



Keitaro Hashimoto

Education

- 2020–2023 **Doctor of Engineering (Ph.D.)**, *Tokyo Institute of Technology*, Tokyo, Japan
Post-quantum key exchange protocols for secure messaging. Supervised by Wakaha Ogata (Tokyo Institute of Technology)
- 2018–2020 **Master of Engineering**, *Tokyo Institute of Technology*, Tokyo, Japan
Major: Information and communication engineering, specialized in cryptography
- 2014–2018 **Bachelor of Engineering**, *Tokyo Institute of Technology*, Tokyo, Japan
Major: Computer sciences

Experience

- 04/2023–Now **Researcher**, *National Institute of Advanced Industrial Science and Technology (AIST)*, Tokyo, Japan
- 04/2022–03/2023 **JSPS Research Fellowship for Young Scientists**, *Japan Society for the Promotion of Science*, Tokyo, Japan
- 07/2022 **Visiting internship**, *PQShield SAS*, Paris, France
- 06/2020–03/2023 **Research Assistant**, *National Institute of Advanced Industrial Science and Technology (AIST)*, Tokyo, Japan
- 08/2018–09/2018 **Summer internship**, *Nippon Telegraph and Telephone Corporation (NTT)*, Tokyo, Japan
- 08/2017–09/2017 **Summer internship**, *Infosec Corporation*, Tokyo, Japan

Teaching

- 08/2019 **Teaching Assistant**, *Tokyo Institute of Technology*, Tokyo, Japan
Teaching Assistant in the exchange Summer School with Zhejiang University
- 04/2019–08/2019 **Teaching Assistant**, *Tokyo Institute of Technology*, Tokyo, Japan
Teaching Assistant in the C Programming class and the Experiments on embedded systems class
- 06/2018–08/2018 **Teaching Assistant**, *Tokyo Institute of Technology*, Tokyo, Japan
Teaching Assistant in the C Programming class

Publications

Journals

- [HKKP22] Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest. An efficient and generic construction for signal's handshake (x3dh): Post-quantum, state leakage secure, and deniable. *Journal of Cryptology*, 35:78 pages, 2022.

* 14 April 1995

+81-50-3522-9656 • ✉ keitaro.hashimoto@aist.go.jp
🌐 keitaro-hashimoto.jp • in keitaro-hashimoto • 🗣 kaminomisiru
🆔 0000-0002-2232-9443 • 📄 smdloD4AAAAJ • 🐦 kaminomisiru_
🌐 09060142574 • Nationality: Japan

- [HO19] Keitaro Hashimoto and Wakaha Ogata. Unrestricted and compact certificateless aggregate signature scheme. *Information Sciences*, 487:97–114, 2019.
- [THO24] Kota Takahashi, Keitaro Hashimoto, and Wakaha Ogata. Chosen-ciphertext secure code-based threshold public key encryptions with short ciphertext. *Designs, Codes and Cryptography*, 92:277–301, October 2024.
- [Conferences](#)
- [CHH⁺24] Sohto Chiku, Keisuke Hara, Keitaro Hashimoto, Toi Tomita, and Junji Shikata. How to apply fujisaki-okamoto transformation to registration-based encryption. In *International Conference on Cryptology And Network Security (CANS)*. Springer, September 2024.
- [HKKP21] Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest. An efficient and generic construction for signal’s handshake (x3dh): Post-quantum, state leakage secure, and deniable. In Juan A. Garay, editor, *Public-Key Cryptography – PKC 2021*, pages 410–440, Cham, 2021. Springer International Publishing.
- [HKP⁺21] Keitaro Hashimoto, Shuichi Katsumata, Eamonn W. Postlethwaite, Thomas Prest, and Bas Westerbaan. A concrete treatment of efficient continuous group key agreement via multi-recipient pkes. In *ACM CCS 2021*. ACM DL, 2021.
- [HKP22] Keitaro Hashimoto, Shuichi Katsumata, and Thomas Prest. How to hide metadata in mls-like secure group messaging: Simple, modular, and post-quantum. In *ACM CCS 2022*. ACM DL, 2022.
- [HKP23] Keitaro Hashimoto, Shuichi Katsumata, and Thomas Prest. Metadata protection for mls and its variants. In *Real World Crypto 2023*, 2023.
- [HKP⁺24] Keitaro Hashimoto, Shuichi Katsumata, Eamonn W. Postlethwaite, Thomas Prest, and Bas Westerbaan. More efficient protocols for post-quantum secure messaging. In *Real World Crypto 2024*, March 2024.
- [YOH24] Hirofumi Yoshioka, Wakaha Ogata, and Keitaro Hashimoto. Towards a tightly secure signature in multi-user setting with corruptions based on search assumptions. In *Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL)*, August 2024.
- [ZHO24] Xichen Zhang, Keitaro Hashimoto, and Wakaha Ogata. Security model for authenticated key exchange, reconsidered. In *International Conference on Security and Cryptography for Networks (SCN)*. Springer, September 2024.
- [Others](#)
- [CHHS23] Sohto Chiku, Keitaro Hashimoto, Keisuke Hara, and Junji Shikata. Identity-based matchmaking encryption, revisited: Strong security and practical constructions from standard classical and post-quantum assumptions. Cryptology ePrint Archive, Report 2023/1435, September 2023.
- [HOT19] Keitaro Hashimoto, Wakaha Ogata, and Toi Tomita. Tight reduction for generic construction of certificateless signature and its instantiation from ddh assumption. Cryptology ePrint Archive, Report 2019/1367, 2019.

Talks

[International conference talks](#)

- 09/2024 **SCN**, *Security Model for Authenticated Key Exchange, Reconsidered.*, Amalfi, Italy
- 08/2024 **CFAIL**, *Towards a Tightly Secure Signature in Multi-User Setting with Corruptions Based on Search Assumptions*, Saint Barbara, USA

* 14 April 1995

☎ +81-50-3522-9656 • ✉ keitaro.hashimoto@aist.go.jp

🌐 keitaro-hashimoto.jp • in keitaro-hashimoto • 🗺 kaminomisosiru
 🆔 0000-0002-2232-9443 • © smdloD4AAAAJ • 🐦 kaminomisosiru_

🌐 09060142574 • Nationality: Japan

- 11/2022 **ACM CCS**, *How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum*, Los Angeles, USA
- 11/2021 **ACM CCS**, *A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs*, Virtual
- 05/2021 **PKC**, *An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable*, Virtual
- [Invited talks](#)
- 09/2023 **Forum on Information Technology (FIT)** , *How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum*, Virtual
- 09/2022 **Workshop on Cryptography and Information Security (WCIS)**, *A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs*, Virtual
- 07/2022 **Talk at ENS de Lyon**, *A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs*, Lyon, France
- 09/2021 **SCIS/CSS Invited Session in IWSEC**, *Design and Implementation of a Post-Quantum Authenticated Key Exchange Protocol for Signal*, Virtual

Miscellaneous

Talks presented by my coauthors

- 09/2024 **CANS**, *How To Apply Fujisaki-Okamoto Transformation To Registration-Based Encryption*, Cambridge, England, Presented by Sohto Chiku
- 03/2024 **RWC**, *More efficient protocols for post-quantum secure messaging*, Toronto, Canada, Presented by Thomas Prest
- 03/2023 **RWC**, *Metadata Protection for MLS and Its Variants*, Tokyo, Japan, Presented by Shuichi Katsumata
- 02/2023 **9th ETSI/IQC Quantum Safe Cryptography Event**, *A Post-Quantum Construction for Signal's Handshake (X3DH)*, Virtual, Presented by Thomas Prest
- 12/2022 **4th PQC Standardization Conference**, *An Efficient and Generic Construction for Signal's Handshake (X3DH)*, Virtual, Presented by Thomas Prest

Languages

Japanese	Native
English	Intermediate
French	Beginner
Chinese	Beginner

Certifications

- 03/2021 **Improve Your English Communication Skills Specialization**, Coursera, A3ZGXJ8RWW5T
- 03/2021 **Introduction to Mathematical Thinking**, Coursera, WQY3UEVLZSEE
- 12/2015 **Applied Information Technology Engineer**, Ministry of Economy, Trade and Industry, AP-2015-10-03112
- 10/2014 **Fundamental Information Technology Engineer**, Ministry of Economy, Trade and Industry, FE-2014-10-04834

Computer skills

* 14 April 1995

☎ +81-50-3522-9656 • ✉ keitaro.hashimoto@aist.go.jp

🌐 keitaro-hashimoto.jp • in keitaro-hashimoto • 🌐 kaminomisosiru
 🆔 0000-0002-2232-9443 • 📄 smdloD4AAAAJ • 🐦 kaminomisosiru_
 🌐 09060142574 • Nationality: Japan

References

- Wakaha Ogata (Ph.D. advisor): ogata.w.aa@m.titech.ac.jp

* 14 April 1995

☎ +81-50-3522-9656 • ✉ keitaro.hashimoto@aist.go.jp
🌐 keitaro-hashimoto.jp • **in** [keitaro-hashimoto](#) • 🔄 [kaminomisosiru](#)
🆔 0000-0002-2232-9443 • © [smdloD4AAAAJ](#) • 🐦 [kaminomisosiru_](#)
🌐 09060142574 • Nationality: Japan