Naoto Yanai

Associate Professor, Department of Multimedia Engineering,
Graduate School of Information Science and Technology, Osaka University.
Address: Room A302, Yamadaoka 1-5, Suita, Osaka, Japan.
E-mail: yanai[at]ist.osaka-u.ac.jp.

My research interests are in information security, especially those security analyses.

DBLP: https://dblp.uni-trier.de/pers/y/Yanai:Naoto.html
GitHub: https://github.com/naotoyanai

Awards

1. A3 Foresight Program Annual Workshop 2013 Research on Next Generation Internet and Network Security, Best Presentation Award, "Ordered Multisignatures under Standard Assumptions, with Applications to Secure Routing", 11th July 2013.
2. The 11th International Workshop on Security (IWSEC 2016), Best Poster Awards, "Malware for Protocol Misidentification," 13th September 2016.
3. The Fourth International Symposium on Computing and Networking (CANDAR 2016), Outstanding Paper Award, "On the Tightness of Deterministic Identity-Based Signatures", 23th November 2016.
4. BSCI2021 Best Paper Award, "Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts", June 2021.
5. 23. The 18th International Workshop on Security (IWSEC 2023), IWSEC2023 Best Poster Award, "KOTO Crypto: Educational cryptography with the Koto," August 30th 2023.

Publications

Invited Talk

1. *Naoto Yanai*, "Multiple-Signability: A Study on Multisignatures and Aggregate Signatures", The Eigth International Workshop on Security (IWSEC 2013), SCIS/CSS Invited Sessions, November 2013.
2. *Naoto Yanai* (Main Contributor: Kazuma Tanaka) , "APAT: An Application of Aggregate Signatures to BGPSEC", The 11th International Workshop on Security (IWSEC 2016), SCIS/CSS Invited Sessions, September 2016.
3. Naoto Yanai, "Security Research on Blockchain," 3rd Joint ERCIM-JST Workshop (2022), Paris, France, October 2022.

Journal

1. *Naoto YANAI*, Eikoh CHIDA, and Masahiro MAMBO, "A Secure Structured Multisignature Scheme Based on a Non-Commutative Ring Homomorphism,"IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E94-A, No.6, pp.1346-1355, June 2011.
2. *Naoto YANAI*, Raylin Tso, Masahiro MAMBO, and Eiji Okamoto, "A Certificateless Ordered Sequential Aggregate Signature Scheme Secure against Super Adversaries," Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, Vol.3, No. 1/2,pp.30-54, March 2012.
3. *Naoto YANAI*, Eikoh CHIDA, Masahiro MAMBO, and Eiji OKAMOTO,"A CDH-based Ordered Multisignature Scheme Provably Secure without Random Oracles", Journal of Information Processing, Vol.22, No. 2, pp.366-375, April 2014.
4. Nobuaki Kitajima, *Naoto Yanai*, Takashi Nishide, Goichiro Hanaoka, Eji Okamoto, "Fail-Stop Signatures for Multiple-Signers: Definitions, Constructions, and Their Extensions," Journal of Information Processing, Vol.24, No.2, pp.275-291, Feburary 2016.
5. Hikaru Kishimoto, *Naoto Yanai*, Shingo Okamura, "SPaCIS: Secure Payment Protocol for Charging Information over Smart Grid", Journal of Information Processing, Vol.25, No.1, pp.12-21, January 2017.
6. *Naoto Yanai*, Tomoya Iwasaki, Masaki Inamura, Keiichi Iwamura, "Provably Secure Structured Signature Schemes with Tighter Reductions", "IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, September 2017 (accepted).
7. Yukou Kobayashi, *Naoto Yanai*, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, Eiji Okamoto, "Password-based Authenticated Key Exchange with a Gateway via Multiple Authentication Servers", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E100-A, No.12, pp.2991-3006, December 2017.
8. *Naoto Yanai*, Toru Fujiwara, "Tighter Reductions for Deterministic Identity-Based Signatures", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E101-A, No.1, pp.64-76, January 2018.
9. Thi Ngoc Diep Pham, Chai Kiat Yeo, *Naoto Yanai*, Toru Fujiwara, "Detecting Flooding Attack and Accommodating Burst Traffic in Delay Tolerant Networks", IEEE Transactions on Vehicular Technology, Vol.67, No.1, pp.795-808, January 2018. (IF 4.066)
10. Jason Paul Cruz, Yuichi Kaji, *Naoto Yanai*, "RBAC-SC: Role-based Access Control using Smart Contract", IEEE Access, Vol.6, pp.12240-12251, March 2018. (IF 3.244)
11. *Naoto Yanai*, "Meeting Tight Security for Multisignatures in the Plain Public Key Model", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E101-A, No.9, pp.1484-1493, September 2018.
12. Hideharu Kojima, *Naoto Yanai*, Jason Paul Cruz, "ISDSR+: Improving the Security and Availability of Secure Routing Protocol", IEEE Access, Vol.7, pp.74849-74868, June 2019. (IF 4.098)
13. Shimamoto Hayato, *Naoto Yanai*, Shingo Okamura, Jason Paul Cruz, Shouei Ou, Takao Okubo, "Towards Further Formal Foundation of Web Security: Expression of Temporal Logic in Alloy and Its

Application to A Security Model with Cache", IEEE Access, Vol.7, pp.74941-74960, June 2019. (IF 4.098)

14. Hiromasa Kitai, Jason Paul Cruz, *Naoto Yanai*, Naohisa Nishida, Tatsumi Oba, Yuji Unagami, Tadanori Teruya, Nuttapong Attrapadung, Takahiro Matsuda, Goichiro Hanaoka, "MOBIUS: Model-Oblivious Binarized Neural Networks", IEEE Access, Vol.7, pp.139021-139034, September 2019. (IF 4.098)
15. Masahiro Kamimura, *Naoto Yanai*, Shingo Okamura, Jason Paul Cruz, "Key-Aggregate Searchable Encryption, Revisited: Formal Foundations for Cloud Applications, and Their Implementation", IEEE Access, Vol. 8, pp.24153-24169, January 2020. (IF 4.098)
16. Naohisa Nishida, Tatsumi Oba, Yuji Unagami, Jason Paul Cruz, *Naoto Yanai*, Tadanori Teruya, Nuttapong Attrapadung, Takahiro Matsuda, Goichiro Hanaoka, "Efficient Secure Neural Network Prediction Protocol Reducing Accuracy Degradation", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E103-A, No.12, pp. 1367-1380, December 2020.
17. Tatsuya Takemura, Naoto Yanai, Toru Fujiwara, "Model Extraction Attacks against Recurrent Neural Networks", Journal of Information Processing, Vol.28, No.12, pp. 1010-1024, December 2020.
18. Kazuki Iwahana, Tatsuya Takemura, Ju Chien Cheng, Nami Ashizawa, Naoki Umeda, Kodai Sato, Ryota Kawakami, Rei Shimizu, Yuichiro Chinen, Naoto Yanai, "MADMAX: Browser-Based Malicious Domain Detection through Extreme Learning Machine", IEEE Access, Vol.9, pp.78293-78314, IEEE, May 2021.
19. Yang Chen, Nami Ashizawa, Chai Kiat Yeo, Naoto Yanai, Seanglidet Yean, "Multi-scale Self-Organizing Map assisted Deep Autoencoding Gaussian Mixture Model for unsupervised intruction detection", Knowledge-Based Systems, Volume224, p.107086, Elsevier, July2021.
20. Yuichiro Chinen, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, "RA: A Static Analysis Tool for Analyzing Re-Entrancy Attacks in Ethereum Smart Contracts", Journal of Information Processing, Vol. 29, No.10, p.537-547, October 2021.
21. Kazuki Iwahana, Naoto Yanai, Jason Paul Cruz, Toru Fujiwara, "SPGC: Integration of Secure Multiparty Computation and Differential Privacy for Gradient Computation on Collaborative Learning," Journal of Information Processing, Vol. 30, Pages 209-22, March 2022.
22. Nami Ashizawa, Naoto Yanai, Jason Paul Cruz, Singo Okamura, "Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts," Blockchain: Research and Applications, Vol. 3, p.100101, Elsevier. December 2022.
23. Naoki Umeda, Naoto Yanai, Tatsuya Takemura, Masayuki Okada, Jason Paul Cruz and Shingo Okamura, "SQUAB: A Virtualized Infrastructure for BGP-Related Experiments and Its Applications to Evaluation on BGPsec", Journal of Information Processing, Vol. 30, p. 829-840, December 2022.
24. Naoki Umeda, Naoto Yanai, Taiji Kimura, "The Juice is Worth the Squeeze: Analysis of Autonomous System Provider Authorization in Partial Deployment," IEEE Open Journal of the Communications Society, Vol.4, pp.269-306, January 2023.

25. Ouyang Junjie, Naoto Yanai, Tatsuya Takemura, Masayuki Okada, Shingo Okamura, Jason Paul Cruz, "APVAS: Reducing the Memory Requirement of AS_PATH Validation by Introducing Aggregate Signatures into BGPsec," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E106-A, No. 3, pp.170-184, March 2023.
26. Kazuhiko Minematsu, Junji Shikata, Yohei Watanabe, and Naoto Yanai, "Anonymous Broadcast Authentication with One-to-Many Transmission to Control IoT Devices," IEEE Access, Vol.11, pp. 62955--62969, IEEE, June 2023.
27. Hiromasa Kitai, Naoto Yanai, Kazuki Iwahana, Masataka Tatsumi and Jason Paul Cruz, "A Study on Quantized Parameters for Protection of Model and Its Inference Input," Journal of Information Processing, Vol. 31, June 2023. (To appear.)
28. Kyosuke Yamashita, Keisuke Hara, Yohei Watanabe, Naoto Yanai, Junji Shikata, "Designated Verifier Signature with Claimability," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, August 2023. (To appear).
29. Koji NAKAO, Katsunari YOSHIOKA, Takayuki SASAKI, Rui TANABE, Xuping HUANG, Takeshi TAKAHASHI, Akira FUJITA, Jun'ichi TAKEUCHI, Noboru MURATA, Junji SHIKATA, Kazuki IWAMOTO, Kazuki TAKADA, Yuki ISHIDA, Masaru TAKEUCHI, Naoto YANAI, "Mitigate: Toward Comprehensive Research and Development for Analyzing and Combating IoT Malware," IEICE Transactions on Information and Systems, Vol. E106.D, No. 9, pp. 1302-1315, IEICE, September 2023.

Book

1. Hikaru Kishimoto, *Naoto Yanai*, Shingo Okamura, "Smart Micro-Grid Systems Security and Privacy", In Chapter of "An Anonymous Authentication Protocol for Smart Grid", Springer Book Series on Advances in Information Security (Series Ed. Jajodia, Sushil), Vol.71, pp.29-52, Springer, September 2018.

International Conference

1. *Naoto Yanai*, Eikoh Chida, and Masahiro Mambo, "A Structured Multisignature Based on a Non-Commutative Ring Homomorphism," Proc. of Joint Workshop on Information Security (JWIS) 2009, 1B-3, pp.1-15, March 2009.
2. *Naoto Yanai*, Eikoh Chida, and Masahiro Mambo, "A Structured Aggregate Signature Scheme," Proc. of International Symposium on Information Theory and its Application (ISITA) 2010, pp.795-800, October 2010, [DOI]
3. *Naoto Yanai*, Raylin Tso, Masahiro Mambo, and Eiji Okamoto, "Certificateless Ordered Sequential Aggregate Signature Scheme," Proc. of International Conference on Intelligent Networking and Collaborative Systems (INCoS) 2011, (Workshop: Third International Workshop on Managing Insider Security Threats (MIST) 2011), ppp.662-667, November - December 2011. [DOI]

4. *Naoto Yanai*, Masahiro Mambo, and Eiji Okamoto, “Ordered Multisignature Schemes under the CDH Assumption without Random Oracles,” Proc. of Information Security Conference (ISC) 2013, LNCS 7807, pp. 367–377, November 2013.
5. Tomoya Iwasaki, *Naoto Yayanai*, Masaki Inamura, and Keiichi Iwamura, “Security Evaluation of an Order-Specified, Identity-Based Aggregate Signature Scheme”, Proc. of International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC) 2013, pp.51–57, December 2013.
6. *Naoto Yanai*, Masahiro Mambo, and Eiji Okamoto, “A CDH-Ordered Multisignature Scheme in the Standard Model with Better Efficiency,” Proc. of International Symposium on Information Theory and its Application (ISITA) 2014, pp.236–240, October 2014. [DOI]
7. Nobuaki Kitajima, *Naoto Yanai*, Takashi Nishide, Goichiro Hanaoka and Eiji Okamoto, ″Constructions of Fail-Stop Signatures for Multi-Signer Setting″, Proc. of the 10th Asia Joint Conference on Information Security (AsiaJCIS 2015), pp.112–123, May 2015.
8. Yukou Kobayashi, *Naoto Yanai*, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, Eiji Okamoto, ″Gateway Threshold Password-based Authenticated Key Exchange Secure against Undetectable On-line Dictionary Attack″, Proc. of the 12th International Conference on Security and Cryptography (SECRYPT 2015), pp.39–52, July 2015..
9. Kenta Muranaka, *Naoto Yanai*, Shingo Okamura and Toru Fujiwara, ″Secure Routing Protocols for Sensor Networks: Construction with Signature Schemes for Multiple Signers″, Proc. of The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2015), pp.1329––1336, August 2015..
10. Kenta Muranaka, *Naoto Yanai*, Shingo Okamura, Toru Fujiwara, ″Toward Secure Routing Protocols for Sensor Networks,″ The 10th International Workshop on Security (IWSEC2015), poster, August 2015.
11. Hikaru Kishimoto, Shingo Okamura, *Naoto Yanai*, ″Secure Payment Protocol for Charging Information over SmartGrid,″ The 10th International Workshop on Security (IWSEC2015), poster, August 2015.
12. Yuma Higashiyama, *Naoto Yanai*, Shingo Okamura and Toru Fujiwara, ″Revisiting Authentication with Shoulder-Surfing Resistance for Smartphones,″ Proc. of The Third International Symposium on Computing and Networking (CANDAR 2015), pp.89–95, December 2015.
13. *Naoto Yanai*, Masahiro Mambo, Kazuma Tanaka, Takashi Nishide, Eiji Okamoto, ″Another Look at Aggregate Signatures: Their Capability and Security on Network Graphs,″ Proc. of The Seventh International Conference on Trusted Systems (INTRUST 2015), LNCS 9565, pp.30–46, March 2016.
14. Tomoya Iwasaki, *Naoto Yanai*, Masaki Inamura, Keiichi Iwamura, ″Tightly-Secure Identity-Based Structured Aggregate Signature Scheme under the computational Diffie-Hellman Assumption,″ Proc. of The 30th IEEE International Conference on Advanced Information Networking and Applications (AINA-2016), pp.669–676, March 2016.
15. Kazuma Tanaka, *Naoto Yanai*, Masayuki Okada, Takashi Nishide, Eiji Okamoto, “APAT: An Application of Aggregate Signatures to BGPSEC,” The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2016), Fast Abstract, June 2016.

16. Kenta Muranaka, *Naoto Yanai*, Shingo Okamura, Toru Fujiwara, "ISDSR : Secure DSR with ID-based Sequential Aggregate Signature," In Proc. of the 13th International Joint Conference on e-business and Telecommunications (ICETE 2016), Vol. 4, SECRYPT, pp. 376-387, July 2016.
17. Yudai Nagamine, *Naoto Yanai*, Shingo Okamura, Toru Fujiwara, "Malware for Protocol Misidentification," The 11th International Workshop on Security (IWSEC2016), poster, September 2016.
18. Hayato Shimamoto, *Naoto Yanai*, Shingo Okamura, Toru Fujiwara, "Web Security Model with Cache," Proc. of International Symposium on Information Theory and its Application (ISITA) 2016, pp.413-417, October-November 2016.
19. Ryo Fukuyama, *Naoto Yanai*, Shingo Okamura, Toru Fujiwara, "Towards a Formal Foundation of Protection against Data-Oriented Attacks," Proc. of International Symposium on Information Theory and its Application (ISITA) 2016 pp.418-421, October-November 2016.
20. *Naoto Yanai,* "Towards Provable Security of Dynamic Source Routing Protocol and Its Applications," Proc. of ER 2016 Workshops, AHA, MoBiD, MORE-BI, MReBA, QMMQ, SCME, and WM2SP, LNCS 9975, pp.231-239 November 2016.
21. *Naoto Yanai*, "On the Tightness of Deterministic Identity-Based Signatures", Proc. of The Fourth International Symposium on Computing and Networking (CANDAR 2016), pp.168-173, November 2016.
22. Hikaru Kishimoto, *Naoto Yanai*, Shingo Okamura, "An Anonymous Authentication Protocol for Smart Grid," Proc. of the 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA 2017), pp.62-67, IEEE, March 2017.
23. *Naoto Yanai*, "Tightly Secure Identity-Based Multisignatures," 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW 2017), pp.253-254, IEEE, June 2017.
24. Yuuji Furuta, *Naoto Yanai,* Masashi Karasaki, Katsuhiko Eguchi, Yasunori Ishihara, Toru Fujiwara, "Towards Efficient and Secure Encrypted Databases: Extending Message-Locked Encryption in Three-Party Model," Proc. of the 12th International Workshop on Data Privacy Management (DPM 2017), co-located in ESORICS 2017, LNCS 10436, pp.55-69, Springer, September 2017.
25. Hideharu Kojima, *Naoto Yanai,* "Performance Evaluation for The Signature Algorithm of ISDSR on Raspberry Pi", Proc. of 10th International Workshop on Autonomous Self-Organizing Networks (ASON 2017), co-located in The Fifth International Symposium on Computing and Networking (CANDAR 2017), pp.230-236, IEEE, November 2017.
26. Nobuaki Kitajima, *Naoto Yanai*, Takashi Nishide, "Identity-Based Key-Insulated Aggregate Signatures, Revisited", Proc. of The 13th International Conference on Information Security and Cryptology (Inscrypt 2017), LNCS 10726, pp.141-156, Springer, November 2017.
27. *Naoto Yanai*, Jason Paul Cruz, "On Security of Anonymous Invitation-Based System", Proc. of the 13th DPM International Workshop on Data Privacy Management (DPM 2018), LNCS 11025, pp.415-421, Springer, September 2018.
28. Takahiro Higuchi, *Naoto Yanai*, Kensuke Ueda, Yasunori Ishihara, Toru Fujiwara, "A Privacy Risk Arising from Communication with TV: Consideration from Attribute Inference for Users", The Network and Distributed System Security Symposium (NDSS) 2019, Poster, February 2019.

29. Shinnosuke Shimizu, Hideharu Kojima, *Naoto Yanai*, Tatsuhiro Tsuchiya,"Implementation and Evaluation of ISDSR in Emulation Environments", Proc. of IEEE Wireless Communications and Networking Conference (WCNC) 2019, pp.1-6, IEEE, April 2019.
30. Hideharu Kojima, *Naoto Yanai*, "A Chain Code Mechanism with Data Encryption on Hyperledger Fabric", The 24th European Symposium on Research in Computer Security (ESORICS 2019), Poster, September 2019.
31. Hideharu Kojima, *Naoto Yanai*, "A State Space Suppression Method for Formal Verification of Secure Routing Protocols with SPIN", the 30th International Symposium on Software Reliability Engineering (ISSRE 2019), IEEE, Fast Abstract, October 2019.
32. Hideharu Kojima, *Naoto Yanai*, "A State Space Reduction Method for Model Checking of Wireless Multi-hop Network Routing Protocols Focusing on Topologies", The Seventh International Symposium on Computing and Networking Workshop (CANDARW 2019), pp.14-20, IEEE, November 2019.
33. Mio Saiki, Hideharu Kojima, *Naoto Yanai*, Tatsuhiro Tsuchiya, "A Chaincode with Attribute-Based Encryption for Protecting Data in Ledgers", The Network and Distributed System Security Symposium (NDSS) 2020, poster, February 2020.
34. Ryota Kawakami, Atsuo Inomata, *Naoto Yanai*, Toru Fujiwara, "Wireless Access Point Spoofing by Unmanned Aerial Vehicles (UAVs)", The Network and Distributed System Security Symposium (NDSS) 2020, poster, February 2020.
35. Yoshiyuki Kido, Nelson Pinto Tou, *Naoto Yanai*, Shinji Shimojo, "sD&D: Design and Implementation of Cybersecurity Educational Game with Highly Extensible Functionality", the Future of Information and Communications Conference (FICC) 2020, AISC 1129, pp.857-873, Springer, March 2020.
36. Hideharu Kojima, *Naoto Yanai*, "A Model Checking Method for Secure Routing Protocols by SPIN with State Space Reduction", Proc. of 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), pp. 627 - 635, IEEE, May 2020.
37. Yuichiro Chinen, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, "RA: Hunting for Re-Entrancy Attacks in Ethereum Smart Contracts via Static Analysis", Proc. of the 3rd IEEE International Conference on Blockchain (Blockcha2020), pp. 327-336, IEEE, November 2020. (To appear.)
38. Yang Chen, Nami Ashizawa, Seanglidet Yean, Chai Kiat Yeo, Naoto Yanai, "Self-Organizing Map assisted Deep Autoencoding Gaussian Mixture Model for Intrusion Detection", Proc. of IEEE Consumer Communications and Networking Conference (CCNC) 2021, pp.1-6, IEEE, January 2021.
39. Tatsuya Takemura, , Naoto Yanai, Naoki Umeda, Masayuki Okada, Shingo Okamura, Jason Paul Cruz, "APVAS+: A Practical Extension of BGPsec with Low Memory Requirement", Proc. of 2021 IEEE International Conference on Communications (ICC 2021), IEEE, June 2021. (To appear.)
40. Naoki Umeda, Naoto Yanai, Tatsuya Takemura, Masayuki Okada, Jason Paul Cruz and Shingo Okamura, "SQUAB: A Virtualized Infrastructure for Experiments on BGP and Its Extensions", The 35th International Conference on Advanced Information Networking and Applications (AINA 2021), Lecture Notes in Networks and Systems (LNNS), volume225, pp.600-613, Springer, May 2021.

41. Yohei Watanabe, Naoto Yanai and Junji Shikata, "Anonymous Broadcast Authentication for Securely Remote-Controlling IoT Devices", The 35th International Conference on Advanced Information Networking and Applications (AINA 2021), Lecture Notes in Networks and Systems(LNNS), volume225, pp.679-690, Springer, May 2021.
42. Nami Ashizawa, Naoto Yanai, Jason Paul Cruz, Singo Okamura, "Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts," Proc. of The Third ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2021), pp.47-59, ACM, June 2021.
43. Kazuki Iwahana, Naoto Yanai, Jasonb Paul Cruz, Toru Fujiwara, "SPGC: An Integrated Framework of Secure Computation and Differential Privacy for Collaborative Learning", Proc. of the 16th DPM International Workshop on Data Privacy Management (DPM 2021), LNCS 13140, pp.89-105, Springer, October 2021.
44. Takumi Okano, Hideharu Kojima, Naoto Yanai and Tatsuhiro Tsuchiya, "Implementing Access Control in Chaincodes on Hyperledger Fabric with Attribute-Based Encryption", Proc. of the Third Workshop on Blockchain-based Architectures (BlockArch 2022), March 2022.
45. Hiromasa Kitai, Naoto Yanai, Kazuki Iwahana, Masataka Tatsumi and Jason Paul Cruz, "MOTUS: How Quantized Parameters Improve Protection of Models and Their Inference Inputs," Proc. of The 15th International Conference on Security for Information Technology and Communications (SECITC 2022), Lecture Notes in Computer Science, Vol 13809, pp.184-202, Springer, December 2022.
46. Chihiro Kado, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, "An Empirical Study of Impact of Solidity Compiler Updates on Vulnerabilities," Proc. of the 4th Workshop on Blockchain theoRy and ApplicatIoNs (BRAIN 2023), pp.92—97, IEEE, March 2023.
47. Tomoya Matsumoto, Takayuki Miura, and Naoto Yanai, "Membership Inference Attacks against Diffusion Models," Proc. of The 6th Deep Learning Security and Privacy Workshop (DLSP 2023), IEEE, May 2023.
48. Janaka Senanayake, Sampath Rajapaksha, Naoto Yanai, Chika Komiya, and Harsha Kumara Kalutarage, "MADONNA: Browser-Based MAlicious Domain Detection through Optimized Neural Network with Feature Analysis," Proc. of the 38th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2023), Springer, June 2023. (To appear.)
49. Chika Komiya, Naoto Yanai, Kyosuke Yamashita and Shingo Okamura, "JABBERWOCK: A Tool for Generation of WebAssembly Dataset," Proc. of the Firth DSN Workshop on Data-Centric Dependability and Security (DCDS) 2023, June 2023. (To appear.)
50. Yumeki Goto, Tomoya Matsumoto, Hamada Rizk, Naoto Yanai, Hirozumi Yamaguchi, "Privacy-Preserving Taxi-Demand Prediction Using Federated Learning," Proc. of the 9th IEEE International Workshop on Sensors and Smart Cities (SSC 2023), IEEE, June 2023.
51. Yohei Watanabe, Naoto Yanai, Junji Shikata, "IoT-REX: A Secure Remote-Control System for IoT Devices from Centralized Multi-Designated Verifier Signatures," The 18th International Conference on Information Security Practice and Experience (ISPEC 2023), Springer, August 2023.

52. Mine Arai, Naoto Yanai and Goichiro Hanaoka, “KOTO Crypto: Educational cryptography with the Koto,” The 18th International Workshop on Security (IWSEC 2023), Poster, August 2023. IWSEC2023 Best Poster Award.
53. Kazuki Iwahana, Naoto Yanai, Toru Fujiwara, ″Backdoor Attacks Leveraging Latent Representation in Competitive Learning,″ Proc. of the 1st Workshop on Security and Artificial Intelligence (SECAI 2023), September 2023. (To appear.)
54. Yumeki Goto, Nami Ashizawa, Toshiki Shibara, Naoto Yanai, ″Do Backdoors Assist Membership Inference Attacks?,″ Proc. of 19th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2023), October 2023.

Misc.

1. Hiromasa Kitai, Jason Paul Cruz, Naoto Yanai, Naohisa Nishida, Tatsumi Oba, Yuji Unagami, Tadanori Teruya, Nuttapong Attrapadung, Takahiro Matsuda, Goichiro Hanaoka, “MOBIUS: Model-Oblivious Binarized Neural Networks”, November 2018. arXiv. (https://arxiv.org/abs/1811.12028)
2. Masahiro Kamimura, Naoto Yanai, Shingo Okamura, Jason Paul Cruz, “Key-Aggregate Searchable Encryption, Revisited: Formal Foundations for Cloud Applications, and Their Implementation”, August 2019. arXiv. (https://arxiv.org/abs/1908.11096)
3. Tatsuya Takemura, Naoto Yanai, Toru Fujiwara, “Model Extraction Attacks against Recurrent Neural Networks”, February 2020. arXiv. (https://arxiv.org/abs/2002.00123)
4. Yuichiro Chinen, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, “Hunting for Re-Entrancy Attacks in Ethereum Smart Contracts via Static Analysis”, July 2020. arXiv. (https://arxiv.org/abs/2007.01029)
5. Ouyang Junjie, Naoto Yanai, Tatsuya Takemura, Masayuki Okada, Shingo Okamura, Jason Paul Cruz, “APVAS: Reducing Memory Size of AS_PATH Validation by Using Aggregate Signatures”, August 2020. arXiv. (https://arxiv.org/abs/2008.13346)
6. Yang Chen, Nami Ashizawa, Seanglidet Yean, Chai Kiat Yeo, Naoto Yanai, “Self-Organizing Map assisted Deep Autoencoding Gaussian Mixture Model for Intrusion Detection”, August 2020. arXiv. (https://arxiv.org/abs/2008.12686)
7. Nami Ashizawa, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, “Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts”, January 2021. arXiv. (https://arxiv.org/abs/2101.02377)
8. Masataka Tasumi, Kazuki Iwahana, Naoto Yanai, Katsunari Shishido, Toshiya Shimizu, Yuji Higuchi, Ikuya Morikawa, Jun Yajima, ″First to Possess His Statistics: Data-Free Model Extraction Attack on Tabular Data,″ September 2021. arXiv. (https://arxiv.org/abs/2109.14857)
9. Yohei Watanabe, Naoto Yanai, Junji Shikata, “IoT-REX: A Secure Remote-Control System for IoT Devices from Centralized Multi-Designated Verifier Signatures,” September 2022. arxiv. (https://arxiv.org/abs/2208.03781)
10. Tomoya Matsumoto, Takayuki Miura, Naoto Yanai, “Membership Inference Attacks against Diffusion Models,” February 2023. arXiv. (https://arxiv.org/abs/2302.03262)

11. Yumeki Goto, Nami Ashizawa, Toshiki Shibahara, Naoto Yanai, “Do Backdoors Assist Membership Inference Attacks?” March 2023. arXiv. (https://arxiv.org/abs/2303.12589)
12. Yumeki Goto, Tomoya Matsumoto, Hamada Rizk, Naoto Yanai, Hirozumi Yamaguchi, “Privacy-Preserving Taxi-Demand Prediction Using Federated Learning,” March 2023. (https://arxiv.org/abs/2305.08107)
13. Chihiro Kado, Naoto Yanai, Jason Paul Cruz, Kyosuke Yamashita, Shingo Okamura, “An Empirical Study of Impact of Solidity Compiler Updates on Vulnerabilities in Ethereum Smart Contracts,” May 2023. arXiv. (https://arxiv.org/abs/2306.04250)
14. Chika Komiya, Naoto Yanai, Kyosuke Yamashita, Shingo Okamura, “JABBERWOCK: A Tool for WebAssembly Dataset Generation and Its Application to Malicious Website Detection,” June 2023. arXiv. (https://arxiv.org/abs/2306.05698)

Software

1. Security Model on Alloy for Web Security. (Published in IEEE Access.)
2. Reference Implementation of Key-Aggregate Searchable Encryption. (Published in IEEE Access.)
3. ISDSR+: Wireless Routing Protocol. (Published in IEEE Access.)
4. RBAC-SC. (Published in IEEE Access.)
5. RA: Security Analyzer for EVM Bytecodes. (Released via arXiv).
6. Eth2Vec: Machine-Learning-Based Analyzer for Solidity. (Published in BSCI 2021.)
7. APVAS+: Implementation for BGPsec with Aggregate Signature. (Published in ICC 2021.)
8. Anonymous Broadcast Authentication.

Academic Contribution

Organizing Committee (for International Conference)

1. The 10th International Workshop on Security (IWSEC 2015), Organizing Committee (Publicity Chair). (26-28th August 2015 at Nara, Japan.)
2. The Nineth International Conference on Provable Security (ProvSec 2015), Organizing Committeee (Publicity Chair). (24-26th November 2015 at Ishikawa, Japan.)
3. The 11th International Workshop on Security (IWSEC2016), Organizing Committee (Publicity Chair). (12-14th September 2016 at Tokyo, Japan.)
4. The 15th International Conference on Applied Cryptography and Network Security (ACNS2017), Organizing Committee (Publicity Chair). (10-12th July 2017 at Ishikawa, Japan.)
5. The 14th International Conference on Information Security Practice and Experience (ISPEC 2018), Organizing Committee (Liaison Chair). (25-27th September 2018 at Tokyo, Japan.)
6. The 22st Workshop on Elliptic Curve Cryptography (ECC 2018), Organizing Committee (Registration Chair). (17-21th November 2018 at Osaka, Japan.)

7. The 13th International Conference on Network and System Security (NSS 2019), Organizing Committee (Publicity Co-Chair). (15-18th December 2019 at Sapporo, Japan.)
8. The 15th International Workshop on Security (IWSEC 2020), Organizing Committee (Local Chair). (2-4th September 2020 at Fukui, Japan.)
9. The 25th Public Key Cryptography (PKC 2022), Organizing Committee (Web Chair). (March 7-11 2022 at Yokohama, Japan.)
10. The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), Organizing Committee (Poster Chair). (30th May-2nd June at Nagasaki, Japan.)
11. The 18th International Workshop on Security (IWSEC 2023), Organizing Committee (Poster Chair). (29-31th August 2018 at Tokyo, Japan.)

Program Co-Chair (for International Conference)

1. The 7th ACM ASIA Public-Key Cryptography Workshop (APKC 2020). (1th June 2020 at Taipei, Taiwan.) (Co-located in AsiaCCS 2020 on 1-5th June 2020 at Taipei, Taiwan.)
2. The 9th ACM ASIA Public-Key Cryptography Workshop (APKC 2022). (30th May 2022 at Nagasaki, Japan.) (Co-located in AsiaCCS 2022 on 30th May1-3rd June 2022 at Nagasaki, Japan.)
3. The First Workshop on Security and Artificial Intelligence (SECAI 2023). (25th-29th September at Hague, Netherlands.) (Co-located in ESORICS 2023 25th-29th September, Netherlands.)

Program Committee

1. The Third International Symposium on Computing and Networking (CANDAR 2015), Track 5 Program Committee. (8-11th December 2015, at Hokkaido, Japan.)
2. The Second International Workshop on Information and Communication Security (WICS 2015), Program Committee. (Co-located in CANDAR 2015 on 8-11th December 2015 at Hokkaido, Japan.)
3. The Fourth International Symposium on Computing and Networking (CANDAR 2016), Track 5 Program Committee. (22-25th November 2016 at Hiroshima, Japan.)
4. The Third International Workshop on Information and Communication Security (WICS 2016), Program Committee. (Co-located in CANDAR 2016 on 22-25th November 2016 at Hiroshima, Japan.)
5. The Fifth International Symposium on Computing and Networking (CANDAR 2017), Track 5 Program Committee. (19-22th November 2017 at Aomori, Japan.)
6. The Third International Workshop on Information and Communication Security (WICS 2017), Program Committee. (Co-located in CANDAR 2017 on 19-22th November 2017 at Aomori, Japan.)
7. The Sixth International Symposium on Computing and Networking (CANDAR 2018), Track 5 Program Committee. (27-30th November 2018 at Hida Takayama, Japan.)

8. The Fourth International Workshop on Information and Communication Security (WICS 2018), Program Committee. (Co-located in CANDAR 2018 on 27-30th November 2018 at Hida Takayama, Japan.)
9. The Seventh International Symposium on Computing and Networking (CANDAR 2019), Track 5 Program Committee. (November 26-29th at Nagasaki, Japan.)
10. The Fifth International Workshop on Information and Communication Security (WICS 2019), Program Committee. (Co-located in CANDAR 2019 on November 26-29th at Nagasaki, Japan.)
11. The Eighth International Symposium on Computing and Networking (CANDAR 2020), Track 5 Program Committee. (November 24-27th at Virtual, Japan.)
12. The Sixth International Workshop on Information and Communication Security (WICS 2020), Program Committee. (Co-located in CANDAR 2021 on November 24-27th at Virtual, Japan.)
13. The 21st World Conference on Information Security Applications (WISA 2020), Program Committee (26-28th August 2020 at Jeju Island, Korea.)
14. The Ninth International Symposium on Computing and Networking (CANDAR 2021), Track 5 Program Committee. (November 23-26th at Virtual, Japan.)
15. The Seventh International Workshop on Information and Communication Security (WICS 2021), Program Committee. (Co-located in CANDAR 2021 on November 23-26th at Virtual, Japan.)
16. The 22st World Conference on Information Security Applications (WISA 2021), Program Committee (11-13th August 2021 at Jeju Island, Korea.)
17. The 5th International Symposium on Mobile Internet Security (MobiSec 2021), Program Committee (7th-9th October 2021 at Jeju Island, Korea.)
18. The Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2022) Program Committee (30th May- 3rd June at Nagasaki, Japan.)
19. The Tenth International Symposium on Computing and Networking (CANDAR 2022), Track 5 Program Committee. (November 21-22th at Himeji, Japan.)
20. The Eighth International Workshop on Information and Communication Security (WICS 2022), Program Committee. (Co-located in CANDAR 2022 on November 21-22th at Himeji, Japan.)
21. The 23st World Conference on Information Security Applications (WISA 2022), Program Committee (24-26th August 2022 at Jeju Island, Korea.)
22. The 6th International Symposium on Mobile Internet Security (MobiSec 2022), Program Committee (15th-17th December 2022 at Jeju Island, Korea.)
23. The Fifth ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2023) Program Committee (10th July - 14th July at Melbourne, Australia.)
24. The 24th World Conference on Information Security Applications (WISA 2023), Program Committee (23-25th August 2023 at Jeju Island, Korea.)

Editors

1. IEICE Transactions on Information and Systems, "Special Section on Security, Privacy and Anonymity of Internet of Things", associate editor, November 2015 to August 2016.

2. IEICE Transactions on Information and Systems, “Special Section on Security, Privacy and Anonymity in Computation, Communication and Storage Systems”, associate editor, May 2016 to August 2017.
3. IEICE Transactions on Information and Systems, “Special Section on Security, Privacy, Anonymity and Trust in Cyberspace Computing and Communications”, associate editor, January 2019 to February 2020.
4. IEICE Transactions on Information and Systems, associate editor on regular issues, June 2019 to June 2023.
5. MDPI, Cryptography, Reviewer Board, from May 2020 (to be continued).
6. IEICE Transactions on Information and Systems, “Special Section on Next-Generation Security Application and Practice”, editor-in-chief, October 2020 to November 2021.
7. IEICE Transactions on Information and Systems, “Blockchain Systems and Applications”, associate editor, October 2020 to November 2021.
8. MDPI, Cryptography, Reviewer Board, from May 2020.
9. IEICE Transactions on Information and Systems, “Special Section on Next-Generation Security Application and Practice”, editor-in-chief, October 2021 to November 2022.