

信息安全学报

Journal of Cyber Security



中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING, CAS



SKLOIS
信息安全国家重点实验室



科学出版社
Science Press

目 次

后量子加密算法的硬件实现综述	1
曹 元, 陆 旭, 吴彦泽, 谢浩东, 乔云凯, 姚恩义, 陈 帅, 叶 靖	
基于 FPGA 的 Leighton-Micali 签名方案密钥生成的高速可配置实现	17
胡 潇, 宋逸峰, 汪文浩, 田 静	
应用于后量子密码的高速高效 SHA-3 硬件单元设计	32
刘冬生, 陈 勇, 熊思琦, 杨 朔, 胡 昂	
基于 MLWE 的格密码高效硬件实现	40
崔益军, 姚 衍, 倪子颖, 王成华, 刘伟强	
CRYSTAL-KYBER 硬件设计优化空间探索	51
穆嘉楠, 赵艺璇, 严 寒, 宋金峰, 叶 靖, 李华伟, 李晓维	
基于格的高效范围证明方案	64
胡春雅	
基于格陷门的高效密钥封装算法	79
谭高升, 张 锐, 姜子铭, 孙 硕	
同源密码中 Montgomery 模型的 w -坐标研究	92
陶 铮, 胡 志	

Contents

The Survey of Post-quantum Cryptography Hardware Implementation	1
<i>CAO Yuan, LU Xu, WU Yanze, XIE Haodong, QIAO Yunkai, YAO Enyi, CHEN Shuai, YE Jing</i>	
High-Speed and Configurable FPGA implementation of the Key Generation for Leighton-Micali Signature Protocol	17
<i>HU Xiao, SONG Yifeng, WANG Wenhao, TIAN Jing</i>	
Design of High-Speed and High-Efficiency SHA-3 Hardware Unit for Post-Quantum Cryptography	32
<i>LIU Dongsheng, CHEN Yong, XIONG Siqu, YANG Shuo, HU Ang</i>	
Efficient Hardware Implementation of MLWE Lattice Based Cryptography	40
<i>CUI Yijun, YAO Kan, NI Ziyang, WANG Chenghua, LIU Weiqiang</i>	
Optimization Space Exploration of Hardware Design for CRYSTAL-KYBER	51
<i>MU Jianan, ZHAO Yixuan, YAN Han, SONG Jinpeng, YE Jing, LI Huawei, LI Xiaowei</i>	
Lattice-based Efficient Range Proofs	64
<i>HU Chunyu</i>	
The Efficient Key Encapsulation Algorithm from the Lattice Trapdoor	79
<i>TAN Gaosheng, ZHANG Rui, JIANG Ziming, SUN Shuo</i>	
On the w -coordinates of Montgomery Model in Isogeny-based Cryptography	92
<i>TAO Zheng, HU Zhi</i>	