Next Generation Security for IoT in Post Quantum Era

Jigar Thakkar[a], Priyalakshmi Gnanasekaran[b], Ge Yao[c]

[a] *School of Computing and Information Systems, The University of Melbourne, Australia, thakkarj@student.unimelb.edu.au*
[b] *School of Computing and Information Systems, The University of Melbourne, Australia, pgnanasekara@student.unimelb.edu.au*
[c] *School of Computing and Information Systems, The University of Melbourne, Australia, gyao1@student.unimelb.edu.au*

Abstract

Internet of Things (IoT) is developing rapidly. As more and more smart devices being connected into network, the security problem has become the primary concern. In the past years, many cryptography based security solutions are proposed in literature. But the building blocks of these solutions are threatened by the arrival of quantum computing era. In this research, we study the cryptographic primitives that are suitable for the resource constrained IoT applications and also strong enough to resist the destructive power of quantum computers. We identify that lattice based cryptography and symmetric key cryptography are among the most simple and efficient algorithms among all the post quantum cryptographic primitives. We then explore the authentication problem in RFID based IoT application and discuss the stream cipher based authentication schemes.

Keywords: Internet of things, Post-quantum cryptography, Lattice based cryptography, Stream cipher, Authentication

1. Introduction

During the last three decades, connecting computers was a major focus, which becomes a global network of computers - the Internet. The Internet has enabled us to do all kinds of jobs which was just a science fiction three decades ago that included activities like group video chatting, www and cryptocurrency. Next revolution started by shaping the network of devices which included wireless sensors, RFIDs and whats more - the Internet of Things (IoT) thus came into being.

For instance, imagine one day in the future when your car not only drives automatically, but also detects the surroundings, downloads all the latest traffic information of that area and chooses the best route to navigate you to office from your home. After dropping you at office, it will find parking space by itself, and if any maintenance is needed it will order parts spontaneously and go to the manufacturer for repair by itself.[1] By the time, you finish your work in the evening, your smartwatch or wristband measures your body temperature and send it to smart home/automatic temperature control system, so that it starts maintaining the temperature. When you arrive and stay at home, your home will know in which part of the home you are and what activity you are doing. Lights will start turning on/ off as you move[2]. There will be refrigerators which will show you the items in it and the sophisticated algorithms will recommend a list of recipes which you can prepare from those items.Probably it should also be able to preorder the items in case it is running out, and smart internet enabled drones delivers it at your doorstep [3] [4]. Apparently everything will be computerised and technologically sophisticated.

IoT not only makes human life easier but also healthier and safer. Smart pacemaker directly sends data of heart to the doctor/or some smart AI system, so that in case of emergency autonomous ambulance immediately takes the patient to the nearest hospital[5]. IoT is not only smart but also efficient, and this is not in the future but it is already the present.According to estimate, IoT will have more than 30 billion internet connected devices before 2020. If we consider 7 billion population in the world, more than 4 devices will be owned by a single person [6]. A huge chunk of this devices are currently used in industries.For example, Australia's largest independent oil and gas company-Woodside has already deployed 200,000 smart internet-connected sensors for plant monitoring in Perth, Western Australia. IoT is not just helping to manage industries but making them more productive and safer [7].

But this all shiny promises of IoT turns dark when it gets hacked. Security is becoming major issues in IoT.If some malicious blackhat criminals hacks your car along with you inside then he can demand or force you to pay a huge ransom inorder to be harmless.Government can even start spying you by your smart home. What can be more dangerous than your body implanted device like pacemaker getting hacked? Industries can be sabotaged in the same way, and this has already happened. Germany recently banned smart doll which was spying, the DDoS attack happened by the network of IP cameras which was used as IoT botnet. Attacks by using IoT devices are much more disastrous than an attack on your computer because this can harm you physically, like bad robots of the Hollywood movies.

Security is challenging for IoT because it is a heterogeneous network. One of the biggest challenges is to ensure the security of small devices with limited capabilities and resources. The majority of these devices are embedded in the system with few MB of RAM and limited storage capabilities. The most common example is Raspberry Pi. Except for the limited resource, the nature of the device itself can be a problem. For example, some devices are custom designed which makes it is difficult to continue after-sales maintenance work once it is put to use. And some devices are hard to be replaced if they are installed in some remote areas like in space or inside human body. Moreover, cryptographic algorithms also have a limited lifespan, like RSA was hard to break before 10 years even with 512-bit key size but nowadays the standard has come to 2048 bit.

With the conventional cryptographic algorithm which is present till date, we can protect our devices only to an extent. However, when the quantum computing era, cryptography will face dramatic changes. The security of the modern cryptographic algorithm is built on hard mathematical problems. For example, RSA is based on the integer factorization problem and RSA problem; ECC relies on the elliptic-curve discrete logarithm problem. But these can be easily broken down by the quantum computers. The work of Proos and Zalka shows that using 4096 qubit quantum computer and Shor's algorithm, RSA - 2048 bit can be broken [8]. Making key size larger is not the solution of this problem as computation power of quantum computers doubles by adding each new qubit, countering this we have to double RSA key size on each qubit.So it is clear that larger key size is an issue here for limited resources of IoT. Now comes the need to design strong and efficient algorithm to protect the heterogeneous IoT.

In our research, we are considering the security solutions of IoT both for now and for the quantum age. First, we have studied algorithms proposed against quantum computers, which are collectively referred to as post-quantum cryptography. Several algorithms are believed to resist classical computers and quantum computers [9], namely lattice based, hash based, multivariate, code based, super singular elliptic curve isogeny and symmetric key quantum resistance algorithm [10]. Our research mainly focuses on lattice based cryptography and symmetric key cryptography as they are considered as the most simple and efficient quantum resistance algorithms. Then we take RFID based IoT as an example and do further research on how to exploit cryptographic primitives to solve authentication problem in resource constrained IoT environment.

2. Lattice based Cryptography

Lattice based cryptography provides great promise for very strong security which is based on worst case hardness with efficient and simple implementation. The backbone of lattice based cryptography is hard mathematical problems like shortest vector problem, closest vector problem, bounded distance decoding etc wherein the public key encryption is built on these computational difficulties.

In the year 1995, Ajtai and Dwork have explained a lattice-based public key cryptosystem which has average case-worst case equivalence. Though it was only theoretical milestone and couldnt be implemented practically. In 1996 Halevi,Goldwasser and Goldreich proposed a practically applicable lattice-based cryptosystem, after being motivated by the work of Dwork and Ajtai. The proposed system of GGH cryptosystem was fast, but then it needs large megabyte-size public keys to be secure while simultaneously, Hoffstein was developing a ring-based cryptosystem known as NTRU that only requires RSA-sized keys. It has been lately indicated that NTRU can be explained by the terms of a special class of lattices which is closely related to the GGH system. Thus, lattice based cryptography includes approaches such as Ring-Learning with Errors, Learning with Errors, Ring-Learning with Errors, the Ring Learning with Errors Key Exchange and Ring-Learning with Errors, the older NTRU or GGH encryption schemes. Few of these approaches like NTRU encryption have been studied for several years without anyone finding a feasible attack whereas other approaches like the Ring-LWE algorithms have proofs that their security can be applied to a worst-case problem [11].

A lattice can be defined as a set of points with a space of n-dimension as illustrated in Figure 1. It is considered that for a set of given n linearly independent vectors. The lattice is generated by the set of vectors where n linearly independent vectors $b_1, , b_n$ are given which forms the basis of the lattice.

$$\zeta(b_1, ..., b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in Z\}$$

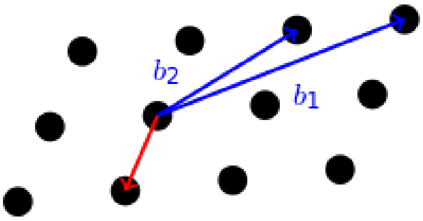

Figure 1: Lattice

For example, in the above figure if we consider the shortest vector problem, we need to find the shortest distance vector for the two vectors $b1$ and $b2$ which are indicated by blue lines. Then red line is the shortest vector which we can find and this is really a very hard mathematical problem when it comes to 500-dimensional lattice. It is interesting that in r-approximate SVP for $r = poly(n)$, the SVP algorithm runs in time runs in time 2^n. Also, it is not considered as the NP-hard problem. The possible poly-time algorithm solves for $r = 2^{nloglogn/logn}$ [12]. Lattice based cryptography provides the possibility of faster encryption and decryption algorithms. For example, let n be the number of bits in the below given problem:

- n = number of bits in an RSA modulus pq
- n = number of bits in a prime p for ECC in $E(Fp)$
- n = (dimension of a lattice L) x (of bits in a coordinate)

Using various methods for encryption/decryption it takes $O(n^2 logn)$ steps for RSA and ECC whereas $O(nlogn)$ steps for lattice-based cryptosystems which makes it more efficient. For learning with error problems, the practical implementation will be to distinguish noisy inner products from the uniform lattices [11].

$$a_1, b_1 = \langle a_1, s \rangle + e_1$$

$$a_2, b_2 = \langle a_2, s \rangle + e_2$$

$$\left(\begin{array}{c} \cdots \\ \mathrm{A}^t \\ \cdots \end{array} \right), \left(\begin{array}{c} \cdots \\ \mathrm{b} \\ \cdots \end{array} \right) = A^t s + e$$

where the generator matrix can be given as:

$$\zeta(A) = \{ z \in Z^m : \exists s.z \equiv A^t smodq$$

By applying it practically in case of Alice and Bob, message encryption, it can be illustrated in the picture as given below:

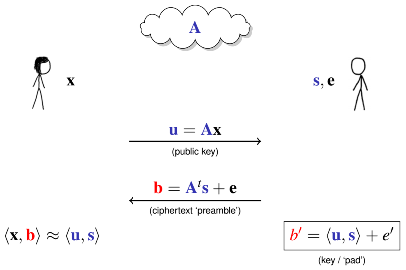
A
x
s, e
$\mathbf{u} = \mathbf{A}\mathbf{x}$
(public key)
$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$
(ciphertext 'preamble')
$\langle \mathbf{x}, \mathbf{b} \rangle \approx \langle \mathbf{u}, \mathbf{s} \rangle$
$b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'$
(key / 'pad')

Figure 2: Lattice based Cryptography

From the above given figure 2, Alice and Bob share a public matrix A where x is the private vector for Alice. Alice sends u vector which is the collision resistant hash function and is the product of the public matrix A and Alices private vector x and so $u = Ax$.Now, Bob has random vectors b and b' where he adds his error terms e, s which are random vectors and sends it Alice such that $b = As + e$ and $b' = su + e'$.Inorder to make sure that the message sent to Alice is by bob and is not intruded by anyone, the decryption techniques is used where a parity error bit of $q/2$ is added to b' which makes it $b' = su + e' + q/2$ bits. When Alice receives it, she multiplies her private vectors with b and b' and checks whether the value of (x, b) is closer to the value of (u, s) which ensures that there has not been any intrusion. If the values were not closer then it is notable that there has been an intruder [13].

Similarly, all the other approaches can also be practically applied in lattice based cryptography for enhancing the security of post quantum cryptography. As of now, for the 128 bits security in NTRU the recommended public key is represented as a degree 613 polynomial having a coefficient of mod $2^1 0$ which gives to a public key size of 6130 bits for which the corresponding private key would be 6743.Further works are being carried out to reduce the key size to increase the efficiency [14].

3. Symmetric Key Cryptography

3.1. Symmetric Key Cryptography in Quantum Computing Age

Although most of asymmetric primitives are vulnerable against quantum computing, symmetric primitives seem less affected by the presence of large scale quantum computers in future. This is because the quantum algorithm works on symmetric key cryptography is based on Grovers algorithm, which is not as shockingly fast as Shors algorithm [9]. Grovers algorithm [15] provides only a quadratic speed-up for exhaustive key search in classical computers. It is believed that this weakness can be compensated by doubling the key size in the design.

Except for exhaustive search, the security of symmetric cipher is also related to cryptanalysis. Several research activities have been carried out to study the quantum attacks based on classical cryptanalytic attacks. In particular, a quantum distinguishing attack presented in [16] is able to attack three-round Feistel. This attack is based on the quantum algorithm of Simon [17]. Similarly, this algorithm is extended to obtain a quantum related-key attack in [18] and a slide attack to break the block cipher operation modes for MACs [19]. Recently, Kaplan et al. [20] analysed the quantum version of differential attack on LAC, KLEIN-64 and KLEIN-96 and concluded that quantizing the best known classical differential attacks may not give the best quantum attack. All these works show that it is necessary to conduct more comprehensive study of how quantum cryptanalysis can affect the security of symmetric ciphers. However, in contrast to public-key cryptography, symmetric cryptographic algorithms are not collapsed against quantum attacks. Therefore, it is more desirable to exploit symmetric primitives when consider the security of IoT, especially for resource constrained IoT devices.

3.2. Authentication in RFID based IoT

In this report, we focus on the authentication problem in IoT. More precisely, we consider the Radio Frequency Identification (RFID) based IoT applications. For instance, RFID is widely used in ticketing. It is embedded in tickets or wristbands and can be used as access to events and festivals. However, possible threats exist in this application. The legitimate RFID tag may be impersonated or a malicious party may replay the data intercepted from former transmission. In order to tackle these security issues, an efficient authentication scheme is a necessity. In the past years, many authentication schemes for resource constrained IoT devices have been proposed. There are mainly two components considered in these designs including underling cryptographic primitives and the series of message exchanges.

Due to the fact that RFID tags have limits on power, area and latency, lightweight cryptography tends to be more suitable than traditional cryptography. Many lightweight asymmetric and symmetric primitives such as ECC, AES, PRESENT, WG-7 and hash functions have been exploited in literature. For RFID applications, the best choice of underlying cryptographic primitive should be the one that guarantees optimum level of efficiency and security in practice.

We compare the hardware performance of three typical algorithms in Table 1. This implementation result is partial of Sghaiers work [21]. They implemented FPGA designs in VHDL and computed several hardware performance metrics including area, frequency and power consumption.

Table 1: Comparison of Hardware Performance

FPGA Implementation			
Cryptographic Primitives	Area (Slices)	Frequency (MHz)	Power (mW)
ECC	9670	147.5	45
SHA-256	1480	73	50
Grain-128	495	238.5	19.22

It is obvious that symmetric primitives are more efficient than asymmetric primitives in hardware implementation. We then compare the hardware performance between different symmetric algorithms. Table 2 shows the results of comparison between AES-128, SHA-1, SHA-256, Grain and Trivium from [22]. Table 3 shows the results of comparison between Trivium, Grain-128 and Mickey 128 from [23].

Table 2: Comparison of Hardware Performance

Cryptographic Primitives	Security (bits)	I_{mean} (μA)	Chip Area (GE)
AES-128	128	3.0	3400
SHA-256	128	5.86	10868
SHA-1	80	3.93	8120
Grain	80	0.8	3360
Trivium	80	0.68	3091

We can conclude from the above tables that stream cipher requires the lowest hardware footprint. More discussion include the quantum computing As another direction, the security of these candidates should also be taken serious consideration. We compare the existing work of cryptanalysis of Grain family ciphers because they are well studied. The result is presented in Table 4. The symbol '$\surd$' means that the attack is successfully amounted on the cipher, while '-' denotes resistance to the attack.

Table 3: Comparison of Hardware Performance

Cryptographic Primitives	Key (bits)	Clock Frequency (MHz)	Area (GE)
Trivium	80	358.4	2599
Grain-128	128	925.9	1857
Mickey	128	413.2	5039

To date, there is no valid attack that has been successfully mounted on Grain-128a, which means it is the most promising underlying cryptographic primitive for authentication schemes in RFID based IoT environment.

Regarding the series of message exchanges, we study the OSK family of authentication schemes and the PFP family schemes. OSK [24] is the first identification protocol aims at providing forward privacy and its variants [25, 26] have been proposed and presented as authentication protocols. Note that these protocols are based on hash functions and their efficiency stands out among the privacy-friendly authentication schemes compared in [27]. However, the OSK family protocols have desynchronization issues and traceability weakness. An alternative authentication scheme called PFP is proposed in [28] to provide stronger forward privacy and its variant PEPS [29] is proposed to accommodate stream cipher. The execution process is shown in Figure 3. First, the Reader initiate a challenge by sending $n/2$-bit message a to the tag. After receiving the challenge, the tag combine it with a randomly generated number b which is also $n/2$-bit. Then initiate the stream cipher with $a||b$ and its current key K and responds with first l-bit output sequence $c = G_t(a||b, K)$. The reader searches for the right key K' to generate the same output as c. Then it sends the subsequent l-bit message $d = G_r(a||b, K')$ to the tag. At the receipt of d, the tag check the validity of d. If the validation passed, it replace the current key K with subsequent k-bit sequence $G_s(a||b, K)$, and the reader also update the information for this tag as $(K', G_s(a||b, K')$. The authentication is completed.

Table 4: Comparison of Security between Grain Family Ciphers

Cryptographic Primitives	Key (bits)	Internal States (NLFSR + LFSR)	Distinguishing Attack	Key Recovery Attack	Time-Memory-Data Trade-Off Attack	Chosen IV Attack	Guess and Determine Attack
Grain v0	80	80 + 80	√	√	√	√	-
Grain v1	80	80 + 80	-	-	√	-	-
Grain-128	128	128 + 128	√	-	-	√	-
Grain-128a	128	128 + 128	-	-	-	-	-

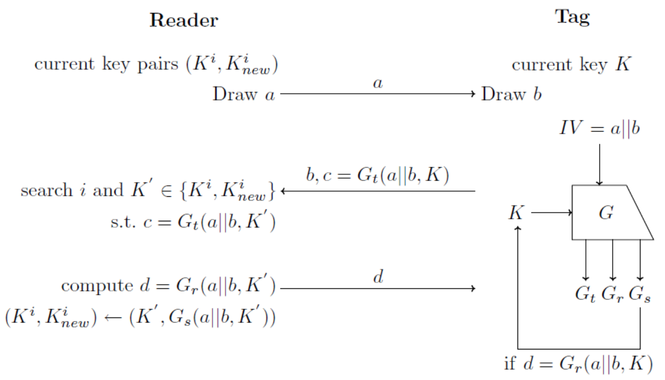
Reader
Tag
current key pairs (K^i, K^i_{new})
current key K
Draw a
a
Draw b
$IV = a||b$
$b, c = G_t(a||b, K)$
search i and $K' \in \{K^i, K^i_{new}\}$
s.t. $c = G_t(a||b, K')$
K
G
compute $d = G_r(a||b, K')$
d
$(K^i, K^i_{new}) \leftarrow (K', G_s(a||b, K'))$
G_t G_r G_s
if $d = G_r(a||b, K)$

Figure 3: PEPS Protocol

The PEPS protocol contains only three message exchanges while provides strong forward privacy and DoS-resistance. More importantly, it is suitable for arbitrary secure stream cipher. Combing the Grain-128a stream cipher with this protocol, we can obtain a very efficient and secure authentication scheme for the RFID absed IoT system.

4. Conclusion

In this report, we introduce the IoT development and application status and discuss the security problem of resource constrained devices. Considering the upcoming quantum computing era, we compare the state-of-art post quantum cryptography and focus on the lattice based cryptography and symmetric cryptography. The underlying mathematical problems and an encryption/decryption process of lattice based cryptography are presented in details. Besides, we study the authentication problem of RFID devices. By comparing the hardware performance and security of existing lightweight cryptogaphy. We conclude that Grain-128a is the most promising building block for RFID based IoT environment. The PEPS is also identified as the most efficient protocols that accommodates stream cipher. The combination of these two candidates achieves an efficient and secure authentication scheme.

References

[1] M. Gerla, E.-K. Lee, G. Pau, U. Lee, Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE, 2014, pp. 241–246.

[2] D.-M. Han, J.-H. Lim, Smart home energy management system using ieee 802.15. 4 and zigbee, IEEE Transactions on Consumer Electronics 56 (3).

[3] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, E. Jansen, The gator tech smart house: A programmable pervasive space, Computer 38 (3) (2005) 50–60.

[4] T. T. Zhou, D. T. Zhou, A. H. Zhou, Unmanned drone, robot system for delivering mail, goods, humanoid security, crisis negotiation, mobile payments, smart humanoid mailbox and wearable personal exoskeleton heavy load flying machine, uS Patent App. 14/285,659 (May 23 2014).

[5] A. I. Hernandez, F. Mora, M. Villegas, G. Passariello, G. Carrault, Real-time ecg transmission via internet for nonclinical applications, IEEE Transactions on Information Technology in Biomedicine 5 (3) (2001) 253–257.

[6] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.

[7] K. Bloede, G. Mischou, A. Senan, R. Koontz, Silicon Valley London THE INTERNET OF THINGS " Smart " Products Demand a Smart Strategy Using M&A for a Competitive Edge Investment Banking Research, WCP.

[8] D. Beckman, A. N. Chari, S. Devabhaktuni, J. Preskill, Efficient networks for quantum factoring, Physical Review A 54 (2) (1996) 1034–1063. doi:10.1103/PhysRevA.54.1034.

[9] D. J. Bernstein, Introduction to post-quantum cryptography, in: Post-quantum cryptography, Springer, 2009, pp. 1–14.

[10] A. Gabriel, B. K. Alese, A. Adetunmbi, O. S. Adewale, Post-quantum crystography: A combination of post-quantum cryptography and steganography, in: Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, IEEE, 2013, pp. 449–452.

[11] J. Hoffstein, J. C. Pipher, J. H. Silverman, J. H. Silverman, An introduction to mathematical cryptography, Vol. 1, Springer, 2008.

[12] C. Du, G. Bai, A family of scalable polynomial multiplier architectures for lattice-based cryptography, in: Trustcom/BigDataSE/ISPA, 2015 IEEE, Vol. 1, IEEE, 2015, pp. 392–399.

[13] E. Crockett, C. Peikert, $\lambda o \lambda$: Functional lattice cryptography, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 993–1005.

[14] A. Aysu, C. Patterson, P. Schaumont, Low-cost and area-efficient fpga implementations of lattice-based cryptography, in: Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on, IEEE, 2013, pp. 81–86.

[15] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twenty-eighth annual

ACM symposium on Theory of computing, ACM, 1996, pp. 212–219.

[16] H. Kuwakado, M. Morii, Quantum distinguisher between the 3-round feistel cipher and the random permutation, in: Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on, IEEE, 2010, pp. 2682–2685.

[17] D. R. Simon, On the power of quantum computation, SIAM journal on computing 26 (5) (1997) 1474–1483.

[18] M. Roetteler, R. Steinwandt, A note on quantum related-key attacks, Information Processing Letters 115 (1) (2015) 40–44.

[19] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia, Breaking symmetric cryptosystems using quantum period finding, in: Annual Cryptology Conference, Springer, 2016, pp. 207–237.

[20] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia, Quantum differential and linear cryptanalysis, arXiv preprint arXiv:1510.05836.

[21] A. Sghaier, M. Zeghid, C. Massoud, M. Mahchout, Design and implementation of low area/power elliptic curve digital signature hardware core, Electronics 6 (2) (2017) 46.

[22] P. Kitsos, Y. Zhang, RFID security: techniques, protocols and system-on-chip design, Springer Science & Business Media, 2008.

[23] T. Good, M. Benaissa, Hardware results for selected stream cipher candidates, State of the Art of Stream Ciphers 7 (2007) 191–204.

[24] M. Ohkubo, K. Suzuki, S. Kinoshita, et al., Cryptographic approach to privacy-friendly tags, in: RFID privacy workshop, Vol. 82, Cambridge, USA, 2003.

[25] M. Ohkubo, K. Suzuki, S. Kinoshita, Efficient hash-chain based rfid privacy protection scheme, in: International Conference on Ubiquitous Computing–Ubicomp, Workshop Privacy: Current Status and Future Directions, 2004.

[26] G. Avoine, E. Dysli, P. Oechslin, et al., Reducing time complexity in rfid systems, in: Selected Areas in Cryptography, Vol. 3897, Springer, 2005, pp. 291–306.

[27] G. Avoine, M. A. Bingöl, X. Carpent, S. B. O. Yalcin, Privacy-friendly authentication in rfid systems: on sublinear protocols based on symmetric-key cryptography, IEEE Transactions on Mobile Computing 12 (10) (2013) 2037–2049.

[28] C. Berbain, O. Billet, J. Etrog, H. Gilbert, An efficient forward private rfid protocol, in: Proceedings of the 16th ACM conference on Computer and communications security, ACM, 2009, pp. 43–53.

[29] O. Billet, J. Etrog, H. Gilbert, Lightweight privacy preserving authentication for rfid using a stream cipher, in: Fast Software Encryption, Springer, 2010, pp. 55–74.