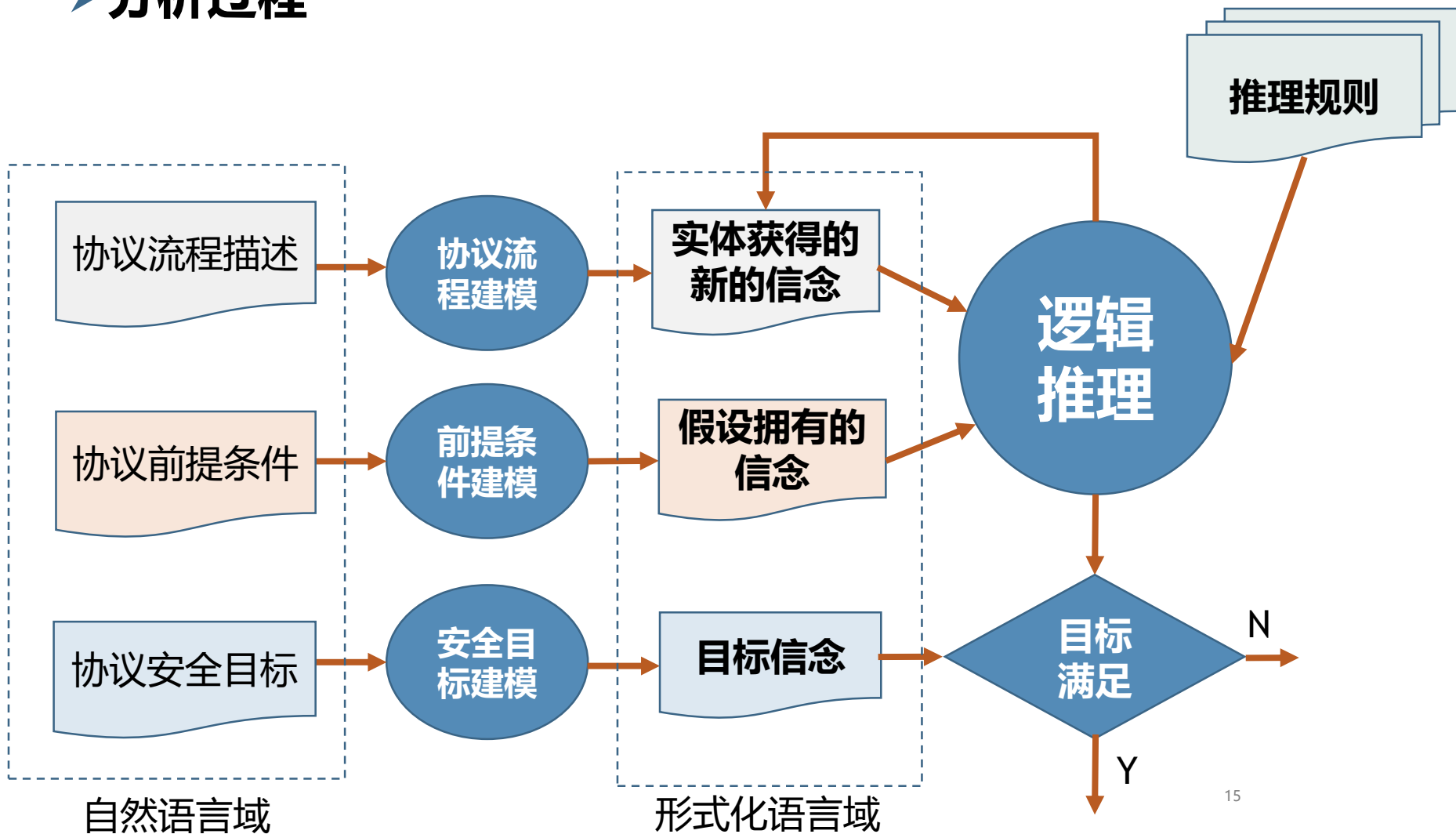
基于逻辑推理的分析方法



- 是分析安全协议的最为重要的方法之一
- 分析并验证了许多重要的安全协议
 - Needham-Schroeder 私钥协议
 - Lowe-Needham-Schroeder 公钥协议
 - Nessett 协议
- 原理
 - 利用知识和信念逻辑，描述和推理安全协议。
 - 用公式表示协议主体的信念或知识，用推理规则从原有公式得到新的信念公式
 - 通过判断新的信念中是否包含安全协议的目标来确认目标是否达到

基于逻辑推理的分析方法

➤ 分析过程



基于逻辑推理的分析方法



➤ BAN逻辑

- 最早的逻辑化分析方法
- 由Michael Burrows, Martín Abadi和Roger Needham
- 于1989年在A logic of Authentication中提出
- 依赖于Dolev-Yao模型的黑盒假设, 按照这些逻辑推导, 成功证明了多个协议满足身份认证的安全目标。其中包括NSPK协议。
- 是基于逻辑推理的密码协议形式化方法的首次尝试, 是开创性工作

➤ 其他方法

- GNY逻辑
- AT逻辑
- SVO逻辑



Martín Abadi



Roger Needham¹⁶
(1935-2003)

基于逻辑推理的分析方法



➤ 逻辑推理方法的优点

- 简洁易用
- 计算效率高
- 可判定
- 可自动化
- 侧重于安全问题的逻辑本质

➤ 逻辑推理方法的缺点

- 抽象层次太高
- 协议分析不彻底
- 存在规则不完善
- 语义不精确

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

基于模型检测的分析方法

➤ 模型检测 (Model Checking) 技术

- 是验证有限状态系统的自动化分析技术，也称为**自动验证技术**
- 主要通过显式状态搜索或隐式不动点计算来验证有穷状态并发系统的模态/命题性质。
- 由**Clarke**和**Emerson**以及**Quelle**和**Sifakis**提出，获2007年图灵奖



Edmund Clarke
1945-2020



Ernest A Emerson



Joseph Sifakis

基于模型检测的分析方法



➤ 模型检测的基本思想

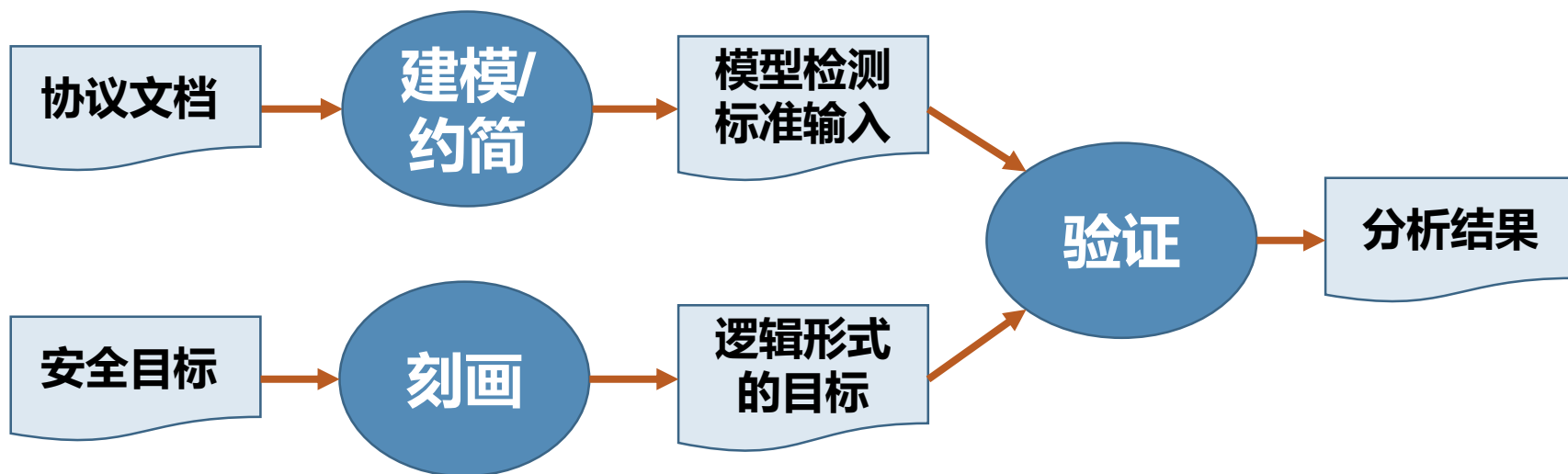
- 是用**状态迁移系统(S)**表示系统的**行为**
- 用**模态逻辑公式(F)**描述系统的**性质**。
- “系统是否具有所期望的性质” 被转化为数学问题 “**状态迁移系统S是否是公式F的一个模型**”，用公式表示为 $S \models F$ 。
- 对有穷状态系统，这个问题是可判定的，即可以用计算机程序在有限时间内自动确定。

基于模型检测的分析方法



➤ 模型检测的过程

- 1、**建模/约简**：把设计转化为被模型检测工具接受的形式；
- 2、**刻画**：声明设计必须满足的性质。
- 3、**验证**：自动验证+人工。分析结果。



基于模型检测的分析方法



➤ 基于模型检测的安全协议分析

- 利用有穷状态机理论，将安全协议建模为状态集合和状态迁移函数
- 通过穷举搜索状态空间来判断一些特殊状态是否可达，或者是否可以生成一条特殊的状态转移路径，以此检测该模型是否具备期望的安全属性
- 理论基础：**Dolev-Yao模型**、**进程代数**等理论

➤ 基于模型检测的安全协议分析的发展过程

- 1996年，**Lowe**首先采用CSP(通信顺序进程)方法和模型检测工具**FDR**发现了针对 NSPK 协议的著名的“中间人攻击”
- 1997 年 Lu 和 Smolka 也使用 **FDR** 验证了 SET 协议中的 5 个错误性质
- 使用**SPIN**验证了著名的无线应用协议中的传输层协议、滑动窗口（Go-Back-N）协议、路由器协议等网络协议。
- 美国航空航天局的软件研究实验室利用 **SPIN** 验证了一个应用于航天器系统的容错控制软件，搜索了其中的 105 个状态，发现了 3个潜在的缺陷。
- **AVISPA**，**ProVerif**和**Tamarin**等

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

基于定理证明的分析方法



➤ 原理

- 将安全协议描述为公理系统，安全协议的安全属性表示成需要证明的定理，将判断安全协议是否满足安全属性转化为，证明公理系统中的目标定理是否成立。

➤ 代表性方法

- 重写逼近法
- Schneider阶函数
- **Paulson归纳证明法（1997年）**
- 串空间模型（Fabrega、Herzog和Guttman提出的）

➤ 主要工具

- Isabelle、HOL、Paradox、ACL2、PVS、**Tamarin和ProVerif**

基于定理证明的分析方法



➤ 一般步骤

- (1) 用一组代数或者逻辑公式定义安全协议的行为，构成系统的**行为集**。
 - (2) 用一组公理和系统行为集作为推理证明的**基础公式集**。
 - (3) 将所期望的系统行为和性质描述为一组公式，称为**定理**
 - (4) 从**基础公式集**出发，进行**定理**证明过程，以达到所期望的结果
- 可以自动证明的系统被称为**定理证明器**
- 与模型检测系统不同，**定理证明器通常需要人的帮助**

基于定理证明的分析方法

➤ Paulson归纳证明法

- 1997年由Paulson提出，借助他1994提出的Isabelle证明器，可部分实现自动化证明
- 使用该方法分析了大量安全协议，包括Kerberos协议和SET协议

➤ 原理：

- 安全协议被归纳定义为事件的迹的集合。

➤ 实体能力

- 发送消息，利用自己的密钥加密和解密消息、生成签名及进行签名验证

➤ 攻击者能力

- 具有主动攻击能力，如伪造消息和破解新鲜性值，是通过推理规则描述的，但消息窃听是被间接描述的。
- 攻击者可以观察所有通信（用集合 H 表示），并发送从集合 $\text{synth}(\text{analz } H)$ 中衍生的欺骗消息。在模型中攻击者被视为参与协议运行的一个主体。

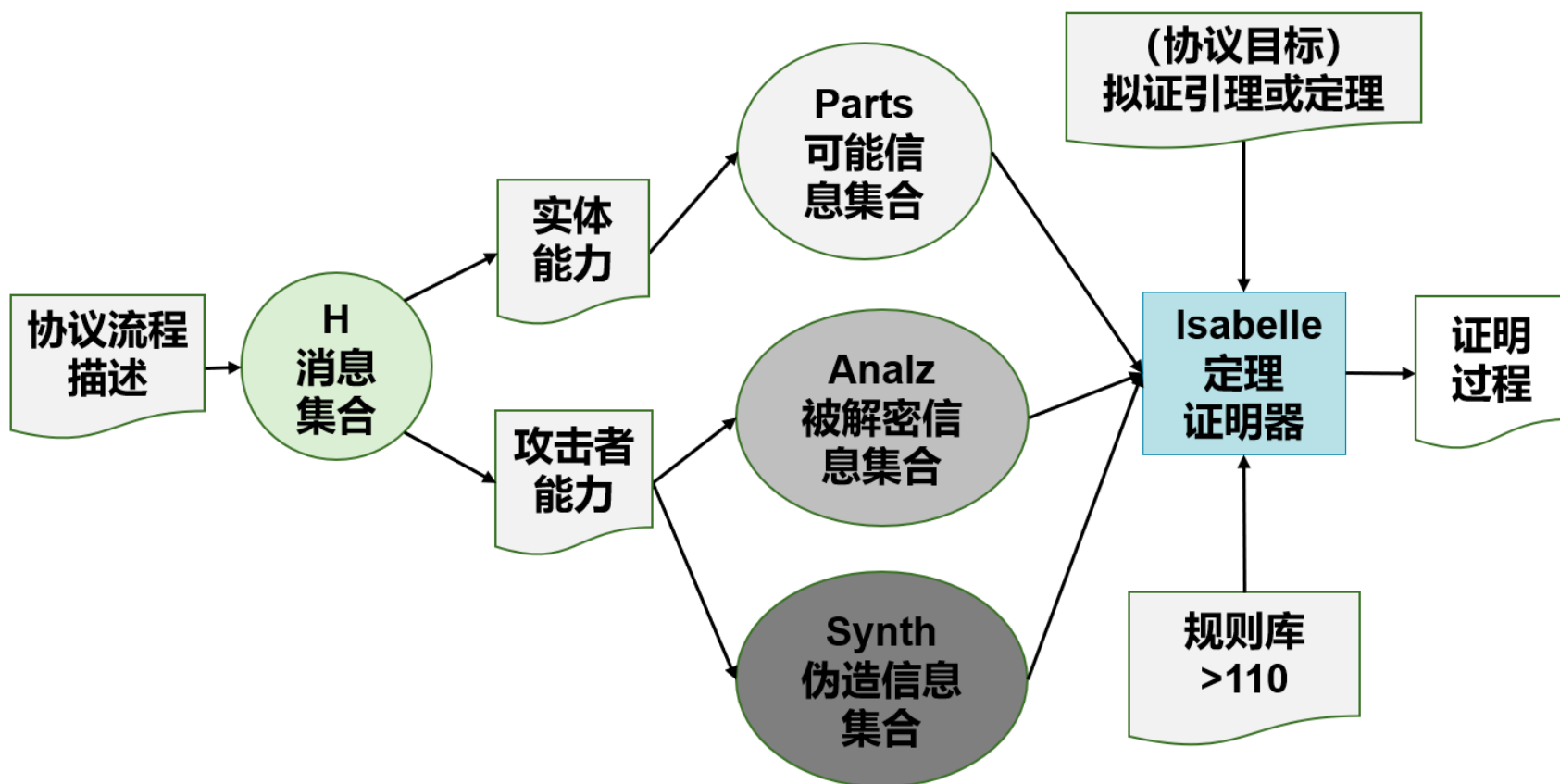


Lawrence C. Paulson FRS

基于定理证明的分析方法

➤原理（续）

- 数学归纳法：首先说明 $P(0)$ 正确，假设 $P(n)$ 正确，证明 $P(n+1)$ 正确。



基于定理证明的分析方法



➤ 优点

- 能够解决无穷状态系统的验证问题
- 用于无限状态空间
- 侧重于证明安全协议的正确性

➤ 缺点

- 难以有效自动化

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具

密码学可证明安全性分析方法



- 使用现代密码学中可证明安全性的理论
- 在复杂理论的框架下提供安全协议安全证明
 - 基于随机比特串的概率分布
 - 攻击者模拟为能以多项式运行的任意图灵机
- 如果攻击者以不可忽略的概率成功攻击协议，意味着攻击者能有效解决一个已知的数学难题
- 一种规约式证明
 - 把协议的安全性规约到某特定的已知难题
- 在一些特定框架下能够给出密码协议的安全性证明

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具



- Lowe 开发的使用模型检测工具FDR的协议分析工具
- 使用该工具发现了NSPK的中间人攻击
- FDR目前仍然被维护，并用于安全协议分析
- 使用了通信顺序进程 CSP（一种面向分布式系统的程序设计语言）
- Lowe还开发了一个小工具Casper，完成协议描述到CSP的转换

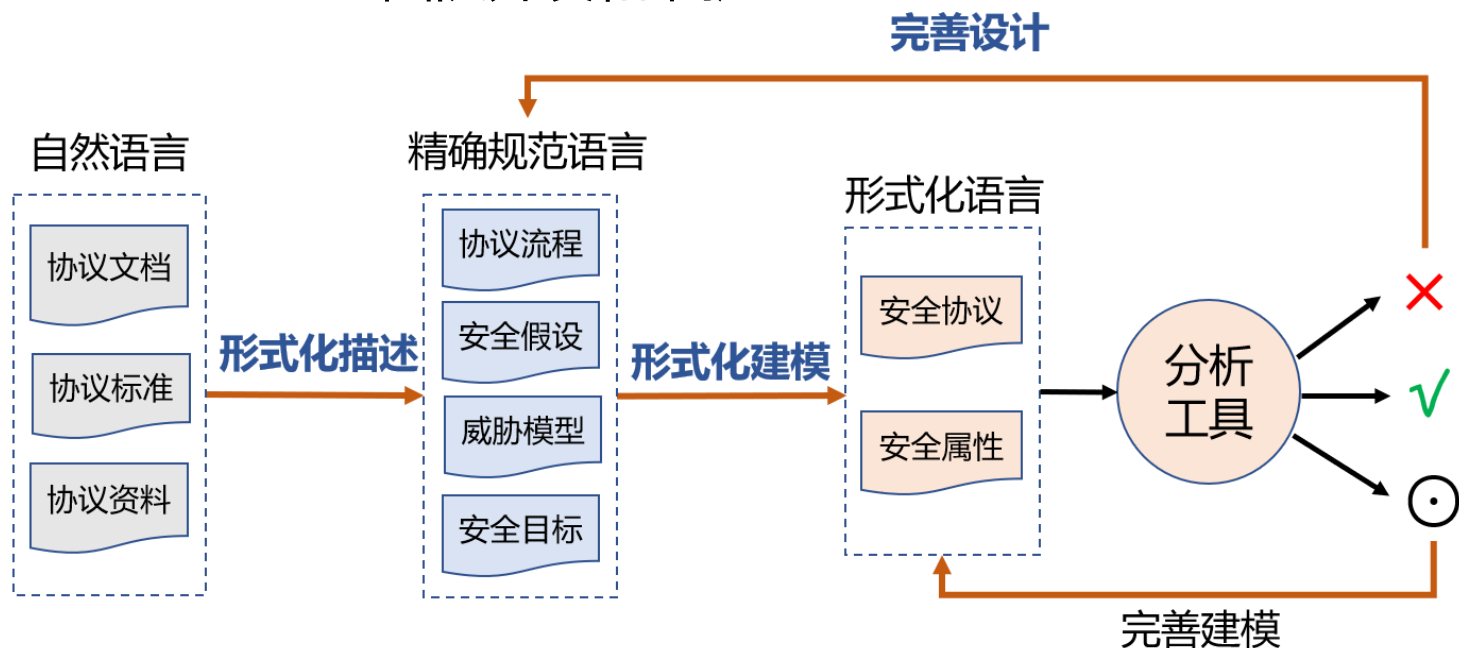
$\langle \text{pkb} := \text{PK}(B) \rangle$
 $1. A \rightarrow B: \{na, A\} \{pkb\}$



$INITIATOR(a, na) =$
 $user.a?b \rightarrow I_running.a.b \rightarrow$
 $comm!Msg1.a.b.Encrypt.kb.na.a \rightarrow$
 $comm.Msg2.b.a.Encrypt.ka?na'.nb \rightarrow$
 $if\ na = na'$
 $then\ comm!Msg3.a.b.Encrypt.kb.nb \rightarrow$
 $I_commit.a.b \rightarrow session.a.b \rightarrow Skip$
 $else\ STOP$

ProVerif

- 开源的安全协议形式化工具
- 由Bruno Blanchet团队开发和维护



- 已经被工具设计者和其他人应用于广泛的协议中，如：JFK、Kerberos, TLS1.3, **FIDO(UAF和FIDO2)**等，提供了与身份验证和密钥建立相关的示例分析。

Scyther, scyther-proof 和 Tamarin



➤ 由ETH和Oxford开发的协议分析工具（开源）

➤ <https://people.cispa.io/cas.cremers/tools/index.html>

➤ Scyther (2008)

- 虽然提供了无限搜索，但没有攻击并不构成正式的安全证明；
- 分析的协议：HMQV, KEA+, NAXOS, JKL, [IKE](#), [ISO/IEC 9798](#) (authentication), [ISO/IEC 11770](#) (key establishment)

➤ scyther-proof(2010)

- 可以给出 Isabelle/HOL形式的逻辑证明。
- 分析的协议： [ISO/IEC 9798](#)

➤ Tamarin(2012)

- 支持Diffie–Hellman 和 bilinear pairings
- 只要分析在终止时没有发现攻击，可提供在符号模型中的安全性证明。
- 分析的协议：KEA+, NAXOS, UM, JKL, STS-MAC, 5G-AKA和TLS 1.3等

计算模型下的两种分析工具



➤ EasyCrypt (2009)

- 由西班牙(IMDEA, 马德里纳米科学研究所)和法国 (INRIA, 法国国家信息与自动化研究所) 开发;
- 被应用于为几种密码原语和协议提供证明;
- 被验证名为miTLS (一种TLS的实现) 中的TLS握手协议和密钥协商协议 NAXOS;

➤ Cryptoverif (2005)

- 由Bruno Blanchet团队开发和维护
- 使用Game技术, 为协议提供计算证明
- 分析的协议: Needham-Schroeder共享密钥协议、Kerberos、SSH和 TLS草案1.3。

分析工具小节




<i>Properties</i> → ↓ <i>Tool</i>	Type	Usage
FDR	Symbolic	Automatic
Maude-NPA	Symbolic	User-guided
ProVerif	Symbolic	Automatic
Scyther	Symbolic	Automatic
Tamarin	Symbolic	Automatic/user-guided
EasyCrypt	Computational	User-guided
CryptoVerif	Computational	User-guided

本讲内容



1. 形式化方法概述
2. Dolev-Yao模型
3. 基于逻辑推理的分析方法
4. 基于模型检测的分析方法
5. 基于定理证明的分析方法
6. 密码学可证明安全性分析方法
7. 常用分析工具



谢谢大家！ 欢迎提问！