

Vincent Hwang

* Year of birth: 1997
✉ vincentvvh7@gmail.com
🌐 <https://vincentvvh.github.io/>
🔗 <https://github.com/vincentvvh>

Education

2023–Now **PhD**, *Max Planck Institute for Security and Privacy*, Bochum, Germany

2021–2022 **MSc.**, *National Taiwan University*, Taipei, Taiwan

2016–2021 **BSc.**, *National Taiwan University*, Taipei, Taiwan

2013–2016 **High school**, *Kaohsiung Municipal Kaohsiung Senior High School*, Kaohsiung, Taiwan

Experience

2023.01— **PhD Student**, *Max Planck Institute for Security and Privacy*, Bochum, Germany, Full time
Academic publications on microcontrollers (×1), mid-tier/high-performance processors (×1), formal verification (×2), survey of polynomial multiplications (×1), portable implementation of cryptography (×1).

2022.07— **Research Assistant**, *Academia Sinica*, Taipei, Taiwan, Full time
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, Bash, Python 3, Clang, CryptoLine, Jasmin compiler.

Academic Services

2026 **Reviewer**
TCHES 2026 (×3), Eurocrypt 2026 (×1)

2026 **Artifact Committee Member**
TCHES 2026 (×2)

2025 Reviewer

TCCHES 2025 ($\times 8$), ArcticCrypt 2025 ($\times 1$), CT-RSA 2025 ($\times 2$), JCEN ($\times 1$)

2025 Artifact Committee Member

TCCHES 2025 ($\times 5$)

2024 Reviewer

Crypto 2024 ($\times 1$), TCCHES 2024 ($\times 3$)

2023 Artifact Committee Member

TCCHES 2023 ($\times 2$)

TCCHES = Transactions on Cryptographic Hardware and Embedded Systems;

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

JCEN = Journal of Cryptographic Engineering;

(\times) = The number of reviews submitted.

Languages

Manderin Native

English Working proficiency

German Basic greetings