姓名：呂及人

學歷：

美國麻州大學安城分校(University of Massachusetts at Amherst) (1999)

現職及經歷：

中央研究院資訊科學所副研究員（2003/10-present）

中央研究院資訊科學所助研究員（1999/8-2003/10）

國立暨南大學資訊工程學系助理教授（1999/2-1999/7）

著作名稱：

1. Chi-Jen Lu. Derandomizing Arthur-Merlin games under uniform assumptions. *Computational Complexity*, 10, pp. 247-259, 2001.

2. Chi-Jen Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: optimal up to constant factors. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC)*, pages 602-611, 2003.

3. Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1), pages 27-42, 2004.

中文簡介：

亂數在計算上，已成為一個有用的資源。利用亂數來幫助解決計算問題，已經成為一種廣泛被採用的方式。對於許多計算問題，隨機演算法(randomized algorithms)提供了最自然、最簡單、或最有效率的解決方法。然而一般隨機式演算法的設計，均假設有完美的亂數供其使用。然而電腦如何能產生完美的亂數？就連自然界是否存在完美的亂數源，也是一個值得爭議的問題。解決此困境的第一種方法，乃是研究如何將隨機式

演算法轉化成決定式演算法(deterministic algorithms)，而不至於大為降低其效率。第二種方法，乃是設計所謂的亂度萃取程序(extractors)，來由稍具亂度的弱亂數源中，萃取近乎完美的亂數，以供隨機演算法使用。

我的第一篇論文 [1] 研究第一種方法。隨機式演算法是否都可以完全轉化成確定式演算法？這乃是計算機科學界當前一個懸而未決的重要問題。我們在非確定式計算(nondeterministic computation)的模型上探討這個問題，而發現此問題與另外兩個看似無關的重要計算問題，有非常密切的關聯。我們一般相信，尋找問題的解答比驗證給予的解答，相對而言簡單的多。同樣的，尋找數學定理的證明比檢查證明的正確性，一般而言似乎簡單的多。但是真的是如此嗎？這是資訊科學中，最重要的 open problem 之一。我們發現若真是如此，那麼在非確定式計算的模型上，隨機式演算法都可以被有效率的轉化成確定式演算法。另一個問題，是計算中時間相對於空間的問題。在計算中，資訊在時間中的流動具有單一的方向性，但是在空間中則無此限制。故一般相信，計算中空間相對於時間，有較強的功能。但是真的是如此嗎？這至今仍是一個重要的 open problem 。我們發現若真是如此，那麼同樣在非確定式計算的模型上，隨機式演算法都可以被有效率得轉化成確定式演算法。

我的第二篇論文 [2] 研究第二種方法。亂度萃取程序利用一個非常短的亂數子(random seed)當催化劑，來由稍具亂度的弱亂數源中，萃取近乎完美的亂數。除了供隨機演算法使用之外，亂度萃取程序亦在其他如複雜度理論、資料結構、分散式計算、編碼理論、組合數學等領域，有不少的應用。他們在虛擬亂度(pseudo-randomness)的理論中，扮演了基本與統一性的角色。他們與計算機科學中的一些重要的基本概念，如 hash 函數、擴展圖(expanding graphs)、抽樣程序(samplers)、虛擬亂數產生器(pseudo-random generators)、錯誤更正碼(error correcting codes)等，也有相當密切的關係。由於其重要性，這方面的研究已有不短的歷史，並受到廣泛重視。我們建構出目前已知最佳的亂度萃取程序，從而解決了一個理論計算機科學中衆所矚目，歷經十多年緊密研究而仍然未解決的 open problem 。

我的第三篇論文 [3]，發現了亂度萃取程序在密碼學中，有出乎意料之外的應用。現今使用中的密碼系統，其安全性通常都有時效性，且隨著電腦科技的快速進展，其被破解的時間可能加快。最近Aumann、Ding 及 Rabin 提出一套通訊加密模式，在竊聽者擁有有限記憶容量的假設下，能保證具有永久的安全性(everlasting security)。此安全性質只根源於當今記憶容量的限制，而就算日後電腦軟硬體或密碼分析技術再發達，竊聽者亦仍然永遠無法得以破解。由於如此吸引人的安全性質，他們的成果立即受到廣泛的重視，並促使大家想要瞭解此安全性質看似神秘的本質。我們將此問題置於亂度萃取程序的研究架構中，證明任何亂度萃取程序皆可用來實現具有如此永久安全性的加密模

式。這指明了該問題背後的原理，而給予此問題一個穩固的理論基礎。多年來發展於亂度萃取程序的理論及技巧，如今都可以運用在此問題上。由此我們得以設計出新的加密程序，不僅具有永久安全性，其效率更遠高於已有的任何建構。

評審簡評：

呂及人博士的主要研究在「計算複雜度」(Computational Complexity)、「密碼學」Cryptography) 等計算機科學中，深具挑戰性且極重要的領域。

其代表作乃針對「計算複雜度」、「密碼學」極重要的問題，提出深具創新性的研究方法與結果。尤其是發表在 STOC 的論文，對於「密碼學」具有非常重要的貢獻及深遠的影響。評審委員提到，這篇論文是一項突破性(breakthrough)的研究成果，解決了在「亂度萃取方法」(Extractor)研究上，長久以來國際學術界公認的一重要 open problem。此結果建構出目前已知最佳的亂度萃取方法。這項成果可說是Extractor多年的研究中，最令人振奮的發展(most exciting development)。這項針對亂度萃取方法的研究成果，除了「密碼學」的直接應用外，對於計算機科學的其他重要領域，包括「計算複雜度」、「資料結構」、「分散式計算」等，均有深遠的影響。

對於呂及人博士的整體表現，評審委員予以高度肯定。委員指出，歷年來呂及人博士的論文發表在 STOC 、SODA 、CRYPTO、 SIAM J. Computing 等國際頂尖會議及期刊。他的研究非常深入，具有一流的研究能力。研究成果在國際舞台上，已獲得高度的肯定與讚賞。

綜合上述 ，呂及人博士的研究成果 ，在「計算複雜度」以及相關領域已產生極重要的貢獻與影響力，研究已具有世界級的水準。