RESEARCH GRANTS COUNCIL

Application for Allocation from the Research Impact Fund (RIF) for 2019 / 20 Preliminary Proposal

- The preliminary proposals should provide sufficient information about the proposed project to allow assessment of the main ideas and approaches.
- All project information must follow the format specified in the application form. Failure to comply with the application format and/or the allowable page may lead to disqualification of the proposal.
- To safeguard the interests of the researcher and the university, the awardee university bears the primary responsibility for prevention, detection and investigation of research misconduct, including but not limited to misuse of funds, data falsification, plagiarism and double-dipping. The university is strongly encouraged to vet the applications using anti-plagiarism software before submitting them to the RGC.

PART I RESEARCH PROPOSAL

[To be completed by the applicant(s)]

1. Particulars of the Project

(a)(i) Name and Academic Affiliation of Applicants:

Role	Name (with title) / ORCID iD	Post	Unit / Department / University / Institution	Current Member of RGC / Subject Panel as at application deadline (Yes / No)	RGC / Name of RGC Subject Panel	Number of Hours Per Week to be spent by the PC and each Co-PI on the Project
Project Coordinator [PC]:	Dr Au Man Ho Allen / 0000-0003-2068-9530	Assistant Professor	Department of Computing / The Hong Kong Polytechnic University	N		8
Co-Principal Investigator [Co-PI]:	Dr Liu Joseph / 0000-0001-6656-6240	Associate Professor	Faculty of Information Technology / Monash University	N		6
	Prof Lu Haitian / 0000-0002-7627-2454	Professor	School of Accounting and Finance / The Hong Kong Polytechnic University	N		6
	Dr Luo Daniel Xiapu / 0000-0002-9082-3208		Department of Computing / The Hong Kong Polytechnic	N		6

			University		
	Dr Wang Cong / 0000-0003-0547-315X	Associate Professor	Department of Computer Science / City University of Hong Kong	N	6
Organisational Partner:	Miss Lee Fong Cing /	CEO	/ Qin Qin Health International Limited		-
	Mr Lin Yanjun /	CEO	/ 9F		-
	Dr Ma Lawrence /	Director	/ Valigo Limited		-

(ii) Title of Project (in English and Traditional Chinese)

Practical Zero-Knowledge Proof: Theory and Applications

實用零知識証明：理論與應用

(iii) Nature of Application

☑ New ☐ Re-submission *Reference no. of relevant project: Funding scheme* ☐ Renewal *Reference no. of relevant project: Funding scheme*

(b) (i) Primary Field: Others - Computing Science & Information Technology(this project is about information security in computer science) & Code 2299
Secondary Field: Computer Science Fundamentals & Code 2202

(ii) A maximum of five sets of keywords to characterise the work of your proposal
(a maximum of 30 characters for each set of keywords)
1) Information Security
2) Privacy-Preserving Technique
3) Zero-Knowledge Cryptography
4) Cryptographic Proof System

(iii) Project Duration : 36 Months

(iv) Funding Requested

Total cost of the project: $ 5,000,000

Less

Matching fund provided by university:	$ 800,000
Matching fund provided by partner(s), if any: *(Should be on 70% (RGC)(excluding on-costs) / 30% (university/partner(s)) basis)*	$ 700,000
Net amount requested from RGC: (exclusive of on-costs)	$ 3,500,000

(b) Project Objectives
[Please list the objectives in point form]

1. To design a zero-knowledge proof generator for ARM program
   We plan to investigate methods to construct a zero-knowledge proof for correct execution an ARM program. More precisely, we will explore the techniques of constructing traditional zero-knowledge proof from group elements, and apply it into our setting.

2. To design a compiler supporting the compilation of C program to ZKP-friendly ARM program
   We plan to design a compiler that can compile any C program into the instruction sets of ARM architecture. In particular, our compiler takes any C program as input, then outputs an instruction set of ARM while keeping the functionality of the original C program. Moreover, the desired compiler is universal which supports the compilation of any C programs into ARM program that is ZKP-friendly.

3. To investigate various enhancements and develop a baseline solution
   We will consider several enhancement, including succinctness and post-quantum security of ZKP. We will also explore the use of hardware-assisted secure computing platform to develop a baseline solution.

4. To develop a privacy-preserving digital identity system prototype
   We plan to develop a self-sovereign digital identity system which allows the identity owners, the identity certification authorities (or validator) and the identity inspectors to create, certify, verify and manage identity in a secure, privacy-friendly and efficient fashion.

5. To develop a privacy-preserving digital health platform prototype
   We plan to develop a digital health platform which connects medical practitioners, clinics and clients in a privacy-friendly manner. It will also support controlled-sharing of health records.

6. To develop an automated compliance checking tool prototype
   We envision the use of AI in the law, account and auditing industry will become popular. Instead of requiring the service user to release its data for these AI compliance check to be executed, we plan to investigate the possibility of to executing the AI application locally to produce a short certificate, which could be verified within a short time to improve efficiency and also prevent malicious tampering of the AI application.

3. Pathways to Impact Statement
[a maximum of two A4 pages]

Project Summary

This project will explore ways to make zero-knowledge proof (ZKP), one of the most abstract and fascinating innovations for data privacy, practical and usable. Although ZKP is still an emerging technology, its security is well-studied, and there has been substantive and continuous progress in making it more practical in terms of performance. However, ZKP is extremely complex to implement and deploy; and the task to render ZKP programmer-friendly is largely left unexplored. This project aims to address to pain point so more industrial applications can enjoy better data privacy through the use of ZKP.

The Challenge

In the technology era, data privacy is an important subject. This is particularly relevant when tech giants are leveraging the vast amount of (sensitive) data they collect every day to their advantage. As such, innovative technologies that protect data privacy, such as ZKP, are receiving increased interest every day. Prototypes supporting ZKP are being adopted from the finance industry for their fintech applications, including the recent launch of ZKP solutions from Ant Financials, ING Bank, JPMorgan and EY.

In a nutshell, ZKPs allow one party to prove the truth of a statement to another party without revealing any extra information. It's fascinating and very counterintuitive nature makes it the ideal technological solution to meet regulatory requirements of open data and protect their privacy at the same time. Yet, it is extremely challenging to apply this cutting-edge technology in practice for two reasons. Firstly, the technology is non-trivial to explain, extremely complex and highly theoretical. Secondly, there is a serious lack of tools to build applications with ZKP.

Pathway to Impact

This proposal has been co-produced with academia from the area of computer science and Law & Finance, as well as industry partners focusing on fintech, digital health, insurance and audit. We plan to co-produce several impactful research outcomes that will provide a measurable benefit to technology companies, practitioner and communities concerns with data privacy. The impact goals are listed below:

- Design ZKP for an instruction set suitable for various application scenarios;
- Critically evaluate and recommend alternative solutions to existing applications with better data privacy protection through the use of ZKP;
- Provide evidence that ZKP can be used to handle various complex applications scenarios for privacy-protection by developing prototypes in digital identity management, digital health and AI-enhanced accounting;
- Develop cost-effective and easy-to-use tools for system developers to build applications with ZKP to enhance its data privacy protection.

Stakeholder Engagement

Stakeholders of this project can be broadly grouped as follows: (1) academia, (2) regulator, law-enforcing agent, (3) standardization bodies, (4) audit & accounting firm, (5) tech companies, (6) general public. We plan to work closely with the widest possible range of stakeholders to maximize the impact. Below we describe the activities we plan to take to maximize the impact.

Activities

Besides disseminating the research outcome via publishing at high-impact journals and conference, we plan to produce input to expert groups, committee and standardization bodies. For instance, Dr. Au and Dr. Liu are expert members of the International Organization for Standardization of China and Australia, respectively. Prof. Lu is the chief editor of the weekly newsletter on "The Impact of Technology on Accounting, Finance, Economics and Law" on behalf of PolyU School of Accounting and Finance. They are good channels to disseminate the results to all stakeholders.

In addition, we are working closely with our collaborators to explore potential applications of ZKP. The list of collaborators includes international corporations such as Ant Financial, AMTD group, along with fintech companies in the greater bay area such as 9F, Valigo Limited, as well as digital health expert Qinqin Health. They will help by contributing domain knowledge for us to complete our prototypes (objective 3 – 6) as evidence to demonstrate the power of ZKP in protecting data privacy. We are also actively reaching out. It is worth noting that the team has extensive experience in industry collaborations and also outstanding records in generating impactful results beyond academia.

Short-Term (1-3 years)

We envision that this project would lead to new privacy-preserving techniques secure against quantum computers. This is extremely important since quantum computers are a major threat to data privacy. It has caused great concerns among major stakeholders such as NSA, NIST, ETSI, Google.

The major milestones of the short-term impact are as follows. We will publish a set of user-friendly development tools to allow programmers to build secure applications with ZKP. To demonstrate how it could be used, we will also develop a new digital identity system utilizing our result. Our partner plan to commercialize this and adopt it in the insurance industry.

Mid-Term (4-10 years)

We envision our results could be included in international standards for data privacy protection. We will also work to raise the awareness of the general public for ZKP, and influence policymaker to update relevant regulations. Another milestone is the adoption of our result to AI-based account & audit, and also adopted in the protection of data privacy in digital health.

Long-Term (over 10 years)

The results of this project will change the landscape of the industry with tight regulations. When account and audit are to be conducted by machines, our results will be used to prevent malicious tampering, thus making AI-based audit more feasible.

Conclusion

Potential applications of ZKP is huge. In the industries under tight regulations, including financial services, insurance, it can be used for diligence, security and verification tool. The success of this project could enhance security and privacy in the technology era and maintain Hong Kong's unique status as a global financial centre.

A maximum of four A4 pages in total, including all attachments and references, in standard RGC format for Sections 4-5 below.

4. Proposed Outline of Research Plan and Methodology

5. Collaboration Plan

[Please identify the role and specific task(s) the PC and each of the Co-PIs/partner(s) is responsible for.]

Proposed Outline of Research Plan and Methodology

Introduced by Goldwasser, Micali and Rackoff [GMR85], a zero-knowledge proof (ZKP) is a method where one party can convince another party a statement is true without revealing any extra information. ZKP is a promising solution in a data-driven society to address key challenges in data integrity, data privacy and verified computing.

ZKP is a breakthrough result from modern cryptography. Despite the fact that theoretically all computationally verifiable statements can be proved using ZKP, their applications in practice is limited to cryptographic applications. One reason is that it is highly non-trivial to implement ZKP. Specifically, it involves translating the computationally verifiable statement into a circuit, followed by a probabilistic verification method in which the verifier asks the prover something about the circuit evaluation. The process involves sophisticated mathematics that is difficult to understand. Worst still, translating a computationally verifiable statement into a circuit is a challenging "hardware engineering" problem that only a selected few can tackle.

In this project, we consider the ease of development of ZKP-enhanced applications. Our goal is to eliminate the circuit design process and replace it a coding process. That is, we aim to make ZKP implementation into a software engineering problem. The key is to design ZKP that supports statements written in a high-level programing language. Then, any software developer can program in their favorite high-level language to represent statements. In other words, they would be able to implement ZKP without the need to worry about the underlying process.

We plan to achieve this goal with a two-step process. Firstly, we plan to choose a target CPU instruction set and develop ZKP for any statement that could be verified using this target instruction set. Secondly, we develop a compiler which can translate any program written in a high-level computer language into the target instruction set. Combining these two results, ZKP-enabled applications can be implemented by anyone who can program in a high-level language. This corresponds to objective 1 and 2 of the proposal.

Objective 1: ZKP Proof for ARM Instruction Set

We intend to adopt ARM [ARM] as the target CPU instruction set. The ARM architecture is widely used in consumer electronic devices, such as smart phones, laptops, and tablet computers, due to its good characteristics, including smaller size, reduced complexity and lower power consumption. Rather than transforming a program written in ARM into a circuit followed by ZKP for the circuit, we plan to adopt group-based cryptographic primitives to prove the computation integrity of the ARM program in zero-knowledge. The proof involves three parts: (1) the validity of the instruction fetching; (2) the validity of the memory access; (3) the validity of the instruction computation. For the execution of each instruction, we will generate a group-dependent zero-knowledge proof for the validity of the above three parts. This can be done via utilizing several group-based cryptographic primitives. We will compare the proof size of our proposed group-based zero-knowledge proofs and the proof size of existing succinct zero-knowledge proofs for the circuit satisfiability. We believe that our proof system is more efficient due to the designed structure.

Objective 2: Compiling C Program to ARM Program

We choose C to be the high-level programming language. Our choice of C and ARM allows us to develop ZKP compatible with many existing tools, and also lower the barrier for system

developers. Nonetheless, the goal of this objective is to develop a compiler that translates any C program into an ARM program that is zero-knowledge friendly.

Different to existing compiler, the focus of ours is to be ZKP-friendly. We plan to measure the cost to support ZKP for various ARM instructions and translate the C program into ARM program make fewer use of the expensive instructions (e.g. fewer memory access, favor addition over multiplication).

Objective 3: Enhance Efficiency, Security, and Provide a Baseline

Succinctness. Succinct ZKP [Kil92] aim to reduce proof size and verification complexity. Succinct ZKP are very popular at the moment thanks to its short proof size and fast verification (at the expense of security and/or proof generation time). Most existing constructions of succinct ZKP are for arithmetic circuits. State-of-the-art follows the two-step approach and include: circuit generator for a low-level language and a compiler to compile a high-level language into the low-level one (vnTinyRAM in [BCT+14]). We also aim to design a succinct version of our ZKP.

Post-Quantum Security. Another innovation of our project is to consider security against quantum computers, which has been recognized as a severe threat by major stakeholders including NSA, NIST, ETSI, Google. To achieve this goal, we will upgrade the basic group-based components in our proposed ZKP to be based on lattice, a method conjectured to be secure against quantum computers. The starting point will be the lattice-based ZKPs for very specific statements [MV03, Lyu08, LLN+16]. We will generalize these techniques to achieve lattice-based ZKP for ARM programs.

A Baseline Solution. Another popular approach to protect data privacy is to employ trusted-computing (e.g. Intel SGX [SGX]), where the verification is done in a hardware-assisted trusted execution environment (TEE). It is relatively easy to set up applications to be executed in TEE, and it can support a vast class of programs. Despite promising, TEE can be broken by a wide spectrum of side-channel attacks [WCP+18], and also rely on the trust of the hardware provider. In this project, we also aim to develop a baseline solution using the hardware-assisted approach. It can be used to compare the efficiency with the ZKP approach, and also allow us to quickly develop prototypes using this baseline solution. Our recent work [DZD+19] on secure crowdsensing will be used as a starting point.

Deliverables of objective 1 to 3 include design of new ZKP with various enhancements, a development tool that streamlines ZKP implementations. We will also compare the ZKP with our hardware-assisted baseline solution. Based on our tools, we will work closely with our industry partners to develop prototype applications to illustrate the usefulness of our tools. The following 3 applications are chosen after initial discussions with our industry partners.

Objective 4: Self-Sovereign Digital Identity

Identity Management provides a single view of identities to various systems. It is a combination of processes and technologies to manage access to the identity information. It includes the entire process of deciding who should have access to the information, and to what information; providing, changing and terminating such access when appropriate.

The new General Data Protection Regulation (GDPR) which regulates how personal data should be handled may have a great impact on existing identity management systems. Personal

data should be handled with great care as required by GDPR. The following aspects greatly affect how an identity management system should be implemented. (1) Data Protection by Design and Default; (2) Consent; (3) Data Portability and (4) Right to be forgotten.

Initially, we will develop this application with input from our industry partner, Valigo Limited. Their client includes large insurance companies and academic institutes and would like to apply the outcome to insurance claim as well as blockchain-based certification.

Objective 5: Digital Health

Through the use of digital technologies, digital healthcare aims to enhance the efficiency of healthcare delivery and provide personalized medical services. Since health records contain highly sensitive information, they must be well protected. However, these health records should also be accessible by doctors and perhaps third-party organizations (e.g., research institutes, etc.). The challenging issue is how to provide necessary information from health record to doctors/third-party organizations while keeping sensitive information private. In this objective, we will devise the next generation digital health platform to connect medical practitioners, clinics and users in a privacy-preserving manner.

Initially, we will develop this application with input from our industry partner, Qin Qin Health International Limited. Their client includes medical practitioners from the greater bay region as well as Malaysia.

Objective 6: Compliance

Financial institutes are tightly regulated. Auditing is usually conducted by consultants from third-party and the process involves data collection and check. Such process is tedious, time-consuming and may be prone to human errors. In this objective, we will leverage our ZKP to simplify such audit process without sacrificing its correctness. More precisely, instead of asking the consultants to audit the target company, the company could generate certifications of its behaviors. Then, the consultants can just check the certification to decide whether the company comply with the regulations or not. In particular, if the target company does not follow the regulations, our scheme allows the consultant to quickly identify the issues through efficient proof verification. Our new approach can largely reduce the cost of performing an audit.

In the future, we envision some of the basic compliance check will be conducted by AI applications. One necessary condition is to prevent the AI application from being tampered with. ZKP can help addressing this issue by incorporating the AI to produce a succinct proof of its integrity. Initially, we will develop this application with input from our industry partner 9F. We have also engaged Ant Financials and EY with positive responses.

Collaboration Plan

The project team members have been working closely in their career, as shown by the high number of joint publications and joint funding projects. PC Au will work closely with all Co-PIs in this project. He has extensive experience in managing large projects involving the industry and the academia, both locally and internationally. PC Au is an expert in ZKP and will be responsible for Objective 1 and 4. Co-PI Luo is an expert in mobile security and the ARM architecture. He will be responsible for objective 2. Co-PI Wang is an expert in cloud computing and trusted computing and will be responsible for objective 3. Co-PI Liu is an expert in blockchain and post-quantum security. He will be responsible for objective 5 and also

contribute to objective 3. Co-PI Lu is an expert in Law and Finance and will be responsible for objective 6 and contribute to objective 4 and 5. The teams will (e-)meet bi-weekly to update the research progress. Seminar and workshop will be held on regular basis. We plan to hire 3-4 RAs or postgraduate assistants (costing will be around $1.6M/year) to carry out the research work. Total budget will be $5M for this project. The relationship between the objectives and the responsible person are shown in Fig. 1.

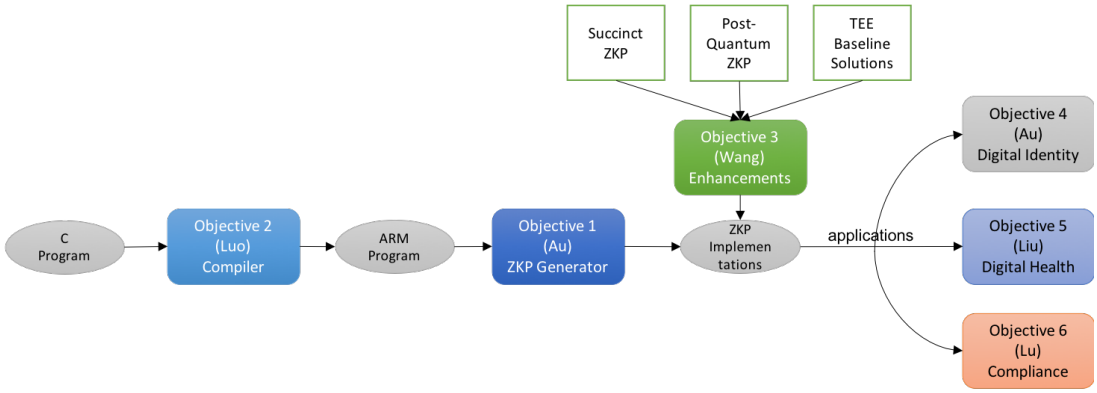

Figure 1. Collaboration Plan

References

[ARM] ARM Architecture Introduction. https://www.arm.com/files/pdf/ARM_Arch_A8.pdf

[BCT+14] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. USENIX Security Symposium 2014: 781-796

[DZD+19] Huaayi Duan, Yifeng Zheng, Yuefeng Du, Anxin Zhou, Cong Wang, Man Ho Au. Aggregating Crowd Wisdom via Blockchain: A Private, Correct, and Robust Realization. IEEE PERCOM 2019 (to appear)

[FFS88] Uriel Feige, Amos Fiat, Adi Shamir. Zero-Knowledge Proofs of Identity. Journal of Cryptology 1(2): 77-94 (1998)

[GMR85] Shafi Goldwasser, Silvio Micali, Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. STOC 1985: 291-304.

[Kil92] Joe Kilian: A Note on Efficient Zero-Knowledge Proofs and Arguments (Extended Abstract). STOC 1992: 723-732

[LLN+16] Benoît Libert, San Ling, Khoa Nguyen, Huaxiong Wang. Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors. EUROCRYPT (2) 2016: 1-31

[Lyu08] Vadim Lyubashevsky. Lattice-Based Identification Schemes Secure Under Active Attacks. Public Key Cryptography 2008: 162-179

[MV03] Daniele Micciancio, Salil P. Vadhan. Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More. CRYPTO 2003: 282-298

[SGX] Intel Software Guard Extensions. https://software.intel.com/en-us/sgx, 2018

[WCP+18] Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter. Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. ACM CCS 2017: 2421-2434

6. Brief Curriculum Vitae (CV) for Applicants

[Please attach a one-page curriculum vitae, in standard RGC format, for the PC and each Co-PI. For organisational partner(s), please also attach a one-page introduction of the organisation.]

Man Ho Allen Au

EDUCATION

- **PhD** (2009), Computer Science and Software Engineering, University of Wollongong
- **MPhil** (2005), Information Engineering, The Chinese University of Hong Kong
- **BEng** (2003), Information Engineering, The Chinese University of Hong Kong

WORK EXPERIENCE

- **Assistant Professor** (2014-), Department of Computing, Hong Kong Polytechnic University
- **Lecture** (2014), University of Wollongong
- **Associate Lecture** (2011-2013), University of Wollongong
- **Postdoctoral Researcher** (2008-2011), University of Wollongong

SELECTED PUBLICATIONS

Dr. Au has published over 140 refereed papers at international conferences and journals. According to Google Scholar1 , his work has been cited over 3700 times. His h-index is 34.

- Cheng Xu, Jianliang Xu, Haibo Hu, Man Ho Au. When Query Authentication Meets Fine-Grained Access Control: A Zero-Knowledge Approach. Proceedings of the 2018 International Conference on Management of Data (SIGMOD 2018), pages 147-162 (2018)
- Shifeng Sun, Man Ho Au, Joseph K. Liu, Tsz Hon Yuen. RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017)
- Yong Yu, Man Ho Au, Giusepe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, Geyong Min. Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage. IEEE Transactions on Information Forensics and Security: 12(4), pp. 1182-1194 (2017)
- Man Ho Au, Joseph K. Liu, Willy Susilo and Jianying Zhou. Realizing Fully Secure Unrestricted IDbased Ring Signature in the Standard Model Based on HIBE. IEEE Transactions on Information Forensics and Security 8(12): 1909-1922 (2013)
- Man Ho Au and Apu Kapadia. PERM: Practical Reputation Based Blacklisting without TTPs. Proceedings of the 19th ACM conference on Computer and communications security (ACM CCS 2012)

SELECTED AWARDS and HONORS

- Best Paper Award: ACISP 2016, ISPEC 2017, ACISP 2018
- 2009 PET runner-up award for outstanding research in privacy enhancing technologies

RESEARCH GRANTS

Dr. Au's research has been generously supported by funding agencies and the industry. In the past 3 years, he has, as the principle investigator, attracted a research income of over 21 million HKD. Below are some of his selected projects.

- Joint Lab on Blockchain & Cryptocurrency, CollinStar Capital & Monash University, HKD 9 million
- Anonymous Digital Signatures in the Post-Quantum Era: Secure and Efficient Constructions, ITF-Tier 3, HKD 1.55 million
- Blockchain-Based Food and Drug Counterfeit Detection and Regulatory System, ITF UICP, HKD 6.03 million

Joseph Liu

EDUCATION

- **PhD** (2004), Information Engineering, The Chinese University of Hong Kong
- **M.Phil.** (2001) and **BE** (1999), Information Engineering, The Chinese University of Hong Kong

WORK EXPERIENCE

- **Associate Professor** (2019-), Faculty of Information Technology, Monash University, Australia
- **Director** (2019-), Monash Blockchain Technology Centre, Monash University, Australia
- **Senior Lecturer** (2015-2018), Faculty of Information Technology, Monash University, Australia
- **Research Scientist** (2007-2015), Institute for Infocomm Research, Singapore
- **Research Fellow** (2005-2007), University of Bristol, UK

SELECTED PUBLICATIONS

- Xiaoqiang Sun, Peng Zhang, Joseph K. Liu, Jianping Yu, Weixin Xie, "Private machine learning classification based on fully homomorphic encryption", IEEE Transactions on Emerging Topics in Computing. Accepted for publication. [impact factor: 3.626]
- Peng Jiang, Fuchun Guo, Willy Susilo, Man Ho Au, Xinyi Huang, Joseph K. Liu, "Efficient and Adaptive Procurement Protocol with Purchasing Privacy", IEEE Transactions on Services Computing. Accepted for publication. [impact factor: 4.418]
- Kai He, Jian Weng, Jiasi Weng, Joseph K. Liu, Xun Yi, "Attribute-based Hybrid Boolean Keyword Search over Outsourced Encrypted Data", IEEE Transactions on Dependable and Secure Computing. Accepted for publication. [impact factor: 4.410]
- Peng Zhang, Joseph K. Liu, F. Richard Yu, Mehdi Sookhak, Man Ho Au and Xiapu Luo, "A Survey on Access Control in Fog Computing", IEEE Communications Magazine 15(2): 144-149 (2018). [impact factor: 9.27
- Cong Zuo, Jun Shao, Joseph K. Liu, Guiyi Wei and Yun Ling, "Fine Grained Two-Factor Protection Mechanism for Data Sharing in Cloud-Storage", IEEE Transactions on Information Forensics and Security 13(1): 186-196 (2018). [impact factor: 5.824]
- Shangqi Lai, Sikhar Patranabis, Amin Sakzad, Joseph K. Liu, Debdeep Mukhopadhyay, Ron Steinfeld, Shifeng Sun, Dongxi Liu, Cong Zuo, "Result Pattern Hiding Searchable Encryption for Conjunctive Queries". ACM Conference on Computer and Communications Security (CCS), pages 745-762, 2018.

SELECTED AWARDS and HONORS

- Dean's Research Impact Award, Monash University, 2018
- ICT Researcher of the Year Award, Australian Computer Society (ACS), 2018

SELECTED RESEARCH GRANTS

- Collinstar Blockchain Research Lab – "Blockchain Research for Cryptocurrency", as the role of the leading Chief Investigator. Grant amount: AU$2.25M = HK$12.5M (2017-2020)
- Australian Research Council (ARC) Discovery Project, "Privacy-preserving Data Processing on the Cloud", as the role of Chief Investigator. Grant amount: AU$450k = HK$2.5M (2018-2020)
- Data 61 Cooperative Research Project, "Designing for data confidentiality and resilience", as the role of Chief Investigator. Grant amount: AU$730k = HK$4M (2017-2020)
- Australian Renewable Energy Agency (ARENA) – "Monash's Smart Energy City", as the role of Chief Investigator. Grant amount: AU$7.6M = HK$42.6M (2018-2020)

Haitian Lu

EDUCATION

- **PhD** (2007), Law, National University of Singapore, Singapore
- **LL.M.** (2002), Law, University of Liverpool, U.K.
- **LL.B.** (2001), Law, Nanjing University, China

WORK EXPERIENCE

- **Professor** (2018-), School of Accounting and Finance, The Hong Kong Polytechnic University
- **Visiting Research Professor (**2016), New York University, Stern School of Business
- **Associate Professor** (2012-2018), School of Accounting and Finance, The Hong Kong Polytechnic University
- **Assistant Professor** (2007-2012), School of Accounting and Finance, The Hong Kong Polytechnic University
- **Visiting Lecturer** (2005-2007), School of Accounting and Finance, The Hong Kong Polytechnic University

SELECTED PUBLICATIONS

- Chen S., Meng W. and Lu H.T. 2018. Patent As Quality Signal in Entrepreneurial Finance: A Look Beneath the Surface. Asia Pacific Journal of Financial Studies (SSCI) 47, 1-26.
- Lu H.T. 2016. The Legalization of Corporate Social Responsibility: Hong Kong Experience of ESG Reporting. Asia Pacific Law Review 24 (2) 123-48 (SSCI)
- Lu H.T., Pan H.B. and Zhang C.Y. 2015, Political Connectedness and Judicial Outcomes: Evidence from Chinese Corporate Lawsuits, Journal of Law and Economics 58 (4), 829-861
- Fu J.J. and Lu H.T., 2014. Structural Changes in the Chinese Stock Market: A Review of Empirical Research. China Accounting and Finance Review 16(2), 39-65
- Tan Y., Huang H., and Lu H.T., 2013, The Effect of Venture Capitalist Investment: Evidence from China's Small and Medium Enterprise Board, Journal of Small Business Management 51(1), 138-57 (SSCI)

Xiapu Luo

EDUCATION

- **PhD** (2007), Computer Science, Hong Kong Polytechnic University
- **M.Sc** (2002), Communications and Information Systems, Wuhan University, China
- **B.Sc.** (1999), Communication Engineering, Wuhan University, China

WORK EXPERIENCE

- **Assistant Professor** (2017-), Hong Kong Polytechnic University.
- **Research Assistant Professor** (2012-2017), Hong Kong Polytechnic University.
- **Research Fellow** (2010-2012), Hong Kong Polytechnic University.
- **Postdoc** (2008-2010), Georgia Institute of Technology, USA.

SELECTED PUBLICATIONS

- Ting Chen, Yuxiao Zhu, Zihao Li, Jiachi Chen, Xiaoqi Li, Xiapu Luo, Xiaodong Lin, and Xiaosong Zhang, "Understanding Ethereum via Graph Analysis", Proc. of IEEE International Conference on Computer Communications (INFOCOM), Honolulu, USA, April 2018. (Best Paper Award)
- Ting Chen, Zihao Li, Hao Zhou, Jiachi Chen, Xiapu Luo, Xiaoqi Li, and Xiaosong Zhang, "Towards Saving Money in Using Smart Contracts", Proc. of the 40th IEEE International Conference on Software Engineering (ICSE), pp. 81-84, Gothenburg, Sweden, May 2018.
- Ting Chen, Xiaoqi Li, Ying Wang, Jiachi Chen, Zihao Li, Xiapu Luo, Man Ho Au, and Xiaosong Zhang, "An Adaptive Gas Cost Mechanism for Ethereum to Defend Against Under-Priced DoS Attacks", Proc. of the 13th International Conference on Information Security Practice and Experience (ISPEC), pp. 3-24, Melbourne, Australia, December 2017. (Best Paper Award)
- Ting Chen, Xiaoqi Li, Xiapu Luo, and Xiaosong Zhang, “Under-optimized Smart Contracts Devour Your Money”, Proc. of the 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER), pp. 442-446, Klagenfurt, Austria, February 2017.
- Lei Xue, Yajin Zhou, Ting Chen, Xiapu Luo, and Guofei Gu, “Malton: Towards On-Device Non-Invasive Mobile Malware Analysis for ART”, Proc. of the 26th USENIX Security Symposium (USENIX SEC), pp. 289-306, Vancouver, Canada, August 2017.

SELECTED AWARDS and HONORS

- 2018 Best Paper Award, 17th National Software Application Conference (NASAC) (Safety and Security of System Software Symposium).
- 2018 Best Paper Award, IEEE International Conference on Computer Communications (INFOCOM).
- 2017 Best Paper Award, 13th International Conference on Information Security Practice and Experience (ISPEC).
- 2017 Best Paper Award, 8th International Conference on Applications and Technologies in Information Security (ATIS).
- 2016 Best Research Paper Award, 27th International Symposium on Software Reliability Engineering (ISSRE).

Granted US Patents

- US 10178204B2, US 9876807B2, US 8885473B2, US 8531952B2

Cong WANG

EDUCATION

- **PhD** (2012), Electrical and Computer Engineering, Illinois Institute of Technology
- **ME** (2007) and **BE** (2004), Electrical and Computer Engineering, Wuhan University

WORK EXPERIENCE

- **Associate Professor** (2018-), City Univ. of Hong Kong, HK
- **Assistant Professor** (2012-2018), City Univ. of Hong Kong, HK

SELECTED PUBLICATIONS

- Y. Zheng, H. Duan, and C. Wang. Learning the Truth Privately and Confidently: Encrypted Confidence-Aware Truth Discovery in Mobile Crowdsensing. IEEE Transactions on Information Forensics and Security, 13(10):2475-2489, Oct., 2018.
- X. Yuan, H. Duan, and C. Wang. "Assuring String Pattern Matching in Outsourced Middleboxes." IEEE/ACM Transactions on Networking, 26(3):1362-1375, Jun., 2018.
- X. Yuan, X. Wang, C. Wang, C. Yu, and S. Nutanong. "Privacy-preserving Similarity Joins Over Encrypted Data." IEEE Transactions on Information Forensics and Security, 12(11):2763-2775, Nov. 2017.
- X. Yuan, X. Wang, J. Wang, Y. Chu, C. Wang, J. Wang, M. Montpetit, and S. Liu. "Enabling Secure and Efficient Video Delivery through Encrypted In-network Caching." IEEE Journal on Selected Areas in Communications, 34(8):2077-2090, Aug., 2016.
- C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou. "Privacy-Preserving Public Auditing for Secure Cloud Storage." IEEE Transactions on Computers, 62(2):362-375, Feb. 2013 (Also in INFOCOM'10, combined Google Scholar Citations = 2495)

SELECTED AWARDS and HONORS

- Founding Members of the Young Academy of Sciences of Hong Kong, Best Student Paper Award of IEEE ICDCS (2017), Best Paper Award for IEEE MSN 2015 and ChinaCom 2009, No. 1 top accessed article in INFOCOM'10 and ICDCS'10 in IEEE Xplore, as of Sep. 2018.

RESEARCH GRANTS

- Secured 2 GRF, 2 ITF (both in Tier-3 with ~1.4 Million each), 1 ECS, and 1 NSFC as PI, and 1 CRF as Co-I, with total amount of ~8Million HKD.

SELECTED PROFESSIONAL SERVICES

- Associate Editor for IEEE Transactions on Dependable and Secure Computing, IEEE Internet of Things Journal, and IEEE Networking Letters
- TPC Co-Chair for Int'l Conf. on Network and System Security (2018), IEEE ICC CISS 2017, AsiaCCS SCC Workshop 2017, IEEE CloudCom 2017, IEEE WiMob 2017, IEEE Trustcom 2016, IEEE CCNC 2016, 10th Int'l Wireless Communication and Mobile Computing Conference 2014

Qin Qin Health International Limited

Qin Qin Health International Limited is a leading comprehensive platform over the Internet. Through this platform, we aim to connect people with health services by making high-quality and convenient health services readily accessible to our users. At the same time, our intelligent terminal and clinic business circle help increase revenues for clinics and pharmaceutical practitioners. Our innovative approach has attracted venture capital support from reputable investment banks, including Goldman Sachs and Merrill Lynch. We also have access to a wide range of high-quality medical resources from mainland China, Hong Kong and Malaysia.

For question regarding to Qin Qin Health International Limited, please feel free to contact by email Katielee@qinqinhealthi.com or by phone 51004810.

9F

Founded in 2006, 9F is committed to offering its users with simple, efficient, high-quality and comprehensive financial services and aimed to create a wealth of values for its users through mobile Internet and Big Data risk management technologies. Currently, 9F Group is a leading Chinese Fintech platform and has more than 68 million registered users with most of them using 9F's mobile applications. 9F was a founding member of National Internet Finance Association of China (NIFA) and elected to be a standing council member of NIFA. Sponsored by the People's Bank of China, the China Banking Regulatory Commission (CBRC), China Securities Regulatory Commission (CSRC) and China Insurance Regulatory Commission (CIRC), NIFA was founded in Shanghai in March 2016.

For further details of our company, please feel free to contact by email linyanjun@9fbank.com.cn or by phone at 25197622.

Valigo Limited

Founded in 2016, Valigo Limited ("Valigo") is a Hong Kong-based blockchain consultancy firm with particular emphasis in ICO practices. Valigo offers full service packages to clients ranging from the development of tokenisation strategies for their businesses to the establishment of proper mechanics for their token sales. Valigo also provides advice and insights to local, regional & international clients by stressing compliance with relevant legal and regulatory requirements and adoption of the latest best practices formulated in the crypto community.

Valigo provide a full range of pre- and post-ICO services and support by working with its partners, such as the Hong Kong Blockchain Lab and other third-party developers, to ensure not only that their clients' ICOs launch successfully and seamlessly, but also that their projects continue to build trust and gain positive reputation in the long run after their ICOs complete. Valigo's services include but are not limited to the following:

1. Providing legal consultation: making sure that relevant laws and regulations are reasonably complied with for every step of the ICO process;
2. Conducting due diligence: evaluation of the ICO team, business plan, market potential, valuation, competition, legal compliance and security;
3. Auditing: with respect to the blockchain economy, business model, finance, cryptography, cybersecurity, code, and legal compliances;
4. Fundraising & fund management: conducting fundraising activities, after which the received funds will be actively monitored by professionals and segregated to be used for various purposes in the project and will be inherently transparent;
5. Shaping investor relations: finding public investors early in order to get feedbacks on the project and ICO before their launch; keeping investors engaged and updated after the ICO finishes by communicating with them on a regulator basis; and
6. Compiling quarterly/annual reports: publish professional quarterly/annual reports to keep investors informed about the financial situation and performance of the ICO company, enriching their insights and opening up to more investment opportunities.
7. Drafting whitepaper: assistance in writing a whitepaper to communicate the project's goals to the audience;
8. Marketing: coordination of advertising and marketing exercises for ICOs campaign including building websites and conducting PR activities with audiences via social media platforms and community forums;

In hindsight, Valigo strives to establish its trust and reputation as the go-to-partner for ICO consultancy within the blockchain community. In addition, Valigo pledges to improve the ICO ecosystem as well as safeguarding clients and investors interest through our ICO best practice protocol.

For questions regarding to Valigo service or you would simply like to talk to one of our consultants, please contact us via: info@valigo.net.

7. Applicants' Experience in Collaboration beyond Academia

[Please describe the experience, if any, of the PC and each Co-PI in collaboration beyond academia (250 words for each person).]

Dr Au Man Ho Allen (PC)	Dr. Au's research has generated significant social and economic impact. One indicator is the huge amount (over 21 million HKD) of research income he received as the principal investigator. Among them, 15 million are supported by the industry (including UBI and OnBoard security from US, Collinstar Capital from Australia, Ant Financials from China and Valigo from Hong Kong) in the form of sponsorship, contract research and high-level consultancy projects. Another indicator is his success in knowledge transfer. Notably, his digital signature technology has been adopted by the Hyperledger Fabric project, the most popular blockchain infrastructure supported by big industry players like IBM, Intel and SAP. Finally, Dr. Au is an expert member of the China delegation of ISO/IEC JTC 1/SC 27 working group 2 - Cryptography and security mechanisms who contribute to various standards related to privacy-preserving technologies.
Dr Liu Joseph (Co-PI)	Dr Liu has extensive experience of collaboration with industry. Since joinging Monash in 2015, he has obtained more than US$2M funding support from different sectors of industry, ranging from blockchain, logicstic, leading global ICT enterprise etc. Dr Liu has provided his expertise in applied cryptography, privacy enhanced technologies and blockchain security to these projects. He is currently the Chief Scientist of a public blockchain cryptocurrency HyperCash, in which he leads the research team in Monash to develop advanced post-quantum secure algorithms for the blockchain system. He is also the advisory board of UCOT, A blockchain powered smart IoT ecosystem, to provide extensive consultancy for the security and privacy of the blockchain system.
Prof Lu Haitian (Co-PI)	Prof. Haitian Lu is a professor in law at PolyU School of Accounting and Finance. He specializes in securities regulations, corporate governance, financial technology (Fintech) and regulatory technology (Regtech). He is leading the project on "A Rating System for (Crypto-) Tokens on (Block-chain based) Platforms" which employs Artificial Intelligence to provide real-time ratings and research reports on major crypto-tokens publicly traded on exchanges (www.imrating.com). He is also the chief editor for the weekly newsletter on "The Impact of Technology in Accounting, Finance, Economics and Law" operated by PolyU School of Accounting and Finance. The weekly newsletter focuses on technology related issues such as big data, artificial intelligence, distributed ledger, Fintech, AccounTech, InsurTech, Regtech, etc, their impact on the profession, managerial practices, ethics, and understanding on how the world works (http://www.polyu.edu.hk/af/afro/fintech_newsletter.html).
Dr Luo Daniel Xiapu (Co-PI)	Xiapu Luo is an assistant professor in the Department of Computing, The Hong Kong Polytechnic University. His research has been supported by RGC GRF/ECS, ITF, NSFC and companies like Tencent and Huawei. His work appeared in top conferences and journals and led to four granted US patents. He serves as PI of the following projects with collaborations beyond academia: 1. PI,"Privacy Leakage Detection Based on Dynamic Taint Analysis: Techniques and System",Funded by Huawei Inc., 2018/12 – 2019/10. 2. PI, "Research and Development of An Advanced IPS System for Aftermarket Telematics", ITF,2018/03-2020/02. 3. PI, "Assessing the Vulnerabilities of Online Services to Advanced DDoS Attacks",ITF,2015/10-2017/09. 4. PI, "Traffic Scheduling Based on One-way End-to-end Network Measurement," Funded by China Computer Federate (CCF) and Tencent Inc.,2013/10-2014/10.

Dr Wang Cong (Co-PI)	Cong has worked with Hong Kong Applied Science And Technology Research Institute Company Limited in the capacity of technical advisor from 13/02/2017 to 15/12/2017. His role was to provide consultancy services in solving complex problems in cybersecurity system and cryptographic algorithms.
Miss Lee Fong Cing (Organisational partner)	
Mr Lin Yanjun (Organisational partner)	
Dr Ma Lawrence (Organisational partner)	

8. Letter of collaboration or supporting statement from each Co-PI and organisational partner

[Please attach a maximum of one A4 page for each Co-PI / organisational partner.]

MONASH University

Department of Computing
The Hong Kong Polytechnic University
Hung Hom, Kowloon
Hong Kong

25 Feb 2019

Dear Dr. Man Ho Allen Au,

Letter of Collaboration - Application for Research Impact Fund
Project: Practical Zero-Knowledge Proof: Theory and Applications

I am writing to confirm that I agree to join the project team as a co-principal investigator for the captioned project (Project Coordinator: Dr. Man Ho Allen Au). We believe advances in practical zero-knowledge proof would bring great benefit to the area of fintech and digital health, one of the strategic areas of Monash.

Thanks for your invitation. We have been collaborating through the PolyU Monash University - Collinstar Capital Joint Lab on Blockchain and Cryptocurrency Technologies. I am confident that this joint project will further strengthen our collaboration relationship.

Yours Sincerely,

Dr. Joseph Liu
Associate Professor
Faculty of Information Technology, Monash University

Department of Computing
The Hong Kong Polytechnic University
Hung Hom, Kowloon
Hong Kong

25 February 2019

Dear Dr. Man Ho Allen Au

Letter of Collaboration - Research Impact Fund 2019/2020

I am writing to confirm that I agree to serve in the project team as a Co-PI for the project titled "Practical Zero-Knowledge Proof: Theory and Applications" (PC: Dr. Man Ho Allen Au). I look forward to collaborating with you.

Yours Sincerely,

Lu Haitian

Dr. Haitian Lu
Professor and Associate Dean
Faculty of Business
The Hong Kong Polytechnic University

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTING
工程學院
電子計算學系

25 February 2019

Dr. Man Ho Allen AU

Department Computing

The Hong Kong Polytechnic University

Hung Hom, Kowloon, Hong Kong

Dear Dr. Man Ho Allen AU,

Project Title: Practical Zero-Knowledge Proof: Theory and Applications

Principal Coordinator [PC]: Dr. Allen Man Ho AU (PolyU)

With reference to the above research proposal for RGC Research Impact Fund (RIF) 2019/20, I agree to be one of the Co-Principal Investigators of the captioned project. Through this joint research project, we hope to strengthen our collaboration in this field.

Yours sincerely,

Dr. Xiapu Luo 

Assistant Professor

Department of Computing
The Hong Kong Polytechnic University
Email: csxluo@comp.polyu.edu.hk
Tel: 852-27667264

February 25th, 2019

香港城市大學
City University of Hong Kong
專業 創新 胸懷全球
Professional·Creative
For The World

Department of Computing
The Hong Kong Polytechnic University

Re: Collaboration Letter of RIF Proposal

Dear Dr. Man Ho Allen AU,

This is to confirm with you that I agree to participate in the Hong Kong RGC's RIF proposal, titled "Practical Zero-Knowledge Proof: Theory and Applications", as Co-PI.

Many thanks for your invitation. Looking forward to working with you.

Sincerely,

Cong Wang, PhD
Associate Professor
Dept. of Compute Science
City University of Hong Kong
83 Tat Chee Avenue, Kowloon, Hong Kong
Tel: +852 3442 2010
Email: congwang@cityu.edu.hk
http://www.cs.cityu.edu.hk/~congwang/

February 26, 2019

Dr. Man Ho Allen Au and Prof. Haitian Lu

The Hong Kong Polytechnic University

Hung Hom, Kowloon

Hong Kong

Dear Dr. Au and Prof. Lu,

I am delighted to learn your novel research development regarding your research project " Practical Zero-Knowledge Proof: Theory and Applications " (the "Project") to be submitted to the Research Grants Council as an application for Allocation from the Research Impact Fund.

As the CEO of QCURE (Qin Qin Health International Limited), I am writing to express my sincere support for the Project and our interest to participate in future collaboration.

QCURE is a leading comprehensive medical service platform over the Internet. Through this platform, we aim to connect people with health services by making high-quality and convenient health services readily assessible to our users. At the same time, our intelligent terminal and clinic business circle help increase revenues for clinics and pharmaceutical practitioners. Our innovative approach has attracted venture capital support from reputable investment banks, including Goldman Sachs and Merrill Lynch. We also have access to a wide range of high-quality medical resources from mainland China, Hong Kong and Malaysia.

I will be interested in further update about this Project, which aim to develop practical zero-knowledge proof, an emerging privacy-enhancing technology. We believe it will have a big impact in the next-generation digital health applications as it can help protect sensitive user information, a necessary requirement for health records to be digitalized and diagnosis to be conducted over the Internet.

For further details of our collaboration, please feel free to contact me by email or by phone at 51004810. I look forward to a fruitful collaboration.

Sincerely,

For and on behalf of
Qin Qin Health International Limited
親親健康國際有限公司

Lee Pong Chung, Katie
Authorized Signature(s)

9F 玖富 9fgroup.com
移动金融大师兄

February 26, 2019

Dr. Man Ho Allen Au and Prof. Haitian Lu
The Hong Kong Polytechnic University
Hung Hom, Kowloon
Hong Kong

Dear Dr. Au and Prof. Lu,

It is my pleasure to write this letter of support for your research project entitled "Practical Zero-Knowledge Proof: Theory and Applications" to be submitted to the Research Grants Council under the call for Allocation from the Research Impact Fund.

Founded in 2006, 9F is committed to offering its users with simple, efficient, high-quality and comprehensive financial services and aimed to create a wealth of values for its users through mobile Internet and Big Data risk management technologies. Currently, 9F Group is a leading Chinese Fintech platform and has more than 68 million registered users with most of them using 9F's mobile applications. 9F was a founding member of National Internet Finance Association of China (NIFA) and elected to be a standing council member of NIFA. Sponsored by the People's Bank of China, the China Banking Regulatory Commission (CBRC), China Securities Regulatory Commission (CSRC) and China Insurance Regulatory Commission (CIRC), NIFA was founded in Shanghai in March 2016.

As the Chief Executive Officer of 9F International and Chief Financial Officer of 9F, I am excited to learn about the research project to be conducted by you and on zero-knowledge proof. We are aware of its potential in fintech applications and plays an important role in account and audit. I will be interested in further update about this project and explore opportunities to adopt the deliverables in our virtual banking services to enhance its security and privacy.

For further details of our collaboration, please feel free to contact me by email linyanjun@9fbank.com.cn or by phone at 2519 7622. I look forward to a fruitful collaboration.

Sincerely,

VALIGO

February 26, 2019

Dr. Man Ho Allen Au
Department of Computing
The Hong Kong Polytechnic University
Hunghom, Hong Kong

Dear Dr. Au,

I am pleased to write in support for Dr. Allen Au's application for the project titled "Practical Zero-Knowledge Proof: Theory and Applications" to the Research Grants Council as an application for Allocation from the Research Impact Fund.

Founded in 2016, Valigo Limited is a Hong Kong-based blockchain consultancy firm. Staffed with qualified and experienced blockchain specialists, we offer full service packages to clients ranging from the development of blockchain-based applications to certified training on blockchain technologies. We strive to deliver quality advice and insights to our local, regional & international clients by stressing compliance with relevant legal and regulatory requirements and adoption of the latest best practices formulated in the crypto community. Our client includes big audit firm and insurance brokers.

We believe the goal of this project, namely, to develop practical zero-knowledge proofs with security against quantum computers, aligns closely with our goal. The success of this project could help protecting our ICT infrastructure, including blockchain, against this upcoming threat. We are particularly interested in applying zero-knowledge proof to identity management.

We would be very interested in supporting Dr. Au's research, by following-up, discussing and contributing to the advances in his project. In particular, we will assist Dr. Au to develop his network, and spread his research outcomes to our clients, and partners. We have had a fruitful collaboration relationship with Dr. Au's team in the past, and we are confident that this project will bring impactful result to the community. In this regard, we are happy to provide cash sponsorship of HK$ 700,000 as matching fund for the project.

Yours Sincerely,

Dr. Lawrence Ma

Director
Valigo Limited

Feb. 26, 2019