

劉兆樑 老師

現職 資訊多媒體應用學系 助理教授

學歷 中興大學資科系博士

專長1

資訊安全

專長2

數學

教師研究成果資料明細



SCI、SSCI、A&HCI、EI、TSSCI期刊論文

1. 劉兆樑(Chao-Liang Liu) ,2008-01, (已刊登)
FINITE FIELDS AND THEIR APPLICATIONS 14卷1期:65頁~75頁
Computing the Modular Inverses Is as Simple as Computing the GCDs
2. 劉兆樑(Chao-Liang Liu) ,2005-06, (已刊登)
IEICE TRANSACTIONS ON COMMUNICATIONS E88-B卷5期:2171頁~2172頁
Cryptanalysis of an Efficient User Identification Scheme Based on ID-Based Cryptosystem
3. 劉兆樑(Chao-Liang Liu) ,2007-01, (已刊登)
APPLIED MATHEMATICS AND COMPUTATION 189卷1期:395頁~409頁
Further Refinement of Pairing Computation Based on Miller's Algorithm
4. 劉兆樑(Chao-Liang Liu) ,2006-12, (已刊登)
APPLIED MATHEMATICS AND COMPUTATION 183卷1期:486頁~490頁
Performance Improvement for the GGM-Construction of Pseudorandom Functions
5. 劉兆樑(Chao-Liang Liu) ,2004-06, (已刊登)
IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS
COMMUNICATIONS AND COMPUT E87-A卷8期:2177頁~2179頁
Security Analysis of a Threshold Access Control Scheme Based on Smart Cards
6. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)
APPLIED MATHEMATICS AND COMPUTATION 卷期:頁~頁
Speeding up Pairing Computation Using Non-adjacent Form and ELM Method
7. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)
JOURNAL OF COMPUTER AND SYSTEM SCIENCES 卷期:頁~頁
Certificateless aggregate signature scheme with constant pairing operations
8. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)
EXPERT SYSTEMS WITH APPLICATIONS 卷期:頁~頁
Generic construction of certificateless encryption with keyword search
9. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)
FUNDAMENTA INFORMATICA 卷期:頁~頁
An Efficient Certificateless Aggregate Signature Scheme
10. 劉兆樑(Chao-Liang Liu)* ,2011-, (已刊登)
COMPUTER JOURNAL 54卷10期:1582頁~1591頁
Refinements of Miller's Algorithm over Weierstrass Curves Revisited

11. 劉兆樑(Chao-Liang Liu)* ,2011-09, (已刊登)

International Journal of Innovative Computing Information and Control

7卷9期:5557頁~5569頁

A provably secure certificateless proxy signature scheme

12. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)

COMPUTERS & SECURITY 卷期:頁~頁

Girault's level-3 security in certificateless cryptography revisited

13. 劉兆樑(Chao-Liang Liu) ,2011-, (已投稿審查中)

IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 卷期:頁~頁

Comments on "A Secure Decentralized Erasure Code for Distributed Networked Storage"