

Guest Editor Call for Papers (III)

「資訊安全通訊雜誌」係由中華民國資訊安全學會發行，並定期於每年一月、四月、七月及十月出版與資訊安全相關領域有關之研究論著，每一期將邀請一位 Guest Editor 針對當期主題進行規劃與邀稿，且為了讓更多的研究者、同好共同開創資訊安全領域研究的天地，將在每一期中刊載下一期 Guest Editor 之規劃主題與論文徵稿方向，供研究者共襄盛舉，以豐富資訊安全研究之園地。2006 年度四月份主題為「密碼系統的實現技術 (Implementation Aspects of Cryptosystems)」，將針對密碼系統的實現技術進行介紹與探討。密碼系統的軟體實現技術探討已久，從早期 DES 晶片與 RSA 演算法於不同硬體平台的軟體實現技術，到最近的橢圓曲線密碼系統的實現技術。相較於過去針對演算法實現速度的追求，現今軟體實現技術需更為周密的考量以防範可能遭受的攻擊。歡迎更多的研究者共同參與此主題的研究。以下僅列舉部份的相關主題，但徵稿論文不受此限：

- * 軟體實現技術 (Software Implementations)
- * 硬體實現技術 (Hardware Implementations)
- * 安全實現技術 (Secure Implementations)
- * 密碼處理器與協同處理器 (Cryptographic Processors and Co-Processors)

投稿須知：

1. 對於論文主題有任何問題，請以 E-mail 聯絡 Guest Editor。
2. 論文請不要有智慧財產與一稿多投之爭議，刊登論文之文責由作者自負。
3. 本刊物只接受電子檔投稿，稿件編輯請參照本刊論文徵稿格式繕打，總頁數在 20 頁內，並將稿件(含作者服務單位、聯絡地址、電話／傳真、e-mail 等基本資料)，email 至 Guest Editor 或本期刊編輯部行政助理(古永昌先生，unicon@mail.cpu.edu.tw)。

重要日期：

論文投稿截止：2006 年 01 月 10 日

製版截止日期：2006 年 03 月 25 日

論文接受通知：2006 年 03 月 10 日

期刊發行日期：2006 年 04 月 10 日

Guest Editor 聯絡方式

姓名：Dr. 楊中皇

隸屬學校及系所：高雄師範大學資教所

單位地址：高雄市苓雅區和平一路 116 號

電子郵件：chyang@nknuc.nknu.edu.tw

本期刊編輯部聯絡方式

主編：Dr. 王旭正(sjwang@mail.cpu.edu.tw)

行政助理：古永昌(unicon@mail.cpu.edu.tw)