Yingchen Wang

Curriculum Vitae

Department of Computer Science
University of Texas at Austin
✉ *yingchen@cs.utexas.edu*
🖱 *My Webpage*

Education

2019–present **Ph.D. in Computer Science**, *University of Texas at Austin*.
Advisor: Hovav Shacham
Research Area: Applied Cryptography, Hardware Security

2014–2019: **Bachelor of Science - Physics**, *University of Southern California*, Major GPA: 3.82/4.00.

2014–2019: **Bachelor of Science - Computer Science**, *University of Southern California*, Major GPA: 3.97/4.00.

Award

2023 **EECS Rising Star**.

2023 **IEEE Micro Top Picks**: Hertzbleed.

2022 **Black Hat Pwnie Award—Best Cryptographic Attack**: Hertzbleed.

2018 **USC Viterbi Undergraduate Awards**: Computer Science Award for Outstanding Research.

Invited Talks

2024 **Hertzbleed: The claim of constant-time is frequency wrong**.
UT Austin System Lunch

2023 **Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86**.
Texas Crypto Day

2022 **Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86**.
Crypto Workshop on Attacks in Cryptography
Intel Security Advisories (Chips & Salsa) Episode 19
Cloudflare TV: Hertzbleed in simple terms
MIT security seminar, USCB security seminar, Stanford security seminar

Conference Talks

2023 **DVFS Frequently Leaks Secrets: Hertzbleed Attacks Beyond SIKE, Cryptography, and CPU-Only Data**.
IEEE Symposium on Security and Privacy 2023

2022 **Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86**.
Usenix Security 2022

Publications

2024 **Yingchen Wang**, Riccardo Paccagnella, Zhao Gang, Willy R. Vasquez, David Kohlbrenner, Hovav Shacham, and Christopher W. Fletcher. GPU.zip: On the side-channel implications of hardware-based graphical data compression. In *IEEE Security and Privacy*, 2024.

2024 Boru Chen, **Yingchen Wang**, Pradyumna Shome, Christopher Fletcher, David Kohlbrenner, Riccardo Paccagnella, and Daniel Genkin. Data marauding prefetcher: Breaking constant-time cryptography on apple cpus. In *Under submission*, 2024.

2023 **Yingchen Wang**, Riccardo Paccagnella, Alan Wandke, Zhao Gang, Grant Garrett-Grossman, Christopher W Fletcher, David Kohlbrenner, and Hovav Shacham. Dvfs frequently leaks secrets: Hertzbleed attacks beyond sike, cryptography, and cpu-only data. In *IEEE Security and Privacy*, 2023.

2023 **Yingchen Wang***, Riccardo Paccagnella*, Elizabeth He, Hovav Shacham, Christopher W. Fletcher, and David Kohlbrenner. Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86. *Ieee Micro*. IEEE, 2023.

2022 **Yingchen Wang***, Riccardo Paccagnella*, Elizabeth He, Hovav Shacham, Christopher W. Fletcher, and David Kohlbrenner. Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86. In *USENIX Security*, 2022.

Blog Posts

2022 **The Cloudflare blog: Hertzbleed explained**.
Yingchen Wang, Armando Faz-Hernández

Disclosures

AMD
Apple
ARM
Imagination
Intel
NVIDIA
Qualcomm

GPU.zip, *Status: Mesa software patch in progress.*
CVE : CVE-2023-44216 (Imagination)
Reporter: Yingchen Wang, Riccardo Paccagnella, Zhao Gang, Willy R. Vasquez, David Kohlbrenner, Hovav Shacham, Christopher W. Fletcher

AMD
Intel

Hertzbleed, *Status: closed; Intel bug bounty awarded.*
CVE : CVE-2022-23823 (AMD), CVE-2022-35888 (Ampere), CVE-2022-24436 (Intel)
Reporter: Yingchen Wang, Riccardo Paccagnella, Elizabeth Tang He, Hovav Shacham, Christopher Fletcher, David Kohlbrenner

Cloudflare **Remote timing attack on CIRCL SIKE library**, *Status: closed; software patch released.*
Reporter: Yingchen Wang, Hovav Shacham

Microsoft **Remote timing attack on PQCrypto-SIDH library**, *Status: closed; Software patch released.*
Reporter: Yingchen Wang, Hovav Shacham

Service

2023 **CHES**, *Artifact evaluation committee.*

2023 **EAI SecureComm**, *External reviewer.*

Leadership Experience

Spring, 2023 **Directed Reading Program**, *Instructor.*
Organize computer security reading group for undergraduate students in computer science at UT Austin.

Teaching Assistantship

Spring, 2018 **ITP439: Compiler Development**, University of Southern California.

Fall, 2017 **ITP365: Managing Data in C++**, University of Southern California.

Spring, 2017
Fall, 2016 **ITP165: Introduction to C++ Programming**, University of Southern California.

Work Experience

Spring, 2023 **Intel**, *Graduate Research Internship.*
Rowhammer attacks on CRYSTALS-Dilithium.

Summer, 2022 **Cloudflare**, *Graduate Research Internship.*
Implementation of Threshold ECDSA signature into Cloudflare CIRCL library.

Computer skills

Programming Languages C/C++, Go, Rust, X86 Assembly, ARM assembly, Python, Java, SQL, PHP, Javascript, HTML

Software & Simulator	Gem5, rr-debugger, LLVM, Linux perf, RAPL, Intel QAT, QEMU, Google sandbox API
Framework	OpenCL, OpenGL, SYCL