

RESEARCH PAPER

Right or wrong collision rate analysis without profiling: full-automatic collision fault attack	032101(11)
An WANG, Yu ZHANG, Weina TIAN, Qian WANG, Guoshuang ZHANG & Liehuang ZHU	
Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability	032102(13)
Kai ZHANG, Hui LI, Jianfeng MA & Ximeng LIU	
Countering JPEG anti-forensics based on noise level estimation.....	032103(14)
Hui ZENG, Jingjing YU, Xiangui KANG & Siwei LYU	
Three new infinite families of bent functions	032104(14)
Libo WANG, Baofeng WU, Zhuojun LIU & Dongdai LIN	
Attacking OpenSSL ECDSA with a small amount of side-channel information	032105(14)
Wenbo WANG & Shuqin FAN	
Impossible differential attack on Simpira v2	032106(13)
Rui ZONG, Xiaoyang DONG & Xiaoyun WANG	
Bi-directional and concurrent proof of ownership for stronger storage services with de-duplication.....	032107(11)
Taek-Young YOUN & Ku-Young CHANG	
Improved meet-in-the-middle attacks on reduced-round Piccolo.....	032108(13)
Ya LIU, Liang CHENG, Zhiqiang LIU, Wei LI, Qingju WANG & Dawu GU	
A better bound for implicit factorization problem with shared middle bits	032109(10)
Shixiong WANG, Longjiang QU, Chao LI & Shaojing FU	
Impossible meet-in-the-middle fault analysis on the LED lightweight cipher in VANETs	032110(13)
Wei LI, Vincent RIJMEN, Zhi TAO, Qingju WANG, Hua CHEN, Yunwen LIU, Chaoyun LI & Ya LIU	
Similar operation template attack on RSA-CRT as a case study	032111(17)
Sen XU, Xiangjun LU, Kaiyu ZHANG, Yang LI, Lei WANG, Weijia WANG, Haihua GU, Zheng GUO, Junrong LIU & Dawu GU	
Privacy-preserving large-scale systems of linear equations in outsourcing storage and computation.....	032112(9)
Dongmei LI, Xiaolei DONG, Zhenfu CAO & Haijiang WANG	
A real-time inversion attack on the GMR-2 cipher used in the satellite phones	032113(18)
Jiao HU, Ruilin LI & Chaojing TANG	
An adaptive system for detecting malicious queries in web attacks.....	032114(16)
Ying DONG, Yuqing ZHANG, Hua MA, Qianru WU, Qixu LIU, Kai WANG & Wenjie WANG	
Orthogonalized lattice enumeration for solving SVP	032115(15)
Zhongxiang ZHENG, Xiaoyun WANG, Guangwu XU & Yang YU	

POSITION PAPER

A systematic framework to understand central bank digital currency.....	033101(8)
Qian YAO	

HIGHLIGHT

Construction of rotation symmetric bent functions with maximum algebraic degree.....	038101(3)
Wenyong ZHANG & Guoyong HAN	
Several classes of negabent functions over finite fields.....	038102(3)
Gaofei WU, Nian LI, Yuqing ZHANG & Xuefeng LIU	
Improved automatic search of impossible differentials for camellia with FL/FL^{-1} layers.....	038103(3)
Yaoling DING, Xiaoyun WANG, Ning WANG & Wei WANG	
More permutation polynomials with differential uniformity six	038104(3)
Ziran TU, Xiangyong ZENG & Zhiyong ZHANG	
Improved cryptanalysis of step-reduced SM3.....	038105(2)
Yanzhao SHEN, Dongxia BAI & Hongbo YU	
Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation	038106(3)
Lixue SUN, Chunxiang XU, Mingwu ZHANG, Kefei CHEN & Hongwei LI	

LETTER

Secure and efficient k -nearest neighbor query for location-based services in outsourced environments	039101(3)
Haiqin WU, Liangmin WANG & Tao JIANG	
Efficient flush-reload cache attack on scalar multiplication based signature algorithm	039102(3)
Ping ZHOU, Tao WANG, Xiaoxuan LOU, Xinjie ZHAO, Fan ZHANG & Shize GUO	
Protecting white-box cryptographic implementations with obfuscated round boundaries	039103(3)
Tao XU, Chuankun WU, Feng LIU & Ruoxin ZHAO	
Efficient and secure outsourcing of bilinear pairings with single server.....	039104(3)
Min DONG & Yanli REN	
Verifiable random functions with Boolean function constraints	039105(3)
Qianwen WANG, Rongquan FENG & Yan ZHU	
Optimal model search for hardware-trojan-based bit-level fault attacks on block ciphers	039106(3)
Xinjie ZHAO, Fan ZHANG, Shize GUO & Zheng GONG	