Hiraku Morita

Joint Postdoctoral Researcher, Aarhus University and University of Copenhagen, Denmark

Åbogade 34
8200, Aarhus
Denmark
✉ *himo@di.ku.dk*

ORCiD: 0000-0003-3547-7725

Professional Positions

2023.1– **Joint Postdoctoral Researcher**, *Aarhus University and University of Copenhagen*, Denmark.

2021.1– **Postdoctoral Researcher**, *University of St.Gallen*, St.Gallen - Switzerland.
2022.12 I worked on applications of secure multi-party computations, especially on biometric identification and machine learning.

2017.4– **Postdoctoral Researcher**, *AIST*, Tokyo - Japan.
2020.12 I worked on secure multi-party computations, especially on constructing efficient protocols for real-world applications. I constructed a secure comparison protocol, secure division protocol, and secure interval test protocol, which are useful to construct advanced secure functions such as functions used for machine learning or data mining.
Mentor: Nuttapong Attrapadung, Goichiro Hanaoka

Education

2012.4– **Ph.D.**, *Engineering*, Nagoya University, Aichi - Japan.
2017.3 Advisor: Tetsu Iwata.
Thesis title: A Study on the Security of Cryptographic Public Key Primitives against Related-Key Attacks

2014.11– **AIST Research Trainee**, *Cryptography*, AIST, Tokyo - Japan.
2017.3 Host: Goichiro Hanaoka.

2011.4– **Research Student**, *Mathematical Science*, Nagoya University, Aichi - Japan.
2012.3

2009.4– **MS**, *Mathematical Science*, Nagoya University, Aichi - Japan.
2011.3 Advisor: Ken-ichi Yoshida
Thesis title: The limitation value of Hilbert-Kunz multiplicity of Fermat hypersurfaces
GPA: 3.59

2007.4– **MS**, *Engineering*, Nara Institute of Science and Technology, Nara - Japan.
2009.3 Advisor: Yuji Matsumoto
Report title: A Survey of Factuality Analysis Research of Textual Information
GPA: 3.48

2003.4– **Bachelor**, *Agriculture*, Kyoto University, Kyoto - Japan.
2007.3 Advisor: Atsuyuki Asami
GPA: 3.13

Scholarships

2007-2009 Japan Student Services Organization Scholarship Type I

2012-2015 Japan Student Services Organization Scholarship Type I

Awards

2019 4th Tsujii Shigeo security paper award from the Japan Society of Security Management

Referee for Peer-Reviewd Conference Proceedings/Journals

Asiacrypt (2020), PKC (2021), CT-RSA, IWSEC, IEICE, etc.

Expertise

Programming Python, Ruby

Language Japanese (Native), English (Intermediate)

Publications

Conference Papers

(C12) Kazunari Tozawa, Hiraku Morita, Takaaki Mizuki: Single-Shuffle Card-based Protocol with Eight Cards per Gate. UCNC 2023 (To appear)

(C11) Nuttapong Attrapadung, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Kazunari Tozawa: Memory and Round-Efficient MPC Primitives in the Pre-Processing Model from Unit Vectorization. AsiaCCS 2022: 858-872

(C10) Nuttapong Attrapadung, Hiraku Morita, Kazuma Ohara, Jacob Schuldt, Tadanori Teruya, Kazunari Tozawa: Secure Parallel Computation on Privately Partitioned Data and Applications. CCS 2022: 151-164

(C9) Nuttapong Attrapadung, Goichiro Hanaoaka, Takahiro Matsuda, Hiraku Morita, Kazuma Ohara, Jacob Schuldt, Tadanori. Teruya, and Kazunari Tozawa. Oblivious Linear Group Actions and Applications. CCS 2021: 630-650

(C8) Hiraku Morita, Nuttapong Attrapadung: Client-Aided Two-Party Secure Interval Test Protocol. CANS 2019: 328-343

(C7) Hiraku Morita, Nuttapong Attrapadung, Tadanori Teruya, Satsuya Ohata, Koji Nuida, Goichiro Hanaoka: Constant-Round Client-Aided Secure Comparison Protocol. ESORICS (2) 2018: 395-415

(C6) Hiraku Morita, Nuttapong Attrapadung, Satsuya Ohata, Shota Yamada, Koji Nuida, Goichiro Hanaoka: Tree-based Secure Comparison of Secret Shared Data. ISITA 2018: 525-529

(C5) Hiraku Morita, Nuttapong Attrapadung, Satsuya Ohata, Koji Nuida, Shota Yamada, Kana Shimizu, Goichiro Hanaoka, Kiyoshi Asai: Secure Division Protocol and Applications to Privacy-preserving Chi-squared Tests. ISITA 2018: 530-534

(C4) Satsuya Ohata, Hiraku Morita, Goichiro Hanaoka: Accuracy/Efficiency Trade-Off for Privacy-Preserving Division Protocol. ISITA 2018: 535-539

(C3) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: On the Security of the Schnorr Signature Scheme and DSA Against Related-Key Attacks. ICISC 2015: 20-35

(C2) Kazuhiko Minematsu, Stefan Lucks, Hiraku Morita, Tetsu Iwata: Attacks and Security Proofs of EAX-Prime. FSE 2013: 327-347

(C1) Kentaro Inui, Shuya Abe, Kazuo Hara, Hiraku Morita, Chitose Sao, Megumi Eguchi, Asuka Sumida, Koji Murakami, Suguru Matsuyoshi: Experience Mining: Building a Large-Scale Database of Personal Experiences and Opinions from Web Documents. Web Intelligence 2008: 314-321

Journal Papers

(J5) Nuttapong Attrapadung, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Takahiro Matsuda, Ibuki Mishina, Hiraku Morita, Jacob C. N. Schuldt: Adam in Private: Secure and Fast Training of Deep Neural Networks with Adaptive Moment Estimation. PETS 2022

(J4) Hiraku Morita, Nuttapong Attrapadung, Tadanori Teruya, Satsuya Ohata, Koji Nuida, Goichiro Hanaoka: Constant-Round Client-Aided Two-Server Secure Comparison Protocol and Its Applications Volume and Number: Vol.E103-A(1):21-32 (2020)

(J3) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: On the Security of Non-Interactive Key Exchange against Related-Key Attacks. IEICE Transactions 100-A(9): 1910-1923 (2017)

(J2) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: On the Security of Schnorr Signatures, DSA, and ElGamal Signatures against Related-Key Attacks. IEICE Transactions 100-A(1): 73-90 (2017)

(J1) Shuya Abe, Kentaro Inui, Kazuo Hara, Hiraku Morita, Chitose Sao, Megumi Eguchi, Asuka Sumida, Koji Murakami, Suguru Matsuyoshi: Mining personal experiences and opinions from Web documents. Web Intell. Agent Syst. 9(2): 109-121 (2011)