基于 PUF 的 RFID 系统安全密钥协商协议

郭丽敏 1， 刘 丹 1，王立辉 1，单伟君 1，李 清 1,2
（1 上海复旦微电子集团股份有限公司，上海 200433; 2 复旦大学 微电子学院，上海 200433）

摘 要：低成本 RFID 标签与读卡器间的相互认证或安全通信都依赖于通信双方预先共享的密钥，而攻击者可以通过物理攻击等手段获得该密钥.利用 PUF 电路的物理不可克隆特性，提出两个基于 PUF 的密钥协商协议，从中通信双方可以产生相同的随机密钥，供后续的认证或安全通信使用.分析结果表明，该协议可以有效抵抗物理、重放、假冒、中间人、离线猜测及在线猜测攻击，同时提供前向安全性和后向安全性.

关键词： RFID 系统；物理不可克隆函数；密钥协商协议；安全

Secure Key Exchange Protocol for RFID System Based on PUF

GUO Li-min 1, LIU Dan 1, WANG Li-hui 1, SHAN Wei-jun 1, Li Qing 1,2
(1 Shanghai Fudan Microelectronics Group Company Limited, Shanghai 200433, China;
2 School of Microelectronics, Fudan University, Shanghai 200433, China)

Abstract：The secure mutual authentication or secure communication between the low-cost RFID tags and the card readers depends on a secret key shared by the two parties, which can be gained directly by a power attacker by means of physical attacks. Taking advantage of the physical unclonable feature of PUF circuits, two secure key exchange protocols are presented in this paper, such that the two parties can generate a same random key which can be used to secure the following authentication or communication. Security analysis shows that these two protocols can resist physical attack, reply attack, counterfeit attack, man-in-the-middle-attack, offline guessing attack and online guessing attack, and also can provide forward security and backward security.

Key words：RFID system; PUF; key exchange protocol; security

作者简介：
郭丽敏 女，(1986-)，硕士，工程师.研究方向为集成电路设计开发.
E-mail:guolimin@fmsh.com.cn.
刘 丹 男，(1981-)，硕士，工程师.研究方向为集成电路设计开发.
王立辉 男，(1982-)，硕士，工程师.研究方向为集成电路设计开发.
单伟君 男，(1988-)，硕士，工程师.研究方向为集成电路设计开发.
李 清 女，(1968-)，硕士，高级工程师.研究方向为集成电路设计开发.