sensors

MDPI

Article

SKINNY-Based RFID Lightweight Authentication Protocol

Liang Xiao [1,2], He Xu [1,2], Feng Zhu [1,2], Ruchuan Wang [1,2] and Peng Li [1,2,*]

[1] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; 1018041201@njupt.edu.cn (L.X.); xuhe@njupt.edu.cn (H.X.); zhufeng@njupt.edu.cn (F.Z.); wangrc@njupt.edu.cn (R.W.)

[2] Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China

* Correspondence: lipeng@njupt.edu.cn; Tel.: +86-137-7661-8849

Received: 19 December 2019; Accepted: 26 February 2020; Published: 2 March 2020

Abstract: With the rapid development of the Internet of Things and the popularization of 5G communication technology, the security of resource-constrained IoT devices such as Radio Frequency Identification (RFID)-based applications have received extensive attention. In traditional RFID systems, the communication channel between the tag and the reader is vulnerable to various threats, including denial of service, spoofing, and desynchronization. Thus, the confidentiality and integrity of the transmitted data cannot be guaranteed. In order to solve these security problems, in this paper, we propose a new RFID authentication protocol based on a lightweight block cipher algorithm, SKINNY, (short for LRSAS). Security analysis shows that the LRSAS protocol guarantees mutual authentication and is resistant to various attacks, such as desynchronization attacks, replay attacks, and tracing attacks. Performance evaluations show that the proposed solution is suitable for low-cost tags while meeting security requirements. This protocol reaches a balance between security requirements and costs.

Keywords: RFID system; security protocol; SKINNY; mutual authentication; GNY logic

1. Introduction

The Internet of Things (IoT) is an object network that communicates with other objects through computers connected using the Internet, which can include any object with remote data collection, control, or communication capabilities, such as Automotive Cyber Physical Systems (ACPS), smart vehicles, home appliances, medical instruments, etc. In other words, the IoT involves many interrelated objects. Radio Frequency Identification (RFID) technology is one of the commonly used technologies in IoT and is widely used in various fields [1]. RFID technology integrates communication, storage, and computing components into accessible tags for wireless communication with readers over long distances. Each tag uniquely identifies its carrier while the carrier may be a product in a warehouse, a commodity in a retail store, an animal in a zoo, or a medical device in a hospital [2–4]. With the popularity of IoT technology, the scope of RFID applications has gradually expanded. Practical RFID systems are used in inventory and logistics management, object tracking, access control, automatic charging, anti-theft, localization, and intelligent transportation. According to market research by IDTechEx [5], the total RFID market in 2019 will reach $11.6 billion, and will increase to $13.4 billion in 2022. There exist various forms of passive tags and active tags, such as electronic tags, RFID cards, RFID readers, RFID keychains, and related software and services.

However, since the tag and the reader are wirelessly communicated in the RFID system, the technology suffers from security and privacy threats, i.e., an attacker can eavesdrop on the communication channel to achieve various attacks. The mutual authentication protocol is usually used

to overcome the security attack between the reader and the tag. Since 2002, a lot of researches to secure RFID systems have been carried out, which are generally divided into four categories [6]: Mature protocol [7], simple protocol [8,9], lightweight protocol [10–12], and ultra-lightweight protocol [6,13,14]. Mature protocol refers to the protocols that require support for encryption algorithms in traditional cryptography, such as symmetric encryption, asymmetric encryption, and encrypted one-way functions; simple protocols apply to tags that support pseudo-random number generators and one-way hash functions; a lightweight protocol refers to a protocol whose tag can support pseudo-random number generator (PRNG) and simple functions such as cyclic redundancy code (CRC) check but does not support one-way hash function; ultra-lightweight protocol refers to a protocol that only involves simple bitwise logical operations such as XOR, AND, OR, etc. However, for RFID systems, the limitations of computing power and storage capacity, traditional cryptographic encryption protocols are difficult to apply to low-cost tags (5K–10K logic gates). Since ultra-lightweight protocols use only simple bit-wise operations, it is difficult to meet the security requirements. Furthermore, a large number of proposed ultra-lightweight protocols have been analyzed and attacked by other researchers [15], thus the use of relatively lightweight cryptographic algorithms to ensure the security certification of RFID systems is currently a research hotspot.

Compared with traditional cryptographic algorithms, lightweight algorithms consume fewer resources during calculation and have a higher efficiency, which is very suitable for devices with limited computing capabilities such as RFID. Luo et al. [16] proposed a succinct and lightweight authentication protocol for low-cost RFID system. The authors claim that the protocol can resist various attacks, but Safkhani [17] proved that the protocol has desynchronization attack. Liu et al. [18] proposed an improved two-way authentication protocol for RFID systems. The author reduced the calculation and storage costs of tags by dividing the results obtained by the hash function into two parts, the left and right, to authenticate tags and readers. PRNG guarantees the dynamic update of keys and communication sub-messages, but the hash operation itself is computationally expensive, which is not suitable for low-cost tags. Gao et al. [19] proposed a lightweight RFID security authentication protocol based on the present encryption algorithm, but this protocol is not suitable for EPC C1 Gen2 compliant tags. Xu et al. [20] proposed a lightweight RFID two-way authentication protocol based on physical unclonable functions, using PUF and logical bit operations as security components. The protocol overcomes desynchronization attack by storing messages from the previous session. However, it has proved to be unable to resist a desynchronization attack and secret leak attack [21]. In addition, the stability of physical unclonable functions needs further research to improve. Zhang et al. [22] proposed a lightweight RFID group authentication protocol with strong track privacy protection. However, Gholami et al. [23] proved that the protocol could not resist a desynchronization attack and timeout problem.

In order to solve the above problems, this paper designs an RFID lightweight authentication protocol that meets the EPC standard based on the adjustable block cipher SKINNY algorithm. In this protocol, tags do not need to use hash functions and pseudo-random operations and rely on readers to complete complex pseudo-random operations, further reducing tag calculation costs. At the same time, the SKINNY encryption component guarantees the security of authentication and uses a dynamic update of the authentication sub-messages required for each session to resist tracking attacks. The security analysis proves that the protocol can resist most of the security threats currently existing in RFID systems.

The rest of this paper is composed as follows: In Section 2, the relevant symbol descriptions and a complete description of the protocol proposed in this paper are given. In Section 3, the security of the protocol is analyzed using GNY's formal proof method and informal method. In Section 4, the four aspects of computing, communication, and storage, and security are compared with existing protocols. Finally, we conclude in Section 5.

2. LRSAS Protocol

2.1. Notations

To simplify the description, the symbols and operation instructions of the LRSAS protocol are shown in Table 1.

Table 1. The description of notations.

Notations	Description
R	reader
T	tag
ID	unique identification of T
FID	pseudonym shared by T and R
K	key shared by T and R
r	random number generated by R
$\oplus$	XOR operation
En(X)	SKINNY Encryption

2.2. SKINNY Algorithm

The SKINNY algorithm is a lightweight block cipher proposed by Beierle et al., in 2016 [24], and its security structure belongs to the SPN cipher. SKINNY is a tweakable block cipher with multiple versions of block size and key size, which results in SKINNY being better adaptable to different application environments and having better performance in hardware implementation. Its block size n has 64-bit and 128-bit versions, and the key size t has n, 2n, and 3n versions. Since this paper studies the application in passive 96-bit-EPC-encoded RFID systems, the SKINNY encryption algorithm with a block size of 128 bits and a key size of n is used.

The SKINNY encryption algorithm includes three modules of initialization, the round function, and key scheduling. The encryption process of the three modules is briefly described below. The number of rounds of the SKINNY algorithm is shown in Table 2. In this paper, the block length is 128 bits, the key size is 128 bits, and the encryption round is 40 times.

Table 2. Number of rounds for SKINNY-n-t.

Block Size n / bit	Key Size t / bit	Round Times
64	64	32
	128	36
	192	40
128	128	40
	256	48
	384	56

Initialization. The 96-bit *FID* is divided into 16 8-bit sub-units, in which the high bits are zero-padded $FID = FID_0 \| FID_1 \| \cdots \| FID_{14} \| FID_{15}$, in which FID_i is an 8-bit plaintext subunit. This is represented by a row priority matrix, where $IS_i = FID_i$ for $0 \leq i \leq 15$:

$$IS = \begin{bmatrix} FID_0 & FID_1 & FID_2 & FID_3 \\ FID_4 & FID_5 & FID_6 & FID_7 \\ FID_8 & FID_9 & FID_{10} & FID_{11} \\ FID_{12} & FID_{13} & FID_{14} & FID_{15} \end{bmatrix}$$

The initial key of 128 bits is represented by K, and K is divided into 8-bit sub-units thus that $K = K_0 \| K_1 \| \ldots \| K_{14} \| K_{15}$, in which K_i is an 8-bit key subunit. The row priority matrix is used, where $TK_i = K_i$ for $0 \leq i \leq 15$:

$$TK = \begin{bmatrix} K_0 & K_1 & K_2 & K_3 \\ K_4 & K_5 & K_6 & K_7 \\ K_8 & K_9 & K_{10} & K_{11} \\ K_{12} & K_{13} & K_{14} & K_{15} \end{bmatrix}$$

The Round Function. One encryption round of SKINNY is composed of five operations in the following order: SubCells, AddConstants, AddRoundTweakey, ShiftRows, and MixColumns. The number of rounds to perform depends on the block and key sizes.

Sub Cells(SC): The plaintext matrix IS_i is nonlinearly transformed by the Sbox in units of single bytes. When the subunit is 8-bit, the Sbox is shown in Table 3 (in hexadecimal notation).

Table 3. 8-bit Sbox S_8 used in SKINNY.

x	8bit (00~ff)															
$S_8[x]$	65	4c	6a	42	4b	63	43	6b	55	75	5a	7a	53	73	5b	7b
	35	8c	3a	81	89	33	80	3b	95	25	98	2a	90	23	99	2b
	e5	cc	e8	c1	c9	e0	c0	e9	d5	f5	d8	f8	d0	f0	d9	f9
	a5	1c	a8	12	1b	a0	13	a9	05	b5	0a	b8	03	b0	0b	b9
	32	88	3c	85	8d	34	84	3d	91	22	9c	2c	94	24	9d	2d
	62	4a	6c	45	4d	64	44	6d	52	72	5c	7c	54	74	5d	7d
	a1	1a	ac	15	1d	a4	14	ad	02	b1	0c	bc	04	b4	0d	bd
	e1	c8	ec	c5	cd	e4	c4	ed	d1	f1	dc	fc	d4	f4	dd	fd
	36	8e	38	82	8b	30	83	39	96	26	9a	28	93	20	9b	29
	66	4e	68	41	49	60	40	69	56	76	58	78	50	70	59	79
	a6	1e	aa	11	19	a3	10	ab	06	b6	80	ba	00	b3	09	bb
	e6	ce	ea	c2	cb	e3	c3	eb	d6	f6	da	fa	d3	f3	db	fb
	31	8a	3e	86	8f	37	87	3f	92	21	9e	2e	97	27	9f	2f
	61	48	6e	46	4f	67	47	6f	51	71	5e	7e	57	77	5f	7f
	a2	18	ae	16	1f	a7	17	af	01	b2	0e	be	07	b7	0f	bf
	e2	ca	ee	c6	cf	e7	c7	ef	d2	f2	de	fe	d7	f7	df	ff

Add Constants(AC): The SC-transformed intermediate matrix is added to the round constant, and the round constant is generated by the linear shift register. The generation method can be referred to [24].

Add Round Tweakey(ART): The first 64-bit of the 128-bit intermediate matrix transformed by AC is xor with the first 64-bit of the round key, that is, $IS_i = IS_i \oplus TK_i$ for $0 \leq i \leq 7$, where the round key passes through the key scheduling algorithm.

Shift Rows(SR): For the intermediate matrix of the ART transformation, the second, third, and fourth cell rows are rotated by 1, 2, and 3 positions to the right, respectively. In other words, a permutation P is applied: $P_T[i]$ = [0,1,2,3,7,4,5,6,10,11,8,9,13,14,15,12] for $0 \leq i \leq 15$.

Mix Columns(MC): The SR-transformed intermediate matrix is right-multiplied by the matrix M.

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

The round function $f(x)$ of the block cipher SKINNY-128-128 is shown in Figure 1.

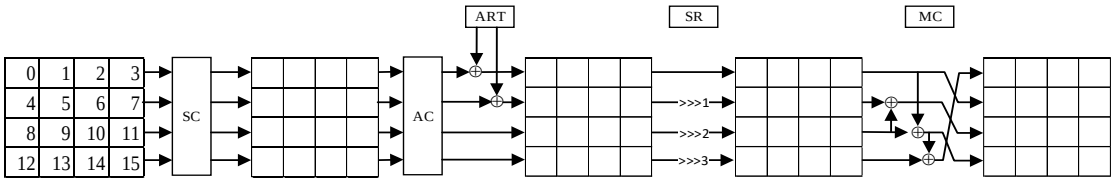

Figure 1. The SKINNY round function.

Key Schedule. Suppose the key size is n, the key scheduling module is implemented by a permutation P_T, which is $P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$. The content of 16 cells are replaced cell by cell according to the subscript rule indicated by P_T, thereby executing key updating.

2.3. LRSAS Protocol Description

In this protocol, passive RFID tags conforming to the 96-bit EPC code are used, which makes the tag limited by hardware and cost and cannot use traditional cryptographic encryption algorithms such as ECC and RSA. However, the lightweight block cipher SKINNY requires only 2391 logic gates under the premise of ensuring security, thus the SKINNY algorithm is very suitable for low-cost tags. The LRSAS protocol mainly includes four phases: Initialization phase, tag identification phase, mutual authentication phase, and update phase.

Initialization phase. There are three values inside each RFID tag: *ID*, *FID*, and *K*. *ID* and *FID* are 96-bit, *K* is 128-bit. *FID* and *K* are updated after each authentication. The back-end database will, respectively, store two sets of entries $\left\{ID, FID^{old}, K^{old}\right\}$ and $\{ID, FID^{new}, K^{new}\}$, which are the values communicated with the tag in the previous and current sessions, where *FID* is the pseudonym obtained by encrypting the *ID* using SKINNY.

Tag identification phase. The reader sends a request message, and the tag sends a response signal FID^{new} to the reader after receiving the request signal. If the reader retrieves the data pair corresponding to FID^{new} in the database, the authentication phase is entered; if the data pair corresponding to FID^{old} is retrieved, the tag may be subjected to a desynchronization attack. In this case, the data pair (FID^{old}, K^{old}) is used for authentication.

Mutual authentication phase. The reader generates a random number *r*, calculates the message M_1 and M_2, and then sends $M_1 \| M_2$ to the tag.

$$M_1 = FID \oplus r \tag{1}$$

$$M_2 = E(FID \oplus ID \oplus r) \tag{2}$$

The tag calculates r' and M'_2. If M_2 and M'_2 are equal, the reader is authenticated. Otherwise, the authentication ends.

$$r' = M_1 \oplus FID \tag{3}$$

$$M'_2 = En(FID \oplus ID \oplus r') \tag{4}$$

The tag calculates message M'_3 and sends it to the reader.

$$M'_3 = En(M'_2 \oplus r') \tag{5}$$

After receiving the message, the reader calculates M_3 according to its own M_2 and *r*. If M_3 and M'_3 are equal, the tag is valid. Otherwise, the authentication ends.

$$M_3 = En(M_2 \oplus r) \tag{6}$$

Update phase. After the reader authenticates the tag, the session enters the updating phase. The reader sends OK information to the tag at the same time. Because the value of the last session tag

is saved, the updating stage is divided into two situations. If the reader uses the (FID^{old}, K^{old}) pair to authenticate, the database will not update the pseudonym and shared key. If the reader uses the (FID^{new}, K^{new}) pair to authenticate, the database will update the pseudonym and the shared key in following way:

$$FID^{old} = FID^{new} \tag{7}$$

$$K^{old} = K^{new} \tag{8}$$

$$FID^{new} = M_1 \tag{9}$$

The updating of the key K^{new} is through the key schedule module in Section 2.2. After receiving the OK message, the tag updates its own pseudonym $FID^{new} = M_1$, and updates the key K^{new} through the key schedule module, which is shown in Figure 2.

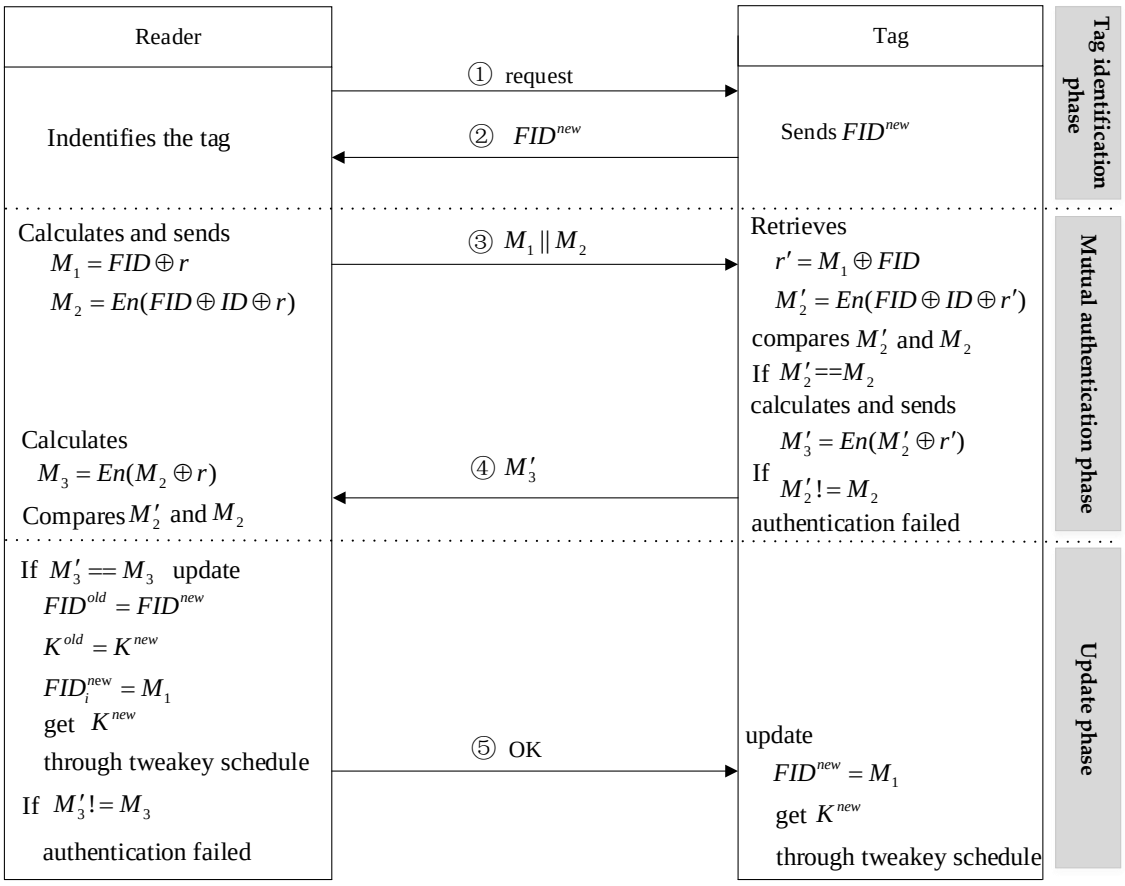

Figure 2. The authentication process of LRSAS.

2.4. Formal Proof of the LRSAS Protocol

In this section, the GNY logic rules are used to prove the security and feasibility of the proposed LRSAS protocol. In this paper, the logical objects of GNY are tags and readers, which are represented by T and R, respectively. The key is represented by K. The formula variables are represented by X and Y. In order to simplify the structure of the article, the details of the GNY logic rules and symbolic representation can be found in [25].

(1) Protocol Initialization Assumption

Before using GNY logic to prove the proposed protocol, several necessary initial assumptions need to be given. Here is a list of specific assumptions:

P1: $T \ni (ID, FID, K)$
P2: $R \ni \left(ID, FID^{old}, K^{old}, FID^{new}, K^{new}, r\right)$
P3: $T \left| \equiv \right. \#(FID)$
P4: $R \left| \equiv \right. \#(r)$
P5: $\mathrm{T} \overset{K,\ FID}{\longleftrightarrow} \mathrm{R}$

(2) Establish an Idealized Protocol Model

M1: R→T: request
M2: T→R: FID
M3: R→T: $FID \oplus \mathrm{r} \left|\right| En(FID \oplus ID \oplus \mathrm{r})$
M4: T→R: $En(En(FID \oplus ID \oplus \mathrm{r}\prime) \oplus \mathrm{r}\prime)$
M5: R→T: confirmation

The above description model can be converted into a model described using GNY logic language as follows:

M1: $T \lhd request$
M2: $R \lhd FID$
M3: $T \lhd FID \oplus r \left|\right| En(FID \oplus ID \oplus r)$
M4: $R \lhd En(En(FID \oplus ID \oplus r\prime) \oplus r\prime)$
M5: $T \lhd$ confirmation

(3) Protocol Target

The proof of the LRSAS protocol is to prove the freshness of the information sent by the other party when communicating with the reader and the reader. The target formula for the proof is as follows:

$$T \left| \equiv \right. R \left| \sim \right. \#(FID \oplus \mathrm{r},\ En(FID \oplus ID \oplus \mathrm{r}))$$
$$R \left| \equiv \right. T \left| \sim \right. \#(En(En(FID \oplus ID \oplus \mathrm{r}\prime) \oplus \mathrm{r}\prime))$$

(4) Protocol Reasoning of GNY Logic

According to GNY logic reasoning and initialization hypothesis, target 1 and target 2 are proved.

a. Proof target 1

According to the inference rule $\frac{\mathrm{A} \lhd (\mathrm{X})}{\mathrm{A} \ni \mathrm{X}}$ and the message M3, it can conclude:

$$T \ni FID \oplus r \left|\right| En(FID \oplus ID \oplus r) \tag{10}$$

According to the inference rule $\frac{\mathrm{A} \lhd (\mathrm{X,Y})}{\mathrm{A} \lhd (\mathrm{X})}$ and the message M3, it can conclude:

$$T \lhd FID \oplus r \tag{11}$$

$$T \lhd En(FID \oplus ID \oplus r) \tag{12}$$

According to the inference rule $\frac{\mathrm{A} \left| \equiv \right. \mathrm{B} \overset{K}{\longleftrightarrow} A, A \lhd \{X\}_K}{A \left| \equiv \right. \mathrm{B} \left| \sim X \right.}$, the assumption P5, and Formula (11), it can conclude:

$$T \left| \equiv \right. \mathrm{R} \left| \sim \right. (FID \oplus r) \tag{13}$$

According to the inference rule $\frac{\mathrm{A}|\equiv \mathrm{B} \overset{K}{\longleftrightarrow} A, A \lhd \{X\}_K}{A|\equiv \mathrm{B}|\sim X}$, the assumption P5, and Formula (12), it can conclude:

$$T|\equiv \mathrm{R}| \sim (En(FID \oplus ID \oplus r)) \tag{14}$$

According to the inference rule $\frac{\mathrm{A}|\equiv \#(\mathrm{X})}{\mathrm{A}|\equiv \#(\mathrm{X},\mathrm{Y}),\mathrm{A}|\equiv \#(\mathrm{F}(\mathrm{X}))}$, the assumption P3, it can conclude:

$$T|\equiv \#(FID \oplus r, En(FID \oplus ID \oplus r)) \tag{15}$$

According to the Formulas (13)–(15), it can conclude: $T \mid\equiv R \mid \sim \#(FID \oplus \mathrm{r},\ En(FID \oplus ID \oplus \mathrm{r}))$

b. Proof target 2

According to the inference rule $\frac{\mathrm{A} \lhd (\mathrm{X})}{\mathrm{A} \ni X}$ and the message M4, it can conclude:

$$R \ni En(En(FID \oplus ID \oplus \mathrm{r}') \oplus \mathrm{r}') \tag{16}$$

According to the inference rule $\frac{\mathrm{A}|\equiv \mathrm{B} \overset{K}{\longleftrightarrow} A, A \lhd \{X\}_K}{A|\equiv \mathrm{B}|\sim X}$, the assumption P5, and the message M3, it can conclude:

$$R|\equiv T| \sim En(En(FID \oplus ID \oplus \mathrm{r}') \oplus \mathrm{r}') \tag{17}$$

According to the inference rule $\frac{\mathrm{A}|\equiv \#(\mathrm{X})}{\mathrm{A}|\equiv \#(\mathrm{X},\mathrm{Y}),\mathrm{A}|\equiv \#(\mathrm{F}(\mathrm{X}))}$, the assumption P4, it can conclude:

$$R|\equiv \#(En(En(FID \oplus ID \oplus \mathrm{r}') \oplus \mathrm{r}')) \tag{18}$$

According to the Formulas (17) and (18), it can conclude: $R \mid\equiv T \mid \sim \#(En(En(FID \oplus ID \oplus \mathrm{r}') \oplus \mathrm{r}'))$

3. Informal Security Analysis

This section will analyze the security of LRSAS from seven security properties, including data confidentiality and integrity, replay attack, impersonation attack, tracking attack, desynchronization attack, denial of service attack, and forward security. The security of LRSAS is demonstrated by the following informal analysis.

Data confidentiality and integrity (DCI). In the authentication process, the (ID, K) of the tag and the r of the reader are transmitted in the form of ciphertext. Due to the security of the SKINNY packet encryption function and the pseudo-random number, the attacker cannot know the corresponding plaintext. In addition, the *FID* is that the tag's pseudonym, which is updated after each successful session, thus the identity information of the tag is not leaked. In this protocol, the random number generation depends on readers with stronger computing capacity. In order to ensure that the random number received by the tag is the same as the random number generated by the reader, M_1 and M_2 contain r and ID. Encryption also guarantees the integrity. The reason is that any bit change of the random number r will result in different results of the ciphertext, leading to authentication failure.

Replay attack (RA). Since the tag and the reader communicate with each other through a wireless communication channel, an attacker can trick another subject by eavesdropping the transmitted sub-message, impersonating the tag or reader, and by replaying the previously received sub-message. It is assumed that the attacker records the information sent by the tag in advance. When the reader communicates with the tag again, the attacker pretends to be a legitimate tag and communicates with the reader through the recorded tag information. The values of *FID* and M_3'. are related to the random number r of the reader. Since the random number of each authentication is different, each value of the tag response is different. Even if the illegal attacker intercepts the previous information, it cannot be used in the next time to forge the value. Therefore, the tag or reader will not accept the copied information.

Impersonation attack (IA). As discussed above, in the process of executing the LRSAS protocol, the tag and the reader need to be mutually authenticated, and the information used by the tag and the reader for mutual authentication is encrypted by the SKINNY algorithm, and the key is already stored in the initialization phase. In the main body, when an attacker wants to spoof another subject by forging one of the subjects, the correct ciphertext for verifying the identity information cannot be generated.

Track attack (TA). In each authentication phase, the tag does not transmit the plaintext of its *ID* or key, and the transmitted messages contain random numbers. In addition, the tag and database update the shared pseudonym *FID* and key *K* after each successful authentication. Second, no unbalanced operations, such as AND or OR operations, are used in the authentication protocol. Therefore, it is not feasible for an attacker to attack the current session by eavesdropping on historical information.

Desynchronization attack (DA). Since the tag and the background database update the pseudonym *FID* and the key *K* in each session, there is a problem that the shared data are inconsistent thus that the legitimate tag is subjected to the desynchronization attack, and thus cannot be authenticated in subsequent sessions. When the adversary tampers with the sub-messages M_1 and M_2, the tag obtains an invalid random number r' through M_1, and then calculates M_2' through the wrong r'. The tag authenticates the reader by comparing whether M_2' and M_2 are equal. Because the protocol guarantees the confidentiality and integrity of the message, the reader authentication fails in this session. The tag does not update information such as pseudonyms and keys and terminates the authentication. In addition, when the attacker interrupts M_3, the illegally generated M_3 will not pass the tag authentication, thus this protocol guarantees the synchronization of the information shared between the tag and the reader.

Denial of service attack (DoS). If the attacker blocks the final confirmation message sent by the reader, the adversary will cause a desynchronization attack. This problem can be overcome by storing the two versions of the (FID, K) values on the reader, storing the old version before the update, and storing the new version after the update. In addition, the tag can send an explicit ACK to confirm that the update phase was successful.

Forward security (FS). Since the pseudonym *FID* and shared key for authentication are updated after each session, and the pseudonym update needs to contain a random number. If the tag is cracked, the attacker cannot discover the historical confidential information. The previous communication of the tag and reader is still secure, which means forward security.

Compared with the security of the protocols proposed with the existing solutions, it can be clearly seen that compared with other protocols, the proposed protocol has the best security performance, as shown in Table 4.

Table 4. Security comparison.

Protocol	DCI	RA	IA	TA	DA	DoS	FS
EMAP [13]	×	√	√	√	×	×	×
SASI [6]	×	√	√	×	√	×	√
Gossamer [14]	√	√	√	√	×	×	√
ECC [7]	√	√	√	√	√	√	√
Present [19]	√	√	√	×	√	√	√
SLAP [16]	√	√	√	√	×	√	√
LRSAS	√	√	√	√	√	√	√

√: Satisfy, ×: Not satisfy.

From Table 4, the EMAP, SASI, and Gossamer protocols, which are ultra-lightweight protocols, are less secure than other lightweight and mature protocols in terms of secret disclosure attacks, denial of service attacks, and desynchronization attacks. Although the protocol based on the elliptic encryption curve achieves effective protection against common attacks, they need too much hardware

resources due to the complexity of the mature encryption algorithm ECC calculation. The lightweight security protocols [16,19] reduce the consumption of hardware resources, but they cannot defend against synchronization attacks and tracking attacks. However, the LRSAS security protocol has reached a balance between security protection and resource consumption. Therefore, the LPSAS protocol has high availability and has a certain role in promoting the development of RFID security authentication protocols.

4. Performance Analysis

In the protocol proposed in this paper, the lightweight block cipher algorithm SKINNY was chosen as a security measure to ensure information confidentiality and integrity. Compared with the SIMON and PRESENT, which are common block ciphers, SKINNY not only has a lightweight key arrangement algorithm but also has the same efficiency as SIMON in execution [24]. This shows that SKINNY is very suitable for a low-cost RFID tag field. In addition, this protocol supports EPC coding for 96 bits. In the following, this paper compares and analyzes the protocol performance in terms of the communication overhead, storage overhead and computational overhead of the tag, as shown in Table 5.

Table 5. Performance comparison.

Overhead	EMAP [13]	SASI [6]	Gossamer [14]	ECC [7]	PRESENT [19]	SLAP [16]	LRSAS
communication	7 L	6 L	6 L	7 L	5 L	4 L	6 L
computational	22×	16×	32× + 3 m	H + r + 2 e + 2 s	4 p + a + r	9 c + 8× + a	4 s + × + a
storage	6 L	7 L	7 L	4 L	4 L	7 L	3 L

Among them, h denotes a hash function operation, r denotes a random number generation operation, e denotes an ECC encryption/decryption operation, a denotes a connection operation, x denotes a logical bit operation, m denotes a MIXBITS operation in Gossamer, c denotes a Con encryption operation in SLAP, s denotes a SKINNY encryption operation, and p denotes a PRESENT encryption/decryption operation. The efficiency of encryption algorithm is x>s>p>m>c>h>e. In addition, L is the length of the pseudonym and key.

The protocol designed in this paper uses one of the SKINNY encryption algorithms and can support 96-bit EPC encoding. The calculation time of the round function used by the SKINNY encryption algorithm in the encryption phase is smaller than the Hash, ECC, and Present encryption calculation. Therefore, the calculation overhead is also applicable to low-cost RFID tags. In addition, the storage overhead of the tag is 3 L, which significantly reduces the storage capacity of the tag compared with other protocols, and lowers the complexity of the logic gate design of the storage structure. Furthermore, in the mutual authentication of the tag and the reader, the protocol has five information interactions, and the total amount of data received and transmitted is 6 L, which is relatively small, thereby ensuring the efficiency of information interaction.

Finally, in terms of the number of equivalent logic gates, different versions of SKINNY have different quantities of equivalent logic gates. This protocol uses SKINNY-128-128 version, the number of equivalent logic gates is 2391, less than 3K. Thus, it can be used in low-cost tags. In addition, the number of equivalent logic gates of other protocols also leads to being vulnerable to certain security attacks. See Table 4 for details.

5. Conclusions

This paper chooses a lightweight block cipher SKINNY, which has the advantages of low hardware power consumption and low computational complexity on the premise of ensuring secure encryption, thus it can be used in low-cost IoT terminal equipment. Based on the algorithm, this paper first designed a lightweight RFID security authentication protocol LRSAS, and then verified its security from

seven security requirements, including data confidentiality and integrity, replay attack, impersonation attack, tracking attack, desynchronization attack, denial of service attack, and forward security, through GNY logic proof and informal security analysis. Finally, the performance analysis of LRSAS and other protocols was performed by comparing communication, storage, and computational overhead, which shows that the protocol can meet the security requirements and hardware overhead of the lightweight protocol.

Author Contributions: Methodology, L.X., and P.L.; validation, L.X., and H.X.; formal analysis, H.X.; writing—original draft preparation, L.X.; writing—review and editing, F.Z.; funding acquisition, R.W. All authors have read and agreed to the published version of the manuscript.

Funding: The subject is sponsored by the National Key R&D Program of China (No. 2018YFB1003201), the National Natural Science Foundation of P. R. China (No. 61672296, No. 61602261, No. 61872196, No. 61872194 and No. 61902196), Scientific and Technological Support Project of Jiangsu Province (No. BE2017166, and No. BE2019740), Major Natural Science Research Projects in Colleges and Universities of Jiangsu Province (No. 18KJA520008), Six Talent Peaks Project of Jiangsu Province (RJFW-111).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, J.; Hassanieh, H.; Katabi, D.; Indyk, P. Efficient and reliable low-power backscatter networks. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *42*, 61–72. [CrossRef]
2. Shahzad, M.; Liu, A.X. Expecting the unexpected: Fast and reliable detection of missing RFID tags in the wild. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 26 April–1 May 2015; pp. 1939–1947.
3. Qi, S.; Zheng, Y.; Li, M.; Lu, L.; Liu, Y. COLLECTOR: A secure RFID-enabled batch recall protocol. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 1510–1518.
4. Xiao, Q.; Chen, M.; Chen, S.; Zhou, Y. Temporally or Spatially Dispersed Joint RFID Estimation Using Snapshots of Variable Lengths. In Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Hangzhou, China, 22–25 June 2015; pp. 247–256.
5. RFID Report. Available online: https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700 (accessed on 2 February 2020).
6. Chien, H. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Trans. Dependable Secur. Comput.* **2007**, *4*, 337–340. [CrossRef]
7. Jin, C.; Xu, C.; Zhang, X.; Zhao, J. A Secure RFID Mutual Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptography. *J. Med. Syst.* **2015**, *39*, 24. [CrossRef] [PubMed]
8. Ding, Z.; Li, J.; Feng, B. Research on RFID security authentication protocol based on hash function. *J. Comput. Res. Dev.* **2009**, *46*, 583–592.
9. Zhou, Y.; Feng, D. Design and analysis of RFID security protocol. *Chin. J. Comput.* **2006**, *29*, 581–590.
10. Wei, G.; Zhang, H. A lightweight authentication protocol scheme for RFID security. *Wuhan Univ. J. Nat. Sci.* **2013**, *18*, 504–510. [CrossRef]
11. Gope, P.; Hwang, T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Comput. Secur.* **2015**, *55*, 271–280. [CrossRef]
12. Zhou, J.; Zhou, Y.; Gu, Z. Lightweight RFID two-way authentication protocol with constant time. *J. Beijing Univ. Posts Telecommun.* **2016**, *39*, 60–63.
13. Peris-Lopez, P.; Hernandez-Castro, J.C.; Estevez-Tapiador, J.M.; Ribagorda, A. EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags. In Proceedings of the On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, and Posters, AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET, OnToContent, ORM, PerSys, OTM Academy Doctoral Consortium, RDDS, SWWS, and SeBGIS 2006, Montpellier, France, 29 October–3 November 2006; pp. 352–361.
14. Peris-Lopez, P.; Hernandez-Castro, J.C.; Tapiador, J.M.E.; Ribagorda, A. advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. *Int. Workshop Inf. Secur. Appl.* **2009**, *5379*, 56–68.
15. Safkhani, M.; Shariat, M. Implementation of secret disclosure attack against two IoT lightweight authentication protocols. *J. Supercomput.* **2018**, *74*, 6220–6235. [CrossRef]

16. Luo, H.; Wen, G.; Su, J.; Huang, Z. SLAP: Succinct and lightweight authentication protocol for low-cost RFID system. *Wirel. Netw.* **2018**, *24*, 69–78. [CrossRef]
17. Safkhani, M.; Bagheri, N. Generalized desynchronization attack on UMAP: Application to RCIA, KMAP, SLAP and SASI+ protocols. *IACR Cryptol. ePrint Archive* **2016**, *2016*, 905.
18. Liu, B.; Yang, B.; Su, X. An improved two-way security authentication protocol for RFID system. *Information* **2018**, *9*, 86. [CrossRef]
19. Gao, X.; Lv, S.; Zhang, H.; Li, X.; Ji, W.; He, Y.; Li, X. A kind of RFID security protocol based on the algorithm of present. In Proceedings of the 5th International Conference on Systems and Informatics, Nanjing, China, 10–12 November 2018; pp. 50–55.
20. Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors* **2018**, *18*, 760. [CrossRef]
21. Bendavid, Y.; Safkhani, M.; Rostampour, S. IoT device security: Challenging a lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors* **2018**, *18*, 4444. [CrossRef]
22. Zhang, W.; Liu, S.; Wang, S.; Yi, B.; Wu, L. An efficient lightweight RFID authentication protocol with strong trajectory privacy protection. *Wirel. Pers. Commun.* **2017**, *96*, 1215–1228. [CrossRef]
23. Gholami, V.; Alagheband, M. Provably privacy analysis and improvements of the lightweight RFID authentication protocols. *Wirel. Netw.* **2019**, 1–17. [CrossRef]
24. Beierle, C.; Jean, J.; Kölbl, S.; Leander, G.; Moradi, A.; Peyrin, T.; Sasaki, Y.; Sasdrich, P.; Sim, S.M. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; pp. 123–153.
25. Gong, L.; Needham, R.; Yahalom, R. Reasoning about belief in cryptographic protocols. In Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 7–9 May 1990; pp. 234–248.