

Special Issue in Communications of the CCISA — Call For Paper

「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 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。

2015 年度一月份主題為「密碼技術理論分析與應用(Theoretical analysis and application of cryptography technology)」。對於高階資安技術人才的培育，除了各類資安理論的研究外，亦包含利用安全理論解決實際安全問題的能力。通過對密碼學及資訊安全理論和應用的研究，可以增強高階資安人員的密碼技術理論能力和實務能力，如密碼算法設計分析、安全協議、密鑰管理、簽名認證、密碼分析方法等都是資訊安全領域重要的密碼安全技術。其他像視覺密碼、數字媒體版權保護技術、隱寫術及隱寫分析、側信道攻擊方法、時間存儲折中方法、基於格基約化分析技術及其在公鑰密碼中的應用等等，皆可成為本期資訊安全通訊想要探討的議題。密碼技術及其相關領域的理論及應用最新研究成果、學術熱點、學術動態及發展趨勢，促進密碼學術交流與人才培養，促進密碼及資訊安全事業發展。歡迎更多研究者共同參與此主題。

以下僅列舉部分的相關主題，但徵稿論文不受此限

- * 對稱密碼算法設計及分析
- * 公鑰密碼算法設計及分析
- * 安全密碼協議
- * 密鑰管理
- * 密碼分析方法(如時間存儲折中攻擊、側信道攻擊、基於格基約化分析技術等)
- * 數字簽名與身份認證
- * 視覺密碼相關技術
- * 數字內容保護技術
- * 多媒體信息版權保護技術
- * 隱寫術及隱寫分析
- * 密碼應用

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，稿件需以 Microsoft Word 編輯，字體為 12 點標楷體(中文)或 times (英文)，總頁數在 20 頁以內，並請參閱資安通訊雜誌論文格式 <http://140.127.40.50/download/isc2.doc>
4. 投稿稿件請將含作者服務單位、聯絡地址、電話、傳真、email 信箱等之基本資料及投稿論文(論文內請勿含基本資料)email 至 Guest Editor 及本期刊編輯部。

重要日期：

論文投稿截止：103 年 12 月 10 日

論文接受通知：103 年 12 月 20 日

期刊發行日期：104 年 1 月

Guest Editor 聯絡方式

姓名：林東岱、劉峰

單位：中國科學院信息工程研究所

地址：北京市海澱區閔莊路甲 89 號

電子郵件：(ddlin,liufeng)@iie.ac.cn

本期刊編輯部聯絡方式

主編：王智弘 (wangch@mail.ncyu.edu.tw)

助理編輯：宋孝謙 (ccisa.editor@gmail.com)

CCISA: <http://www.ccisa.org.tw/>

