Curriculum Vitae

Shin’ichiro Matsuo, Ph.D.

Address: 2111 Wisconsin Ave NW Apt 120 Washington DC 20007, USA
Phone: +1-617-866-3052
E-mail: matsuo@mac.com

1. Summary

- I am a research professor of computer science at Georgetown University and co-PI at CyberSMART Research Center.

- I have three aspects of specialities. Research scientist in cryptography, expert in international standardization and building new architecture for security evaluation of information systems

- Deeply involved in blockchain academic research
  - Building an international neutral academic research test network “BSafe.network.” Co-founder of this project.
  - Research on security analysis on blockchain technology.
  - Co-chair of Blockchain Governance Initiative Network (BGIN)
  - Committed to ISO TC307 standardization as a committee member and liaison between ISO/IEC JTC1 SC27 and ISO TC307

- Research scientist and system designer in cryptography and its application
  - Designed cryptographic protocols from fundamental protocols to application protocols include followings.
    - Key management protocols suitable for smartphone and RFID tags
    - Digital cash schemes
    - Cryptocurrency and blockchain technology
    - Digital time-stamping schemes based on PKI and hash-chain
    - Digital voting schemes
    - Privacy enhancing technologies including anonymous digital signature and anonymous entity authentication protocols
  - Above schemes are accepted high level academic conferences, patented and implemented into software (server side and client side) and hardware (RFID tag and FPGA).
  - Design many mechanisms to securing huge information systems including e-banking, credit-card system, governmental ID system, PKI and certificate authority, at the laboratory of NTTDATA.
  - In 2011, we achieved the world record of solving discrete logarithm problem (DLP) over elliptic curve. This result is referred by a guideline of secure use of cryptography.

- Expert in international standardization of cryptography and information security.
  - I was a head of Japanese national body of ISO/IEC SC27/WG2. I am an editor of ISO/IEC 29128 (Verification of Cryptographic Protocols), ISO/IEC 20009-2 (Anonymous Entity Authentication), ISO/IEC 19592 (Secret Sharing Scheme) and Standing Document 4 (Analysis and status of cryptographic algorithms).
  - I am an editor of ISO TR23576 (Security of Digital Asset Custodians).
  - I was a member of Japanese Governmental committees for cryptographic technologies
  - I found an international consortium on security evaluation of cryptographic protocols, named "CELLOS". US, European and Japanese universities, research institutes, companies and individuals participate this consortium. I am a chair of technical working group of this consortium.
  - Proposed a new evaluation criteria of hash functions suitable for real information system and a common evaluation platform for SHA-3 candidates, and conducted evaluation for 14 finalists.The result was presented at NIST SHA-3 candidate workshop and gave contribution to the selection.

VISA Status: Legal Permanent Resident (Green card holder) in United States

2. Work Experience

- July 1st, 2019 - Present

Head of Blockchain Research
NTT Research Institute

- October 1st, 2017 - Present

Research Professor
Georgetown University

- August 1st, 2016 - Present

Project professor
Keio University

- May 25th, 2016 – September 1st, 2019

Research Affiliate - Director's Liaison for Financial Cryptography
MIT Media Lab

- April 1st, 2016 – Present

Research Fellow
University of Tokyo

- December 26th, 2015 – May 31st, 2019

Chief Security Scientist
MagicCube Inc.
Abstract: The main mission are designing secure communication protocol and evaluating security of its implementation for mobile computing environment.

- April 1st 2014 – December 25th 2015

Managing Director
National Institute of Information and Communications Technology (NICT)
Abstract: The main mission are planning and managing R&D strategy and deployment strategy of NICT research activities.

- April 1st 2012 – March 31st, 2015 (3 years teaching)

Part-time lecturer
Tsuda College
Class Title: Information Security
Abstract: This is a class for undergraduate student. This class contains basic concept of information security and its management, fundamental techniques including cryptography, digital signature, authentication, virus prevention and privacy issues.

- April 1st 2011 – March 31st 2014

Director of Security Architecture Laboratory
National Institute of Information and Communications Technology (NICT)
Abstract: The main topics of this laboratory are (1) applying cryptography to ensure system security and privacy for cloud computing and IoT, and (2) risk evaluation of end-to-end information system and giving guidances for proper technology use. In this laboratory, many papers were accepted by top conferences including CRYPTO, EUROCRYPT, ASIACRYPT, TCC and PKC. I supervised these works. I also founded an international consortium on security evaluation of cryptographic protocols, named “CELLOS.” US, UK, French, Switzerland, Estonian and Japanese universities and research institutes joined this consortium.

- October 1st 2013 – March 31st 2014 (6 months teaching)

Part-time lecturer
Chuo University
Class Title: Advanced course of cryptography
Abstract: This is a class for Ph.D student. This class contains mathematical treatment of cryptography and its application including modeling, how to prove the security on symmetric key cryptography, public key cryptography and cryptographic protocols.

- August 1st 2012 – March 31st 2013 (10 months teaching)

Part-time lecturer
Takushoku University
Class Title: Information Security
Abstract: This is a class for undergraduate student. This class contains basic concept of information security and its management, fundamental techniques including cryptography, digital signature, authentication, virus prevention and privacy issues.

- April 1st 2009 – March 31st 2011

Senior Research Scientist
National Institute of Information and Communications Technology (NICT)
Abstract: I designed many cryptographic protocols for low power devices and RFID and usable cryptographic protocols. I also evaluate many cryptographic primitives for Japanese government and SHA-3 contest. They contain achieving the world record of solving discrete logarithm problem, giving guidance of proper cryptography and protocol use for government systems. I had also a head of Japanese committee of ISO/IEC standardization for security technology.

- April 1st 2006 – March 31st 2009 (3 years teaching)

Part-time Lecturer
Tokyo Institute of Technology
Title: Communication Systems
Abstract: This is class for master course student. This class covers how to design the communication systems. This includes designing combinations of network, storage, computational power with aligning to requirements of actual social needs. This also includes how to secure the system in the design phase.

- April 1st 1996 – March 31st 2009

Senior Research Scientist
Name of Employer: NTT Data Corporation
Abstract: I designed many cryptographic protocols for digital cash system (with Bank of Japan), Intelligent Transportation System, E-voting, time-stamping and authentication. The protocols are proposed through academic conferences and papers, implemented in the experimental systems, and standardized.

3. Education

- Tokyo Institute of Technology

Ph. D, Computer Science
2001 – 2003

- Tokyo Institute of Technology

Master's Degree, Computer Science
1994 – 1996

- Tokyo Institute of Technology

Bachelor's Degree, Computer Science
1990 – 1994

- Komaba Toho High School

High School
1987 – 1990

4. Awards

- Award on New International Standard

Information Technology Standard Commission of Japan
February 2014
Award for finalizing of standardization of ISO/IEC 20009-2 "Anonymous Entity Authentication - Mechanism based on group public key”

- Award on New International Standard

Information Technology Standard Commission of Japan
February 2012
Award for finalizing of standardization of ISO/IEC 29128 "Verification of Cryptographic Protocols"

- Award for outstanding contribution in International Standardization

Information Technology Standard Commission of Japan
April 2014
Award for outstanding and continuous activities and results in ISO/IEC SC27

- Distinguished service award

The institute of Electronics, Information and Communication Engineers
May 2010
Award for long effort for editing journals on information security and cryptography

5. External Funds and Grant

- NSF I/UCRC CyberSMART Research Center

Grants-in-Aid for Scientific Research
NSF
July 2021 - June 2026
Amount: $1,000,000

- A research on design theory of cryptographic techniques which have easily verifiable security by third party

Grants-in-Aid for Scientific Research
Japan Society for the Promotion of Science
April 2014 - March 2019
Amount: $50,000 / year

- A Research on usable cryptographic protocols and their mathematical security model

Grants-in-Aid for Scientific Research
Japan Society for the Promotion of Science
April 2010 - March 2011
Amount: $5,000 / year

- A research on design theory of cryptographic protocols for low-power devices with considering implementation

Grants-in-Aid for Scientific Research
Japan Society for the Promotion of Science
April 2012 - March 2015

Amount: $12,000 / year

- A research on cryptographic techniques and digital signatures which have continuous security

National research institute of Information and Communications Technology
April 2008 - March 2009
Amount: $700,000 / year

6. Publications

7.1. Doctoral Thesis

“A Study on Cryptographic Protocols for Electronic Commerce,” September 30th, 2003, Tokyo Institute of Technology
Supervisor: Wakaha Ogata and Kaoru Kurosawa

7.2. Journal Paper

(1) Shin’ichiro Matsuo, and Hikaru Morita, “Secure Protocol to Construct Electronic Trading,” IEICE Transaction of Fundamentals Vol.E84-A No.1 pp.281-288, 2001.

(2) Shin’ichiro Matsuo and Wakaha Ogata, “Electronic Ticket Scheme For ITS,” IEICE Transaction of Fundamentals Vol.E86-A No.1 pp.142-150, 2003.

(3) Shin’ichiro Matsuo and Wakaha Ogata, “Matching Oblivious Transfer: How to Exchange Valuable Data,” IEICE Transaction of Fundamentals Vol.E86-A No.1 pp.189-193, 2003.

(4) Natsuki Ishida, Shin’ichiro Matsuo and Wakaha Ogata, “Efficient Divisible Voting Scheme,” IEICE Transaction of Fundamentals Vol.E88-A No.1 pp.230-238, 2005.

(5) Yasumasa Hirai, Takashi Kurokawa, Shin’ichiro Matsuo, Hidema Tanaka and Akihiro Yamamura, “Classification of Hash Functions Suitable for Real-life Systems,” IEICE Transaction of Fundamentals Vol.E91-A No.1, 2008.

(6) Miroslav Knezevic, Kazuyuki Kobayashi, Jun Ikegami, Shin'ichiro Matsuo, Akashi Satoh, Ünal Koçabas, Junfeng Fan, Toshihiro Katashita, Takeshi Sugawara, Kazuo Sakiyama, Ingrid Verbauwhede, Kazuo Ohta, Naofumi Homma, Takafumi Aoki: “Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates,” IEEE Trans. VLSI Syst. 20(5): 827-840 (2012)

(7) Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, Tsuyoshi Takagi: “Solving a 676-Bit Discrete Logarithm Problem in $GF(3^{6n})$,” IEICE Transactions 95-A(1): 204-212 (2012)

(8) Takeshi Takahashi, Joona Kannisto, Jarmo Harju, Seppo Heikkinen, Bilhanan Silverajan, Marko Helenius, Shin’ichiro Matsuo, “Tailored Security: Building Nonrepudiable Security Service-Level Agreements,” IEEE VT magazine, Vol 8. No. 3, 2013

(9) Daisuke Moriyama, Shin’ichiro Matsuo and Miyako Ohkubo, “Relations among Notions of Privacy for RFID Authentication Protocols,” IEICE Transactions E-97A. 2014

(10) Joona Kannisto, Takeshi Takahashi, Jarmo Harju, Seppo Heikkinen, Marko Helenius, Shin'ichiro Matsuo, Bilhanan Silverajan, “A Non-repudiable Negotiation Protocol for Security Service Level Agreements,” International Journal of Communication Systems, 2014.

(11) Yuta Takanashi, Shin’ichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, Hirotoshi Sato. Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging

Blockchain-Based Financial Ecosystem, Part 1 of 2. Stanford Journal of Blockchain Law and Policy, 2020.

(12) Yuta Takanashi, Shin’ichiro Matsuo, John Jacobs, Eric Burger, Clare Sullivan, James Angel, Tatsuya Sato, Toshiki Hashirisaka, Hirotoshi Sato. Consideration on better tokenization practices and regulations concerning investor protection. CAPCO Journal #51: WEALTH & ASSET MANAGEMENT, 2020.

(13) Yuta Takanashi, Shin’ichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, Hirotoshi Sato. Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem, Part 2 of 2. Stanford Journal of Blockchain Law and Policy, 2020.

7.3. Refereed International Conference

(1) Shin’ichiro Matsuo, Takahiro Maekawa, Yoshiyuki Hashikawa, Hiroaki Sakamoto and Shigeyoshi Tamura,”Electronic Ticket for ITS,” In Proceedings of 8th ITS World Congress, Sydney, Australia, 2001.

(2) Shin’ichiro Matsuo and Wakaha Ogata, “A Method for Exchanging Valuable Data: How to Realize Matching Oblivious Transfer,” In Proceedings of ACM Symposium on Principles of Distributed Computing (PODC) 2003, pp.201, 2003, Boston, USA.

(3) Natsuki Ishida, Shin’ichiro Matsuo and Wakaha Ogata, “Divisible Voting Scheme,” In Proceedings of Information Security Conference (ISC) 2003, Lecture Notes in Computer Science 2851, pp.137-150, 2003, October 1-3, 2003, Bristol, UK.

(4) Shin’ichiro Matsuo and Hiroaki Oguro, “User-side Forward-dating Attack on Time-stamping Protocols,” In Proceedings of The Third International Workshop for Applied PKI, 2004, October 3-5, 2004, Fukuoka, Japan.

(5) Toshihiko Matsuo and Shin’ichiro Matsuo, “On Universal Composable Security of Time-stamping Protocol ,” Applied Public Key Infrastructure - 4th International Workshop: IWAP 2005, pp.169-181, 2005, IOS Press, September 21-23, 2005, Singapore.

(6) Yasumasa Hirai, Takashi Kurokawa, Shin’ichiro Matsuo, Hidema Tanaka and Akihiro Yamamura, “Classification of Hash Functions Suitable for Real-life Systems,” In Proceedings of NIST 2nd Cryptographic Hash Function Workshop, August 24-25, 2006, Santa Barbara, USA.

(7) Shin’ichiro Matsuo, Kunihiko Miyazaki, Akira Otsuka, David A. Basin: “How to Evaluate the Security of Real-Life Cryptographic Protocols? - The Cases of ISO/IEC 29128 and CRYPTREC,” Financial Cryptography Workshops 2010: Lecture Notes in Computer Science 6054, pp. 182-194, 2010.

(8) Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, Tsuyoshi Takagi: “Solving a 676-Bit Discrete Logarithm Problem in GF($3^{6}n$),” Public Key Cryptography 2010: Lecture Notes in Computer Science 6056, pp. 351-367, 2010.

(9) Shin’ichiro Matsuo, Le Trieu Phong, Miyako Ohkubo, Moti Yung: “Leakage-Resilient RFID Authentication with Forward-Privacy," RFIDSec 2010: Lecture Notes in Computer Science 6370, pp. 176-188, 2010.

(10) Kazuyuki Kobayashi, Jun Ikegami, Kazuo Sakiyama, Kazuo Ohta, Miroslav Knezevic, Ünal Koçabas, Junfeng Fan, Ingrid Verbauwhede, Eric Xu Guo, Shin'ichiro Matsuo, Sinan Huang, Leyla Nazhandali, Akashi Satoh: “Prototyping Platform for Performance Evaluation of SHA-3 Candidates. HOST 2010”, pp. 60-63, 2010

(11) Shin’ichiro Matsuo, Miroslav Knezevic, Patrick Schaumont, Ingrid Verbauwhede, Akashi Satoh, Kazuo Sakiyama and Kazuo Ota, “How Can We Conduct "Fair and Consistent" Hardware Evaluation for SHA-3 Candidate? ,” NIST Second SHA-3 Candidate Workshop 2010

(12) Le Trieu Phong, Shin'ichiro Matsuo, Moti Yung: “Leakage Resilient Strong Key-Insulated Signatures in Public Channel," INTRUST 2010: Lecture Notes in Computer Science 6802, pp. 160-172, 2010.

(13) Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, Kazuo Ohta: “A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication,” Financial Cryptography Workshops 2011: Lecture Notes in Computer Science 7126, pp. 70-87, 2011.

(14) Daisuke Moriyama and Shin’ichiro Matsuo, “Security/Privacy Models for "Internet of things": What should be studied from RFID-schemes? ”, NIST Workshop on Cryptography for Emerging Technologies and Applications, 2011.

(15) Daisuke Moriyama, Shin'ichiro Matsuo and Miyako Ohkubo, “Relation among the Security Models for RFID Authentication Protocol ,” In Proceedings of ECRYPT Workshop on Lightweight Cryptography, http://www.uclouvain.be/crypto/ecrypt_lc11/static/post_proceedings.pdf, 2011.

(16) Shin’ichiro Matsuo, Daisuke Moriyama, Moti Yung: “Multifactor Authenticated Key Renewal," INTRUST 2011: Lecture Notes in Computer Science 7222, pp.204-220, 2011.

(17) Takeshi Takahashi, Gregory Blanc, Youki Kadobayashi, Doudou Fall, Hiroaki Hazeyama, Shin'ichiro Matsuo, “Enabling secure multitenancy in cloud computing: Challenges and approaches,” (BCFIC), 2012

(18) Shin’ichiro Matsuo, Akira Kanaoka, Takeshi Takahashi, Tadashi Minowa, “Prototype System for Visualizing Security Risks on Mobile Device,” Symposium On Usable Privacy and Security (SOUPS); 06/2012”

(19) Takeshi Takahashi, Shin'ichiro Matsuo, Akira Kanaoka, Keita Emura, Yuuki Takano, “Visualization of user's end-to-end security risks”, Symposium On Usable Privacy and Security (SOUPS); 06/2012

(20) Daisuke Moriyama, Shin’ichiro Matsuo and Miyako Ohkubo, “Relations among Notions of Privacy for RFID Authentication Protocols,” ESORICS2012, Lecture Notes in Computer Science 7459, pp. 661-678, 2012.

(21) Takeshi Takahashi, Joona Kannisto, Seppo Heikkinen, Bilhanan Silverajan, Marko Helenius, Shin'ichiro Matsuo, Jarmo Harju, "An Accountable Security Mechanisms in Light of Security Service Level Agreement,” WWRF; 10/2012

(22) Shin’ichiro Matsuo, “Mobile Device Trust: How do we link social needs, technical requirements techniques and standards?”, INTRUST 2012, Lecture Notes in Computer Science 7711, pp. 63-64, 2012.

(23) Takeshi Takahashi, Keita Emura, Akira Kanaoka, Shin'ichiro Matsuo, Tadashi Minowa, “Risk Visualization and Alerting System: Architecture and Proof-of-Concept Implementation," SESP; 04/2013.

(24) Daisuke Moriyama, Miyako Ohkubo, and Shin'ichiro Matsuo, “A Forward Privacy Model for RFID Authentication Protocols,” WISTP 2013, Lecture Notes in Computer Science 7886, pp. 98-111, 2013.

(25) Takeshi Takahashi, Joona Kannisto, Seppo Heikkinen, Bilhanan Silverajan, Marko Helenius, Shin'ichiro Matsuo, Jarmo Harju, "Accountable Security Mechanism based on Security Service Level Agreement," The Eighteenth IEEE Symposium on Computers and Communications.

(26) Wakaha Ogata, Akira Kanaoka, Shin'ichiro Matsuo: "Toward Practical Searchable Symmetric Encryption," IWSEC 2013: Lecture Notes in Computer Science 8231, pp. 151-167, 2013.

(27) Dan Bogdanov, Keita Emura, Roman Jagomagis, Akira Kanaoka, Shin'ichiro Matuso and Jan Willemson, "A Secure Genetic Algorithm for the Subset Cover Problem and its Application to Privacy Protection," Workshop in Information Security Theory and Practice Series 2014

(28) Takeshi Takahashi, Joona Kannisto, Jarmo Harju, Akira Kanaoka, Yuuki Takano, Shin'ichiro Matsuo: Expressing Security Requirements: Usability of Taxonomy-Based Requirement Identification Scheme. SERVICES 2014: 121-128

(29) Takeshi Takahashi, Jarmo Harju, Joona Kannisto, Bilhanan Silverajan, Jarmo Harju, Shin'ichiro Matsuo: Tailored Security: Building Nonrepudiable Security Service-Level Agreements. CoRR abs/ 1403.7088 (2014)

(30) Shin'ichiro Matsuo and Pindar Wong, "How Formal Analysis and Verification Add Security to Blockchain-Based Systems", Blockchain Protocol Analysis and Security Engineering 2017, January, 2017, Stanford USA.

(31) Masahi Sato and Shin'ichiro Matsuo: Long-term public blockchain: Resilience against Compromise of Underlying Cryptography, IEEE Security and Privacy on the Blockchain (IEEE S&B) April 2017, Paris

(32) Masahi Sato and Shin'ichiro Matsuo: Long-term public blockchain: Resilience against Compromise of Underlying Cryptography, Workshop on Privacy, Security, Trust & Blockchain Technologies, ICCCN 2017, August 2017, Vancouver Canada.

(33) Jianan Su, Andrew Stange, Ryosuke Ushida, Shin'ichiro Matsuo. How to Dynamically Incentivize Sufficient Level of IoT Security. In Proc. of 4th Workshop on Trusted Smart Contracts, a workshop of Financial Cryptography and Data Security 2020., 2020.

(34) Shinichiro Matsuo, Effectiveness of Multi-stakeholder Discussions for Decentralized Finance: A Conference Report of CoDeFi 2020, In. Proc. of the 1st Workshop on Coordination of Decentralized Finance

(35) Michael Bartholic, Jianan Su, Ryosuke Ushida, Yusuke Ikeno, Zhengrong Gu and Shinichiro Matsuo, Proof of No-Work: How to Incentivize Individuals to Stay at Home, In. Proc. Of 4th International Workshop on Cryptocurrencies and Blockchain Technology - CBT 2020

(36) Yoko Shibuya Go Yamamoto Fuhito Kojima Elaine Shi Shin'ichiro Matsuo Aron Laszka, Short Paper: Selfish Mining Attacks Exacerbated by Elastic Hash Supply, In Proc. of Financial Cryptography 2021

(37) Kentaro Sako, Shin'Ichiro Matsuo and Sachin Meier, Fairness in ERC token markets: A Case Study of CryptoKitties, In Proc. of 5th Workshop on Trusted Smart Contracts

7.4. Invited Paper and keynote speech/lecture

(1) Shin'ichiro Matsuo, Takahiro Maekawa, Yoshiyuki Hashikawa, Hiroaki Sakamoto and Shigeyoshi Tamura,"Electronic Ticket for ITS," In Proceedings of Wireless Personal Mobile Communication (WPMC) 2001, S2K.3, pp.717-722, 2001, Aalborg, Denmark.

(2) Keynote speech “Cryptographic Protocol is and isn’t like LEGO,” IWSEC 2015.

(3) Key note speech “BSafe Network: Purpose, Development and Operation,” Workshop on Privacy, Security, Trust & Blockchain Technologies, ICCCN 2017, August 2017, Vancouver Canada (to appear).

(4) Invited Lecture, “Formal Analysis and Verification and Blockchain-Based Systems,” Joint lecture of MEMOCODE 2017 and FMCAD17, October 2017, Vienna Austria.

(5) Keynote speech, “The Future of Blockchain: Perspectives on Bitcoin,” Blockchain@UBC Mini-Conference on The Future of Blockchain, 2018

(6) Keynote speech, “Era of Elusiveness in Security and Privacy,” 14th International Conference on Information Security Practice and Experience

(7) Keynote speech, “Building a sound ecosystem through multi-stakeholder governance,” b.tokyo 2019.

7.5 Other Presentations in International Conference and Events

(1) University of Electro-Communications (2009)
“Next Step of CRYPTREC: New Evaluation Framework of Cryptographic Techniques for Japanese E-government”

(2) JWCAA (Joint Workshop on Cryptographic Algorithm and its Application) 2010
“Cryptographic algorithms in ISO/IEC JTC1/SC27 and CRYPTREC,”
“The Overview of Evaluation on Cryptographic Mechanisms in CRYPTREC”

(3) JWCAA (Joint Workshop on Cryptographic Algorithm and its Application) 2011
“Cryptographic algorithms in ISO/IEC JTC1/SC27 and CRYPTREC,”

(4) Shin’ichiro Matsuo, “A Platform on Evaluation of Secure Protocols,” NICT-ETRI Joint Workshop 2012

(5) JWCAA (Joint Workshop on Cryptographic Algorithm and its Application) 2012
“Cryptographic algorithms in ISO/IEC JTC1/SC27 and CRYPTREC,”

(6) Shin’ichiro Matsuo, “Risk Awareness in e-banking,” in Panel Discussion of Financial Cryptography 2013.

(7) JWCAA (Joint Workshop on Cryptographic Algorithm and its Application) 2013
“New CRYPTREC e-government recommended cipher list”

(8) 1st Bitcoin Scaling Workshop, “Lessons learnt from NIST SHA-3 competition for scaling Bitcoin,” September 13, 2015, Montreal Canada.

(9) New Context Conference 2016 Tokyo, “Academia makes Blockchain technology healthy”

(10) Fintech Summit 2016 Panel Discussion, “Dawn of Blockchain era”

(11) New Context Conference 2016 San Francisco, “How Can We Convince the Security of Blockchain in Theory?”

(12) CONSTRUCT 2017 Panel Discussion, “Academic Comparison of Protocols”

(13) MIT Bitcoin Expo 2017, “Building Neutral Bitcoin/Blockchain Research Network by Academia: BSafe.network”

(14) New Context Conference 2017 Tokyo, “Blockchain’s today and tomorrow are the scholar of yesterday”.

(15) Shin'ichiro Matsuo, "How Global Scale Academic Research Network helps Crypto-Economics Research," October 2017. Crypto Economics Security Conference: Berkeley USA.

(16) Shin'ichiro Matsuo, "Technology challenges toward maturing Blockchain," September 2017. Fintech Summit 2017: Tokyo Japan.

(17) Shin’ichiro Matsuo, “Virtual Currencies - Increasing the impact and importance of Virtual Currency -,” FinCoNet International Conference 2017

(18) Shin’ichiro Matsuo, “Blockchain Technology,” Penn Blokchcain Conference

(19) Shin’ichiro Matsuo, “How academia can help maturing blockchain technology and ecosystem,” xChain2: Blockchain for Supply Chain and Logistics Forum, 2018.

(20) Shin’ichiro Matsuo, “Governance of regulations and innovations - Data and Privacy,” New Context Conference 2018 Tokyo

(21) Shin’ichiro Matsuo, “Academic Research on (public) blockchain Direction and update of BSafe.network,” The 2nd Workshop Basing Blockchain

(22) Shin’ichiro Matsuo, “Panel discussion: Identity/Security/Supply Chain,” Unlocking Blockchain for Government

(23) Shin’ichiro Matsuo, “Blockchain X-boarder talk with tech community,” Fintech Summit 2018

(24) Shin’ichiro Matsuo. “Panel: Future of Finance: Multi-Stakeholder Governance for Blockchain Based New Financial Ecosystem,” DC Blockchain Summit 2019

(25) Shin’ichiro Matsuo, “Make Blockchain Mature: academic and multi-stakeholder process,” Consensus 2019

(26) Shin’ichiro Matsuo, “The BSafe.network: Academic research network,” Lecture series Spring 2019, University of Zurich Blockchain center

(27) Shin’ichiro Matsuo, “Global scale research network and multi-stakeholder collaboration,” Blockchain@UBC Annual Conference 2019

(28) Shin’ichiro Matsuo, “Activities of BSafe Network and the Next Steps for Multi-Stakeholder Discussions.” G20 meets G-20: Blockchain Multi-stakeholder Workshop

(29) Shin’ichiro Matsuo, “Revisiting Security of Crypto Assets,” Fintech Summit 2019

(30) Shin’ichiro Matsuo, “Legendary Talk - Implication of Governance for DeFi as Learned From Wisdom of Internet Governance,” Fintech Summit 2019

(31) Shin’ichiro Matsuo, “Lecture 1: Why we need Multi-stakeholder discussion - What G20 discussed,” Decentralized Financial Architecture Workshop

(32) Shinichiro Matsuo, “Designing Multi-stakeholders Cooperation in Blockchain-based Economy - New Governance System for the DeFi,” Fintech Summit 2019

(33) Shin’ichiro Matsuo, “An Open, Global and Multi-Stakeholder Platform for Financial Diversity - New Genesis -” Blockchain Global Governance Conference (BG2C)

(34) Shin’ichiro Matsuo, “Re-designing Financial and Social Systems After the Pandemic - Maximizing Social Welfare with Decentralized Technologies,” Blockchain Global Governance Conference (BG2C)

29.International Standard

- ISO/IEC 29128, “Verification of Cryptographic Protocols”
- ISO/IEC 20009-2, “Anonymous Entity Authentication - Mechanisms based on signatures using a group public key“
- ISO/IEC 19592-1, “Secret Sharing Scheme - Fundamental mechanisms”
- ISO/IEC SC27/WG2 Standing document 4, “Analysis and Status of Cryptographic Algorithm”
- ISO TR 23576, Security of digital asset custodians
- Committee member of ISO/IEC JTC1 SC27/WG2 (Information security, cryptographic techniques) and ISO TC307 (Blockchain and Distributed Ledger Technology)

30.Patents

- Electronic Cash System/Method for payment to plural receivers

Japan 3558544
Issued August 25, 2004

- System and method for supporting use of electronic ticket

Japan 3693969
Issued September 14, 2005

- Electronic voting system, voting data generating server, terminal equipment, tabulation server and computer program

Japan 3910529
Issued April 25, 2007

- Apparatus and method for lapse confirmation

Japan 4071474
Issued April 2, 2008

- Security Level Management System using State Certificate

Japan 4330973
Issued September 16, 2009

- Time stamp system, time stamp requesting device, time stamp verifying device and computer program

Japan 4566567
Issued October 20, 2010

- Attribute Information Management System, Information Summary System, Terminal device, Authentication organization server, Management Server and Program

Japan 4574212
Issued November 4, 2010

- Password authentication key exchange device, system, method, and computer program
Japan 4757591
Issued August 24, 2011

- Information Processing Apparatus, Information Processing System and Program
Japan 4762673
Issued August 31, 2011

- Protection method of secret information and communication apparatus
Japan 4794970
Issued October 19, 2011

- Server device, client device, method for exchanging shared password, and computer program
Japan 4818702
Issued November 16, 2011

- System and program for generation of anonymous identification information
Japan 4822842
Issued November 14, 2011

- Storage service system and file protection program
Japan 5162396
Issued March 13, 2013

31.Editorial Board and Editorial Committee

- Special Issue on Cryptography and Information Security
The Institute of Electronics, Information and Communication Engineers
January 2008 – January 2010

- LEDGER Journal
Editorial Committee member
September 2015 – Present

- IEEE Transactions on Dependable and Secure Computing
September 2019 - Present

32. Program Committees

- Program Committee member
Security Standardization Research
January 2014 – Present

- Program Committee member
International Conference on Trusted Systems
April 2011 –

- Program Committee member
W3C Blockchain and the Web Workshop

- Program Committee Chair
Security Standardization Research 2015

- Program Committee Chair
Symposium on Cryptography and Information Security 2007

- Steering Committee Member
Security Standardization Research

- Program Committee Member
W3C Workshop on Distributed Ledgers on the Web

- Program Committee Member
Scaling Bitcoin Workshop 2016

- Program Committee Member
ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC) 2017

- Program Committee Member
IEEE Security and Privacy on the Blockchain (IEEE S&B) 2017

- Program Committee Member
2nd International Workshop on Linked Data and Distributed Ledger

- Program Committee Member
International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2017), ESORICS 2017

- Program Committee Member
CRYPTO-ECONOMICS SECURITY CONFERENCE 2017

- Program Committee Chair
Scaling Bitcoin 2018

- Program Committee Blockchain Track Chair
Code Blue 2018

- Program Committee Member
International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2018), ESORICS 2018

- Program Committee Member
Blockchain Protocol Analysis and Security Engineering 2018

- Program Committee Member
Scaling Bitcoin 2019

- Program Committee Blockchain Track Chair
Code Blue 2019

- Program Committee Member
International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2019), ESORICS 2019

- Program Committee Member
Security Standardization Research 2019

- ACM MobiHoc Workshop on Blockchain for Network Resource Sharing (BlockNet) 2020

- Program Committee Member
International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2020), ESORICS 2020

- Program Committee Blockchain Track Chair
Code Blue 2020

- Program Committee Member

International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2021), ESORICS 2021

- Program Committee Member

3rd Conference on Blockchain Research & Applications for Innovative Network and Services (BRAINS) 2021

- Program Co-Chair

IEEE International Conference on Blockchain and Cryptocurrency (IEEE IECB) 2022

33. Reviewer

- AsiaCrypt
- RFIDSec Asia
- INTRUST
- IWSEC
- Indocrypt
- ACISP
- Security Standardization Research
- International Conference on Trusted Systems
- Information Security Conference (ISC)
- IEEE Transactions on Vehicular Technology
- IEICE transactions of fundamentals
- IT Transactions
- International Journal of Information Security
- Journal of Information Procession Society of Japan

34.Other Committees

- Member
  Fintech study group, Bank of Japan
  April 2016 - Present

- Expert
  The Panel of Experts on Fintech Start-ups, Financial Agency Services
  May 2016 - Present

- Head of Japan National Body committee (HoD of Japan NB)
  JAPAN national body of ISO/IEC JTC1 SC27/WG2
  February 2011 – December 2015

- Chair of the technical working group
  Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) Consortium
  December 2013 – Present

- Member of Information Security Committee
  The Institute of Electronics, Information and Communication Engineers
  April 2005 – Present

- Member of Computer Security Committee
  Information Processing Society of Japan
  May 2014 – Present

- Committee member
  ITU Japanese mirroring committee on Information Security
  January 2012 – March 2015

- Member
  Advisory Board for Cryptographic Technology, CRYPTREC, Japanese Govenment
  May 2011 – March 2015

- Member
  Cryptographic Operation Committee, CRYPTREC
  April 2010 – March 2013

- Member
  Cryptographic Techniques Study Working Group, CRYPTREC
  April 2010 – March 2013

- Member
  Japanese Governmental Committee on Risk evaluation method
  October 2012 – March 2015

35.Membership

- International association for cryptologic research (IACR)
- International Financial Cryptography association (IFCA)
- The Institute of Electronics, Information and Communication Engineers (IEICE)
- IEEE
- ACM

36. Interests

- Securing the society. Not only finding attacks, but also building ecosystem to secure the computing environment.
- Cryptography and cryptographic protocol for real-life application
- Crypto-currency, Blockchain and its ecosystem
- Security evaluation of ICT systems
- Privacy enhancing technology
- International standardization and deployment