DOI:10.1145/3378428

RAPHAËL CW PHAN
Monash University, Malaysia

MASAYUKI ABE
NTT, Japan

LYNN BATTEN
Deakin University, Australia

JUNG HEE CHEON
SNU, Korea

ED DAWSON
QUT, Australia

STEVEN GALBRAITH
University of Auckland, New Zealand

JIAN GUO
NTU, Singapore

LUCAS HUI
ASTRI, Hong Kong

KWANGJO KIM
KAIST, Korea

XUEJIA LAI
SJTU, China

DONG HOON LEE
Korea University, Korea

MITSURU MATSUI
Mitsubishi Electric, Japan

TSUTOMU MATSUMOTO
YNU, Japan

SHIHO MORIAI
NICT, Japan

PHONG NGUYEN
University of Tokyo, Japan

DINGYI PEI
Guangzhou University, China

DUONG HIEU PHAN
University of Limoges, France

JOSEF PIEPRZYK
CSIRO Data61, Australia

HUAXIONG WANG
NTU, Singapore

HANK WOLFE
University of Otago, New Zealand

DUNCAN WONG
CryptoBLK, Hong Kong

TZONG-CHEN WU
NTUST, Taiwan

BO-YIN YANG
Academia Sinica, Taiwan

SIU-MING YIU
HKU, Hong Kong

YU YU
SJTU, China

JIANYING ZHOU
SUTD, Singapore

Members of the International Association for Cryptologic Research explore regional work and collaboration activities.

Advances in Security Research in the Asiacrypt Region

THE CRYPTOGRAPHIC AND security research community is very closely knit in the sense that irrespective of which country we are in, or which region we come from, we are aligned to a single formal association—the International Association for Cryptologic Research (IACR). Regional flagship IACR conferences allow fellow researchers to gather regularly. The three main

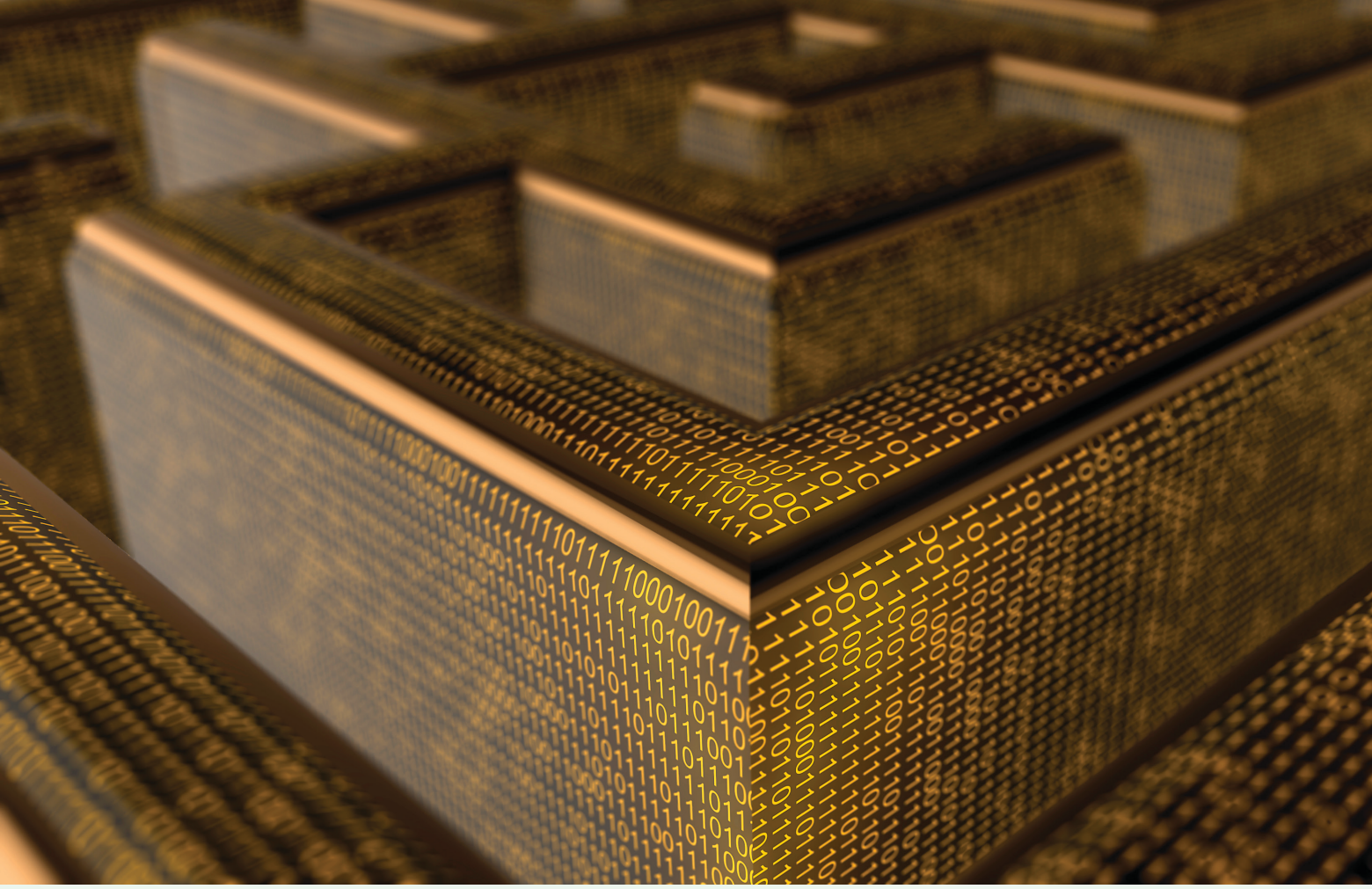

IMAGE BY IMMERSION IMAGERY

regions hosting security research conferences are the U.S. (Crypto), Europe (Eurocrypt), and Asia + Oceania (Asiacrypt). These events provide a sense of belonging and are one main reason researchers continually involve themselves in such regional activities. In this article, we focus on regional collaborative activities as well as highlight each country's security research.

Asiacrypt. In 1990, the first Auscrypt was held in Sydney, spearheaded by Jennifer Seberry and Josef Pieprzyk, both of UNSW. The aim was to have a regional collaborative venue similar in style to Crypto and Eurocrypt, both of which started in the 1980s. In 1991, Japanese cryptographers initiated Asiacrypt in Fujiyoshida as the first crypto conference in Asia. It was organized by Hideki Imai (YNU), Ron Rivest, and Tsutomu Matsumoto. After Auscrypt 1992 at Gold Coast, Australian cryptographers combined Auscrypt into Asiacrypt by hosting Asiacrypt 1994 in Wollongong. As a bi-annual conference, Asiacrypt 1996 and Asiacrypt 1998 were hosted in Korea and China, respectively; followed by Asiacrypt 1999 in Singapore. Subsequently a strong suggestion was made to IACR by the Asiacrypt Steering Committee for the conference to be held annually. As a result, Asiacrypt has been the annual IACR flagship conference for the Asian region since 2000 and holds the same status within the industry as the Crypto and Eurocrypt conferences. Each year, more than 200 papers are submitted to Asiacrypt of which about one-third are selected by multiple peer review to be published in the proceedings. Attendance on average has been over 250 participants.

Australia and New Zealand. In 1996, the first Australasian Conference on Information Security and Privacy (ACISP) was held in Wollongong and organized by Josef Pieprzyk and Jennifer Seberry. The event is designed to complement, not to compete with, Asiacrypt. The concept of an Australia-New Zealand security conference was to encourage researchers to communicate and provide feedback to develop strong papers suitable for Asiacrypt and journals in various areas of information security and privacy. The venues move around universities and cities in Australia and New Zealand in order to encourage inclusiveness.

Japan and Korea. There are workshops jointly organized with countries in Asia. The Japan-Korea Joint Workshop on Information Security and Cryptology (JW-ISC) was initiated by major research institutes in Japan and Korea in 1993. It was later extended to the Asia Joint Conference on Information Security (AsiaJCS) in 2005. These events provide opportunities for young researchers in Asia to extend their activities by giving talks to international audiences and exchanging their ideas with invited experts.

Country-Specific Initiatives for Security and Crypto

China. In 2005, the State Key Laboratory of Information Security (SKLOIS) of the Chinese Academy of Sciences organized the first international conference on Information Security and Cryptography (Inscrypt, formerly CISC) in Beijing. ChinaCrypt is another major crypto event organized by the Chinese Association for Cryptologic Research (CACR) since 2007.

ChinaCrypt is the biggest regional

Regional collaboration map based on IACR flagship conferences (CRYPTO, Eurocrypt, Asiacrypt) for the last six years 2019–2014.

	2019	2018	2017	2016	2015	2014
Australia	C		C	C		S
China	AHJS	JKS	AJS	AJS	J	JKS
Hong Kong	C		T			
Japan	C	CS	CS	CS	C	CS
Korea		C				CS
Singapore	CT	CJ	CJ	CJ		ACJK
Taiwan	S		H			

forum for Chinese researchers and practitioners in cryptography where talks are given in Chinese except for non-Chinese invited speakers. At each conference, organizations on behalf of their cities bid to host the next year's ChinaCrypt, voted by the CACR committee. In 2018, CACR initiated the National Cryptographic Algorithm Design Competition to solicit and evaluate innovative cryptographic algorithms nationwide. In September 2019, 24 proposals advanced to the second round; and winners will be announced in 2020. The Chinese National Standards for cryptographic algorithms currently in use include the SM2, SM3, SM4, and SM9 that correspond to algorithms for public-key cryptography, cryptographic hash functions, block ciphers, and identity-based cryptography, respectively. SM2, SM3, and SM9 have acquired international recognition under ISO/IEC14888-3/AMD1 and ISO/IEC10118-3:2018.

Hong Kong. The Centre for Information Security and Cryptography (CISC) was formally established in HKU in 1998. Since then, cryptography became a major research area in Hong Kong. Besides contributions to many fundamental cryptographic primitives, researchers in Hong Kong were among the first to apply cryptographic techniques in various application areas such as education, digital forensics, privacy-preserving computations in VANET (vehicular ad hoc network), smart grids, bioinformatic computations, and recently on blockchains and cryptocurrencies. In 2017, Asiacrypt was held in Hong Kong for the first time.

Japan. The three-year Cryptography Research and Evaluation Committees (CRYPTREC) was organized in 2000 to evaluate cryptographic techniques publicly applied and widely used in industries and select those that excel in security and implementation. In 2003, the Ministry of Internal Affairs and Communication and the Ministry of Economy, Trade, and Industry publicized the list of ciphers recommended for the procurement of e-government. Annual symposiums, known as the Symposium on Cryptography and Information Security (SCIS) since 1984 and the Computer Security Symposium (CSS) since 1998, are organized by local research communities, the Institute of Electronics, Information and Communication Engineers (IEICE) and Information Processing Society (IPSJ) in Japan, respectively. These symposiums have jointly attracted over 1,200 participants in recent years.

Korea. The Korea Institute of Information Security and Cryptology (KIISC) was established in 1990 by the government to promote the academic advancement of information security and cryptology. KIISC organizes two domestic annual conferences every summer and winter, and since 1998 timed the annual International Conference on Information Security and Cryptology (ICISC) to occur a week before Asiacrypt. In 2000, KIISC began hosting the Workshop (now renamed World Conference) on Information Security Application (WISA) to bridge academia and industries, focusing on the practices and applications of information security and cryptology. WISA has been consistently co-sponsored by the Ministry of Science and ICT (MSIT), the Korea Internet and Security Agency (KISA), the National Security Research Institute (NRI), the Electronics and Telecommunications Research Institute (ETRI) and the leading domestic security industries. Korea has its own block-cipher standards—SEED, ARIA, and HIGHT—for domestic applications listed in the international standard. KIISC has hosted Asiacrypt (1996, 2004, 2011), FSE 2010, and CHES2014, and will be hosting Asiacrypt2020 and PQCrypto2021.

Malaysia. The inaugural Mycrypt

Asiacrypt 2019, Kobe, Japan.

Asiacrypt 2020, Daejeon, South Korea.

was pioneered by Raphaël Phan in 2005 to expose the local security community to the culture of international crypto conferences. Held in Kuala Lumpur, the program chairs were Serge Vaudenay and Ed Dawson (QUT) and featured an unconventional cryptography session spotlighting a paper on the new notion of questionable encryption by Adam Young and Moti Yung. Subsequently, Phan led the bidding team to host Asiacrypt in Malaysia for the first time in 2007. This was held in Kuching in the Borneo state of Sarawak. Mycrypt was rejuvenated in 2016, focusing on paradigm-shifting unconventional crypto, with Phan and Yung as the program chairs. In terms of government initiatives, the Malaysian government agency CyberSecurity Malaysia initiated in 2016 an effort similar to CRYPTREC (Japan) to propose a list of trusted cryptographic algorithms for Malaysia. MySEAL produced a recommended list of existing algorithms in 2017.

Singapore. In 2018, two multidisciplinary research centers each funded by a $10 million grant from the National Research Foundation of Singapore were set up under Nanyang Technological University (NTU) and National University of Singapore (NUS), respectively. The centers are to develop capabilities, technologies, and skilled manpower toward scalable and customized privacy preserving technologies that are aligned with national priorities of Singapore in the services and digital economy of the Research, Innovation, and Enterprise (RIE2020) plan.

Taiwan. Taiwan's burgeoning cryptographic community hosted Asiacrypt 2003 and 2014. Taiwan is known for specialties in post-quantum cryptography and cryptographic implementations. For example, Bo-Yin Yang (Academia Sinica) was the co-inventor of Ed25519, a widely used elliptic curve digital signature scheme, which is a de facto standard on the Internet, and of which the U.S. National Institute of Standards and Technology (NIST) has said will be part of the U.S. standard FIPS 186-5. Taiwanese scholars contributed to the multivariate digital signatures MQDSS and Rainbow in the second round of the NIST post-quantum standardization process.

Vietnam. The Vietnam Cryptographic Branch was formed in 1945 soon after independence, and the development of cryptography was exclusively realized by the government's secret agencies such as the Ban Co Yeu (Cryptographic Bureau). The first official collaboration between a secret agency and a public research institute occurred in 1987 in a project called M-87, led by Phan Dinh Dieu (VNU)—the founder of the Vietnamese IT Society. Since then, research in cryptography has increased in public institutions as well as public universities where cryptography/security courses were created. The first international cryptology conference in Vietnam (Vietcrypt) was held in 2006, led by Vietnamese researchers abroad: Khanh Nguyen (Singapore), Phong Nguyen and Duong Hieu Phan (France) and Duy Lan Nguyen (Australia) and supported by Phan Dinh Dieu (as general chair). Vietcrypt attracted numerous prominent cryptographers including Jacques Stern, Tatsuaki Okamoto, Phil Rogaway, and inspired new young students to follow cryptography research. Subsequently, Vietnam hosted its first Asiacrypt in 2016, led by Duong Hieu Phan as one of the general chairs, along with Ngo Bao Chau (VIASM).

Asiacrypt has been the annual flagship conference for the Asian region since 2000 and holds the same status within the industry as the Crypto and Eurocrypt conferences.

Security Research Highlights of the Asiacrypt Region

Australia. The pioneers of Australian crypto include Jennifer Seberry (Wollongong) and Ed Dawson (QUT) who have made research contributions to the field of symmetric cryptography. Yuliang Zheng (Monash) introduced the signcryption notion in 1997, which to date has been cited over 1,500 times. The aim of signcryption is to provide both confidentiality and authentication of messages more efficiently than by independent encryption and signing, by means of intertwining both cryptographic operations. Josef Pieprzyk (Macquarie) in joint work with Nicolas Courtois that has been cited over 1000 times, proposed a method to break ciphers whose S-boxes can be expressed by an over-defined system of algebraic equations. Desmedt,

Research collaborations in the Asiacrypt region actively occur among security researchers and cryptographers.

Pieprzyk, Steinfeld (Macquarie), and Wang at Crypto 2007 studied the secure n-party computation in the passive, computationally unbounded attack model of the n-product function $f_G(x_1,...,x_n)=x_1 \cdot x_2 \cdots x_n$ in an arbitrary finite group $(G, \cdot)$, where the input of party P_i is $x_i \in G$ for $i=1,...,n$. The problem of constructing such protocols was reduced to a combinatorial coloring problem in planar graphs. Ron Steinfeld (Monash) is one of Australia's leading researchers in lattice cryptography and homomorphic encryption. His papers with Stehlé at Asiacrypt 2010 and Eurocrypt 2011 have been influential to lattice cryptography using cyclotomic rings and made major inroads to the efficiency of homomorphic encryption. Lynn Batten (Deakin) and Xun Yi (RMIT) have made considerable contributions to privacy-preserving digital cash, notably the first detailed analysis of e-commerce-based personal information distribution from the purchaser viewpoint and solving the change-giving problem; as well as to privately querying aggregated medical data such that the privacy of the data, the query, the querier, and data owner are guaranteed simultaneously.

China. Xiaoyun Wang (Shandong) at Crypto 2005 broke the established hash functions SHA-0, SHA-1 (cited over 1,800 times), following her earlier work at Eurocrypt 2005, which broke the hash function MD5 (cited over 1,700 times) used in many commercial systems.

Japan. Within symmetric cryptology, Mitsuru Matsui (Mitsubishi) introduced the technique of linear cryptanalysis, which was the first attack that effectively broke the Data Encryption Standard (DES); this work has been cited in excess of 3,300 times and remains one of the top cryptanalysis techniques to guard against any new cipher designs. More recently, Yosuke Todo (NTT) invented the cryptanalytic technique of division property-based integral attack, which has broken the full rounds of the MISTY-1 cipher that had been proven secure against two top attack techniques, that is, differential and linear cryptanalysis. Tetsu Iwata (Nagoya) and Kaoru Kurasawa (Ibaraki) designed the one-key CBC MAC (OMAC1 aka CMAC) block cipher-based message authentication code (MAC), which has made the CRYPTREC list and specified as NIST SP 800-38B.

For the context of public-key crypto, the Fujisaki-Okamoto (NTT) at Crypto 1999 is a well-known technique to upgrade the security of public-key encryption schemes from chosen plaintext resistance to adaptively chosen ciphertext security. It has been cited close to 1,000 times to date. The Okamoto identification scheme at Crypto 1992 is the first identity scheme that withstands adaptive attacks in the random oracle model, by proposing a new way of embedding an instance of the discrete-logarithm problem in the security proof. The notion of structure-preserving signatures (SPS) was introduced by Abe (NTT), Fuchsbauer, Groth, Haralambiev, and Ohkubo (NICT) at Crypto 2010. SPS is a proof-friendly signature scheme over pairing groups allowing to efficiently prove signatures without explicitly showing the signature, the message nor the verification key. It is used as a building block in privacy-preserving cryptographic protocols such as anonymous credential systems. Sakai, Ohgishi, and Kasahara developed the first identity-based key exchange scheme in 2000, which is the first constructive application of pairings over elliptic curves that preceded the first identity-based encryption (IBE) scheme by Boneh and Franklin in 2001. This opened the door to pairing-based cryptography that is widely deployed in real-world applications now. Tatsuaki Okamoto (NTT) and Katsuyuki Takashima (Mitsubishi) at Asiacrypt 2009 introduced a technique called dual pairing vector spaces that extends pairing groups to a vector space. It was a breakthrough to many applications such as attribute encryption and functional encryption scheme. In the context of real-world security, Tsutomu Matsumoto et al. (YNU) in their work that has been cited over 1,000 times, showed the surprising result that fingerprints artificially copied on silicone rubber fingers could effectively cheat fingerprint identification

systems, leading to a new research direction of liveness detection for fingerprint systems.

Korea. Kwangjo Kim et al. (KAIST) suggested a set of DES S-boxes that can be resistant against differential cryptanalysis and linear cryptanalysis (Asiacrypt 1991). Jung Hee Cheon et al. (SNU) developed cryptanalytic techniques for the CLT13 (Eurocrypt 2015) and CLT15 (Eurocrypt 2016) multilinear maps, as well as against the obfuscations based on the GGH13 (CRYPTO 2018) and GGH15 (Crypto 2019) multilinear maps. Cheon et al. also contributed substantially to solving variants of the discrete log problem (DLP), which directly affects the hardness of many security systems, as well as designed the first-known homomorphic encryption operating on real numbers that was subsequently used for privacy-preserving machine learning (Asiacrypt 2017). Korean researchers have also contributed substantially to research on broadcast encryption with improved efficiency (computation and transmission), identity-based encryption, and functional encryption with extra features such as tighter security reduction, revocability, and reduced key size, as well as on authenticated key exchange protocols including features such as dynamic grouping and forward secrecy.

Malaysia. Cryptographic research in Malaysia dates back to the early 2000s, and throughout the last two decades, the cryptographic community of actively publishing researchers in Malaysia remains largely the same. Main novel contributions from the community include new types of block cipher cryptanalysis techniques (double slides, realigning slides, overlapping multiset attacks, and bitslice tuple attacks) by Raphaël Phan, cryptanalysis of provable security (Phan, Bok-Min Goi and Wei-Chuen Yau), and variants of identification schemes by Swee-Huay Heng et al.

New Zealand. Early pioneers of information and computer security research in New Zealand include Hank Wolfe (Otago), Lech Janczewski (Auckland), Ray Hunt (Canterbury), Peter Gutmann (Auckland), and Ian Welch (Victoria). Theoretical research in cryptography began with the return to New Zealand of Steven Galbraith (Auckland). Quantum computers, if they can be built to run Shor's algorithm at large scale, will break most public key cryptosystems in widespread use today. Two major research directions in post-quantum crypto are lattice crypto and isogeny crypto, based on mathematical problems that cannot be solved by Shor's algorithm. Galbraith is a major contributor to lattice cryptanalysis and introduced a significant optimization to lattice signatures, which has been used in submissions to the NIST PQCrypto standardization process. In isogeny crypto, Galbraith is a leading researcher—he illustrated an adaptive attack on isogeny crypto that has widely influenced the field (Asiacrypt 2016), and has made major advances (Asiacrypt 2017, Eurocrypt 2019) in isogeny signatures.

Singapore. Jian Guo (I^2R), Thomas Peyrin (NTU), and Axel Poschmann (NTU) designed the PHOTON lightweight hash function family (Crypto 2011), which was adopted as an ISO standard in 2016. Hongjun Wu's (NTU) hash function design JH was selected as one of the five finalists of the SHA-3 competition in 2011; Hongjun Wu's authenticated encryption schemes ACORN and AEGIS, as well as Deoxys-II co-designed by Ivica Nikolić (NUS) and Thomas Peyrin (NTU) were selected as the final winners of the CAESAR competition in 2019. NTU's Jian Guo, Thomas Peyrin, and Hongjun Wu also contributed significantly on the cryptanalysis of symmetric-key primitives. Joseph Liu and Jianying Zhou et al. designed a lightweight identity-based signature scheme, which was adopted as an ISO standard in ISO/IEC 29192-4 in 2013. Yanjiang Yang and Jianying Zhou et al. designed password-based anonymous entity authentication scheme, which was adopted as an ISO standard in ISO/IEC 20009-4 in 2017.

Cross-Country Research Collaborations

Research collaborations in the Asiacrypt region actively occur among security researchers and cryptographers. To showcase this, consider the papers published for the IACR flagship conferences—Crypto, Eurocrypt and Asiacrypt—in recent years. The accompanying table gives the summary of joint papers published in the past six years at these three main venues that involved researchers across multiple Asiacrypt countries, and if so, which countries they collaborated with. China actively collaborates, mainly with Australia, Japan, and Singapore. Moreover, Japan and Singapore also collaborate closely.

Ideas for even closer collaborations. Besides the practice of East Asia and Oceania countries taking turns hosting the flagship Asiacrypt conference, and cross-country research collaborations and joint publications, the following ideas could further strengthen collaborations and are worth exploring:

- Joint Ph.D. studentships among Asiacrypt universities: Universities in Asiacrypt countries could devise jointly supervised and jointly awarded Ph.D. degrees wherein the Ph.D. student spends a year in a host university where the co-supervisor is based.
- Research visits co-located with Asiacrypt: Arrange co-located research visits before and after Asiacrypt to be hosted by universities in the Asiacrypt-hosting country. This way, researchers aiming to attend Asiacrypt could leverage the trip as a research visit to a university in that country before or after the Asiacrypt period.

References

1. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystem. In *Proceedings of 1990 Crypto*, 2–21.
2. Courtois, N. and Pieprzyk, J. Cryptanalysis of block ciphers with overdefined systems of equations. In *Proceedings of 2002 Asiacrypt*, 267–287.
3. Fujisaki, E. and Okamoto, T. Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of 1999 Crypto*, 537–554.
4. Matsui, M. Linear cryptanalysis method for DES cipher. In *Proceedings of 1993 Eurocrypt*, 386–397.
5. Matsumoto, T. Gummy and conductive silicone rubber fingers. In *Proceedings of 2002 Asiacrypt*, 574–576.
6. Wang, X., Yin, YL., and Yu, H. Finding collisions in the full SHA-1. In *Proceedings of 2005 Crypto*, 17–36.
7. Wang, X. and Yu, H. How to break MD5 and other hash functions. In *Proceedings of 2005 Eurocrypt*, 19–35.
8. Zheng, Y. Digital signcryption or how to Achieve cost (signature and encryption)<<cost(signature) + cost(encryption). In *Proceedings of 1997 Crypto*, 165–179.

For information regarding this article, contact Raphaël CW Phan, raphael.phan@monash.edu.