

編輯序

CCISA 的出版在本期中，我們推出的主打「菜單」為“Common Criteria”。對於資訊安全的密碼模組實用於科技產業界時，該如何有一套參考的規範，以為設計的參考？對於此一需求，本期的 Guest-editor: 虎尾科技大學，郭文中教授特別為本期的重頭戲擔當重任，為此廣集各方的文稿，並彙整精選內容而成為本次的“Special Issue”。依慣例，仍請各位看官／讀者別忘了先瀏覽“Preface of Guest Editor”來品味此次主題的「開胃佳餚」。之後，對於所收錄的七篇精品文章將能有事半功倍之效用。

另外本編輯部亦提醒讀者，CCISA 在 Sept.01, 2004，正式推行“CCISA Newsletter”的電子刊物，內容記錄最新的國內外學術活動與 CCISA 的重要工作推展，以期能回饋讀者在資訊安全研究上的最新訊息了解及需求。此電子期訊是由清華大學孫宏民教授所主持，並由淡江大學黃仁俊、中山大學范俊逸兩位教授所協同主持。本期訊是以 E-mail 方式進行傳送，期能達最快與最具時效的通訊目的。

對於“CCISA Newsletter”電子信件傳送的創刊，代表 CCISA 繆力推動學術研究／分享的決心與成果展現。藉此使得本編輯部的刊物／訊息傳播得以文章紙本與訊息郵件並行。期使讀者能掌握最新動態。盼讀者繼續對學會熱情支持與踴躍參與學會的產學研究等相關活動。對此，2004 年六月，台灣科技大學的全國資訊安全會議，論文的大量投稿／六成的錄取率／踴躍的報名，CCISA 已能感受讀者／會員對學會的肯定。謝謝您們。

最後在 Call-for-paper，我們詳列了 2005 年一月至十月（全年度）的徵稿訊息（Call-for-paper）。其中的四月份裡有二個並行的主題，分別為“Call-for-paper(II-1): Visual Secret Sharing”與“Call-for-paper(II-2): Quantum Cryptography”。由於 Quantum 的物理性質已是計算研究的熱門議題，因此我們提前規劃此議題。並接著在十月份為 Quantum Cryptography 再做一次完整介紹。

此 Quantum Cryptography 的二次密集完整性論述，將是明年度，2005，除其它重要議題外的最新主題，值得讀者關切與踴躍投稿。密碼學／資訊安全研究也因此又開啟了新的研究與討論空間。

“Communications of the CCISA”是屬於所有讀者的。我們現在亦僅分送給本學會的會員。由於過去數年來發行之龐大，已達到資訊安全知識分享之目的，現在已不再主動寄送給非會員與圖書機構／館／室。盼讀者繼續訂閱本期刊或投書各需求圖書館踴躍訂閱本期刊，得以延續期刊對於重要資訊安全研究／趨勢的傳播。

王旭正

visits at

Dept. of Computer Science/ Dept. of Computer and Information Science and Engineering
Florida State University (FSU)/University of Florida (UF)
Tallahassee/Gainesville, Florida, USA
Oct. 2004