UCLouvain

icteam

Davide Bellizia, PhD

Post-Doc Researcher

UCLouvain Crypto Group
(Belgium)

davide.bellizia@uclouvain.be

Davide Bellizia was born on June 20th 1989. He received the M.S. degree (summa cum laude) and Ph.D. degree in Electronics Engineering from University “La Sapienza” of Rome (Italy), respectively in 2014 and 2018. In 2014 he received the “Laureato Eccellente” award for the best graduate student of the year. In 2017, he joined to the Crypto Group of Université Catholique de Louvain (UCLouvain), Louvain-la-Neuve, Belgium, as postdoc researcher. His main research interests include the design and evaluation of circuits for hardware security, with particular attention to development of countermeasures against side-channel attacks and PUFs.

He serves as reviewer for many international journals and conferences concerning electronics, physical security and applied cryptography (TCAS, TVLSI, IoT, JCEN, Access, ISCAS, DATE, etc.) and he has been PC member of several internal conf. (COSADE20, CARDIS21, IndoCrypt20, Mal-IoT21).

Sapienza - DIET

- Laurea Triennale Ing. Elettronica (2008-2011)
  - Tesi: ambito elettr. analogica, Prof. Trifiletti (CSGB)
- Laurea Magistrale in Progettazione Elettronica (2012-2014)
  - Tesi: ambito DSP-satellitare su FPGA, Prof. Scotti (CSGB, in coll. con Thales Alenia Spazio Italia)
- Dottorato di Ricerca ICT (2014-2018)
  - Tesi: ambito hardware security e contromisure side-channel analysis, Prof. Scotti (CSGB)

Percorso d'Eccellenza & Laureato Eccellente

- Percorso d'Eccellenza (2013)
  - Tesi: ambito DSP-satellitare su FPGA
  - Azienda: Thales Alenia Spazio Italia
  - Rel.: Prof. Scotti, Dr. Lulli

- Laureato Eccellente (AA 2013-2014)

UCLouvain Crypto Group (ICTEAM/ELEN)

- Coordinatori: Prof. FX. Standaert, Prof. O. Pereira, Prof. T. Peters
  - Gruppo fortemente internazionale
  - Svariate collaborazioni con enti e aziende del settore dell'hardware security e crittografia

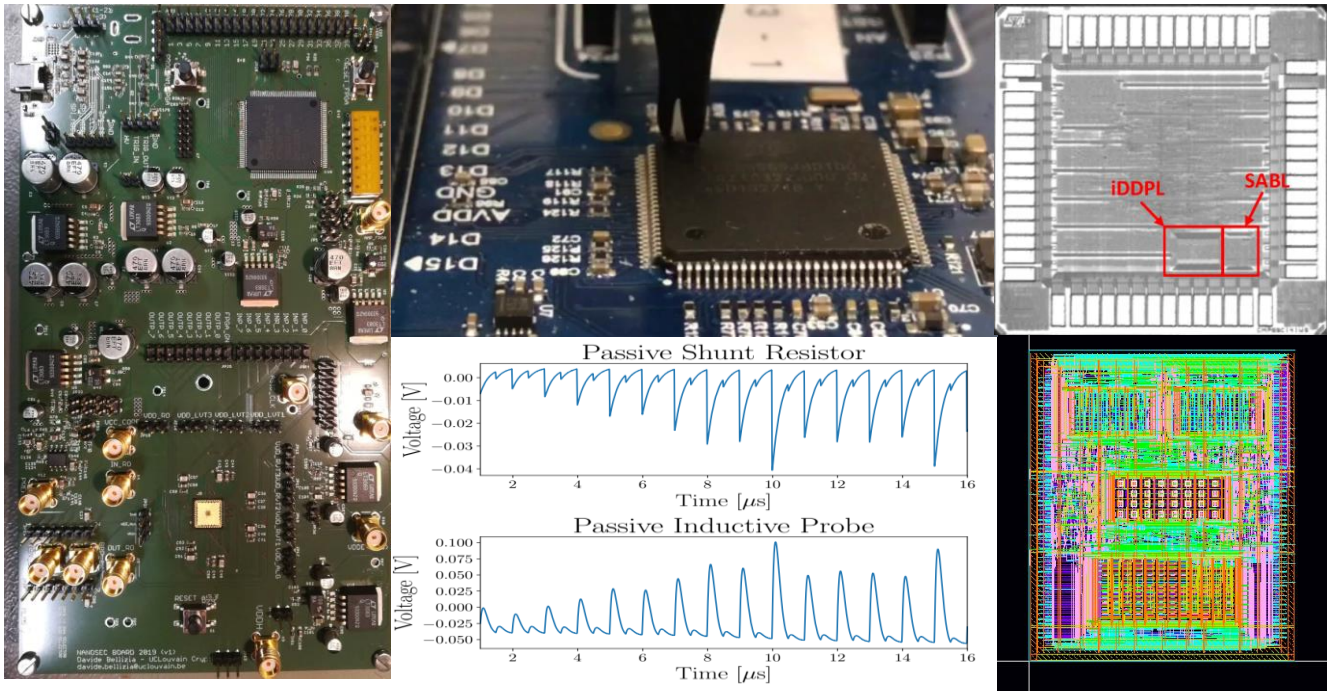
- Contributo
  - Design FPGA/ASIC di circuiti SCA-resistant
  - Design primitive RNGs/PUFs sicuri
  - Test e analisi side-channel e fault injection

UCLouvain Crypto Group (ICTEAM/ELEN)

- Progetti:
  - H2020 REASSURE
  - ARC NANOSEC
  - ERC SWORD
- Milestones:
  - Algoritmo “Spook” candidato al LWC del NIST
  - Video Tutorial e Seminario (CARDIS2018) con RISCURE+UniBri
  - 3 tapeout (UCL, UCL+BIL, UCL+Sapienza)
  - Organizzazione evento CtF a CHES2020

Pubblicazioni Recenti

- Bellizia et al., “Learning Parity with Physical Noise: Imperfections, Reductions and FPGA Prototype”, IACR TCHES 2021 (to appear).
- Bellizia et al., “Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher”, IACR ToSC 2020.
- Bellizia et al., “Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography: A Practical Guide Through the Leakage-Resistance Jungle”, IACR CRYPTO 2020.
- Bellizia et al., “SC-DDPL: A Novel Standard-Cell Based Approach for Counteracting Power Analysis Attacks in the Presence of Unbalanced Routing”, IEEE TCAS-1 2020.
- Levi et al., “Ask Less, Get More: Side-Channel Signal Hiding, Revisited”, IEEE TCAS-1 2020.
- Azouaoui et al., “A Systematic Appraisal of Side Channel Evaluation Strategies”, SSR 2020.



Email: davide.bellizia@uclouvain.be