Securing Internet-of-Things *

Guang Gong[0000−0003−2684−9259]

Department of Electrical and Computer Engineering, University of Waterloo,
Waterloo Ontario N2L 3G1, Canada
ggong@uwaterloo.ca

Abstract. In this survey, we first present some vulnerabilities and attacks on IoT systems, and classification of IoT devices, we then show the evolution of the development of lightweight cryptography for securing IoT, the metrics for the design of lightweight cryptography, and the applications in privacy preserving authentication protocols. We use examples including the development of Simon, Simeck, and sLiSCP/sLiSCP-Light lightweight ciphers to demonstrate those approaches.

Keywords: Internet-of-Things (IoT) · security and privacy · lightweight cryptography.

1 Introduction

The IoT connects an extraordinarily wide range of computing technologies, spanning from computers and servers through to smart devices. Sensors, actuators, radio frequency identification (RFID) tags, vehicular ad hoc networks (VANETs) and micro-controllers equipped with RF transceivers capture and communicate various types of data related to, for example, industrial and building control, e-health (e.g., wearable devices embedded in our clothing), smart energy grid, home automation (Internet-connected appliances in our increasingly smart homes, such as washing machines, dryers, and refrigerators), self driving cars, and embedded systems. That data is transmitted through the Internet via wireless, wired and/or hybrid to back-end business application/integration servers that receive and process it into meaningful information (such as data analytic services and cloud analytic services). Personal and potentially sensitive information may flow through shared data centres and the cloud, where it can be exposed to multiple shareholders and, more broadly, to countless business partners. A graphic schematic of information flow in the IoT system is shown in Figure 1.

There is consensus that IoT will continue to grow by approximately 20% per year, and the greatest risks for IoT are security, scalability, and reliability [14]. In 2017, IoT devices outnumbered the world's population! It is expected that there will be 30 billion connected devices by 2020, each with different operational and security requirements. Much of the growth in IoT stems from the volume and

* Supported by NSERC

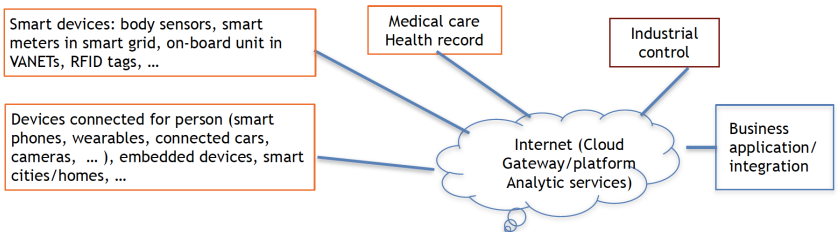


Fig. 1. A diagram of information flow of the IoT

diversity of data produced by IoT devices. The value of this data has given rise to new economic opportunities, such as *data markets*. At the same time, it also generates new vulnerabilities for security and privacy due to rapidly increasing cyber attacks against the critical infrastructure. According to current developments, the most rapid growing applications of IoT are smart cities ($\approx 26\%$), industrial IoT ($\approx 24\%$), connected health ($\approx 20\%$), followed by smart homes ($\approx 14\%$), then connected cars, wearables, and smart utilities.

This survey article intents to provide the envisions of vulnerabilities, attacks and countermeasures in securing IoT. The rest of the paper is organized as follows. In Section 2, we introduce vulnerabilities and attacks on IoT systems, and some efforts for standardization of IoT security mechanisms. In Section 3, we provide the classification of IoT devices according to their communication transmission systems. In Section 4, we show the evolution of how lightweight cryptography (LWC) has been merged as a new interdisciplinary research field of electrical and computer engineering, cryptography, and computer science from lightweight cipher suites' design to privacy preserving authentication protocols. Section 5 provides an example of such an evolution for LWC using our work from Simeck to sLiSCP/sLiSCP-light. We conclude this paper in Section 6 by presenting some open problems and remarks.

2 Challenges in Securing IoT

The challenges for securing IoT come from security (how to securely share private information), scalability (how to interface different protocols and to optimize connectivity (e.g. 5G cellular systems), and reliability (how much available resources can be allocated to each task).

2.1 Attacks

The complexity, large volume and need for real-time access to data (coined as big data) within IoT systems make it extremely challenging to implement security and privacy protection mechanisms. These challenges are compounded by a historically ad hoc approach to Internet-based security. In the last several decades, since the inception of the Internet, security has been handled as an afterthought and not by design. Quick-fix add-ons developed post-attacks have

proven ill equipped to address new security risks presented by an ever-expanding stream of technologies and applications. For example, Wi-Fi service, which is pervasive in today's society, was introduced with serious security flaws. The Wired Equivalent Privacy (WEP) algorithm is now used as the textbook example for how easily security can fail. In current IoT systems, attackers continue to find the simplest, easiest and most cost efficient ways to access secure systems. We can classify the reported attacks on commercial products into the following three categories.

A. Weak authentication yields malware attacks. In this class, noticeable examples are as follows.

- Weak login password: Mirai malware attack launched in 2016 [22]. Those attacks first exploit the weakness of the password based authentication at login phase of IoT devices like cameras, routers, DVRs, or even baby monitors in order to break in those devices to install malware (e.g., when they connect to the Internet through Telnet or SSH), in sequel the attacker can conduct brute force search for login information since its using only about 60 known default passwords.
- Single master key for updating software: Attacks on Philips Hue smart bulbs which infected millions of ZigBee sensors connected to Internet through WiFi. In those attacks [27], the attacker exploits manufacturers unprofessional practices, i.e., one master key for all bulbs for firmware updates. However, this is just simply repeated an old attack on radio frequency identification (RFID) proximity card in 2005 [18]! The lesson is never learned.

B. Weakness of underlying cryptographic algorithms. Those attacks are launched by observing some weakness of employed cryptographic algorithms and protocols. We list some of them below.

- In 2011, Lockheed Martin networks were breached and, in 2012, the Master Key for Sony Playstation 3 system was leaked. Both used weak pseudorandom bit generators.
- In 2014, compatibility downgrade attacks were demonstrated on TLS (i.e., forcing a connection which runs TLS v1.2 down to SSL v3, where an insecure cipher (i.e., DES) is employed).
- In 2008, MIFARE RFID tag encryption [21] was cracked and, in 2012, HID iClass cards were cloned for which, weak cipher suites are employed (both are privately designed (violating Kerchoff) publicly released by reverse engineering approaches).
- In 2015, hackers took remote control of Jeep and Chevrolet Corvette vehicles while on route (due to weak authentication).

C. Attacks on protocols which connect IoT devices. In 2013, we have reported in [29] that message authentication code of 4G-LTE can be forged when it conjuncted with its authenticated key agreement (AKA) protocol. The significant

effect of this attack is that it may migrate to future 5G which designates to connect IoT devices, since 5G will adopt 4G-LTE's AKA and cipher suites [4]. The attack works together with the man-in-the-middle (MITM) attacks. An MITM attacker first records all user data messages and control messages, including the authentication and key agreement (AKA) messages. When this attacker observes the package he wants to forge, he shuts down the radio of the victim and then turns it on. The MITM attacker uses the recorded AKA messages to conduct a replay attack. In the AKA protocol, mobile devices are not required to verify whether the random number has been received before or not. They only check the freshness of radio resource control sequence number (RRC SQN). However, in some cases, we can make the RRC SQN wrap around. Thus, the victim believes it is talking to the real network.

Notice that the AKA is claimed to be mutually authenticated. The user equipment (UE) proves its identity to the mobility management entity (MME) by replaying to the challenge from the MME. However, since the UE does not send the challenge to the MME, the MME can prove itself only by transmitting the valid messages protected by the correct session key in the succeeding communication. This enables the replay attack. Such attack makes the UE accept the fake MME. Generally, the attacker can get nothing from the replay attack, because he still cannot get the key. However, in this case, it forces the IV to repeat, so a meaningful MAC can be forged.

Four years later, in 2017, Vanhoef and Piessens [28] found that WiFi systems suffered a similar attack to the attack described above for 4G-LTE, i.e., forcing IV repeated in the IEEE 802.1X 4 way authentication and key establishment by applying a man-in-the-middle attack.

2.2 Law and standardization efforts

California just became the first state with an *Internet of Things cybersecurity law* (Sep 28, 2018). It states that starting on January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure. The most improving part is that the law requests a unique password for each device when they will connect to the internet!

The second is the event of NIST Lightweight Crypto Standardization competition for low-end IoT devices, which was initialized in 2017 [24]. It announced the call-for-submission for the standardization of lightweight cryptographic primitives to protect IoT devices in April 2018 where the 128-bit security is minimal requirement and submissions are due in Feb. 2019. Note that ISO has the initiative to standardize lightweight cryptographic primitives for several years now, see [13].

3 Classification of IoT devices

In this section, we first introduce IoT devices and how they can be connected to Internet. Then we conclude why lightweight cryptography is needed for imple-

menting security mechanisms. According to the complexity of transmitter and receiver (Tx/Rx) structures, we may classify the IoT devices or cyber physical devices [2] into the following three classes.

- Single Tx/Rx pairs, such as GPS receivers, RFID tags [3], cameras, etc..
- Single input and single output (SISO) devices: BlueTooth or BlueTooth Low Energy (BLE), ZigBee [1], NB-IoT, etc..
- More complicated structures, i.e., multiple input multiple output (MIMO) devices, such as WiFi, 4G-LTE, 5G and beyond, Wi-MAX, etc..

In Tables 1-3, we provide their communication protocols, operation frequencies, multiple access methods and possible applications. For a more detailed list of IoT devices, the reader is referring to [2, 26].

Table 1. IoT devices with simple Tx/Rx

Communication Protocol	Spectrum	Trans. Rate and Trans. Range	Multiple Access	Applications
RFID tags	125-135 KHz	5-98 Kbps, < 50 cm	Pure Aloha	Low: smart cards, ticketing, tagging, access control
	13.56 MHz	$\sim$ 106 Kbps, ~ 1 m	F-TDMA	High: anti-theft, supply chain, indexing
	866-960 MHz	$\sim$ 115 Kbps, $\sim$ 2-7 m	CSMA/CA	UHF: vehicle ID, supply Chain, indexing, access /security
NFC	13.56 MHz	106-424 Kbps, < 20 cm	Single service coupling	Mobile commerce, bootstrap setups, social networking, identification
wireless cameras	900 MHz, 2.4/5.8 GHz	1.5-150 Mbps, <4800m	CSMA/CA	Surveillance, video streaming
GPS	Spectrum: 1575.42 (L1), 1227.6 (L2), 1176.45 (L5) MHz			Location service

3.1 Why lightweight crypto?

According to the above classifications, IoT devices are distinguished from general computing platforms in both their structure and behaviour. They have small limited memory and computation resources, compared with their counterpart, servers, and are used in a specific application domain, e.g., automotive on board unit, Electronic Product Code (EPC) tags, and sensors, actuators, etc.. They also use specialized network protocols to communicate wirelessly with back-end data-aggregation and computing servers, e.g. RFID (EPC and NFC), ZigBee, Bluetooth/BLE, 4G-LTE or 5G, WiFi, etc. (see Tables 1, 2 and 3). In Table 4, we emphasize the security constrains in some applications.

Nevertheless, a standard cryptography aimed for securing Internet communication may not be suitable for IoT applications. We will discuss this deeply in the next section.

Table 2. SISO IoT devices

Communication protocol	Spectrum	Trans. rate and Trans. range	Multiple access	Applications
ZigBee	2.4 GHz/866 MHz	20 - 250 Kbps, $\sim$ 40 m	CSMA /CA	Smart home, physical security, medical devices (including implantable devices) smart meter, home automation
BlueTooth 3.0	2.4 GHz	$\sim$ 25 Mbps, $\sim$ 10 m	TDMA	Wearable electronics, peripherals, device pairing, vehicle entertainment
BLE	2.4 GHz	$\sim$ 1 Mbps, $>$ 100 m	TDMA	Medical devices, wearable electronics, sensor networks, electronic leashing
UWB	$>$ 500 MHz	$\sim$ 100 Mbps, $\sim$ 30 m	TDMA, CDMA	Video streaming, wireless displays, wireless printing/scanning (WPS), file transfers, peer-to-peer (P2P) connections

4 Evolution of Lightweight Cryptography for IoT

In the literature, metrics for what constitutes a lightweight cryptographic design have been studied. More precisely, researchers have investigated throughput, power consumption, latency, but most importantly hardware area. In fact, it is long commonly set in the literature that an upper bound of 2000 GE (gate equivalents) hardware area is what defines a lightweight design [8, 19]. Such a bound is derived from passive RFID tags whose areas range between 1000 and 10000 GE, out of which, a maximum of 20% is to be used for all security functionalities [19]. Note that although lightweight applications span over a spectrum of devices which vary from highly constrained in terms of area and power consumption such as EPC tags [3,19] and implantable medical devices, to less constrained ones such as vehicular embedded system where latency may be the most important metric [20], the 2000 GE bound is one of the design criteria for a lightweight cryptographic primitive.

From those practices, we understand that lightweight cryptography lies in the interdisciplinary areas of electrical engineering, cryptography and computer science. Hence, we single out the criteria below for a cipher qualified as a lightweight primitive [7].

4.1 Criteria of lightweight cryptography

Definition 1. *(The requirements of lightweight cryptography (LWC)) A cryptographic primitive is said to be* lightweight *if the hardware area of the implementation is less than 2000 GE, its power consumption is very small and it supports a sustained throughput of 1 bit per clock cycle at a clock speed of 2 MHz. For a cryptographic primitive together with a mode (e.g., authenticated encryption), the GE requirement will be loosened up to 3000 GE.*

From this definition, we may bound how small we can do given the security and throughout requirements.

Table 3. MIMO IoT devices

Communication Protocol	Spectrum	Transmission rate and Trans. range	Multiple Access	Applications
WiFi	2.4/5.8 GHz	50 - 320 Mbps, $\sim$ 100 m	CSMA /CA	Internet access points (AP), video streaming, wireless displays, WPS, file transfers, P2P connections
Wi-Max	2-11 GHz	$\sim$ 70 Mbps, $\sim$ 50 km	OFDMA	Portable internet AP, smart meters, air traffic communications, smart cities, VoIP
3G	700-3500 MHz (UMTS), 450-2100 MHz (CDMA)	$<$ 2.4 Mbps, 5-70 km	TD-CDMA, CDMA	GPS services, high-speed data (emails, maps, directions, News, shopping, e-commerce, interactive gaming, etc.)
4G-LTE	400 MHz - 3.5 GHz	300 Mbps (D), 75 Mbps (U), 2-103 km	OFDMA (D), SC-FDMA (U)	Video streaming, mobile Internet, telecommunications, ubiquitous computing with location intelligence
5G and beyond	up to 90 GHz	up to 1Gbps, 2 - 150 km	various	Supporting IoT, smart city, industrial automation

D = downlink and U = uplink

Table 4. Bit security, and the corresponding dedicated GE area and cost in applications using common communication protocols

	Trans. rate	Bit security	Sec. area (approx)	Cost (approx)
Internet	10 Gbps	128-512	200 kGE	\$50
BLE	1 Mbps	128	40 kGE	\$2
ZigBee	20–250 Kbps	128	10 kGE	\$0.1
NFC	106–424 Kbps	128	5 kGE	\$0.01
EPC	26.7–128 Kbps	80	2 kGE	\$0.01

Definition 2. *(Cryptographic minimal design.) A cryptographic algorithm is said to be a* minimal design *if the design with well justified building components has minimal overhead for providing multiple cryptographic functionalities including encryption, hashing, authentication, and pseudorandom bit generation without compromising the security and decreasing the throughput.*

The key point of the design of lightweight cryptographic primitives is to balance trade-offs among three requirements: security strength, the hardware area, and throughput.

4.2 LWC development and reverse engineering

At the earlier time, the effort of the research was concentrated at low-cost implementations of AES (Advanced Encryption Standard), hash-based RFID privacy

enhancements, and some non cryptographic approaches, like minimalist. Only in recent years, it is devoted to investigate new cryptographic schemes under the constraints of hardware area, key sizes and power consumption.

Along this approach, there are a number of lightweight ciphers which were designed secretly in the industrial community for low-cost applications (violating Kerckhoffs' principle published in 1883) and publicly released by reverse engineering approaches. Examples include

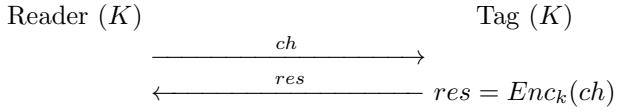
- Keeloq (Microchip Technologies Inc., designed in 1985) used for car immobilizer and in garage doors (designed in 1985, released and broken in 2007);
- MIFARE RFID tag encryption algorithm (2008), cipher in HID iClass cards (2012);
- GMR (2012) in satellite telecommunication systems;
- A5/1 (1991) in GSM cellular communication networks; and
- RC4 (not lightweight) for web, gmail (used until 2015), and many Internet applications.

All those ciphers, except for RC4, use linear feedback shift register (LFSR) based structures.

4.3 Privacy preserving entity authentication for RFID systems

RFID systems are the first which demand to use lightweight ciphers for privacy preserving entity authentication. The link between RFID readers and back-end database is assumed to be secured by known security mechanisms (e.g., TLS and IPSec), and wireless links between RFID readers and RFID tags are insecure. An entity authentication protocol is a challenge-response protocol, as shown below.

Privacy preserving authentication in RFID



A general approach for preserving privacy of devices is that device's ID is not sent. In order to verify the validity of the response, the back-end server is required to do an exhaustive search in the space of the pairing ID and key to identify the tag, therefore, verifies the device's response. So, this imposes the request that the implementation of a cipher at server side should be of high speed (see our work [15] for details about this argument). In addition to the protocol design, this puts another dimension of challenges for securing IoT which requests an asymmetric design for underlying cryptographic primitives having the smaller hardware area of the implementation for device sides and high speed software implementation for server sides as well.

The decision of the success of an entity authentication protocol can be implemented by two different methods.

1. *Deterministic verification*: Use an LWC primitive to generate an authentication tag (e.g., ISO/IEC 9798 2 or 3-pass mutual authentication protocol).
2. *Probabilistic verification*: Use a new hard problem, learning parity with noise (LPN), e.g., HB like protocols [17, 19] as well as our work [23], which can resist all known attacks on LPN based entity authentication.

4.4 Security associations in IoT

In order to have a shared key ahead of communication, currently, in the most of IoT applications, a master key is embedded into an IoT device during its manufacture. In near future, elliptic curve cryptography will be deployed as there are four curves that have been recommended for NFC, ZigBee, and VANETs [16] a few years ago. The authentication for establishing an authenticated channel for key sharing is to use the certificate based authentication. This is the same approach as is now used in TLS. However, this requests public-key infrastructure (PKI), which may be not suitable for many IoT applications. Thus, this remains a challenging problem.

5 Examples of LWC

In this section, we introduce an evolutional process from lightweight ciphers Simon and Speck to Simeck to sLiSCP/sLiSCP-light.

5.1 Simon and Simeck

A Feistel structure in block cipher design is a two-stage NLFSR with input. The most noticeable cipher in 2-stage NLFSR is DES, developed in 1976 which has 56 bit key. In 2013, a group of the researchers from NSA (National Security Agency, USA) published a paper, called their ciphers *Simon and Speck* [9]. Simon family is optimized in hardware and Speck, optimized in software (both are submitted to the ISO for possible standardization [13]). Shortly after that, we have found a way to further decrease Simon's hardware footprint with slightly decreasing security, namely, *Simeck* [30] (i.e., the design is aimed at extracting good features from both Simon and Speck).

The round function of both Simon and Simeck is given in Figure 2 where (x_0, x_1) is an initial state and the feedback function is a simplest quadratic function where $<<<$ is the (circular) left shift operator. For encryption, (x_0, x_1) is loaded as a plaintext, and the ciphertext is the internal state after r rounds. Simon (2013)/Simeck (2015) have register sizes $m/2$ where $m = 32, 48, 64$ and r varies according to different m. The hardware implementations of the Simeck family are shown in Table 5. Currently, they are the smallest ciphers compared with those having the same parameters including Simon family.

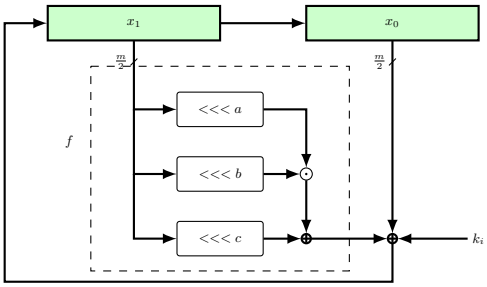


Fig. 2. Simeck round function as an 2-NLFSR with the input key k_i and $(a, b, c) = (1, 8, 2)$ for Simon and $(a, b, c) = (0, 5, 1)$ for Simeck.

Table 5. Performance of hardware implementations of Simeck

Size		**Area**	**Throughput**	**Power**
Simeck	**Tech**		@100KHz	@100KHz
	(nm)	(GEs)	(Kbps)	(μW)
32/64	130	**505**	5.6	0.417
32/64	65	**454**	5.6	1.292
48/96	130	**715**	5.0	0.576
48/96	65	**645**	5.0	1.805
64/128	130	**924**	4.2	0.754
64/128	65	**828**	4.2	2.304

5.2 sLiSCP/sLiSCP-light families

Simeck is a block cipher family. So we need to use modes to provide authenticity. Currently, the main approaches to add authentication to a block cipher are CBC MAC (cipher-block-chain message authentication code) or GCM (polynomial evaluations). Both are very costly. In the search of minimal designs, we find that permutation-based sponge duplexing [10] is well suited for a minimal cryptographic design and thus, we resolve to designing a lightweight family of permutations to efficiently provide multiple cryptographic functionalities with one circuit. This results in the two families of LWC, i.e., sLiSCP: Simeck-based Permutations for Lightweight Sponge Cryptographic Primitives and sLiSCP-light. For the details in this subsection, the reader is referring to [6, 7].

Both sLiSCP and sLiSCP-light can be used in a unified sponge duplex construction in order to provide (authenticated) encryption and hashing functionalities. The sLiSCP family of permutations adopts two of the most efficient and extensively analyzed cryptographic structures, namely a 4-subblock Type-2 Generalized Feistel-like Structure (GFS) [11, 25], and a round-reduced unkeyed version of the Simeck encryption algorithm [30]. A Type 2 GFS, a general nonlinear feedback shift register (NLFSR) generator in Galois mode, consists of multiple branches of Feistel stuctures, which is shown in Figure 3.

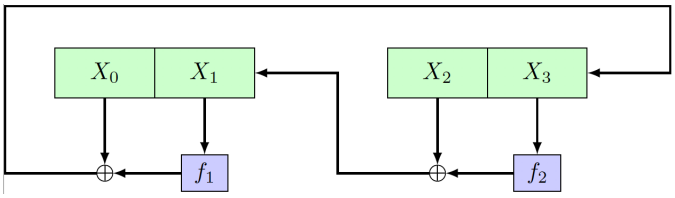


Fig. 3. 2-branches GFS in sLiSCP/sLiSCP-light designs.

In sLiSCP/sLiSCP-light designs, both f_1 and f_2 are identical and implemented by an unkeyed Simeck round function with multiple rounds. Their specifications are given in Table 6.

Table 6. Branch size: m, state size: $b = 4m$, # Simeck rounds: u, and # GFS steps: s.

Permutation (b-bit)	Subblock width m	Rounds u	Steps s	Total # rounds $(u \cdot s)$
sLiSCP/sLiSCP-light-192	48	6	18/12	108/72
sLiSCP/sLiSCP-light-256	64	8	18/12	144/96

The sLiSCP-light is obtained by turning sLiSCP to a partial substitute permutation network (SPN) structure to get 16% reduction in HW footprint, better diffusion and algebraic properties. We have implemented the sLiSCP/sLiSCP-light instances in the CMOS 65 and 130 nm technology. The performance is shown in Table 5.2 and the resourse allocation for different operations in the implementation is shown in Figure 4.

Table 7. The performance of hardware implementations of sLiSCP/sLiSCP-light

State size (b bits)	**Security** (bits)	**Process** (nm)	**Area** (GE)	
			sLiSCP	sLiSCP-light
192	80-112	65	2153	1820
		130	2318	1892
256	128	65	2833	2397
		130	3040	2500

We can provide multi-cryptographic primitives using a single sLiSCP permutation as a unified round function in the sponge, i.e., to provide an *all-in-one module* in-

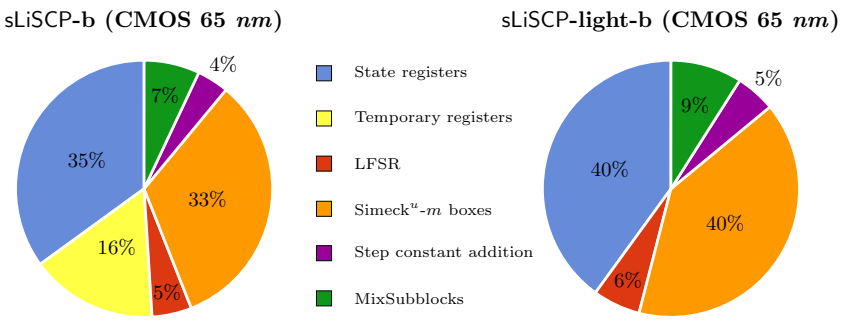


Fig. 4. Resource allocation for sLiSCP/sLiSCP-light

cluding authenticated encryption, stream cipher, pseudorandom bit generation, MAC and hash function.

6 Concluding Remarks

IoT is bringing an exciting new era of the digital world as well as nightmare due to their security concerns for civilian applications. In this survey, we presented vulnerabilities and attacks on recent IoT products, and pointed out that in all of those attacks, attackers exploited the weakness of the underlying cryptographic primitives including those malware attacks. We have walked through the path for the development of lightweight cryptography for securing IoT. Now we present some possible future research problems.

Future Research Problems

a) How to balance the tradeoffs between *security, throughout and hardware footprint* for lightweight cryptographic primitives?
b) How to balance the tradeoffs between *usability and security* (e.g., relay attacks occur because reducing the communication cost for user easiness, in 4G-LTE message authentication in data field is not required, $\cdots$), and *safety and security* (e.g., the emergency case in a smart hospital)?
c) How to implement *machining learning* for efficiency of IoT as well as for detection of malicious behaviours in IoT?
d) Can *physical layer security* (i.e., using signals, channels, antennas, $\cdots$) solve some problems in IoT without using crypto (e.g., in control area networks, see some solutions from our earlier work in [12])?
e) Recently, there are a number of work to investigate blockchain based IoT security mechanisms (e.g., our attempt on using blockchain to solve ownership transfer problem in supply chains [5]). However, how to solve the *scalability and privacy* of blockchains for IoT applications?

References

1. Zigbee smart energy profile specification (sep) 1.2, revision 4. ZigBee Alliance (Dec 2014)
2. CPS PWG draft cyber-physical systems (CPS) framework. National Institute of Standards and Technology (NIST), Online: https://pages.nist.gov/cpspwg/ (Sep 2015)
3. EPC radio frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860mhz-960mhz version 2. EPCglobal Inc. Specification documents (Apr 2015), https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf
4. 5G-PPP: Deliverable d2.7 security architecture (final) - 5G-Ensure. Online. Available: www.5gensure.eu/sites/default/files/5G-ENSURE_D2.7_SecurityArchitectureFinal.pdf (August 2018)
5. AlTawy, R., Gong, G.: *Mesh*: A supply chain solution with locally private transactions. In: Privacy Enhancing Technologies, pending revisions (2018)
6. AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.: sLiSCP-light: Towards lighter sponge-specific cryptographic permutations. ACM Transactions on Embedded Computing Systems **17**, 1–26 (2018)
7. AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.: Towards a cryptographic minimal design: The sLiSCP family of permutations. IEEE Transactions on Computers **67**, 1341–1358 (2018)
8. Armknecht, F., Hamann, M., Mikhalev, V.: Lightweight authentication protocols on ultra-constrained RFIDs - myths and facts. In: Saxena, N., Sadeghi, A.R. (eds.) RFIDSec 2014. pp. 1–18. Springer (2014)
9. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013), http://eprint.iacr.org/2013/404
10. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Permutation-based encryption, authentication and authenticated encryption. DIAC (2012)
11. Bogdanov, A., Shibutani, K.: Generalized feistel networks revisited. Designs, Codes and Cryptography **66**(1), 75–97 (2013)
12. Chai, Q., Gong, G.: Buple: Securing passive RFID communication through physical layer enhancements. In: Proceedings of the 7th International Conference on RFID Security and Privacy. pp. 127–146. RFIDSec'11 (2012)
13. Chen, L.: Lightweight cryptography standards developed in ISO/IEC SC27. Online available at https://www.nist.gov/sites/default/files/documents/2016/10/17/chen-presentation-lwc2016.pdf (2016)
14. Columbus, L.: A roundup of 2018 enterprise Internet of Things forecasts and market estimates (2018)
15. Engels, D., Fan, X., Gong, G., Hu, H., Smith, E.M.: Hummingbird: ultra-lightweight cryptography for resource-constrained devices. In: et al., R.C. (ed.) The 14th International Conference on Financial Cryptography and Data Security - FC 2010, LNCS 6054. pp. 3–18 (January 2010)
16. Fan, X., Gong, G.: Securing NFC with elliptic curve cryptography - challenges and solutions. In: RFIDSec Asia 2013. vol. 11, pp. 97–106 (2013)
17. Hopper, N., Blum, M.: Secure human identification protocols. In: Advances in Cryptology - ASIACRYPT 2001, pp. 52–66. LNCS 2248 (2001)
18. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications **24**, 381 – 394 (2006)

19. Juels, A., Weis, S.A.: Authenticating Pervasive Devices with Human Protocols. In: Advances in Cryptology CRYPTO 2005, pp. 293–308. LNCS 3621 (2005)
20. Knežević, M., Nikov, V., Rombouts, P.: Low-latency encryption – is "lightweight = light + wait"? In: Prouff, E., Schaumont, P. (eds.) CHES. pp. 426–446. Springer (2012)
21. Koning Gans, G., Hoepman, J.H., Garcia, F.D.: A practical attack on the MIFARE classic. In: Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications. pp. 267–282. CARDIS '08 (2008)
22. Krebs, B.: Hacked cameras, DVRs powered todays massive internet outage. Online. Available: `https://krebsonsecurity:com/2016/10/hackedcameras-dvrs-powered-todays-massive-internet-outage/` (October 2016)
23. Li, Z., Gong, G., Qin, Z.: Secure and efficient lcmq entity authentication protocol. IEEE Transactions on Information Theory **59**(6), 4042–4054 (June 2013)
24. McKay, K., Bassham, L., Sönmez Turan, M., Mouha, N.: Report on lightweight cryptography (NISTIR8114) (2017), `http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf`
25. Nyberg, K.: Generalized feistel networks. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT. pp. 91–104. Springer (1996)
26. Perera, C., Liu, C., Jayawardena, S.: The emerging internet of things marketplace from an industrial perspective: A survey. IEEE Transactions on Emerging Topics in Computing **3**, 585 – 598 (Dec 2005)
27. Ronen, E., Shamir, A., Weingarten, A., O'Flynn, C.: Iot goes nuclear: Creating a zigbee chain reaction. In: 2017 IEEE Symposium on Security and Privacy (SP). pp. 195–212 (May 2017)
28. Vanhoef, M., Piessens, F.: Key reinstallation attacks: Forcing nonce reuse in WPA2. In: CCS 2017 (Oct 2017)
29. Wu, T., Gong, G.: The weakness of integrity protection for LTE. In: Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13), April 17-19, 2013, Budapest. pp. 79–88 (2013)
30. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) CHES. pp. 307–329. Springer (2015)