

RESEARCH PAPER

Improved impossible differential cryptanalysis of large-block Rijndael.....	032101(14)
Ya LIU, Yifan SHI, Dawu GU, Bo DAI, Fengyu ZHAO, Wei LI, Zhiqiang LIU & Zhiqiang ZENG	
Related-tweakey impossible differential attack on reduced-round Deoxys-BC-256	032102(12)
Rui ZONG, Xiaoyang DONG & Xiaoyun WANG	
EFFECT: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid	032103(14)
Zhitao GUAN, Yue ZHANG, Liehuang ZHU, Longfei WU & Shui YU	
Identity-based public auditing for cloud storage systems against malicious auditors via blockchain	032104(16)
Jingting XUE, Chunxiang XU, Jining ZHAO & Jianfeng MA	
Partially known information attack on SM2 key exchange protocol.....	032105(14)
Wei WEI, Jiazhe CHEN, Dan LI & Beibei WANG	
CATH: an effective method for detecting denial-of-service attacks in software defined networks	032106(15)
Yi GUO, Fu MIAO, Liancheng ZHANG & Yu WANG	
A new discrete Fourier transform randomness test.....	032107(16)
Meihui CHEN, Hua CHEN, Limin FAN, Shaofeng ZHU, Wei XI & Dengguo FENG	
New observation on the key schedule of RECTANGLE.....	032108(13)
Hailun YAN, Yiyuan LUO, Mo CHEN & Xuejia LAI	
A regulated digital currency	032109(12)
Yanbing WU, Haining FAN, Xiaoyun WANG & Guangnan ZOU	
A novel approach to public-coin concurrent zero-knowledge and applications on resettable security	032110(14)
Zhenbin YAN & Yi DENG	
Automatic search method for multiple differentials and its application on MANTIS	032111(15)
Shiyao CHEN, Ru LIU, Tingting CUI & Meiqin WANG	
Pseudo random oracle of Merkle-Damgård hash functions revisited.....	032112(15)
Kamel AMMOUR, Lei WANG & Dawu GU	
Universally composable secure geographic area verification without pre-shared secret	032113(15)
Junwei ZHANG, Ning LU, Jianfeng MA & Chao YANG	

LETTER

A more compact multi-id identity-based FHE scheme in the standard model and its applications.....	039101(3)
Xueqing WANG, Biao WANG, Bei LIANG & Rui XUE	
A revised CVSS-based system to improve the dispersion of vulnerability risk scores.....	039102(3)
Chensi WU, Tao WEN & Yuqing ZHANG	
A rejection sampling algorithm for off-centered discrete Gaussian distributions over the integers	039103(3)
Yusong DU, Baodian WEI & Huang ZHANG	
Some characteristics of logistic map over the finite field	039104(3)
Bo YANG & Xiaofeng LIAO	
Side channel attack of multiplication in $GF(q)$ -application to secure RSA-CRT.....	039105(3)
Sen XU, Weiya WANG, Xiangjun LU, Zheng GUO, Junrong LIU & Dawu GU	
UMBRELLA: user demand privacy preserving framework based on association rules and differential privacy in social networks.....	039106(3)
Chunliu YAN, Ziyi NI, Bin CAO, Rongxing LU, Shaohua WU & Qinyu ZHANG	
Finding the best answer: measuring the optimization of public and authoritative DNS.....	039107(3)
Jia ZHANG, Haixin DUAN, Jian JIANG, Jinjin LIANG & Jianping WU	
High-efficient generation algorithm for large random active shield.....	039108(3)
Ruishan XIN, Yidong YUAN, Jiayi HE, Yuehui LI & Yiqiang ZHAO	
Real-time state recovery attack against MORUS in nonce-misuse setting.....	039109(3)
Tairong SHI & Jie GUAN	
Decomposition of nonlinear feedback shift registers based on Boolean networks	039110(3)
Jianghua ZHONG & Dongdai LIN	
Secure key-aggregation authorized searchable encryption	039111(3)
Haijiang WANG, Xiaolei DONG, Zhenfu CAO, Dongmei LI & Nanyuan CAO	