IEEE SP Magazine'22-Basin-Tamarin: Verification of Large-Scale, Real-World, Cryptographic Protocols

本既述：(G) Tamarin是一种开源的密码协议分析工具，当前已经较为成熟，可以用于模型化和分析密码协议，在学术界和工业界都引发了许多讨论。(T)本文旨在进一步描述Tamarin可以如何根据设计范围，可模型化和推断的属性及复杂性进行扩展。(A)首先简要描述Tamarin的主要工作方式和原理，随后提供了一些例子表明Tamarin可以用于找出协议的问题并纠正协议设计。(R)最终总结出Tamarin的发展历程，并从技术层面和应用层面给出了未来工作的方向。

优点：①对Tamarin的主要技术做了介绍。②给出web应用的协议、移动通信协议和支付协议的例子，表明Tamarin在协议应用及标准化过程中起到了关键作用。

问题：① 本文对Tamarin的介绍更多地集中于应用Tamarin的效果，对于技术细节介绍较少

② 在探讨未来工作时应简要提及Tamarin可能存在的不足，例如可能无法验证某些协

③ 应与同类型的密码分析和验证工具做一个对比与分析。

1. Tamarin的输入：协议模型，敌手的能力和目标的安全属性。
提供了算法用于找到安全属性的反例(即攻击方式)，若没有找到，则构造安全证明

2. 使用Tamarin做验证。

1> 协议和敌手通过基于multiset rewriting rules的expressive language来描述

①rules定义了一个labeled transition system，它的状态由敌手的知识，网络消息来生成的信息及协议参与者的本地状态的符号表示。

②敌手和协议通过更新网络信息及生成新的信息来交互

③Tamarin也支持各种密码操作符的等式规范，如Diffie-Hellman exponentiation, exclusive-or, 以及bilinear pairings.

④安全属性模型化为trace properties，根据transition system的trace或根据两个transition system的对等关系来检测。

2>. 基石出。

①equational theory E定义密码操作，multiset rewriting system R定义协议

formula ϕ 定义trace property Tamarin可以检查协议module E的traces的validity和satisfiability

表示为a fragment of first-order logic，并对时间点进行量化

①validaty检查可以简化为检查否定公式的satisfiability

Tamarin采用constraint solving对满意的trace执行符号搜索，搜索空间的状态通过constraint system表示，例如constraint表示为重写步骤或一次执行中没有出现的行为，

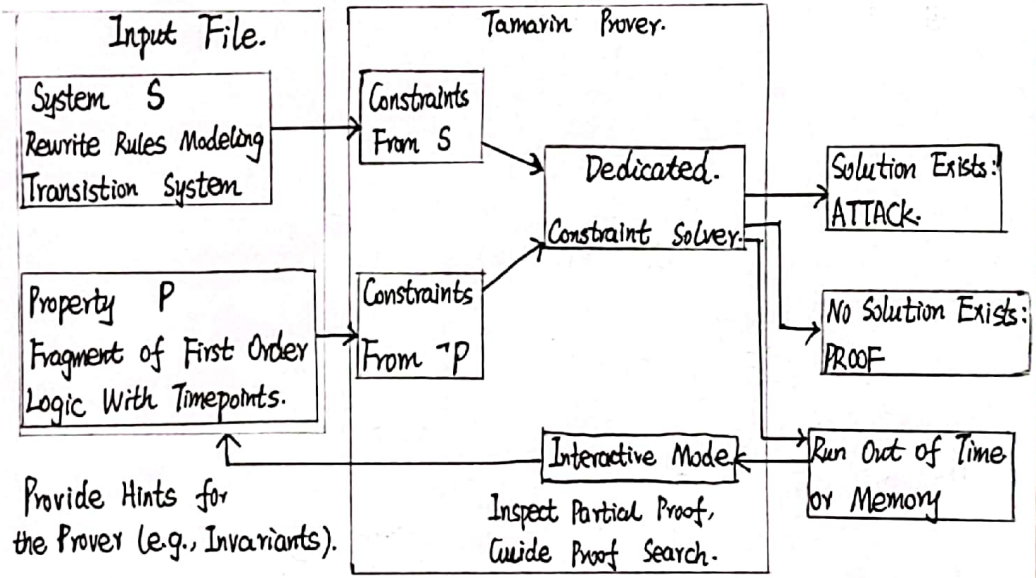
▲若无规则可以应用且没有satisfying trace存在，则可以证明协议安全性。

最新版本的Tamarin只要求用户指定的equational theories是收敛的，并确保finite variant property，使得Tamarin可以使用一大类equational theories.

③对安全协议的验证是不可判定性问题，例如主动敌手可以执行许多会话，另外敌手可以从它看到的信息中得到什么也是不可确定的。

为了缓解这样的问题，Tamarin结合了许多方法，使术语和演绎规范化，使用启发式方法，倒数后向搜索。另外还提供了在证明过程中与用户的交互过程。

3>. Tamarin提供了两种方法构造证明。{自动化模式：结合演绎、等式推理及启发式证明；交互式模式：通过检测和人工交互来解决自动化过程的问题}



4>. 许多协议在标准化或应用过程中通过Tamarin发现错误，改进设计，例如TLS1.3, 5G-AKA和EMV

3. 未来工作

1> 技术层面，增强可扩展性。

2> 使用更加智能，更可编程的证明策略改进自动化模式，扩大应用范围，支持证明重用

3> 增强易用性，改进用户接口及文档。