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

研究計畫

1.劉兆樑 國科會 2007.08.1 ~2008.07.31
雙線性配對計算之研究與實作

2.劉兆樑 校內計畫 2009.08.1 ~2010.07.31
適用於PAIRING 密碼系統之伺服器輔助演算法之研究

3.劉兆樑 國科會 2009.08.1 ~2010.07.31
雙線性配對計算效能提升之研究

4.劉兆樑 國科會 2010.08.1 ~2011.07.31
有限體下橢圓曲線計點演算法效能改進之研究

5.劉兆樑 國科會 2011.08.1 ~2012.07.31
免憑證式公開金鑰密碼系統信任層級之探討

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 INFORMATICAE 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”

研討會論文

1.劉兆樑(Chao-Liang Liu) 2011.05.26~2011.05.27
Practical Necessity of Girault’s Level-Three Security in Certificateless Cryptography
Cryptology and Information Security Conference 2011

2.劉兆樑(Chao-Liang Liu) 2002. . ~ . .
Wang- Chang 之以智慧卡為驗證基礎之通行碼確認方法的改進
第四屆網際空間：資訊、法律與社會學術研究暨實務研討會

3.劉兆樑(Chao-Liang Liu) 2003. . ~ . .
以智慧卡為驗證基礎之人性化遠端使用者確認方法
第十三屆全國資訊安全會議

4.劉兆樑(Chao-Liang Liu) 2003. . ~ . .
以橢圓曲線密碼學改良之多人授權予多人的代理簽章法
2003 年全國計算機會議

5.劉兆樑(Chao-Liang Liu) 2003. . ~ . .
Cryptanalysis of a Remote User Authentication Scheme Based on Smart Cards
Proc. of the National Computer Symposium

6.劉兆樑(Chao-Liang Liu) 2003. . ~ . .
Security Enhancement for a One-Time Password Authentication Scheme Using Smart Cards
2003 Workshop on Consumer Electronics

7.劉兆樑(Chao-Liang Liu) 2004. . ~ . .
一個遠端認證方法之改進以及軍事上之應用
陸軍官校八十週年校慶綜合研討會暨國科會國防科技航空技術學門研究成果發表會

8.劉兆樑(Chao-Liang Liu) 2004. . ~ . .
以智慧卡為基礎之安全群播機制
第十四屆全國資訊安全會議

9.劉兆樑(Chao-Liang Liu) 2004. . ~ . .
Security Analysis of a Tripartite Authenticated Key Agreement Protocol Based on Weil Pairing
Proc. of the International Computer Symposium

10.劉兆樑(Chao-Liang Liu) 2005. . ~ . .
Performance Improvement for the GGM-Construction of Pseudorandom Functions
Proc. of the National Computer Symposium

11.劉兆樑(Chao-Liang Liu) 2006. . ~ . .
Further Refinement of Pairing Computation Based on Miller's Algorithm
Proc. of the sixteenth National Conference on Information Security

12.劉兆樑(Chao-Liang Liu)、劉兆樑(Chao-Liang Liu) 2007. . ~ . .
變形Miller 演算法之研究
第十七屆全國資訊安全會議

13.劉兆樑(Chao-Liang Liu)、劉兆樑(Chao-Liang Liu)、陳柏諭 2011.04.15~2011.04.15
一個免憑證式金鑰交換協議之安全分析與改進
第六屆國際健康資訊管理研討會

14.劉兆樑(Chao-Liang Liu) 2008.12.5 ~2008.12.5
植基於離散對數問題之多關鍵字可搜尋加密法
2008年民生電子研討會

15.劉兆樑(Chao-Liang Liu) 2010.03.26~2010.03.26
一個植基於智慧卡之遠端雙向認證協定
第五屆國際健康資訊管理研討會

獲獎

1.劉兆樑(Chao-Liang Liu) 2010-03-
九十八學年度優良教學獎

2.劉兆樑(Chao-Liang Liu) 2011-03-
九十九學年度優良教學獎

指導碩博士論文

1.劉兆樑
身份認證與免憑證式金鑰交換協議之研究
陳柏諭

參與研討會

1.劉兆樑 2008-05-18~2008-05-19
第三屆台灣數位學習發展研討會

2.劉兆樑 2008-12-20~2008-12-21
九十六年全國計算機會議

3.劉兆樑 2009-11-06~2009-11-06
第三屆資訊教育與科技應用研討會

4.劉兆樑 2011-03-11~2011-03-11
第四屆資訊教育與科技應用研討會

5.劉兆樑 2011-07-19~2011-07-22
The 5th International Multi-Conference on Society, Cybernetics and Informatics: IMSCI 2011

6.劉兆樑 2012-12-02~2012-12-03
2011全國計算機會議

7.劉兆樑 2012-03-23~2012-03-23
第五屆資訊教育與科技應用研討會(IETAC 2012)

8.劉兆樑 ~
第二十二屆全國資訊安全會議

參與期刊編輯

1.劉兆樑 2008-01-09~2008-01-09
Computer Communications

學術/社會服務資料

1.劉兆樑 2011-02-20~2011-09-30
海關緝毒犬寄養家庭

2.劉兆樑 2008-06-11~2008-06-11
口試委員

3.劉兆樑 2008-06-11~2008-06-11
口試委員

4.劉兆樑 2008-06-11~2008-06-11
口試委員

5.劉兆樑 2008-07-11~2008-07-11
口試委員

6.劉兆樑 2008-07-11~2008-07-11
口試委員

7.劉兆樑 2007-07-28~2007-07-28
口試委員

8.劉兆樑 2009-07-29~2009-07-29
口試委員

9.劉兆樑 2010-06-10~2010-06-10
口試委員

10.劉兆樑 2010-07-07~2010-07-07
口試委員

11.劉兆樑 2010-09-15~2011-1-05
教學服務(社區資訊成長班)

12.劉兆樑 2011-02-24~2011-11-17
全方位電腦應用講師

13.劉兆樑 2010-10-30~2011-10-23
中興大學資工系系友會第一屆常務監事

14.劉兆樑 2011-05-13~2011-05-13
出席嘉義興華高中進班宣導

15.劉兆樑 2007-09-01~2011-06-30
亞洲大學資應系4A導師

16.劉兆樑 2011-04-16~2011-04-16
資應系100學年度碩士班招生考試面試委員

17.劉兆樑 2011-04-09~2011-04-10
資應系100學年度大學甄選資料審查與面試委員

18.劉兆樑 2011-03-04~2011-03-04
新民高中進班宣導

19.劉兆樑 2010-05-25~2010-05-25
豐原高商進班宣導

20.劉兆樑 2010-04-10~2010-04-10
資應系99學年度大學甄選資料審查與面試委員

21.劉兆樑 2009-06-01~2010-12-31
98學年度資應系專題指導老師

22.劉兆樑 2011-03-04~2011-03-04
新民高中進班宣導

23.劉兆樑 2010-11-10~2010-11-10
桃園縣永平工商升學博覽會

24.劉兆樑 2010-07-21~2010-07-21
新民高中進班宣導

25.劉兆樑 2011-06-02~2011-06-02
桃園振聲高中進班宣導

26.劉兆樑 2011-07-25~2011-07-25
口試委員(中興資工)

27.劉兆樑 2011-09-20~2011-10-03
論文審查委員

28.劉兆樑 2011-11-30~2011-11-30
南投縣五育高級中學進班宣導

29.劉兆樑 2011-12-14~2011-12-14
國立卓蘭實驗高中進班宣導