XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Webinar series:

Cryptography under the hood

Tuesday, Nov 16, 2021

15:00 CET

Advantages of FPGA -based cryptography

Speaker

Kimmo Järvinen

CTO & Co-founder, Xiphera

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Advantages of FPGA-based cryptography

Kimmo Järvinen

CTO, Co-founder, Xiphera Ltd.

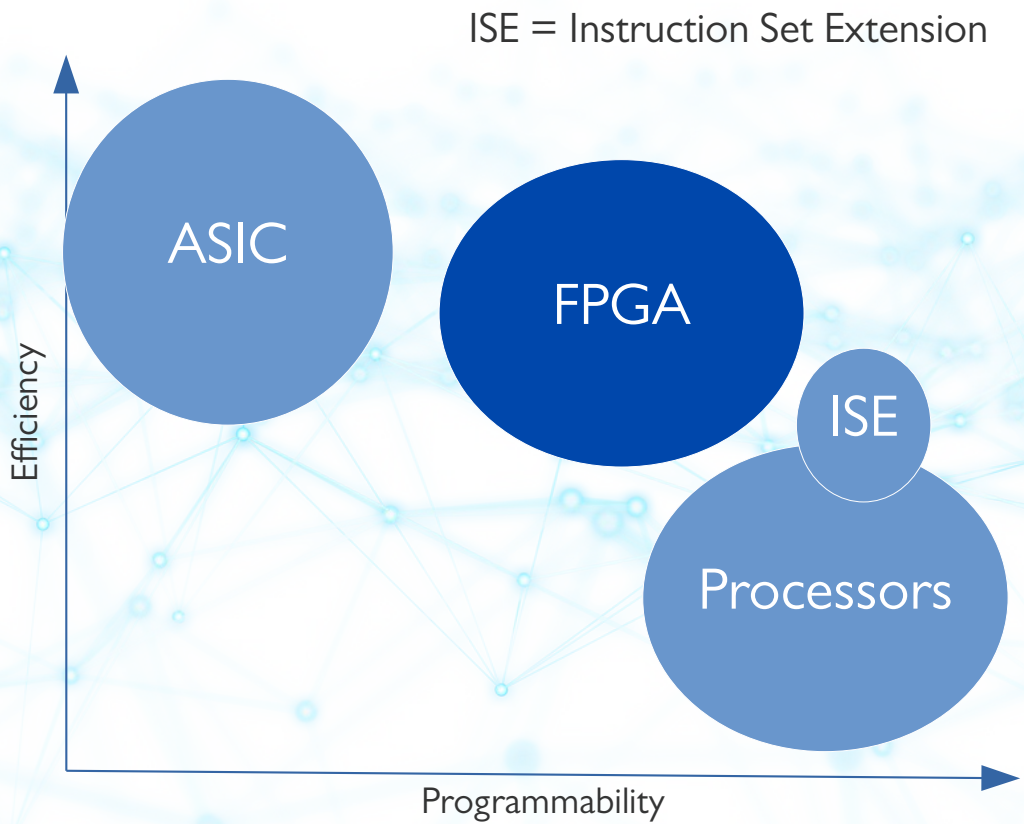
Nov. 16, 2021

Agenda

- Why is HW faster than SW?
- Why is hardware (HW) more secure than software (SW)?
- Benefits of Field Programmable Gate Arrays (FPGAs)

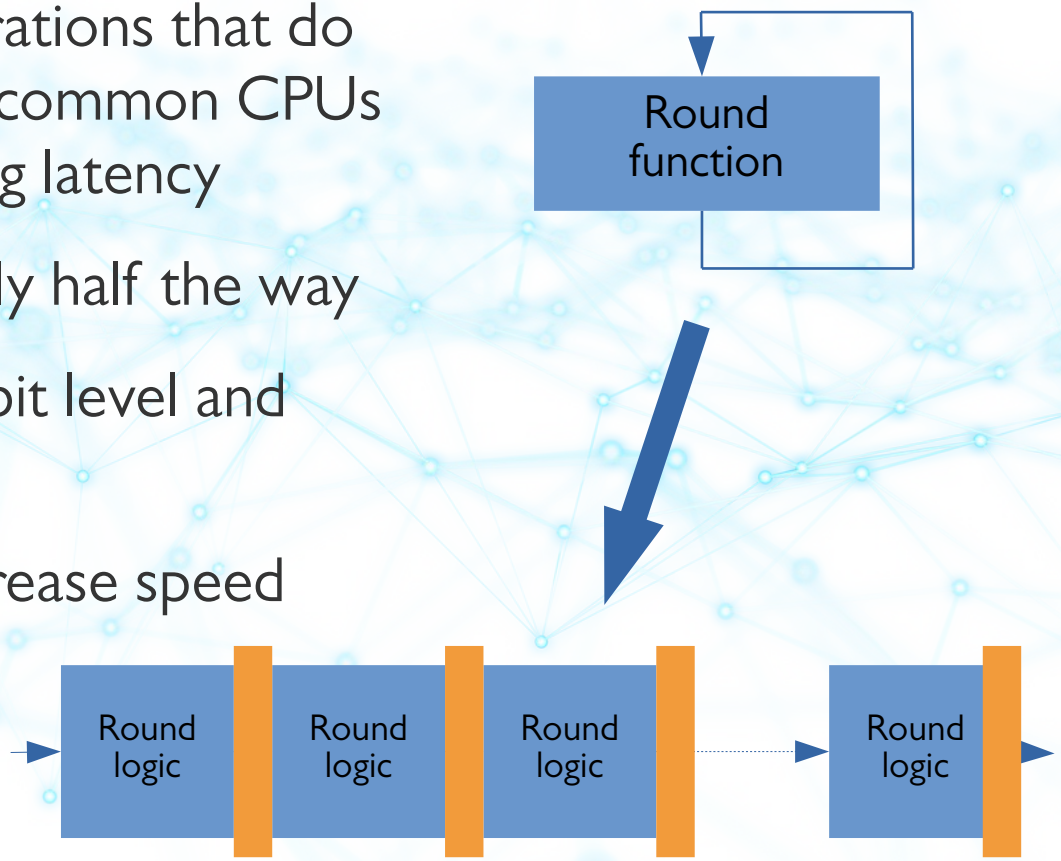
Processors, ASICs, FPGAs, …

- **Processor:** An Integrated Circuit (IC) that executes programs consisting of instructions supported by the processor's Instruction Set Architecture (ISA)
- **Application Specific Integrated Circuit (ASIC):** An IC designed for a specific application
- **Field Programmable Gate Array (FPGA):** An IC designed to be programmable on the logic level



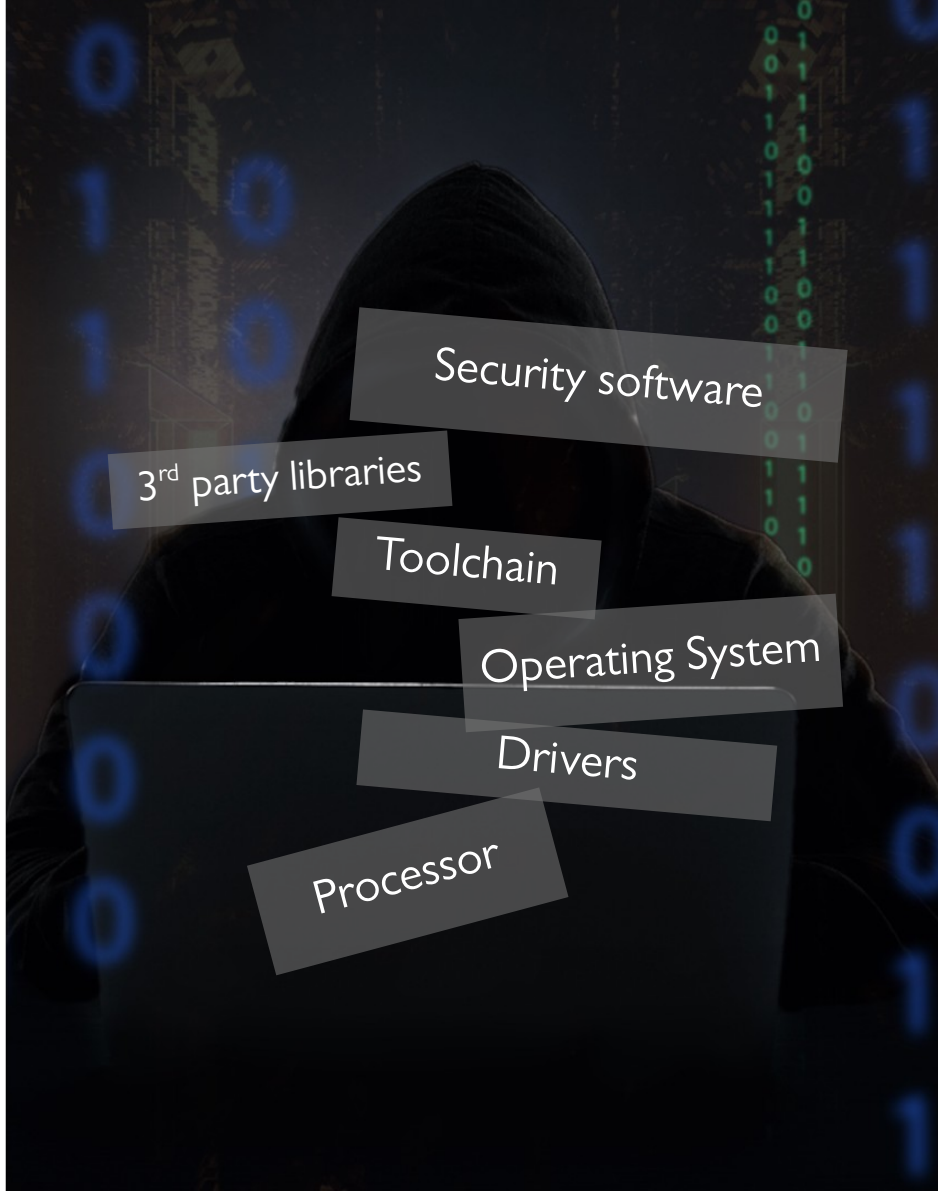
Fast Cryptography with HW

- Cryptography often uses operations that do not map well into the ISAs of common CPUs → Multiple instructions → Long latency
- ISE (e.g. AES-NI) helps but only half the way
- Hardware (incl. FPGA) allow bit level and clock cycle level optimisations
- Unrolling and pipelining to increase speed



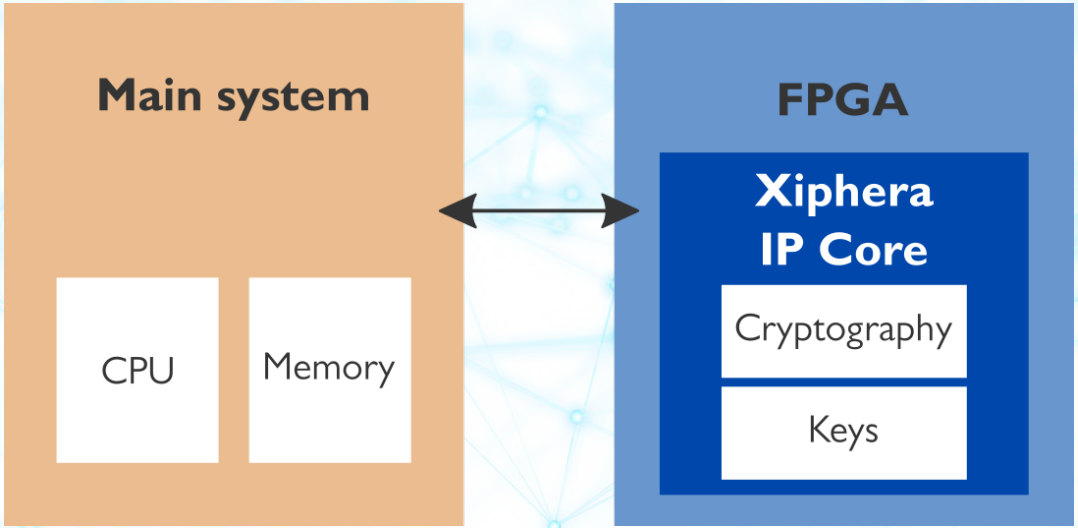
Deep Software Stack

- In SW-only systems cryptography and keys are “just” regular programs and data
  - Keys are in the main memory when in use, stored in the hard drive, etc.
- Bugs and features in the deep SW stack can compromise security



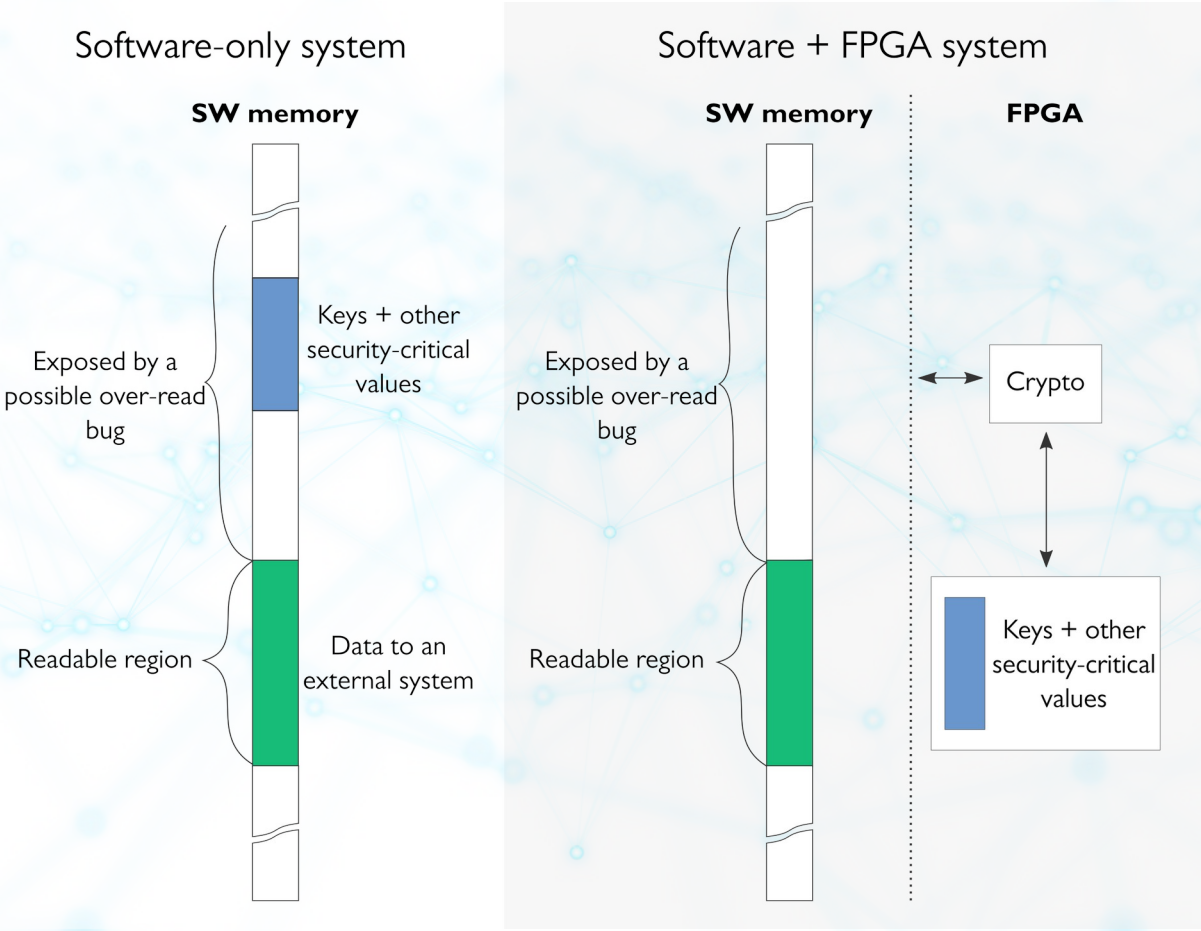
Isolation of Cryptography

- HW based cryptosystems can isolate cryptographic computations and keys
  - Even if the SW side is compromised, keys remain protected



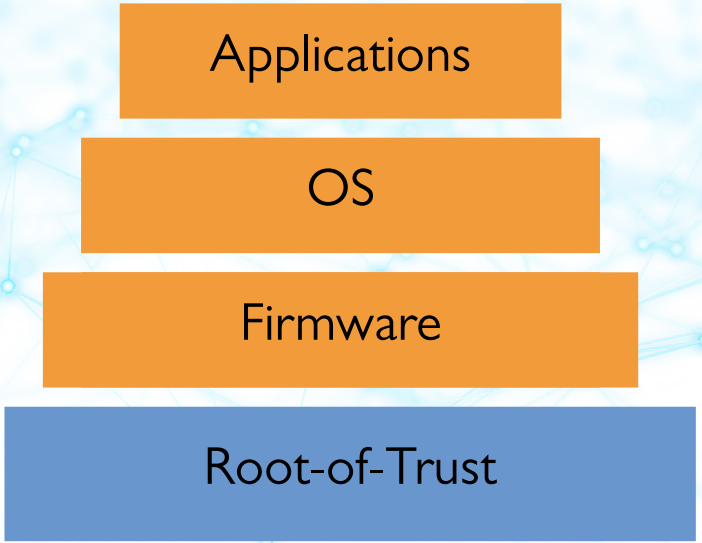
IP Core = Intellectual Property Core

Example: Heartbleed



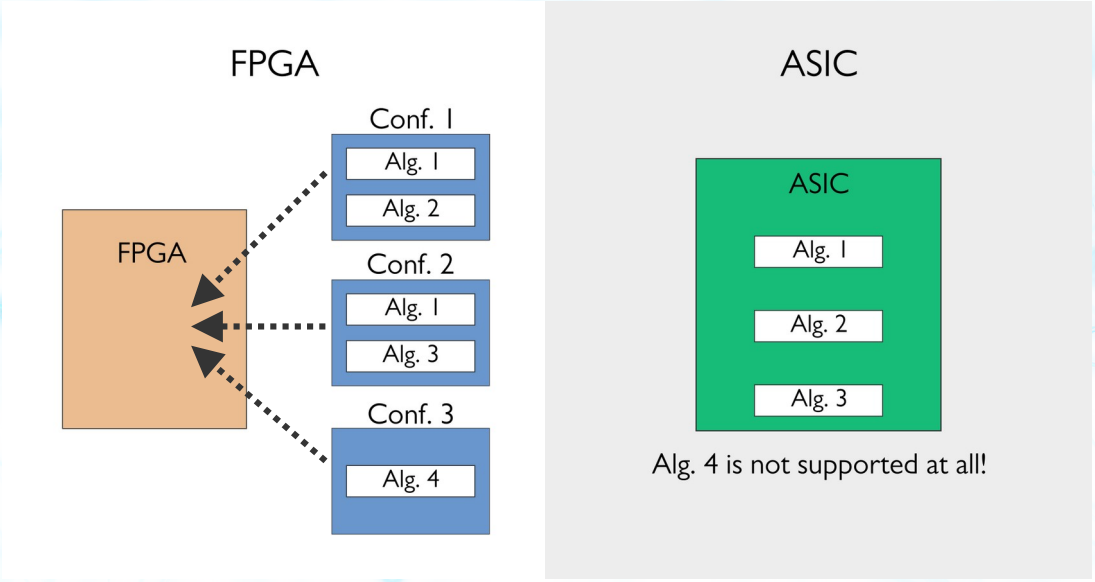
Hardware Root-of-Trust

- Isolated cryptography and keys is only half of the story
- If compromised SW can call HW cryptography, then system level security is still likely to fail
- Trust to the entire system can be built upon a trusted HW component, the Root-of-Trust



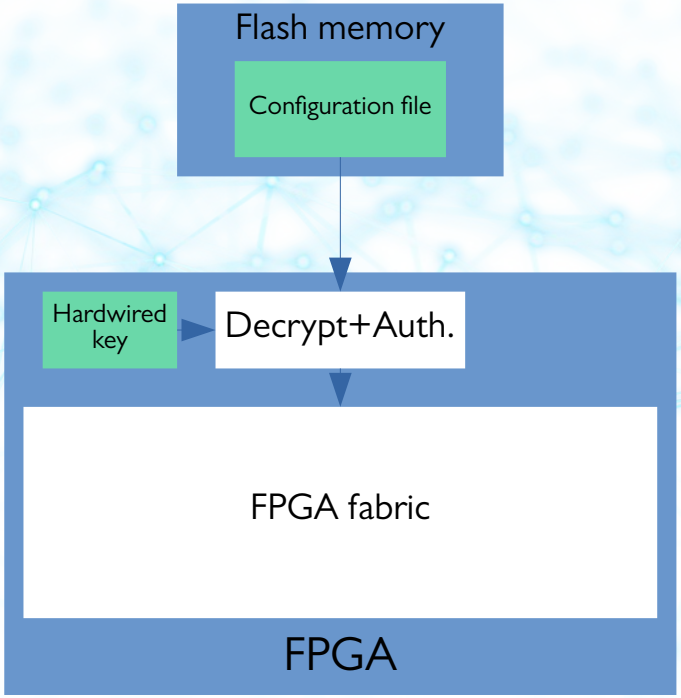
Crypto Agility

- Ability to add, replace or remove algorithms
  - Broken algorithms
  - New algorithms
- Very important currently
  - Post Quantum Cryptography (PQC) algorithms are coming but are not standardized yet



FPGA Device Security

- Integrity of the FPGA configuration is at least as important as the SW integrity!
- If secrets are embedded into the configuration, then it must also remain confidential
- Modern FPGAs support encrypted and authenticated configuration



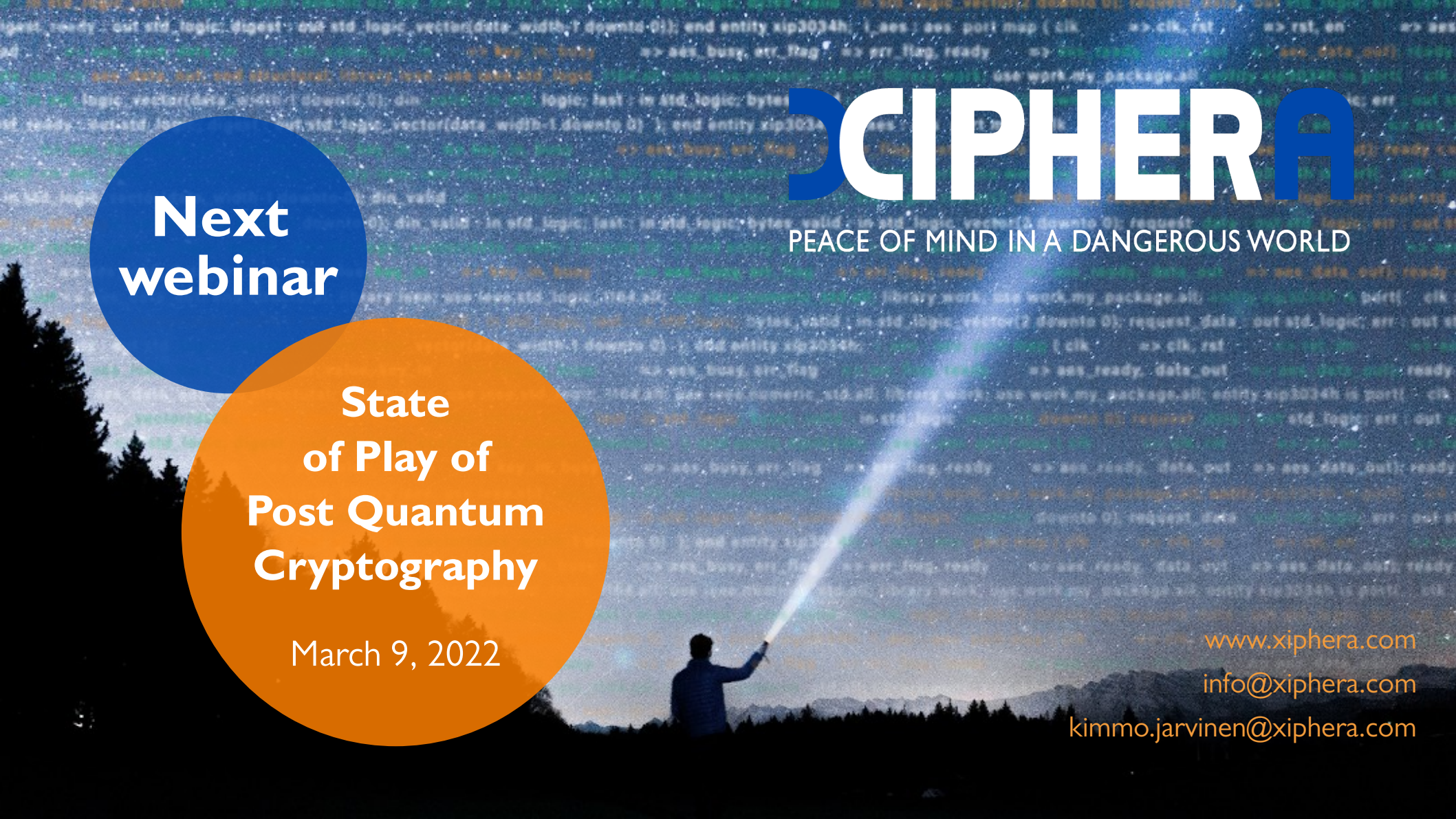
Comparison

	Speed	Agility	Energy	Isolation	Integrity
SW-only	•	•••••	•	•	•
SW + ISE	•••	•••••	••	•	•
SW + TEE	••	••••	•	•••	•••
ASIC: TPM	•	•	••••	••••	•••••
ASIC: Accelerator	•••••	•	•••••	•••••	•••••
FPGA	••••	••••	•••	•••••	•••••

When to Use FPGA Cryptography?

- Fast encryption speeds (>10Gbps)
- Energy/performance budget is too tight for SW
- High security requirements
  - The highest security certifications typically require isolated cryptography
- Long product life-time
- Crypto agility (+ any on the left) needed
- Retro-fitting security to FPGA-based products on the field (“brownfield”)
- FPGAs are the best option more often than generally thought...


XIPHERA
Thank you!
www.xiphera.com
info@xiphera.com
kimmo.jarvinen@xiphera.com


XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD
Next webinar
State of Play of Post Quantum Cryptography
March 9, 2022
www.xiphera.com
info@xiphera.com
kimmo.jarvinen@xiphera.com