國立中山大學資訊工程學系
(07)5252-000 轉 4301, 4302, 4303
804 高雄市鼓山區蓮海路 70 號

每週演講心得分享 03

Weekly Seminar Memoir 03

官振傑 教授

Prof. Albert Guan

108 年 03 月 15 日(星期五)14:10~15:40
Mar. 15, 2019 (Fri.) 14:10~15:40
電資大樓 EC1009 室
EC 1009, Building of EE & CS

發布日期： 108 年 03 月 18 日

演講資訊

講題 TOPIC

植基於通道雜訊的不確定性之密碼協定
Cryptographic Protocols based on Unpredictable Channel Noise

主講人 SPEAKER

官振傑 教授/國立中山大學應用數學系
Prof. Albert Guan / Department of Applied Mathematics National Sun Yat-sen University

摘要 ABSTRACT

Security is an important issue in information systems and secure cryptographic protocols are essential tools for the security of information systems. Randomness plays an important role in the design of the security of cryptographic protocols. There are many sources to obtain randomness. Unpredictable noise in communication channel is a good source of randomness which can be used in many cryptographic protocols. In this talk, I will discuss how unpredictable noise in communication channel can be used in the design of some fundamental tools in cryptographic protocols. These protocols include: (1) Secret key establishment (2)Oblivious transfer, and (3)Bit commitment.

心得分享

黃正嘉

碩士班一年級，作業系統實驗室

這次演講主題是有關資訊安全，講師一開始先解說兩種資訊安全的模型: (1)計算安全 (2)無條件安全。前者是利用計算上的不可行來保護資訊，例如 RSA 的加密方式，透過對大整數做因數分解的難度，來提高加密訊息的可靠性，但這類型的技術通常需要繁重的計算，執行上得仰賴硬體的超強計算能力；後者則是即使有無限的計算能力，也會因為資訊量的不足，無法破解機密訊息，這樣的加密方式不需要複雜的計算，所以適合應用在物聯網的設備上，而講師也是主攻這方面的研究。

講師接著介紹有關這一方面的相關知識，像是 Bounded Storage Model，雖受限設備儲存能力有限，而透過傳輸大量的位元，接收端隨機存取某幾個位元，將資訊處理過後傳送給對方，並且取出交集，進而得到共有的金鑰；而 Noisy Channel Model 則是將通道內雜訊的干擾，利用接收端干擾程度不同進行運算，最後取得金鑰，使用這種方式無法預測，而且是一個很好隨機的來源。講師也將自己的研究應用在 Key establishment、Oblivious-Transfer 和 Bit commitment 等問題上，清楚且詳細的介紹每個問題並且提出解決方式。

資訊安全一直以來是個不容忽視的議題，量子電腦的出現又將掀起一波資訊新革命，感謝講師今天帶來精彩的演講和辛苦的研究成果，讓我們對密碼學有了更進一步的認識。

劉欣承

碩士班二年級，作業系統實驗室

今日講者一開始先說明演講綱要，從基本介紹到各項研究成果，金鑰建立、模糊傳送，解說如何才是安全的金鑰傳遞，其中提到雖然目前廣泛使用 RSA 加密方法，但是隨著時代演進，硬體設備的提升或量子電腦的產生都有可能造成安全性的影響。

講者也提到解密的困難在於需要分解大質數與解決離散問題，無法在有限的資源及時間內，解決計算量如此繁重的問題。接著講者開始說明有名的 Diffie-Hellman 的詳細流程、以及說明一些類似的相關研究，點出講者本身的研究重點在於隨機性建立安全的溝通架構。讓密碼協定的安全性計算變得不難解，是講者在研究上的貢獻，運算量只需要基本的運算單元，很適合在計算量很低的裝置，例如 IoT、通訊頻道上的雜訊。

接下來進入講者的研究重點，首先是金鑰的建立，他可以用很簡單的幾行算式，建立有效的安全金鑰，講者還以簡單的範例引導大家了解流程。金鑰建立完成後，再以兩張實驗數據圖表分析此研究方法的安全性，第一張可以發現不失安全性下有更好的建立方法，第二張是與其他方法的比較，讓我們更容易了解，不同方法是建立在哪些基礎概念上，以及他們分別有哪些優勢。

這次演講讓我受益良多，使我瞭解在金鑰的運作上，可以用十分簡單的運算方式達到雙方有效安全的溝通。

單　位：國立中山大學資訊工程學系
聯絡人：吳秀珍行政助理，分機 4301
　　黃莉萍行政助理，分機 4303
總　機：(07)5252000