International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 9
September 2017

Lightweight Cryptography using Stream Ciphers on Low Cost RFID Devices

Bobby Singh Rathore
Charotar University of Science and Technology (CHARUSAT)
Chandubhai S. Patel Institute of Technology
U & P U. Patel Department of Computer Engineering, Changa, India

Parth Anand Shukla
Charotar University of Science and Technology (CHARUSAT)
Chandubhai S. Patel Institute of Technology
U & P U. Patel Department of Computer Engineering, Changa, India

ABSTRACT

In our present modern world, comprising of e-commerce and other tech driven transactions, like Net Banking, PayPal, etc, there shouldn't be any compromises in which us the consumers abandon broadening amounts of their privacy at the price of better expediency. Here, we talk about RFID (Radio Frequency Identity). It is being rapidly expanded to the prevailing markets with various innovative applications, to name a few: tariff payment in commute, automobile manufacturing, animal tracking, and engineering control. Due to these huge promising applications of RFID, the security of RFID has drawn widespread debate in the academic and industrial world. Now, this is a challenge, to take care of privacy, authentication, integrity, and even availability, all at once. If powerful cryptography mechanisms are to be embedded inside the RFID chips, what lacks is high computing resources. One of the many major challenges while taking care of security in RFID is their very limited resources, which can be up to only 100 bits. In this research, we try to explain some protocols concerning cryptography and security in low cost RFID (also called passive RFID), and compare the outputs and results with a subjective approach

Keywords

Low Cost RFID, Lightweight Cryptography, Security, Authentication

INTRODUCTION

An RFID tag's internal structure is actually quite basic: it has two primary components [1-4]. One is an antenna whose function is to receive and emit radio signals [3]. The other one is a chip consisting of a demodulator and modulator for processing the signal and for memory, a circuit. Other processing of information, and functions dedicated to particular functions such as calculating the scale of a physical phenomenon are also taken care of using this circuit [4-5]. RFID tags are strongly correlated with smart cards, which more than often require physical contact to exchange data with each other. RFID tags also can be minuscule, starting from as little as hundreds of μm2 to a few cm2.

Implementing standard cryptographic solutions on passive low cost RFID just isn't feasible. This dilemma is similar to the problem cryptography experienced in the late 20th Century when smart cards came into the picture. Cryptographers tried to make smart cards safer by implementing more efficient cryptographic primordial and embedding powerful control units in those cards [3].

But although the shortcomings are analogous, the present state of affairs is different. The limiting issue currently isn't technology however price. So, although implementing subtle cryptographic protocols on a small chip is potential for the most part, for cheaper RFID tags, the circuit made for security cannot outstrip a definite space [7].

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 9
September 2017

To come up with appropriate solutions, cryptographers have utilized four primary procedures that were developed in parallel: expeditiously implementing pre-defined ciphers, selecting pre-defined ciphers with terse parameters, planning advanced ciphers, and programming totally dedicated solutions.

PRIVACY CONCERNS

In this section, we discuss about the Popularity of RFID tags and its privacy conerns. The dissemination of RFID tags has given rise to many considerations regarding the loss of privacy such devices may undergo. To take an instance, for a RFID tag needed to determine a product, some assaulter can manipulate the tag to uncover its identifier to figure out the character of the merchandise it's connected to [7, 8-12].

Even sluggish attacks can compromise privacy. Attackers can escalate tracing offenses by connecting the dots of transcripts of many protocol instances to see whether or not identical tag created all the transcripts. Looking on the kind of tag and therefore the attacker's skills, the intruder may be able to manipulate the tag and procure its private key and therefore the memory data held temporarily.

Serge Vaudenay presented a privacy model for RFID tags based on the idea that a security compromise should mirror protocol message outflow [2]. Serge outlined an RFID tag's privacy as adversary's incompetence to glean any useful data from observing each and every interaction within the tag system. The author have outlined security as the tag's competence to be immune to masquerading attacks during which the attacker intends to make the reader settle for a tag with which it didn't exchange data with

- Privacy Model for Low cost RFID systems

Transcribing privacy into mathematical terms has been established as a difficult task, and scientists have planned several approaches. Like for instance, author Stephen Weis and Ari Juels asserted that a protocol is non-public when no attacker can determine what tag, amongst 2 attainable ones he/she has chosen, the protocol is communicating with. Robert Deng and his comrade described an additional generic way to define, by demanding the tags' interactions to be "zero-knowledge" therein the attacker cannot acquire any info from collaborating with a tag [4].

Anyhow, the former two explanations do not take into consideration the case within which the adversary uses many tags at the same time to collapse privacy. While discussing in this regard, Vaudenay's definition is indubitably a lot more complete. Even then, the establishment of the same instinct in mathematical terms imbalances the instinct itself. The definition presumes the presence of a simulator that can yield identical output as the attacker, however without having clearance to protocol messages. Thanks to this discrepancy, scientists have believed achieving advanced levels of privacy are not possible for each of the one-sided authentications, within which the tag solely authenticates itself, and collective authentication, within which both the reader and tag certify them to one another. Khaled Ouafi presented correcting this explanation by providing the machine with all the attacker's information to determine whether or not a statement is important [5].

- Privacy Levels

However, the entire range of RFID tags is not equivalent relating to protection against manipulation. Whilst weaker ones are able to be manipulated while not getting damaged, manipulation of rest of the tags is either not possible or destruction prone. This inequality among tags engenders many privacy levels. Weak level of privacy is intended for attackers that can't manipulate a tag. In forward privacy, change of state eradicates a tag to avert the attacker from uncovering any prior activity of the tag. Strong privacy, that ought to be implemented on feeble tags, takes into account that attackers might find a way to the tags' secrets some other way [1]. Hence, feeble tags, due to their weaker defense structure, assume a skillful attacker, that successively needs stronger security elements.

A person may attain weak privacy by employing a Pseudorandom Function (PRF), by applying the PRF using a secured cipher like Advanced Encryption Standard. Considering that symmetric-key and public-key cryptography are not interdependent on one another, forward privacy sanctions employing public-key encryption. Strong privacy demands even higher number of these leading cryptography primitives. IND-CCA

public-key cryptography protocol like RSA-OAEP (RSA-Optimal uneven Encryption Padding), that satisfies forward privacy, is not adequate to fashion a strong privacy protocol. Rather, a plaintext-aware designed public-key like the Cramer-Shoup cryptosystem provides the most robust privacy.

DEDICATED SOLUTIONS

As we cited earlier, typical cryptographic primitives are not appropriate for RFID tags. Even freshly introduced solutions, that essentially simplify customary solutions, barely match RFID tags' security and performance needs. So, we require additional ingenious solutions

One potential solution is cryptography that has NP-complete issues as the foundation. This field has gone through a lot of analysis and brainstorming since cryptography's origin. That same analysis gave rise to the development of public-key cryptography and also the ambition of coming up with cryptosystems that have "conveniently quantifiable" machine security.

Sadly, the overwhelming bulk of designs based upon NP-complete issues were cracked. As a result, cryptographers cut their focus back to issues that weren't proven to be NP-complete, like discrete logarithms. Anyhow, the prior decade has manifested many ingenious propositions for protocols based upon LPN (Learning Parity with Noise) issue and its generalization, along with the LWE (Learning with Errors) drawbacks. Both issues are proved to be NP-complete. Particularly, scientists have studied these issues to form the HB (Hooper and Blum) group of economical authentication protocols.

- HB protocol

Developed for personal use, the HB (Hooper and Blum) protocol needs terribly easy operations. Which means, for every authentication, each side compute a bit which equals dot product of 2 binary vectors, and also the prover casts its output with probability v to mirror the LPN's noise. The procedure replays r times; and the authentication accomplishes if at least some number of procedures thrive. This protocol is safe solely against attackers who indirectly pay attention to the communication line.

- HB^{+} protocol (Variation 1)

Understanding that RFID tags additionally would require protocols with terribly straightforward operations, Weis and Juels suggested applying the HB protocol for RFID authentication [6]. Later, they developed HB+, a variation that provides security against active attackers. (Regarding RFIDs, this interprets into assuming that the attacker may bluntly reach out to tags and readers, though not at the same time). Sadly, HB+ renders insecure once the attacker has continuous access to all the parts, as shown by the GRS (Gilbert, Robshaw, and Sibert) attack [7].

- $HB^{\#}$ protocol

After an array of experiments to mend HB+ and make it resistant against the GRS attack, Henri Gilbert and his comrades developed HB# [5]. They justified that it is safe against attackers like those taken into account by the GRS attack, till the LPN issue is difficult to unravel. Additionally, they substantiated that HB# was safe against typical man-in-the-middle attacks. This hypothesis clothed to be untrue, because an OOV attack on HB# proved otherwise. Until now, nobody has developed a solution for HB#.

- RFID Parts

We know every RFID system consists of 3 main parts: tag, reader or transceiver and a database, whose function is to store the data required for RFID transferences. The entire RFID tags' network has a couple connections among triple axes of an RFID system, each consisting of a reader, tag and a DB.The link among the DB and reader is made secure using a hard-wired network. The only SPF (single point of failure) which can threaten the safety of a hale system here is the network between the tag & the reader which in most cases is wireless and is open to multiple attacks from various adversaries due to the air medium. Hence, all the efforts would be focused on protecting this media using some cryptography schemes. They must be lightweight based on shortcomings anticipated for computing powers required for storage and hashing for tag and DB, whilst taking the price into consideration.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 9
September 2017

SECURITY ANALYSIS

In favor of satisfying authentication requirements, we must consider the lightweight cryptography techniques which:

- Require little area when built in hardware,
- Have minimum instructions when embedded on a processing chip/device.
- Execute in minimum clock cycles when running on a processing chip/device

Meeting these basic needs is not only cumbersome to achieve but also difficult to provide the same level of security that other standard cryptographic algorithms provide. This requires some well thought out cryptanalysis.

We expect that the intruder is well skilled to get hold of the RFID tag easily and able to do all sorts of manipulation with the device, which might or might not involve getting access to each and every secret data stored in the chip. However, it is our motive that the tampering of the RFID tag should somehow lead to the self-destruction of it. In other words, each tag should afford some secret information that is unique to that tag only, and the reader should have a private key, hence establishing a two-way authentication protocol.

- Symmetric VS Asymmetric

Normally, people choose among the use of symmetric and asymmetric cryptographic approaches. As we have seen above multiple times, the computational power of a tag is limited and in most cases is not sufficient for productive implementation of such high end operations like modular exponentiation that is required by asymmetric encryption algorithms. Hence, the natural choice would be to go with symmetric ciphers accompanied by stream cipher properties, in particular. This choice also requires us to provide a unique secret key to every tag and for the reader to afford to obtain these keys during every authentication session. This is a well-known dilemma which is often solved using a key hierarchy

- Stream Ciphers

There are many arguments pointing towards the fact that stream ciphers are generally faster and give room to more compact hardware design than what block ciphers have to offer. Research in stream ciphers is much behind what block ciphers have gained in the recent years. Stream ciphers mainly deal with military use, and in some cases even governmental use, which might explain the lack of research so as to keep the ciphers secure. However, recent efforts have substantially breached this gap in our proficiency of these 2 sides of a coin that is symmetric encryption. As a response to the challenge by ECRYPT (European Network of Excellence for Cryptology) to develop new stream cipher primitives, over 30 submissions took place from all over the world, by different industrial as well as academic authors. One of the submissions, Pomaranch stream cipher, developed by Cees Jansen turned out to be quite promising, which will be explained next. This stream cipher focuses on hardware implementation, which can be used to cryptanalyze the other submitted stream ciphers as well.

- The Pomaranch Stream cipher

The stream cipher Pomaranch is already considered to be a strong choice for being used in RFID tags, or any other device that uses inductively coupled channels as a communication medium.

The central design principle of this cipher is the use of LFSRs (Linear Feedback Shift Registers) that are clocked sporadically and are aligned in a cascade. Some of other properties of Pomeranch ciphers are:

i) Huge possibilities of adjusting hardware complexity to match the present requirements, all thanks to cascade construction.
ii) The irregular clocking of LFSRs produce 1 bit/cycle.
iii) Presence of keyed bijection allows for block stream ciphers to incorporate block cipher modes which are useful for efficient key managing.
iv) Resistance to side-channel attack.

- The Triangular Cipher

This is another stream cipher that was one of the submissions to ECRYPT, developed in Norway by Professor Igor Semaev. Some properties of this design are as follows:

v) This cipher doesn't use LFSRs and even round structures for that matter. Rather it works with blocks of bits.

vi) Has flexible design as far as software is concerned; hardware implementation requires further research.

vii) If reduction of block size occurs twice, it results in around 3 or 4 times reduction in implementation costs.

viii) A 128-bit software implementation works at least 2 times faster than AES.

ix) No need of specially designed initialization procedures that might affect encryption efficiency.

ȷ Other Security Protocols

i) There are quite many security protocols and schemes like RHLK (Randomized Hashed Lock Scheme), HIDV, SRAC (Semi-Randomized Access Control), HBIV, Li et al. and Hung-Yu Chien and Chen Wei Huang.

ii) RHLK is susceptible to a Spoofing attack.

iii) A-SRAC and Lee et al. are resistant to Replay attacks.

iv) SRAC on the other hand is open to replay attacks. Attacker can impersonate either as a tag or a reader by replaying older transactions.

v) HBIV, LCAP, SRAC and Hung-Yu Chien and Chen Wei Huang are schemes that completely back Forward Security, whereas A-SRAC, LCRP and Li et al. partially back Forward Security.

vi) HIDV, A-SRAC and Li et al support Resynchronization, whereas LCRP doesn't.

vii) HIDV, LCAP and Li et al. provide zero traceability while other protocols like SRAC, HBIV, LCRP and RHLK are not supported against traceability.

viii) LCRP, RHLK, HBIV, LCAP and SRAC are susceptible to DOS attacks, whereas Li et al. is safe against them.

CONCLUSION

Cryptographers are generally pessimistic and tend to consider the worst case scenario, that the attacker is regulating each communication medium. We can perceive the ascent of low cost RFID tags and other devices which cannot execute the convoluted computations necessary. So must make do with what we've got.

On the hardware side of the coin, magnetic memories are the way to go and must replace traditional ones in the coming future. As experts promote new kinds of these magnetic memory devices, cryptographers may be able to make use of that to enhance security like never before. There must be a balance between both software and hardware to achieve a decent level of privacy and most importantly, security

REFERENCES

[1] Benoit Calmels, Sebastien Canard, Marc Girault, and HerveSibert, 2006. Low-Cost Cryptography for Privacy in RFID Systems. France Telecom R&D, France.

[2] S. Vaudenay, "On Privacy Models for RFID," Advances in Cryptology—AsiaCrypt 2007, LNCS 4833, Springer, 2007, pp. 68–97

[3] A. Juels and S.A. Weis, "Defining Strong Privacy for RFID," Proc. 5th Ann. IEEE Int'l Conf. Pervasive Computing and Communications Workshops, IEEE Press, 2007, pp. 342–347; http://eprint.iacr.org/2006/137.

[4] R.H. Deng, "A Zero-Knowledge Based Framework for RFID Privacy," J. Computer Security, vol. 19, no. 6, 2011, pp. 1109–1146.

[5] H. Gilbert, M.J.B. Robshaw, and Y. Seurin, "HB#: Increasing the Security and Efficiency of HB+," Advances in Cryptology—EuroCrypt 2008, LNCS 4965, Springer, 2008, pp. 361–378.

[6] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," Advances in Cryptology—Crypto 2005, LNCS 3621, Springer, 2005, pp. 293–308.

[7] Thomas Eisenbarth, ChristofPaar and Axel Poschmann, Sandeep Kumar, Leif Uhsadel. 2007.A survey of lightweight Cryptography implementations - Co published by the IEEE CS and the IEEE CASS.
[8] P. Bhimani, G. Panchal, "Message Delivery Guarantee and Status Update of Clients based on IOT-AMQP", International Conference on Internet of Things for Technological Development (IoT4TD-2017)-SIST-Springer, Gandhinagar, Gujarat
[9] J. Patel, G. Panchal, "An IoT based Portable Smart Meeting Space with Real-Time Room Occupancy", International Conference on Internet of Things for Technological Development (IoT4TD-2017) - SIST-Springer, Gandhinagar, Gujarat
[10] N. Patel, G. Panchal, "An Approach to Analyze Data Corruption and Identify Misbehaving Server", International Conference on ICT for Intelligent Systems (ICTIS – 2017) - SIST-Springer SIST-Series, Vol. 1, pp. 278-284, Ahmedabad, India
[11] S. Mehta, G. Panchal, "File Distribution Preparation with File Retrieval and Error Recovery in Cloud Environment", International Conference on ICT for Intelligent Systems (ICTIS – 2017) - Springer SIST-Series, Vol. 1, pp 301-307, India
[12] K. Soni, G. Panchal, "Data Security in Recommendation System Using Homomorphic Encryption", International Conference on ICT for Intelligent Systems (ICTIS – 2017) - Springer SIST-Series, Vol. 1, pp. 308-313, India.