鐘楷閔

中央研究院資訊科學研究所研究員

代表著作：

- T-H. Hubert Chan, **Kai-Min Chung***, Elaine Shi, 2017, "On the Depth of Oblivious Parallel RAM", *The 23rd Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2017)*, 31.
- Elette Boyle, **Kai-Min Chung***, Rafael Pass, 2016, "Oblivious Parallel RAM and Applications", *The 13th IACR Theory of Cryptography Conference (TCC 2016)*, 30.
- Yu-Chi Chen, Sherman S. M. Chow, **Kai-Min Chung***, Russell W. F. Lai, Wei-Kai Lin, Hong-Sheng Zhou, 2016, "Cryptography for Parallel RAM from Indistinguishability Obfuscation", *The 7th Innovations in Theoretical Computer Science (ITCS 2016)*, 12.

簡評：

鐘博士的專長領域為密碼學、複雜度理論與量子理論，在密碼學領域上有非常傑出的表現，多次在由國際密碼研究協會所舉行的 TCC 及 AISACRYPT 等重要會議發表論文，對於我國推動密碼與資安的基礎研究有重大效益，同時亦提升我國密碼學領域在國際間的地位。三篇代表論文聚焦在平行計算模式下的資料加密。傳統資料加密模型多考慮循序運算模型，但是平行計算、分散計算與量子計算已日益成熟，在平行運算模式下的密碼學及多方安全計算益形重要，鐘博士的論文在平行計算的安全計算議題具有學理原創性，讓許多傳統需要用到大數計算（例如超過 1024 bits 以上）的密碼演算法，透過平行運算程式及搭配的編譯程式可以獲得實現，運算速度可以大幅獲得改善，兼具理論及實務應用的貢獻。

簡歷：

Kai-Min Chung received his Ph.D. from Harvard University in 2011 under the supervision of Salil Vadhan. After his Ph.D., he worked with Rafael Pass as a postdoctoral researcher at Cornell University for three years and supported by Simons postdoctoral fellowship in 2010-2012. He joined the Institute of Information Science, Academia Sinica as an assistant research fellow in 2013 and became a research fellow in 2020.

Kai-Min's research interests lie in the field of cryptography and its interplay with quantum and complexity theory. He has contributed to several lines of research in classical cryptography such as cryptography for parallel computation models, zero-knowledge proofs, and delegation of computation. In recent years, his research gradually focuses more on the interdisciplinary field of quantum cryptography, where he has worked on several topics such as device-independent randomness amplification, security in the quantum random oracle (QROM) model, and classical verification of quantum computation. He also enjoys applying cryptographic techniques to study other fields in theoretical computer science. For example, he applied cryptographic techniques to study the complexity of classical-quantum hybrid computations with bounded quantum depth and the massively parallel computation model.

代表作簡介：

Cryptography in Parallel RAM (PRAM) Model

Background & Approach:

In cryptography, a central question is how to carry out desired computation with desired security (e.g., MPC & Delegation in Fig 1, 2). The computation is typically expressed as a circuit, and recent works consider RAM model of computation (see Fig. 3). However, both models do not capture either random data access or parallelism, and may suffer significant efficiency loss (cf. Fig. 4). We suggested to develop the theory of cryptography in the Parallel RAM (PRAM) model, a model captures both random data access and parallelism.

Outcome & Significance:

We made major contributions in developing the theory of cryptography in the PRAM model.

We initiated the study by introducing and constructing Oblivious PRAM (OPRAM). We showed general feasibility that under sufficiently strong cryptographic assumptions, many important primitives, such as delegation schemes, secure multiparty computations (MPC), and functional encryptions (FE), could be constructed in the PRAM model. Finally, we further investigated whether there is an inherent parallel runtime overhead for OPRAM compilers and resolved the question by establishing nearly tight upper and lower bounds.

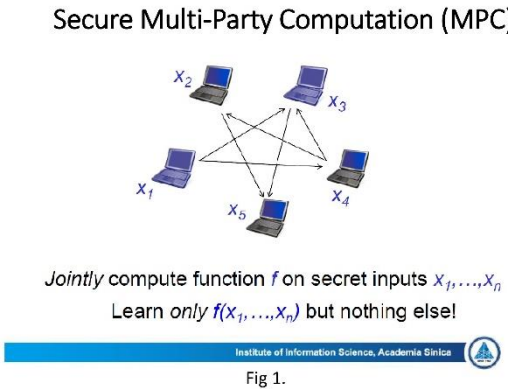

Fig 1.

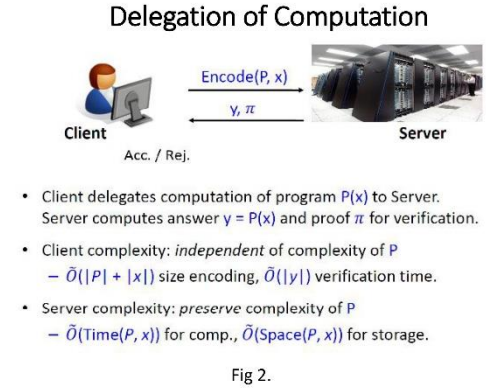

Fig 2.

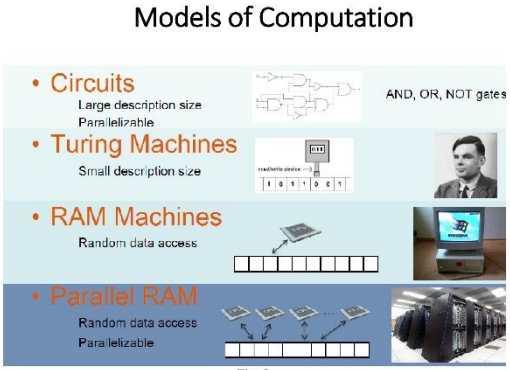

Fig 3.

Efficiency Gap

Problem	Comp. Model	Total Time	Parallel Time
Binary search (input size n)	Circuit	$\Omega(n)$	
	RAM	$O(\log n)$	
Sorting	Circuit		$O(\log n)$
	RAM		$\Omega(n\log n)$
Keyword search/ Range query (output size m)	Circuit	$\Omega(n)$	$O(\log n)$
	RAM	$O(m\log n)$	$\Omega(m\log n)$
	PRAM	$O(m\log n)$	$O(\log n)$

Institute of Information Science, Academia Sinica

Fig 4.

得獎感言：

非常感謝中研院年輕學者研究著作獎的肯定。我也要十分感謝中研院長期以來提供充分的研究資源、完全自由的研究環境與種種支持，讓我能心無旁騖的研究我最感興趣的理論課題。另外，我要感謝在我過去求學階段指導與幫助過我的師長，許多關鍵的幫助與指引讓我能順利的走向我熱愛的研究道路。當然我也要感謝家人的陪伴與支持，讓我能沒有後顧之憂的堅持我的學術研究。在這快與「年輕」兩字告別的時間點，也期許自己能將對過去的種種感謝，化為對未來年輕研究者的支持。