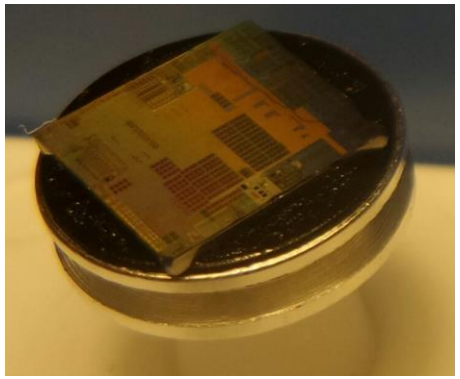
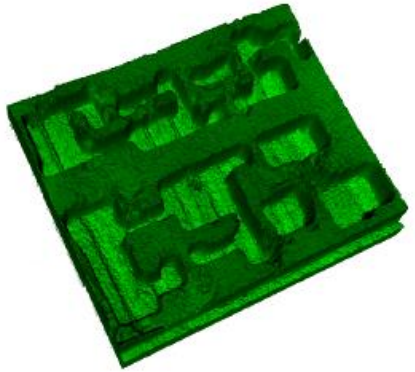
LEVERHULME TRUST

Isaac Newton Trust

UNIVERSITY OF CAMBRIDGE

Partial hardware reverse engineering for combined attacks and authenticity verification





Dr. Franck Courbon

Leverhulme Trust Early Career Fellow

Department of Computer Science and Technology,
University of Cambridge, UK

IC life cycle control and root of trust characterization

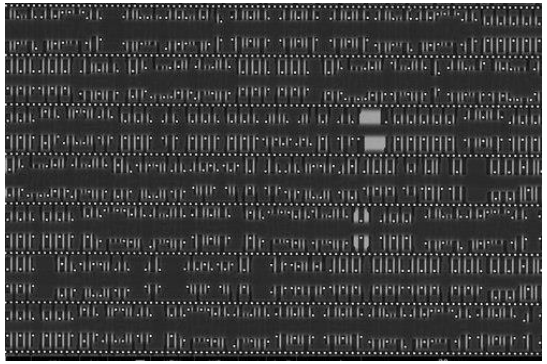
- **Current reverse engineering techniques (layer by layer, xRay, Electron source)**
  - Multiple goals (Copy, IP verification, combined attack)
  - Multiple approaches (layer, xRay, Electron source)
  - Features: cost, complexity, time, output

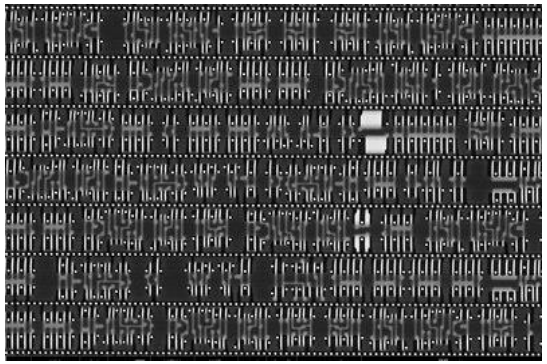
- **In-house single layer reverse engineering development (sample preparation, sample imaging, image alignment, pattern recognition, statistical analysis)**

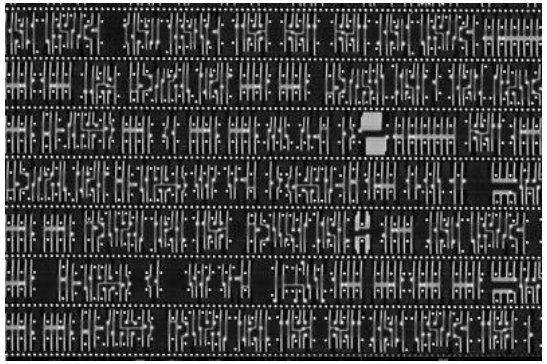
- **Our goal is not to reverse the full circuit but only to extract enough information (digital logic design, memory contents) for combined attacks or authenticity verification (fast, low-cost, scalable)**

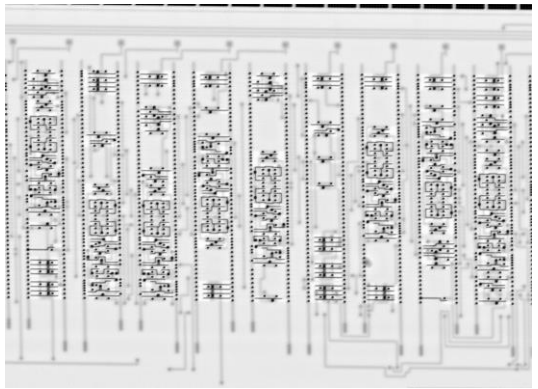
Sample preparation and imaging

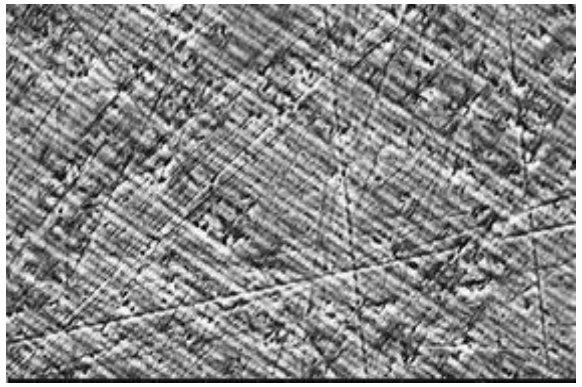
- **Low cost frontside/backside approaches**
  - Full area compliant
  - Many different imaging parameters
  - Computational power can help further now

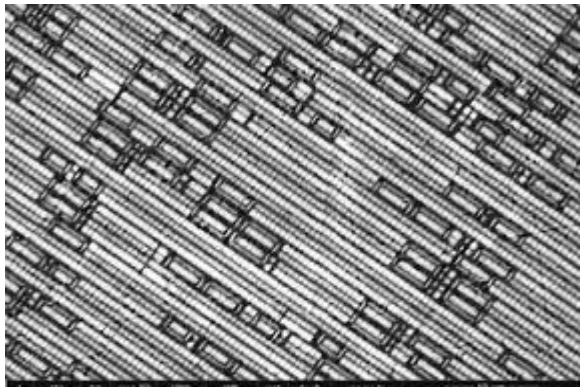


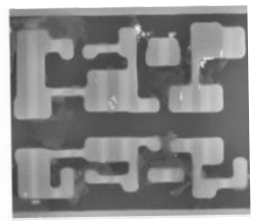




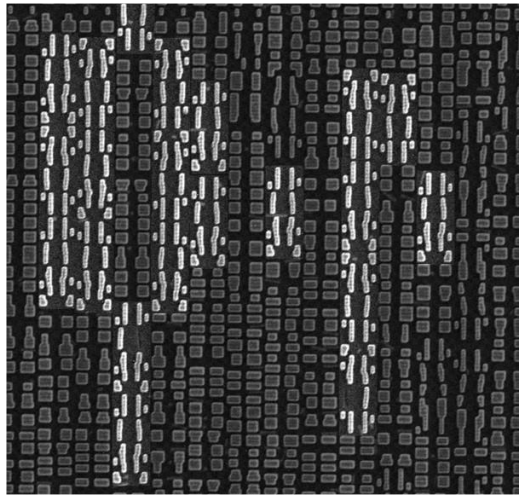




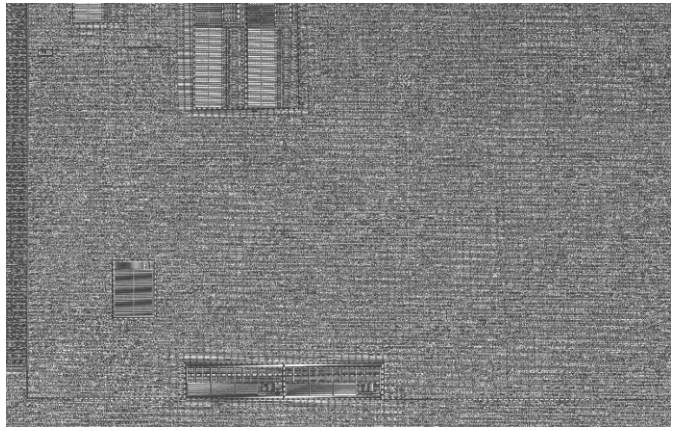




Standard Cells Statistical Analysis

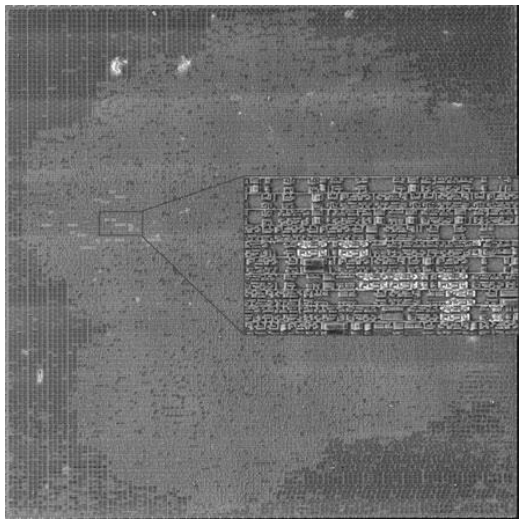


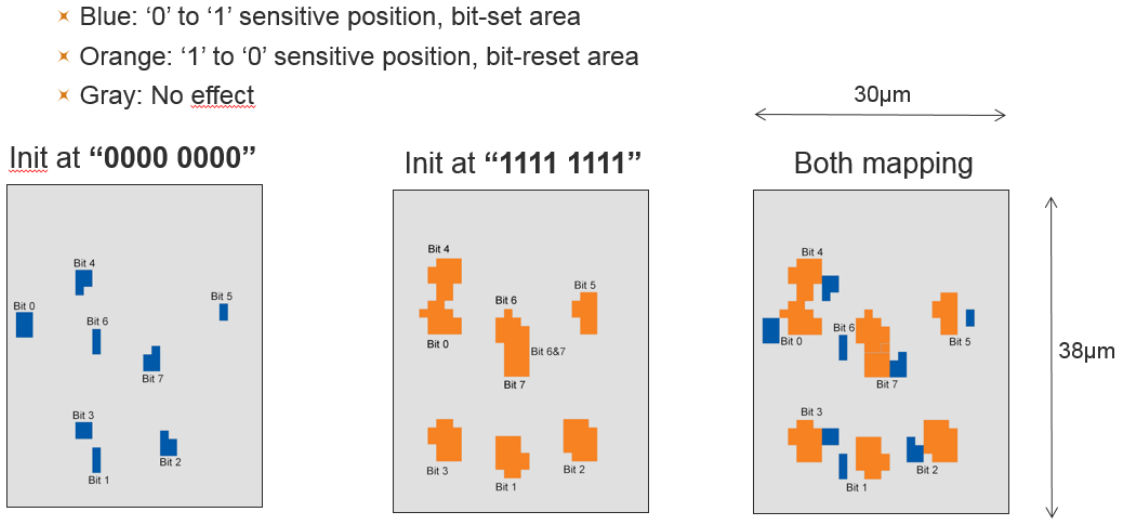
- **Error-free dictionary creation**
  - Design and sample preparation robust
- **Able to perform large partial reverse engineering campaigns**
  - Intra- and inter-chip design information extraction

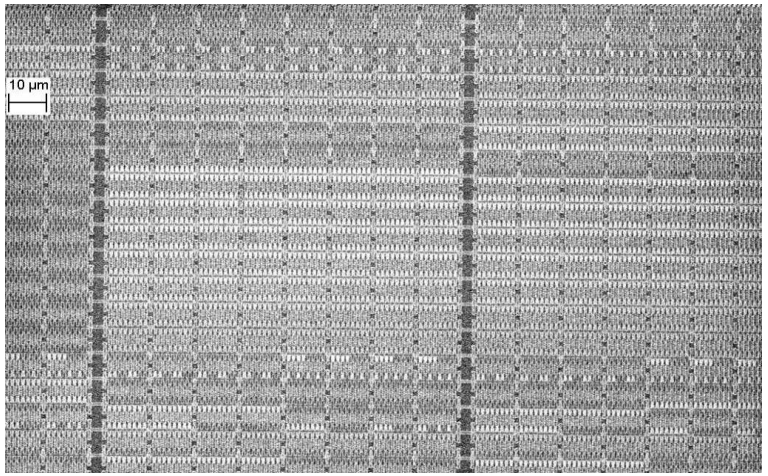


Hardware Trojan detection/laser fault attacks/memory content extraction

- **SEM-based investigations:**
  - HT detection by correlation file design output (DEF/GDSII) or golden model
  - Fine laser fault attacks
  - EEPROM/FLASH content extraction
- **On-going tool development, technique improvement and product application**







Thank you for your attention

UNIVERSITY OF CAMBRIDGE

LEVERHULME TRUST

[1] Franck Courbon, Philippe Loubet-Moundi, Jacques J. A. Fournier and Assia Tria; Adjusting Laser Injections for Fully Controlled Faults, COnstructive Side-channel Analysis and secure DEsign - 5th Intl. Workshop, **COSADE**, Paris, France, 04/2014.

[2] Franck Courbon, Philippe Loubet-Moundi, Jacques J. A. Fournier and Assia Tria; A high efficiency hardware trojan detection technique based on fast SEM imaging, Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, **DATE**, Grenoble, France, 03/2015.

[3] Franck Courbon, Sergei Skorobogatov, Christopher Woods; Reverse engineering Flash EEPROM memories using Scanning Electron Microscopy, 15th Smart Card Research and Advanced Application Conference, **CARDIS**, Cannes, France, 11/2016.

[4] Franck Courbon; In-house transistors' layer reverse engineering characterization of a 45nm SoC; 42th International Symposium for Testing and Failure Analysis, **ISTFA**, Phoenix, Arizona, USA, 10/2018.