

Vincent Hwang

* Year of birth: 1997
✉ vincentvbh7@gmail.com
🌐 <https://vincentvbh.github.io/>
📄 <https://github.com/vincentvbh>

Education

- 2023.01— **PhD (thesis submitted in 2025.07)**, *Max Planck Institute for Security and Privacy*, Bochum, Germany
2026.03
- 2021.09— **MSc.**, *National Taiwan University*, Taipei, Taiwan
2022.06
- 2016.09— **BSc.**, *National Taiwan University*, Taipei, Taiwan
2021.06
- 2013.09— **High school**, *Kaohsiung Municipal Kaohsiung Senior High School*, Kaohsiung, Taiwan
2016.06

Experience

- 2026.04— **Senior Software Engineer**, *A startup*, Boston, USA, Full time.
Now
- 2023.01— **PhD Student**, *Max Planck Institute for Security and Privacy*, Bochum, Germany, Full time.
2026.03
Academic publications on microcontrollers (×1), mid-tier/high-performance processors (×1), formal verification (×2), survey of polynomial multiplications (×1), portable implementations of cryptography (×1).
- 2022.07— **Research Assistant**, *Academia Sinica*, Taipei, Taiwan, Full time.
2022.12
Academic publications on mid-tier/high-performance processors (×2).
- 2022.02— **Teaching Assistant**, *National Taiwan University*, Taipei, Taiwan, Voluntary.
2022.06
Final project evaluation.
- 2021.07— **Research Assistant**, *Academia Sinica*, Taipei, Taiwan, Full time.
2021.08
Academic publications on microcontrollers (×4), mid-tier/high-performance processors (×1), and formal verification (×1).
- 2020.07— **Summer Intern**, *Academia Sinica*, Taipei, Taiwan, Full time.
2020.08
Academic publications on microcontrollers (×2).

Skills

Programming

Assembly (Armv7-M, Armv7E-M, Armv8-A, Armv9-A, AVX2, AVX-512), C/C++, CUDA, Haskell, Sage.

Tools

Arm GNU toolchain, GCC, Clang, GNU Make, GNU Bash, Python 3, Clang, CryptoLine, Jasmin compiler.

Preferred Work Locations

Citizenship

USA, Taiwan.

Publications

2021-2026 **List of all publications.**

Academic Service

2026 **Reviewer**

TCHES 2026 (×6), Eurocrypt 2026 (×1), Crypto 2026 (×2)

2026 **Artifact Committee Member**

TCHES 2026 (×6), Eurocrypt 2026 (×4)

2025 **Reviewer**

TCHES 2025 (×8), ArcticCrypt 2025 (×1), CT-RSA 2025 (×2), JCEN (×1)

2025 **Artifact Committee Member**

TCHES 2025 (×5)

2024 **Reviewer**

Crypto 2024 (×1), TCHES 2024 (×3)

2023 **Artifact Committee Member**

TCHES 2023 (×2)

TCHES = Transactions on Cryptographic Hardware and Embedded Systems;

CT-RSA = The Cryptographers' Track at RSA Conference;

JCEN = Journal of Cryptographic Engineering;

(·) = The number of reviews submitted.

Languages

Manderin Native

English Working proficiency

German Very basic