

Article

Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography

Byoungjin Seok ¹, Jose Costa Sapalo Sicato ¹, Tcydenova Erzhena ¹, Canshou Xuan ¹,
Yi Pan ² and Jong Hyuk Park ^{1,*}

¹ Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung-ro, Nowon-gu, Seoul 01811, Korea; sbj7534@seoultech.ac.kr (B.S.); josecostasicato@seoultech.ac.kr (J.C.S.S.); etcydenova@seoultech.ac.kr (T.E.); shou19@seoultech.ac.kr (C.X.)
² Department of Computer Science, Georgia State University, Atlanta, GA 30302-5060, USA; yipan@gsu.edu
* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-02-970-6702

Received: 12 November; Accepted: 23 December 2019; Published: 27 December 2019



Abstract: Device-to-device (D2D) communication is a direct means of communication between devices without an intermediate node, and it helps to expand cell coverage and to increase radio frequency reuse in a 5G network. Moreover, D2D communication is a core technology of 5G vehicle-to-everything (V2X) communication, which is an essential technology for autonomous driving. However, typical D2D communication in an 4G network which is typical telecommunication network has various security challenges including impersonation, eavesdropping, privacy sniffing, free-riding attack, etc. Moreover, when IoT technology emerges with 5G networks in massive machine type communication (mMTC) and ultra-reliable low latency communication (URLLC) application scenarios, these security challenges are more crucial and harder to mitigate because of the resource-constrained nature of IoT devices. To solve the security challenges in a 5G IoT environment, we need a lightweight and secure D2D communication system that can provide secure authentication, data confidentiality/integrity and anonymity. In this paper, we survey and analyze existing results about secure D2D communication systems in terms of their security considerations and limitations. Then, we lastly propose a secure D2D communication system to address the aforementioned security challenges and the limitations of the existing results. The proposed secure D2D communication was designed based on elliptic curve cryptography (ECC) and lightweight authenticated encryption with associated data (AEAD) ciphers to cover resource-constrained IoT devices.

Keywords: D2D communication; 5G IoT network; lightweight cryptography; authentication

1. Introduction

D2D communication is a peer-to-peer communication mechanism between devices without an intermediate node [1,2]. D2D communication has many advantages in mobile networks [3]. First, it can expand coverage of each cell in a cellular network as a communication bridge for transmitting data to the node located outside of cell coverage. Second, D2D communication helps to reduce the energy consumption of the base station by transmitting data directly between devices. Lastly, the efficiency of reusing the same radio frequency is increased. In D2D communication, the distance between devices is quite shorter than the distance between a device and a base station. This means the interference of radio frequency decrease in D2D communication scenario, and it helps to transmit the multiple data using the same radio frequency. Moreover, D2D communication is a core technology of V2X communication [4]. Due to these advantages, the 5G network also includes D2D communication technology such as the LTE-advanced (4G) network.

However, typical D2D communication in a mobile network has some security challenges [5]. The D2D communication mechanism consists of three procedures, device discovery, link setup and data transmission [6]. In this process, there is no authentication process for validating device identity. When a device sends a request for a setup link to transmit data, another node replies by sending an acknowledgement message. Moreover, D2D communication does not use encryption for confidentiality and message authentication for integrity in the communication process. This means the attacker can conduct attacks such as impersonation, eavesdropping, privacy sniffing, free-riding and location spoofing. Besides, IoT technology is combined with the 5G network to address their service demands [7], and it corresponds to mMTC and URLLC, which are the use-cases of the 5G network [5]. However, IoT applications deal with many sensitive data, and IoT devices have limited resources [8] in terms of performance, memory and power consumption. These features of IoT make the aforementioned security challenges more critical and harder to address because typical security solutions cannot be implemented or processed properly. To overcome the security challenges of D2D communication in the 5G IoT network, we need a secure D2D communication system that contains a proper authentication process between devices. Moreover, considering the resource-constrained environment, it has to be made light.

Lightweight cryptography can be a proper solution for covering resource-constrained devices. Elliptic curve cryptography (ECC), which is most representative of lightweight asymmetric-key algorithms, can provide 128-bit cryptographic security using a 256-bit key, which is significantly smaller than the 3072-bit key of the most widely used public-key encryption algorithm RSA [9]. ECC has been applied to various cryptographic algorithms including elliptic curve Diffie–Hellman (ECDH) and the elliptic curve digital signature algorithm (ECDSA). ECDH and ECDSA are both cryptographic public-key algorithms but they have different purposes: ECDH is used for key exchange and ECDSA is a variation of the digital signature algorithm. ECDH is a variation of the Diffie–Hellman algorithm for elliptic curves, which is a cryptographic key agreement protocol that allows two parties with public/private key pairs on elliptic curves to obtain a shared secret key using an unprotected communication channel. ECDSA is a public key algorithm for creating a digital signature, similar in structure to a DSA, but defined, in contrast to it, not above the ring of integers, but in a group of points of an elliptic curve. In the case of the symmetric-key algorithms, many lightweight AEAD ciphers have been proposed recently to deal with a resource-constrained environment; moreover, the standardization project at the National Institute of Standards and Technology (NIST) is in process [10]. AEAD ciphers can provide not only data confidentiality but also data integrity and authentication using a message authentication code (MAC) with associated data during the encryption process. These lightweight cryptographic algorithms help to make D2D communication secure and able to process communication efficiently.

In this paper, we propose a secure D2D communication system for a 5G IoT network based on lightweight cryptography ECC and the AEAD cipher. First, we analyze typical security threats and present security considerations for D2D communication in a 5G IoT network. Moreover, we survey the existing research on secure D2D communication schemes and make a taxonomy of these results based on our security considerations. Finally, we propose a lightweight cryptography-based secure D2D communication system that can provide anonymity, user authentication, data confidentiality/integrity and efficiency. Because of its lightweight construction, the proposed D2D communication system can be applied efficiently on the 5G IoT network. Our main contributions can be summarized below:

- We analyze existing typical security threats and secure D2D communication. Then we present security considerations for secure D2D communication for a 5G IoT network.
- We survey and analyze existing research based on our security considerations, including authentication, data confidentiality/integrity, anonymity and efficiency.
- We propose a lightweight and secure D2D communication system. The proposed D2D communication system is designed based on lightweight cryptography. It can be implemented simply and can efficiently process resource-constrained 5G IoT devices.

The remainder of this paper is organized as follows. Section 2 introduces related works where we surveyed D2D communication and analyzed security considerations for secure D2D communication. In Section 3, we propose a secure D2D communication system for a 5G IoT network. In Section 4, we show the simulation results of our proposed D2D communication system. In Section 5, we analyze our proposed D2D communication system based on our security considerations and finally conclude in Section 6.

2. Related Work

2.1. Typical Security Threats of D2D Communication

D2D communication involves three steps, device discovery, link setup and data transmission, to make a direct connection between devices. In the device discovery step, the device searches for nearby devices. Then devices that are discovered in the previous step make a connection for transmitting data in the link setup step. After a connection is established, the data is transmitted through a direct link in the data transmission step. However, if there are no proper security measures, the data can be vulnerable to some security threats by attackers. Typical security threats of D2D communication introduced in [5] are as follows:

- Impersonation attack. In this attack the attacker acts like a legitimate user by using an identity such as an international mobile subscriber identity (IMSI). To prevent this attack proper authentication of users has to be considered.
- Eavesdropping. This is a type of attack where the attacker passively listens to communication between users and thereby the attacker can capture the transmitted data and also can fabricate the data. To prevent this attack, data confidentiality and integrity have to be considered.
- Privacy sniffing. D2D communication has to broadcast request messages to search for nearby devices. However, the attacker uses this feature to find and track the victim device. To mitigate this security threat, the devices have to use an anonymous identity, and it has to be authenticated.
- Free riding attack. Selfish devices receive the desired data from other devices but do not share their resources because of energy consumption and because of this they reduce system availability. To mitigate this attack, the user identity has to be authenticated and managed by a base station.
- Location spoofing. In this attack a malicious device may broadcast a request message with wrong or artificial location information to disrupt D2D communication in the device discovery step. To mitigate this attack, the request message has to be processed only from validated devices in D2D communication.

2.2. Security Considerations for a 5G IoT Network

In a 5G network, IoT applications correspond to mMTC and URLLC scenarios. For the security of D2D communication against threats, the D2D communication system has to provide security functions including authentication, data confidentiality/integrity and anonymity. However, IoT devices have limited resources in terms of performance, memory and power consumption. Therefore, the security functions must also provide efficiency, meaning that each security function has to be implemented lightly and run faster. The detailed description of security considerations are as follows:

- Authentication. Authentication is a key requirement for securing D2D communication in the 5G IoT network. For most types of attacks, proper user authentication is the most basic and appropriate solution. Every network should be able to verify the identity of users in order to guarantee the security of the network.
- Data confidentiality and Integrity. The data transmitted in the IoT network contains sensitive information, and due to a variety of attacks that can eavesdrop on or modify that information, confidentiality and integrity are a big concern. For providing this, we have to encrypt the transmitted data and use hash functions or message authentication algorithms.

- **Anonymity.** Anonymity refers to hiding the identity of origin and sensitive information such as location. Anonymity is a necessary security function to prevent attackers from targeting specific users for their purpose. In such cases, when anonymity is not provided, the attacker can choose a specific target for the attack. If you take the example of autonomous vehicles, the attacker may decide to attack a specific car. Therefore, anonymity should be considered extensively.
- **Efficiency.** Efficiency is the communication system's ability to be implemented and to operate economically. This consideration is about availability, which means that authorized users can access the information at any time they request it. This consideration is especially critical when it comes to the IoT network because IoT devices have limited resources.

2.3. Existing Research

Mingsheng Cao et al. [11] proposed a secure lightweight D2D communication system with multiple sensors. Their proposed communication system is designed based on lightweight key generation and a distribution scheme by leveraging an acceleration sensor and secure near field authentication by using a device's microphone and speaker as sensors and for data transmission, which includes encryption/decryption by audio and RF channels. Adeel Abro et al. [12] proposed a lightweight authentication scheme based on elliptic ElGamal encryption, which is public key algorithm based on elliptic curve discrete logarithm problem (ECDLP). This paper presents an authentication scheme based on public key infrastructure (PKI) and uses a combination of ECC to select key pair and ElGamal encryption to exchange the secret key. Yasir Javed et al. [13] also proposed a lightweight security scheme based on ECC and ElGamal encryption over public key infrastructure. This paper uses ECC to create keys and ElGamal for encryption and decryption. Atefeh Mohseni-Ejyeh et al. [14] proposed an incentive-aware lightweight secure data sharing scheme for D2D communication in 5G networks. In their proposed scheme, users obtain digital signatures to prove successful data sharing and, in the sharing process, the symmetric encryption algorithm and MAC are used. Haowen Tan et al. [15] proposed a D2D authenticating mechanism employing smartphone sensor behaviour analysis. Their authentication scheme is designed based on certificateless cryptography for group authentication and user's behavior analysis extracted from smartphone sensors is employed for continuous authentication. Sheeba Backia, Mary Baskaran et al. [16] proposed a lightweight key exchange mechanism for LTE-A assisted D2D communication that can be applied in 5G networks. Their mechanism is designed by using ECC-based symmetric keys. Yunqing Sun et al. [17] proposed privacy protection device discovery and an authentication mechanism for D2D using the identity-based prefix encryption and ECDH key agreement protocol. All of these studies can provide authentication and data confidentiality/integrity and most of them use ECC based cryptographic algorithms. However, they have some limitations in that some of the results cannot provide anonymity or the researches did not deeply consider the data transmission step of D2D communication. Moreover, most of the existing schemes use only lightweight public key algorithms not lightweight symmetric encryption algorithms. Table 1 shows a taxonomy of strategies of existing research in terms of the security functions provided (confidentiality/integrity, authentication, anonymity) and the steps considered (device discovery, link setup, data transmission). Since our proposed system uses ECC and lightweight AEAD cipher for covering our security considerations and all of the steps in D2D communication, it can improve the efficiency and security of D2D communication.

Table 1. Taxonomy of strategies of existing secure device-to-device (D2D) communication.

Ref.	Security Function			Considered D2D Step		
	Conf. / Int.	Auth.	Anon.	D.D.	L.S.	D.T.
Mingsheng Cao et al. [11]	✓	✓		✓	✓	✓
Adeel Abro et al. [12]	✓	✓		✓	✓	✓
Yasir Javed et al. [13]	✓	✓		✓	✓	✓
Atefeh Mohseni-Ejyeh et al. [14]	✓	✓		✓	✓	✓
Haowen Tan et al. [15]	✓	✓	✓	✓	✓	
Sheeba Backia Mary Baskaran et al. [16]	✓	✓	✓	✓	✓	
Yunqing Sun et al. [17]	✓	✓	✓	✓	✓	

3. Secure D2D Communication

3.1. Proposed D2D System Model

In this section, we propose a secure D2D communication mechanism for a 5G IoT network based on lightweight AEAD ciphers. The proposed secure D2D communication model is shown in Figure 1. Objects participating in D2D communication consist of 5G network components including user equipment (UE), general node-B (gNB), access and mobility management function (AMF)/security anchor function (SEAF) and user data management (UDM). UE is a device that is a mobile entity in a 5G network, and UE is an actual device that communicates with other devices directly in our system. gNB is a base station responsible for connecting UE to mobile networks. In our system, gNBs share their public key with other gNBs in advance and use their private key to generate D2D tokens ($D2DTK_{gNB_x}$) via ECDSA. Moreover, AMF is responsible for the management of a mobile entity. SEAF is a middle entity of authentication between UE and a 5G network and is co-located with AMF. UDM stores information about mobile entities in a 5G network. A 5G network provides the authentication framework using 5G-AKA to verify the identity of the UE. 5G-AKA is used to authenticate the UE's validity before generating a D2D token for use in communication in the proposed secure D2D communication. It is corresponded to step 0 in the proposed D2D system, and this process is performed only once for each UE.

After generating a D2D token, the D2D communication process has three steps similar to a typical D2D communication system: Device discovery, link setup and secure data transmission. However, in each process, there are features for security such as anonymity, authentication and confidentiality/integrity. We will discuss the details of these features in Section 3.2. The brief descriptions of each process are as follows:

- Device discovery is a process that searches for nearby nodes. In this step, nodes in a network broadcast a request message to discover other nodes. If a node receives a request message, it sends a response message to another node. The broadcast or response message in this process includes each UE's encrypted identity SUCI and the issued D2D token.
- Link setup is a process for making a peer-to-peer connection between two nodes. During this process, each node sends a verification request to its base station, gNB, with the SUCI and D2D token of the target UE being received in the device discovery phase. After verification, ECDH is used to exchange secret keys for secure data transfer.
- Secure data transmission is a process where data is transmitted. The main feature of this step is that the data is encrypted using a lightweight AEAD cipher before transmission. In the encryption process, the sender node uses its D2D token identity and context sequence, thereby the confidentiality and integrity of the data are ensured. Moreover, authentication is processed in every transmission.

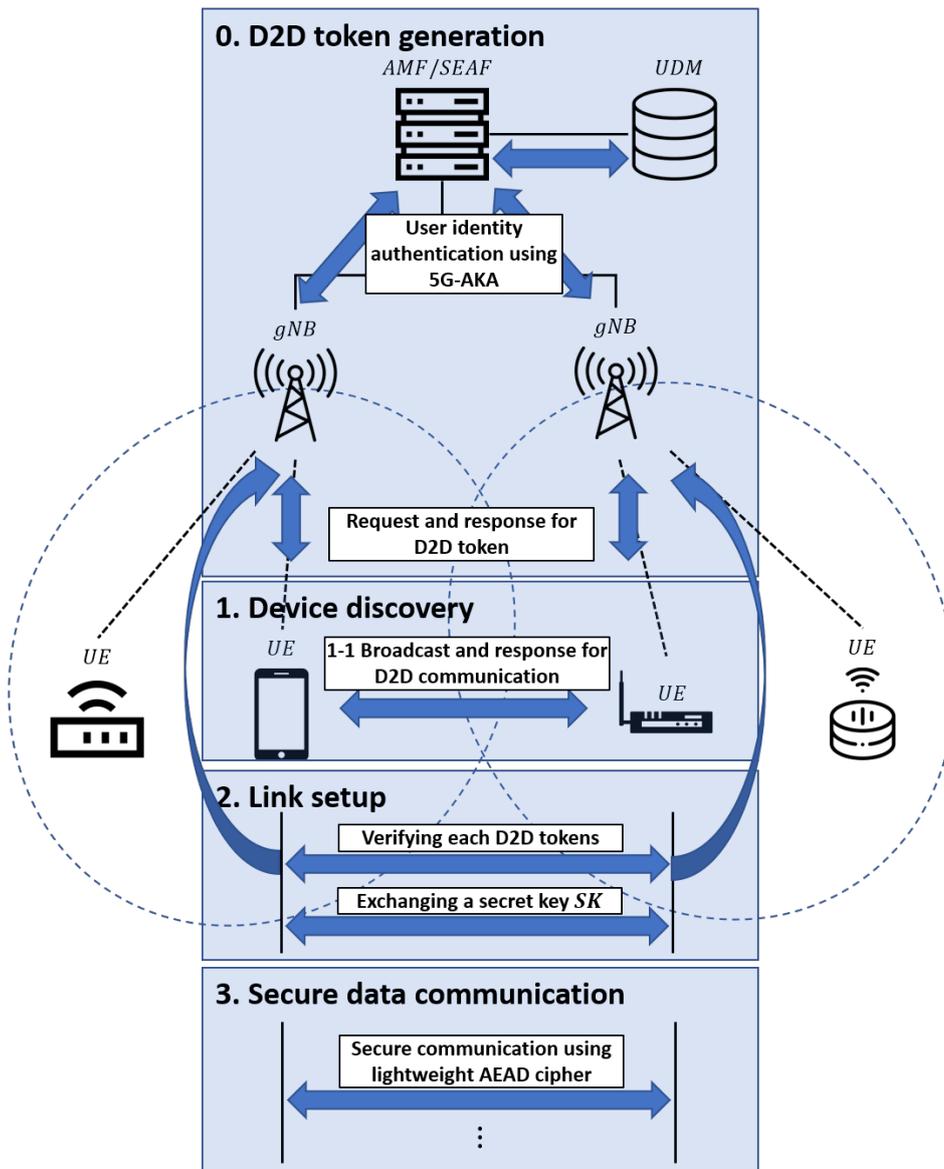


Figure 1. Secure D2D communication system model for a 5G Internet of Things (IoT) network.

3.2. Details of Communication Mechanism

This section deals with the detailed process for the proposed D2D communication system. As described in the system model, the proposed D2D communication system has four steps in total. These four steps may be classified into one pre-processing step performed before D2D communication and the remaining three steps in which actual D2D communication is performed. The pre-processing step is the D2D token generation step (corresponding to step 0), and the steps in which D2D communication is performed are device discovery, link setup and secure data transmission (corresponding to steps 1–3, respectively).

First, in the D2D token generation step, each UE sends a request to the gNB to generate a D2D token for later use in D2D communication. The gNB that receives the D2D token generation request first verifies the identity of the UE that sent the request. At this time, the identity of the UE verifies the SUCI, which is an encrypted identity that emerges for user privacy in a 5G network. Unlike IMSI, the identity of the UE used in existing 4G networks, the SUCI can provide anonymity for the UE as a result of encrypting the IMSI using a public key (PUK). The verification for SUCI is performed using 5G-AKA, an authentication framework for performing primary authentication of UE registration in

5G networks. The subject that performs the actual verification is AMF/SEAF, and the verification is performed by comparing the credentials obtained by decrypting SUCI with the user credentials stored in the UDM. When the SUCI verification is completed, the result is transmitted to the gNB, and accordingly the gNB generates a D2D token and transmits it to the requesting UE. The generation of the D2D token uses the digital signature value calculated by the ECDSA of the UE's SUCI using the gNB's private key (PRK). The issued D2D token may also give anonymity to the UE with a value generated through a cryptographic algorithm by using the identity of the UE like SUCI. The issued D2D token can be verified if the SUCI of the UE and the public key of the gNB are known (note that each gNB shares the public key we mentioned in the previous section). The D2D token generation procedure is shown in Figure 2.

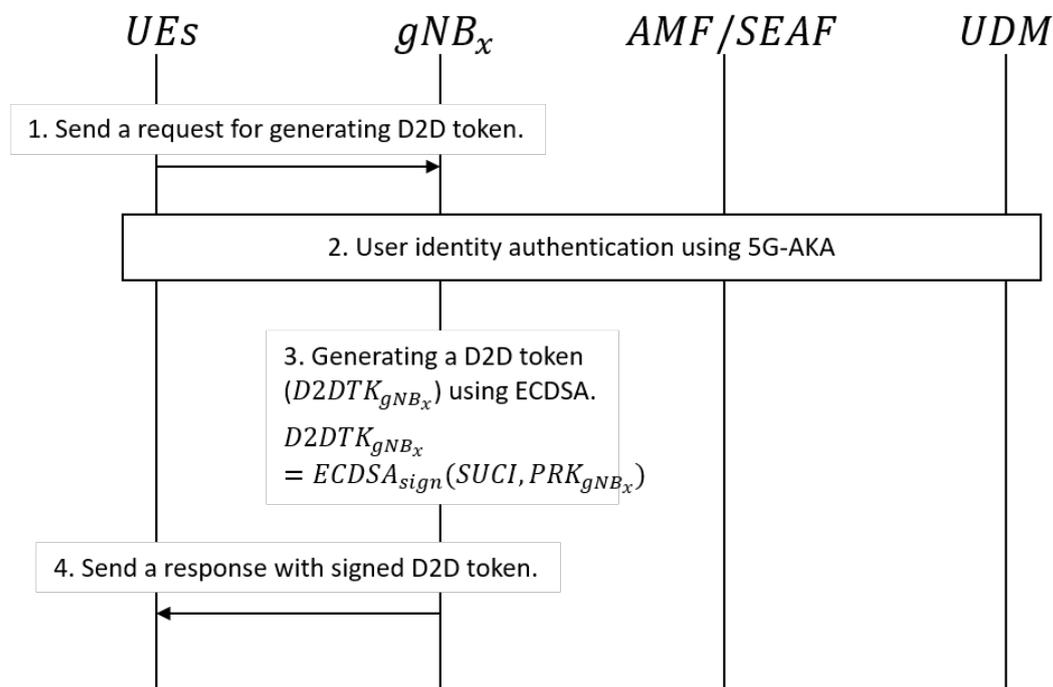


Figure 2. D2D token generation procedure.

From now on, actual D2D communication performing steps will be described. The whole process of proposed D2D communication is shown in Figure 3. Step 1 is device discovery, which is a process of searching for a nearby device with which to perform D2D communication. Here, each UE desiring D2D communication broadcasts a message requesting to perform D2D communication, and UEs in a state capable of D2D communication transmit a response message to the received D2D request message. Here, the broadcast message or response message includes the D2D token issued in step 0 and its SUCI. If a response message to the broadcasted request message is received, the process proceeds to the next step.

The second stage of D2D communication is the link setup to establish a communication session. In this step, prior to establishing a communication session, verification is performed on the D2D token exchanged through device discovery. The verification of the D2D token performed here is similar to the UE identity verification performed in the D2D token generation, but the authentication is performed in the gNB without connecting to the core network. The D2D token can be verified using the public key and SUCI of each gNB, which authenticates that the D2D token has been issued from the gNB by request by a pre-authenticated UE. When the verification of the D2D token is completed, the secret key exchange used in the encryption process of the data transmission step is performed according to the result. The exchanged secret key is a secret key derived from the secret keys of both UEs using ECDH.

Therefore, even if the attacker taps the data transmitted in the middle of the key exchange, the secret key cannot be derived.

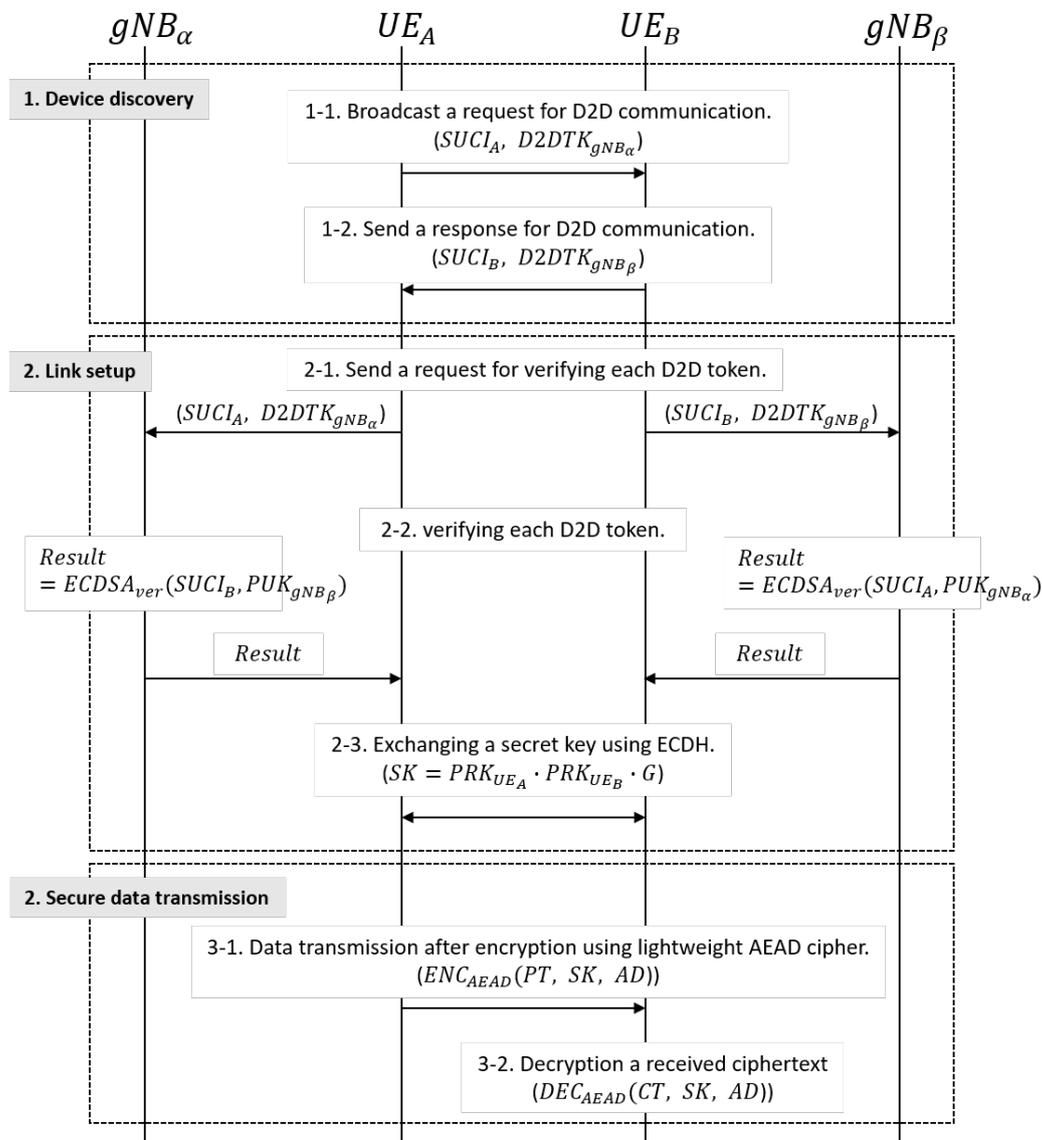


Figure 3. The whole process of secure D2D communication.

Secure data transmission, the last step of the proposed D2D communication, performs data encryption communication. At this time, encryption uses a lightweight AEAD cipher. The lightweight AEAD cipher is a cryptographic algorithm that provides not only confidentiality but also integrity and authenticity. It encrypts the data to be transmitted and creates a MAC for authenticating data integrity. Moreover, in the encryption process, the AEAD cipher uses additional information about a communication session and the other party, called the associated data (AD), thereby the AEAD cipher provides authenticity, which means the message is transmitted from the right party at the right time. In the proposed D2D communication system, the AD consists of the D2D token and context sequence information and manages the sequence for each transmission. Upon receiving the cipher text using the AD configured as described above, the UE may check whether the other UE performing D2D communication has received data corresponding to the current situation along with authentication. The data format used in secure data transmission is shown in Figure 4. In this step, any lightweight AEAD cipher can be applied according to available resources. Table 2 shows available lightweight

AEAD ciphers which are candidate cipher from NIST lightweight cryptography standardization (Round 2) [10].

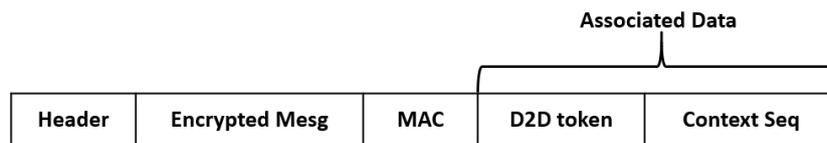


Figure 4. Data format for data communication.

Table 2. A list of lightweight authenticated encryption with associated data (AEAD) ciphers (National Institute of Standards and Technology (NIST) lightweight cryptography standardization (Round 2)).

Candidates	Type	Functionality
ACE	Permutation based	AEAD and Hashing
ASCON	Permutation based	AEAD and Hashing
COMET	Block cipher based	AEAD only
DryGASCON	Permutation based	AEAD and Hashing
Elephant	Permutation based	AEAD only
ESTATE	Tweakable block cipher based	AEAD only
ForkAE	Tweakable block cipher based	AEAD only
GIFT-COFB	Block cipher based	AEAD only
Gimli	Permutation based	AEAD and Hashing
Grain-128AEAD	Stream cipher based	AEAD only
HYENA	Block cipher based	AEAD only
ISAP	Permutation based	AEAD only
KNOT	Permutation based	AEAD and Hashing
LOTUS-AEAD/LOCUS-AEAD	Tweakable block cipher based	AEAD only
mixFeed	Block cipher based	AEAD only
ORANGE	Permutation based	AEAD and Hashing
Oribatida	Permutation based	AEAD only
PHOTON-Beetle	Permutation based	AEAD and Hashing
Pyjamask	Block cipher based	AEAD only
Romulus	Tweakable block cipher based	AEAD only
SAEAES	Block cipher based	AEAD only
Saturnin	Block cipher based	AEAD and Hashing
SKINNY-AEAD/SKINNY-HASH	Tweakable block cipher based	AEAD and Hashing
SPARKLE	Permutation based	AEAD and Hashing
SPIX	Permutation based	AEAD only
SpoC	Permutation based	AEAD only
Spook	Tweakable block cipher based	AEAD only
Subterranean 2.0	Permutation based	AEAD and Hashing
SUNDAE-GIFT	Block cipher based	AEAD only
TinyJambu	Block cipher based	AEAD only
WAGE	Permutation based	AEAD only
Xoodyak	Permutation based	AEAD and Hashing

4. Simulation Results

In this section, we conduct a simulation to evaluate the proposed D2D communication system in terms of performance and efficiency. The performance in this section shows the whole processing time of the proposed D2D communication process. Moreover, for evaluating the efficiency of the proposed D2D communication, we perform analysis of implementation cost of lightweight AEAD ciphers, and simulate energy consumption according to AEAD ciphers.

The proposed D2D communication includes cryptographic algorithms for providing our security considerations (authentication, data confidentiality/integrity, anonymity). In detail, the applied cryptographic algorithms are the digital signature, the Diffie–Hellman key exchange algorithm and the AEAD cipher. We suppose that the processing time of each cryptographic algorithm is as follows.

The processing time for signing of a digital signature $t_{DS_{sign}}$, the processing time for verification of a digital signature $t_{DS_{ver}}$, the processing time for key exchange t_{DH} and the processing time for the AEAD cipher t_{AEAD} . Then we suppose the transmission latency in D2D communication is l_{tr} . Finally, we can estimate the total length of the D2D communication processing time t_{D2D} through Equation (1).

$$t_{D2D} = \sum l_{tr} + \sum t_{DS_{sign}} + \sum t_{DS_{ver}} + \sum t_{DH} + \sum t_{AEAD} \tag{1}$$

For calculating the summation of each processing time, we analyze the proposed D2D communication in terms of the number of transmissions and the usage count of the cryptographic algorithm at each step. In D2D token generation (step 0), there are two transmissions, request and response, for a D2D token; this step also includes 5G-AKA for user identity authentication. The 5G-AKA have 10 transmissions between UEs, gNB, AMF and UDM. In terms of the usage of the cryptographic algorithm, the D2D token generation step uses ECDSA-signing to process token generation. Moreover, we assume that the 5G-AKA consists of ECDSA-signing and ECDSA verification because the 5G-AKA is based on the ECC certificate. In device discovery (step 1), the requested UE broadcasts the request message; this means that the number of transmissions for a request message equal the number of devices (m), which are located near the sender UE. Moreover, in this step, there is a transmission to response. In link setup (step 2), when two devices set the connection, there are transmissions, including two for token verification, two for response of verification and two for key exchange, and there are the usages of the cryptographic algorithm, including two for ECDSA verification and one for ECDH. Lastly, the secure data transmission (step 3) has transmissions according to the amount of data (n bytes), and we assumed that data are transmitted in packets and in units of 1460 bytes, which is a general maximum transmission unit (MTU) size. Moreover, the AEAD cipher is used twice (encryption/decryption) in this step. Then we can finally calculate the summation of processing time by multiplying each processing time by the number of transmissions or the usage count of the cryptographic algorithm. Table 3 shows the summary of processing time at each step of proposed D2D communication.

Table 3. The summary of processing time of proposed D2D communication.

Step	Transmission Latency	Processing Time of Cryptographic Algorithm			
		ECDSA-Sign	ECDSA-Verify	ECDH	AEAD
Step 0	$(2+10) * l_{tr}$	$(1+1) * t_{DS_{sign}}$	$1 * t_{DS_{ver}}$	-	-
Step 1	$(m+1) * l_{tr}$	-	-	-	-
Step 2	$(2+2+2) * l_{tr}$	-	$2 * t_{DS_{ver}}$	$1 * t_{DH}$	-
Step 3	$(n/1460) * l_{tr}$	-	-	-	$2 * t_{AEAD}$
Total ($\sum l$ or $\sum t$)	$(19+m+n/1460) * l_{tr}$	$2 * t_{DS_{sign}}$	$3 * t_{DS_{ver}}$	$1 * t_{DH}$	$2 * t_{AEAD}$

When we simulate Equation (1) using processing time in Table 3, we set each time parameter based on 5G network requirements and existing implementation results of the cryptographic algorithm. The 5G network requires a transmission latency of 1 ms [18]; accordingly, we set l_{tr} as 0.001. Moreover, we set the processing time of the ECC-based algorithm based on the performance presented in [19] ($t_{DS_{sign}} = 0.122, t_{DS_{ver}} = 0.458, t_{DS_{DH}} = 0.1672$). In the case of t_{AEAD} , we can calculate processing time by multiplying the throughput (Mbps) of the algorithm by the amount of data (n' (Mb) = n (MB) * $8/10^6$). For simulating various AEAD ciphers, we set the parameter following five AEAD ciphers (AES-GCM, ASCON, SpoC, Spook and GIFT-COFB) based on the performance results presented in [20]. Each case of t_{AEAD} is as follows (power measured: 50 MHz): $t_{AES-GCM} = n'$ (Mb)/31.2 (Mbps), $t_{ASCON} = n'$ (Mb)/39.0 (Mbps), $t_{SpoC} = n'$ (Mb)/28.8 (Mbps), $t_{Spook} = n'$ (Mb)/88.3 (Mbps), $t_{GIFT-COFB} = n'$ (Mb)/120.8 (Mbps). Figure 5 shows the simulation result of the proposed D2D communication. The AEAD ciphers used in the simulation consist of one general-purpose

AEAD cipher (AES-AEAD) and four lightweight AEAD ciphers. Simulation results show that three lightweight AEAD ciphers (ASCON, Spook and GIFT-COFB) are faster than AES-GCM (optimized). In particular, GIFT-COFB shows about 18.71% faster performance than AES-GCM when transmitting 10 KB data.

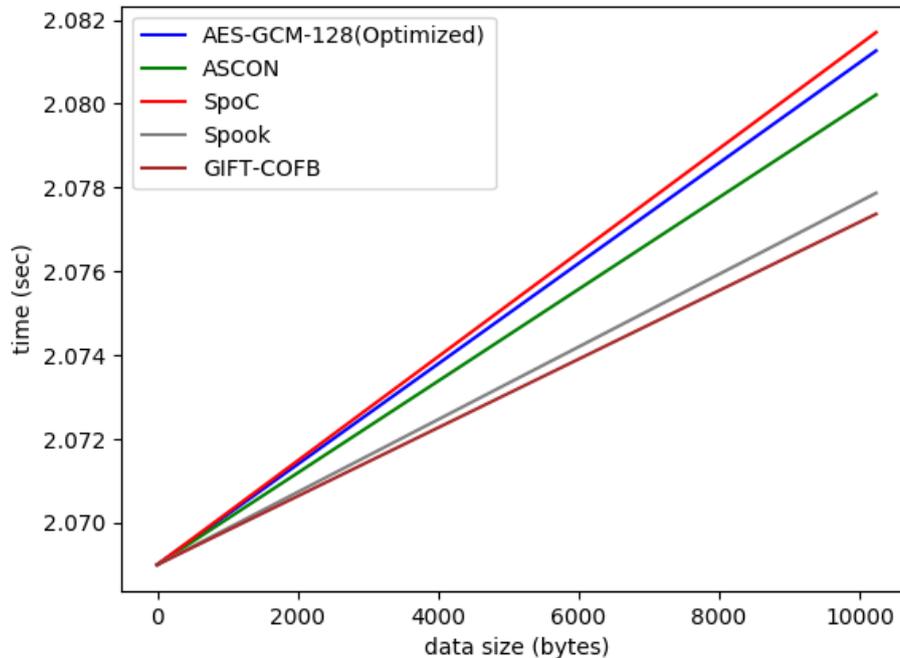


Figure 5. The processing time of the proposed D2D communication system.

However, because 5G IoT networks have limited resources, good performance of cryptographic algorithms may not cover all of the 5G IoT devices. This means the cryptographic algorithm has to be implemented lightly and must consume a small amount of power. Table 4 shows the hardware implementation results of AEAD block ciphers [19]. Even though Spook is faster than AES-GCM (optimized), Spook has the highest implementation cost, as in the mentioned area for implementing a look-up tables (LUTs).

Table 4. The hardware implementation result of AEAD ciphers.

AEAD Cipher	Area (LUTs)	Power (mW)	Throughput (Mbps)	Energy (nJ/bit)
AES-GCM (Optimized)	1532	35.9	31.2	1.15
ASCON	1808	33.6	39.0	0.86
SpoC	1344	34.7	28.8	1.20
Spook	7082	125.9	88.3	1.43
GIFT-COFB	2695	36.6	120.8	0.30

Figure 6 shows energy consumption by amount of data based on energy efficiency in Table 4. In terms of energy consumption, GIFT-COFB and ASCON consume less energy than AES-GCM (optimized), but SpoC and Spook consume more energy. Considering that both GIFT-COFB and ASCON show better performance than AES-GCM (optimized) in the performance simulation, when GIFT-COFB or ASCON is applied to the proposed D2D communication, both speed and energy efficiency of the proposed D2D communication are better than for AES-GCM (optimized)-based D2D communication.

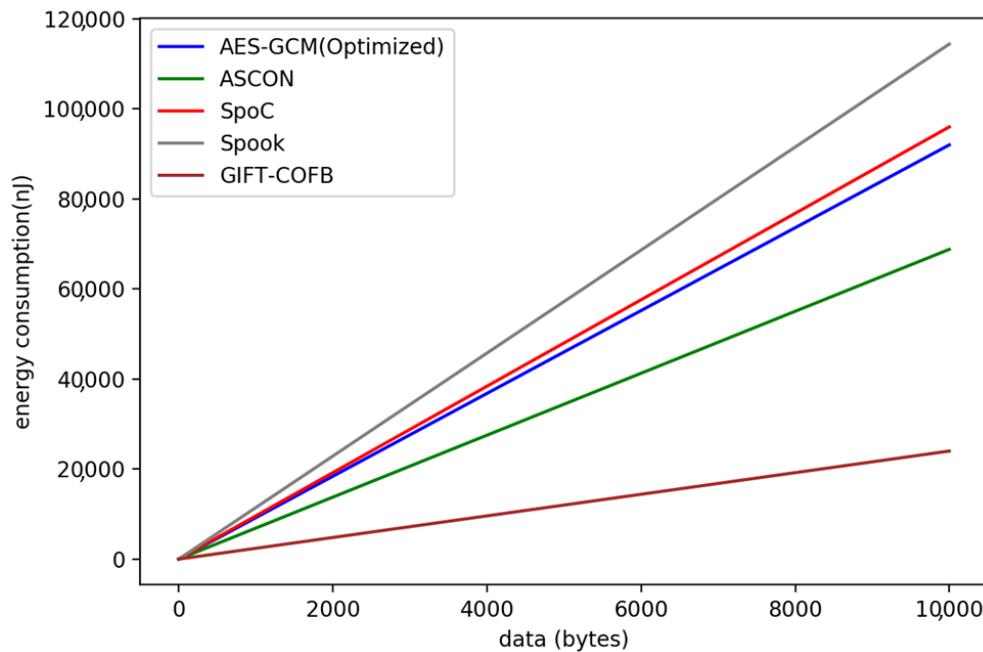


Figure 6. The energy consumption of AEAD ciphers.

5. Security Analysis

In this section, we perform security analysis of the proposed secure D2D communication system. As we mentioned before, secure D2D communication requires authentication, data confidentiality/integrity and anonymity. In addition, considering the resource-constrained nature of a 5G IoT network, it must be implemented lightly and must perform efficiently. We first discuss the proposed D2D communication system based on our security considerations. Moreover, we discuss security against typical threats of D2D communication.

5.1. Analysis Based on Security Considerations

- **Authentication:** The proposed D2D communication system performs primary authentication using 5G-AKA, which is an authentication framework provided by 5G, to perform authentication for a UE before issuing a D2D token. Moreover, the issued token can perform secondary authentication through verification of the process of creating a link of D2D communication through the gNB's public key and SUCI. Finally, in the data transmission step, the token is used as an AD to authenticate the other party for each transmission of data. In this way, authentication of the UE is performed in all processes of data communication before issuing a token for D2D communication so that more secure communication can be performed.
- **Data confidentiality and integrity:** The proposed D2D communication system generates D2D communication using SUCI, which is the encrypted UE identity, and the secret key of the gNB during the D2D generation process. In this process, there is no case where the identity of the unencrypted UE is transmitted. In addition, in the step of actual data transmission after creating a D2D link, encryption is performed using a lightweight AEAD cipher. AEAD cryptography can provide integrity and authentication as well as data confidentiality. Therefore, the proposed D2D communication system can guarantee the confidentiality/integrity of the identity and communication data of the UE.
- **Anonymity:** In 5G networks, SUCI is an encrypted identity for UE anonymity, which provides anonymity for the UE itself. Moreover, the D2D token used in the proposed D2D communication is a value obtained by signing SUCI with the private key of the gNB, which also provides anonymity by not being able to recognize the identity of the UE directly.

- **Efficiency:** Both the authentication process and the data encryption process used in the proposed D2D communication system are based on lightweight cryptography. The lightweight ciphers used in this paper are the ECC-based public key cryptosystem and the lightweight AEAD cipher. The ECC-based public key cryptosystem uses a 256-bit key and operates faster than RSA, which uses a 1024-bit key. Moreover, the lightweight AEAD cipher is designed to be efficiently implemented in a resource-constrained environment such as in IoT and provides data confidentiality/integrity and authentication.

5.2. Security against Typical Threats

- **Impersonation attack.** In D2D the token generation step, each UE is issued a D2D token, which is signed by the gNB. When gNBs generate the token, they authenticate the validity of the UE by comparing the identity of the UE in UDM. After this authentication process, gNBs complete the generation of D2D tokens by using their private key. Because of this procedure, the attacker cannot impersonate other UE.
- **Eavesdropping.** In a secure data transmission step, every instance of data transmission is protected by the lightweight AEAD cipher. In the AEAD encryption process, UE uses its D2D token and context sequence as associated data. Using this associated data, MAC is generated, and thereby UE can check the integrity of the message and the validity of the sender UE. For these reasons, the attacker cannot eavesdrop and cannot fabricate a message.
- **Privacy sniffing.** The proposed D2D communication system uses the D2D token, which is generated based on SUCI of UE and digital signature of gNB using ECDSA. The D2D token can provide anonymity as a cryptographic identity. For this reason, the attacker cannot recognize the original identity of the UE.
- **Free riding attack and location spoofing.** When the D2D token is generated by gNB, the validity of the UE is authenticated. This means that each instance of validating a UE is managed by gNB. The D2D token is authenticated in the link setup step in the proposed D2D communication system, and the data transmission is protected by AEAD encryption using a D2D token. Therefore, if a free-riding attack or location spoofing occurs in D2D communication, gNB can handle these situations by eliminating malicious UE.

6. Conclusions

In this paper, we propose a secure D2D communication system in a 5G IoT environment. The proposed D2D communication is designed based on an ECC-based public key cryptosystem and a lightweight AEAD cipher for efficiency in 5G use cases corresponding to IoT scenarios, mMTC and URLLC. Before the D2D communication is performed, the UE identity is verified based on the 5G-AKA provided by the 5G network, and then a token is used as the ECDSA for the D2D communication. The generated token could authenticate the legitimacy of the corresponding UE identity in the link setup process after device discovery. This can be done without connecting to the core network. In addition, by performing the encrypted communication through the lightweight AEAD cipher using the token as the associated data in the secure data communication step, the confidentiality/integrity of the data and authentication of the UE can be performed in each data transmission step. This approach can provide higher performance and energy efficiency than a general-purpose AEAD cipher-based communication system, and can also provide security against security threats such as impersonation, eavesdropping, privacy sniffing, free-riding and location spoofing.

Author Contributions: Conceptualization, B.S., J.H.P.; methodology, B.S. and J.C.S.S.; investigation, J.C.S.S., T.E. and C.X.; writing—original draft preparation, B.S.; project administration, J.H.P.; funding acquisition, J.H.P. and Y.P. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: This study was supported by the Advanced Research Project funded by the SeoulTech (Seoul National University of Science and Technology).

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

References

1. Tehrani, M.N.; Uysal, M.; Yanikomeroglu, H. Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions. *IEEE Commun. Mag.* **2014**, *52*, 86–92. [CrossRef]
2. Jeong, M.; Ahn, S. A network coding-aware routing mechanism for time-sensitive data delivery in multi-hop wireless networks. *J. Inf. Process. Syst.* **2017**, *13*, 1544–1553.
3. Doppler, K.; Rinne, M.P.; Janis, P.; Ribeiro, C.; Hugl, K. Device-to-device communications; functional prospects for LTE-advanced networks. In Proceedings of the 2009 IEEE International Conference on Communications Workshops, Dresden, Germany, 14–18 June 2009; pp. 1–6.
4. Chen, S.; Hu, J.; Shi, Y.; Peng, Y.; Fang, J.; Zhao, R.; Zhao, L. Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. *IEEE Commun. Stand. Mag.* **2017**, *1*, 70–76. [CrossRef]
5. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. *Comput. Netw.* **2019**, *162*, 106871. [CrossRef]
6. Lin, Z.; Du, L.; Gao, Z.; Huang, L.; Du, X. Efficient device-to-device discovery and access procedure for 5G cellular network. *Wirel. Commun. Mob. Comput.* **2016**, *16*, 1282–1289. [CrossRef]
7. Li, S.; Da Xu, L.; Zhao, S. 5G Internet of Things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [CrossRef]
8. Daoud, W.B.; Obaidat, M.S.; Meddeb-Makhlouf, A.; Zarai, F.; Hsiao, K.F. TACRM: Trust access control and resource management mechanism in fog computing. *Hum.-Centric Comput. Inf. Sci.* **2019**, *9*, 28. [CrossRef]
9. Stallings, W. *Cryptography and Network Security: Principles and Practice*; Pearson: Upper Saddle River, NJ, USA, 2017.
10. NIST Computer Security Resource Center. Lightweight Cryptography Project. Available online: <https://csrc.nist.gov/projects/lightweight-cryptography> (accessed on 8 December 2019).
11. Cao, M.; Wang, L.; Xu, H.; Chen, D.; Lou, C.; Zhang, N.; Zhu, Y.; Qin, Z. Sec-D2D: A Secure and Lightweight D2D Communication System With Multiple Sensors. *IEEE Access* **2019**, *7*, 33759–33770. [CrossRef]
12. Abro, A.; Deng, Z.; Memon, K.A. A Lightweight Elliptic-Elgamal-Based Authentication Scheme for Secure Device-to-Device Communication. *Future Internet* **2019**, *11*, 108. [CrossRef]
13. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. EEoP: A lightweight security scheme over PKI in D2D cellular networks. *J. Telecommun. Electron. Comput. Eng.* **2017**, *9*, 99–105.
14. Mohseni-Ejyeh, A.; Ashouri-Talouki, M.; Mahdavi, M. An Incentive-Aware Lightweight Secure Data Sharing Scheme for D2D Communication in 5G Cellular Networks. *ISeCure* **2018**, *10*, 15–27.
15. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. Secure D2D group authentication employing smartphone sensor behavior analysis. *Symmetry* **2019**, *11*, 969. [CrossRef]
16. Baskaran, S.B.M.; Raja, G. A Lightweight Incognito Key Exchange Mechanism for LTE-A Assisted D2D Communication. In Proceedings of the 2017 Ninth International Conference on Advanced Computing (ICoAC), Chennai, India, 14–16 December 2017; pp. 301–307.
17. Sun, Y.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. Privacy-Preserving Device Discovery and Authentication Scheme for D2D Communication in 3GPP 5G HetNet. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 425–431.
18. Carugi, M. Key features and requirements of 5G/IMT-2020 networks. In Proceedings of the ITU Arab Forum on Emerging Technologies, Algiers, Algeria, 14–15 February 2018.
19. Tschofenig, H.; Pegourie-Gonnard, M.; Unit, I.B. Performance of State-of-the-Art Cryptography on ARM-based Microprocessors. In Proceedings of the NIST Lightweight Cryptography Workshop 2015 Session VII: Implementations & Performance, Gaithersburg, MD, USA, 20–21 July 2015.
20. Rezvani, B.; Diehl, W. Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look. In Proceedings of the NIST Lightweight Cryptography Workshop 2019, Gaithersburg, MD, USA, 4–6 November 2019.

