2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)
Singapore, 7-9 April 2015

Securing Wireless Body Sensor Networks using Bijective Function-based Hardware Primitive

Ethiopia Nigussie*, Teng Xu†, and Miodrag Potkonjak†
*Department of Information Technology, University of Turku, Finland
†Computer Science Department, University of California, Los Angeles, USA
email: ethiopia.nigussie@utu.fi, {xuteng, miodrag}@cs.ucla.edu

***Abstract*—We present a novel lightweight hardware security primitive for wireless body sensor networks (WBSNs). Security of WBSNs is crucial and the security solution must be lightweight due to resource constraints in the body senor nodes. The presented security primitive is based on digital implementation of bidirectional bijective function. The one-to-one input-output mapping of the function is realized using a network of lookup tables (LUTs). The bidirectionality of the function enables implementation of security protocols with lower overheads. The configuration of the interstage interconnection between the LUTs serves as the shared secret key. Authentication, encryption/decryption and message integrity protocols are formulated using the proposed security primitive. NIST randomness benchmark suite is applied to this security primitive and it passes all the tests. It also achieves higher throughput and requires less area than AES-CCM.**

I. Introduction

Wireless Body Sensor Networks (WBSNs) enable a wide range of applications in health care [1], sports [2], and emergency care [3]. The use of WBSNs in health care applications facilitates early diagnosis and treatment at low-cost with little interruptions to the person's day-to-day activities. A number of potential health care applications using WBSNs have been demonstrated by the research communities [4], [5], [6]. WBSN consists of sensor nodes deployed on or implanted in the human body for continuous monitoring of biosignals and a central controller which collects the sensed biosignal data and forward it to the remote server. Each sensor node consists of biosignal sensor, processing unit, memory, radio transceiver and power unit. Since WBSNs collect sensitive and critical biosignal data, privacy and security of this information are crucial. As WBSN nodes use wireless communication and radio links are in general insecure, eavesdropping, replay, injection and other types of attacks can happen in this network. These attacks may cause a life-threatening consequences if in time delivery of the correct data to the health care professional is failed. Thus, security is of paramount importance because it maintains the WBSN system properly functional and reliable by protecting the information. The network must be adequately protected against malicious threats that can affect its functionality. Protection against security threats can be achieved by adopting different techniques which are able to enforce confidentiality, integrity, authenticity and availability of the data and communication. Conventional security and privacy ensuring techniques which are designed for other networks prove to be too expensive to use in a resource constrained WBSNs and hence, a lightweight security solution must be devised.

Majority of existing security solutions for WBSNs are software oriented and usually implemented at MAC layer. In this work, we propose a hardware-based security primitive. The design principle of this primitive use the Physically Unclonable Function (PUF) concept. PUF is a multiple-input multiple-output system that is hard to physically replicate and reverse engineer. It is a hardware primitive and its behavior is determined by the physical structure of the hardware itself and its construction. A variety of security solutions using PUF have been proposed, for example secret key generation [7], [8], random number generator [9], and device authentication [10]. Its use in resource constrained sensor networks security is also emerging [11]. Most of existing PUF designs face output instability problem due to supply voltage and temperature variations which cause delay uncertainties in different parts of the circuit. This may result in different responses for the same inputs in a given PUF instance. We tackle this problem by relying on the circuit network configuration instead of delay matching. The security primitive uses bidirectional bijective function implementation in a network of lookup tables. To achieve excellent confusion and diffusion, the interstage interconnection is reshuffled at each stage of the lookup table connection. Authentication, confidentiality and data integrity protocols are developed using the proposed security primitive and their performance is compared with conventional block ciphers.

II. Related Work

In WBSNs security is an essential feature to reliably deliver the desired services as well as for its full acceptance by users. Due to resource constraints in body sensor nodes, most of the existing security solutions have used symmetric cryptography instead of asymmetric one. Symmetric cryptographic algorithms are based on the use of secret shared keys between communicating entities. These keys have to be pre-assigned or exchanged using key management schemes. Due to this, most of security solutions focuses on developing efficient key management strategies. The use of biometrics is emerging as a potential approach for key distribution because of its sufficient randomness properties [12]. Hybrid security solution where the key exchange protocol is performed using Elliptic Curve Cryptography (ECC) and the authentication and encryption protocols using AES has been proposed in [13]. In our proposed security solution, key exchange or distribution are not required because the configuration of the interstage LUT connections serve as a secret key. It is impossible to compromise this key due to difficulty to clone or reverse engineer the configuration.

978-1-4799-8055-0/15/$31.00 ©2015 IEEE

PUF designs exploiting different physical entities (e.g. delay, voltage) and employing different architectures (e.g. SRAM, ring oscillator, arbiter) have been reported in the literature during the last decade [14], [15]. The use of PUF for sensor networks security has been demonstrated in [16], [17]. But these approaches have instability drawbacks because of its dependency on delay and leakage variations which can be affected by environmental variations. Unlike these existing works, the input-output mapping of the proposed security primitive relies on the LUT matrix configuration which is not affected by process and environmental variations.

III. Security Requirements of Wireless Body Sensor Networks

As in other wireless networks, the main security requirements of WBSNs are confidentiality, authentication, data integrity, data freshness, and availability. Depending on the application type and requirements some of the security requirements are more important than the others. Authentication is a prerequisite and the most important feature for secure operation of WBSN since the communicating nodes and the controller must ascertain the legitimacy and authenticity of each other. It must be executed as the first step of all communications. It is essential for each node and the central controller to verify that the data was sent by the trusted sensor and not by an attacker that tricked the communicating parties into accepting fake data. Data confidentiality and integrity are also vital in WBSNs. Ensuring the confidentiality of the sensed health data is necessary in order to protect the disclosure of sensitive information to unauthorized party even when such information is not identifying. Data confidentiality can be achieved through the use of encryption. In our proposed security scheme, the digital LUT-based PUF is used for encryption and decryption of the data as well as for node authentication.

In secure communication, the message receiver should be able to verify whether the message has been modified on the way to the receiver by the adversaries. In other words, the middle-man cannot modify the message content without being detected. It is critical to satisfy the data integrity requirement in WBSNs, since malicious modification of the data may result in life-threatening consequences. The usual approach for ensuring data integrity is either using public key based digital signatures or symmetric key based message authentication codes. In this work, message authentication code and integrity check protocol are formulated using the proposed security primitive. Data confidentiality and integrity is not always enough unless supported by data freshness. The adversary may capture data in a transit and replay them later to confuse the data sink. Data freshness ensures that the data frames are in order and are not replayed by an attacker. In addition, availability must also be satisfied. The most common attack on availability are denial of service (DoS) and jamming attacks. The attacker may flood the central node with continuous authentication requests, hindering its availability to the legitimate nodes. During a communication between the wearable sensor and the central node, the adversary can launch a jamming attack, making the wireless channel saturated and cause delay in the delivery of critical data. Since it is difficult to thwart DoS and jamming attacks, the solution is to alleviate their impact by employing different techniques including signal processing at physical layer. Node authentication, encryption/decryption, data freshness and message integrity protocols which are developed using the proposed hardware-based security primitive are presented in Section V.

Wireless body sensor networks are usually star topology where the wearable sensor nodes transmit their sensed data directly to the central sink node without a need for relaying through intermediate nodes. The reason for this is that the nodes are within the communication range of the sink node and relaying the data causes unnecessary energy wastage. In this work, the aim is to fulfill the authentication, confidentiality, data integrity and data freshness security requirements of the communication between the wearable body sensor node and the central sink node.

IV. Architecture

In this work, bidirectional bijective function (BBF) principle is followed to implement the hardware security primitive. In formal mathematical terms, a bijective function $f : \mathbf{x} \rightarrow \mathbf{y}$ is a one-to-one and onto mapping of a set X to a set Y. The BBF consists of two functions: $f_{original}$, and $f_{inverse}$. These functions achieve completely inverse one-to-one mappings of each other. Assume that $\mathbf{x}$ and $\mathbf{y}$ are two n-bit vectors, then the mappings realized by $f_{original}$ and $f_{inverse}$ can be defined by Equation 1.

$$\begin{aligned} f_{original} &: \mathbf{x} \rightarrow \mathbf{y} \\ f_{inverse} &: \mathbf{y} \rightarrow \mathbf{x} \end{aligned} \tag{1}$$

A. Implementation of BBF using Lookup Tables

One-to-one mapping of the BBF can be easily supported using lookup tables (LUT) as shown in Figure 1. The structure is built from a number of k-input LUTs connected in series and parallel. It has n inputs/outputs and m levels of LUTs. Between levels of LUTs, the outputs of the previous level LUTs are fed as inputs to the next level LUTs after interstage shuffling. Both the contents of the LUTs and the interstage shuffling can be customized by the users. This architecture implements a mapping between two n-bit vectors and can be used as the architecture for both $f_{original}$ and $f_{inverse}$. Note that $f_{original}$ and $f_{inverse}$ use a separate hardware implementation to realize two mappings of opposite directions.

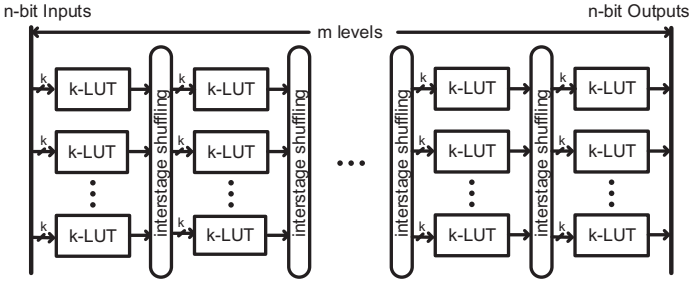


Fig. 1: Architecture of bidirectional bijective function.

A motivational example of $f_{original}$ and $f_{inverse}$, and their LUT implementations are shown in Figure 2. To simplify the description, we consider the mapping between two 3-bit vectors. Given the mapping of $f_{original}$, we use three 3-input LUTs for implementation. We use $x_0x_1x_2$ as inputs for each LUT, then based on the mapping, we allocate contents of the LUTs to each memory location. For example, in the

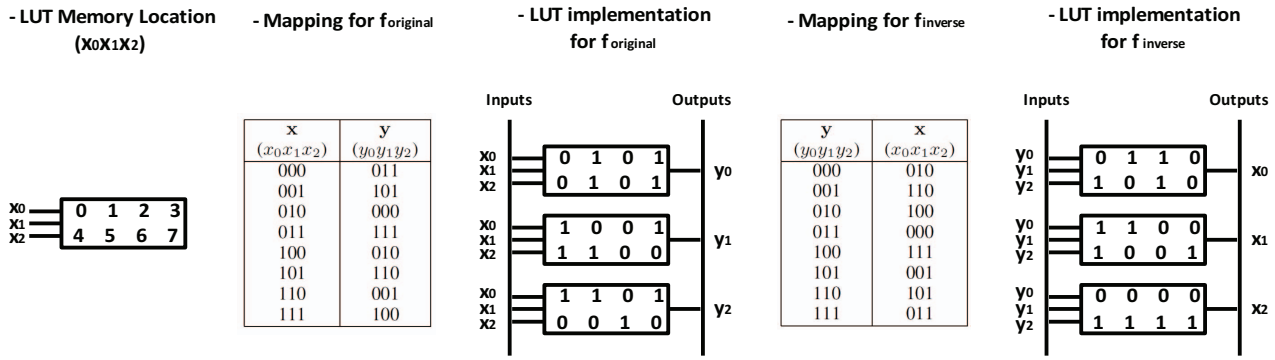


Fig. 2: An example mapping of $f_{original}$ and $f_{inverse}$, and their LUT implementations.

mapping shown in Figure 2, when given inputs as 100, the corresponding outputs are 010, thus, we assign $0, 1, 0$ to the memory location 4 of the three LUTs respectively. By repeatedly filling all the memory locations of the LUTs, a one-to-one mapping can be implemented. For $f_{inverse}$, exactly the same procedures can be followed. The inverse mapping and the implementation can be found in the last two figures in the motivational example.

There exist many Derivatives of the structure. For example, for each individual LUT, the order of the inputs does not have to be fixed. In the motivational example, instead of using $x_0x_1x_2$ as the inputs for all the LUTs, we can switch the inputs to be in any order of $x_0x_1x_2$ combination. When implementing the original mapping, the LUT locations to fill in the values need to be adjusted accordingly. As long as the derivatives can still keep the properties of one-to-one mapping, they can be applied.

B. Large Mapping Networks

The motivational example in Figure 2 shows the BBF with 3-bit inputs and 3-bit outputs. A key question is how to build a large-scale LUT network, for example, 128-bit inputs/outputs mapping. The idea is to connect the small scale mapping network both in parallel and in series. As for parallel connection, we can increase the number of LUTs as well as the number of inputs. For instance, we can duplicate the structure in the motivational example with a new set of 3-bit inputs and 3 more LUTs. If we put them in parallel, the system will become a 6-inputs/outputs system composed of six 3-input LUTs. However, using only one level of LUTs may make the structure easily breakable by the attackers. To increase Shannonś confusion and diffusion to this system, we connect m parallel LUTs in series. The structure can be formed by simply connecting the outputs of previous level LUTs to the inputs of next level LUTs after shuffling the interstage interconnections. It is necessary to determine the optimal levels (m value) of LUTs which can achieve good security with low power and area overhead. To do so, the output hamming distance of avalanche effect tests are carried out for different number of levels. The ideal case for 64-bit LUTs is 32 which indicates completely no correlation between the inputs and the outputs. The tests reveal that at least 9 levels are required to achieve good security in this architecture. The exponential connection possibilities between the LUTs enable the system to achieve excellent confusion and diffusion. Hence, $f_{original}$ and $f_{inverse}$ bijective functions are implemented using this architecture and its one-to-one mapping is maintained through appropriate constraint formulations.

In this work, BBF's $f_{original}$ and $f_{inverse}$ LUT-based architectures are assumed to be implemented in body sensor node and central data collecting node, respectively. The configuration of the LUTs interstage interconnection serve as a secret key. For convenience, the BBF $f_{original}$ and $f_{inverse}$ LUT-based architectures are called $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$, respectively. LUTC stands for lookup table cipher.

V. Protocols Design

In this section, authentication, encryption/decryption and data integrity check protocols are designed using the above LUT-based security architecture. Data freshness is also supported through the use of counter in both wearable body sensor node and the central sink node. In Figure 3, the block level implementation of the three protocols in the two communicating parties is shown. In WBSNs communicating parties authentication has to be performed at the start of the communication in order to check the trustworthiness of the involved nodes. The authentication process can be initiated from body sensor node or central data collecting node depending on the agreed communication protocol. Before responding to the command of the central data collecting node, the wearable node has to authenticate central node's legitimacy. Similarly, before starting to receive the sensed biosignal data the central sink node has to make sure the node's authenticity in order to avoid receiving data from malicious node which pretends to be a legitimate one. This helps to save the unnecessary energy waste due to processing of malicious command or data. The authentication protocol (Protocol 1) is presented below and it takes advantage of the respectively matched $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$ in sender and receiver nodes.

Generally, confidentiality is achieved by encrypting the data with a secret key that is known only by the intended receivers. In the proposed data encryption/decryption protocol (described below), after matching their LUTC, the sender uses its $LUTC_{BBFOrg}$ to encrypt the sensed biosignal message and the receiver uses its $LUTC_{BBFInv}$ to decrypt the received message. Message counter is used in both sender and receiver and the encrypted counter value is embedded in the message frame in order to prevent replay attack, see Figure 3. The

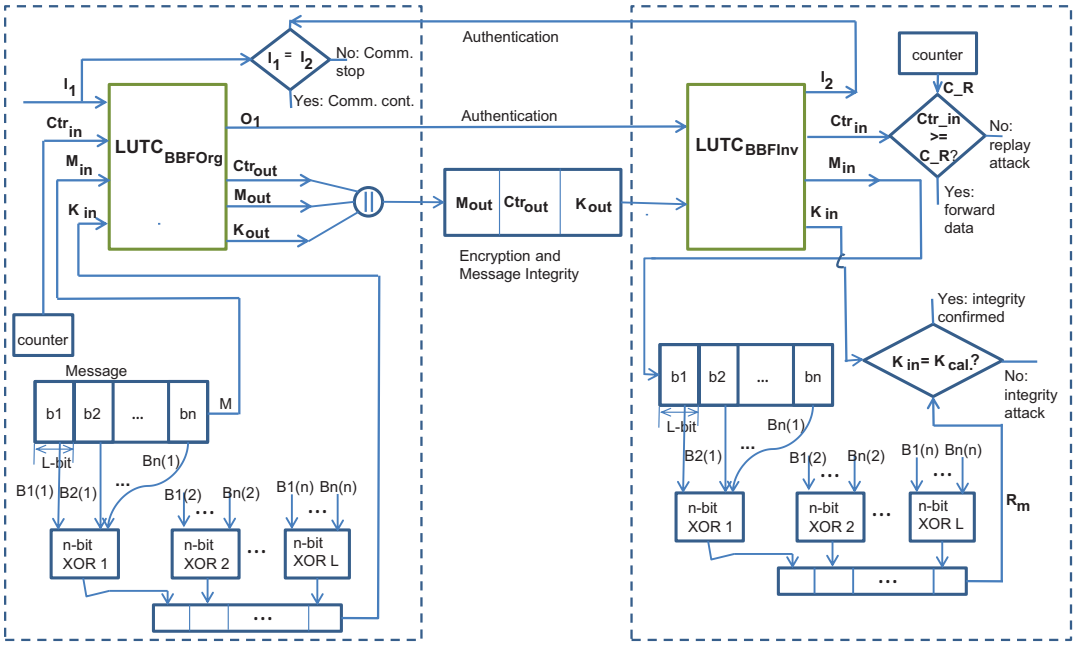


Fig. 3: Block diagram of Protocols Processing.

Protocol 1 Authentication

Authenticator: sensor1
Supplicant: sensor2

1: Sensor1 and sensor2 match their $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$.
2: Sensor1 chooses a random seed as input vector I_1 for $LUTC_{BBFOrg}$ and computes the corresponding output vector O_1.
3: Sensor1 sends O_1 to sensor2.
4: Sensor2 computes output vectorI_2 using the received O_1 and its matched$LUTC_{BBFInv}$.
5: Sensor2 sends I_2 to sensor1.
6: Sensor1 compares I_1 with I_2, only when $I_1 = I_2$, sensor1 authenticates sensor2.

Protocol 2 Encryption/Decryption and Data Freshness

Message sender: sensor1
Message receiver: sensor2

1: Sensor1 and sensor2 match $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$.
2: Sensor1 uses the message M_{in} and Ctr_{in} as input vector for $LUTC_{BBFOrg}$ and computes the corresponding output vector M_{out} and Ctr_{out}. Ctr_{in} is the message counter output.
3: Sensor1 sends M_{out} and Ctr_{out} to sensor2.
4: Sensor2 uses M_{out} and Ctr_{out} as input to $LUTC_{BBFInv}$ and retrieve M_{in} and Ctr_{in}.
5: Sensor2 compares the retrieved Ctr_{in} and its own counter value C_R. If Ctr_{in} is greater than or equal to C_R, the data freshness is confirmed. Otherwise, there is replay attack and data should be discarded.

receiver checks the decrypted counter value with its counter output. The received data freshness is confirmed if the two counter values are equal or the decrypted counter value is not less than the receiver's count.

Confidentiality alone cannot ensure a secure communication. Though the attackers are unable to access the content of an encrypted message, they still can flip some bits of the encrypted message in such a manner that its receiver will believe that the flipped message was the message originally sent. So, the purpose of message authentication schemes is to ensure data integrity and authenticity by means of a key-dependent authentication code of length n. The presence of a secret key assures that only authorized users are able to create and verify those codes. The code length is an important security parameter and should be chosen according to the presumed capabilities of the attackers as well as by taking into account the application requirements and communication overhead. In Protocol 3, message integrity check protocol using $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$ in sender and receiver nodes, respectively is presented. The sensed message in the sensor node is divided into n blocks where each block consists of L-bits data and one output from each block is XORed together as can be seen in Figure 3. The output of the XOR gates is concatenated together to form a vector. This vector is passed through the$LUTC_{BBFOrg}$ in the sender node and the output is the message integrity code (MIC). This MIC is appended to the encrypted message as a subpart of the frame which will be sent to the central data collecting node. The receiver uses the MIC it gets from the sender node, its $LUTC_{BBFInv}$ and XOR gates to check whether the data integrity is intact or not.

VI. Performance Comparison

IEEE 802.15 Task Group 6 proposes three security levels for body area networks, level 0 as first level with no security [18]. For level 1 only authentication and level 2 authentication along with encryption is recommended. It has been mentioned in the standard that the authentication and

Protocol 3 Message Integrity Check

Message sender: sensor1
Message receiver: sensor2

1: Sensor1 and sensor2 match $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$ and agree on the number of blocks (n) the message to be divided.
2: Sensor1 divides the message into n blocks with L-bits in each block. One output from each block is XORed together and concatenating the XORs output results in K_{in} which is an L-bit vector.
3: Sensor1 uses vector K_{in} as input to its $LUTC_{BBFOrg}$ and computes the corresponding output vector K_{out}, which is the message integrity code.
4: Sensor1 sends K_{out} to sensor2
5: Sensor2 receives K_{out} and uses it as input to its $LUTC_{BBFInv}$ and computes the output vector K_{in}.
6: Sensor2 uses the decrypted message in Protocol 2 and divides it into n blocks. Then XORed one output from each block and concatenating them results in R_m.
7: Sensor2 compares K_{in} and R_m, if they are equal then the integrity of the data is confirmed. If they are not equal, integrity violation is detected and the received message will be discarded instead of forwarding it to the remote server.

Design	Area (Slices)	Max. Delay (ns)	Clock Cycles	Block Size (bits)	Throughput (Mbps) at f_{max}
AES[19]	393	14.21	534	128	16.86
AES-CCM[20]	487	186	46	128	687
64-BBF	32	67.32	1	64	950.69
128-BBF	64	156.38	1	128	818.53

TABLE I: Comparisons of LUTC security-cipher with the conventional block ciphers.

encryption/decryption of the data in Level 2 can be done based on AES-128 CCM (counter mode for message encryption and cipher block chaining mode for message authentication). For the authentication only scheme in level 1, cipher block chaining mode has been suggested. The proposed bidirectional bijective function (BBF)-based cipher is tested on the Spartan-3 XC3S50-5 FPGA and results are generated by the Xilinx ISE Design Suite 14.3. Delay, area, and throughput of the BBF-based LUTC along with existing AES and AES-CCM implementations on the Spartan-3 XC3S50-5 are listed in Table I. The results show that the BBF-based LUTC achieved higher throughput and requires less area than the other two, making it a better alternative for WBSNs.

VII. Security Analysis

In this section, the security properties of the $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$ are analyzed using statistical model. Since $LUTC_{BBFOrg}$ and $LUTC_{BBFInv}$ are exact inverse of one another, carrying out the security analysis in one of them is sufficient.

A. Output Randomness

We quantify the statistical randomness of the $LUTC_{BBFOrg}$ outputs by applying the industry-standard statistical test suite of the National Institute of Standards and Technology (NIST). The outputs stream is generated as follows: configuration of $LUTC_{BBFOrg}$ is performed, a random seed is used as the primary inputs to the $LUTC_{BBF}$ and the corresponding outputs are generated. In each subsequent clock cycle, the outputs are XORed with the previous inputs to generate the inputs for the next clock cycle. We repeat the process until we collect enough outputs required by the benchmark suite. The pass rate for each test in NIST statistical test suite is shown in Table II. The results high scores confirms the excellent randomness in the output stream.

Statistical Test	Avg. Success Ratio
Frequency	100%
Block Frequency (m=128)	99.2%
Cusum-Forward	98.7%
Cusum-Reverse	98.9%
Runs	98.4%
Longest Runs of Ones	97.8%
Rank	99.4%
Spectral DFT	97.5%
Non-overlapping Templates ($m = 9$)	96.8%
Overlapping Templates ($m = 9$)	98.2%
Universal	100%
Approximate Entropy ($m = 8$)	98.2%
Rand. Excursions ($x = 1$)	98.1%
Rand. Excursions Variant ($x = -1$)	97.5%
Serial ($m = 16$)	98.1%
Linear Complexity ($M = 500$)	99.1%

TABLE II: The average success ratio for the NIST statistical test suite. 1000 bitstreams of 10000 bits are passed to each test. The test passes for p-value$\geq \sigma$, where σ is 0.01.

B. Avalanche Effect

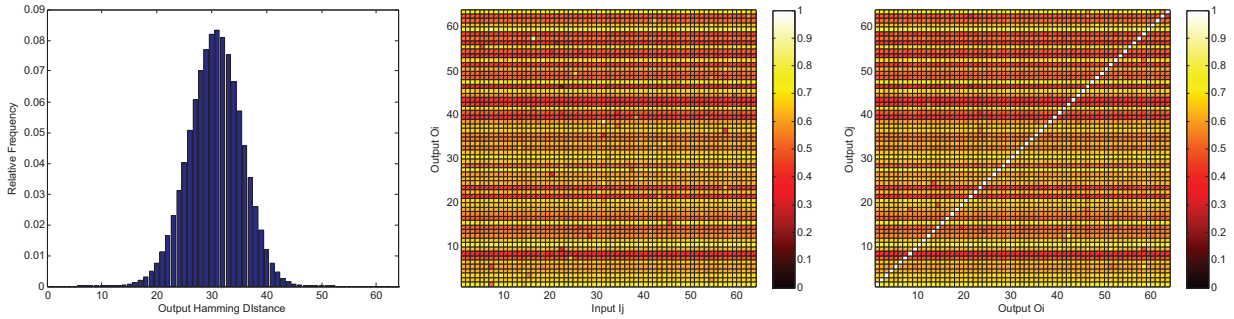
In this attack, the attacker tries to predict outputs using knowledge of the outputs for similar inputs. This attack is dangerous when output vectors with similar input vectors are highly correlated with one another. To test this, we used 32 levels 64-bit LUTC and analyze the hamming distance between output vectors by changing one bit of the input vectors at each iteration. Ideally, the distribution should be in the form of a binomial distribution with the peak at half of the number of output bits, thus indicating that the avalanche effect is achieved. The result in Figure 4a shows an almost perfect binomial distribution which indicates our matched device is highly resilient against this type of attack.

C. Input-Output Correlation

Another type of attack is the one which attempts to build correlation mappings between an output bit, O_i, and an input bit, I_j. The goal in this attack is to predict the conditional probability, $P(O_i = c_1|I_j = c_2)$, where c_1 and c_2 are either 1 or 0. For example, if the attacker observes that output O_i is equal to 1 for most of the time when the input I_j is 1, then he/she can guess with a high probability that output O_i is 1 when I_j happens to be 1. The ideal situation is when the probabilities remain 0.5. The conditional probability $P(O_i = 1|I_j = 1)$ for 32 levels 64-bit LUTC is shown in Figure 4b. Majority of the probability results are around 0.5, proving the strength of the cipher to this type of attack.

D. Output-based Correlation

Similar to the previously described attack, this attack attempts to predict an output bit O_i according to the value



(a) (b) (c)

Fig. 4: (a) Distribution of output hamming distances in testing the avalanche effect, (b) Conditional probabilities between output bits O_i and input bits I_j, (c) Conditional probabilities between output bits O_i and output bits O_j.

of a corresponding output bit O_j. In this case, if two output bits have a strong correlation, then the attacker can deduce the output vector by knowing a subset of the output bits. We present a conditional probability map of $P(O_i = 1|O_j = 1)$ in Figure 4c depicting the low potential for prediction based on output to output correlation.

VIII. Conclusion

We have developed lightweight hardware security primitive for wireless body sensor networks by following bidirectional bijective function principle. The one-to-one input-output mapping of the function was realized using a network of lookup tables (LUTs) with exponential interstage interconnection possibility between consecutive levels of LUTs. The security primitive has passed all NIST randomness tests and its viability for relevant attacks has been confirmed through statistical analysis. In addition, authentication, encryption/decryption, and message integrity protocols were developed based on the presented lightweight security primitive. The performance comparison with AES and AES-CCM showed the superiority of the proposed security primitive in terms of throughput and area.

References

[1] J. Caldeira, J. Rodrigues, and P. Lorenz, "Toward ubiquitous mobility solutions for body sensor networks on healthcare," *Communications Magazine, IEEE*, vol. 50, no. 5, pp. 108–115, 2012.

[2] R. C. King, D. G. McIlwraith, B. Lo, J. Pansiot, A. H. McGregor, and G.-Z. Yang, "Body sensor networks for monitoring rowing technique," in *Wearable and Implantable Body Sensor Networks, 2009. BSN 2009. Sixth International Workshop on*. IEEE, 2009, pp. 251–255.

[3] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. Ko, J. H. Lim, A. Terzis, A. Watt, J. Jeng, B.-r. Chen *et al.*, "Wireless medical sensor networks in emergency response: Implementation and pilot results," in *Technologies for Homeland Security, 2008 IEEE Conference on*. IEEE, 2008, pp. 187–192.

[4] P. Hanley, P. Fergus, and F. Bouhafs, "A wireless body sensor platform to detect progressive deterioration in musculoskeletal systems," 2013.

[5] Y. Fu, D. Ayyagari, and N. Colquitt, "Pulmonary disease management system with distributed wearable sensors," in *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*. IEEE, 2009, pp. 773–776.

[6] F. Rincón, P. R. Grassi, N. Khaled, D. Atienza, and D. Sciuto, "Automated real-time atrial fibrillation detection on a wearable wireless sensor platform," in *Engineering in Medicine and Biology Society (EMBC), 2012 Annual International Conference of the IEEE*. IEEE, 2012, pp. 2472–2475.

[7] Z. Paral and S. Devadas, "Reliable and efficient puf-based key generation using pattern matching," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, June 2011, pp. 128–133.

[8] M. Bhargava and K. Mai, "An efficient reliable puf-based cryptographic key generator in 65nm cmos," in *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, March 2014, pp. 1–6.

[9] T. Xu and M. Potkonjak, "Lightweight digital hardware random number generators," in *SENSORS, 2013 IEEE*, Nov 2013, pp. 1–4.

[10] P. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini, "Efficient and practical authentication of puf-based rfid tags in supply chains," in *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, June 2010, pp. 182–188.

[11] J. B. W. Teng Xu and M. Potkonjak, "Matched digital pufs for low power security in implantable medical devices," in *IEEE International Conference on Healthcare Informatics*, Sept 2014, pp. 1–6.

[12] F. Miao, S.-D. Bao, and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security," *Information Security, IET*, vol. 7, no. 2, pp. 87–96, June 2013.

[13] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on*, June 2010, pp. 98–103.

[14] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 13, no. 10, pp. 1200–1205, 2005.

[15] A.-R. Sadeghi and D. Naccache, Eds. New York, NY, USA: Springer-Verlag New York, Inc., 2010.

[16] M. Potkonjak, S. Meguerdichian, and J. L. Wong, "Trusted sensors and remote sensing," in *Sensors, 2010 IEEE*. IEEE, 2010, pp. 1104–1107.

[17] J. B. Wendt and M. Potkonjak, "Nanotechnology-based trusted remote sensing," in *Sensors, 2011 IEEE*. IEEE, 2011, pp. 1213–1216.

[18] "Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks," *IEEE Std* 802.15.6 – 2012, pp. 1–271, Feb 2012.

[19] P. Yalla and J.-P. Kaps, "Lightweight cryptography for fpgas," in *Reconfigurable Computing and FPGAs, 2009. ReConFig'09. International Conference on*. IEEE, 2009, pp. 225–230.

[20] A. Aziz and N. Ikram, "An fpga-based aes-ccm crypto core for ieee 802.11 i architecture." *IJ Network Security*, vol. 5, no. 2, pp. 224–232, 2007.