Jun Kurihara

Graduate School of Information Science,
University of Hyogo
7-1-28 Minatojima-minamimachi, Chuo-ku,
Kobe, Hyogo 650-0047, Japan

E-mail: kurihara@ieee.org
Web (Personal): https://junkurihara.github.io/
Web (Lab): https://secarchlab.github.io/
GitHub: https://github.com/junkurihara
LinkedIn: https://www.linkedin.com/in/junkurihara

Summary and Qualification

- B.E. in computer science, M.E. in communication engineering, and Ph.D. in engineering all from Tokyo Institute of Technology, Japan, in 2004, 2006, and 2012, respectively.
- Deep and wide R&D experiences in networking architecture, information security, applied cryptography, coding-theoretic techniques, at a telecommunication company, a startup software company, and a university for 10+ years in total.
- Experiences of planning and managing large projects to launch a new mobile core network.
- Experiences of launching a security start-up project as a main contributor and architect.
- Experiences of teaching students at universities, and lecturing engineers at companies.
- Active contribution to open source software of cryptography, security, and networking.
- More than 30 scientific papers published in international conferences and journals including IEEE and ACM ones. 50+ patents applied within 10 years.
- Excellent coding experiences for prototyping and product development with a variety of languages and environments, e.g., TypeScript/JavaScript, Rust, Go, Python, etc. (See my GitHub).
- Outstanding interpersonal, motivational, and presentation skills.
- Excellent communication skills in oral and written English and Japanese.

Education

Tokyo Institute of Technology
Ph.D. in Engineering, September 2012
Dissertation: A Study on Design and Security Analysis of Secret Sharing Schemes
Supervisor: Professor Tomohiko Uyematsu

Tokyo Institute of Technology
M.E. in Communications and Integrated Systems, March 2006
Thesis: Nonbinary Coding Systems Approaching the Shannon Limit by Using Product Accumulate Codes
Supervisor: Professor Tomohiko Uyematsu

Tokyo Institute of Technology
B.E. in Computer Science, March 2004
Thesis: Software Radio Receiver Utilizing RF Filter Bank
Supervisor: Professor Hiroshi Suzuki

Work Experience

Associate Professor

Graduate School of Applied Informatics, University of Hyogo, Japan

2020 Jan.–Present

His responsibility includes researching the wide range of security and dependability in networking and computing. Currently he is mainly working on the following research and development projects.

Security, privacy and anonymity in Domain Name Systgem (DNS)

He developed and leads an experimental software project of anonymized DNS protocols called *Mutualized oblivious DNS* (μODNS) by fully leveraging his networking and cryptography R&D background. Extending IETF draft technologies, implementing its proof-of-concept software as open-source software, and operating developed DNS servers on the Internet. (See GitHub repos for codes)

Private information retrieval

He researches and develops coding-theoretic protocols of *private information retrieval* to hide the requester's interests from the server's observation and preserve the privacy of the requester. He especially focuses on the dependability of the protocol against the active attacks, i.e., destruction of the information.

He also lectures mathematics, security, and networking to university students and engineers. In particular, he has classes of lectures in "Information Security" for the basics of cryptography, "Network Security" for security protocols in networks, and "Security Engineering"[1] for the standardization technologies used on the Internet, e.g., IETF RFC.

Principal Researcher/Software Engineer

Zettant Inc., Japan

2018 Jan.–Present

He mainly works on research and development projects related to cryptographic primitive libraries, blockchain architecture, security, and access control systems. In particular, he launched the project of a security platform, called *SecurityHub*, enabling the easy-to-use and secure usage of crypto keys. In the project, he presented the initial concept of SecurityHub, designed its initial and detailed architectures, and has already submitted some patents. Currently, he is leading its development to release the platform as a service shortly. He is also committing an open-source software project called *jscu* that is a TypeScript cryptographic library providing unified APIs for browsers and Node.js.

Visiting/Cooperate Scholar

Advanced Telecommunication Research Institute International (ATR), Japan

2019 Jun.–2019 Dec. (Cooperate Researcher), and 2020 May–Present (Visiting Scholar).

He works on research and development projects related to security in networking architectures including ICN as a researcher.

Strategic Planner, Engineer

KDDI Corp., Japan

2016 Oct.–2017 Dec.

His responsibility mainly included the followings related to the mobile core network architecture:

- Planning the mobile core network architecture and its road-map for the future (e.g., LPWA, 5G, etc.) mobile services.

- Designing the mobile core network structure (e.g, 4G Evolved Packet Core) and its platform structure (e.g., charging system, networking functions behind the PGW, etc.) for the various business demands.

- Planning (negotiating) the strategic collaboration with global network operators and hardware/software manufactures in the various technological area (e.g., LPWA, 5G networking use cases, etc.).

[1] The slide deck of Security Engineering is fully available on GitHub `https://github.com/junkurihara/lecture-security_engineering`.

Researcher

KDDI R&D Labs., Inc., Japan
2006 Apr.–2016 Sep.
He mainly worked on the following research projects for the security and networking architecture.

Research project on information centric networking (ICN) architecture and its security, 2013–2016

Started this project in order to design and lead the clean-slate ICN architecture in KDDI core network. First created a new access control framework during the one-year stay in Palo Alto Research Center (PARC), CA, USA as a visiting researcher. Next, struggled with the reduction of router's workload and created a new technology to realize a dramatically-lightweight processing using a grouping method of request messages. Thirdly, as a member of ICN2020 project, launched a new sub-project on a novel ICN-specific method for censorship circumvention, which maximize the benefit of ICN like in-network caching.

Research project on secure and reliable network coding/distributed storage, 2011–2015

Launched this project in order to realize efficient and reliable communication in the network of the future. First proposed an explicit construction of universal strongly secure network coding scheme using maximum rank distance codes, which had been remained an open question. Next, pioneered the theory of new code parameters generalizing the rank distance, and revealed that these parameters precisely characterize the security and error-correction capability of universal secure network coding scheme.

Research project on secret sharing schemes and linear error-correcting codes, 2010–2014

Launched this project in order to design secret sharing schemes suitable for cryptographic applications. Revealed that the security performance of secret sharing schemes based on linear codes is precisely expressed in terms of parameters of the codes, which are called relative dimension/length profile and relative generalized Hamming weight. Further, demonstrated that security analysis in existing researches by the minimum Hamming weight are loose and not precise.

Development of authentication method for broadcasting stream, 2007–2009

Proposed a new authentication method for TV broadcasting stream, which is suitable for resource constraint environments. Developed mobile terminals with the method, and demonstrated its efficiency and effectiveness. The mobile terminals which the scheme have been used at the demonstration in the 34th G8 summit took place in Toyako, Hokkaido, Japan.

Design of secret sharing schemes and their applications, 2006–2012

Pioneered this area of high-speed secret sharing schemes. Proposed a novel construction of a secret sharing scheme realizing extremely rapid computations, which uses only exclusive-or operations to encode and decode the secret data. Currently, this novel scheme is used in several commercial services of KDDI and other companies as a core technology, e.g., a secure distributed file system, a backup service using multiple cloud storage services, etc. The core library for the scheme itself is released as a product called "SProDa (secure protection of data)" from KDDI R&D Labs., Inc. (See http://www.kddilabs.jp/english/products/sproda.html.)

Visiting Researcher

Palo Alto Research Center, CA, USA
2013 Sep.–2014 Sep.

Research project on access control in information centric networking (ICN), 2013–2014

Launched this project in order to design a ICN-specific framework for access control. Designed the framework using a new network message called manifest, which flexibly realizes arbitrary access control instances.

Appendix: List of Publications, Grants and Other Qualifications

Publications

Peer-Reviewed Journal Articles and Letters

1. J. Kurihara, T. Nakamura and R. Watanabe, "Private information retrieval from coded storage in the presence of omniscient and limited-knowledge Byzantine adversaries", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E104-A, no. 9, pp. 1271–1283, Sep. 2021.

2. Y. Koike, T. Hayashi, J. Kurihara and T. Isobe, "Virtual Vault: A practical leakage resilient scheme using space-hard ciphers," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E104-A, no. 1, pp. 182–189, Jan. 2021.

3. J. Kurihara, and T. Nakamura, "On the resistance to Byzantine and unresponsive servers in code-based PIR schemes," *IEICE Communications Express*, vol. 9, no. 7, pp. 342–347, Jul. 2020.

4. K. Ueda, K. Yokota, J. Kurihara, A. Tagami, "Two-level named packet forwarding for enhancing the performance of virtualized ICN router," *IEICE Transactions on Communications*, vol. E102-B, no. 2, pp. 1813–1821, Sep. 2019.

5. J. Kurihara, K. Yokota, and A. Tagami, "List interest: Simply packing interests dramatically reduces router workload in content-centric networking," *IEICE Transactions on Communications*, vol. E99-B, no. 12, pp. 2520–2531, Dec. 2016.

6. J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding" *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

7. J. Kurihara, and Y. Miyake, "Securing distributed storage systems based on arbitrary regenerating codes," *IEICE Communications Express*, vol. 2, no. 10, pp.442–446, Oct. 2013.

8. J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2012.

9. Y. Nakano, J. Kurihara, S. Kiyomoto, and T. Tanaka, "Stream cipher-based hash function and its security," *Revised Selected Papers in the 7th International Joint Conference e-Business and Telecommunications, ICETE 2010, Athens, Greece, July 26–28, 2010*, ser. Communications in Computer and Information Science, vol. 222, Heidelberg, Germany: Springer-Verlag, pp. 188–202, 2012.

10. J. Kurihara, and T. Uyematsu, "A novel realization of threshold schemes over binary field extensions," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 6, pp. 1375–1380, Jun. 2011.

11. J. Kurihara, S. Kiyomoto, R. Watanabe, and T. Tanaka, "A stream authentication method for one-seg broadcasting," *Journal of the Institute of Image Information and Television Engineers*, vol. 64, no. 12, pp. 1921–1932, Dec. 2010. (in Japanese)

12. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A fast (k, L, n)-threshold ramp secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E92-A, no. 8, pp. 1808–1821, Aug. 2009.

13. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "On a fast (k, n)-threshold secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 9, pp. 2365–2378, Sep. 2008.

14. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A fast $(3, n)$-threshold secret sharing scheme using exclusive-or operations," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 1, pp. 127–138, Jan. 2008.

15. A. Deininger, S Kiyomoto, J. Kurihara, and T. Tanaka, "Security vulnerabilities and solutions in mobile WiMAX," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, no. 11, pp. 7–15, Nov. 2007.

Peer-Reviewed Conference Proceedings

1. R. Watanabe, A. Kubota, and J. Kurihara, "Resource Authorization Methods for Edge Computing," to Appear in *Proceedings of the 36-th International Conference on Advanced Information Networking and Applications (AINA 2022)*, Sydney, Australia (Virtual), Apr. 13-15, 2022.

2. K. Suksomboon, A. Tagami, A. Basu, and J. Kurihara, "In-device proxy re-encryption service for information-centric networking access control," in *Proceedings of the 43rd IEEE Conference on Local Computer Networks (LCN 2018)*, Chicago, IL, USA, Oct. 1–4, 2018, pp. 303–306.

3. K. Suksomboon, A. Tagami, A. Basu, and J. Kurihara, "IPRES: In-device proxy re-encryption service for secure ICN," in *Proceedings of the 4th ACM Conference on Information-Centric Networking (ICN 2017)*, Berlin, Germany, Sep. 26–28, 2017, pp. 176–177.

4. K. Ueda, K. Yokota, J. Kurihara, and A. Tagami, "Towards the NFVI-assisted ICN: Integrating ICN forwarding into the virtualization infrastructure," in *Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM 2016)*, Washington, DC, USA, Dec. 4–8, 2016.

5. J. Kurihara, K. Yokota, and A. Tagami, "A consumer-driven access control approach to censorship circumvention in content-centric networking," in *Proceedings of the 3rd ACM Conference on Information-Centric Networking (ICN 2016)*, Kyoto, Japan, Sep. 26–28, 2016, pp. 186–194.

6. K. Yokota, K. Sugiyama, J. Kurihara, and A. Tagami, "RTT-based caching policies to improve user-centric performance in CCN," in *Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA 2016)*, Crans-Montana, Switzerland, Mar. 23–25, 2016, pp. 124–131.

7. J. Kurihara, K. Yokota, K. Ueda, and A. Tagami, "List interest: Packing interests for reduction of router workload in CCN 1.0," in *Proceedings of IEEE MASS 2015 Workshop on Content-Centric Networking (CCN 2015)*, Dallas, TX, USA, Oct. 19–22, 2015, pp. 500–505.

8. K. Ueda, K. Yokota, J. Kurihara, and A. Tagami, "A performance analysis of end-to-end fragmentation in content-centric networking," in *Proceedings of IEEE MASS 2015 Workshop on Content-Centric Networking (CCN 2015)*, Dallas, TX, USA, Oct. 19–22, 2015, pp. 531–536.

9. J. Kurihara, E. Uzun, and C. A. Wood, "An encryption-based access control framework for content-centric networking," in *Proceedings of IFIP Networking Conference 2015*, Toulouse, France, May 20–22, 2015, pp. 1–9.

10. J. Kurihara, T. Uyematsu, and R. Matsumoto, "New parameters of linear codes expressing security performance of universal secure network coding," in *Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2012)*, Monticello, IL, USA, Oct. 1–5, 2012.

11. J. Kurihara, T. Uyematsu, and R. Matsumoto, "Explicit construction of universal strongly secure network coding via MRD codes," in *Proceedings of 2012 IEEE International Conference on Information Theory (ISIT 2012)*, Cambridge, MA, USA, Jul. 1–6, 2012, pp. 1483–1487.

12. J. Kurihara, and T. Uyematsu, "Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight," in *Proceedings of the 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2011)*, Monticello, IL, USA, Sep. 28–30, 2011, pp. 951–957.

13. J. Kurihara, and T. Uyematsu, "Vulnerability of MRD-code-based universal secure error-correcting network codes under time-varying jamming links," in *Proceedings of the Fourth International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2011)*, Budapest, Hungary, Apr. 17–22, 2011, pp. 35–39.

14. Y. Nakano, J. Kurihara, S. Kiyomoto, and T. Tanaka, "On a construction of stream-cipher-based hash functions," in *Proceedings of SECRYPT 2010*, Athens, Greece, Jul. 26–28, 2010, pp. 334–343.

15. C. Cid, S. Kiyomoto, and J. Kurihara, "The Rakaposhi stream cipher," in *Information and Communications Security, 11th International Conference, ICICS 2009, Beijing, China, December 14–17, 2009. Proceedings*, ser. Lecture Notes in Computer Science, S. Qing, C. J. Mitchell and G. Wang, Eds., vol. 5222. Heidelberg, Germany: Springer-Verlag, 2009, pp. 32–46.

16. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A new (k, n)-threshold secret sharing scheme and its extension," in *Information Security, 11th International Conference, ISC 2008, Taipei, Taiwan, September 15–18, 2008. Proceedings*, ser. Lecture Notes in Computer Science, T.-C. Wu, C.-L. Lei, V. Rijmen and D.-T. Lee, Eds., vol. 5222. Heidelberg, Germany: Springer-Verlag, 2008, pp. 455–470.

Articles in Magazines

1. T. Asami, J. Kurihara, D. Kondo, and H. Tode, "Network operations as an infrastructure for diverse businesses," *Journal of Institute of Electronics, Information and Communication Engineers*, vol. 103, no. 2, pp. 155–161, Feb. 2020. [Online]. Available: `https://www.journal.ieice.org/bin/pdf_link.php?fname=k103_2_155&lang=E&year=2020` (in Japanese).

2. J. Kurihara, R. Matsumoto, and T. Uyematsu, "Security of secret-sharing schemes can be characterized by relative parameters of linear codes (Invited paper)," *IEICE ESS Fundamentals Review*, vol. 9, no. 1, pp.14–23, Jul. 2015. [Online]. Available: `https://www.jstage.jst.go.jp/article/essfr/9/1/9_14/_pdf` (in Japanese).

3. J. Kurihara "A stream authentication scheme for 1-seg broadcasting," *Material Stage*, vol. 7, no. 12, pp. 22–25, Mar. 2008. (in Japanese)

Miscellaneous (Technical papers/talks)

1. J. Kurihara, "Security and Privacy in DNS (Tutorial)," in *Proceedings of the 2021 Society Conference of IEICE*, Online, Sep. 14–17, 2021.

2. J. Kurihara, and T. Kubo, "Mutualized oblivious DNS (μODNS): Hiding a tree in the wild forest," *Technical Report of IEICE*, vol. 121, no. 102, NS2021-44, pp. 63–68, Jul. 2021.

3. J. Kurihara, and T. Kubo, "Mutualized oblivious DNS (μODNS): Hiding a tree in the wild forest," Apr. 2021. [Online]. Available: `https://arxiv.org/abs/2104.13785`.

4. J. Kurihara, T. Nakamura, and R. Watanabe, "On the Resistance to Byzantine and Unresponsive Servers in Code-based PIR Schemes," in *Error-Correcting Codes Workshop (ECCWS) 2020*, Online, Sep. 2–3, 2020. (in Japanese)

5. D. Kondo, J. Kurihara, H. Tode, and T. Asami, "Name Prefix Security Applications in NDN," in *Proceedings of the 2019 Society Conference of IEICE*, Osaka, Japan, Sep. 10–13, 2019.

6. J. Kurihara, D. Kondo, H. Tode, and T. Asami, "Introduction to Name Prefix Security in NDN," in *Proceedings of the 2019 Society Conference of IEICE*, Osaka, Japan, Sep. 10–13, 2019.

7. J. Kurihara, and T. Kubo "Formal expression of BBc-1 mechanism and its security analysis," Oct. 31, 2017. [Online]. Available: `https://beyond-blockchain.org/public/bbc1-analysis.pdf`.

8. J. Kurihara, "Current security-related topics and content protection in information-centric networking [Tutorial]" in *Proceedings of the 2016 Society Conference of IEICE*, Hokkaido, Japan, Sep. 20–23, 2016. (in Japanese)

9. J. Kurihara, and M. Mosko, "Proposed proof of concept contribution by KDDI R&D Labs., Inc.," in *ITU-T Focus Group on IMT-2020*, Seoul, Korea, Mar. 8–11, 2016.

10. J. Kurihara, "1-to-n matching between interest and content objects for reduction of router workload," in *Proceedings of the 94-th IETF Meeting*, IRTF ICNRG, Yokohama, Japan, Nov. 4, 2015.

11. J. Kurihara, K. Yokota, K. Ueda, and A. Tagami, "Reduction of router workload by using list-type interests," in *Kick-off Workshop of IEICE Technical Committee on Information-Centric Networking*, Tokyo, Japan, Apr. 7, 2015. (in Japanese)

12. Y. Yokota, J. Kurihara, A. Tagami, "A study of TCP-like congestion control using interest aggregation in content-centric networking," in *Technical Report of IEICE. NS*, vol. 114, no. 477, pp. 173–178, Mar. 2015. (in Japanese)

13. B. Namsraijav, T. Asami, Y. Kawahara, J. Kurihara, K. Sugiyama, A. Tagami, T. Yagyu, and T. Hasegawa, "Identity-based aggregate signatures applied to NDN for short message transfers," in *Technical Report of IEICE. IN*, vol. 114, no. 478, pp. 319–324, Mar. 2015.

14. T. Sunaga, T. Asami, Y. Kawahara, K. Sugiyama, J. Kurihara, A. Tagami, T. Yagyu, and T. Hasegawa, "Optimization of ICN potential based routing for disasters," in *Technical Report of IEICE. IN*, vol. 114, no. 478, pp. 313–318, Mar. 2015. (in Japanese)

15. J. Kurihara, R. Matsumoto, and T. Uyematsu, "Security of secret-sharing schemes can be characterized by relative parameters of linear codes (Invited talk)," in *Technical Report of IEICE. IT*, vol. 114, no. 470, pp. 239–246, Feb. 2015. (in Japanese)

16. J. Kurihara, "Relative generalized rank weight of linear codes and its applications to network coding (Invited talk)," in *SITA 2014 workshop on current topics of coding in distributed systems*, Toyama, Japan, Dec. 9–12, 2014. (in Japanese)

17. J. Kurihara, "A secret sharing scheme based on linear codes and its security analysis (invited talk)", in *Workshop on Discrete Mathematics Related to Information Security*, Nagano, Japan, Aug. 2013. (in Japanese)

18. J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes can be precisely characterized by the relative generalized Hamming weight," in *Proceedings of the 2012 IEICE General Conference*, Okayama, Japan, Mar. 20–23, 2012.

19. J. Kurihara, "An XOR-based high-speed secret sharing (Invited talk)," in *One day workshop on secret sharing and cloud computing, Institute of Mathematics for Industry, Kyushu University*, Fukuoka, Kyushu, Jun. 2011.

20. J. Kurihara, and T. Uyematsu, "Time-varying jamming links for MRD-code-based universal secure error-correcting network codes," in *Proceedings of the 2010 Society Conference of IEICE*, Osaka, Japan, Sep. 14–17, 2010. (in Japanese)

21. J. Kurihara, and T. Uyematsu, "Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight," in *Technical Report of IEICE. IT*, vol. 111, no. 142, pp. 35–40, Jul. 2007.

22. Y. Nakano, J. Kurihara, S. Kiyomoto, and T. Tanaka, "A message injection in SCH," in *Proceedings of the 2010 IEICE General Conference*, Miyagi, Japan, Mar. 16–19, 2010.

23. J. Kurihara, T. Uyematsu, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Rediscovery of XOR-based threshold schemes in MDS codes," in *Proceedings of the 27th Symposium on Cryptography and Information Security (SCIS 2010)*, Takamatsu, Japan, Jan. 19–22, 2010.

24. J. Kurihara, T. Uyematsu, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A novel realization of (k, n)-threshold schemes over binary field extensions," in *Proceedings of the 27th Symposium on Cryptography and Information Security (SCIS 2010)*, Takamatsu, Japan, Jan. 19–22, 2010.

25. Y. Nakano, J. Kurihara, S. Kiyomoto, and T. Tanaka, "A study on stream-cipher-based hash functions," in *Technical Report of IEICE. SITE*, vol. 109, no. 114, pp. 153-159, Jun. 2009.

26. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Revocation and addition mechanisms for fast (k, n)-threshold schemes" in *Proceedings of the 2009 IEICE General Conference*, Ehime, Japan, Mar. 17–20, 2009.

27. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Fast (k, n)-threshold schemes for hierarchical access structures" in *Proceedings of the Computer Security Symposium 2008 (CSS 2008)*, Okinawa, Japan, Oct. 8–10, 2008.

28. J. Kurihara, S. Kiyomoto, R. Watanabe, and T. Tanaka, "A stream authentication scheme for 1-seg broadcasting,"in *Proceedings of the 2008 IEICE General Conference*, Fukuoka, Japan, Mar. 18–21, 2008. (in Japanese)

29. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A new (k, n)-threshold secret sharing scheme and its extension," Cryptology ePrint Archive, Report 2008/409, 2008. [Online]. Available: `http://eprint.iacr.org/2008/409`.

30. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "An extension of fast threshold schemes using XOR operations (2)," in *Technical Report of IEICE. ISEC*, vol. 107, no. 209, pp. 9–15, Sep. 2007.

31. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "An extension of fast threshold schemes using XOR operations (1)," in *Technical Report of IEICE. ISEC*, vol. 107, no. 209, pp. 1–8, Sep. 2007.

32. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A fast $(4, n)$-threshold secret sharing scheme using exclusive-or operations, and its extension to (k, n)-threshold schemes," in *Technical Report of IEICE. ISEC*, vol. 107, no. 44, pp. 23–30, May 2007.

33. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "The completeness proof of $(3, n)$-threshold secret sharing scheme using XOR operations," in *Proceedings of the 24th Symposium on Cryptography and Information Security (SCIS 2007)*, Nagasaki, Japan, Jan. 23–26, 2007. (in Japanese)

34. J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A $(3, n)$-threshold secret sharing scheme using XOR operations," in *Proceedings of the 24th Symposium on Cryptography and Information Security (SCIS 2007)*, Nagasaki, Japan, Jan. 23–26, 2007. (in Japanese)

35. J. Kurihara, T. Uyematsu, and R. Matsumoto, "Efficient nonbinary coding systems approaching the shannon limit by using product accumlate codes," in *Technical Report of IEICE. CS*, vol. 105, no. 460, pp. 45–50, Dec. 2004. (in Japanese)

36. J. Kurihara, and H. Suzuki "Software radio receiver utilizing RF filter bank," in *Technical Report of IEICE. RCS*, vol. 104, no. 257, pp. 79–84, Aug. 2004. (in Japanese)

Patents

48+ patents on distributed storage codes, network coding, secret sharing schemes, stream authentication, information-centric networking, etc. have been filed in Japan. Until Feb. 2019, 27 patents have been accepted in Japan. Some of them have also been filed in US as well and one patent have been accepted.

Honors and Awards

IEICE Kiyasu Zen'ichi (Best Paper) Award (2014).

IEICE Excellent Paper Award (2014).

IEICE Academic Encouragement Award of Engineering Sciences Society (2013).

Excellent Paper Award in Computer Security Symposium 2008 (2008).

Grants from External Organizations

JSPS KAKENHI (Grant no. JP20K23329), PI, 2020-2021

JSPS KAKENHI (Grant no. JP21H03442), Co, 2021-2023

University of Hyogo (Special Research Grant (Young Researchers)), PI, 2020/2021

KDDI Research, Inc. (Funded Research Project), PI, 2020/2021

HORIZON2020 (Grant Agreement No. 723014) / NICT (Contract No. 184), 2016–2019

NICT (Contract No. 19103), 2016–2021

Membership

A member of the Institute of Electrical and Electronics Engineers, Inc. (IEEE)

A member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Certifications

Network Specialist (Dec. 2017, Information-technology Promotion Agency (IPA), Japan)

Registered Information Security Specialist (Jun. 2017, Information-technology Promotion Agency (IPA), Japan)[2]

Applied Information Technology Engineer (Dec. 2016, Information-technology Promotion Agency (IPA), Japan)

Lectures

Security Engineering (2020–2021, Graduate School of U-Hyogo)

Network Security (2020–2021, Graduate School of U-Hyogo)

Information Security (2020–2021, Graduate School of U-Hyogo)

FIDO2 –Modern Authentication– (2020, Zettant)

Introduction to End-to-End Encryption using JavaScript (2019, Zettant)

[2]National qualification in cybersecurity. Passed the examination but not registered to the Japanese government yet. Registration is possible anytime.

Professional Services

Organizing Committee, IPSJ CSS 2020.

Technical Program Committee, DISS Workshop in NDSS 2019.

Technical Program Committee, ACM ICN 2018.

Poster and Demo Program Committee, ACM SIGCOMM 2017.

Organizing Committee, ACM ICN 2016.

Organizing Committee, IEICE SCIS 2010.

Reviewer for *IEEE Transactions on Information Theory*, *IEEE Transactions on Information Forensics and Security*, *IEEE Journal on Selected Areas in Communications*, *IEEE Communications Letters*, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *IEICE Transactions on Communications*, *IEICE Transactions on Information and Systems*, *IPSJ Journal*, *Advances in Mathematics of Communications*, *IEEE International Symposium on Information Theory*, *IEEE International Communication Conference*, *IEEE Globecomm*, *IEEE Information Theory Workshop*, *IEEE International Symposium on Network Coding*, *International Symposium on Information Theory and Its Applications*, *ACM International Conference on Information-centric Networking*, etc.