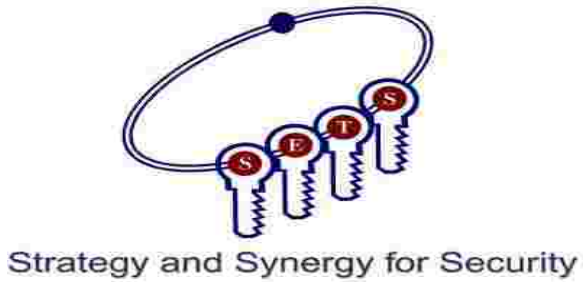
CHALLENGES IN HARDWARE REALIZATION OF KEY DISTILLATION ENGINE FOR QKD

SARIKA K

SETS India, Chennai



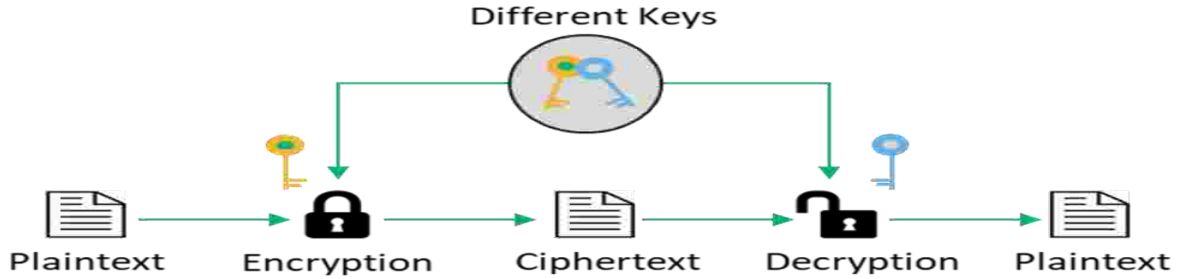
CRYPTOGRAPHY

- Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

CONVENTIONAL CRYPTOGRAPHY

- **Symmetric** : use the same (secret) key to encrypt and decrypt a message
  - Eg: AES, DES

- **Asymmetric**: Use one key (public) to encrypt a message and a different key (private) to decrypt it. So this also known as public key cryptography.
  - Eg: RSA,ECC



QUANTUM COMPUTERS – CURRENT STATE

Company	Type	Technology	Now	Next Goal
Intel	Gate	Superconducting	17	49
Google	Gate	Superconducting	72	TBD
IBM	Gate	Superconducting	50	1000(2023)
Rigetti	Gate	Superconducting	8	TBD
IonQ	Gate	Ion Trap	7	20-50
Silicon Quantum Computing Pty	Gate	Spin	N/A	10
Harvard/MIT	Quantum Simulator	Rydberg Atoms	51	TBD
Univ. of Maryland / NIST	Quantum Simulator	Ion Trap	53	TBD
D-Wave	Annealing	Superconducting	2048	5000
NTT/Univ. of Tokyo/Japan NII	Qtm Neural Network	Photonic	2048	100,000

THREATS TO CONVENTIONAL CRYPTOGRAPHY

- Traditional public key cryptosystems (RSA, DSA) are breakable by Shor's algorithm.
  - Shor's algorithm efficiently solves integer factorizations and discreate algorithms lead to breaking asymmetric cryptographic schemes.
  - Increasing key size or changing parameters does not mitigate the attack

- Symmetric Key crypto systems can potentially be broken by brute force using Grover's algorithm
  - Speed up the key search over symmetric key algorithms
  - For example, AES128 requiring 2^{128} operations can be compromised by 2^{64}operations by a quantum computer.

WHAT IS THE SOLUTION??

1)Post Quantum Cryptography(PQC)

- It's a group of algorithms that remain secure, even in presence of sufficiently powerful quantum computers
- Algorithms are based on the complexity of mathematical problems
- PQC will be widely used for data encryption and digital signature

2)Quantum Key Distribution(QKD)

- It enables two parties to produce a shared random key which is used to encrypt and decrypt message.
- It applies a cryptographic protocol based on quantum mechanics
- QKD is only used to produce and distribute a key

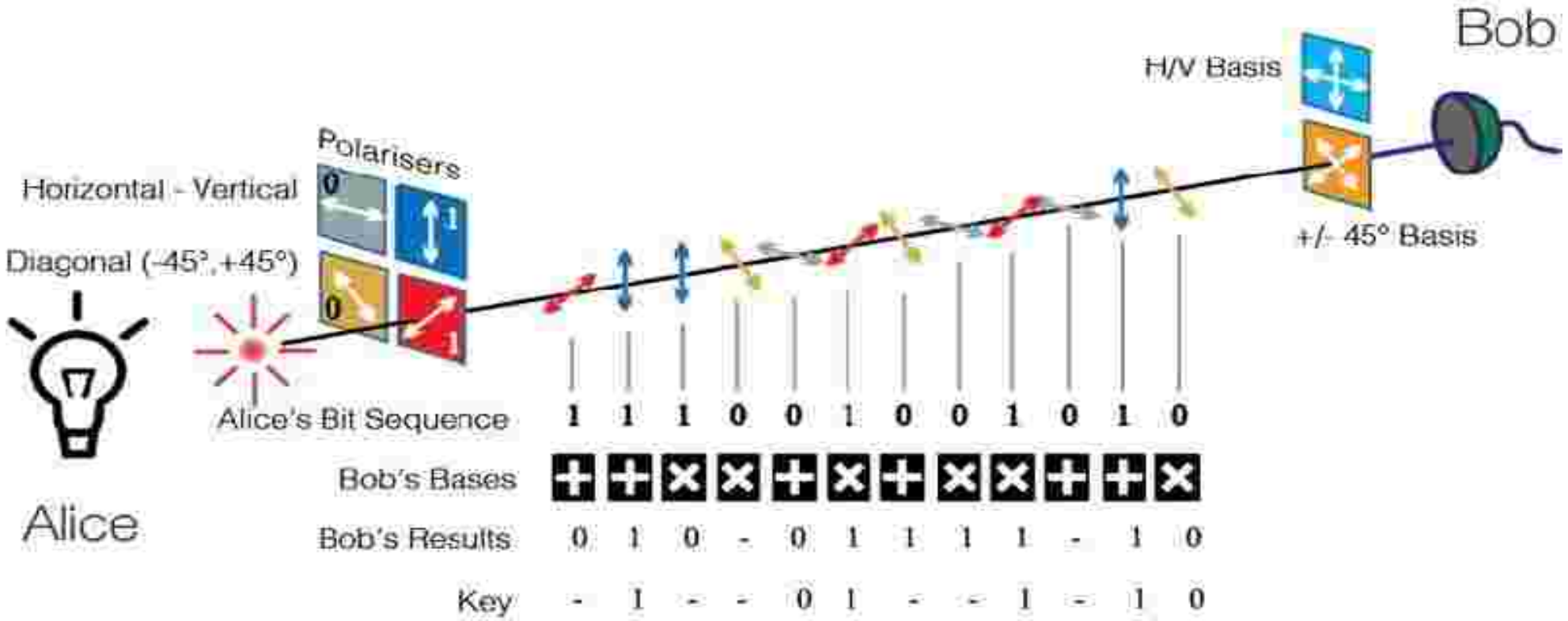
WHY QKD?

- QKD is theoretically provably secured way for two distinct parties to establish a common secret key
  - Key must be truly random and never reused
  - QRNG and One Time Pad(OTP)
- It deploying quantum mechanical properties to perform cryptographic tasks
- QKD tell us all attempts of eavesdropping
- The first protocol in quantum cryptography was proposed in 1984 by Bennett and Brassard(BB84)

QUANTUM THEORY

- **Heisenberg uncertainty Principle:** states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of other with certainty
  - If Eavesdropper introduces errors, then measurements of the quantum state disturbs
- **Non-cloning theorem:** It states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum states
  - Quantum information cannot be copied perfectly by eavesdropper

QKD PROTOCOL – BB84



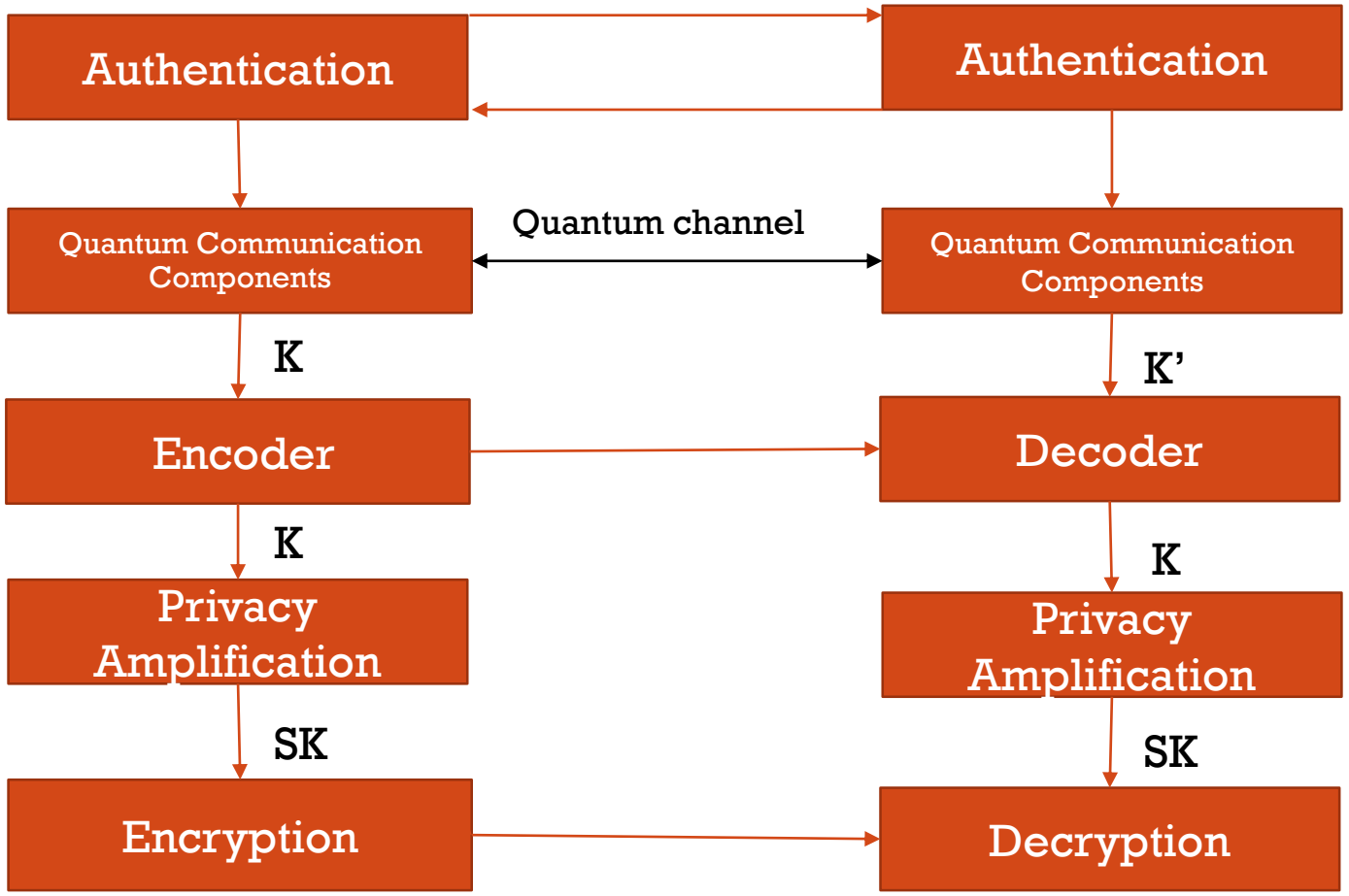
THE BB84 PROTOCOL

- Alice chooses a random classical bit string 1010010110…..
- For each bit, Alice sends a photon in either ‘+’ or ‘x’ basis, making the choice randomly
- Bob measures each photon in either ‘+’ or ‘x’ basis by his random choice
- Alice and Bob compare their choices, end up with a secret key whenever their basis choices coincides.

NEED FOR KEY DISTILLATION

- QKD transmission occurs through two channels:
  - Imperfect private channel - quantum channel
  - An authenticated public channel - classical channel.
- The private channel is imperfect in various ways:
  - Transmission errors.
  - Partial information can leak to Eve.
  - Eve can also modify the transmissions arbitrarily.
- The public channel transmits information accurately, but the entire contents becomes known to Eve.

KDE FLOW DIAGRAM



AUTHENTICATION

- **AUTHENTICATION:** To verify message's integrity
- Hashing Algorithm with key used for authentication
- Universal Hash Function**(UHF):** UHF are particularly useful for algorithms that need multiple hash functions
- Why poly1305: Information Theoretically Secure → the collision probability is negligible.

ERROR CORRECTION

- To send information across a noisy channel with near zero errors observed, the only way is to add some extra information along with the message.

- This extra information appended is referred to as error correcting codes.

- Low Density Parity Check(LDPC) codes:
  - It exhibit excellent error correction performance
  - Hardware friendly due to inherent parallelism

PRIVACY AMPLIFICATION

- Privacy Amplification (PA) is the most significant post processing procedure of QKD system.
- It converts weak key into a uniform secured key to eliminate the knowledge of EVE about the key.
- Technique used for our privacy amplification is universal hashing.
- Using hashing the raw key is compressed.

TOEPLITZ HASHING

- Toeplitz hashing is performed by a single matrix – vector multiplication over GF(2)

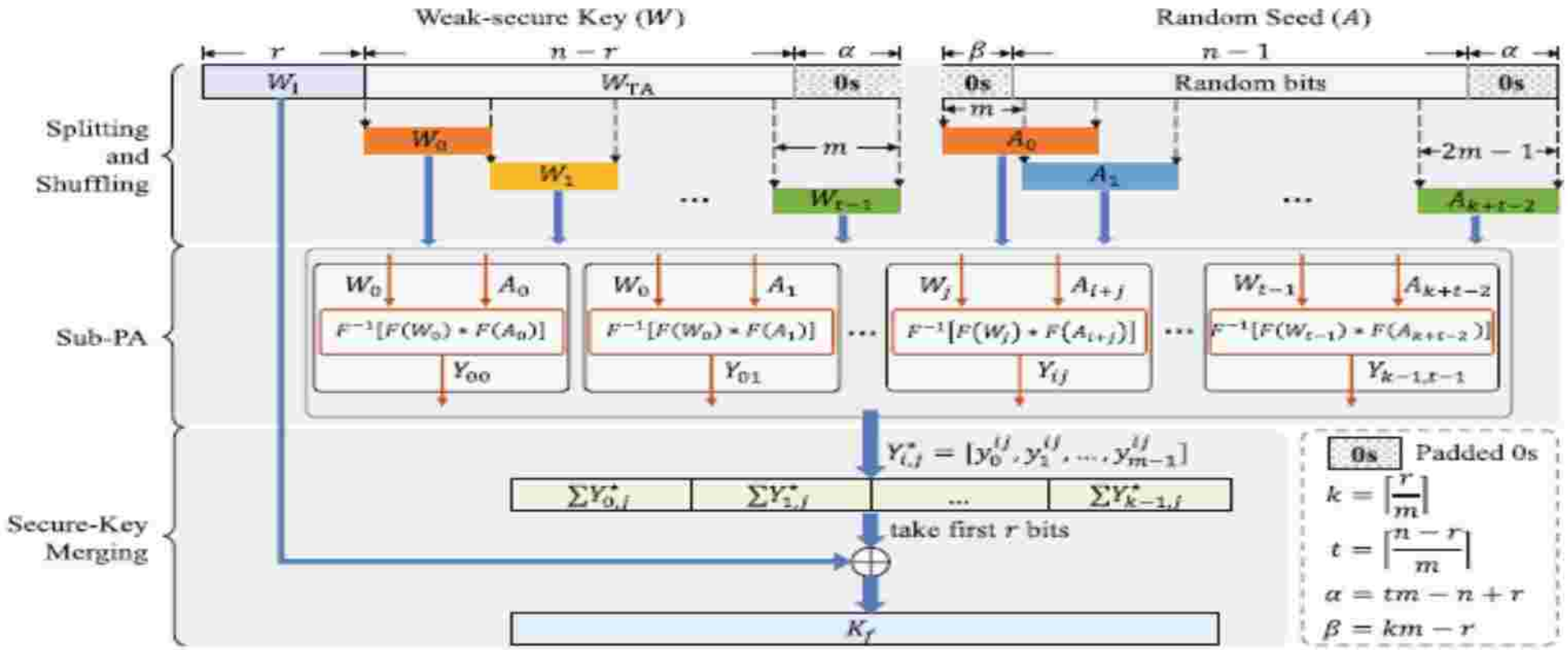
- ri → random bits
- xj → raw key bits
- yi → secret key/secured key bits

$$\begin{pmatrix} r_1 & r_2 & \cdots & r_n \\ r_{n+1} & r_1 & \cdots & r_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n+m-1} & r_{n+m-2} & \cdots & r_{n-m-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

IMPLEMENTATION CHALLENGES OF PRIVACY AMPLIFICATION

- Computational complexity:
  - larger matrix multiplications are computationally intensive.
  - Computation complexity can reduce from O(n^2) to O(nlogn) by using FFT multiplication
- Memory allocation:
  - To store larger values of data in terms of millions bits is difficult in block RAM.
  - Need to interface external memory
- High speed for QKD systems:
  - Post processing solutions are required to run in GHz speed to match the speed of the quantum channel
  - Parallel processing will improve speed of operation

PRIVACY AMPLIFICATION ARCHITECTURE



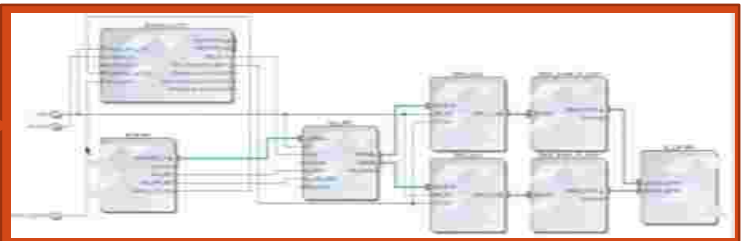
VIVADO HLS

C,C++,System C

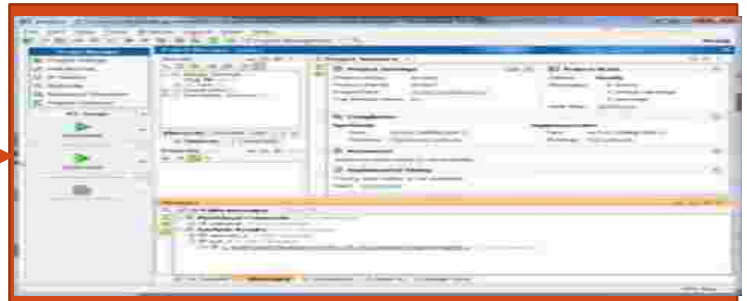
Vivado™ HLS

Verilog or VHDL

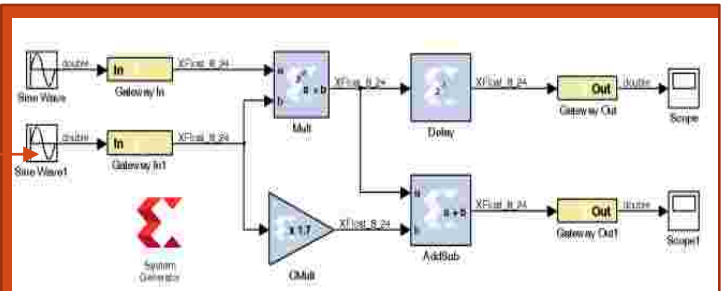
Vivado IP Catalog



Vivado Ip integrator



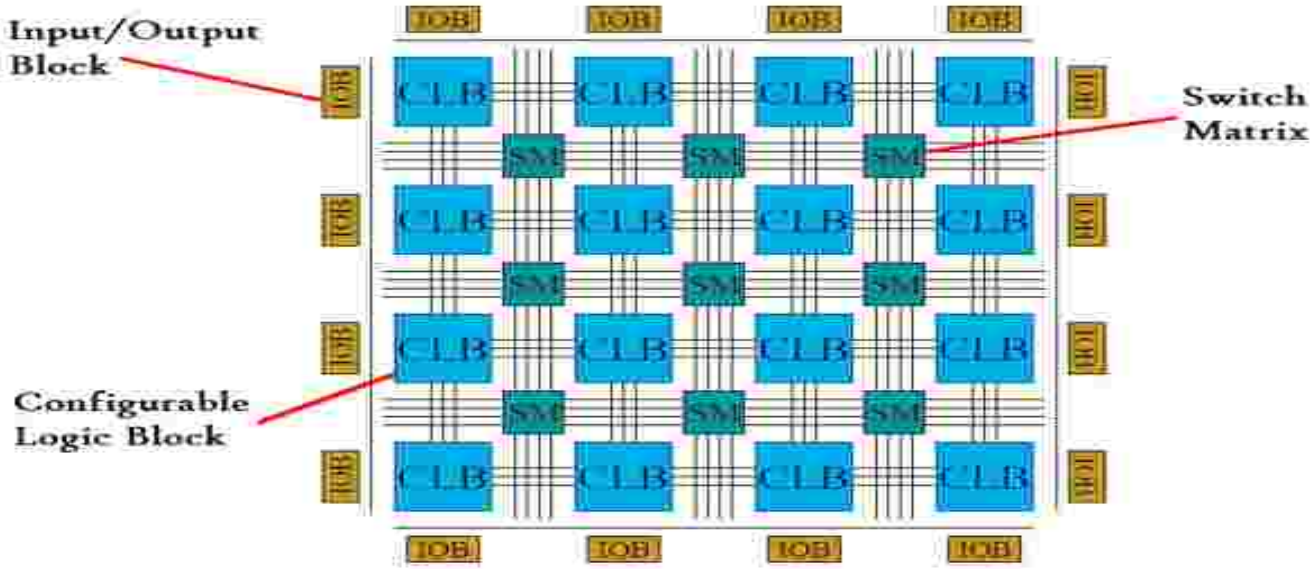
Vivado RTL

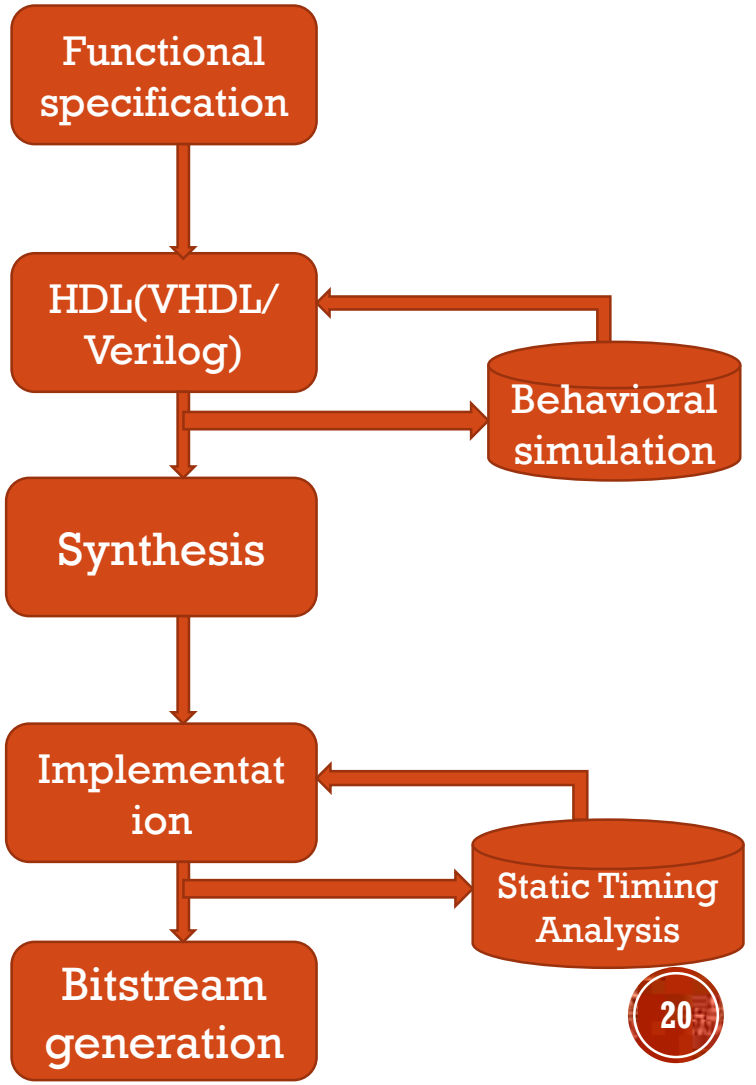


System generator

HARDWARE IMPLEMENTATION IN FPGA

- Field Programmable Gate Array (FPGA) is a semiconductor Device with higher density and capable of implementing different function in a short period of time.
- Its based around a matrix of configurable logic blocks (programmable gates) connected via programmable interconnects.





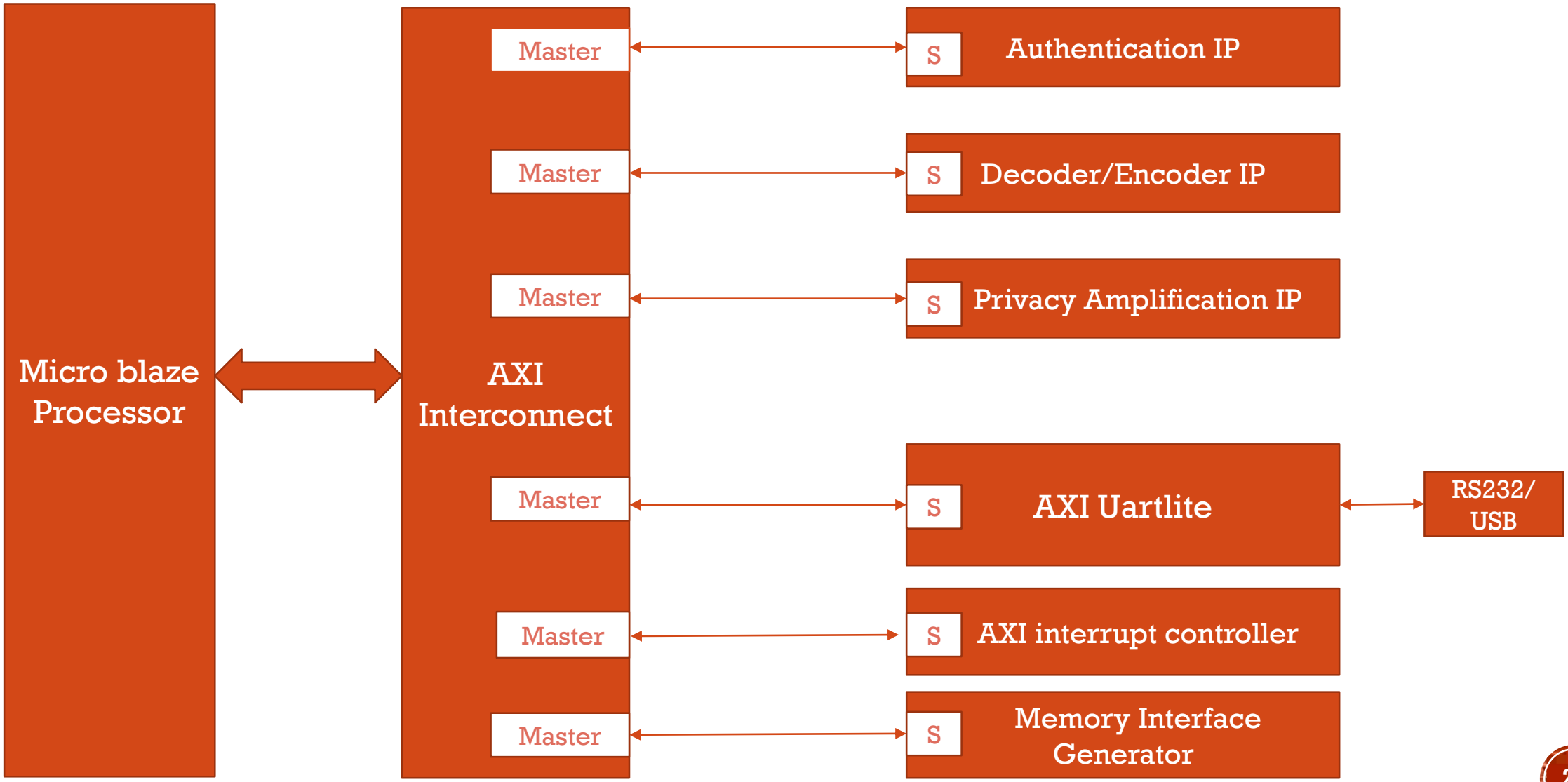
SELECTING THE FPGA SYSTEM

- **Capacity:** gate level capacity of FPGA is enough to accommodate your design
- **Scalability:** ability to add capacity to improve design functionality. Eg – memory
- **Extensibility:** adding components such as communication interface for system interface
- **Performance:** the whole purpose of building FPGA prototype is to achieve sufficient performance with careful interconnection and I/O design.

7 SERIES FPGA FAMILIES

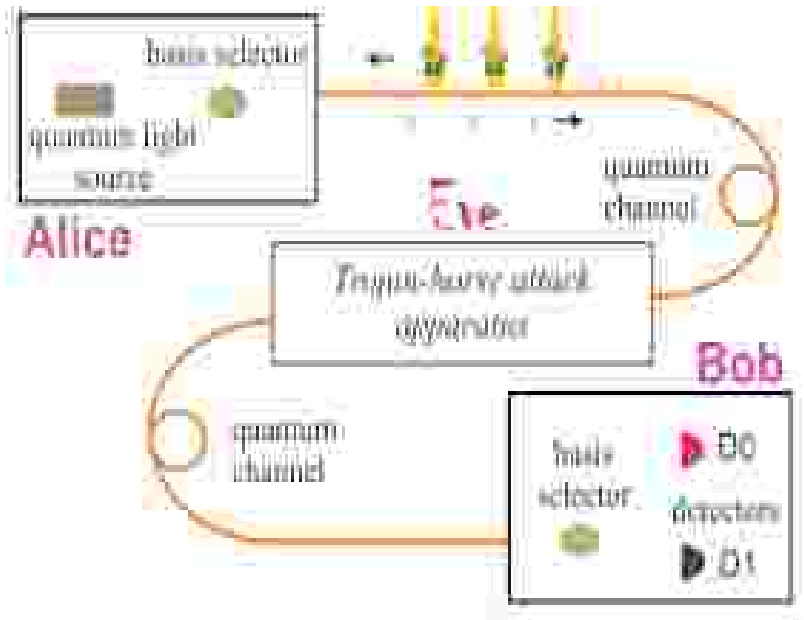
Maximum Capability	ARTIX Lowest Power and Cost	KINTEX Industry's Best Price/Performance	VIRTEX Industry's Highest System Performance	ZYNQ Extensible Processing Platform
Logic Cells	20K – 355K	70K – 480K	285K – 2,000K	30K – 350K
Block RAM	12 Mb	34 Mb	65 Mb	240KB – 2180KB
DSP Slices	40 – 700	240 – 1,920	700 – 3,960	80 – 900
Peak DSP Perf.	504 GMACS	2,450 GMACs	5,053 GMACS	1080 GMACS
Transceivers	4	32	88	16
Transceiver Performance	3.75Gbps	6.6Gbps and 12.5Gbps	12.5Gbps, 13.1Gbps and 28Gbps	6.6Gbps and 12.5Gbps
Memory Performance	1066Mbps	1866Mbps	1866Mbps	1333Mbps
I/O Pins	450	500	1,200	372
I/O Voltages	3.3V and below	3.3V and below 1.8V and below	3.3V and below 1.8V and below	3.3V and below 1.8V and below

INTEGRATION OF KDE MODULE WITH MICRO-BLAZE

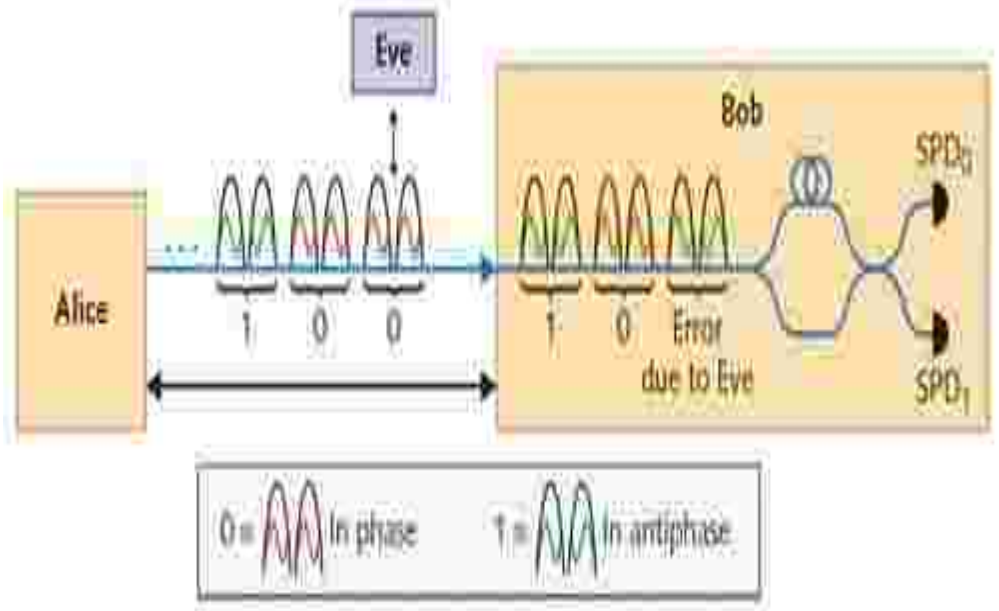


ATTACKS ON QKD PROTOCOL COMPONENTS

Trojan horse attack



Jamming attack on photons



REFERENCES

1. Bennett C.H., & Brassard G. (1984). Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the IEEE international conference on computers, systems and signal processing* (pp. 175–179). New York: IEEE Press.
2. Jeremy Constantin Et al. (2015)An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems, journal of Signal processing Systems, **volume 86**, pages1–15, Springer.
3. Bang-Ying Tang, Bo Liu Et al.(2019),High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution, Scientific Reports, Article number: 15733,natureresearch.
4. Daniel J Bernstein (2005),The Poly1305-AES message-authentication code, Proceedings of 12th international conference on East Software Encryption, pages 32 – 49.

sarika@setsindia.net

THANK YOU