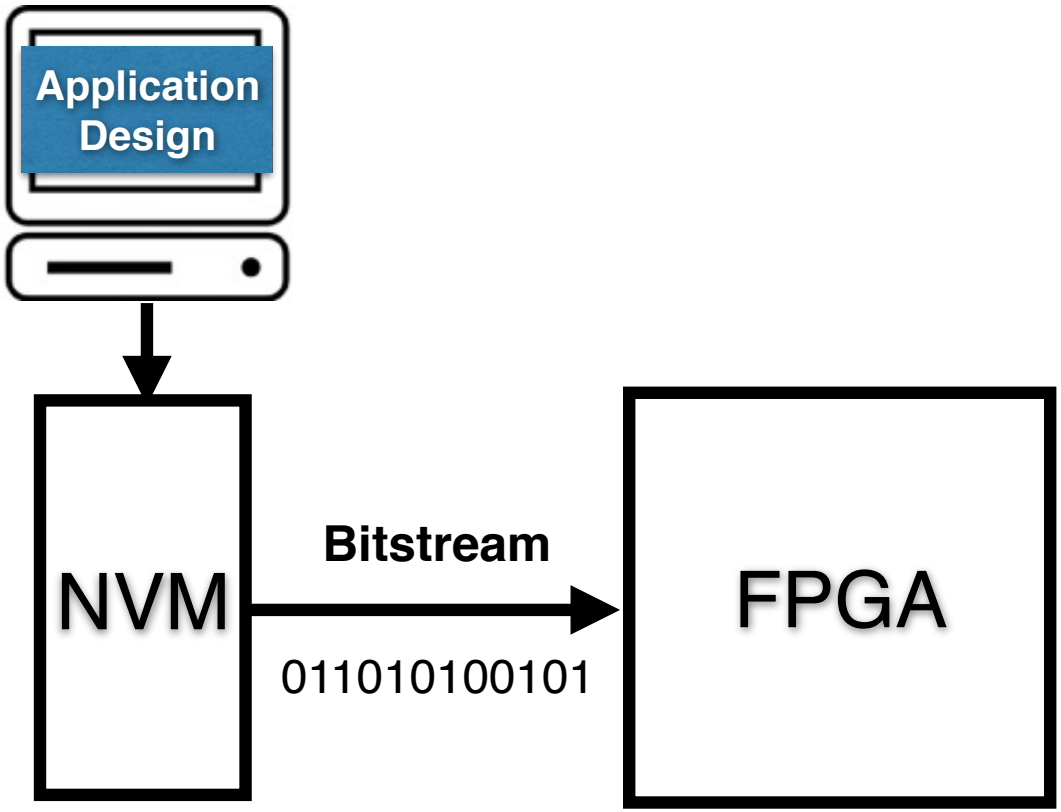
No Place to Hide:
Contactless Probing of Secret Data on FPGAs

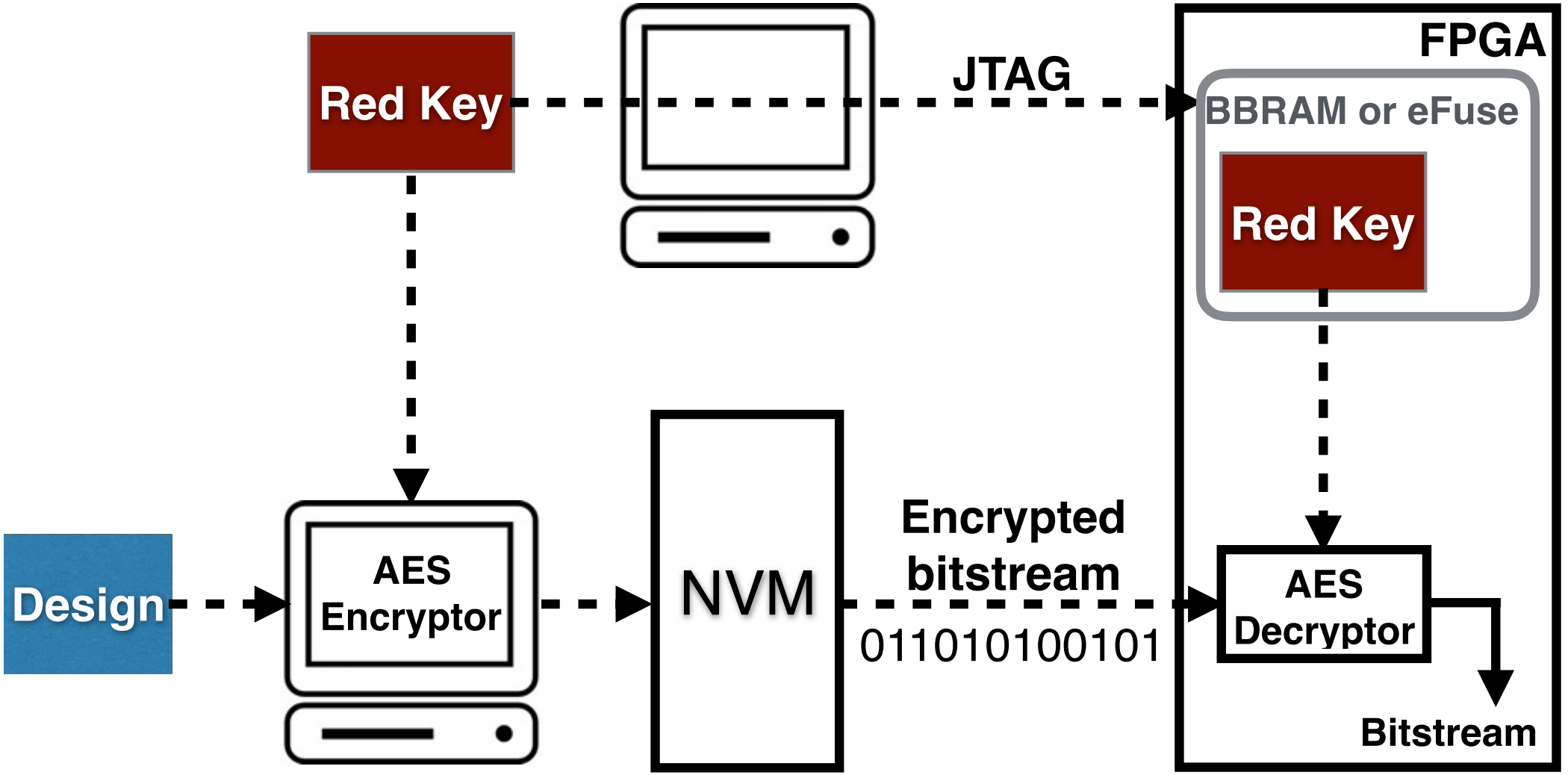
Heiko Lohrke, **Shahin Tajik**, Christian Boit, and Jean-Pierre Seifert
August 17, CHES 2016

FPGA and SoC Security

- Programming the application design once into the NVM in a safe environment
- The bitstream can be loaded in the field (**adversarial environment**)
- **Threats:** Cloning/Building, Reverse Engineering, Tampering, Spoofing



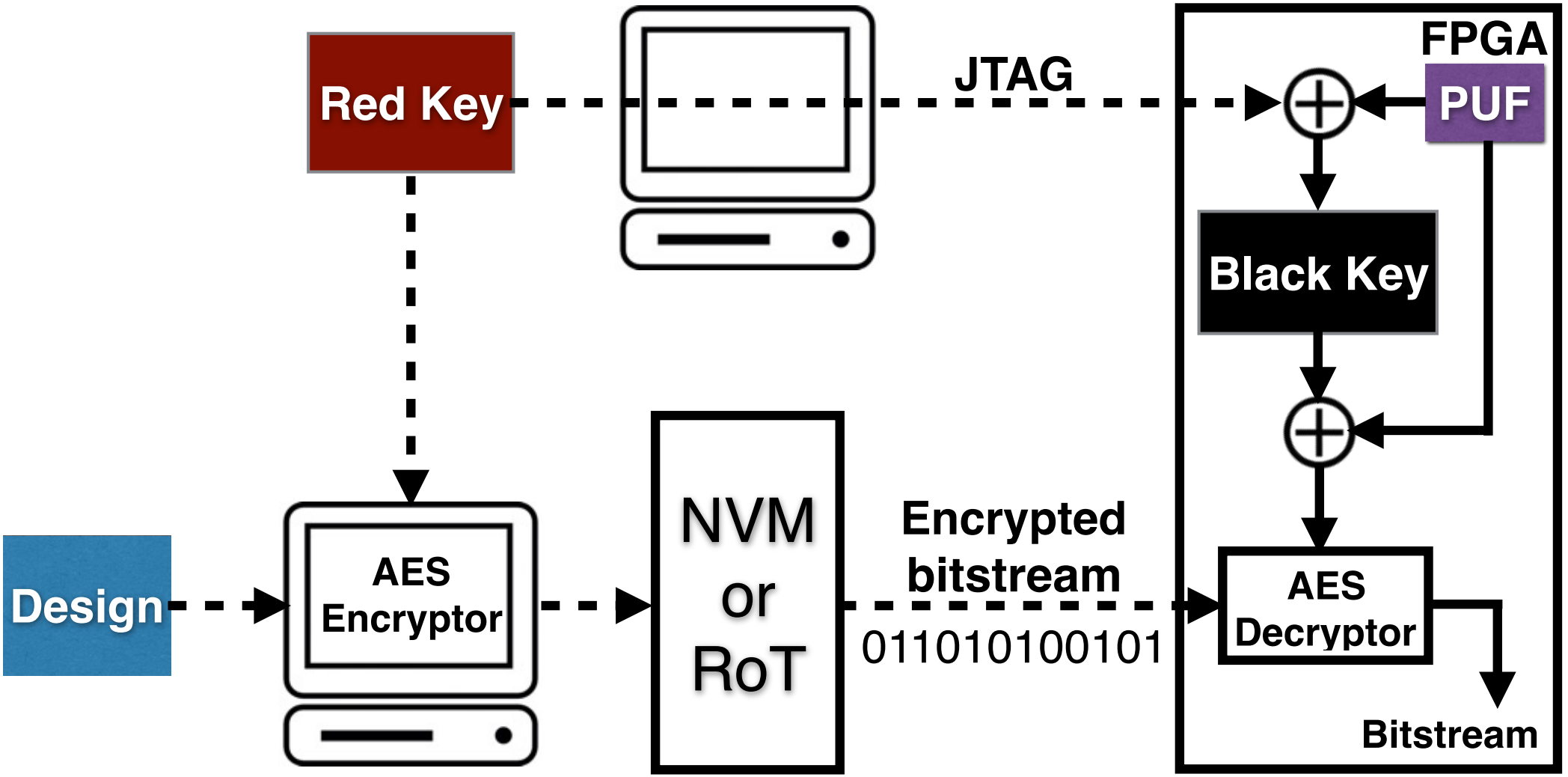
Bitstream Encryption



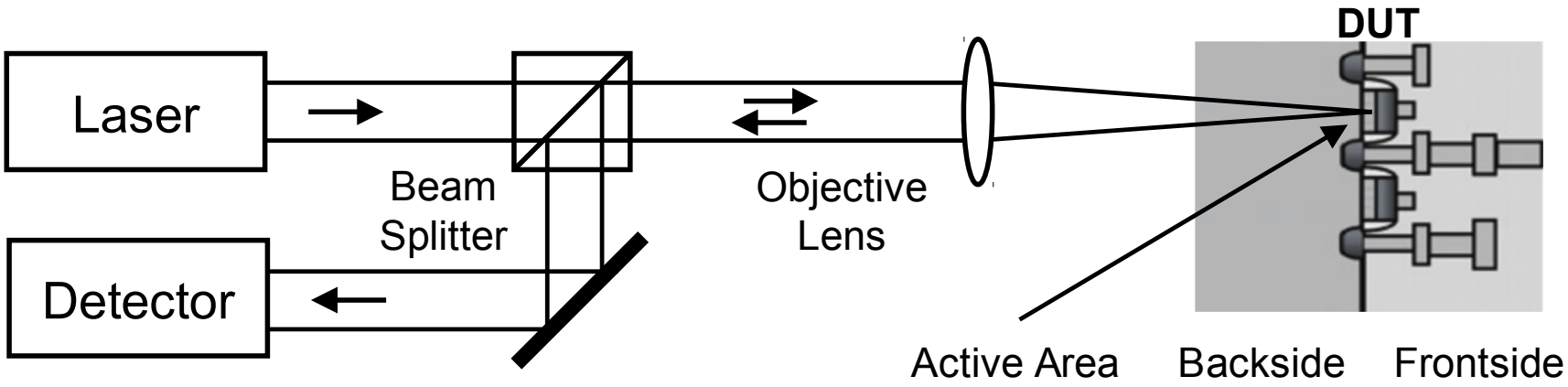
Attacks against Red Key

- **Non-invasive attacks:** Differential Power Analysis (DPA)
  - **Solutions:** Asymmetric authentication, Key rolling, DPA-resistant decryption cores (hard & soft IP cores)
- **Semi-invasive attacks:** Scanning Electron Microscopy (SEM)
  - **Solutions:** Physically Unclonable Functions (hard & soft IP cores)
- **No Countermeasures for the FPGA backside yet!**

Protecting Key from Tampering



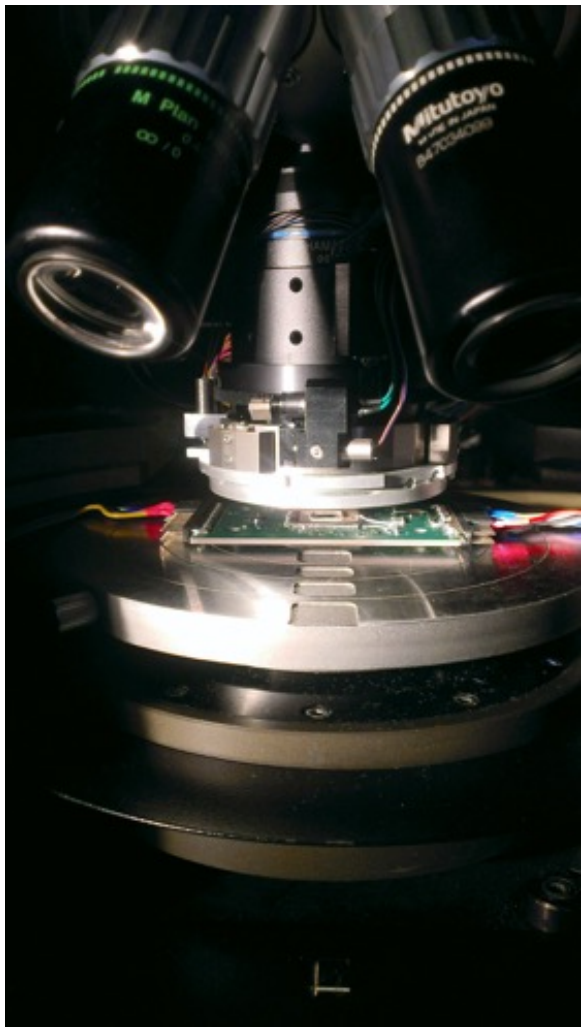
Our Proposed Attack: Optical Contactless Probing



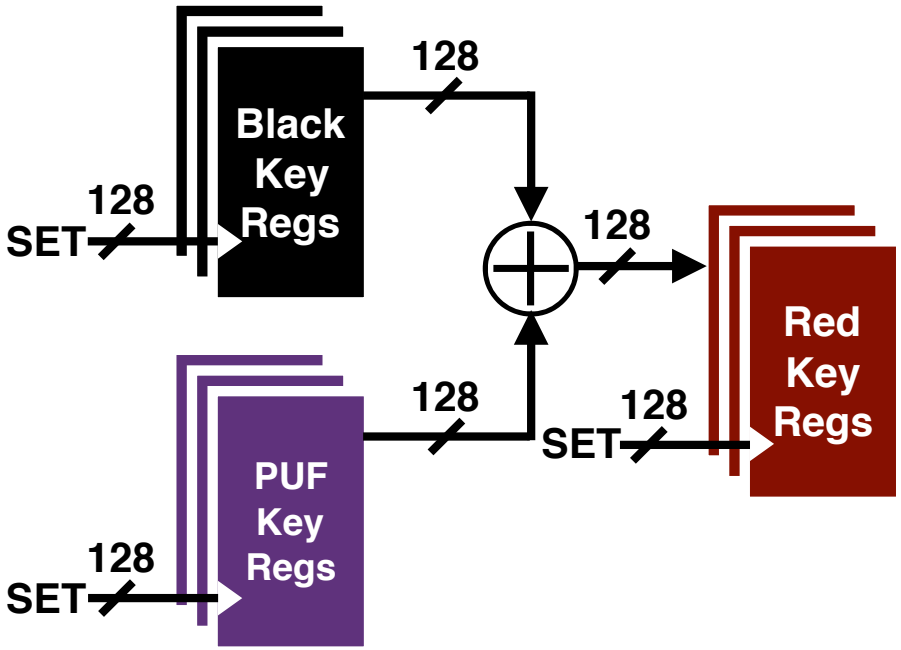
- Changes of absorption coefficient and refractive index of device in active area by electrical field and current.
- **Laser Voltage Probing (LVP):** Optical beam intensity altered by reflection >> probing of electrical signal on the node
- **Laser Voltage Imaging (LVI):** Feeding the reflected signal to a detector with a narrow band frequency filter >> detecting node switching with this frequency

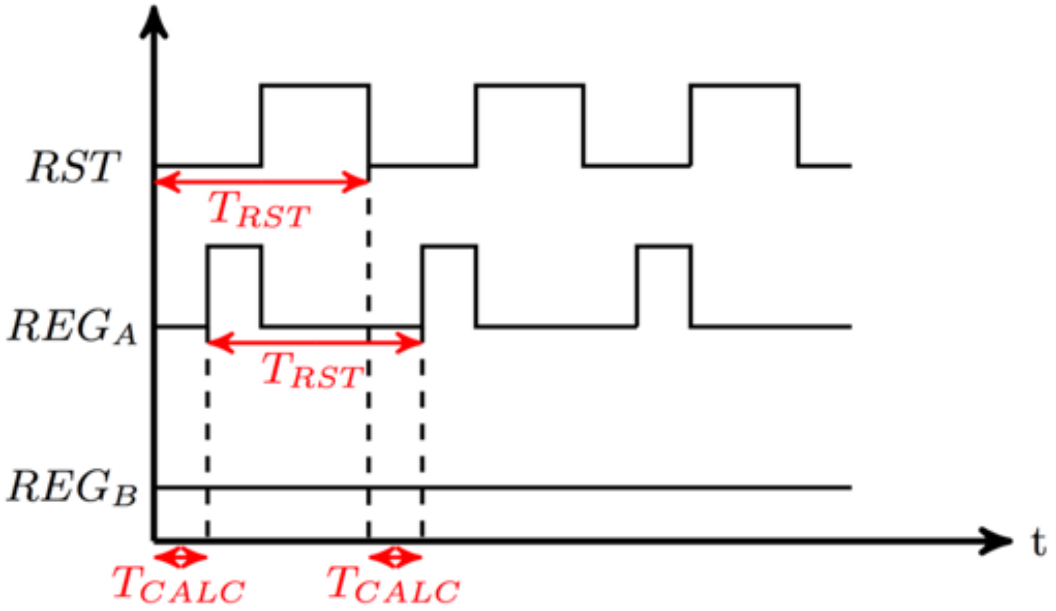
Experimental Setup

- DUT: Altera Cyclone IV FPGA (60 nm)
- Laser wavelength: 1.3 μm
- PoC Red Key calculation
- Soft PUF: Ring-oscillator PUF
- Optical Setup: HAMAMATSU PHEMOS 1000

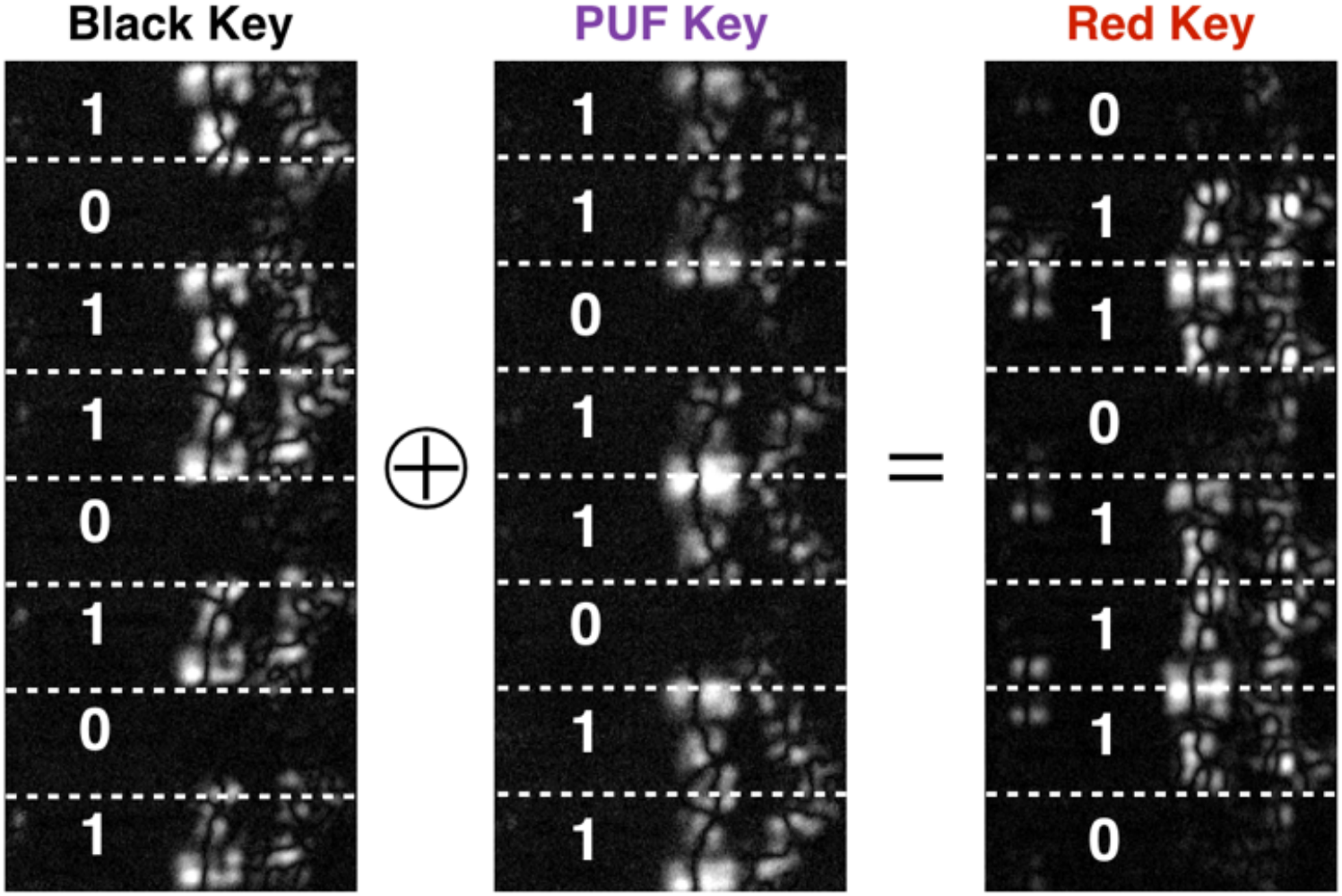


Red Key extraction with LVI (1)

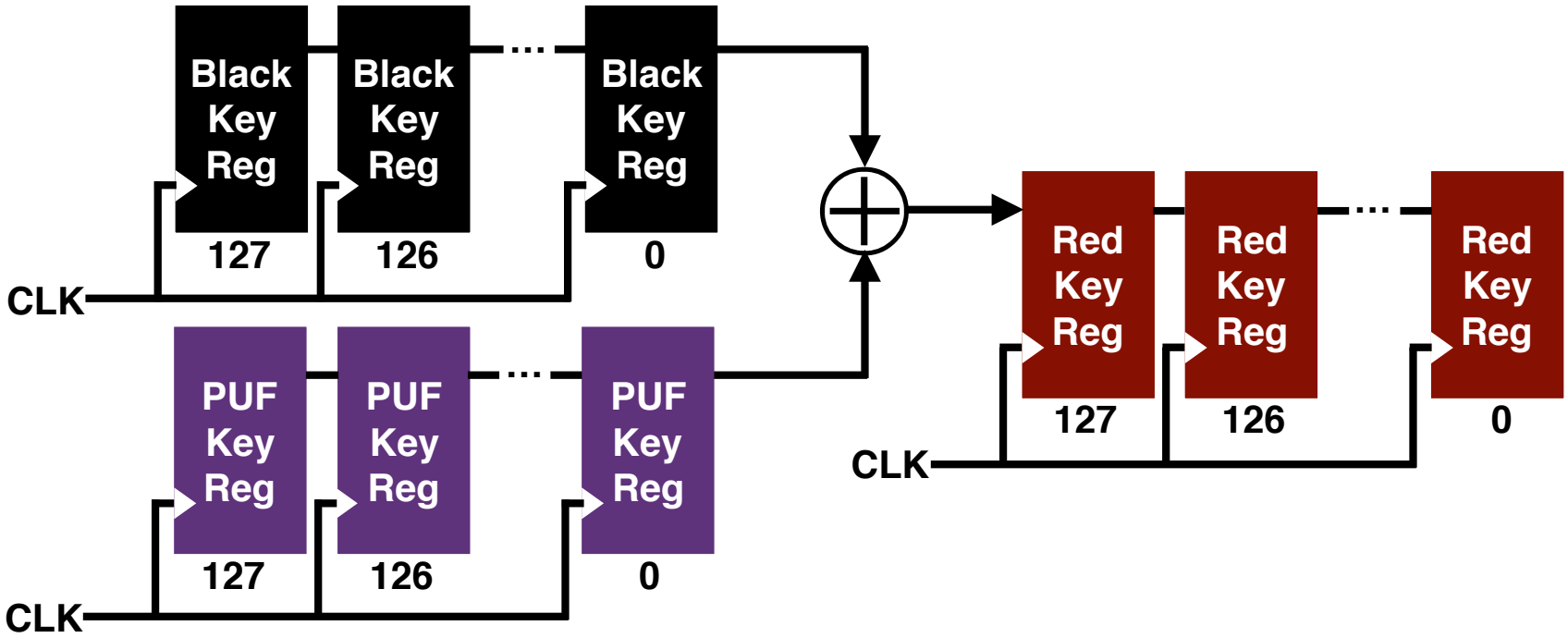




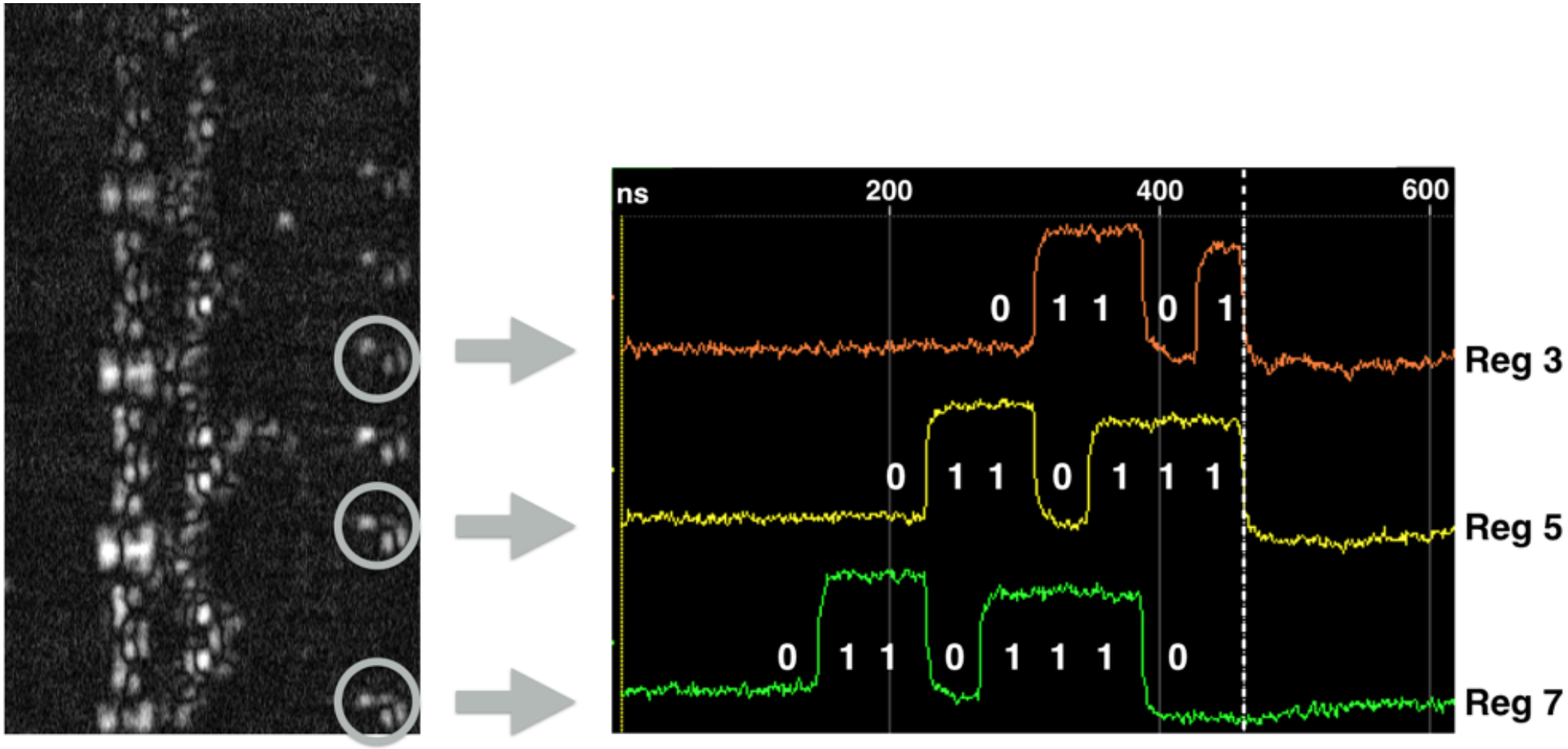
Red Key extraction with LVI (2)



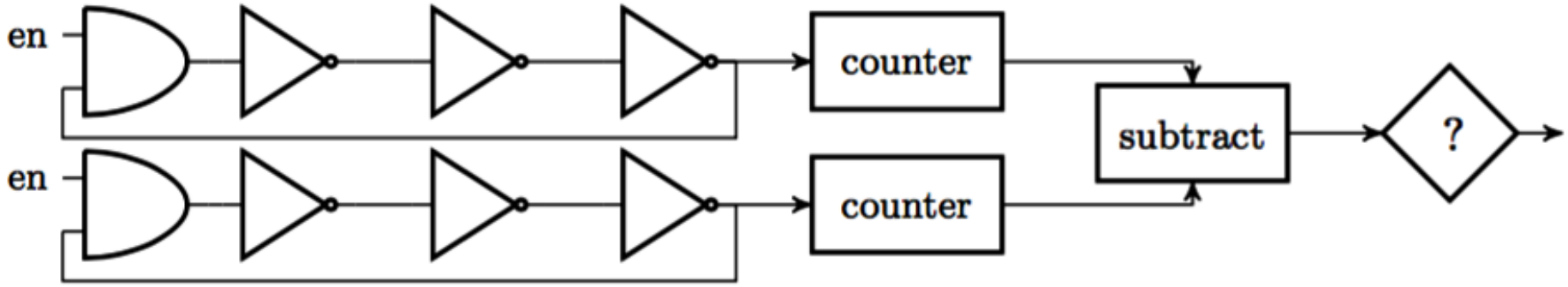
Red Key extraction with LVP (1)

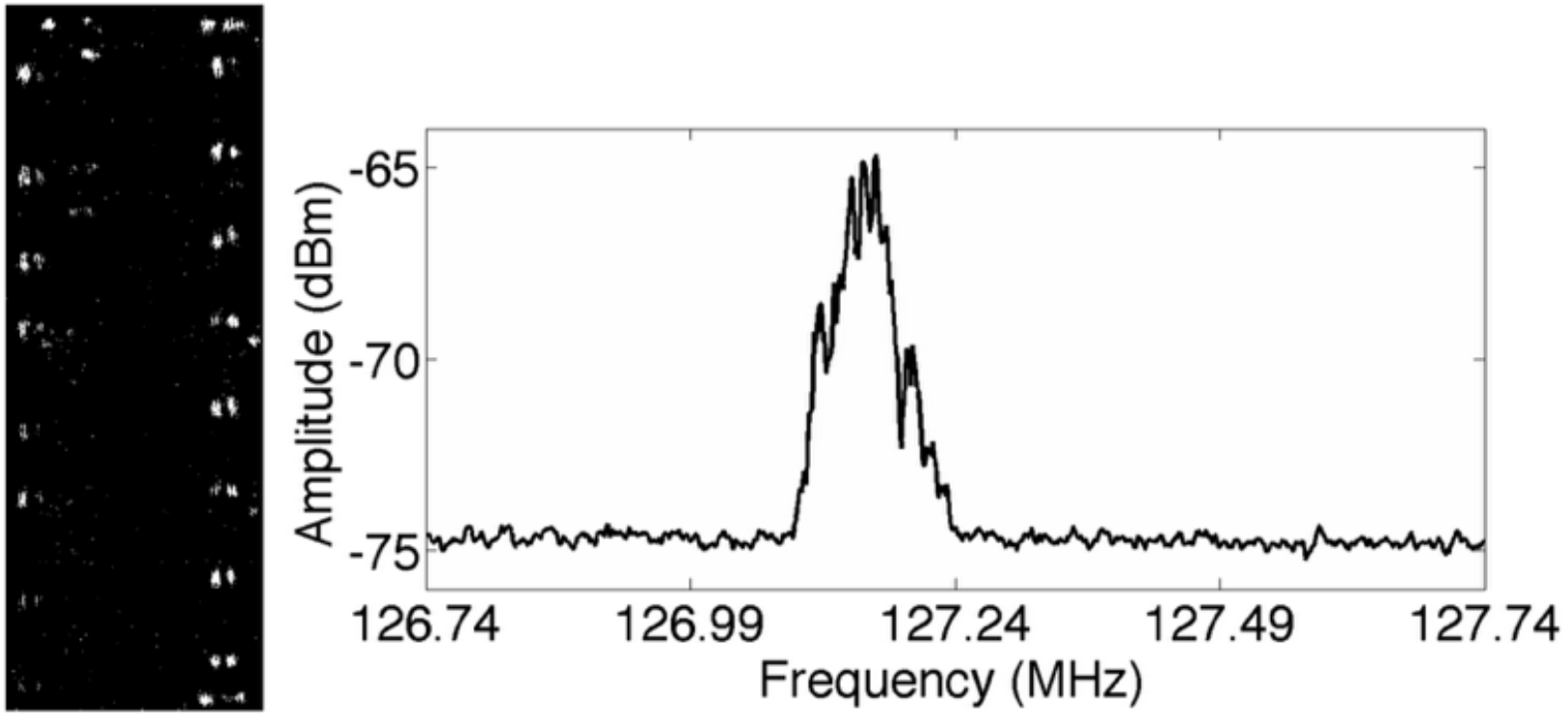


Red Key extraction with LVP (2)



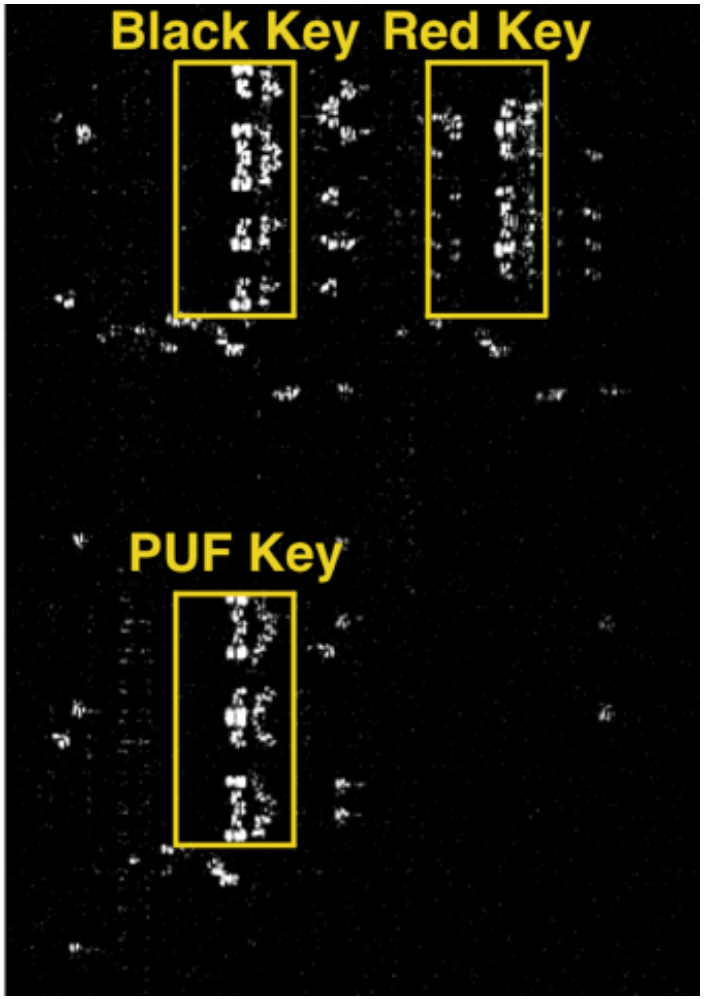
RO-PUF Characterization with LVI





Localization of Registers

- **FSBL not encrypted:** IP cores configurations can be intercepted and analyzed in a similar device
- **FSBL encrypted:** DPA against the hard decryption core to extract the FSBL
- **DPA not possible:** Gaining access to the IP cores by insider or being a potential customers.
- **Hard PUFs**: Reverse-engineering of ASIC to localize the registers



Countermeasures

- Silicon light sensors cannot be used if the laser laser beam has a longer wavelength than the silicon band gap!
- **Possible algorithmic countermeasure:** Randomization of the reset states of the registers

Conclusion

- Replacing the eFuses or BBRAMS with controlled PUFs does not raise the security level of the key storage as high as one would expected in the first place.
- Controlled PUFs can be attacked
- Much less time is required for optical contactless probing of different signals than FIB microprobing
- Future generations of FPGAs remain vulnerable to contactless probing, if the vendors do not implement proper protections or countermeasures