TECHNISCHE UNIVERSITÄT DRESDEN

Chair for Embedded Systems

Department of Computer Science, Chair for Embedded Systems

INFLUENCE OF OPERATING CONDITIONS ON RING OSCILLATOR-BASED ENTROPY SOURCES IN FPGAS

Entropy Source

Why true random numbers?

- Random numbers are essential for all kinds of cryptographic protocols

Why entropy sources on FPGA?

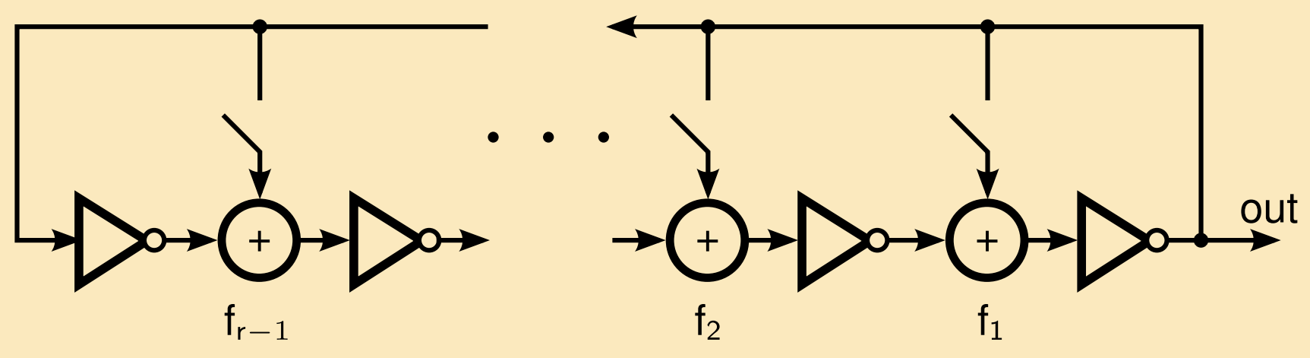
- Self containment is an important property of cryptographic systems

How to build an entropy source?

- Ring oscillators provide as entropy sources and use only digital circuitry, have a simple design and small footprint

Project goals

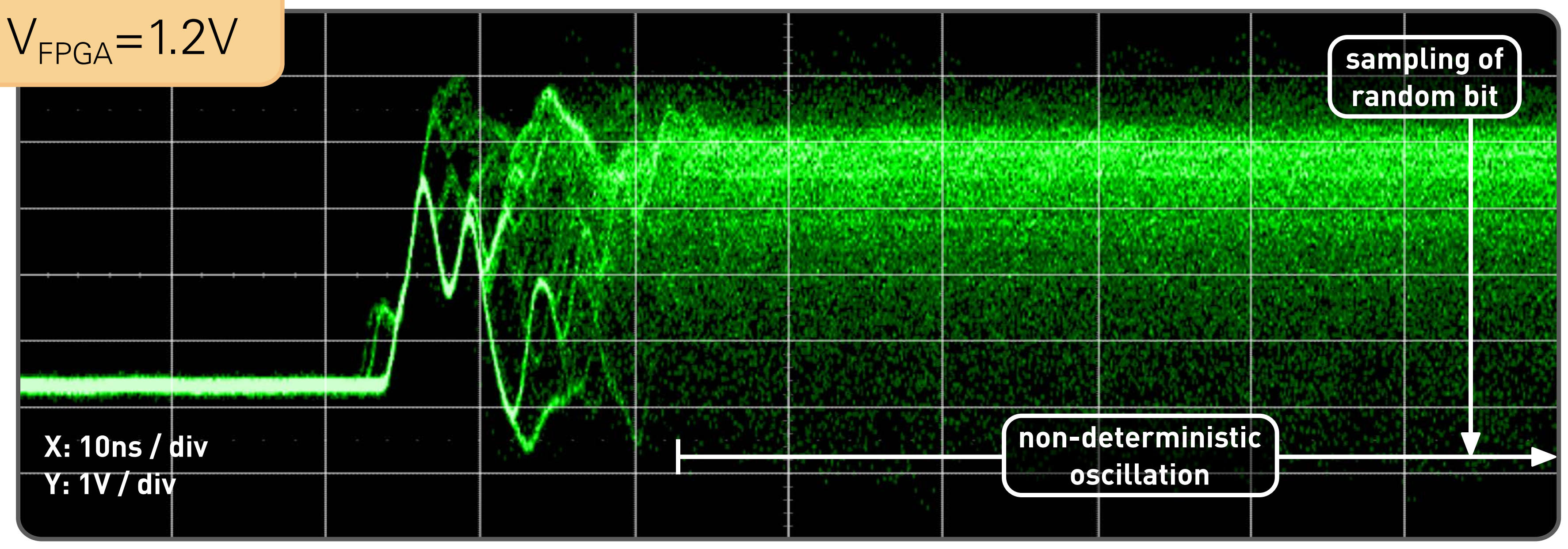
- Investigate the properties of different entropy sources built with FPGAs and possibilities to influence them
- Develop a framework to easily instantiate a random number generator that has certain security properties



Non-deterministic output

Nominal conditions

T_{FPGA}=30°C • V_{FPGA}=1.2V

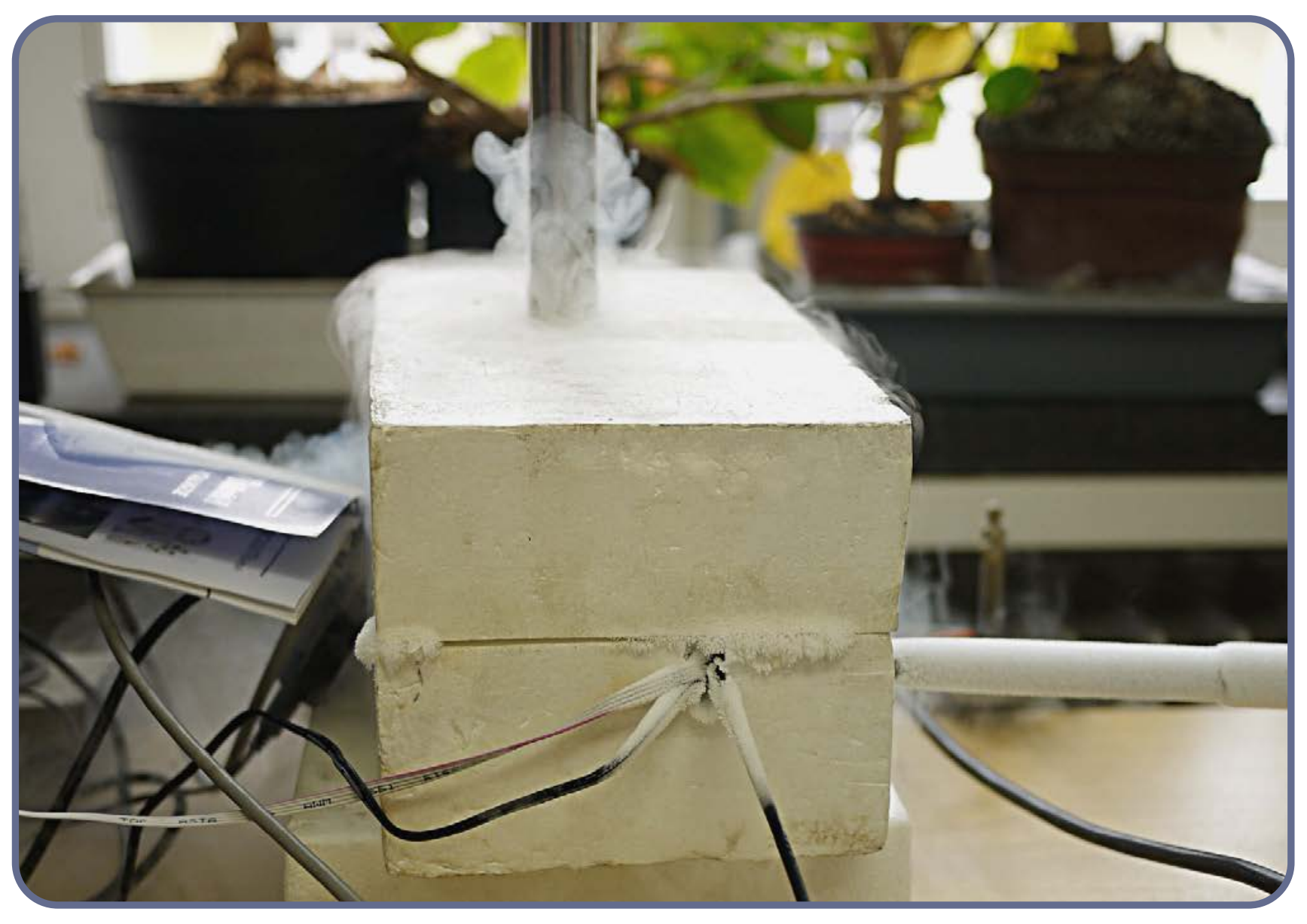


GARO on Lattice ECP3

Tamper-safety under extreme conditions

Temperature +30 ... -130°C

- Nitrogen gas of -160°C fed into insulated box
- Continuous capturing of random bits while temperature decreased by approximately 2-5K/min



FPGAs under test

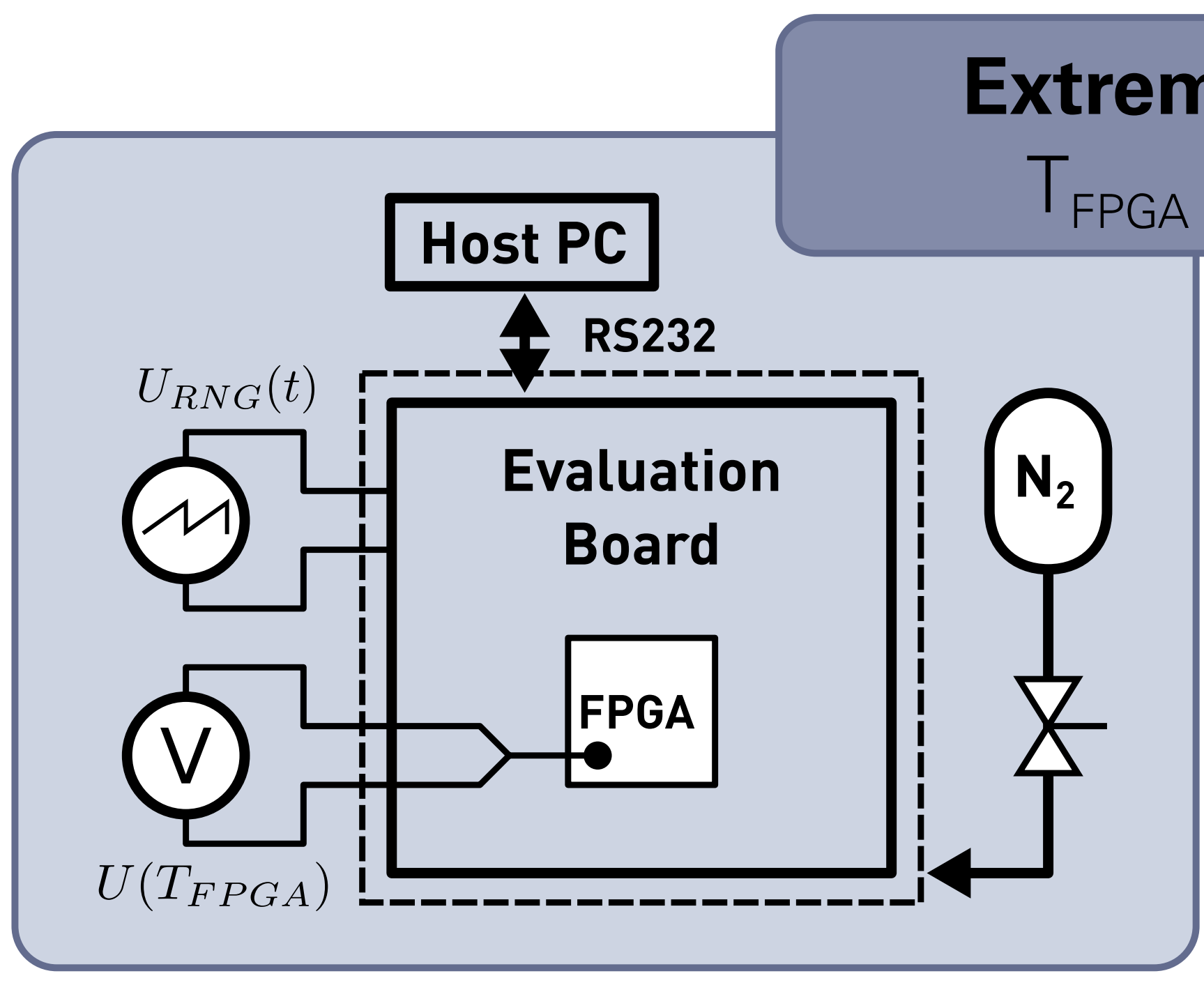
Xilinx	Spartan-6 LX45	45nm	45k LUTs
Lattice	ECP3 LFE3-35	65nm	35k LUTs

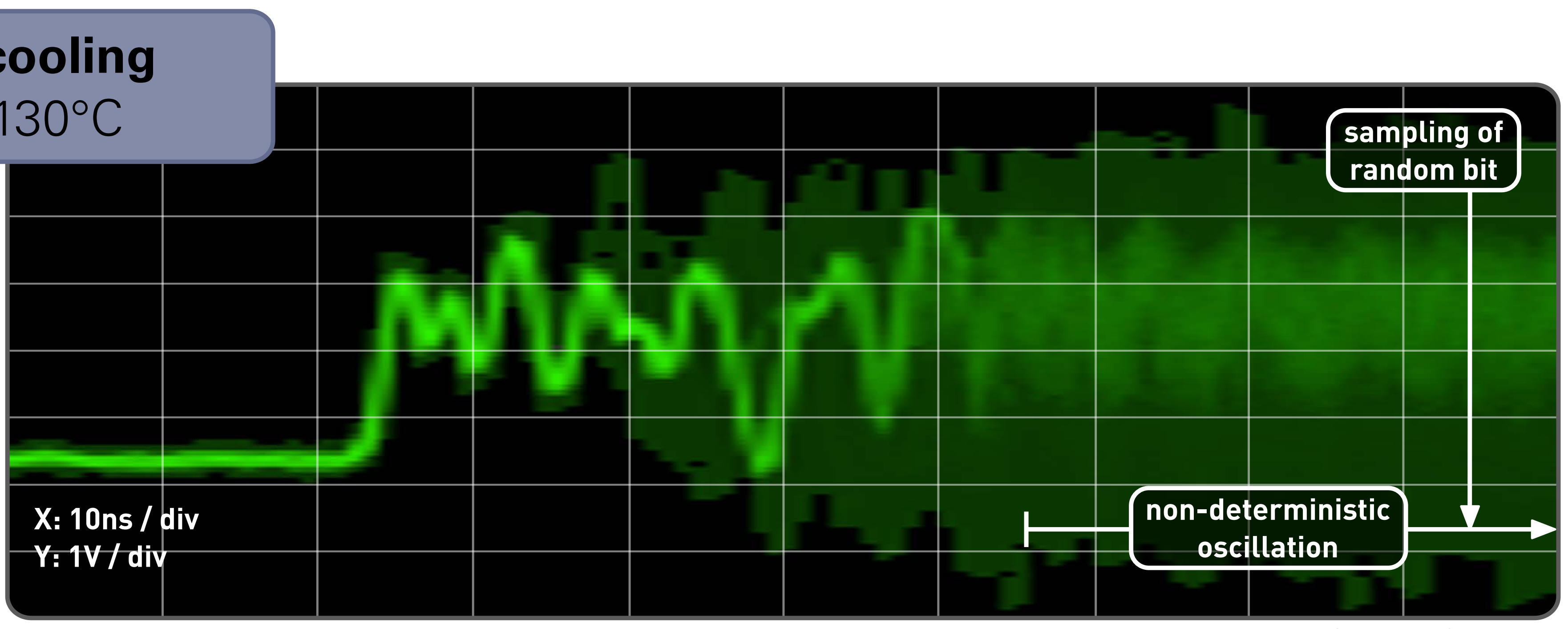
Core voltage 1.2 ... 0.9V

- On-board voltage regulator replaced by external supply input
- Random bit sequences captured at each voltage level decreasing in steps of 50mV

Extreme cooling

T_{FPGA} = -130°C

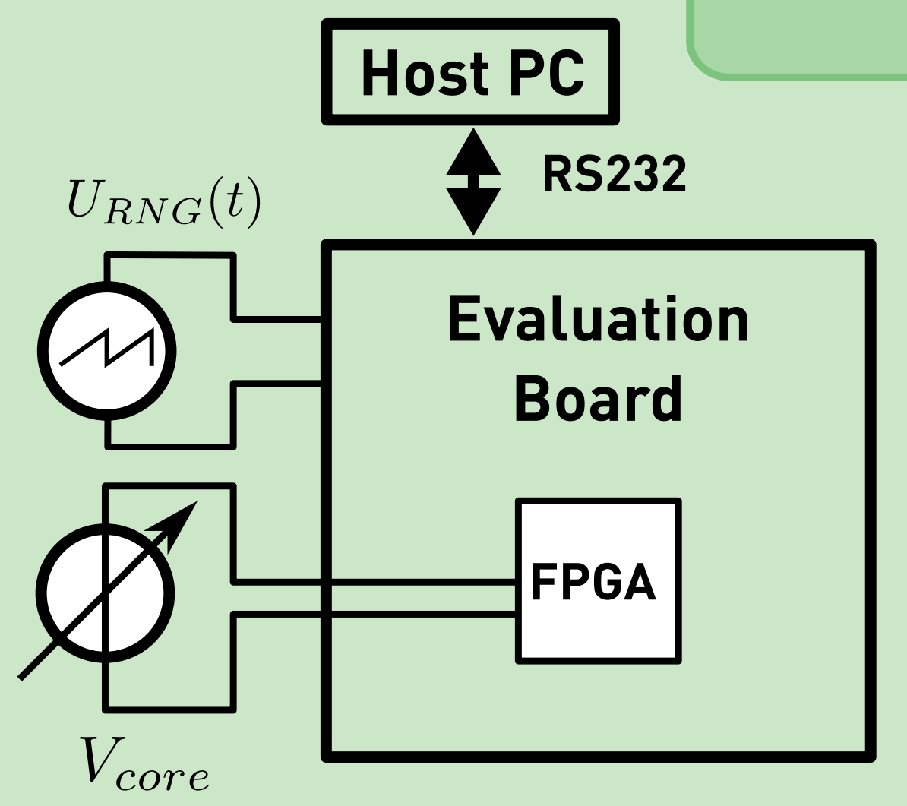


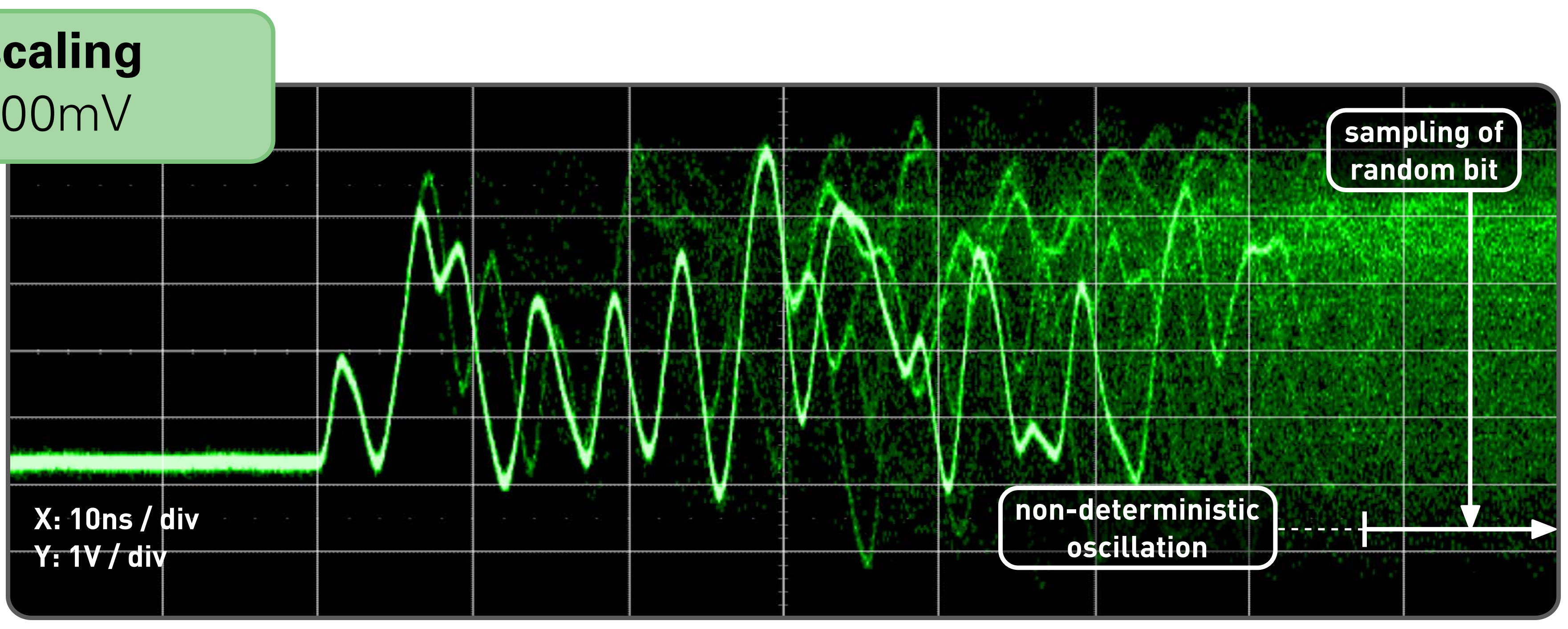


FIRO on Xilinx Spartan6

Voltage scaling

V_{FPGA} = 900mV

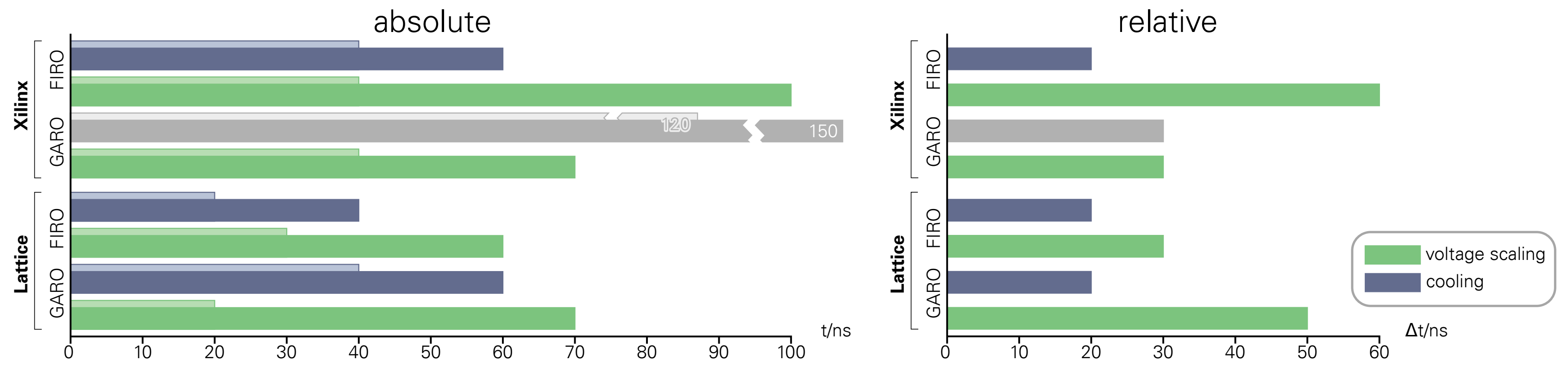




GARO on Lattice ECP3

Results and future work

Increase of acquisition-time under extreme conditions depending on architecture and type of TRNG



- **No serious degradation of randomness was seen at low temperature or low voltage regardless of observed variation in one-zero distribution.**
- Duration to pass deterministic oscillation increases under such conditions, while voltage has stronger impact than temperature
- No indication of complete failure or loss of entropy output which is further proved by statistical tests (NIST)
- Random number generators can be secured against such types of influence with attention to the sampling point
- Current research covers experiments on the influence of radiation and strong static magnetic fields

Chair for Embedded Systems
University of Technology Dresden
Chair for Embedded Systems

SIEMENS
Siemens AG
Corporate Technology

secunet
secunet Security Networks AG
Business unit High Security

Founded by German Federal Ministry of Education and Research (BMBF)

Federal Ministry of Education and Research

Christian Hochberger, Changgong Li, Michael Raitza, Markus Vogt
Chair for Embedded Systems
Technische Universität Dresden, Germany
Email: {christian.hochberger | changgong.li | michael.raitza | markus.vogt}@tu-dresden.de

www.dicecup.de