Matteo Scarlata

Personal Data

EMAIL	matteo@hjkl.space
PGP	DEE2 2850 0F31 AE39 33C0 C614 0631 28F5 A461 2B3C

Education

MARCH 2021 - CURRENT	PhD student, Applied Security Group, Institute of Information Security, *ETH Zurich*
SEPTEMBER 2018 - FEBRUARY 2021	Master of Science ETH in Computer Science, *ETH Zurich*
SEPTEMBER 2014 - JULY 2017	Bachelor Degree of Computer Science, *University of Pisa*, Cum Laude (Grade 110L/110L)
SEPTEMBER 2016 - JUNE 2017	Erasmus scholarship - exchange year at *University College London*, UK, as part of BSc of Computer Science, University of Pisa

Selected Coursework

PROGRAMMING	ETHZ Advanced Operating Systems Project - Microkernel development **C, radare2**
SYSTEM DEPLOYMENT	ETHZ Applied Security Lab Project **cfssl, NixOS**

Research Experience

APPLIED CRYPTOGRAPHY	2020 – Supervisor: prof. Kenny Paterson – *Post-Compromise Security and TLS 1.3 Session Resumption*, Master Thesis project. **Formal Protocol Analysis, Game Hopping, TLS 1.3**
PUBLIC KEY INFRASTRUCTURES	2019-2020 – Supervisor: prof. Adrian Perrig – *SCION End-Entity PKI*, Research project. **Resilient PKIs, Certificate Transparency, Google Trillian**
CLASSICAL CRYPTANALYSIS	2018 – Supervisor: prof. Nicolas Courtouis – *How many weak-keys exists in T-310?*, published in *Tatra Mountains Mathematical Publications, vol 73, pp 61-82.* **Differential Cryptanalysis, Python, C++**

Publications

2019	- Courtois, N. T., Scarlata, M, How Many Weak-Key Exist in T-310?, Tatra Mountains Mathematical Publications. - Courtois, N. T., Georgiou, M., Scarlata, M, Slide Attacks and LC-Weak Keys in T-310, Cryptologia, 43 (3), 175-189.
2017	- Courtois, N. T., Schmeh, K., Drobick, J., Patarin, J., Oprisanu, M. B., Scarlata, M., & Bhallamudi, O. Cryptographic Security Analysis of T-310.