计算机工程与应用 2007 43 (21): 8-11 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

密码协议形式化分析的计算合理性

王全来[1,2]，王亚弟[1]，韩继红[1]

1.解放军信息工程大学 电子技术学院，郑州 450004
2.解放军防空兵指挥学院，郑州 450052

收稿日期 修回日期 网络版发布日期 2007-7-9 接受日期

摘要 基于Abadi-Rowgaway的形式化加密的计算合理性定理，提出和证明了密码协议形式化分析的计算合理性定理。通过对群密钥分配协议安全性的分析，说明定理对协议的可选择攻击具有较强的分析能力，提出了群密钥分配协议的形式化方法与计算方法下安全性的形式化定义，并证明了其合理性。

关键词 形式化方法 计算方法 合理性定理 密码协议分析

分类号

Computational soundness of formal analysis of cryptographic protocols

WANG Quan-lai[1,2]，WANG Ya-di[1]，HAN Ji-hong[1]

1.Institute of Electronic Technology，the PLA Information Engineering University，Zhengzhou 450004，China
2.The PLA Air Defense Forces Command College，Zhengzhou 450052，China

Abstract
Based on the Abadi-Rowgaway computational soundness theorem of formal encryption，this paper proposes and proves our computational soundness theorem of formal analysis of cryptographic protocols.Through the analysis for group key distribution protocols，our soundness theorem is stronger and powerful in adaptive attacks.This paper proposes formal definitions of security for group key distribution protocols both in the formal methods and the computational methods，then proves soundness of the formal definition.

Key words formal method computational method soundness theorem cryptographic protocol analysis

DOI:

通讯作者 王全来 E-mail：wql_lai@126.com