SRAM-Based Physical Unclonable Functions on an Atmel ATmega Microcontroller

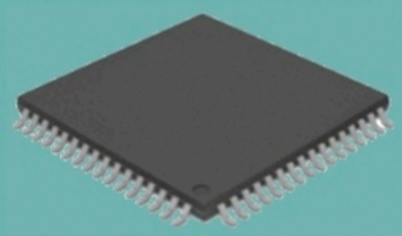
Master's thesis

Mikhail PLATONOV
Supv. Dr. Josef HLAVAC

Could we implement a PUF on a simple AVR microcontroller?

Discovering of a possibility to use initial SRAM content for device identification and key generation.

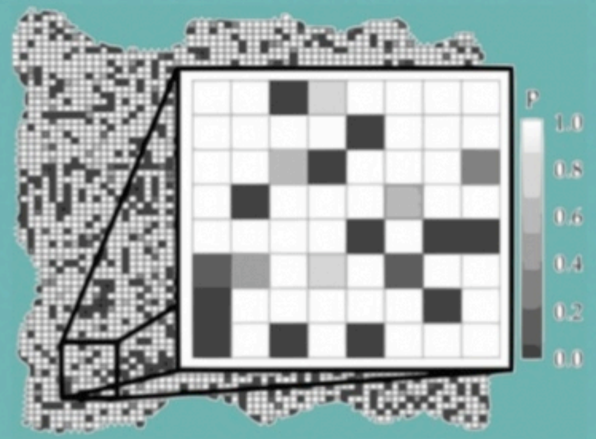
Experimental Setup



10 Atmel ATmega 1284p

3000 SRAM readouts

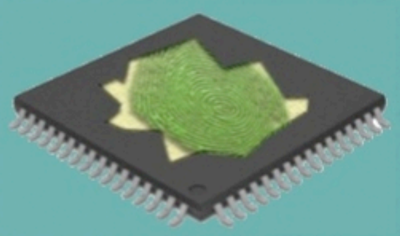
Measurements



Statistical analysis of SRAM PUF:

- Uniqueness
- Stability
- Predictibility
- Correlation
- Enviromental effects

Results



chips can be **identified** by the initial content of SRAM

after applying correction with repetition factor, SRAM can be used to generate **stable key**