Armando Faz Hernandez

Security, Cryptography, Software Optimization

San Francisco, CA. USA
armfazh@gmail.com
armfazh.github.io
armfazh
armfazh

Interests

Systems Security
Secure software development. Authentication protocols. Privacy-enhacing technologies. Role-based access control. Federated learning.

Cryptography
Post-Quantum Cryptography. Web PKI & TLS. Zero-knowledge Proofs. Anonymous Credentials. Formal methods.

Software Optimization
Performance profiling. Parallel Architectures. ARM and x64-86 Assembler.

Software Engineering
Proof of concept development. Scaling applications. Analysis of real-world constraints.

Work Experience

2018–2026 **Research Engineer**, *Cloudflare, Inc.*, San Francisco, CA. USA
- Anonymous Credentials: Privacy Pass, zkAttest for WebAuthn, unlinkable tokens and rate-limiting.
- CIRCL, founder of Cloudflare's open source Go cryptographic library.
- Transition to Post-Quantum Cryptography: experimentation and advanced constructions.
- Performance optimization and secure software development.

2012 **Research Intern**, *Microsoft Research*, Redmond, WA. USA
- Security and Cryptography team formerly known as the eXtreme Computing Group.
- Design of secure algorithms for elliptic curve cryptography.

Education

2013–2022 **PhD in Computer Science**, *University of Campinas*, SP. Brazil, 3.5/4.0
High-Performance Elliptic Curve Cryptography: A SIMD Approach to Modern Curves
- Improve efficiency of cryptographic algorithms: ECDSA, EdDSA, and X25519 by using SIMD parallel instructions. Under supervision of Julio López, PhD.

2009–2012 **MSc in Computer Science**, *Center for Research and Advanced Studies of IPN*, Mexico, 95/100
Multi-core Implementation of Scalar Point Multiplication over Koblitz Curves
- Improve efficiency of Koblitz curves using multi-core parallel processing and the carry-less multiplier. Under supervision of Francisco Rodríguez Henríquez, PhD and Debrup Chakraborty, PhD.

2004–2009 **BSc in Computer Engineering**, *Autonomous University of San Luis Potosi*, Mexico, 93/100
- Graduated with Honors.

Skills

Programming	C, Go, Rust, Assembly, Python, JS/TS	Internet	TLS, DNS, QUIC, HTTPS
Security	OWASP, Vault, Semgrep	Parallel	OpenMP, SIMD, AVX2/AVX512, GPU
Tools	Kubernetes, Docker, Prometheus	Tools	Git, Jira, CI/CD, Slack

Languages

English Portuguese Spanish

Specifications

Patents

US-2022/0321354-A1, *Using a zero-knowledge proof to prove knowledge that a website visitor is a legitimate human user*, Oct, 2022.

Internet RFC at IETF

A. Faz-Hernandez, S. Scott, N. Sullivan, R. S. Wahby, and C. A. Wood, "Hashing to elliptic curves," Internet Research Task Force, Tech. Rep. RFC 9380, Aug. 2023.

A. Davidson, A. Faz-Hernandez, N. Sullivan, and C. A. Wood, "Oblivious pseudorandom functions (OPRFs) using prime-order groups," Internet Research Task Force, Tech. Rep. RFC 9497, Dec. 2023.

C. Yun, C. A. Wood, and A. Faz-Hernandez, "Privacy Pass issuance protocol for anonymous rate-limited credentials," Internet Engineering Task Force, Tech. Rep., Mar. 2026, (Work in Progress).

Scientific Publications

Journal Articles

A. Faz-Hernandez and J. López, "High-performance elliptic curve cryptography: A SIMD approach to modern curves (Thesis Distillation)," *Journal of the Brazilian Computer Society*, vol. 32, no. 1, p. 516–526, Mar. 2026. doi: 10.5753/jbcs.2026.5548

——, "High-performance elliptic curve cryptography: A SIMD approach to modern curves (extended thesis summary)," *CLEI Electronic Journal*, vol. 27, no. 3, Aug. 2024. doi: 10.19153/CLEIEJ.27.3.3

A. Faz-Hernández, J. López, and R. Dahab, "High-performance implementation of elliptic curve cryptography using vector instructions," *ACM Transactions on Mathematical Software (TOMS)*, vol. 45, no. 3, p. 1–35, Jul. 2019. doi: 10.1145/3309759

A. Faz-Hernández, J. López, E. Ochoa-Jiménez, and F. Rodríguez-Henríquez, "A faster software implementation of the supersingular isogeny Diffie-Hellman key exchange protocol," *IEEE Transactions on Computers*, vol. 67, no. 11, p. 1622–1636, Nov. 2018. doi: 10.1109/TC.2017.2771535

A. Faz-Hernández, P. Longa, and A. H. Sánchez, "Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV-GLS curves (extended version)," *Journal of Cryptographic Engineering*, vol. 5, no. 1, p. 31–52, Apr. 2015. doi: 10.1007/s13389-014-0085-7

J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, and J. López, "Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction," *Journal of Cryptographic Engineering*, vol. 1, no. 3, p. 187–199, Sep. 2011. doi: 10.1007/s13389-011-0017-8

Peer-Reviewed Conference Articles

R. Cabral, A. Faz-Hernandez, and J. López, "Accelerating HQC key encapsulation mechanism with AVX-512," in *Proceedings of the 13th ACM on ASIA Public-Key Cryptography Workshop*, ser. APKC '26. ACM, 2026, p. 1–10. doi: 10.1145/3803627.3805815

A. Faz-Hernandez, "Rhizomes and the roots of efficiency—Improving Prio," in *Progress in Cryptology — LATINCRYPT 2025*, ser. Lecture Notes in Computer Science, vol. 16129. Medellin, Colombia: Springer, Oct. 2025, p. 425–449. doi: 10.1007/978-3-032-06754-8_16

W. Ladd, T. Verma, M. Venema, A. Faz-Hernandez, B. McMillion, A. Wildani, and N. Sullivan, "Portunus: Re-imagining access control in distributed systems," in *2023 USENIX Annual Technical Conference (USENIX ATC 23)*, J. Lawall and D. Williams, Eds. Boston, MA: USENIX Association, Jul. 2023, p. 35–52. [Online]. Available: https://www.usenix.org/conference/atc23/presentation/ladd

T. Whalen, T. Meunier, M. Kodali, A. Davidson, M. Fayed, A. Faz-Hernández, W. Ladd, D. Maram, N. Sullivan, B. C. Wolters, M. Guerreiro, and A. Galloni, "Let the right one in: Attestation as a usable CAPTCHA alternative," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Boston, MA: USENIX Association, Aug. 2022, p. 599–612. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/whalen

A. Faz-Hernández, W. Ladd, and D. Maram, "ZKAttest: Ring and group signatures for existing ECDSA keys," in *Selected Areas in Cryptography – SAC 2021*, BC, Canada, Oct. 2021, p. 68–83. doi: 10.1007/978-3-030-99277-4_4

S. Celi, A. Faz-Hernández, N. Sullivan, G. Tamvada, L. Valenta, T. Wiggers, B. Westerbaan, and C. A. Wood, "Implementing and measuring KEMTLS," in *Progress in Cryptology – LATINCRYPT 2021*, P. Longa and C. Ràfols, Eds. Bogota, Colombia: Springer, Oct. 2021, p. 88–107. doi: 10.1007/978-3-030-88238-9_5

A. Faz-Hernández and J. López, "Generation of elliptic curve points in tandem," in *XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, I. M. Moraes and L. Kowada, Eds., vol. 20. Petrópolis, RJ, Brasil: Sociedade Brasileira de Computação, Oct. 2020, p. 1–9. doi: 10.5753/sbseg.2020.19230

T. Oliveira, J. López, H. Hişil, A. Faz-Hernández, and F. Rodríguez-Henríquez, "How to (pre-)compute a ladder: Improving the performance of X25519 and X448," in *Selected Areas in Cryptography - SAC 2017*, C. Adams and J. Camenisch, Eds. Cham: Springer International Publishing, 2018, p. 172–191. doi: 10.1007/978-3-319-72565-9_9

A. Faz-Hernandez, J. López, and A. K. D. S. de Oliveira, "SoK: A performance evaluation of cryptographic instruction sets on modern architectures," in *Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop*, ser. APKC '18. Incheon, Republic of Korea: ACM, 2018, p. 9–18. doi: 10.1145/3197507.3197511

A. Faz-Hernández, H. Fujii, D. F. Aranha, and J. López, "A secure and efficient implementation of the quotient digital signature algorithm (qDSA)," in *Security, Privacy, and Applied Cryptography Engineering*, S. S. Ali, J.-L. Danger, and T. Eisenbarth, Eds. Cham: Springer International Publishing, 2017, p. 170–189. doi: 10.1007/978-3-319-71501-8_10

A. Faz-Hernández and J. López, "Speeding up elliptic curve cryptography on the P-384 curve," in *XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, vol. 16. Niteroi, Brazil: Sociedade Brasileira de Computação - SBC, Nov. 2016, p. 170–183. doi: 10.5753/sbseg.2016.19306

——, "Fast implementation of Curve25519 using AVX2," in *Progress in Cryptology - LATINCRYPT 2015*, K. Lauter and F. Rodríguez-Henríquez, Eds. Guadalajara, Mexico: Springer, 2015, p. 329–345. doi: 10.1007/978-3-319-22174-8_18

A. Faz-Hernández, R. Cabral, D. F. Aranha, and J. López, "Implementação eficiente e segura de algoritmos criptográficos," in *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, E. Souto, M. Wangham, and J. Fraga, Eds. Florianópolis, Brazil: Sociedade Brasileira de Computação, Nov. 2015, vol. 183, ch. 3, p. 93–140. ISBN 978-85-7669-304-8

A. Faz-Hernández and J. López, "On software implementation of arithmetic operations on prime fields using AVX2," in *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, ser. SBSeg, vol. 14. Minas Gerais, Brazil: Sociedade Brasileira de Computação, Nov. 2014, p. 338–341. doi: 10.5753/sbseg.2014.20148

A. Faz-Hernández, P. Longa, and A. H. Sánchez, "Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV-GLS curves," in *Topics in Cryptology - CT-RSA 2014*, J. Benaloh, Ed. San Francisco, USA: Springer, 2014, p. 1–27. doi: 10.1007/978-3-319-04852-9_1

D. F. Aranha, A. Faz-Hernández, J. López, and F. Rodríguez-Henríquez, "Faster implementation of scalar multiplication on Koblitz curves," in *Progress in Cryptology - LATINCRYPT 2012*, A. Hevia and G. Neven, Eds. Santiago, Chile: Springer Berlin Heidelberg, 2012, p. 177–193. doi: 10.1007/978-3-642-33481-8_10

J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, and J. López, "Software implementation of binary elliptic curves: Impact of the carry-less multiplier on scalar multiplication," in *Cryptographic Hardware and Embedded Systems - CHES 2011*, B. Preneel and T. Takagi, Eds. Nara, Japan: Springer Berlin Heidelberg, 2011, p. 108–123. doi: 10.1007/978-3-642-23951-9_8

Conference Presentations

G.-V. Policharla, B. Westerbaan, A. Faz-Hernández, and C. A. Wood, "Post-quantum privacy pass via post-quantum anonymous credentials," Real World Crypto Symposium, Mar. 2023. [Online]. Available: https://eprint.iacr.org/2023/414

S. Celi, A. F. Hernández, P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," Real World Crypto Symposium, Jan. 2021.

Awards

Jun, 2026 **Best Paper Award**, granted to "Accelerating HQC Key Encapsulation Mechanism with AVX-512" paper by APKC 2026,

Sep, 2024 **Honorific Mention**, granted by SBSeg 2024 for best PhD thesis,

Aug, 2023 **Finalist at Brazilian National Contest**, The 36th ed. Thesis and Dissertation Contest organized by the Congress of the Brazilian Computing Society,

Apr, 2022 **Honorific Mention**, UNICAMP Highlight Thesis Award, granted by the University of Campinas,

Dec, 2022 **Best Doctoral Thesis Award**, granted by the Institute of Computing,

Nov, 2016 **Best Paper Award**, granted to "Speeding up the elliptic curve cryptography on the P-384 curve" paper by SBSeg 2016,

Speaking Opportunities

Feb, 2026 **NIST Crypto Reading Club**, *Hashing to Curves: From Theory to RFC 9380 Specification*, Virtual, Invited Speaker.
csrc.nist.gov/presentations/2026/crclub-2026-02-18

Nov, 2025 **CyberQ 2025**, *PQC Pilots in the World – What We've Learned*, Abu Dhabi, UAE, Invited Speaker.
cyberq.ae/speakers

Sep, 2025 **Latincrypt 2025**, *Rhizomes and the Roots of Efficiency – Improving Prio*, Medellin, Colombia, Contributed Talk.
ciencias.medellin.unal.edu.co/eventos/latincrypt

Sep, 2025 **CatioCrypto 2025**, *Elliptic Curves and Zero-knowledge Proofs*, Medellin, Colombia, Invited Lecturer.
octavio.pk/catiocrypto/2025

Oct, 2024 **3rd RCI 5.0**, *Salvaguardando los bits de Internet*, Puebla, Mexico, Invited Speaker.
ciberseguridadindustria.inaoep.mx/2024

Sep, 2023 **NIST MPTS 2023**, *Requirements for Threshold TLS*, Virtual, Contributed Talk.
csrc.nist.gov/Presentations/2023/mpts2023-day2-talk-threshold-tls-rsa

Sep, 2023 **NIST MPTS 2023**, *Verifiable Oblivious PRF*, Virtual, Contributed Talk.
csrc.nist.gov/Presentations/2023/mpts2023-day3-talk-verifiable-oprf

Oct, 2021 **ASCrypto 2021**, *Love in the Time of Hash to Curve*, Bogota, Colombia, Invited Speaker.
www.youtube.com/watch?v=_W1iCoQXEzk

Open-Source Software

C & Assembler

fld-ecc-vec — **RFC 8032**, SIMD implementation of X25519, Ed25519, X448 and Ed448.
`github.com/armfazh/fld-ecc-vec`

rfc7748_precomputed — **RFC 7748**, Optimized code for Diffie-Hellman functions X25519 and X448.
`github.com/armfazh/rfc7748_precomputed`

nistp384_avx2 — **ECDSA/ECDH**, AVX2 Implementation of the P-384 elliptic curve.
`github.com/armfazh/nistp384_avx2`

hpke-simdium — **RFC 9180**, SIMD accelerated HPKE hybrid public-key encryption.
`github.com/armfazh/hpke-simdium`

Rust

arc — **ARC**, Library for Anonymous Rate-limiting Credentials.
`github.com/cloudflareresearch/arc`

h2c-rust-ref — **RFC 9380**, Hash to curve implementation.
`github.com/armfazh/h2c-rust-ref`

Go

CIRCL — **PQC/ECC**, A high-performance library for elliptic curves and post-quantum cryptography.
`github.com/cloudflare/circl`

h2c-go-ref — **RFC 9380**, Hash to curve implementation.
`github.com/armfazh/h2c-go-ref`

TypeScript

Silk — **Privacy Pass**, Client browser extension to get and redeem Privacy Pass tokens.
`github.com/cloudflare/pp-browser-extension`

zkp-ecdsa — **ZKAttest**, Proves knowledge of an ECDSA signature under one of many public keys.
`github.com/cloudflare/zkp-ecdsa`

blindrsa-ts — **RFC 9474**, Library for Blind RSA Signatures.
`github.com/cloudflare/blindrsa-ts`

voprf-ts — **RFC 9497**, Library for OPRF: Oblivious Pseudorandom Functions.
`github.com/cloudflare/voprf-ts`

privacypass-ts — **RFC 9578**, Library for the Privacy Pass Protocol.
`github.com/cloudflare/privacypass-ts`

opaque-ts — **RFC 9807**, Library for OPAQUE: Password-Authenticated Key Exchange.
`github.com/cloudflare/opaque-ts`