Modelling Fuzzy Logic Quantum Key Distribution using Simulink

Dr C R S Kumar

Department of Computer Engineering

Defence Institute of Advanced Technology(DIAT)

Girinagar, Pune 411025, India
Email: suthikshnkumar@diat.ac.in
Web: www.diat.ac.in

Presentation at Matlab Expo 2015, 28th April 2015, Pune, India

Overview

- Introduction
  - Quantum Mechanics
  - Quantum Computing
  - Quantum Cryptography
  - Quantum Key Distribution
  - Unconditional Security
  - Fuzzy Logic
- Fuzzy Logic Quantum Key Distribution
- Modelling using Simulink
- Results
- Summary and Conclusion

Intro to Quantum Cryptography

- **Quantum cryptography**
- use of quantum mechanical effects (i.e., quantum communication and quantum computation) to perform
  - Cryptographic tasks
  - Cryptanalysis tasks
- Examples are :
  - quantum key distribution(QKD)
  - Quantum Computers for Prime Factorisation of large numbers

Advantages Quantum Cryptography

- Measuring quantum data such as photon polarization disturbs that data;
- Eavesdropping in quantum key distribution can be detected.
- UnConditional Security: As any tapping/eavesdropping can be detected.

Quantum Mechanics

- **Quantum mechanics** (**QM**) deals with physical phenomena at sub-atomic particle (electrons/Photons) scales.
- Quantum mechanics provides a mathematical description:
  - the dual *particle-like* and *wave-like* behavior
  - interactions of energy and matter.
- Quantum mechanics has played a significant role in the development of many modern technologies.

Uncertainity Principle

- The **uncertainty principle** deals with mathematical inequalities asserting a fundamental limit to the precision with which certain pairs of physical properties of a particle known as complementary variables can be measured accurately.
- Complementary variables (position *x* and momentum *p)* *of subatomic particle such as an electron* can be expressed as (h = Planck's constant):

$$\Delta x \cdot \Delta p_x \geqslant \frac{\hbar}{2}$$

Wave-Particle Duality

- current scientific theory holds that *all* particles *also* have a wave nature (and vice versa).
- This phenomenon has been verified for elementary particles.
- For example, Light can be thought either to consist of Photons or Emwaves.

Quantum Computing

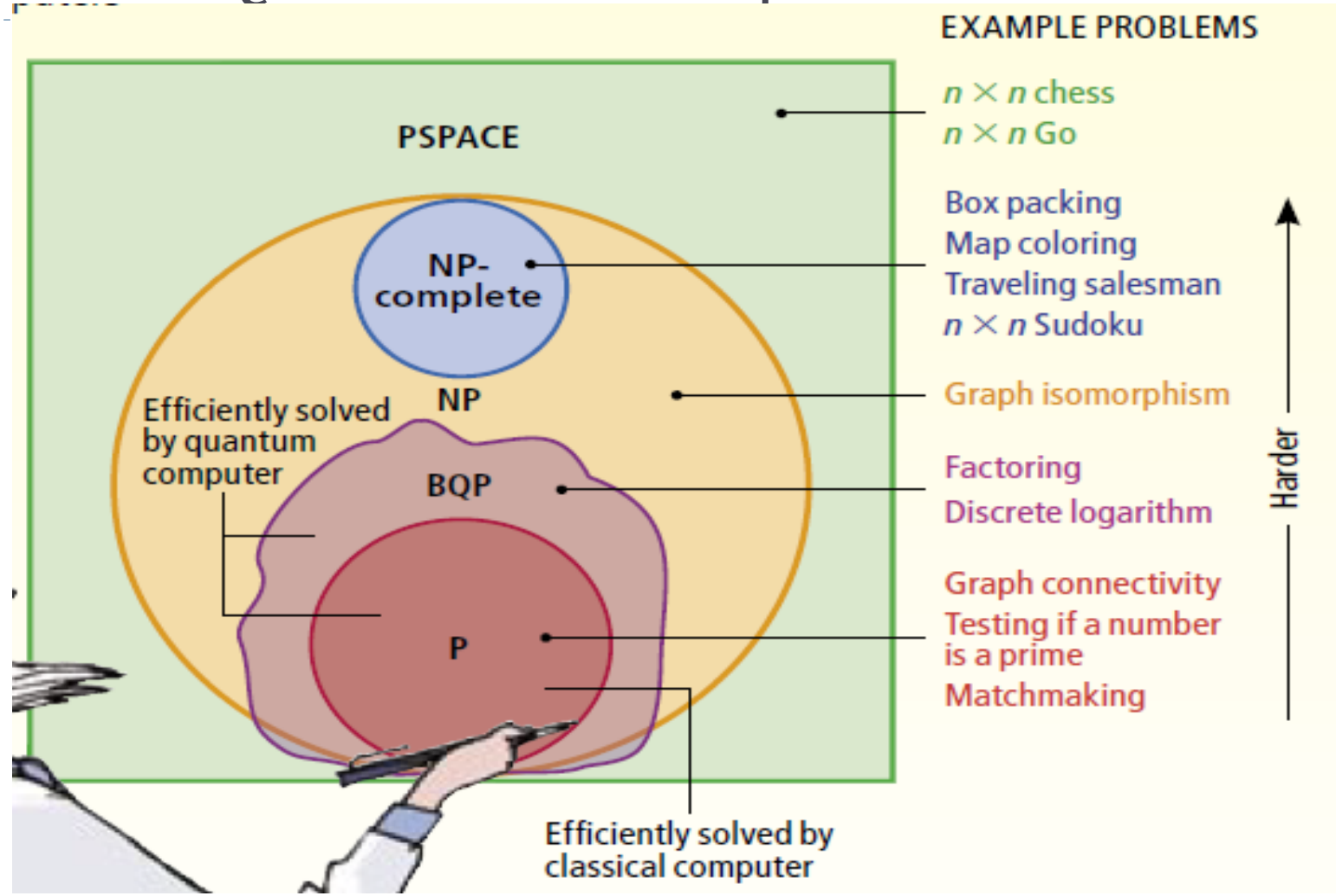
Quantum computers are based on the rules of quantum mechanics to process information.

- QC can solve problems such as factoring integers, much faster than today's computers,
- but for most conventional problems quantum computers may not be suited.

Quantum Computing: qubits

- The fundamental feature of a quantum computer is that it uses **qubits** instead of bits.
- A qubit may be a particle such as an electron, with "spin up" (*blue) representing 1, "spin down" (red) representing 0, and quantum states called super-positions that involve spin up and spin down simultaneously (yellow).*
- A small number of particles in superposition states can carry an enormous amount of information:
  - a mere 1,000 particles can be in a superposition that represents every number from 1 to $2^{1,000}$ (about 10^{300}),
- a quantum computer would manipulate all those numbers in parallel

Where Quantum Computers Fit in



Shor's Algorithm

- Quantum Computing Algorithm for Prime Factoring large number by Peter Shor (MIT).
- The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings.
- The factorization also needs huge numbers of quantum gates.
- In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3 × 5, using an NMR implementation of a quantum computer with 7 qubits.

Quantum Key Distribution

- The most well known and developed application of quantum cryptography is quantum key distribution (QKD).
- QKD describes the process of using quantum communication to establish a shared key between two parties.
- This is achieved by Alice encoding the bits of the key as quantum data and sending them to Bob;
- if Eve tries to learn these bits, the messages will be disturbed and Alice and Bob will notice.
- The key is then typically used for encrypted communication such as AES(Block Cipher), One-time pad(Stream Cipher) etc.

Unconditional Security

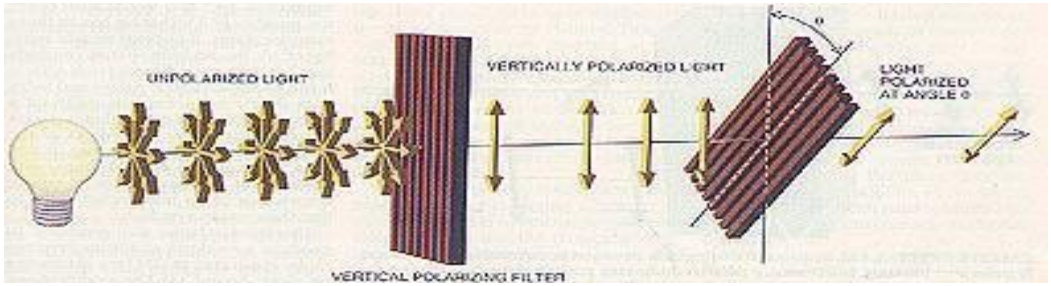
- The security of QKD can be proven mathematically.
- This is known as "**unconditional security**", assuming that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other,
- i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible.

QKD

- Quantum key distribution takes advantage of certain phenomena that occur at the subatomic level, so that any attempt by an enemy to obtain the bits in a key not only fails, but gets detected as well.
- Specifically, each bit in a key corresponds to the state of a particular particle, such as the polarization of a photon.
- The sender of a key has to prepare a sequence of polarized photons, which are sent to the receiver through an optical fibre or a similar medium.
- In order to obtain the key represented by a given sequence of photons, the receiver must make a series of measurements.
- A few explanations are necessary before the full implications of this procedure can be understood.

Polarization

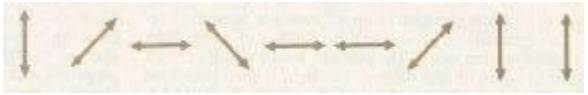
- Polarization is a physical property that emerges when light is regarded as an electromagnetic wave.
- The direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal.

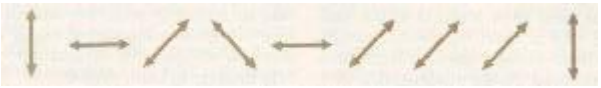


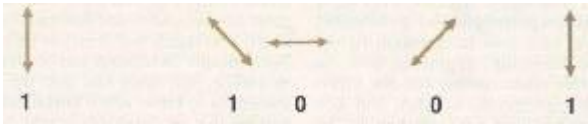
- A photon which is **rectilinearly polarized** has a polarization direction at 0° or 90° with respect to the horizontal.
- A **diagonally polarized** photon has a polarization direction at 45° or 135°.
- **0** is represented by Rectilinear 0° or Diagonal 45°
- **1** is represented by Rectilinear 90° or Diagonal 135°

QKD using Polarization

- Alice sends photons with one of the four polarizations, which she chooses at random.
- For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (X).
- Bob records the result of his measurements but keeps it a secret.
- After the transmission, Bob tells Alice the measurement types he used (but not his results) and Alice tells him which were correct for the photons she sent.
- Alice and Bob keep all cases in which Bob should have measured the correct polarization. These cases are then translated into bits (1s and 0s) to define the key.







Conjugate Coding

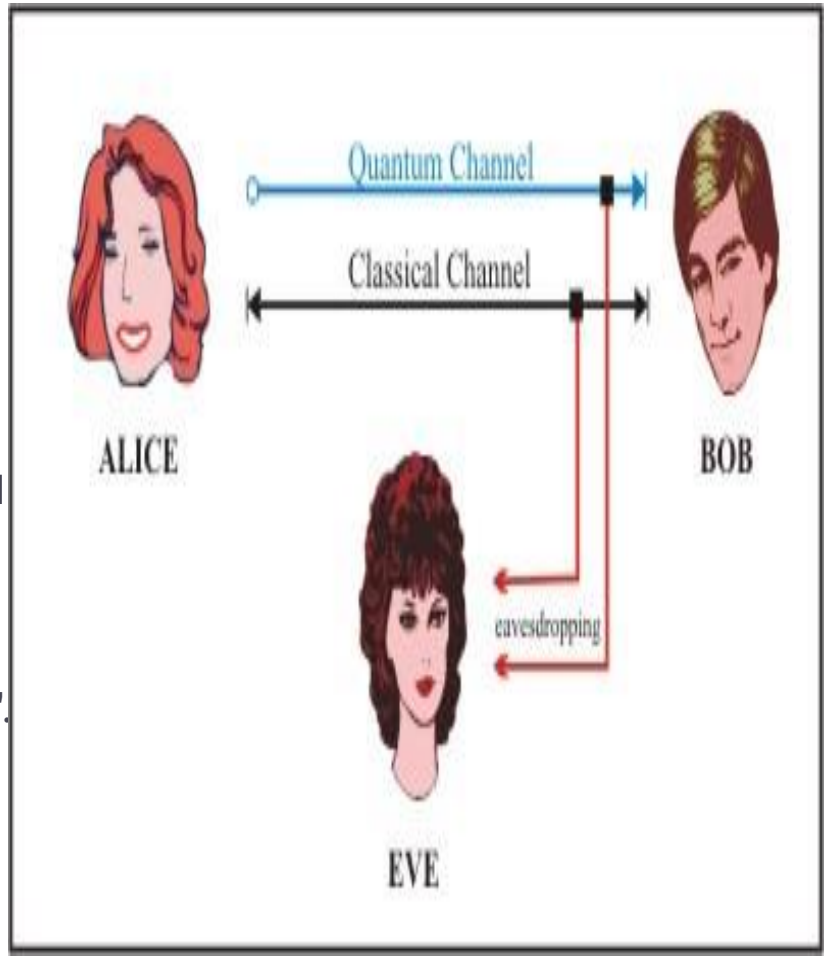
- the process of mapping a sequence of bits to a sequence of rectilinearly and diagonally polarized photons is referred to as **conjugate coding**,
- while the rectilinear and diagonal polarization are known as **conjugate variables**.
- Quantum theory stipulates that it is impossible to measure the values of any pair of conjugate variables simultaneously.
- The position and momentum of a particle are the most common examples of conjugate variables.
- This same impossibility applies to rectilinear and diagonal polarization for photons:
- if you try to measure a rectilinearly polarized photon with respect to the diagonal, all information about the photon's rectilinear polarization is lost - permanently.

Quantum Key Distribution with BB84

- BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984 .
- BB84 allows two parties, conventionally "Alice" and "Bob", to establish a secret, common key sequence using polarized photons.

BB84: QKD illustration

- Alice chooses which type of photon to use (rectilinearly polarized, "R", or diagonally polarized, "D") in order to represent each bit in *s*..
- Alice creates a sequence *p* of polarized photons whose polarization directions represent the bits in *s*.
- Alice sends the photon sequence *p* to Bob over a suitable quantum channel, such as an optical fibre.
- For each photon received, Bob makes a guess as to whether it is rectilinearly or diagonally polarized, and sets up his measurement device accordingly. Let *b*' denote his choices of basis.
- Bob measures each photon with respect to the basis chosen in step 5, producing a new sequence of bits *s*'.
- Alice and Bob communicate over a classical, possibly public channel. Specifically, Alice tells Bob her choice of basis for each bit, and he tells her whether he made the same choice. The bits for which Alice and Bob have used different bases are discarded from *s* and *s*'.



QKD Illustration

ALICE

Bit sequence, *s[i]*	0	0	1	1	0
Encoding bases, *b[i]*	R	D	R	D	D
Transmitted photons	→	↗	↑	↖	↗

EVE

Eve's measurement bases, *eb[i]*	R	R	D	D	D
Eve's measurement results, *es[i]*	0	1	0	1	0
New, transmitted photons	→	↑	↗	↖	↗

BOB

Bob's measurement bases, *b'[i]*	R	D	D	R	D
Bob's measurement results, *s'[i]*	0	1	0	0	0

eavesdropping detected and communication aborted

FINAL KEY would have been:	0	0

Secret Key Reconciliation

- The process of reconciliation is a special error correction procedure which eliminates:
  - errors due to incorrect choices of measurement basis;
  - errors induced by eavesdropping;
  - and errors due to channel noise, if any exists.
- Reconciliation is performed as an interactive binary search for errors.
- Alice and Bob divide their bit sequences into blocks and compare each other's parity for each block.
- They follow a divide and conquer approach to determine the error bits.
- When an error has been located, Alice and Bob may decide to discard the corresponding bit, or agree on the correct value.
- During this process, Alice and Bob can communicate over a classical (i.e. "non-quantum“ “Insecure”) channel..

Privacy Amplification

- The process of reconciliation results in a bit sequence which is common to Alice and Bob
- To eliminate "leaked“ information, Alice and Bob must apply, in common, a binary transformation (usually, a random permutation)
- The precise choice of transformation and the number of bits discarded, of course, determine the amount of secrecy of the final key.
- The objective of this step is to minimize the quantity of correct information which the eavesdropper may have obtained about Alice and Bob's common bit sequence.

Limitations of QKD

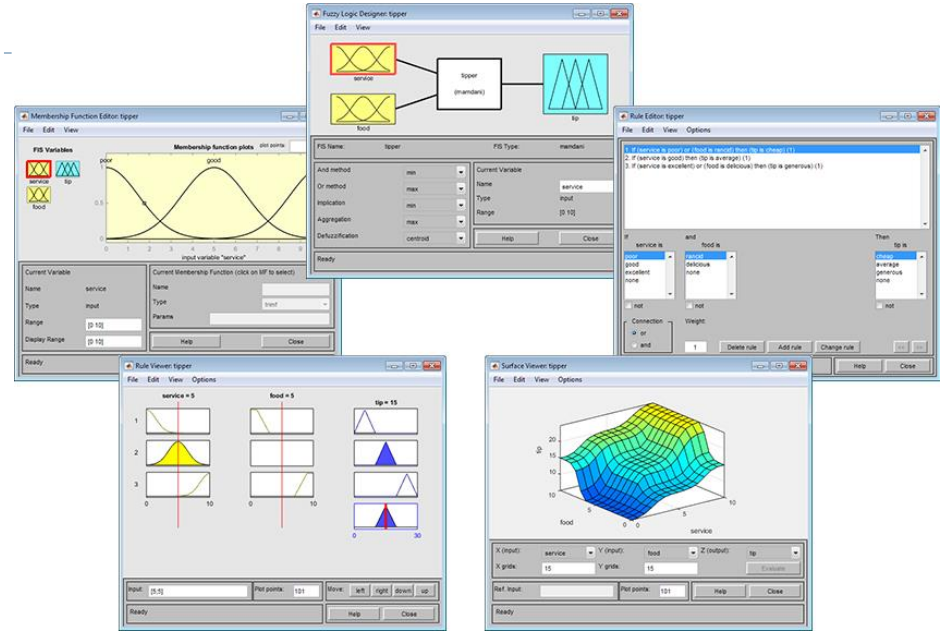
- Only part of QKD involves quantum mechanical phenomena - using polarized photons to represent a binary sequence
- It is necessary to perform a set of "non-quantum" communications over insecure communication channel for
  - key reconciliation
  - privacy amplification

Limitations of QKD

- Generally, as soon as an eavesdropper is detected, the procedure must be aborted and postponed to a later date.
- That is to say, the legitimate users (Alice and Bob) have to "keep trying" until no eavesdropper is found on the channel.
- It is now known that, if Alice and Bob share a small amount of information prior to quantum key distribution, it will always be possible for them to establish a secret key .
- This may sound awkward, since there is little point in performing quantum key distribution if the users are capable of establishing common, secret data via other means
- -- this is a known issue and remains to be tackled.

Fuzzy Logic

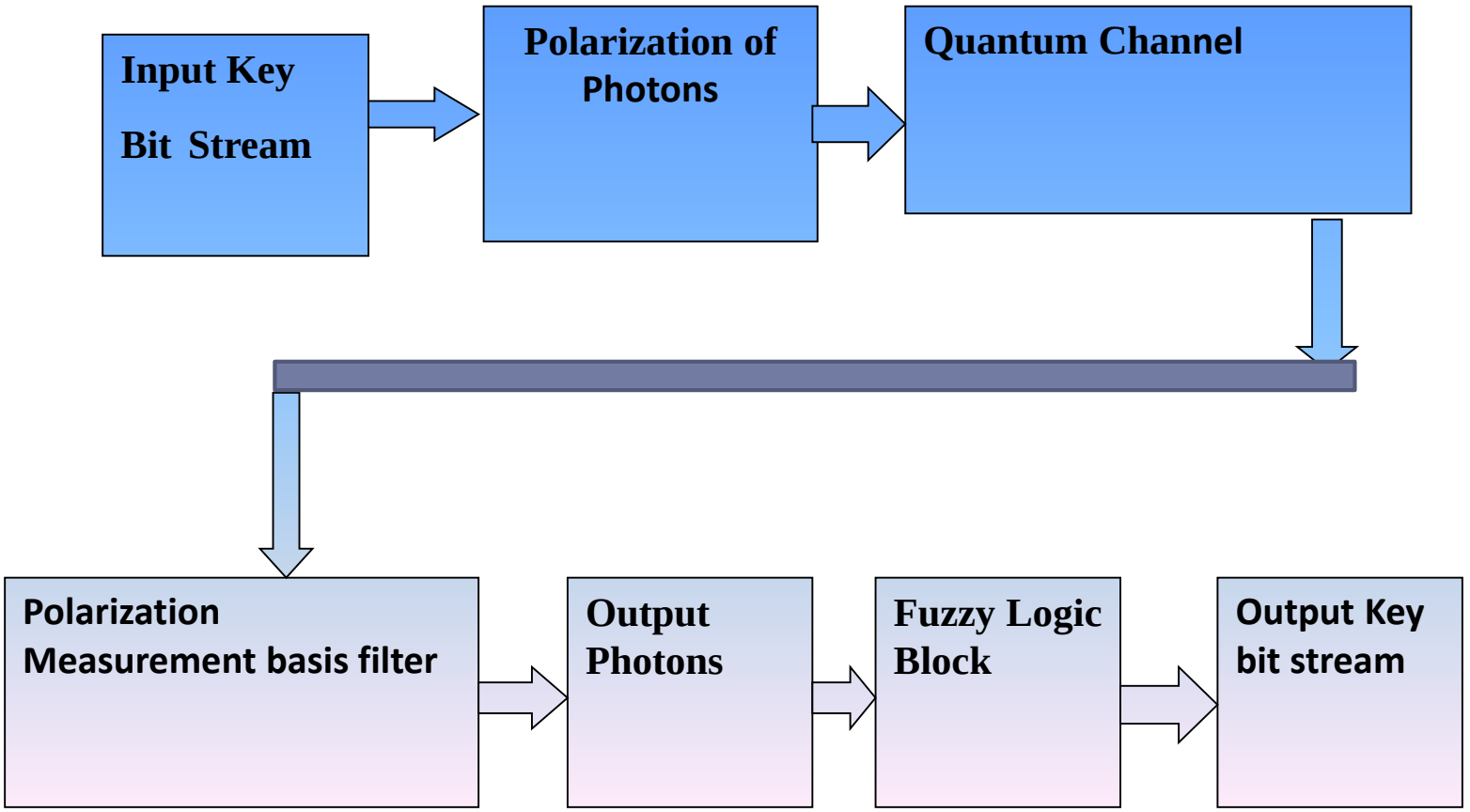
- **Fuzzy logic** is a form of logic which deals with reasoning that is approximate rather than fixed and exact.
- Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false.
- Fuzzy logic has been applied to many fields, from control theory to artificial intelligence.



Fuzzy Logic toolbox in Matlab provides a fuzzy controller block that can be used in Simulink to model and simulate a fuzzy logic control system.

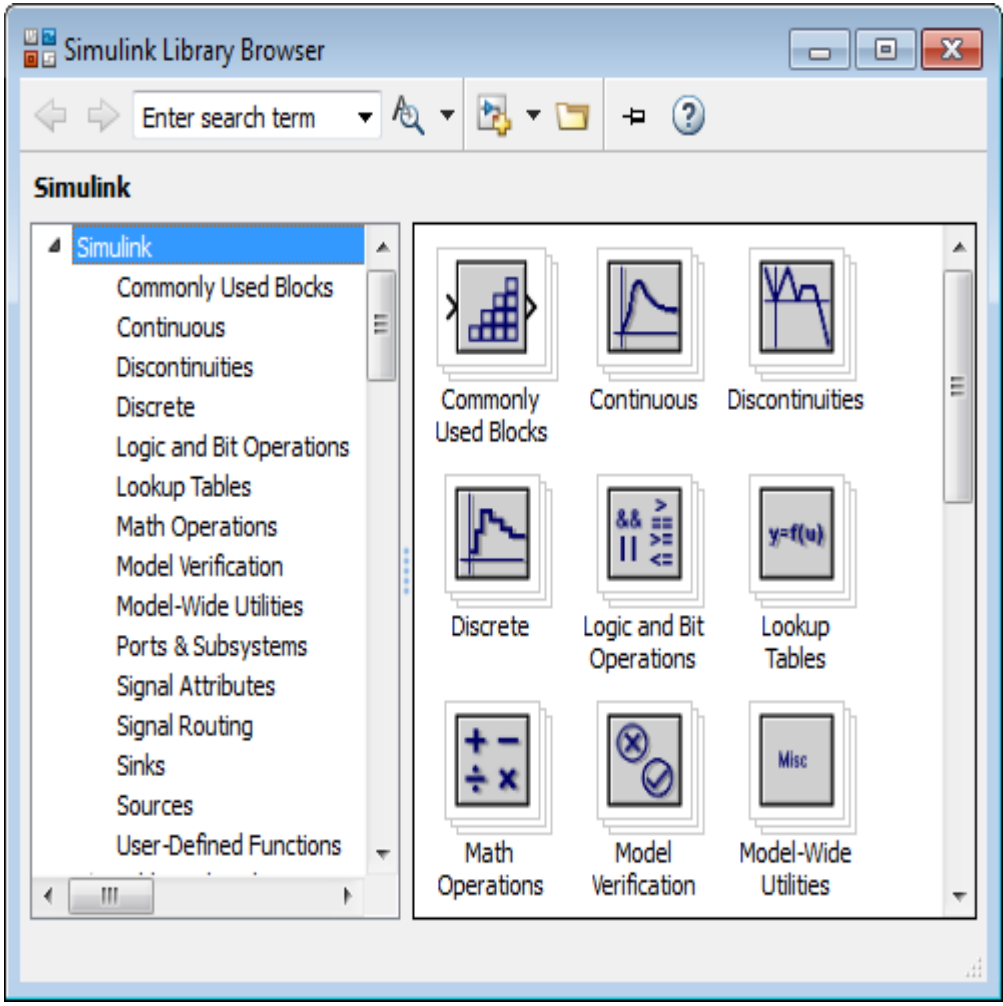
The Toolbox provides : FIS Editor, Membership Function Editor, Rule Editor, Rule viewer and Surface viewer.

Fuzzy Logic QKD

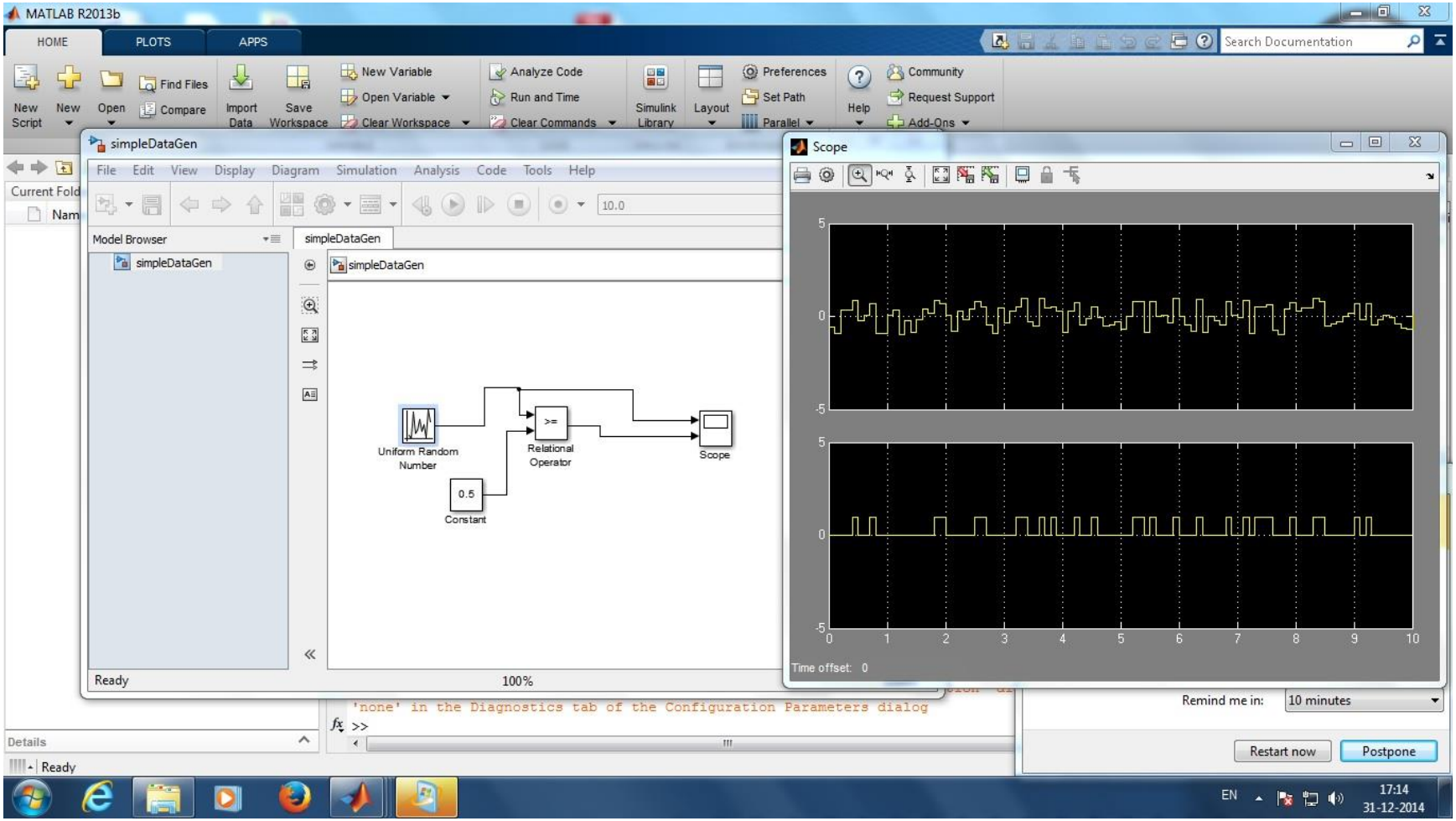


Modelling using Simulink

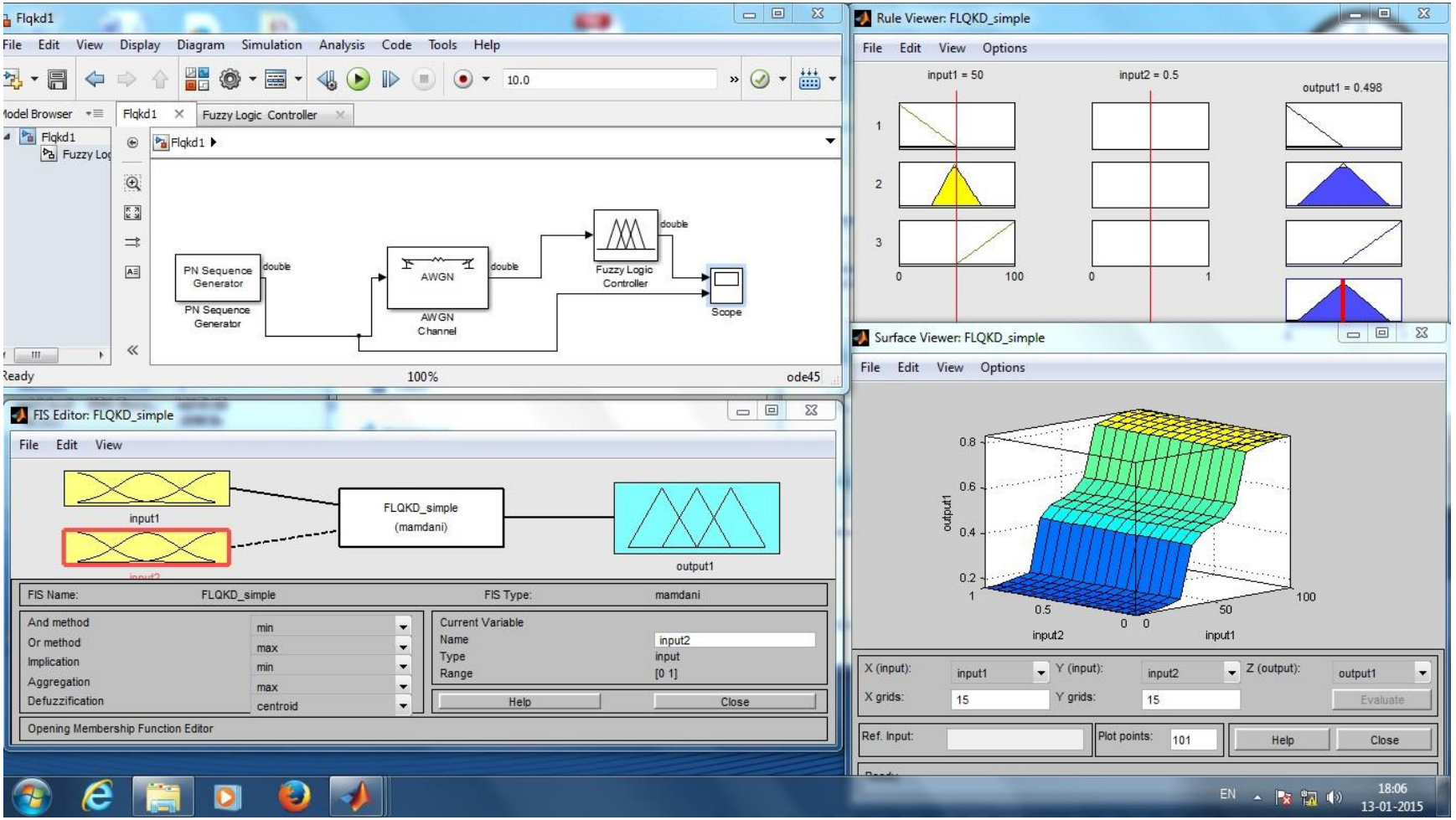
- Simulink® is a block diagram environment for Modelling, simulation and Analysis.
- It supports simulation, automatic code generation, and continuous test and verification of embedded systems.
- Simulink provides a graphical editor, customizable block libraries, and solvers for modeling and simulating dynamic systems.
- It is integrated with MATLAB®, enabling the user to incorporate MATLAB algorithms into models and export simulation results to MATLAB for further analysis.



Data Generator for FLQKD using Simulink



Simulink Modelling of FLQKD



Summary and Conclusions

- Quantum cryptography provides Unconditional Security based on the Quantum Mechanical principles.
- QKD can be combined with One-Time pad to achieve Unconditional Security and Perfect secrecy for communication.
- We have demonstrated modelling and simulation of FLQKD using Simulink.
- Simulink facilitates the modelling and simulation of FLQKD as it provides rich library of components required.