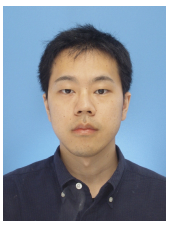
Haruka Hirata, Ph.D.

h.haruka@uec.ac.jp haruka.hirata11@gmail.com hhirata11
https://ykm11.phd



Employment History

2026 – **Postdoctoral researcher** The University of Electro-Communications.

Education

2026 **Ph.D. in Engineering, The University of Electro-Communications**
Thesis title: *Evaluation and Improvement of M&M-Protected AES Hardware: Zero-Value Attacks, Countermeasures, and Optimization*

2023 **M.E., The University of Electro-Communications**

2021 **B.E., The University of Electro-Communications**

Research Publications

Journal Articles

1. K. Li, **H. Hirata**, D. Miyahara, et al., "Toward cost-effective combined countermeasures: Multiplicative masked m&m," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 109, no. 3, pp. 290–304, 2026. DOI: 10.1587/TRANSFUN.2025CIP0024.
2. M. Tsukahara, Y. Harada, **H. Hirata**, et al., "Practical randomness effects on physical security in second-order threshold implementation of AES," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 108, no. 3, pp. 193–206, 2025. DOI: 10.1587/TRANSFUN.2024CIP0010.
3. **H. Hirata**, D. Miyahara, V. Arribas, et al., "All you need is fault: Zero-value attacks on AES and a new λ-detection m&m," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2024, no. 1, pp. 133–156, 2024. DOI: 10.46586/TCHES.V2024.I1.133-156.
4. R. Hatano, **H. Hirata**, K. Matsuda, et al., "Evaluation of side-channel attack resistance on lfi detection circuits," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (Japanese Edition)*, vol. J104-A, no. 5, pp. 118–126, 2021, ISSN: 1881-0195. DOI: 10.14923/transfunj.2020jap1023.

Conference Proceedings

1. **H. Hirata**, K. Furuno, D. Miyahara, et al., "Experimental evaluations of fault sensitivity imbalance for masked AES using t-test and entropy," in *Thirteenth International Symposium on Computing and Networking, CANDAR 2025, Yamagata, Japan, November 25-28, 2025*, IEEE, 2025, pp. 127–132. DOI: 10.1109/CANDAR68384.2025.00024.
2. **H. Hirata**, D. Miyahara, Y. Hara, et al., "Let's share a secret: Share-reduced design of m&m for the AES s-box," in *Applied Cryptography and Network Security Workshops - ACNS 2025 Satellite Workshops: AIHWS*, M. Manulis, Ed., ser. LNCS, Springer, 2025, pp. 144–160. DOI: 10.1007/978-3-032-01799-4_9.
3. **H. Hirata**, Y. Harada, Y. Hara, et al., "Yet another physical leakage assessment with the wasserstein distance," in *Asian Hardware Oriented Security and Trust Symposium, AsianHOST 2024, Kobe, Japan, December 16-18, 2024*, IEEE, 2024, pp. 1–6. DOI: 10.1109/ASIANHOST63913.2024.10838480.

4 K. Li, **H. Hirata**, D. Miyahara, et al., "Multiplicative masked m&m: An attempt at combined countermeasures with reduced randomness," in *23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2024, Sanya, China, December 17-21, 2024*, IEEE, 2024, pp. 726–733. DOI: 10.1109/TRUSTCOM63139.2024.00112.

5 M. Tsukahara, **H. Hirata**, M. Yang, et al., "On the practical dependency of fresh randomness in AES s-box with second-order TI," in *Eleventh International Symposium on Computing and Networking, CANDAR 2023 - Workshops, Matsue, Japan, November 27-30, 2023*, IEEE, 2023, pp. 286–291. DOI: 10.1109/CANDARW60564.2023.00054.

Skills

Languages — Japanese (native), English (working proficiency), German and Dutch (very basic)

Coding — C, C++, Python, Verilog-HDL.

Miscellaneous

Awards and Achievements

2025 — **Student Award**, The University of Electro-Communications (FY2024).

2023 — **Best Paper Award**, CANDAR 2023.

Grants

2025-04 – 2027-03 — JSPS Fellows Grant.

Declined — JST SPRING Program.