实例依赖的可验证随机函数的高效构造*

Construction of high performance instance-dependent verifiable random functions

中文关键词：零知识协议 实例依赖 可验证随机函数

英文关键词：zero knowledge protocol instance-dependent verifiable random function

基金项目：北京市属高等学校人才强教计划资助项目（PHR200906210）;北京市教育委员会科研基地建设项目;北京市教育委员会科技计划资助项目（KM200810037001）

作者	单位
师鸣若1, 姜中华2	(1. 北京物资学院, 北京 101149; 2. 中国科学院 软件研究所 信息安全国家重点实验室, 北京 100080)

中文摘要：

实例依赖的可验证随机函数是由文献[1]提出的一个新的密码学概念，它也是构造高安全性的零知识协议（如可重置零知识论证系统）的一个强有力的工具，而这些高安全性的零知识协议在智能卡和电子商务中有着重要的潜在价值。基于非交互ZAP证明系统和random oracle模型中ΣOR-协议，给出了实例依赖的可验证伪随机函数的两个高效的实现和相应的安全性证明，提升了这一工具的应用价值。

英文摘要：

Instance-dependent verifiable random function (IDVRF) was a new cryptographic concept proposed by reference[1], which was a powerful tool to construct high security zero knowledge protocols such as resettable zero knowledge proof system. These powerful protocols could be well applied to intelligence card and electronic ecommerce applications. Based on non-interactive ZAP and ΣOR-under random oracle model, this paper gave two kinds of high efficient implementation of IDVRF and proved their security. The application value of IDVRF is greatly enhanced by the two implementations.