Survey on Lightweight Primitives and Protocols for RFID in Wireless Sensor Networks

Manjulata, Adarsh Kumar

Department of Comp. Sc. Engg. and Info. Tech., Jaypee Institute of Information Technology, Noida, India
lata.manju25@gmail.com, adarsh.kumar@jiit.ac.in

Abstract**:** The use of radio frequency identification (RFID) technologies is becoming widespread in all kind of wireless network-based applications. As expected, applications based on sensor networks, ad-hoc or mobile ad hoc networks (MANETs) can be highly benefited from the adoption of RFID solutions. There is a strong need to employ lightweight cryptographic primitives for many security applications because of the tight cost and constrained resource requirement of sensor based networks. This paper mainly focuses on the security analysis of lightweight protocols and algorithms proposed for the security of RFID systems. A large number of research solutions have been proposed to implement lightweight cryptographic primitives and protocols in sensor and RFID integration based resource constraint networks. In this work, an overview of the currently discussed lightweight primitives and their attributes has been done. These primitives and protocols have been compared based on gate equivalents (GEs), power, technology, strengths, weaknesses and attacks. Further, an integration of primitives and protocols is compared with the possibilities of their applications in practical scenarios.

Keywords**:** Cryptography, Lightweight, Primitives, Protocols, RFID.

1. Introduction

RFID with its applications in inventory management, object identification, and tracking large scale data management etc. makes it interesting for common purpose use. It is also having low cost platform that provide ubiquitous acceptance for its use. RFID network identifies, locates and tracks objects, people, and animals etc. using radio frequency (RF) through tags and readers. Tags are small memory devices with limited storage capacity. This memory storage unit stores identification types and other specifications of objects. This data size is limited to 2-3 Kilobytes (KB) only. Tags are classified into two categories: active and passive. Active tags are costly devices enabled with own transmitting and battery source as compared to passive tags. Passive tags are low cost devices without any battery source. Power to operate or transmit is collected from destination through electromagnetic waves. Active tags are having longer transmitting range thus preferred to identify objects over long distances such as road side units in traffic management, health care applications, animal tracking, object locating in logistics markets etc. Another type of tag is semi-passive tag which is having own battery source to operate but consumes destination energy for communication. Like active tags, semi-passive tags are also costlier [1]. Readers are the devices to read tags for object identification and record management. Readers scan the objects and store information in back end systems. Information in back end system is communicated to other devices for increasing the availability of data. Range of data availability is a major challenge in RFID networks. Wireless sensor devices can be integrated with RFID devices to increase availability of data range [1].

Integration of small sensor devices with wireless, sensing, computing and communication capabilities to RFID devices are having many applications. For example, monitoring and diagnosing deceases in healthcare system, analyzing the physical structural change in objects, analyzing and evaluating the problems in real life such as home entertainment, integration of social network devices etc. [2]. Both RFID and sensor networks are pervasive environments. Integration of these two pervasive computing environment results to reliable energy efficient, survivable and cost effective solutions for various applications. For example, the information can be easily collected from multiple RFID tags spread over a large area by integrating RFID reader to sensor device. Readers are capable of reading multiple RFID tags and pass the required information to backend systems. Backend systems can be accessed for analyzing, record management, processing etc. RFID and sensor device integration increases the range and availability of data.

RFID-sensor node integration can be performed through different ways. In [3], four types of integration are proposed: (i) tags attached to sensor devices and communicate with reader, (ii) reader attached to sensor device, (iii) mixed architecture and (iv) tags communicate themselves. Now, tags are integrated with sensor devices and reader can scan tags for information gathering. When readers are used to scan tags, analog signal of sensor devices is converted to digital signal and this signal data is forwarded to readers. These readers may use infrastructure or infrastructure-less networks for processing and storing information in backend systems. Now, tags could be active, passive or semi-passive. In [4][5], passive tags based environmental sensing and reader scanning system is discussed. This passive tag operates in 13.56 MHz, reads up to 200 millimeters, size of 20mmx10mm and cost around 5 pounds each. In [6], 0.25µm CMOS fabricated with 0.6 mmx0.7mm chip size passive tags on 860-960MHz external power ISM band and RF signals is studied and designed. In [7], 90x60x4 mm and 60x25x4 mm sizes for 900 MHz and 2.45 GHz bands are developed. Response time for these tags can be achieved from 9 meter to 30 meters. In [8][9], Wireless Identification and Sensing Platform (WISP) with sensing and computational capabilities is designed. WISP is battery free sensors that scavenge energy from readers and give response up to 8 metres. WISP operates on a wireless channel and provides bidirectional communication. According to Liu *et. al.* [10], major challenges in passive tag scenario are designing of ultra low

power integrated circuits, antenna design for improving the signal range, protocol design for power improvement etc. In [11][12], various security attacks on passive tags are explored like: sniffing, tracking, spoofing, replay, Denial of Service (DoS) attack etc.

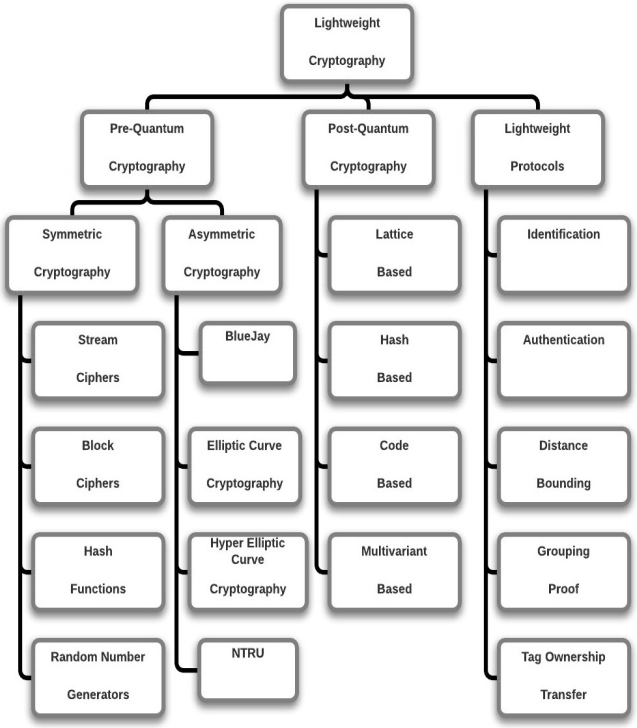

Figure 1. Classification of lightweight cryptography

Both RFID and sensor devices are resource constraint devices with limited computational, stringent processing, storage and communication capabilities. Hence, sending aggregated and secure data with minimum energy is a major challenge. In [13], security issues in an integrated environment are discussed. This includes attacks and their remedies. Security threats in WSNs and RFID integrated networks are: capturing microcontroller, memory or fabricating complete sensor node, jamming at physical layer, collisions of packets and exhaustion of node's battery through retransmission at data link layer, spoofing-replaying-altering data packets or wormhole, Sybil and sinkhole attacks at network layer, misled sensor nodes in localization protocols, adversary attack over energy saving aggregated nodes, masquerading or manipulation in timing messages of time synchronization protocol etc. Among other attacks, tag spoofing and cloning is also feasible in RFIDs [14][15]. Various defence mechanisms are designed to protect integrated nodes from these attacks. These defences aim to protect the system through cryptographic primitives and protocols [16]. Cryptography primitives include confidentiality, integrity, authentication, non-repudiation and availability. Cryptographic protocols include identification, authentication, grouping, distance bounding, ownership transfer etc. Since there is scarcity of resources among these pervasive environments thus lightweight cryptographic primitives and protocols are required to be designed. Lightweight means lesser number of gate equivalents (GE). GE is a ratio of total number of logical gates used to number of NAND gates. In resource constraint networks mechanisms with minimum number of GE and with strong protection against attacks is preferred. According to Moore's law 30-40% of total GEs are reserved for security purposes. This figure is expected to be increased with advancement of technology [17]. Lightweight Cryptography can be classified as: Pre-Quantum Cryptography and Post Quantum Cryptography. Term pre-quantum cryptography is used to classify the cryptography aspects that can be broken using quantum computers and post-quantum cryptography aspects cannot be broken using quantum computers. Figure1 shows the classification of lightweight cryptography aspects.

In this work, section 2 shows pre-quantum lightweight cryptography primitives. Section 3 presents pre-quantum lightweight cryptography protocols. Post-quantum lightweight cryptography aspects are discussed in section 4. Section 5 analyzes the possible combinations of lightweight primitives for protocols to provide secure network environment with consumption of atmost 30% of hardware resources. Finally, conclusion is drawn in section 6.

2. Pre-Quantum Lightweight Cryptography Primitives

As shown in figure1, this type of cryptography is broadly classified as: lightweight primitives and lightweight protocols [16]. Lightweight cryptographic primitives provide confidentiality, integrity, authentication, non-repudiation and availability. These terms are explained as follows:

-Confidentiality: protecting data from being accessed by changing its form for example, protection from impersonation, masquerading etc.

-Integrity: mechanism to check data correction at destination for example, Message Authentication Code (MAC).

-Authentication: provide collision resistant, compression, integrity characteristics with integration to other cryptographic mechanisms.

-Non-Repudiation: ensuring that sender is the originator of message.

-Availability: nodes should be available for communication for example, protection from Denial of Service (Dos) attack etc.

Lightweight primitives are largely classified into symmetric and asymmetric primitives. These primitives are explained as follows:

2.1 Symmetric Primitives

In these primitives same key is used at both ends for encryption and decryption. As shown in figure1, this type of mechanisms can be classified as: stream, block, pseudo random number generation and hashing. Various lightweight mechanisms under this category are explained as follows:

2.1.1 Stream Ciphers

In stream ciphers a continuous stream of bits/numbers/strings is generated with the help of initialized vector and key. Some mathematical operations are then performed to generate cipher text from plain text with the use of key and initialized vector. GE for lightweight stream cipher varies from 300 to 18,819. Lightweight stream ciphers are preferred over block ciphers

because of compact size, less time complexity etc. These mechanisms are used with pseudo random number generator and hashing mechanism to provide cryptographic services. Characteristics of well known lightweight stream ciphers are explained as follows:

A2U2: David *et al.* proposed this mechanism in 2011 [18]. Strengths of this mechanism are: (a) provides high throughput (1 bit per clock cycle), (b) requires very less number of GE and (c) compactness and simple computational operations make it well suited for RFID devices. Weakness: Qi Chai found that it easy to recover secret key of A2U2.

Enocoro: Watanabe *et al.* proposed this stream cipher in 2007. Various versions of this cipher are: Enocoro-80 and Enocoro-128v2. Enocoro-80 and Enocoro-128v2 are having key length of 80 bits and 128 bits respectively. Strengths: (a) 128 bit key length cipher (Enocoro-128v2) provides very good resistance against majority of attacks and (b) very low implementation cost make it preferable over other ciphers [19].

MICKEY: Babbage *et al.* proposed Mutual Irregular Clocking KEYstream generator (MICKEY) [20]. MICKEY 1.0 was proposed in 2005 and MICKEY 2.0 was proposed in 2006. MICKEY has low complexity and strong security. Strength: Protects from any attack faster than exhaustive key search.

Salsa20: Bernstein *et al.* designed this family of stream ciphers in 2005 [21]. This family of stream ciphers is well suited for the applications where speed is more important than confidence. Weaknesses: (a) Crowley discovered 2^{165} –operation attack on Salsa20/5 and (b) Hongjun Wu applied related cipher-attack on Salsa20 in 2012.

Trivium: Canniere *et al.* proposed this stream cipher in 2005 [22]. Strength: well suited for applications which require a flexible hardware implementation. Weaknesses: (a) Correlations guess & determine attacks and (b) algebraic attacks and resynchronization attacks are possible in some scenarios [22].

Grain: Hell *et al.* proposed this lightweight stream cipher in 2004 [23]. Various versions of Grain are Grain version 0.0, Grain version 1.0, Grain-128 and Grain-128a. Strengths: (a) it is a bit oriented stream cipher and (b) throughput varies from one bit per clock to sixteen bits per clock. Weakness: Attacks like algebraic, time, memory, data trade-off, fault etc. are possible.

SOSEMANUK: Berbain *et al.* developed this mechanism in 2008 [24]. It has variable key length which can vary between 128 and 256 bits. Strengths: (a) high throughput, (b) require reduced amount of static data and (c) reduced internal state size.

Table 1. Stream Ciphers and its characteristics

Algorithm	GE	Technology
A2U2	<300	0.13
Grain v1	1,294 2,200	0.13 0.13
Enocoro v.2	2,700	0.18
Trivium	2,599 2,800	0.13 0.13
MICKEY2(88)	3,188	0.13
MICKEY128	5,039	0.13
Salsa20	10,000	0.18
SOSEMANUK	18,819	0.13

Comparison: Table 1 shows the comparative analysis of various stream ciphers. It shows that most of ciphers are compared over 0.13µm technology. A2U2 is having minimum GE and SOSEMANUK is having maximum. Thus A2U2 is preferable choice for resource constraint networks.

2.1.2 Block Cipher

Instead of bit, a block is encrypted with symmetric or asymmetric key. Well known symmetric key mechanisms are: Advanced Encryption Standard (AES), Data Encryption Standard (DES) etc. These block ciphers are not acceptable for resource constraint devices due to high computational and hardware requirements. This work provides brief description of twelve block ciphers: LED[25][26], KLEIN[27][28], PICCOLO[29], LBLOCK[30], PRINT[31][32], KATAN/KATANTAN[33], CLEFIA[34], PRESENT[35][36], HIGHT[37][38], SEA[39], mCRYPTON[35], AES[40]. Details can be referred in original literature.

LED: Guo *et al.* proposed this cipher in 2011. Strengths of this cipher are: (a) two variants of key length: 64-bits and 128-bits, (b) secure against meet-in-the-middle attack, (c) 64-bit key uses 32 rounds and 128-bit key uses 48 rounds of AddConstants, SubCells, ShiftRows, and MixColumnsSerial operations and (d) it is nibble-oriented block cipher with an MDS P-layer. Weakness: Not secure against related-key and single-key attacks [26].

KLEIN: Gong *et al.* proposed this block cipher in 2011. Strengths: (a) block size of 64, 80 and 96-bits with key length of 64, 80 and 96 bits are used, (b) it is possible to implement it in lightweight manner with both hardware and software, (c) KLEIN is resistant to related-key attacks, agility of the keys and side-channel attacks, (d) SubNibbles, RotateNibbles, MixNibbles and AddRoundKey are the major operations used in this cipher, (e) it is nibble oriented block cipher with MDS S-layer and P-layer over GF(2^8) and (f) 64, 80 and 96-bit cipher uses 12, 16 and 20 rounds of operations respectively. Weakness: Not secure against key-recovery integral attack [28].

Piccolo**:** Shibutani *et al.* proposed this block cipher in 2011 [29]. Strengths: (a) block size of 64-bits and key length of 80 and 128 bits are used, (b) protected from Meet-in-the-Middle and related-key attacks and (c) it is energy efficient protocol and achieves good performance.

LBlock: Wenling Wu *et al.* proposed this block cipher in 2011 [30]. Strengths: (a) block size of 64-bits and key size of 80-bits is used, (b) it is implementation efficient on both hardware and software platforms and (c) protected from differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis, and related key attacks etc.

PRINT: Lars Knudsen proposed this cipher in 2010. Strengths: (a) block size of 48-bits and 96-bits are used and (b) it is based on sequential permutation network. Weakness: Invariant coset attack is possible [31].

KATAN/KTANTAN: Canniere *et al.* designed this block cipher in 2009 [33]. Strengths: (a) more hardware oriented, (b) block size of 32, 48 and 64-bits and key length of 80-bits are used and (c) secure against related-key, differential and algebraic attacks.

CLEFIA: Taizo Shirai *et al.* proposed this block cipher in 2007 [34]. Strengths: (a) it is a 128 bit block cipher, (b) proven to be highly secure and efficient and (c) over low cost, resource constraint devices; it provides protection against various attacks like: differential, linear and saturation cryptanalysis.

PRESENT: Bogdanov *et al.* proposed this block cipher in 2007. Strengths: (a) based on sequential permutation network, (b) block length of 64 bits and key length of 80 and 128 bits are used and (c) 80-bits key length has very low GE and high throughput. Weakness: Affected by related key rectangle attack [35].

HIGHT: Hong *et al.* proposed this block cipher in 2006. Strengths are: (a) block length: 64-bits and key length: 128-bits

are used, (b) provides high security and lightweight implementation and (c) it is an ultra-lightweight stream cipher for low cost, low power and resource constraint devices. Weakness: Possible attacks on this cipher are: impossible, differential and related key rectangle attacks [37].

SEA: Standaert *et al.* designed this mechanism in 2006 [39]. Strengths: (a) designed for small embedded applications, (b) common in image encryption for example, JPEG2000 images, (c) integration of encryption and decryption mechanisms over single resource constraint device provides less implementation complexity, (d) protected from various attacks like: linear and differential and (e) implementation design is very simple.

mCRYPTON: Lim and Korkishko proposed this mechanism in 2005. Strengths: (a) 64-bits block size is used, (b) three different key sizes: 64 bits, 96 bits and 128 bits are used and (c) it is considered to be good cipher for low cost, resource constraint RFID tags and devices. Weakness: It is found that related key rectangle attack is possible over 128 bits key length with 8-rounds of encryption [35].

Table 2. Block Ciphers and its characteristics

Algorithm	Area (GE)	Mean Power (µW)	Technology (µm)
PRINT	402	2.6 @ 100 kHz	0.18
Piccolo	616	-	0.13
KTANTAN	688	0.292	0.13
KATAN	1,054	0.555	0.13
KLEIN	1,220	-	0.18
LBlock	1,320	-	0.18
SEA(93 rounds)	1,333	3.22 @ 100 kHz	0.13
PRESENT-80 (4 bits)	1,650 1,075	3.86 @ 100 kHz 2.52 @ 100 kHz	0.18 0.18
LED	1,872	-	0.18
mCRYPTON	2,500	-	0.13
HIGHT	3,048	-	0.25
AES-optimized	3,400	4.5 @ 100 kHz	0.35
CLEFIA	4,950	-	0.09

AES: Joan Daemen and Vincent Rijmen proposed this block cipher in 1998 [40]. Strengths: (a) block size is 128 bits, (b) key lengths used in this cipher are: 128, 192 or 256 bits, (c) provide good amount of security and (d) less implementation complexity. Weaknesses: (a) various attacks possible over this mechanism are: side channel, timing attacks, (b) GE used is comparatively very high and (c) heavy algorithm as compared to other block ciphers.

Table 2 shows the block ciphers and their characteristics. PRINT block cipher is having minimum GE thus it is more hardware preferable choice for MANETs. In some cases, GE increases with increase in number of encryption rounds. Security of these block ciphers also varies with encryption rounds.

2.1.3 Hash Functions

A hash function is a mechanism that can be integrated with digital signature or message authentication code (MAC). It provides collision resistance, efficiency, and compression etc. characteristics. Various lightweight hashing mechanisms are as follows:

Keccak: Bertoni *et al.* designed this hash-function and was selected by NIST in 2012 [41]. Strengths: (a) it is based on "sponge" construction, (b) it can accept input and output in infinite amount and (c) flexible and secure against generic attacks.

Photon: Guo *et al.* designed this mechanism in 2011 [42]. Strengths: (a) various instances of Photon are: Photon-80/20/16, Photon-128/16/16, Photon-160/36/36, Photon-224/32/32 and Photon-256/32/32, (b) strong against: differential and linear cryptanalysis and (c) it is good in terms of lesser no of GE, throughput and performance trade-offs.

Spongent: Bogdanov *et al.* proposed this mechanism in 2011 [43]. Strengths: (a) various instances of output generated by this block cipher are: 88, 128, 160, 224 and 256 bits and (b) secure against collision, preimage and second preimage.

Quark: Aumasson *et al.* designed this mechanism and presented at CHES conference in 2010 [44]. Strengths: (a) based on "sponge" construction, (b) sponge construction reduces area and power consumption, (c) three instances of Quark are: D-Quark, U-Quark and S-Quark and (d) protected from collision, second preimage, length extensions, multicollisions etc.

ARMADILLO: Badel *et al.* proposed this mechanism in 2010. Strengths: (a) two versions of this mechanism are: ARMADILLO1 and ARMADILLO2, (b) provides secure authentication in a challenge-response protocol. Weakness: Attack on secret key is possible in polynomial time [45].

Table 3 shows various lightweight hashing mechanisms with power consumption and technology values. Spongent is an efficient hash function for MANETs. Strong points of these functions are dependent on image resistant characteristics: first pre-image, second pre-image and collision resistant.

Table 3. Hash functions and its characteristics

Algorithm	Area (GE)	Mean Power (µW)	Technology (µm)
Spongent	738	1.57	0.13
Photon-80	865	1.59	0.18
Keccak	1,300	-	0.13
U-Quark	1,379	2.96	018
D-Quark	1,702	3.95	0.18
S-Quark	2,296	5.53	-
Armadillo2-A	2,923	44	-
Armadillo-A	3,972	69	-
Armadillo2-B	4,353	65	-
Armadillo2-C	5,406	83	-
Armadillo2-D	6,554	102	-
Armadillo-B	6,598	117	-
Armadillo-C	8,231	146	-
Armadillo-D	8,650	177	-
Armadillo2-E	8,653	137	-
Armadillo-E	13,344	228	-

2.1.4. Random Number Generators

Random numbers generator (RNG) or pseudo random number generator (PRNG) is a mechanism for generating random number with provided seed. RNG and PRNG are having applications in various areas like: stream cipher, block cipher, key generation, initial vectors etc. Various lightweight RNG are as follows:

Mandal *et al.*: This scheme was proposed by Mandal *et al.* in 2011 [46]. It is NLFSR (Non-Linear Feedback Shift Register) based PRNG. It requires 36 clock cycles for key initialization and 80 clock cycles for running phase. Strengths: (a) used for securing tag identification protocols and (b) suitable for EPC Class 1 Generation 2.

Multiple-Polynomial LFSR based PRNG: Melia-Segui proposed this mechanism for EPC Gen2 RFID Tags in 2011 [47]. It is configured with multiple feedback polynomials and is based on a linear feedback shift register (LFSR). Strengths: (a) simple hardware implementation, (b) satisfy the randomness requirements of EPC Gen2 standard and (c) simple design.

AKARI: Martin, H. *et al.* proposed this scheme in 2011 [48]. Strengths: (a) two variants of AKARI are: AKARI-1 and AKARI-2, (b) improves the reliability and security of the system.

Ultra-lightweight TRNG: Wu *et al.* proposed ultra-lightweight true random number generators (TRNGs) in 2010 [49]. These are based on the concept that the resulting state may be random, when a circuit switches from a metastable state to a bi-stable state. Strengths: (a) low hardware cost and (b) most lightweight TRNGs.

LAMED: Peris *et al.* proposed this mechanism in 2009 [50]. Strengths: (a) realistic approach for low cost RFID tags, (b) output of LAMED succeeded in all randomness tests, (c) can be implemented with less number of gates, (d) provides 17.2 kbps throughput and (e) operations used can be easily implemented in hardware.

Naor-Reingold Pseudorandom Function: Naor *et al.* described this pseudorandom function in 1997 [51]. Strengths: (a) efficient for cryptographic primitives, (b) simple algebraic structure of the functions and (c) more efficient than other previous proposals.

ISAAC (Indirection, Shift, Accumulate, Add and count): This cryptographically secure PRNG was designed by Robert J. Jenkins Jr. in 1996 [52]. Strengths: (a) very fast on 32-bit computers, (b) less biased and (c) useful as a stream cipher for simulation. Weaknesses: (a) Marina Pudovkina recovered the initial state in 2001 and (b) Jean-Philippe Aumasson discovered different sets of weak states in 2006.

Blum Blum Shub (B. B. S.): Blum *et al.* proposed this pseudo random number generator in 1986 [53]. It is as secure as RSA encryption. Weaknesses: (a) not good for simulations and (b) very slow.

Table 4 shows the analysis of various lightweight RNG. AKARI-1 is having minimum GE and it is preferable choice for lightweight implementation. TRNGs serve as the core part of IT security because virtually any security application relies on unpredictable numbers. Naor-Reingold function can be used as the basis of symmetric encryption, authentication and digital signatures. ISAAC random number generator can be used more efficiently for simulation purpose as compared to Blum Blum Shub PRNG.

Table 4. Random Number Generators and its characteristics [16]

Algorithm	Area (GE)	Technology (µm)
Multiple-Polynomial LFSR based PRNG	453	-
AKARI-1	476	009
AKARI-2	824	-
Mandal *et al.*	1,242	-
LAMED	1,566	-

2.2 Asymmetric Primitives

In this mechanism a public and a private key is used to encrypt and decrypt message. In practice public key is used for encryption and the encrypted message is then decrypted by the corresponding private key. The various asymmetric mechanisms are explained as follows:

2.2.1 BlueJay

Markku-Juhani O. Saarinen proposed this mechanism in 2012 [54]. Strengths: (a) well suited for ultra-lightweight platforms such as microsensors and RFID tags, (b) faster than RSA and ECC and require less number of GEs, (c) hardware implementation requires very less gate equivalents, (d) it is the integration of Hummingbird-2 algorithm and Passerine, (e) it is based on the Rabin cryptosystem and (f) hard to break.

2.2.2 NTRU

Jeffrey Hoffstein *et al.* founded this asymmetric primitive in 1996 [55] and then it was approved for standardization in 2009 by IEEE. Strengths: (a) faster key generation, (b) "disposable" keys are allowed for use and thus reduce cost, (c) less memory usage allows it to use in mobile devices and smart-cards and (d) it is a lattice based cryptosystem.

2.2.3 HECC

Koblitz proposed hyper elliptic curve cryptography in 1989. Strengths: (a) provides security against adaptive chosen cipher text attacks and (b) short operand size make it suitable for real world applications in which memory and computing power is constrained [56].

2.2.4 ECC

Victor Miller *et al.* proposed elliptic curve cryptography (ECC) in 1985 [57]. Strengths: (a) smaller key sizes and greater flexibility, (b) provides high speed and require less storage which makes it to be useful in smart cards, cellular phones, pagers etc. and (c) mainly used in key exchange, digital signature authentication etc.

Table 5. Asymmetric Primitives and its characteristics

Algorithm	Area (GE)	Technology (µm)
BlueJay	≤3,000	0.18
NTRU	3,000	018
ECC	8,104	0.18
HECC	14,500	0.13

Table 5 shows the comparative analysis of asymmetric protocols. Among these protocols BlueJay is having least GE. As shown in table 1, table 2 and table 3, Symmetric ciphers are having minimum GE as compared to asymmetric. Symmetric ciphers are preferred over asymmetric in terms of speed but asymmetric ciphers are used to provide high security.

3. Pre-Quantum Lightweight Cryptography Protocols

As shown in figure 1 lightweight protocols can be classified into five major categories such as: identification, authentication, distance bounding, grouping proof and tag ownership transfer protocol. Lightweight protocols provide properties like identification, authentication etc. by using lightweight primitives.

Table 6. Identification Protocols and its characteristics

Protocols	Characteristics and Attacks
Alomair *et al.*'s Protocol	Identification efficiency is improved by utilizing available resources in RFID systems.
Non-Cryptographic Approach	• Require O(N) space for storing tag information at server side. • Low computational overhead. • Attack: DoS attacks.
Cimato's Lightweight Protocol	• It is based on skip lists. • Supports dynamic identification of tags. • Attack: Desynchronization between the reader and the tag. However this problem can be ignored.
HQT Protocol	• The number of collisions between tags is reduced by using 4-ary query tree instead of a binary query tree. • Slotted backoff mechanism reduces idle cycles.
VEDFSA Algorithm	During the whole reading process, the group will change dynamically to improve the group solution of the algorithm.
IQT Protocol	Improved tag read efficiency in RFID systems.
DFSA using Fast Tag Estimation Method	• Better performance regardless of the number of tags. • Reader identifies more tags with shorter time.
Tree Slotted Aloha Protocol	If collision occurs in a slot then next identification request will be broadcast to only those tags which collided in that slot by the reader.
ABS Protocol	Collision-free time slots are assigned by timeslot allocation procedure and unnecessary timeslots are removed by empty timeslot elimination procedure.
EDFSA ALOHA Algorithm	• Anti-collision algorithm. • In case of 1000 number of tags, EDFS improves the slot efficiency by 85~100% compared to the conventional approaches.
Myung *et al.*'s Protocol	Prefixes are used to reduce identification delay and to avoid collisions.
Henrici and Muller's Protocol	• Uses one-way hash functions. • Attack: Desynchronizing the system's database, traceability and corruption of hash value send by reader.
Jolle, Jakobsson, Jules and Syverson's Protocol	• Based on the concept of universal encryption. • Attacks: Tracking, attack based upon interception, attack based on eavesdropping and attack based on invariants.
Saito, Ryau and Sakurai's Protocol	• With a check protocol: • Aim: Detect an attacker sending a wrong re-encrypted identifier. • With a one-time pad protocol: based on universal re-encryption. • Attacks: Attack based upon random values, desynchroniztion.
Juel's Protocol based upon XOR	• An attacker can completely destroy the mechanism. • Attack: Tag detectable, desynchronization.

3.1 Identification Protocols

In RFID systems, the reader acquires tag's identity by using identification protocol. Unique identification numbers are generated using random number generation techniques and are assigned to nodes. Some of these mechanisms are explained as follows:

Alomair *et al.*'s Protocol: This protocol was proposed by Alomair *et al.* in 2012 [58]. It is a symmetric-key privacy-preserving authentication protocol along with constant-time identification. Strengths: (a) no communication overhead, (b) able to withstand tag compromise attacks and (c) improved time efficiency for tag identification.

Non-Cryptographic Approach: Chen *et al.* proposed this approach for identifying tag in constant time in 2011 [59]. This scheme does not use any cryptographic primitives. For representing tag it uses a line on a plane. Strengths: (a) keep tag untraceable, (b) scalable and (c) guards user location privacy.

Cimato's Lightweight Protocol: Stelvio Cimato proposed this protocol for dynamic RFID identification in 2008 [60]. Strengths: (a) increased security level, (b) secure tag-reader transactions, (c) reduced number of communication rounds, (d) recognize tags in a dynamic way and (e) untraceability and cloning resistance properties.

HQT Protocol: Ryu *et al.* proposed hybrid query tree (HQT) protocol combining a tree based query protocol with a slotted backoff mechanism in the year 2007 [61]. Strengths: (a) reduces average identification delay regardless of tags are mobile or not, (b) reduced additional idle cycles and (c) reduced collisions.

VEDFSA Algorithm: Peng *et al.* proposed Variant Enhanced Dynamic Frame Slotted ALOHA Algorithm (VEDFSA) in 2007 for improving system efficiency [62]. Strengths: (a) performance is higher than EDFSA and (b) dynamic group solution.

IQT Protocol: Bhandari *et al.* proposed Intelligent Query Tree (IQT) Protocol for tag identification in the year 2006 [63]. Strengths: (a) more efficient identification process, (b) memoryless protocol and (c) suitable where products may have same product Ids.

DFSA using Fast Tag Estimation Method: Cha *et al.* proposed ALOHA-based Dynamic Framed Slotted ALOHA algorithm (DFSA) using Tag Estimation Method (TEM) in 2006 [64]. Strengths: (a) lower complexity and (b) better delay performance.

Tree Slotted Aloha Protocol: Bonuccelli *et al.* proposed this protocol for RFID tag identification in 2006 [65]. Strengths: (a) better performance than Framed Slotted Aloha and Query Tree based protocols and (b) reduced number of transmission collisions.

ABS Protocol: Adaptive Binary Splitting (ABS) protocol was proposed by Myung *et al.* in 2005 [66]. The information of the last processes of tag identification is used for efficient tag identification and collision reduction. Strengths: (a) tag recognization with faster and less transmissions, (b) low communication overhead and (c) reduced total dealy for identifying all tags.

EDFSA ALOHA Algorithm: Lee *et al.* proposed Enhanced Dynamic Framed Slotted ALOHA (EDFSA) for RFID tag identification in 2005 [67]. In this method for reading the tags number of slots increase linearly as the number of tags increase. Strengths: (a) improved slot efficiency and (b) simple to implement. Weakness: Waste of slots.

Myung *et al.*'s Protocol: Myung *et al.* proposed adaptive memoryless tag anti-collision protocol in 2005 for RFID networks [68]. Information already known by the reader about tags is used for efficient tag identification. Strengths: (a) low communication overhead and (b) reduced total delay in identifying all tags.

Henrici and Muller's Protocol: This protocol was proposed in the year 2004 by Henrici and Muller [69]. It is simple and efficient protocol based on one-way hash functions. In RFID systems it is used for providing communication between the reader and the tags. Strength: (a) secure against tracking attack, (b) simple and efficient protocol, (c) enhanced location privacy and (d) secure against many attacks like eavesdropping, spoofing, message interception and replay attacks. Weaknesses: (a) attack based on lack of randomness, (b) attack based on de-synchronization and (c) Avoine *et al.* pointed out some flaws [70].

Golle, Jakobsson, Jules and Syverson's Protocol: Golle *et al.* proposed this protocol in 2004 [71]. It is based on universal re-encryption scheme. In this protocol re-encryption does not require the knowledge of the key initially used for encryption. Strengths: (a) provides the ability of constructing a mixnet in which servers hold no public or private keying material and (b) supports privacy-preserving architectures. Weakness: An attack was pointed out by Saito.

Saito, Ryau and Sakurai's Protocol: Saito *et al.* proposed this scheme in 2004 [72]. There are two categories of this protocol which are as follows: (1) with a check protocol – Strength: it prevents violation of the location privacy, Weakness: cost of RFID tags calculation is high and (2) with one-time pad – Strength: prevents modification of RFID tags, Weakness: Cost of RFID tags calculation is reduced.

Juel's Protocol based upon XOR: This protocol was proposed in 2004 by Juel. It is used for updating identifier of a tag and thus tag will be used within a process of interrogation-answer type. It has more weak points, rather than having strong points [73].

Table 6 shows the comparative analysis of identification protocols. These protocols are classified into various categories: Tree-based, Non-Tree based, Collision-free, Anti Collision-free etc.

3.2. Authentication Protocols

Authentication mechanism is used for the validity of message between tags and readers by using some secret information. Authentication protocols are categorized into four major classes: protocols based on cryptographic primitives, protocols based on ultra lightweight operations, protocols based on the capabilities of EPCglobal Class1 Generation and protocols based on the notion of physical primitives [16].

Protocols based on ultra lightweight operations: These protocols ensure authentication by using simple bitwise and modular arithmetic on-tag operations. Protocols based on ultra lightweight operations are further classified into minimalist cryptography and protocols based on NP-hard mathematical problems [16].

-Minimalist Cryptography: MAP-family (LMAP, EMAP, M2AP, etc), SASI and Gossamer protocols are based on the work of this scheme. Ultra lightweight Mutual Authentication Protocols (UMAP) family was proposed by Peris *et al.* in 2006. SASI protocol was proposed by Hung-Yu Chien in 2007 and it provides strong authentication and security [74].

-Protocols based on NP-hard mathematical problems: This category includes HB family authentication protocols. First HB authentication protocol was proposed by Hopper and Blum in 2001 [75].

Protocols based on the notion of physical primitives: Physically Unclonable function (PUF) is the part of this class. PUF is used for generating hardware specific finger print and protects from Men-in-the-Middle (MITM) attack [76].

Table 7. Various Authentication Protocols based on the Minimalist Cryptography and its characteristics [74]

Protocol	Resistant Against Attacks
U-MAP	Forward Secrecy, Anonymity
U-LAP	Forward Secrecy, Anonymity, Replay Attack, Forgery, man in middle attack
E-MAP	Forward Secrecy, Anonymity, Replay Attack, Forgery, Forgery Resistant
LMAP	Forward Secrecy, Anonymity, Replay Attack, Forgery, Data Recovery
SASI	Forward Secrecy, Anonymity
HBVI	Anonymity, Replay Attack, Forgery, Forward Secrecy, Data Recovery
SA	Replay, Attack, Anonymity, Confidentiality
Gossamer	Desynchronization, disclosure, Forward Secrecy, Anonymity, Forward Secrecy, Anonymity

Table 8. Various proposed and broken HB variants [75].

Protocol	Year of Protocol Proposal	Possible Vulnerabilities
HB	2001	Man in middle attack*, Gilbert attack, Wagner's attack,
HB+	2005	Eavesdropping, Gilbert active attack, Walkner algorithm attack,
HB++	2006	Gilbert active attack
HB-MP	2007	Passive attacks due to walkner algorithm
HB*	2007	Gilbert active attack,
HB-MP+	2008	Man in middle, Passive attacks due to walkner algorithm
Trusted-HB	2008	Man in middle*, additional cost of hashing, integrity and confidentiality to protect against man in middle attack.
HB#	2008	Man in middle*
GHB#	2012	Provable secure

(*) requiring many challenge-response pairs

Table 7 depicts the various authentication protocols based on minimalist cryptography in which an ultra lightweight protocol based on one-time authenticators is suggested for mutual authentication between tags and readers. Table 8 shows variants of HB family authentication protocols based on NP-hard mathematical problems [16] [75]. The security of these algorithms is reduced to Learning with Parity Noise (LPN) problem. Table 9 describes the comparative analysis of various authentication protocols. These authentication protocols help to authenticate messages and users in a highly un-trusted environment.

3.3. Distance Bounding Protocols

Distance bounding protocols are integrated into the physical layer and verify that the tag is within a certain distance. It provides protection against those attacks which are related to

locations and cannot be handled by protocols that operate in the application layer [16].

Distance Bounding Protocols Using Mixed Challenges: Avoine *et al.* proposed KA1, KA1+ and KA2 protocols in 2011 [77]. KA1+ is the modification of KA1 to decrease the success probability of intruder in the case of distance fraud. Success probability of intruder is reduced by KA2 for both mafia and distance frauds. KA2 requires less memory than KA1. Strengths: (a) require little memory, (b) improved efficiency and (c) three physical states are not required.

YKHL Protocol: Yum *et al.* proposed this protocol in 2011 [78]. This protocol requires final confirmation message. It is a mutual distance bounding protocol. In this protocol there is no assumption of time synchronization between users. Strength: flexible, Weakness: Avoine *et al.* [79] found that success probability of adversary is higher than Yum *et al.*'s claim.

Poulidor: Martin *et al.* proposed this protocol based on graphs in 2010 [80]. Strengths: (a) resists to mafia and distance frauds and (b) fast, simple and flexible protocol.

Avoine and Tchamkerten's Distance Bound Protocol: Avoine *et al.* proposed this protocol using decision tree in 2009 [81]. Strengths: (a) good security against mafia fraud, (b) low complexity and (c) verifier can make rational decisions in the case when protocol does not end properly.

Munilla and Peinado's Distance Bounding Protocol: It is a modified version of Hancke and Kuhn's protocol proposed by Munilla *et al.* in 2006 [82]. In this protocol "void challenges" are applied. Strength: success probability of intruder is reduced. Weakness: Three physical states: 0, 1 and void, required by this protocol may be difficult to implement.

An RFID Distance Bounding Protocol: First distance bounding protocol for RFID systems was proposed in 2005 by Hancke and Kuhn in 2005 [83]. It is based on ultra-wideband pulse communication. Strengths: (a) simple and asynchronous, (b) low-power hardware in the token, (c) suitable for passive low-cost tokens and high speed applications and (d) provides security against relay attacks.

Brands and Chaum's Distance Bounding Protocol: The first distance bounding protocol was proposed by Brands *et al.* in 1993. This protocol includes a fast-bit exchange phase. Strength: It provides highest time resolution [77].

Comparisons: (i) Distance Bounding Protocols using Mixed Challenges are designed by measuring the round-trip times of message exchanged between the reader and the tag to prevent mafia fraud attack. (ii) YKHL Protocol is flexible in choosing false acceptance rate and forgery of message authentication code is infeasible. This protocol does not assume any time synchronization between the users. (iii) Poulidor is based on graphs and ensures good security against mafia fraud or distance fraud. It provides greater design flexibility, a high security level and low memory consumption. (iv) Avoine and Tchamkerten's Distance Bound Protocol is low complexity authentication protocol based on single bit challenge/response exchanges and does not require final signature. It achieves false acceptance rate equal to $(1/2)^n$ in the presence of mafia frauds. (v) Munilla and Peinado's Distance Bounding Protocol is the modification of Hancke and Kuhn's protocol to reduce the success probability of the adversary by applying void challenges. (vi) The purpose of an RFID Distance Bounding Protocol is to prove to the verifier that the prover is located within a specified distance from the verifier. This protocol requires low power and processing resources from the token. (vii) Brands and Chaum's Distance Bounding Protocol provides highest time resolution, as it depends only on propagation time, pulse width, and processing delay.

Table 9. Authentication Protocols and its characteristics

Protocol	Characteristics	Weaknesses
Protocols based on cryptographic primitives	Types: (a) User Authentication Protocols (b) Key Management Protocols: These protocols provide increased security level. Encryption and digital signatures are a special case of cryptographic protocols.	Complex Design of user authentication protocols.
Protocols based on ultra lightweight operations	Ensures authentication by using simple operations. Provides strong authentication and security.	Affected by De-synchronization attack and Full-disclosure attack.
Protocols based on the capabilities of EPCglobal Class1 Generation	Universal standard for low-cost RFID tags. Receives power supply from readers.	Exposed to information leakage and traceability.
Protocols based on the notion of physical primitives	Resist physical attacks. Not possible to clone a PUF. Not feasible to predict the output and the output looks random.	Increased complexity.

3.4. Yoking / Grouping Proof Protocols

Juels proposed Yoking Proof in 2004. In this protocol simultaneous scanning of a pair of RFID tags is performed with the generation of a proof. Grouping proofs are generalization of yoking proof. Grouping proofs involve multiple tags in the generation of proof. These protocols mainly scan tags sequentially. But Lien *et al.* proposed that tags should be scanned in parallel in order to make the schemes more practical [16].

GUPA: Liu *et al.* proposed grouping-proofs-based authentication protocol (GUPA) in July 2013 [84]. It is efficient for resource-constrained distributed RFID systems. Strengths: (a) low computation load and communication overhead, (b) hierarchical protection is enhanced by assigning tags into diverse groups and (c) fault-tolerant against an illegal reader or tag.

GKMP: Group Key Management Protocol (GKMP) has the ability of creating and distributing the keys within groups of arbitrary size and there is no intervention of a centralized key manager. Strengths: (a) no requirement of central key distribution site, (b) the key is available to only group

members and (c) multicast communication protocols can be used [85].

GSAKMP: Group Secure Association Key Management Protocol (GSAKMP) protocol is responsible for creating and managing cryptographic groups on a network. It reduces the no of message exchanged for secure group establishment. It supports rekeying algorithm such as Logical Key Hierarchy (LKH) for maintaining group secrecy during members joining and leaving the group or an unauthorized access to a cryptographic key [86].

GDOI: Group Domain of Interpretation (GDOI) protocol is used for key management. It is based on Internet security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange version 1 (IKE). It is run between a group member and a group controller for establishing a security association among two or more group members [87].

Grouping-proof Protocol for RFID Tags: Duc *et al.* [88] proposed scalable grouping-proof protocol for RFID tags. This protocol is based on secret sharing. In this protocol there are no relaying messages. It properly addresses the mafia fraud attack. It solves the scalability issues of previous protocols.

Clumping Proof: Peris-Lopez proposed this mechanism in 2007 [89]. It is based on simultaneous scanning proofs. Strengths: (a) solves multi-proofs session attack, (b) protection against tracking and (c) secure against replay attacks.

Coexistence Proof: Lin *et al.* presented two techniques: a secure timestamp proof (sects-proof) and a timestamp-chaining proof (chaining-proof) in 2007 [90] to solve the problem of existence-proof technique. SecTS-proof requires an online verifier environment and chaining-proof is used on the off-line verifier environment. Strength: Avoid replay attacks.

Comparison: Yoking/Grouping proof protocols guarantee the existence of a particular tag at a specific location, at a specific time or with other particular tags. In these protocols tags are scanned either sequentially or in parallel. Some of the scalability issues of previous protocols can be solved by using grouping-proof protocol for RFID tags. Schemes can be made more practical by scanning tags in parallel.

3.5. Tag Ownership Transfer Protocols

When a tag's owner is changed, tag ownership transfer protocol is used to transfer tag's information in a secure manner. There are two phases, authentication phase and ownership transfer phase. These protocols are divided into two groups: (a) protocols utilizing a trusted third party for example solution given by Saito et al and (b) decentralized proposals without using a trusted third party [16].

Chen *et al.*'s Secure Ownership Transfer Protocol: Chen *et al.* proposed RFID ownership transfer protocol in 2013 [91]. Strengths: (a) provides user location privacy, (b) resist forged-tag attack and forged-server attack, (c) secure against man-in-the-middle attack, (d) conforms to EPCglobal C1G2 standards and (e) able to resist Pedro *et al.*'s attack.

ROTIV Protocol: Blass *et al.* proposed RFID ownership transfer with issuer verification (ROTIV) protocol in 2012 [92]. Strengths: (a) secure against malicious owners, (b) prevents injection of fake tags from malicious partners, (c) constant-time authentication, (d) high security and (e) requires only a tag to evaluate a hash function.

Lo *et al.*'s Ownership Transfer Protocol: Lo *et al.* proposed this protocol using lightweight computing operators for RFID objects in the year 2011 [93]. Strengths: (a) stronger security robustness and (b) higher performance efficiency. Weakness: Safkhani *et al.* [94] presented tag's secret disclosure attack, new owner's secret disclosure and fraud attack against Lo *et al.*'s protocol.

TPOT Protocol: Yin *et al.* proposed this protocol in 2011 [95]. It is a hash based method to transfer RFID tag ownership to customers. In this scheme ownership transfer is done by readers instead of back-end servers. Strength: suitable for large-scale RFID systems.

Comparison: Tag ownership transfer protocols transfer tag's information in a secure manner when a tag's owner is changed. These protocols are broadly classified into two categories: protocols utilizing a trusted third party and protocols without using a trusted third party. For secure ownership transfer against malicious owners ROTIV protocol is best suited.

4. Post-Quantum Lightweight Cryptography

Most of the popular public-key cryptosystems are based on the integer factorization problem or discrete logarithm problem. Both of these can be solved on large quantum computers. In order to secure from quantum computers, post-quantum cryptography came into existence. Post quantum cryptographic primitives cannot be broken using quantum computers. As shown in figure1 post quantum cryptography can be classified into four major classes: lattice based, hash based, code based and multivariant based [96].

4.1. Lattice Based

In 1996, Miklos Ajtai made use of lattices as cryptography primitive. First fully homomorphic encryption scheme was proposed by Craig Gentry in 2009. Strengths: (a) security of lattice based schemes is based on worst-case problems, (b) this scheme requires very less and easy operations for the computation of signatures or ciphertexts and (c) fast operations are used than current classical systems like RSA or ElGamal [97].

Ajtai-Dwork Cryptosystem: In 1997, Ajtai and Dwork proposed a public key lattice based cryptosystem using worst/average case equivalence. Author claims to share strong and efficient cryptosystem using two different distributions. Weakness: Nguyen and Stern found possibility of heuristic attack in 2011 [98].

GGH Cryptosystem: Goldreich, Goldwasser and Halevi proposed this scheme in 1996 using integral lattices. Strength: more closer to a practical lattice-based cryptosystem. Weakness: Because of limited parameter set, the original GGH cryptosystem was broken in 1999 by Nguyen [98].

NTRU: Hoffstein *et al.* presented first version of NTRU cryptosystem in 1996. It consists of NTRUEncrypt cryptosystem and NTRUSign signature scheme. NTRssU is described as a polynomial ring cryptosystem [98].

Ideal lattices: It is based on the fact that set of all lattice vectors forms a special type of subset in a certain ring. This provides a possible solution to the efficiency problem. These are used to implement cryptographic primitives based on lattice problems in ideal lattices [98].

Table 10. Post-Quantum Lightweight Cryptography classes and its characteristics

	Hash-based	Code-based	Multivariate -based	Lattice-based
Signature	Y	Y	Y	Y
Encryption	N	Y	Y	Y
Hashing	N	Y	N	Y
Collision Resistance	Y	Y	N	Y
Basis	Numeric	Code based	Equation system	Lattice Based
Good for software	Y	N	N	Y
Good for Hardware	N	Y	Y	N
Speed	Fast	Good	Untested	Untested
Examples	MSS,CMSS, GMSS, SPR-MSS, XMSS etc.	McEliece, Niederreiter, Original CFS, Parallel CFS etc.	Oil and Vinegar, Matsumoto-Imai A, Hidden field equations etc.	SVP/CVP, GGH/NTRU, Fiat & Shamir, Hash and sign etc.

Y=Yes, N= No

4.2. Hash Based

Hash based cryptography includes the development of digital signature schemes which are not dependent on the existence of secure trapdoor functions. Related examples are: Lamport signature cryptosystem invented in 1979 by Leslie Lamport and Merkle signature scheme developed by Ralph Merkle in the late 1970s. Strengths: (a) efficient software implementation, (b) implementation is highly scalable, (c) requires smaller code size and provides faster verification times and (d) improved performance [99].

Hash-based one-time signatures: Lamport proposed Lamport-Diffie One-Time Signature schme (LD_OTS) in 1979. It requires collision resistant hash function and each public/private key-pair is used to sign one message only. Weakness: Large signatures are produced [98].

The Merkle Signature Scheme: Using one-time signature requires creation and distribution of keys every time when it is used, which is not practical. In 1979 Merkle proposed solution for this problem by creating a tree structure of large number of these keys. Weakness: Quite low efficiency [98].

4.3. Code Based

In 1978 McEliece cryptosystem was introduced based on algebraic coding theory. Strengths: (a) encryption process is very fast and efficient, (b) high security level, (c) provides protection against quantum computers and (d) full protection against cache-timing attacks and branch-prediction attacks [100].

Binary Linear Codes: In this scheme single-bit error detection is done by repeating each bit at least twice and single-bit error correction is performed by repeating each bit at least three times. Weakness: Code repetition is highly inefficient [98].

The McEliece Cryptosystem: McEliece proposed this scheme in 1978 which is based on binary irreducible Goppa codes. Weakness: Binary Goppa codes require large memory [98].

4.4. Multivariant Based

Multivariate cryptography is based on multivariate polynomials over finite fields. In 1998 Matsumoto *et al.* proposed Multivariate-Quadratic based signature scheme known as Matsumoto-Imai-Scheme. In an another multivariate based system, hidden monomial cryptosystems was developed by Jacques Patarin [101]. In 1997 he developed balanced Oil and vinegar. By extending this work in 1999, unbalanced oil and vinegar was proposed. Strengths: (a) efficient computation, (b) efficient basic operations and (c) suitable for smart card, active RFID tags, wireless sensor networks and embedded devices. Many traditional multivariate cryptosystems have been broken such as: SFLASH signature scheme was broken by Dubois *et al.* and the Square signature scheme was broken by Billet *et al.* at ASIACRYPTO'09 [101].

Table 10 shows various classes of lightweight cryptography and its comparative analysis. The comparison is done on the basis of different speeds, security reduction and schemes. For excellent security reduction lattice-based cryptography is the preferred choice.

5. Comparative Analysis

In resource constraint networks, major security challenge is to reduce the size of implementation while keeping the reading range as good as possible. Size of antenna or other hardware units can also be minimized without changing the minimum requirements of hardware in implementing necessary security requirements [102]. Integration of resource constraint networks monitor the real world by sensing, processing and communicating through small embedded devices. In order to defend against attacks, wireless sensor networks should be equipped with security mechanisms like: confidentiality and authentication [103]. Table 11 shows the possible lightweight primitives combinations. Characteristics of these combinations are as follows:

A2U2 Cipher with some Hash Function: A2U2 avoids the issue of predictable bit streams on power-up caused by identical initialisation values. In the design of A2U2 the focus is on synchronous stream ciphers with a nonlinear update function to achieve best security and performance. Compactness is achieved by using short-length registers and reusing existing capabilities [18].

(a) Spongent: Squeezed sponge construction with finite number of input bits produces a fixed n-bit output. Low area consumption is an important characteristic of simple hash function. Spongent follows hermetic sponge strategy. In terms of serialization degree and speed, it is highly flexible. Area requirements of spongent are highly dependent on technology used but it has the smallest footprint among all hash functions [104].

(b) Photon: Photon family uses a sponge like construction as domain extension algorithm. It is sequential permutation network based primitive. As internal un-keyed permutation, it results into a compact hash function. It is suitable for generic applications as it provides a high security level of 128-bit collision resistance [42].

(c) Keccak: Keccak derives the flexibility of the sponge and duplex constructions which make it provably secure against

generic attacks. It has good software performance and excels in hardware performance. Keccak has arbitrary output length which makes it suitable for tree hashing [41].

(d) Quark: Quark minimizes memory requirements and as a sponge construction, it can be used for message authentication, stream encryption, or authenticated encryption. Quark follows hermetic spong strategy. Hardware implementation is easier because of use of shift registers. Feed forward values in sponge construction avoid the additional hardware memory requirements. [44].

Table 11. Possible combinations of lightweight mechanisms

Cipher	Hash	GE
A2U2	Spongent	<1038
A2U2	Photon-80	<1165
A2U2	Keccak	<1600
A2U2	U-Quark	<1679
PRINT	Spongent	1140
PRINT	Photon-80	1267
PRINT	Keccak	1702
PRINT	U-Quark	1781
Piccolo	Spongent	1354
Piccolo	Photon-80	1481
Piccolo	Keccak	1916
Piccolo	U-Quark	1995
KTANTAN	Spongent	1426
KTANTAN	Photon-80	1553
KTANTAN	Keccak	1988
KATAN	Spongent	1792
KATAN	Photon-80	1919
KLEIN	Spongent	1958

PRINT Cipher with some Hash Functions: Block and key sizes requires least amount of area (402 GE) in the serialized implementation of $PRINT_{CIPHER.}$ PRINT cipher is secure even in the absence of key schedule [105].

(a) Spongent: When PRINT cipher is combined with Spongent hash function the overall area (GE) requirement will be reduced. The combination of both will provide security even in the absence of key schedule and flexibility in terms of speed.

(b) Photon: PRINT cipher can be combined with Photon. Reusability of gates reduces the amount of area required in its implementation. Photon provides good performance and throughput.

(c) Keccak: Keccak provides strong security against generic attacks. It is suitable for tree hashing and can provide good performance when implemented with PRINT cipher.

(d) Quark: It avoids the need of additional memory components and thus it can be efficiently used for various encryption schemes. It greatly reduces area and power consumption when combined with PRINT cipher.

Piccolo with some Hash Functions: Because of permutation based key scheduling Piccolo is suitable for both flexible key and fixed key setting. It has low power and energy consumption. In Piccolo adding decryption functions is almost free. It achieves best performance with respect to energy consumption [29].

(a) Spongent: It provides security against collision, pre-image and second pre-image. Power and energy consumption can be reduced by combining it with Piccolo cipher.

(b) Photon: It can be made suitable for both flexible key and fixed key setting by combining it with Piccolo cipher. It provides strong security against differential and linear cryptanalysis.

(c) Keccak: It is flexible and can accept infinite amount of input and output. It is secure against generic attacks. It achieves best performance with respect to energy consumption when combined with Piccolo cipher.

(d) Quark: It is secure against collision, second preimage, length extensions and multicollisions. Addition of decryption function can be made almost free by combining it with Piccolo cipher.

KATAN/KTANTAN with some Hash Functions: For KATAN key is stored into memory of devices and will then be repeatedly clocked which results into more secure cipher. In KTANTAN key is hardcoded in devices once and it can never be altered which makes it more compact [106].

(a) Spongent: It can be made more secure by combining it with KATAN cipher. Compactness of Spongent hash can be increased by combining it with KTANTAN family. It provides simplicity in design with low area requirement.

(b) Photon: It is collision resistant which makes it suitable for generic applications. It is most compact hash function and its compactness can be greatly increased by combining it with KTANTAN cipher.

KLEIN with Spongent Hash Function: KLEIN block cipher combines a 4-bit Sbox with Rijndael's byte-oriented MixColumn. KLEIN allows low-memory implementations in low-end software and hardware [28]. Area requirement of KLEIN can be reduced by combining it with Spongent hash function.

6. Conclusion

In RFID privacy, the expectations of lightweight cryptographic primitives and protocols with enhanced security are increasing with advancement of technology. Hardware technology demands minimization of device cost with less number of GEs and software technology requires improvement in quality of service parameters like: throughput, power consumption, delay, jitter, coverage and routing cost etc. These demands in primitives are achieved through improvements in confidentiality, integrity, authentication, non-repudiation and availability mechanisms. In protocols, demands can be fulfilled through improvements in identification, authentication, distance bounding, grouping and tag ownership protocols.

Most of these protocols are breakable through quantum computers thus post quantum cryptosystem plays an important role. Various mechanisms of post-quantum cryptosystem provide in-built error detection and correcting mechanism. This

reduces the chances of false identification, authentication and data transmission. In this work, various primitives are integrated to achieve complete security for any system. During integration, strengths and weaknesses of protocols are analyzed.

References

[1] L. Zhang, Z. Wang, "Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problem," Grid and Cooperative Computing Workshops, pp. 463-469, Oct. 2006.

[2] Y. Zhang, L. T. Yang, J. Chen, "RFID and Sensor Networks: Architecture, Protocols, Security and Integrations," CRC Press, Taylor & Francis Group, Boca Raton, London, New York, 2009.

[3] L. Zhang and Z. Wang, "Integration of RFID into wireless sensor networks: Architecture, opportunities," In Proceedings of the 5th International Conference on Grid and Cooperative Computing Workshop (GCCW'06), Changsha, china, pp. 463-469, 2006.

[4] Instrumentel Ltd., http://www.intrumentel.com

[5] H. Liu, M. Bolic, A. Nayak, I. Stojmenovi, "Integration of RFID and wireless sensor networks," in proceedings of Sense IP 2007 Workshop at SenSys, Sydney, Aurtralia, pp. 463-469, 2007.

[6] N. Cho, S. J. Song, J. Y. Lee, S. Kim and H. J. Yoo, "1-μW UHF RFID tag chip integrated with sensors for wireless environmental monitoring," European Solid-State Circuits Conference (ESSCIRC), Greoble, pp. 279-282, 2005.

[7] H. Kitayoshi, K. Sawaya, "Long Range Passive RFID tag for Sensor Networks," Proc. Of 62nd IEEE Vehic. Tech. Conference, Dallas, USA, pp. 2696-2700, 2005.

[8] M. Philipose, J. R. Smith, B. Jiang, A. Mamishev, "Battery free wireless identification and sensing," IEEE Pervasive Computing, Vol. 4, No. 1, pp. 37-45, 2005.

[9] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, J. R. Smith, "Design of an RFID-Based Battery-Free programmable sensing platform," IEEE Transactions on Instrumentation and Measurement, Vol. 57, No. 11, pp. 2608-2615, 2008.

[10] H. Liu, M. Balic, A. Nayak, I. Stojmenovic, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," IEEE Network, Vol. 32, No. 6, pp. 26-35, 2008.

[11] L. Mirowski, J. Hartnett, R. Williams, "An RFID Attacker Behaviour Taxonomy," IEEE Pervasive Computing, Vol. 8, No. 4, pp. 79-84, 2009.

[12] M. Rieback; B. Crispo, A. Tanenbaum, "The Evolution of RFID Security," IEEE Pervasive Computing, Vol. 5, No. 1, pp. 62-69, 2006.

[13] B. Sun, Y. Xiao, C. C. Li, T. A. Yang, "Security Co-existence of Wireless Sensor Networks and RFID," Journal Computer Communications, Vol. 31, No. 18, pp. 4294-4303, 2008.

[14] D. Molnar, D. Wagner, "Privacy and Security in Library RFID: Issues, Practices and Architectures," ACM CCS'04, Washington, pp. 210-219, 2004.

[15] T. Dimitriou, "A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks," IEEE Secure Communication'05, Athens, Greece, pp. 59-66, 2005.

[16] M. R. S. Abyaneh, "Security Analysis of Lightweight Schemes for RFID Systems," Ph. D. Thesis, The University of Bergen, 8 August, 2008.

[17] G. E. Moore, "Cramming Moore Components onto Integrated Circuits," (http://www.intel.com), 1965.

[18] M. David, D. C. Ranasinghe, T. Larsen, "A2U2: A Stream Cipher for Printed Electronics RFID tags," IEEE International Conference on RFID (RFID 2011), Orlando, FL, USA, pp. 176-183, 2011.

[19] M. Hell, T. Johansson, "Security Evaluation of Stream Cipher Enocoro-128v2," CRYPTREC Technical Report, 2010.

[20] S. Babbage, M. Dodd, "The MICKEY Stream Ciphers," New Stream Cipher Designs- The eSTREAM Finalists, LNCS 4986, Springer Berlin Heidelberg, Germany, pp. 191-209, 2008.

[21] D. J. Bernstein, "The Salsa20 family of stream ciphers," New Stream Cipher Designs- The eSTREAM Finalists, , LNCS 4986, Springer Berlin Heidelberg, Germany, pp. 84-97, 2008.

[22] C. D. Canniere, B. Preneel, "TRIVIU," ISBN: 978-3-540-68351-3, New Stream Cipher Designs- The eSTREAM Finalists, LNCS 4986, Springer Berlin Heidelberg, Germany, pp. 244-266, 2008.

[23] M. Hell, T. Johansson, W. Meier, "Grain – A Stream Cipher for Constrained Environments," International Journal of Wireless and Mobile Comouting (IJWMC), Vol. 2, No. 1, pp. 86-93, 2007.

[24] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, "SOSEMANUK, a fast software-oriented stream cipher," New Stream Cipher Designs- The eSTREAM Finalists, LNCS 4986, Springer Berlin Heidelberg, Germany, pp. 98-118, 2008.

[25] J. Guo, T. Peyrin, A. Poschmann, M. Robshaw, "The LED Block Cipher," In: Cryptographic Hardware and Embedded Systems- CHES 2011, Nara, Japan, pp. 326-341, 2011.

[26] F. Mendel, V. Rijmen, D. Toz, K. Varici, "Differential Analysis of the LED Block Cipher," 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, pp. 190-207, 2012.

[27] Z. Gong, S. N. Kova, Y. W. Law, "KLEIN: A New Family of Lightweight Block Ciphers," A. Juels, C. Paar (eds.), RFIDSec 2011, Amherst, Massachusetts, US, pp. 1-18, 2012.

[28] J-P. Aumasson, M. Naya-Plasencia, M-J. O. Saarinen, "Practical attacks on 8 rounds of the lightweight block cipher KLEIN," 12th International Conference on Cryptology in India, Chennai, India, pp. 134-145, 2011.

[29] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai, "Piccolo: An Ultra-Lightweight Blockcipher," CHES 2011, Nara, Japan, pp. 342-357, 2011.

[30] W. Wu, L. Zhang, "LBlock: A Lightweight Block Cipher," ACNS 2011, Nerja, Spain, pp. 327-344, 2011.

[31] S. Bulygin, M. Walter, J. Buchmann, "Many weak keys for $PRINT_{CIPHER:}$ fast key recovery and counter measures," Topics in Cryptology – CT-RSA 2013, CA, USA, pp. 189-206, 2013.

[32] L. Knudsen, G. Leander, A. Poschmann, M. J. B. Robshaw, "PRINTCIPHER: A Block Cipher for IC-Printing," Cryptographic Hardware and Embedded Systems, CHES 2010, Santa Barbara, USA, pp. 16-32, 2010.

[33] C. De Canniere, O. Dunkelman, M. Knezevic, "KATAN & KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers," CHES 2009, Switzerland, pp. 272-288, 2009.

[34] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, "The 128-bit Blockcipher CLEFIA," FSE 2007, Luxembourg, Luxembourg, 181-195, 2007.

[35] J. H. Park, "Security analysis of mCrypton proper to low-cost ubiquitous computing devices and applications," International Journal on Communication Systems, Vol. 22, No. 8, pp. 959-969, 2009.

[36] A. Bogdnov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," Cryptographic Hardware and Embedded Systems – CHES 2007, Vienna, Austria, LNCS 4727, pp. 450-466, 2007.

[37] S. S. M. AlDabbagh, I. A. Shaikhli, "Lightweight Block Ciphers: a Comparative Study," Journal of Advanced Computer Science and Technology Research, Vol. 2, No 4, pp. 159-165, 2012.

[38] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," Cryptographic Hardware and Embdeed Systems – CHES 2006, Yokohoma, Japan, LNCS 4249, pp. 46-59, 2006.

[39] F-X. Standaert, G. Piret, N. Gershenfeld, J-J. Quisquater, "SEA a Scalable Encryption Algorithm for Small Embedded Applications," CARDIS 2006, Tarragona, Spain, LNCS 3928, pp. 222-236, 2006.

[40] J. Daemen, V. Rijmen, "AES Proposal: Rijndael," NIST AES Proposal, 1998.

[41] G. Bertoni, J. Daemen, M. Peeters, G. V. Assche, "Keccak," 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, pp. 313-314, 2013.

[42] J. Guo, T. Peyrin and A. Poschmann, "The PHOTON Family of Lightweight Hash Functions," 31st Annual Cryptology Conference, Santa Barbara, CA, USA, pp. 222-239, 2011.

[43] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, I. Verbauwhede, "SPONGENT: A Lightweight Hash Function," CHES 2011, Nara, Japan, pp. 312-325, 2011.

[44] J-P. Aumasson, L. Henzen, W. Meier, M. Naya-Plasencia, "Quark: A Lightweight Hash," Journal of Cryptology, Volume 26, No. 2, pp. 313-339, April 2013.

[45] P. Sepehrdad, P. Susil, S. Vaudenay, "Fast Key Recovery Attack on ARMADILLO1 and Variants," CARDIS 2011, Leuven, Belgium, pp. 133-150, 2011.

[46] K. Mandal, X. Fan, G. Gong, "Wabler: A Lightweight Pseudorandom Number Generator for EPC Class 1 Gen2 RFID Tags," In: Radio Frequency Identification System Security: RFIDsec 2011 Asia Workshop Proceedings (Cryptology and Information Security), Amherst, Massachusetts, pp. 73-84, 2012.

[47] J. Melia-Segui, J. Garcia-Alfaro, J. Herrera-Joancomarti, "Multiple-Polynomial LFSR based Pseudorandom Number Generator for EPC Gen2 RFID Tags," 37th Annual Conference on IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, pp. 3820-3825, November 2011.

[48] Martin, H., San Millan, E., Entrena, L., Lopez, P.P., Castro, "AKARI-X: A pseudo random number generator for secure lightweight systems," IOLTS 2011, Athens, pp. 13-15 July, 2011.

[49] J. Wu, M. O'Neill, "Ultra-lightweight true random number generators," Electronics Letters, Vol. 46, No. 14, pp. 988-990, 2010.

[50] P. Peris-Lopez, J. Cesar Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "LAMED – A PRNG for EPC Class-1 Generation-2 RFID specification," Journal Computer Standards & Interfaces, Vol. 31 No. 1, pp. 88-97, January, 2009.

[51] M. Naor, O. Reingold, "Number-theoretic constructions of pseudo-random functions," 38th Symposium on Foundations of Computer Science, Washington, USA, pp. 458-467, 1997.

[52] J. Robert, Jr. Jenkins, "ISAAC," FSE 1997, Cambridge, UK, LNCS 1039, pp. 41-49, 1996.

[53] L. Blum, M. Blum, M. Shub, "A simple unpredictable pseudo random number generator," SIAM Journal on Computing, Vol. 15. No. 2, pp. 364-383, May 1986.

[54] M-J. O. Saarinen, "The BlueJay Ultra-Lightweight Hybrid Cryptosystem," IEEE Symposium on Security and Privacy Workshops. pp. 27-32, 2012.

[55] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," ANTS-III Portland, Oregon, USA, LNCS 1423, pp. 267-288, 1998.

[56] J. Pelzl, T. Wollinger, J. Guajardo, C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves (Update)," CHES 2003, Cologne, Germany, LNCS 2779, pp. 351-365, 2003.

[57] V. S. Miller, Slide on "Elliptic Curve Cryptography: Invention and Impact: The invasion of the Number Theorists", 2007 http://www.iacr.org/conferences/eurocrypt2007/slides/s14t1.pdf

[58] B. Alomair, A. Clark, J. Cuellary, R. Poovendran, "Scalable RFID Systems: a Privacy-Preserving Protocol with Constant-Time Identification," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 8, pp. 1536-1550, Aug. 2012.

[59] Y. Chen, J-S. Chou, C-L. Wu, C-F. Lin, "Identifying Large-Scale RFID Tags Using Non-Cryptographic Approach," IACR Cryptology ePrint Archive 2011, 167, 2011.

[60] S. Cimato, "A Lightweight Protocol for Dynamic RFID Identification," COMPSAC 2008, Turku, pp. 673-678, 2008.

[61] J. Ryu, H. Lee, Y. Seok, T. K., Y. Choi, "A hybrid Query Tree Protocol for Tag Collision Arbitration in RFID systems,", ICC 2007, Glasgow, pp. 5981-5986, June 2007.

[62] Q. Peng, M. Zhang, W. Wu, "Variant Enhanced Dynamic Frame Slotted ALOHA Algorithm for Fast Object Identification in RFID System," IEEE International Workshop on Anti-counterfeiting, Security, Identification 2007, Xiamen, Fujian, pp. 88-91, April 2007.

[63] N. Bhandari, A. Sahoo, S. Iyer, "Intelligent Query Tree (IQT) Protocol to Improve RFID Tag Read Efficiency," ICIT 2006, Bhubneswar, India, pp. 46-51, Dec. 2006.

[64] J-R. Cha, J-H. Kim, "Dynamic Framed Slotted ALOHA Algorithms using Fast Tag Estimation Method for RFID System," CCNC 2006, Las Vegas, NV, USA, pp. 768-772, Jan. 2006.

[65] M. A. Bonuccelli, Francesca Lonetti, Francesca Martelli, "Tree Slotted Aloha: a New Protocol for Tag Identification in RFID Networks," WoWMom 2006, Buffalo-Niagara Falls, NY, USA, pp. 602-608, 2006.

[66] J. Myung, W. Lee, "Adaptive Binary Splitting: A RFID Tag Collision Arbitration Protocol for Tag Identification," BroadNets 2005, Seoul, South Korea, pp. 347-355, Oct. 2005.

[67] S-R. Lee, S-D. Joo, C-W. Lee, "An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification," Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, San Diego, California, pp. 166-174, July 2005.

[68] J. Myung and W. Lee, "An Adaptive Memoryless Tag Anti-Collision Protocol for RFID Networks," IEEE Transactions on Multimedia, Vol. 8, No.5, pp. 1096-1101, 2006.

[69] D. Henrici, P. Muller, "Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Florida, USA, pp. 149-153, 2004.

[70] E. Vahedi, R. K. Ward, I. F. Blake, "Security Analysis and Complexity Comparison of Some Recent Lightweight Protocols," CISIS 2011 at IWANN 2011, Spain, LNCS 6694, pp. 92-99, 2011.

[71] P. Golle, M. Jakobsson, A. Juels, P. Syverson, "Universal re-encryption for mixnets," Cryptographers' Track at the RSA Conference – CT-RSA, California, USA, LNCS 2964, pp. 163–178, February 2004.

[72] J. Saito, J-C. Ryou, K. Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," Embedded and Ubiquitous Computing – EUC 2004, Aizu-Wakamatsu City, Japan, LNCS 3207, pp. 879–890, August 2004.

[73] G. Avoine, "Adversarial Model for Radio Frequency Identification," IACR Cryptology ePrint Archive 2005, 49, 2005.

[74] P. Peris-Lopez, J. C. Hernandez-Castro, J. M.E. Tapiador, A. Ribagorda, "Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol," WISA 2008, Island, Korea, LNCS 5379, pp. 56-68, 2008.

[75] E. Zenner, "Authentication for RFID Tags: Observations on the HB Protocols," 4th Interdisciplinary Seminar on Applied Mathematics, Aalborg, pp. 1-20, 2009.

[76] A. Schaller, V. van der Leest, "Physically Unclonable Functions found in Standard Components of Commercial Devices." First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE 2013), Avignon, France, pp. 1-2, 2013.

[77] C. H. Kim, G. Avoine, "RFID Distance Bounding Protocols with Mixed Challenges", IEEE Transactions on Wireless Communications, Vol. 10, No. 5, pp. 1618-1626, May 2011.

[78] D. H. Yum, J. S. Kim, S. J. Hong, L. P. Joong, "Distance bounding Protocol with Adjustable False Acceptance Rate," IEEE Communications Letters, Vol. 15, No. 4, pp. 434-436, 2011.

[79] G. Avoine and C. H. Kim, "Mutual Distance Bounding Protocols," IEEE Transactions on Mobile Computing, Vol. 12, No. 5, pp. 830-839, May 2013.

[80] R. Trujillo-Rasua, B. Martin and G. Avoine, "The Poulidor distance bounding protocol," RFIDSec 2010, Istanbul, Turkey, LNCS 6370, pp. 239-257, 2010.

[81] G. Avoine and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement," ISC 2009, Pisa, Italy, LNCS 5735 pp. 250-261, 2009.

[82] J. Munilla A. Ortiz and A. Peinado, "Distance bounding protocols with void-challenges for RFID," Workshop on RFID Security (RFIDSec 2006), Graz, Austria, 2006.

[83] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," 1st IEEE International Conf. Security Privacy Emerging Areas Communications. Networks, Athens, Greece, pp. 67-73, 2005.

[84] H. Liu, Y. Zhang, Q. Xiong, "Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 7, pp. 1321-1330, July 2013.

[85] H. Harney, C. Muckenhirn, "RFC 2094 – Group Key Management Protocol (GKMP) Architecture," Internet Request for Comments 2094, July 1997.

[86] F. Mah, "Group Key management in Multicast Security," Helsinki University of Technology, Article, 2004.
http://www.tml.tkk.fi/Publications/C/18/mah.pdf

[87] C. Meadows, "Experiences in the formal analysis of the GDOI protocol." Slides, Dagstuhl Seminar: Specification and Analysis of Secure Cryptographic Protocols (2001).
http://www.stanford.edu/class/cs259/WWW04/lectures/04-GDOI.pdf

[88] D. N. Duc, J. Kim, K. Kim, "Scalable Grouping-proof Protocol for RFID Tags." The 2010 Symposium on Cryptography and Information Security (SCIS 2010), Takamatau, Japan, pp. 1-6, 2010.

[89] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags," SECPERU 2007, Istanbul, pp. 55-60, July 2007.

[90] C-C. Lin, Y.-C. Lai, J.D. Tygar, C-K. Yang, C-L. Chiang, "Coexistence Proof Using Chain of

Timestamps for Multiple RFID Tags," Advances in Web and Network Technologies and Information Management 2007, Huang Shan, China, LNCS 4537, pp. 634-643, 2007.

[91] C-L. Chen, Y.-C. Huang, J.-R. Jiang, "A secure ownership transfer protocol using EPC global Gen-2 RFID," Telecommunication Systems, Vol. 53, No. 4, pp. 387-399, June 2013.

[92] K. Elkhiyaoui, E.-O. Blass, R. Molva, "ROTIV: RFID Ownership Transfer with Issuer Verification," RFID Security and Privacy 2011 (RFIDSec 2011), Amherst, USA, LNCS 7055, pp. 163-182, 2012.

[93] N.-W. Lo, S.-H. Ruan, T.-C. Wu, "Ownership transfer protocol for rfid objects using lightweight computing operators," In 6th International Conference on Interney Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, pp. 484–489, 2011.

[94] M. Safkhani, N. Bagheri, M. Naderi, A. Mahani, "On the security of Lo et al.'s ownership transfer protocol," IACR Cryptology ePrint Archive 2012, 023, 2012.

[95] X. Yin, Z. An, Y. Xu, H. Long, "TPOT: A Two-Party Privacy-Preserving Ownership Transfer Protocol for RFID Tags," WiCOM 2011, Wuhan, pp. 1-5, Sept. 2011.

[96] D. J. Bernstein, J. Buchmann, E. Dahmen, "Post-quantum cryptography," 1st edition, Springer, Berlin, ISBN 978-3-540-88701-0, 2009.

[97] C. gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the forty-first annual ACM symposium on Theory of computing, Maryland, USA, pp. 169-178, 2009.

[98] M. Ajtai and C. Dwork, "A public key cryptosystem with worst-case/average-case equivalence." STOC '97 Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, TX, USA, pp. 284-293, 1997.

[99] S. Rofde, T. Eisenbarth, E. Dahmen, J. Buchmann, C. Paar, "Fast Hash-Based Signatures on Constrained Devices," CARDIS 2008, Surrey, UK, LNCS 5189, pp. 104-117, 2008.

[100] E. Persichetti, "Improving the Efficiency of Code-Based Cryptograph," Ph. D. Thesis, University of Auckland, November 23, 2012.

[101] W. H. Zhen and H. G. Zhang, "Hash-based Multivariate Public Key Cryptosystems," IACR Cryptology ePrint Archive 2010, 296, 18 May 2010.

[102] F. Abdelhak, F. Najib, G. Ali, "A Sierpenski Slot Antenna as a TAG RFID Antenna," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 2, No. 3, pp. 248-252, December 2010.

[103] J. Sen, "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, pp. 59–82, 2009.

[104] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, I. Verbauwhede, "SPONGENT: The Design Space of Lightweight Cryptographic Hashing," IEEE Transactions on Computers, Vol. 62. No. 10, pp. 2041-2053, 697, 2013.

[105] L. Knudsen, G. Leander, A. Poschmann, M. J. B. Robshaw, "PRINTcipher: A Block Cipher for IC-Printing," CHES 2010, Santa Barbara, USA, pp. 16-32, 2010.

[106] N. A. N. Abdullah, N. H. Lot, A. Zawawi, H. A. Rani, "Analysis on Lightweight Block Cipher, KTANTAN," IAS 2011, Malacca, Malaysia, pp. 46-51, 2011.