Edouard Dufour

@ me@ed0u.com ☎ +1 (412) 626 - 4097 www.ed0u.com github.com/edufourfr

EXPERIENCE

System Software Engineer, Security - SPEAR team

Apple Inc. - SEAR

July 2023 - *Now*

Cupertino, CA

First engineer to join the team.

- Leading initiatives to secure Apple devices through memory safety.
- Hardened Apple's xnu kernel by using modern techniques to enforce robust input validation by developers.

Security Software Engineer, Apple Vision Pro

Apple Inc. - Technology Development Group, Security

Feb 2020 - June 2023

Sunnyvale, CA

- Led the design and implementation of the secure enclave software for the R1 chip.
- Developed cryptographic drivers, firmware, and other low-level software in C.
- Supported client teams in securely adopting our cryptographic APIs for their applications.
- Proposed and implemented novel cryptographic protocols, improving on existing designs.
- Collaborated with factory teams to enable silicon key provisioning and device certification.

Software Engineering Intern

Google LLC - Enclave Crypto

Summer 2019

Sunnyvale, CA

- Designed cryptographic protocols for hardware enclaves, enabling new applications that distribute trust.
- Implemented a protocol using Oblivious PRFs and secret sharing in C++, presenting a demo to senior management.
- Proposed an enhanced protocol with elliptic curve pairings, simplifying interactions between the enclaves.

Software Engineering Intern

Google LLC - Machine Learning Infrastructure Reliability

Summer 2018

Pittsburgh, PA

- Designed and implemented subgraph caching in TensorFlow Serving using C++ and Python.
- Improved model inference performance and reduced latency through efficient resource usage.

PUBLICATIONS

Dynamic Decentralized Functional Encryption by Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, David Pointcheval. In Advances in Cryptology - Proceedings of CRYPTO '20 – Part I, Springer, vol. 12170, pp. 747-775, 2020

Partially Encrypted Machine Learning using Functional Encryption by Théo Ryffel, Edouard Dufour-Sans, Romain Gay, Francis Bach, David Pointcheval. In Advances in Neural Information Processing Systems (NeurIPS 2019), 2019

Unbounded Inner Product Functional Encryption, with Succinct Keys by Edouard Dufour-Sans, David Pointcheval. In Conference on Applied Cryptography and Network Security (ACNS '19), Springer, vol. 11464, pp. 426-441, 2019

Decentralized Multi-Client Functional Encryption for Inner Product by Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, David Pointcheval. In Advances in Cryptology - Proceedings of ASIACRYPT '18, Springer, vol. 11273, pp. 703-732, 2018

TALKS

Dynamic Decentralized Functional Encryption
Presented at CRYPTO 2020.
Santa Barbara, CA, USA, August 17th 2021.

Partially Encrypted Machine Learning using Functional Encryption
Presented at PPML 2019 (a CRYPTO 2019 workshop).
Santa Barbara, CA, USA, August 18th 2019.

Unbounded Inner Product Functional Encryption, with Succinct Keys
Presented at ACNS 2019.
Bogota, Colombia, June 6th 2019.

EDUCATION

M.S. in Computer Science

Carnegie Mellon University
Sept 2018 – Dec 2019
Pittsburgh, PA

Selected Coursework: Cryptography, Computer Security, Operating Systems, Machine Learning.

CQPA: 3.95

Diplôme d'Ingénieur polytechnicien

Ecole polytechnique
2014 – 2017
Palaiseau, France

Mathematics and Computer Science program.

GPA: 3.77

TEACHING

Teaching Assistant for 15-440/15-640 Distributed Systems

Carnegie Mellon University
Spring 2019 & Fall 2019
Pittsburgh, PA

Led a recitation, designed homework and exam questions, and held office hours.

ADDITIONAL REVIEWER

- 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'21).
- 24th European Symposium on Research in Computer Security (ESORICS'19).
- 11th International Conference, Security and Cryptography for Networks (SCN'18).

PROGRAMMING LANGUAGES

C C++ Go Python

LANGUAGES

French	Native speaker
English	Fluent