swiss scientific initiative in health / security / environment systems

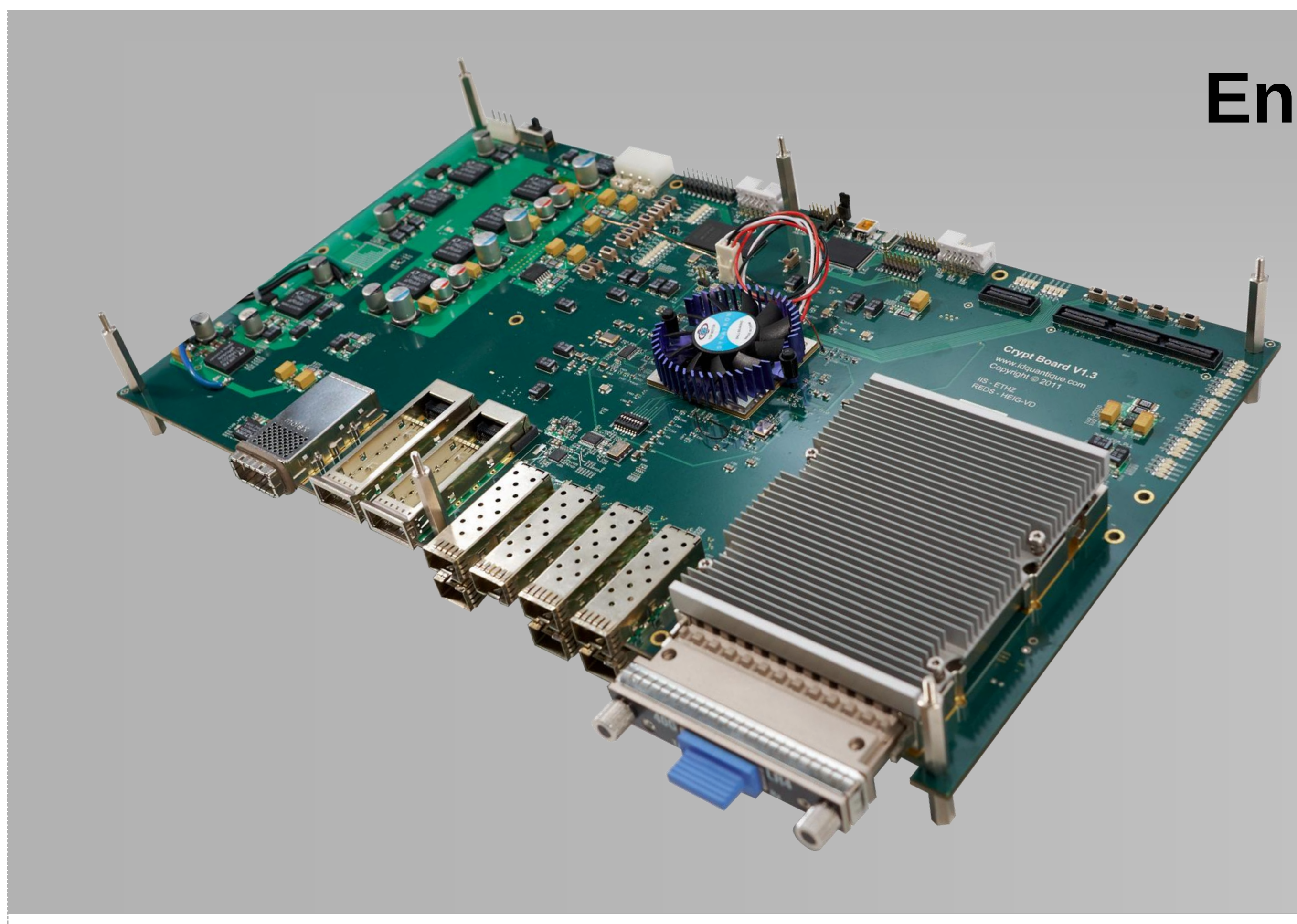
QCrypt RTD 2010

100Giga Fast Encryption Engine

O. Auberson[1], G. Curchod[1], Y. Graf[1], E. Messerli[1], L. Monat[2]

[1]HES-SO Yverdon, [2]idQuantique SA

Encryption Engine Prototype



We develop a next generation encryption device that can be seamlessly embedded in existing network infrastructures to provide quantum enhanced security

- High-speed serial links @ 10Giga managed in FPGA
- 10 Ethernet channels @ 10Giga
- 100 Gbps AES encryption engine
- 100 Gbps data channel over a single fiber

Encryption Design for Secure Channel

FPGA Design

The user side receives, merges and encrypts 10 SFP+ modules @10G to one CFP module @100G on the client side.

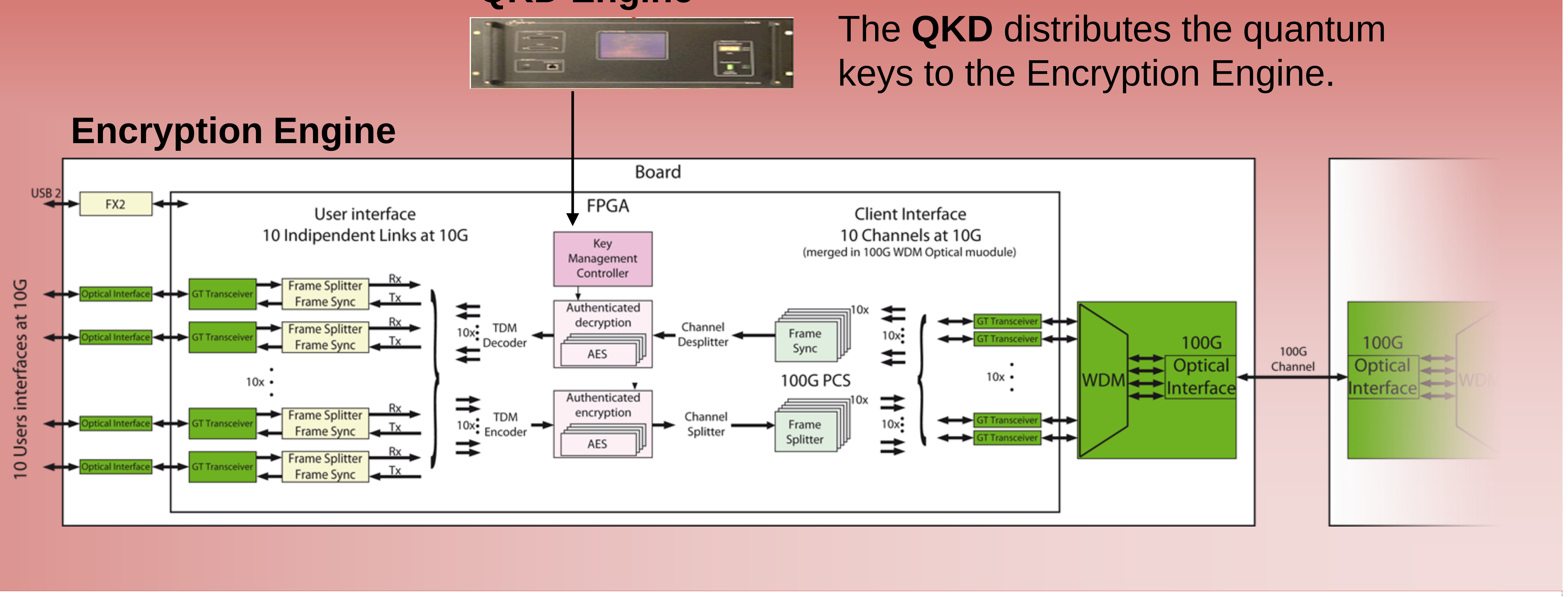
The AES encryption uses the quantum keys distributed by the QKD Engine.

FPGA: Stratix IV GT (EP4S100G5)

QKD Engine

The **QKD** distributes the quantum keys to the Encryption Engine.

Encryption Engine

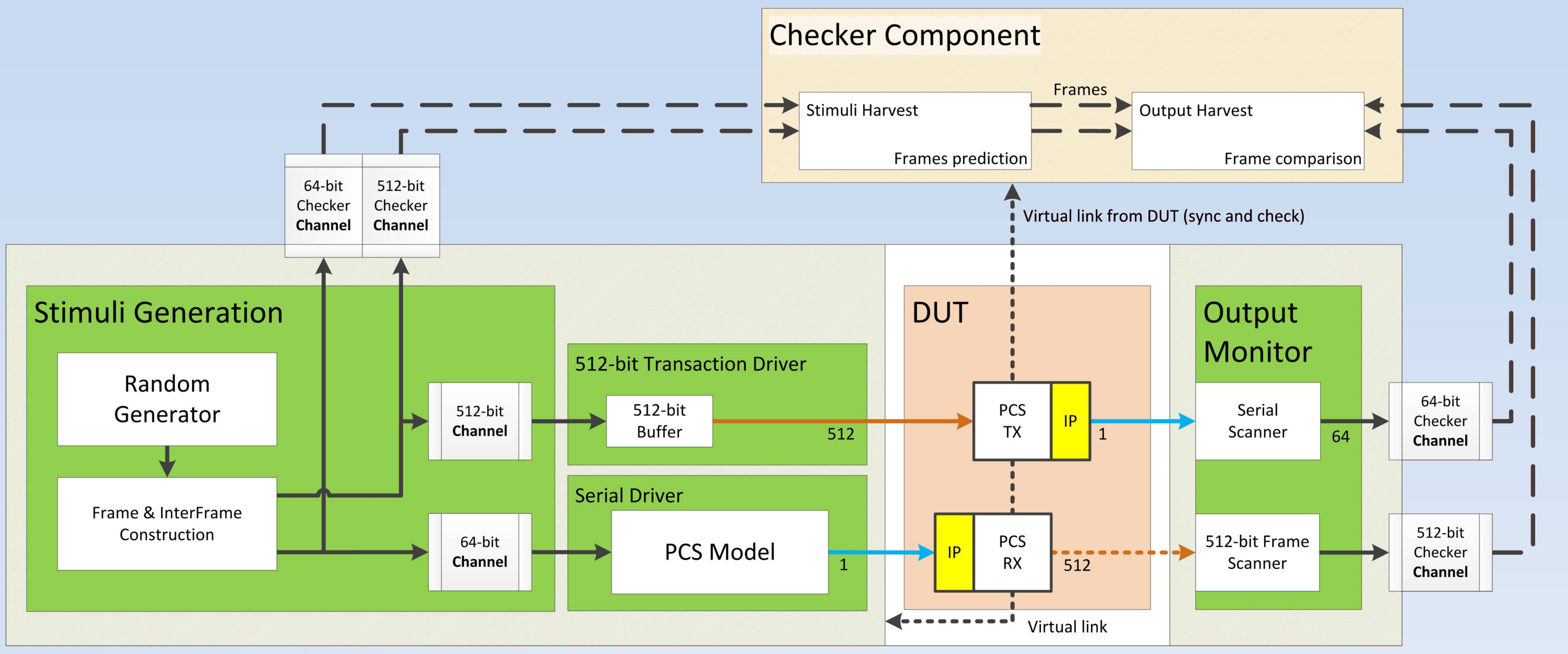


SystemVerilog Test Environment

Testbench

The testbench is based on the newest SystemVerilog verification framework. The latter provides several functionalities such as

- Objet-oriented;
- Random generation;
- Transaction channels.
- Verification methodologies (OVM, UVM)



Features

- SystemVerilog Model of the 10G PCS
- Frame checker component
- Ethernet frame generation with random values and sizes

Randomized Ethernet frame

Ethernet Frame structure	Preamble	Dest. MAC	Source MAC	Ether type	Payload	CRC/FCS	Inter Frame
Byte number	1 2 3 4 5 6 7 8	1 2 3 4 5 6	1 2 3 4 5 6	1 2	1 2 … 46 - 1500	1 2 3 4	
Values	78 5555_5555_5555_D5	Random	Random	8100	Random	Calculate	1E 1E … 1E 1E
Random values in %	2%	100%	100%	2%	100%	0%	2%
Size of blocs	Fixed = 8	Fixed = 6	Fixed = 6	Fixed = 2	Random 45 to 1500	Fixed = 4	Random 0(1%), 1(10%), to N
					Sequence of size		
					Payload End Symbol End Payload		

Principal investigator: Nicolas Gisin (Nicolas.Gisin@unige.ch)

Contact: Etienne Messerli (etienne.messerli@heig-vd.ch)
Norbert Felber (felber@iis.ee.ethz.ch)