通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

汤殿华1,祝世雄1,王林1,杨浩淼2,范佳1.基于RLWE的全同态加密方案[J].通信学报,2014,(1):173~182

基于RLWE的全同态加密方案

Fully homomorphic encryption scheme from RLWE

投稿时间： 2012-05-12

DOI：10.3969/j.issn.1000-436x.2014.1.020

中文关键词：全同态加密 重线性化 模转换

英文关键词:fully homomorphic encryption relinearization modulus switching

基金项目:国家自然科学基金资助项目（61206437）

作者	单位
汤殿华1，祝世雄1，王林1，杨浩淼2，范佳1	1. 保密通信重点实验室，四川 成都 610041；2.电子科技大学 计算机学院，四川 成都 610054

中文摘要:

基于Kristin Lauter等人的somewhat同态方案，提出“带密钥转换的重线性化技术”。结合该技术与“模转换”，设计了一个基于RLWE的非自举的层次化全同态加密方案。该方案的同态操作简单，而且给出的平凡门操作使得电路层结构更清晰。最后利用自举技术作为优化提升了方案的同态运算能力。

英文摘要:

Based on the somewhat homomorphic scheme of Kristin Lauter et al. a new technique, called Relinearization with key switching was presented. Combining this technique with modulus switching, a (leveled) fully homomorphic encryption scheme without bootstrapping from RLWE were designed. Homomorphic operations of this scheme is simple, and trivial gate operation given in the scheme can make level structure of circuit clearer. Finally, bootstrapping was used as optimization to evaluate capability of the proposed scheme.

查看全文 查看/发表评论 下载PDF阅读器

关闭