Strategy and Synergy for Security

SETS Key Distillation Engine (KDE) IP Core

Product Description

Key Distillation Engine is a post-processing for Quantum Key Distribution (QKD) Systems and enables two parties to establish a final shared secret over noisy channels. SETS KDE IP core consists of three main building blocks of QKD protocols, namely error-correction, privacy amplification and authentication. SETS IP core implements Low-density parity-check (LDPC) codes for error correction, binary multiplicative hashing for privacy amplification and polynomial evaluation for authentication. This IP core includes reference design for Xilinx FPGA. It will be useful to those who wish to develop QKD systems.

The technical support for issues like bug fixing will be available up to 6 months from the date of purchase. Contact office for price.

Key Features

- Tailor-made for QKD applications
- Compliant with IEEE 802.11n
- Adaptable for LDPC code rates (1/2, 2/3,3/4,5/6)
- Adaptable for all LDPC block lengths (648, 1296, & 1944 bits)
- Available for FPGAs (Xilinx, Altera)

Benefits

- Customised and low-complexity design
- Corrects up to 11% errors in data
- Early stopping criterion for iterative LDPC decoder
- Trade-off between performance and throughput

The following components will be provided as part of this IP Core licensing:

- HDL source code and sample testbench
- HDL simulation model
- Matlab simulation model
- Technical Documentation

About SETS

Society for Electronic Transactions and Security (SETS) is an initiative of the Office of the Principal Scientific Advisor (PSA) to the Government of India. It was set up for the purpose of nucleating, sensitizing and developing solutions by performing advanced research in Information Security. The idea of such an exclusive organisation working in information security was conceived by Dr.A.P.J. Abdul Kalam and implemented by Dr. R. Chidambaram, through the O/o PSA to GoI.

The main charter of SETS is to conduct Directed Basic Research (DBR) – the term coined by Dr R Chidambaram—and translational research in the area of cyber security. Accordingly, SETS is focusing on three verticals, namely cryptology, hardware security and network security, having activity-based teams working on Quantum Key Distribution, Side-Channel Analysis, Physically Unclonable function, Post-Quantum Cryptography, Deep-packet inspection, and Blockchain technology.

Contact Us

Society for Electronic Transactions and Security (SETS)
M.G.R Knowledge City, C.I.T Campus
Taramani, Chennai – 600113
Tamil Nadu, India

Phone: 044-66632521,515
Website: www.setsindia.in
Email: jothiram@setsindia.net
dillibabu@setsindia.net