達姆城科技大學(TU Darmstadt) 約翰那斯・布赫曼教授
(Professor Johannes Buchmann) 及他的研究團隊

一、約翰那斯・布赫曼教授(Professor Johannes Buchmann)的簡歷：

布赫曼教授是達姆城科技大學(TU Darmstadt)密碼學及計算代數(Cryptography & Computer Algebraic)研究團隊的帶領人，也是達姆城科技大學(TU Darmstadt)現任的副校長。布赫曼教授於 1953.11.20 生於科隆(Köln)，1974~1979 年於科隆大學(Universität zu Köln)修習數學、物理、哲學及教育，獲得碩士學位。1980~1982 年於科隆大學攻讀博士獲得科學博士學位。1985~1986 年獲得紅堡獎學金(Humboldt-Stiftung)到美國俄亥俄州州立大學研究進修。1986~1988 年於杜塞道夫大學數學研究所(Mathematischen Institut der Universität zu Köln)擔任教職，1988~1996 年於沙朗邦大學(Universität des Saarlandes)資訊系擔任教授(C3,C4 Professor)。1993 年獲得德國傑出科學研究獎(Leibnizpreis der Deutschen Forschungsgemeinschaft)，1995~1997 在美國及歐洲獲得 17 個研究獎項。1996 年至今擔任達姆城科技大學(TU Darmstadt)資訊系的教授(C4 Professor)。2000 年與其研究團隊共同創設了 FlexSecure 公司，爲達姆城科技大學移轉成立的公司，其產品主要爲關於與公開金鑰相關的資訊安全軟體。2001 年獲選爲達姆城科技大學的副校長擔任至今。2003 年獲選爲資訊安全應用技術學會的大會主席(CAST:Competence Center Applied Security Tecchnolgy)擔任至今。

二、約翰那斯・布赫曼教授(Professor Johannes Buchmann)研究團隊的特色：

1. 以基礎理論的研究爲主，但也含蓋部份實務的研究：
   布赫曼教授的學習過程、博士學位及初期的教職均是以數學爲主，其博士論文題目爲關於數論方面，而數論及代數爲密碼學及資訊安全的研究基礎及工具。所以其研究團隊的研究大都爲密碼學及資訊安全方面基礎且尖端的研究。但其團隊也有從事關於具彈性的公開金鑰環境及應用(Flexible Public-Key Infrastructures and Applications)的實務研究，這部份的研究成果成爲 FlexSecure 公司的技術及產品來源。
2. 研究目標明確且深入、踏實：
   在我於其研究團隊報告關於我的研究後布赫曼教授會後與我討論，他的第一個問題便是問我下一步的目標爲何？從布赫曼教授的網頁關於其研究內容的部分，我們可發現在每一個研究專案或研究小組其研究內容的介紹，除了研究題目他們首先交待的就是他們的目標(What we want)。在我報告關於我的研究後，他反覆詢問直到他能完全能掌握及了解爲止(完全不會不好意思)，可見其研究態度的深入、踏實。

3. 研究團隊國際化：
   布赫曼教授研究團隊成員有將近1/3的成員來自德國之外(目前26位中有8位)，來自蘇俄、希臘、台灣(我1位)、大陸、墨西哥及印度；之前還有來自美國及日本等國家，大都爲攻讀博士學位，也有少數像我們來短期爲學術交流的。
4. 培養優秀研究人才：
   或許是名師出高徒吧，這裡有許多傑出的研究人才，他們的研究成果常發表在密碼學及資訊安全國際頂級的會議(Conference)像 Crypto、EuroCrypto 及國際頂級的期刊(Journal)像 IEEE Transections 等。其中有一位日本人 Tsuyoshi Takagi 曾於此研究團隊攻讀博士學位，於 2001 年取得姆城科技大學(TU Darmstadt)的博士學位，或許是因爲研究能量的長期累積，也或許是名師出高徒吧，這裡產生許多傑出的研究人才，他們的研究成果常發表在密碼學及資訊安全國際頂級的會議(Conference)像 Crypto、EuroCrypto、AsciCrypto 及國際頂級的期刊(Journal)像 IEEE Transections, Journal of Cryptography 等。其中有一位日本人 Tsuyoshi Takagi 曾於此研究團隊攻讀博士學位，於 2001 年初取得姆城科技大學(TU Darmstadt)的博士學位，並於 2002 年(他 32 歲時)成爲不僅是姆城科技大學、也是全德國最年輕的助理教授(Juniorprofessor)。在他畢業前，有 6 篇 SCI journal (其中有一篇是 Journal of Cryptography)，有 9 篇國際 Conference (其中有 2 篇 Crypto, 1 篇 EuroCrypto, 1 篇 AsiaCrypto)。

5. 團隊相處融洽和諧：
   在其研究團隊中的博士生包括一位年輕的助理教授(Alexander May)，中午時候常互相邀約一同到學生餐廳用餐，氣氛融洽。每週有一次的工作會議，Professor Buchmann 大都親自主持，討論的項目不僅包括研究工作的部份，也包括一些生活方面需要討論的事項，例如這兩週有許多時間在討論關於 12 月 6 日的聖誕節 Party 的籌備；在此工作會議中的發言非常踴躍且常常充滿歡樂的笑聲。