Biomedical Research 2017; Special Issue: S51-S58 *ISSN 0970-938X*
www.biomedres.info

Medical data transmission through PLCC with QFT-PUF encoder for data authentication.

Sharmila Durai*, Rangarajan Parthasarathy

RMK Engineering College, Kavaraipettai, Tamil Nadu, India

Abstract

The egression of new technologies has led to the development of new security concerns. The current technology is inadequate to handle new security challenges in fields of networking, banking and health care. Security concerns arise in both wired and wireless communication medium. The wireless communication covers small area, lacks in security and data loss. In wired communication, the layout of wires and amplifiers increases the infrastructure cost. To overcome the above problem, we propose Power line carrier communication with (Physically Unclonable Function) PUF to secure the data. The proposed model Power line carrier communication with PUF is termed as PPUF. To improve data security in wired communication without new infrastructure for establishing the communication network in the hospital, we apply Quantum Fourier PUF to access individual modules and enable data encryption over the transmission line of Power Line Communication. The Quantum Fourier PUF performs better than existing PUF models in terms of lower order of magnitude delays, energy consumption, and resilience to various attacks.

Keywords: System-on-chip, Physical unclonable function, Quantum computing, Quantum fourier transform, BIST, FPGA.

Accepted on January 09, 2017

Introduction

Data security plays vital role in application such as client server model computing, banking, health care, sharing data between devices through cloud and e-commerce to avoid hacking. Security methods develop due increases in data transfer between cloud centers and embedded processor. The mobile phone transfers the computation to desktop systems, data center, and clusters, due to energy and power restrictions. The growth of mobile phone-based medical instruments in health care rises the importance of data security to the higher level. In addition to security in many medical applications, data privacy also is given much importance. In fact, the guarantee of privacy is difficult in telemedicine, where intimate data about patients is being collected, stored, transmitted, and viewed. In security, Public Key Cryptographic (PKC) communication protocols apply for the data privacy. The PKC requires high computational resources and power consumption. The public key cryptographic protocol increases the area, energy and power consumption of the processor. Therefore, deployment in medical sensing environments is complex.

To overcome the problem as discussed above, we propose two security primitives, such as primitive security advantages with a new hardware-based technique Programmable System-on-Chip (PSoC) FPGA and the QFT-PUF. A PUF is a settled multiple-input multiple-output system that can simulate and perform reverse engineering. Silicon PUFs support to build hardware-based security systems that resilient to side channel and physical attacks. The limitations of PUF system exists in cryptographic algorithm due to occupy the large memory space to generate secret key and security protocols. Recently developed public key PUF schemes such as physical unclonable functions (PUFs) and SiMulation Possible (SIMPL), but Laborious systems removes limitations but still requires complex computation.

In this paper, we proposed QFT-PUF preserves all advantages of PUFs but implements the system in single cycle computation to explore security protocols in a wide range. Therefore, in a sense, the PUF provides ultimately low latency and low energy security protocol that support the device to operate in different environments. QFT-PUF helps to overcome secure-key storage on non-volatile memory by using Quantum Fourier Transform and its inverse. The properties of Hamming distance calculate difference between challenge-responses pairs (CRPs) in the proposed QFT-PUF, with authentication mechanism use PRNG (Pseudo-Random Number Generator) to avoid replay attacks.

In addition, the proposed QFT-PUF resiliency against the arbitrary side channel or physical attack. Since the proposed model has, the intra-body integrated security circuit in transmitter side with patient data acquisition system and an external device, the programmer (i.e. doctor) has access at the receiver side for the statistical analysis. The two PUFs matched

at implantation time, such that they implement the same functionality (i.e. their input-output mappings are identical). Their function remains unpredictable and complex, to maintain security, and takes the reasonable actions to ensure the system is unclonable after implantation.

Related Work

The term Physical Unclonable Function (PUF) refers to a physical object. The output is random and hard to clone (Table 1).

Table 1. *Related works.*

Ref. No	Author	Description
[1]	Majzoobi et al.	To ensure security and robustness of Physically Unclonable Functions (PUFs), the methodology employs three key principles i) placed multiple delay lines for response bit creation ii) combination and transformation of the challenge bits and iii) for reliable PUF, combine multiple delay lines.
[2]	Maisel and Kohno	To improve the privacy and security of implantable medical devices is important. Medical devices ensure data integrity, secure communication, and confidentiality. By considering the importance of health care records, developed as a universal security requirement to provide secure medical devices and personal health information.
[3]	Yalla and Kaps	The proposed Lightweight Cryptography for FPGA introduces cryptographic algorithms for block cipher optimization techniques. The implementation of block cipher faster the operation compared with stream cipher and achieves security policies for new applications to FPGAs. However, research does not concrete on porting these algorithms to FPGAs.
[4]	Majzoobi et al.	Ring Oscillator (RO) PUF and Arbiter PUF generate the large bit stream over process variations deployed during IC production. This process variations differs based on IC manufacture and provide security implemented in wide applications, but they are not suitable for FPGA cores such as key generation, intellectual property (IP) protection and digital circuit management.
[5]	Potkonjak et al.	Hardware Trojan Horses alter the specifications and working of known hardware without the consent of user. The changes made to the hardware, specified by the hacker. Hackers use tools and configuration scripts to make change to the hardware.
[6]	Potkonjak et al.	Ultra-low power and high-speed public physically unclonable function (PPUF) had developed for Smart Card (SC) security purposes. An analyze with several potential security attacks to ensure the performance of new PPUF.
[7]	Xu et al.	Digital bimodal function (DBF) supports ultra-low energy security protocols and allow the computation of legitimate communicating sides. In this DBF approach, energy efficiency over traditional security key cryptographic security technique (e.g., AES) compared with RSA.
[8]	Chang et al.	The practically expose of using body physiological values for sharing keys over exchange messages is evaluated. Furthermore, Electrocardiography (ECG) signals due to deployment on the body and outsiders capability to remotely sense.
[9]	Xu and Potkonjak	Here introduces the new way to handle standard analog delay PUF with develop FPGA-based digital PUF to observe the stable challenge inputs and the PUF output regardless of environment and operation conditions. With this stable inputs, enrollment the look-up tables to configured digital PUF.
[10]	Beckmann and Potkonjak	Even though after alternating the huge resources for Multiple-input and Multiple-output of PUF, the system exposes the structural complexity and computation time. With public key protocols and new secret key exchange avoids adversity against side channel and physical attacks and which doesn't include the mathematical conjectures, there is a reduced complexity and computational time.
[11]	Wendt and Potkonjak	A nanotechnology-based architecture ensures security and fast authentication through partial simulation.
[12]	Xu and Potkonjak	Digital hardware random number generator (DHRNG) implemented as recursive structure in FPGA with low energy to extract random bits and connect configurable logic blocks randomly during configuration.
[13]	Burleson et al.	The author summarizes the IMD security measures and possible traps that exist. In addition, improving the implanted devices enhances the configuration of devices. The configuration parameters include sensing, security, bio-interfaces and efficiency.
[14]	Rukhin et al.	The testing and selection of pseudorandom number generators for cryptographic applications, generators fulfill requirements of cryptographic applications and generates the strong keys in unpredictable manner without any knowledge on inputs.

Design Flow for Utilizing the Pufs in Tele-Healthcare System

To build a Tele-healthcare system, must consider the numerous design properties and metrics, such as a deployment on the body, cost, low power, accuracy, etc. However, the important aspects of the system in the physical world to provide security and privacy over their operation. Regarding security and privacy, user information at sensing system takes protection at all levels such as storage, transmission, data collection and processing. In addition, users typically authenticate the system to access data information from its sensor origin. But, physical attacks cause problems to remotely authenticate the system. To resolve the physical attacks, the cryptographic methods

develop trust over user information with their new protocols and mechanism, but in real time it overheads the area and implementation complexity. To solve area overhead and implementation complexity, a new approach is developed.

To secure patients biosignal (pulse, Blood pressure) or tele-health care system and their sensors operation with privacy for user information, we introduce new approach with trust mechanism called PUF. This new approach of integrating PUF within existing hardware design to secure system and information flow and prevent the system from side channel, physical and software attacks with minimal computational power and hardware implementation complexity. The PUF architecture design with multiple-input and output physical system and the system produces sufficient large bit stream pairs of challenge/response vectors. The Figure 1 illustrates the PUF structure which consists of encryption and decryption blocks. The PUF produce unique response pair when PUF apply with challenge vector through inter stage network which involve encryption and decryption blocks.

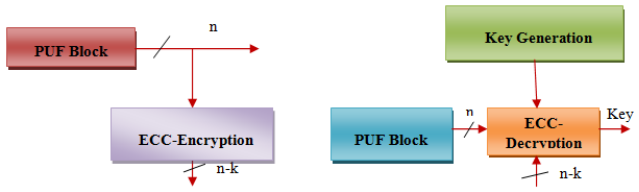

Figure 1. *The PUF architecture.*

Each physically unique PUF, due to clock frequency variations, will produce different challenge/response pairs. For example, one or more motes sampling and transmitting data from sensors across a patient's body can be equipped with a PUF that can be matched to a PUF in a receiving device at the doctor's end. We propose a trust base approach for patient sensing. The proposed model comprises of two PUF structures with challenge generation mechanism and sensing module. Figure 1 shows the model of proposed structure. Furthermore the trusted authority apply binary key to the PUF structure to produce pseudo-random bits. The first PUF block used to authenticate the collected sensor data and the second PUF, used to authenticate the integrated subsystem to collected sensor data through the clock activation duration, which coordinated with sender and receiver.

Power Line Carrier Communication (PLCC)

Communication defines not only connection to make access to internet browsing and data sharing through wired and wireless methods. Nowadays, data security issues became an important factor over wired and wireless methods. Due to developing features of communication methods such as Wi-Fi, mobile networks, fiber-optic cable, secure the data is the main problem. Over wireless methods, wired communication methods show more advantage and performance metrics. Because, wireless communication has more disadvantages such as cost, security, capacity, etc. For advance research requirement to provide a suitable infrastructure for communication medium achieved through the PLCC. A Power line carrier communication introduces with all advantages of security and fast data. A PLCC communication allows existing wiring power cables for data communication medium with high data transmission over a short field, so it's suitable for home network (HAN), and near-me area network (NAN) and also control passive and active of distribution lines. In addition, demonstration concept with PLCC, LAN network covers entire building to rise data transmission bits per second to million bits per second. The PLCC technology fulfills the different data transmission rate by using various frequency band scales and divide data communication technologies into Narrowband Power line carrier communication (NBPLCC) and Broadband Power line carrier communication (BPLCC) (Table 2).

Table 2. *Summarizes the comparison of wired and wireless communication.*

Technology	Advantages	Disadvantages
Wired-PLCC	Security High Capacity Data rate Cost Effective Extension Coverage	Signal attenuation High noise
Wired-Optical Fiber	Stable characteristics High Capacity	Cost of operation Network infrastructure
Wireless	Rapid installation Mature technology	Limited coverage Cost Long Delay Low Capacity Lack Security

In PLCC technology, the aspects to monitoring the signal attenuations and electrical noises arise more due to, high inductances working to increase the efficiency of power lines to reach the maximum data transmission rate and allow access to various frequency channels with the design of low pass filters and to block high frequencies. To control noise and signal attenuation in power transmission lines, Broadband Power line carrier communication couplers attach to increase the channel characteristics and minimizes noise to allow signal to reach everywhere. Broadband Power line carrier communication implement at physical layer with high-speed rate over 100 Mbps, communication assets by electric power lines with standard transmission frequencies below 100MHz. BPLCC supports all kind of devices used for first-mile/last-mile connection under 1500 m to the premise and also extend to build LANs, broadband services, smart grid applications and data distribution with distance less than 100 m between the devices. Communication established through the internet from home automation with available power lines.

Narrowband Power line carrier communication technology specifies low-frequency less than 500 kHz, assets through direct current and alternating current electric power lines. NBPLCC standard supports indoor and outdoor communication with medium and low voltage power lines in both urban and rural applications with transmission frequencies

less than 500 kHz. Application requirements and network conditions effected to data rates will be measured to 500 kb/s with frequency spectrum from 9 to 140kHz. This technology ensures reliable, cost-effective and more security.

QFT-PUF Trust Model Implementation

The health centers should invoke trust, with both the doctors and patients. The data shared by patients with the doctors should be confidential, and data should not be open to access for the third party when data transferred from patient to the doctor. To enable the sensors data to exchange messages with the programmer's external device, they are matched in such a way that both devices can produce identical responses streams based on the given challenges inputs. Therefore, we use the shared responses stream to encrypt messages through sensor controller module and subsequently decrypt them using the programmer's device, and vice versa. In this implementation, we address two properties in the programmer's device related to its Unclonability and its extensiveness. Unclonability ensures that even if an attacker steals the device, they cannot reproduce its functionality. Extensiveness refers to the device's capability to be used as a platform for communication with a multiple of intra-body sensors modules using only small modifications or even no modifications at all. A general use case for this scenario might be a single doctor with one external device that can communicate securely with many patients.

QFT-PUF Algorithm

Algorithm-QFT-PUF mechanism

1. The doctor generates PRNG (Pseudo-Random Number Generator) with various clock frequencies for an individual patient ID, transmit through the PLCC.
2. For example, PSoC1-PA1 in QFT implementation block receives the PRNG number and performs QFT formation for that number in QFT-PUF block.
3. Sensor controller module enables through the QFT transformation and collects patient information. Finally encrypt into packet, set QFT transformation as header and put in PLCC.
4. From Secure SoC block, IQFT-PUF receives packet information and applies Inverse-QFT for packet header to compare with MEM block PRNG number.
5. If matching becomes true, PUF enables patient data monitoring system to retrieve patient information from PLCC network.

The Figure 2a shows the QFT implementation block with PLCC. PLCC works with the help of repeater at low range frequencies and lower data rates up to 500 KHz with data rate 100 kbps (cover several kilometers). Figure 2b show QFT implementation with PSOC on hardware. Moreover, the data rates and distance limits changing over one place to another place while in the power-line communication. However, high-voltage transmission lines carry low-frequency carriers with two analog voice circuits. The QFT-PUF, which enables challenge/response pairs to coordination of PUFs owned by multiple parties. The protocol proceeds as described in algorithm for a patient and doctor, and results in each party having an identical PUF without the possibility of any attacker being able to match the same configuration. Doctor can issue patient a challenge and verify his response by executing it on her own PUF, enabling a myriad of low-energy cryptographic protocols that require neither high storage nor simulation. The Figure 2 explains the protocol that requires the patient and doctor to coordinated their PUFs to match an identical configuration. The protocol proceeds as specified in Algorithm, for a patient in sending the data to a doctor. In addition, the overhead power distribution network causes high impedance faults in public area. This developed system derived the overall impedance at different frequencies. However, the medium voltage topologies verified, and outputs examined. In addition to that earth, magnetic properties concluded by using parametric analysis and an earth magnetic properties such as ground resistivity and relative permittivity. Finally, fault occurrence at all location on a transmission line is verified and analyzed.

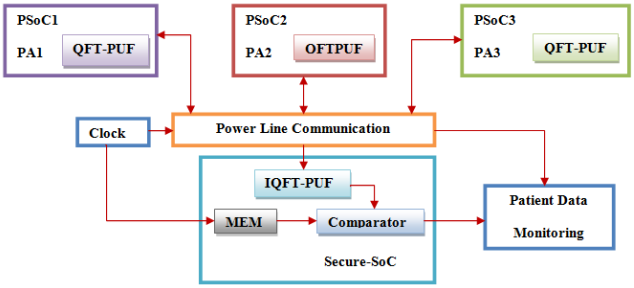

Figure 2A. *QFT implementation block with PLCC architecture.*

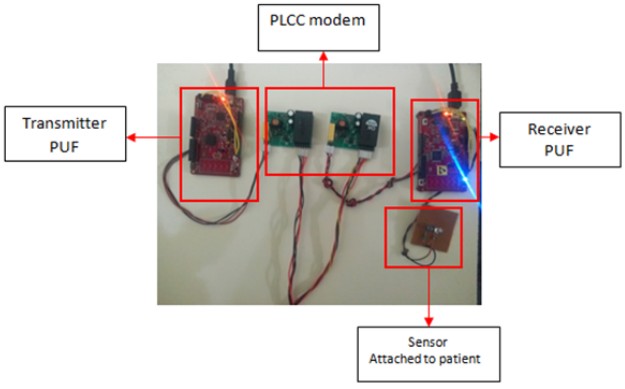

Figure 2B. *QFT implementation on PSOC with PLCC architecture.*

This kind of fault occurrence causes increasing load current of the systems. For that purpose, an operational point is set at the twice the level of the maximum feeder load. The feeder's circuit breaker contain relay to detect the increasing load in the system. But in these relay not able to detect the faults in the system. Therefore, the inability of high impedance fault (HIF) detection causes danger for public safety because the harmful step voltage leads to the fire. Medical IR Sensor interface with PSoC-FPGA to collect the patient data.

QFT Design Analysis

Authentication mechanism implement to secure cryptographic blocks, the mechanism allow access only for authenticated tester to test IP core. In addition the method prevent side channel attackers. The quantum computing implement by quantum Fourier transform and linear transformation on qubits. However, the discrete Fourier transform implement by hadamard gate for quantum circuit with 2n amplitude, Where n–qubits. The transform act on quantum gate and map <Xi|i> to <Yi|i>which, transforms discrete fourier transform for quantum fourier transform application. The classical transformation vectors (x_0,x_1...x_{N-1}) maps with vector (y_0,y_1... y_{N-1}) with N^{th} root of unity according to below formulae,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j w^{jk},\ Where\ w^{jk} = e^{2\pi i \frac{jk}{N}}$$

Equivalently, Quantum Fourier Transforms act on state vector, which view as unitary matrix , is given by

$$F_N = \frac{1}{\sqrt{N}} \begin{vmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & w^4 & \cdots & w^{2(N-1)} \\ 1 & w^3 & w^6 & w^9 & \cdots & w^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & w^{3(N-1)} & \cdots & w^{(N-1)(N-1)} \end{vmatrix}$$

Here $w = e^{2\pi i \frac{jk}{N}}$ is a primitive Nth root of unity.

The clk signal activates PRNG to produce 'R' values. The 'R' value represent hamming distance. The 'R' value reset PRNG after every authentication process. The PRNG value produce with 16-bit LSFR.

For16-bitLFSR module generates random value with feedback polynomial,

$x^{16}+x^{15}+x^{13}+x^4+1$

The 32-bitLFSR implement with feedback polynomial to produce key gen block.

$x^{32}+x^{30}+x^{26}+x^{25}+1$

Hamming distance and QFT matrix produces 'Ci' challenges, stored in CRPSoc database.

We definethe 1 × 1 Hadamard transform H_0 by the identity H_0=1, and then define H_m form >0 by

$$H_m = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$$

Where the 1/√2 is a normalization, that is sometimes omitted.

Form>1, we can also define H_m by:

$$H_m = H_1 \otimes H_{m-1}$$

In the domain of tele-healthcare, low power is key for long sensing lifetime and low cost. Because the PUF response can be computed in a single cycle, only a very small number of cycles for either party is required to conduct the key communication protocol to secures the send data from one user to the other. The sensor signal security further improves by employing unpredictable and nonlinear functions. The results share with patients and for key observations for QFT-PUF result analysis. QFT-PUF results are for with functional components with many outputs which improve data resiliency against attackers. Each sensor component standard consists, signal transducer and DAC (digital analog conv.) with functional IC blocks to process the signal. Table 3 discusses the previous technique and algorithm worked to better performance and comparison with proposed [15-19].

Table 3. *Performance comparison between exiting technique and proposed technique.*

Authors Name	Work	Area Overhead	Remarks
Chiu and Li	Boundary Scan Attacks	43%	STW lost to protect encryption operation in internal scan chain.
Das and Knezevic	Challenge-Responses based Cryptographic	12%	Cipher Block increases Key Storage Memory
Jhug and Park	AES secret key protect	23%	AES algorithm reduce performance over key generation
Proposed	QFT-Transformation based Secure Wrapper	10%	Generate reliable key with secure storage and transformation

Performance Metrics for Security Analysis

The proposed QFT-PUF algorithm was statistically analysed based on the various performance metrics for different potential security attacks.

Avalanche effect

Based on knowledge of similar inputs, the attacker easily traces the outputs, and causes every serious issue when the output and similar input vector highly correlated with one another. A change in input (e.g. one bit) results in a significant change occurs at the output; that action called the avalanche effect. Avalanche effect by measuring the distribution indicate that proposed system does not implement the avalanche effect and is highly resilient to the related attack.

To test proposed system over an avalanche effect, the Hamming distance measured between output vectors upon changing one bit of the input vector for each iteration. Figure 3a illustrates the output Hamming distance on relative frequency to measure distribution over output bits. With relative frequency, the average of output bits change over similar input vectors (at one-bit change) during same clock activation duration. When relative frequency percentage

increases more, output achieves the maximum of 0.65 quantile and minimum 0.15 quantile with respect to frequency distribution on a set of output values with similar input vector. From Figure 3b measures the Hamming distance between the two output bits with activation duration over a frequency distribution. With same activation duration, outputs generated on various FPGAs to calculate mean and deviation of Hamming Distance with respect to output bits.

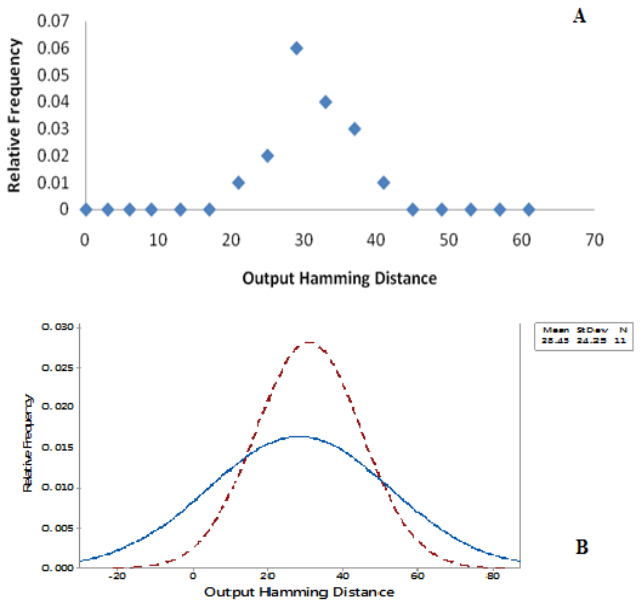

Figure 3. *Avalanche effect by measuring the distribution and mean and deviations of differences between two output vectors (hamming distance).*

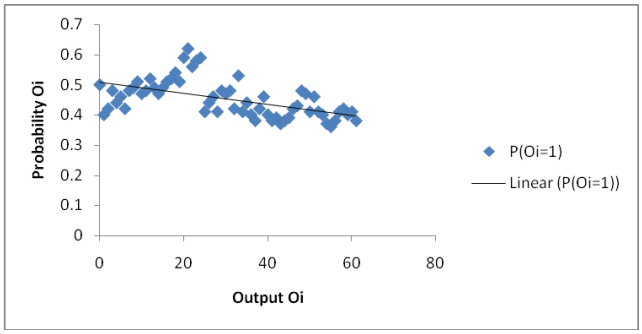

Figure 4. *Probability that an output bit is equal to 0.5 to 1.*

Frequency prediction

An attacker traces the output data from one of the matched devices and finds probability distribution for each output. The attacker predicts the output Oi based on statistical distributions with Conditional Probability (c) P(Oi=c) where c=0 or 1.The ideal secure situation is that an output is 0 with a probability of 0.5. Figure 4 shows the mean value of the probability that each output bit is equal to 1 and illustrate the linearity with respect to Probability of output Oi to c. Figure 5 respects the average probability of output Oi and the average probability shows high tendency to be close to 0.5 in percentage, which indicates resilience to this type of attack.

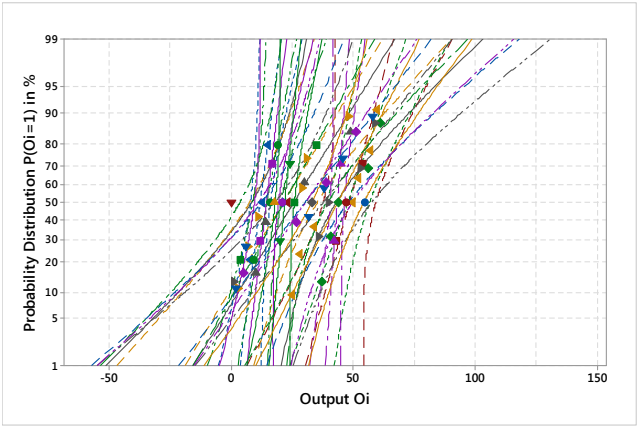

Figure 5. *Probability of output Oi.*

Input-based correlation and regression

With Input-based Correlation, the attack attempts between an input bit I_j and an output bit O_i analysis based on the correlation. The aim of the attempt is to find out the conditional probability of c_1 and c_2 mapping as a $P(O_i=c_1|I_j=c_2)$, either 1 or 0. For example, the attacker measures the time that input I_j and output O_i at 1 in the large majority. By assuming that the attacker will calculate the high probability between the current input I_j and output O_j is 0.5, easily predict the responses of QFT-PUF.

With Input-based linear Regression, the number of attacks analyzed with input I_j and output O_i. The analysis determines the probability of mapping for c1 and c2 as P(Oi=c1|Ij=c2), either 1 or 0. The attack time is measured with Ij and Oi. The probability of attack is calculated with Ij and Oj on the PUF responses. Figure 6 represents the Input-based Correlation mapping as P(Oi=c1|Ij=c2).

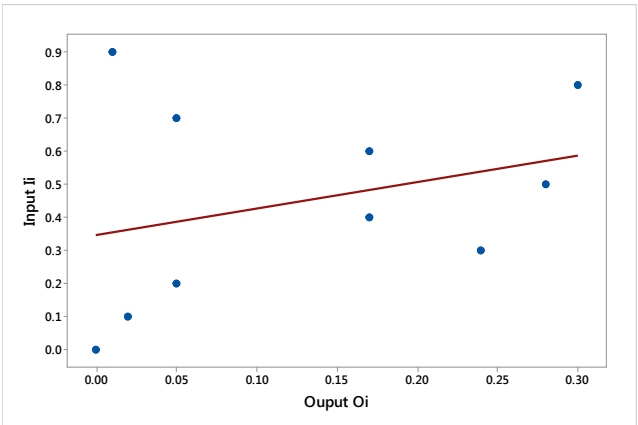

Figure 6. *Input-based correlation mapping as $P(O_i=c_1|I_j=c_2)$.*

Output and intermediate output-based correlation

The Output and Intermediate Output-based Correlation describes the output bit O_i and intermediate Output bit O_j correlation. From the attack, it traced the output bit O_i through the value corresponding to the intermediate output bit O_j. In the first case, the attacker easily traces out the logic by

knowing the subset of two output bit, by finding out a strong correlation between output and intermediate value. In the second case, the attacker traces out the results with side channel attacks possibly through intermediate output bits in clock cycle 16, means it easily predicts the output bits in clock cycle 32 based on output bits mapping. Figure 7 illustrate distribution of conditional probabilities $P(O_i=1|I_j=1)$ and Figure 8 represents the Conditional probabilities $P(O_i)$.

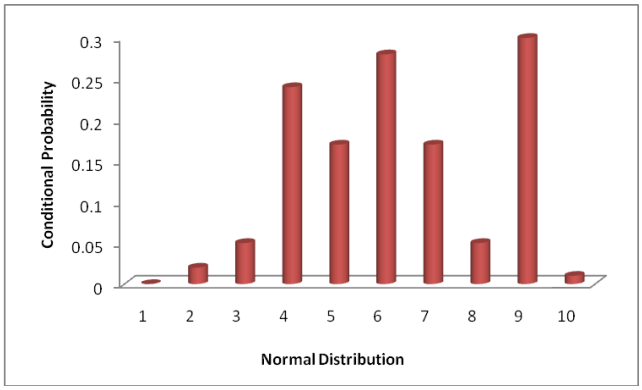

Figure 7. *Distribution of conditional probabilities $P(O_i=1|I_j=1)$.*

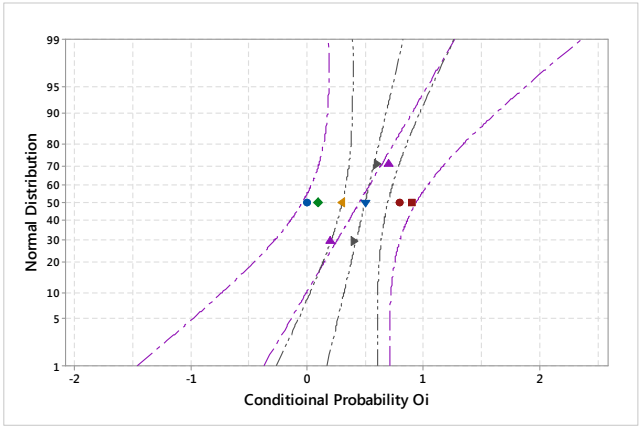

Figure 8. *Conditional probabilities $P(O_i)$.*

Conclusion

In this paper, an encryption algorithm is proposed based on Quantum Fourier Transform to secure data transmission over power line communication. The Quantum Fourier Transform and inverse Quantum Fourier Transform implement at transmitter and receiver side to encode and decode the data in power line communication. The proposed method applied in medical application for data encryption between server and the user. The proposed QFT is immune to attack from third party devices. The setup can be tested in larger network with more sensors for more than 50 members.

Acknowledgement

The authors thank Mr. A. Vignesh of Chase Research and Development Solutions for valuable support in reviewing the article.

References

1. Majzoobi M, Koushanfar F, Potkonjak M. Lightweight secure PUFs. IEEE/ACM International Conference on Computer-Aided Design 2008.
2. Maisel WH, Kohno T. Improving the security and privacy of implantable medical devices. N Engl J Med 2010; 362: 1164-1166.
3. Yalla P, Kaps JP. Lightweight cryptography for FPGAs. International Conference on Reconfigurable Computers FPGAs 2009.
4. Majzoobi M, Koushanfar F, Potkonjak M. Techniques for design and implementation of secure reconfigurable PUFs. TRETS 2009; 2: 1-33.
5. Potkonjak M, Nahapetian A, Nelson M, Massey T. Hardware Trojan horse detection using gate-level characterization. IEEE/ACM Design Automation Conference, 2009.
6. Potkonjak M, Meguerdichian S, Nahapetian A, Wei S. Differential public physically unclonable functions: architecture and applications. IEEE/ACM Design Automation Conference, 2011.
7. Xu T, Wendt B, Potkonjak M. Digital Bimodal Function: An Ultra-Low Energy Security Primitive. ISLPED, 2013.
8. Chang SY, Hu YC, Anderson H, Fu T, Huang E. Body area network security: robust key establishment using human body channel. Health Sec 2012.
9. Xu T, Potkonjak M. Robust and Flexible FPGA-based Digital PUF. International Conference on Field Programmable Logic and Applications (FPL), Munich, 2014.
10. Beckmann N, Potkonjak M. Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions. Information Hiding: 11th International Workshop, Darmstadt, Germany, 2009.
11. Wendt JB, Potkonjak M. Nanotechnology-Based Trusted Remote Sensing. IEEE Sensors, 2011.
12. Xu T, Potkonjak M. Lightweight digital hardware random number generators. IEEE Sensors, 2013.
13. Burleson W, Clark SS, Ransford B, Fu K. Design challenges for secure implantable medical devices. Design Automation Conference, 2012.
14. Rukhin A. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology, 2010.
15. Potkonjak M, Meguerdichian S, Wong JL. Trusted Sensors and Remote Sensing. IEEE Sensors, 2010.
16. Holcomb D, Burleson W, Fu K. Power-up SRAM state as an identifying fingerprint and source of true random numbers. IEEE Trans Comput 2009; 58: 1198-1210.
17. Hu C. OPFKA: secure and efficient ordered-physiological feature- based key agreement for wireless body area networks. INFOCOM, 2013.
18. Pappu R, Recht B, Taylor J, Gershenfeld N. Physical one-way functions. Science 2002; 297: 2026-2030.

19. Chang SY, Hu YC, Anderson H, Fu T, Huang E. Body area network security: robust key establishment using human body channel. Health Sec 2012.

***Correspondence to**

Sharmila Durai

RMK Engineering College

Tamil Nadu

India