An Efficient and Fault-Tolerant Privacy-Preserving D2D Group Communication

Hung-Yu Chien

Department of Information Management, National Chi Nan University, Taiwan
hychien@ncnu.edu.tw

Abstract

Device-to-Device (D2D) communications and the fostered services have been expected to play a key role in the next generation mobile communication networks (5G) and the Internet of Things (IoT) ecosystems. D2D Group Communications (D2DGCs) push forward the technology of two-device communications to that for group-of-device communications. However, they also expose new security threats and raise great privacy concern. Resource-and-battery constraints in the terminal devices further amplify the challenges of designing secure D2DGC. Existent Privacy-Preserving Authenticated Key Agreement (PPAKA) schemes for D2DGC are far from being practical in terms of their computational complexities and weak fault-tolerance. This paper, based on the Modified Computational Diffie-Hellman Problem (MCDHP) and the proposed Certificate-Less Aggregate Signature (CLAS) scheme, proposes a new Privacy-Preserving Authenticated Key Agreement (PPAKA) scheme which greatly improves the computational performance, the communication performance, and the fault tolerance. The improvements are amplified as the number of devices in a group increases. The analysis shows that that, even for the smallest group of two devices, a device in our scheme only demands 4% the computational complexity of Wang-Yan's PPAKA-Identity-Based Signature scheme, which is the state-of-the-art scheme for privacy-preserving D2DGC.

Keywords: 5G, Authenticated key agreement, Device-to-device communication, Fog services, Privacy preserving

1 Introduction

In both the next generation mobile communication networks (5G) and the IoT ecosystems, D2DC are key technologies and are expected to foster new services and boost the economics [1]. D2DGC pushes forward the technology of two-device communications to that for group-of-device communications. D2DGC facilitates the great potential for developing group-based services and fog services [1]. However, both D2DC and D2DGC invite new security threats and privacy-disclosure concerns. The threats affect not only the system security but also the physical safety of users.

It is expected that, in the coming future, there will be a large amount of devices participating in various D2D communications. Among them, many are resource-constrained and they are expected to operate in a low-power state so that they can prolong their batteries and their deployment lifetime. Narrowband Internet of Things (NB-IoT) is one of such technologies that focuses specifically on low cost, long battery life, and high connection density. NB-IoT technology can securely access the fifth generation core network [4] through the 3GPP access network.

For securing D2DC and D2DGC, Authenticated Key Agreement (AKA) is prerequisite. There exist many AKA schemes for the D2DC scenarios and some for the D2DGC scenarios [10-17]. But, only until recently, Wang and Yan [17] proposed the first PPAKA schemes for the D2DGC. They proposed two PPAKA schemes. One is the PPAKA-HMAC and the other is the PPAKA-IBS, where IBS stands for Identity-Based Signature. But, the two schemes are far from being efficient and practical in terms of computational efficiency and fault tolerance.

This paper aims at designing efficient and practical PPAKA scheme for D2DGC scenarios. Based on the MCDHP [20] and the proposed CLAS scheme, we propose a new PPAKA scheme called PPAKA-CLAS. The contributions of this paper are listed here. (1) It greatly improves the computational complexities, even if the size of the group is small; the improvement is greatly amplified as the size of the group increases. (2) Both the communication performance and the fault tolerance are improved. (3) The overall improvement makes the scheme much more efficient and practical. The rest of this paper is organized as follows. Section II discusses the related work. Section III presents the system model, the security model, and the design objectives. Section IV proposes our CLAS scheme and our PPAKA-CLAS for the D2DGC scenarios. Section V analyzes the security. Section VI evaluates the performance. Section VII states our conclusions.

*Corresponding Author: Hung-Yu Chien; E-mail: hychien@ncnu.edu.tw
DOI: 10.53106/160792642021122207006

2 Related Work

It has been estimated that there will be billions of IoT devices accessing the networks in the immediate future [1]. For those systems that consist of the geographical-widely deployed IoT devices, no matter whether static devices or mobile devices, it is cost effective to choose public mobile systems as their backbone to leverage the advantages of the ubiquitous coverage, high reliability, and very competitive cost. In such scenarios, a User Equipment (UE) is registered in its Home Network (HN), and might visit and access several Service Networks (SN).

When these UEs are authenticated using the conventional AKA schemes like UMTS-AKA and LTE-AKA [3], they are expected to experience long signaling latency because authenticating a mobile UE still need the account data from its HN [6]. Aggregating all the authenticating requests from tons of UEs would generate tremendous communication overhead [6]. Therefore, there are many efforts like [6-8, 31-33] aiming at improving the performance of authenticating these UEs. In addition to authenticating UEs and granting access to mobile network systems, AKA schemes for D2DC have been intensively investigated recently [10-15].

In [16], two anonymous group D2D communication protocols have been proposed, but they only addressed the group anonymity for the two-device case. For D2DGC, Wang and Yan [17] recently proposed two PPAKA schemes, PPAKA-HMAC and PPAKA-IBS. PPAKA-HMAC can only protect the security from outside attackers, and PPAKA-IBS that applies IBS can protect security and privacy from both inside attackers and outside attackers. As many UEs are resource-limited and often deployed in hostile environments, they are prone to various attacks; therefore, it is inevitable to design secure schemes that can resist both inside attackers and outside attackers. Unfortunately, Wang-Yan's PPAKA-IBS scheme demands lots of computation-costly pairing computations, and it would reject all the device requests even if only one device fail to commit the authenticity in the initial phase of the process. The weak fault tolerance would make the scheme being vulnerable to Denial-of-Service (DOS) attacks.

Most of existent AKA schemes are based on the Computational Diffie-Hellman Problems (CDHP) [18] and its variants [18-19, 32]. Chien noticed that a naïve Diffie-Hellman (D-H) Key agreement scheme would require each party at least two modular exponentiations, which is acceptable for computers but it is computation-stressing for those resource-constrained devices. Therefore, Chien [20] formulated a new Non-Polynomial (NP) hard problem called the MCDHP and proved its security being equivalent to the CDHP. Based on the MCDHP, Chien proposed a generic approach of converting conventional 2-party AKA schemes into more efficient 2-party AKA schemes [20], and a MCDHP-based 3-party AKA scheme [21]. In this paper, we will apply the MCDHP to securely deliver ephemeral D-H keying materials. For authentication in the multi-server environments, [32] proposed a biometrics-based solution, and [33] surveyed several papers and analyzed the various desirable features.

Al-Ryiami and Paterson [26] first proposed the CertificateLess Public Key Cryptography (CLPKC) to overcome the key escrow problem inherited in the identity-based cryptography and to eliminate the certificate maintenance cost embedded in the conventional Public Key Infrastructure (PKI). Since then, there are many certificate-less cryptographic protocols being designed. Based on Wang-Qi's CertificateLess Aggregate SignCryption (CLASC) [22], [23] recently proposed a fast authentication and data transfer for massive NB-IoT scenarios. [24] proposed a CLAS, but [25] show the scheme being vulnerable to forgery attacks when the attackers can access the partial secret key. In this paper, we will convert Wang-Qi's CLASC into a new CLAS scheme, and apply it in our PPAKA-CLAS scheme. Table 1 sorts out the functions and features of the cryptographic systems discussed in this paper.

Table 1. Functions and features of cryptographic systems

Scheme	Functions and features
Public-Key Cryptography (PKC) Public Key Infrastructure (PKI)	PKC is a cryptographic system that uses pairs of (public key, private key) to facilitate asymmetric cryptographic algorithms like digital signature, public key encryption, and so on. Conventional PKC needs the support of Public Key Infrastructure (PKI), in which one or more trusted third parties (called Certificate Authorities- CAs) certify a user's certificate which explicitly specifies the public key and the identity of the user.
Identity-Based Cryptography (IBC)	IBC is a special type of public-key cryptography in which a publicly known string (like email address, IP address, etc) representing an individual or organization is used as a public key. In conventional PKI systems, an entity needs to verify a certificate before it uses the public key. On the contrary. IBC relieves an entity's burden of verifying a certificate. However, the trusted third party, called the private key generator (PKG), knows the private key of the user. It is called the key-escrow problem.

Table 1. Functions and features of cryptographic systems (continue)

Scheme	Functions and features
CertificateLess Public Key Cryptography (CL-PKC)	CL-PKC also uses an entity's publicly known string as its public key. But the trusted third party (called Private Key Generator- PKG) co-operates with each registered entity to generate the private key in such a way that PKG cannot unilaterally determine the private key. CL-PKC has neither the certificate management problem nor the key-escrow problem.
Aggregate Signature (AS)	Aggregate signature allows an entity to aggregate several instances of digital signatures into one short signature, and simplifies the verification of multiple signatures into one verification.
SignCryption (SC)	Signcryption fulfills the task of signature generation and encryption in one step. Compared to separating signature generation and encryption in two steps, signcryption usually demands less computation cost.
CertificateLess Signature (CLS), CertificateLess SignCryption (CLSC)	CertificateLess signature/Signcryption is a signature/signcryption scheme that is based on CL-PKC. Compared to a signcryption scheme, a signature scheme provide only signature generation but not encryption.
CertificateLess Aggregate Signature (CLAS)	CLAS is an aggregate signature scheme that is based on a CL-PKC.
CertificateLess Aggregate SignCryption (CLASC)	CLASC is an aggregate signaryption scheme that is based on a CL-PKC.

3 System Model, Security Model, and Objectives

3.1 System Model

We follow Wang-Yan's system model. There are two kinds of entities: SN and D2D UE. For those UEs within the wireless network coverage of a SN, they can establish secure connections with the SN via existing infrastructure and AKA schemes like [3, 6-8]. A UE can discover other nearby UEs and then establish group communications via the help of the SN. The SN generates and manages pseudonyms for those authenticated UEs. It manages the key pairs for these UEs and helps UEs to establish D2DGC. Figure 1 shows the system model of D2D group communications.

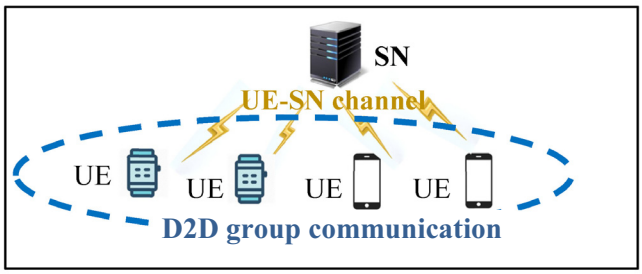


Figure 1. The system model of our D2 DGC

3.2 Security Model

The channel between an authenticated UE and the SN is assumed to be secure like Wang-and-Yan work [17], as they could be established by applying secure AKA schemes like [3, 6-8]. The wireless channel among UEs is insecure. A SN is secure and trusted. A UE is a resource-constrained device and it might be compromised. An attacker could launch passive attacks and even active attacks (like replay, modification, impersonation, etc.) on the channels among UEs to violate the security or the identity privacy.

3.3 Design Objectives

The main goal of our scheme is to establish authenticated group keys among UEs and protect the identities of the UEs. The goals are discussed as follows.

Authentication. Each UE should be securely authenticated.

Identity privacy. During the process of the D2DGC, the identity of a UE should be protected, and an attacker cannot learn or infer the information of the identities.

Group session key privacy. Only those legitimate UEs in the process can access the group session key, and even the SN cannot derive the key.

Group backward secrecy. For supporting dynamic group management, backward secrecy should be ensured so that new joining devices cannot learn the previous group session keys.

Group forward secrecy. Forward secrecy should be ensured so that any leaving devices cannot learn the new group session keys after their leaving.

Computational efficiency. Since many UEs are resource-constrained, it is desirable that the protocols should be computationally efficient.

Fault tolerance. As the wireless channels and the UEs are prone to many attacks, the protocol should support good fault tolerance that un-authenticated UEs cannot deter legitimate UEs from establish the group session keys.

4 The Proposed PPAKA for D2DGC

To achieve our goals, we have the following design principles. (1) Re-inventing the building blocks to

make them much more efficient. (2) Reducing the number of interactions and replacing the costly UE-SN unicast interactions in Wang-Yan's design with UE's broadcasting in our design, when it is feasible. (3) Letting SN verify UEs' commitment of ephemeral public keys as soon as possible so that, when UEs enter the session establishment phase, they can continue their session establishment and group key computation; this arrangement can enhance fault tolerance.

Before presenting our schemes, we first introduce two new building blocks respectively as follows. Table 2 lists the notations used in the rest of this paper.

Table 2. The notations

$E(F_p)$	Elliptic Curve over a Galois field F_p.
G, P, q	G: an ECC group of order q. P is the generator for G.
H_1, H_2, h	hashing functions.
SN, UE, KGC	SN: Service Network; UE: User Equipment; KGC: Key Generating Center.
P_{pub}, s	KGC owns the public key $P_{pub}=sP$ and the private key s.
UE_i, PID_i	UE_i: *ith User Equipment;* PID_i: UE_i's pseudonym.
m_i, δ_i, δ	m_i: *plaintext*; δ_i: *individual signature*; δ: *an Aggregate signature*
(x_i, y_i) (X_i, Y_i)	(X_i, Y_i): the public key for UE_i. (x_i, y_i): *private key*
K_i^L, K_i^R, $\overline{K}_i$	Keying materials.
SID, R_{SID}	SID: group session identity; $R_{SID} = (PID_1, \ldots, PID_{n'})$.
$Sign_{SN}(\ )$	$Sign_{SN}(\ )$: SN's signature.
SK_i^{SIKD}	Group session key derived by UE_i

4.1 Review of the MCDHP

The security of our PPAKA-CLAS is based on three hard problems- the Discrete Logarithm Problem (DLP), the CDHP and the MCDHP. The MCDHP can reduce the computational complexities of UEs in the session request phase of our scheme. We review the new MCDHP as follows. The conventional DLP problem and CDHP problem are referred to [18].

Definition 1. The M*odified Computational Diffie-Hellman Problem* (the MCDHP) for an Elliptic Curve Cryptography (ECC) [27]: given an elliptic curve over a finite field F_p, a point $P \in E(F_p)$ of order q, a+x, and points $A = xP$, $B = bP \in < P >$ where $a, b, x \in_R Z_q^*$, find the point $C = abP$.

The following theorem from [20] reduces the hardness of the MCDHP to that of the CDHP.

Theorem 1. The MCDHP problem is as hard as the CDHP problem [20].

Proof. We prove this by reduction. The MCDHP problem is reduced to the CDHP. Given an instance of the MCDHP problem- (x+a, P, xP and bP), then we can compute $(x+a)P - xP = aP$ and get the instance (P, aP and bP) for the CDHP problem. Assume there is one oracle that can answer the CDHP problem. Now we input the instance (P, aP and bP) to the oracle, and we get the answer abP.

The CDHP problem is reduced to the MCDHP problem.

Assume there is one oracle that can answer the MCDHP problem: given (x+a, P, xP and bP), it outputs abP.

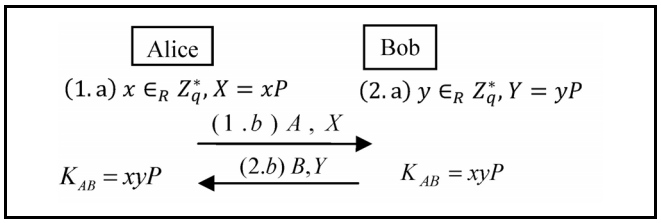
Now given an instance of the CDHP problem- (P, aP and bP), we then choose a random value t, and input the instance (t, P, aP and bP) to the MCDHP oracle. The oracle will answer $b(tP - aP) = b(t-a)P = tbP - abP$. Using the response, we can derive $-(tbP - abP - t(bP)) = -(-abP) = abP$. That is, we get the answer for the CDHP problem- (P, aP and bP).

Based on the above arguments, we prove the theorem. ■

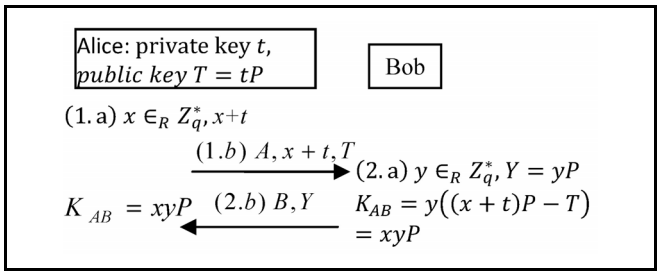
Figure 2. shows how we apply the MCDHP to improve the computational performance in the D-H key agreement. Figure 2(a) shows a naïve D-H key agreement, where Alice and Bob respectively exchange their ephemeral public keys and establish the D-H key $K_{AB} = xyP$. In this scenario, Alice would require two modular exponentiations. Figure 2(b) shows a MCDHP-based D-H key agreement; Instead of sending $X = xP$, Alice sends $x + t \bmod q$ to Bob, and then Bob uses Alice's public key $T = tP$ to derive $K_{AB} = y(x+t)P - T) = xyP$. This arrangement can save Alice one modular exponentiation. This arrangement is attractive to those scenarios where the client Alice is a resource-constrained device. We will apply this technique in our PPAKA-CLAS scheme.

4.2 The New CLAS Scheme

Here, we propose our new CLAS scheme, and will adopt the CLAS as one of the building blocks of our PPAKA-CLAS scheme for the following merits. (1) CLAS does not have the key escrow issue and does not have the costly certificate maintenance overhead. (2) It



(a) The D-H key agreement



(b) The enhanced D-H key agreement

Figure 2.

facilitates a SN in our system dynamically binds UEs' time-bound pseudonyms to the pubic keys, and distributes the corresponding partial private keys to those registered UEs.

Inspired by Wang-Qi's CLASC, we convert it into our CLAS scheme, as our PPAKA-CLAS scheme does not require the encryption of the keying materials in the Group Session Request of our PPAKA-CLAS. Our CLAS scheme consists of seven parts- System Initialization, User Key Selection, Private Key Extraction, Signature Generation, Signature Aggregation, Individual Signature Verification, and Aggregate Signature Verification.

System Initialization (denoted as CLAS-SI(k)): Key Generator Center (KGC) selects a safety parameter k, and then defines a cyclic group G with prime q ($q > 2^k$), P is the generator of group G. Then it chooses three cryptographic secure hash functions. $H_1 : \{0,1\}^{L_1} \times G \times G \to Z_q^*$; $H_2 : \{0,1\}^{L_1} \times \{0,1\}^{L_2} \times G \to Z_q^*$; $h : G \to Z_q^*$; L_1 is the bit length of the user identity and L_2 is the bit length of the plain text. Finally, KGC chooses a random number s as the master key and computes the public key P_{pub}=sP. It then publishes Params:=< q, P, G, P_{pub}, H_1, H_2, h> as system parameters and keeps the master key s secret.

User Key Selection (denoted as CLAS-UKS()): UE_i selects $x_i \in_R Z_q^*$, and computes the public parameter $X_i = x_i P$.

Private Key Extraction (denoted as CLAS-PKE(PID_i, X_i)): Here, we bind the keys to a device's dynamic pseudonym to protect the privacy. Upon the receipt of $\{ID_i, X_i\}$ from UE_i, the KGC chooses PID_i, randomly chooses $r_i \in Z_q^*$, and computes $Y_i = r_i P$, $h_{i1} = H_1(PID_i, X_i, Y_i)$, $y_i = r + s \cdot h_{i1} \bmod q$. The private key and the public key for UE_i are (x_i, y_i) and (X_i, Y_i), respectively. The private key is securely distributed from KGC to UE_i. The private key (x_i, y_i) satisfies the following equation.

$PID_i \overset{def}{=} \{pseudonym, Expire\}$, where $Expire$ specifies the valid period.

$$\begin{aligned}(x_i, y_i)P &= (x_i + r_i + s \cdot h_{i1})P \\ &= X_i + Y_i + sH_1(PID_i, X_i, Y_i)P \\ &= X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}\end{aligned} \quad \textbf{(1)}$$

Signature Generation (denoted as CLAS-SG (m_i, x_i, y_i)): UE_i signs the message m_i as follows:

Randomly choose $\alpha_i \in Z_q^*$, and then compute $V_i = \alpha_i P$.

Compute $h_{i2} = H_2(PID_i \| m_i, V_i)$.

Compute S_i in (2), and $\delta_i = (V_i, S_i)$ is the signature for m_i.

$$S_i = \alpha_i + (x_i + y_i)H_2(PID_i \| m_i, V_i) \bmod q \quad \textbf{(2)}$$

Signature Aggregation (denoted as CLAS-SA $(\{m_i, \delta_i\}_{i=1\sim n} = \delta)$: Upon receiving several signatures $\{m_i, \delta_i\}_{i=1\sim n} = \{(m_i, V_i, S_i)\}_{i=1\sim n}$, compute $S = \Sigma_{i=1\sim n} S_i$. The messages and the aggregated signature is δ =< $(m_i, V_i)_{i=1\sim n}, S$ >.

Individual Signature Verification (denoted as CLS-ISV (m_i, δ_i)): Each individual signature can be validated by checking whether the following equation holds.

Compute $h_{i1} = H_1(PID_i, X_i, Y_i)$, $h_{i2} = H_2(PID_i \| m_i, V_i)$.

$$\text{Verify } S_i P ? = V_i + h_{i2}(X_i + Y_i + h_{i1} P_{pub}). \quad \textbf{(3)}$$

Aggregate Signature Verification (denoted as CLS-ASV (δ =< $(m_i, V_i)_{i=1\sim n}, S$ >)) : An aggregated signature can be validated by checking whether the following equation holds.

For $i = 1 \sim n$, *compute* $h_{i1} = H_1(PID_i, X_i, Y_i)$, $h_{i2} = H_2(PID_i \| m_i, V_i)$.

$$\text{Verify } S_i P ? = \Sigma_{i=1\sim n}(V_i + h_{i2}(X_i + Y_i + h_{i1} P_{pub})). \quad \textbf{(4)}$$

4.3 The Proposed PPAKA-CLAS for D2DGC

In this section, we propose our Privacy-Preserving Authenticated Key Agreement using CertificateLess Aggregate Signature, called PPAKA-CLAS, for the D2D group communications. The PPAKA-CLAS consists of seven parts: System Setup, Device Registration, D2D Discovery, Group Session Request, Session Establishment, Group Session Activation, and

Key Update.

System Setup: A SN acts as a KGC, and performs the system setup as the system initialization described in Section IV.B. It publishes the public parameters < q, P, G, P_{pub}, H_1, H_2, h>, and keeps the secret key s privately.

Device Registration: An UE_i with its real identity ID_i chooses its random number x_i, computes $X_i = x_i P$, and performs the Private Key Extract function described in Section IV.B to derive the private key (x_i, y_i) and the public key (X_i, Y_i). Additionally, the SN chooses a pseudonym PID_i for UE_i. The SN binds PID_i to the private key generation. It maintains the mapping of the real identities, the pseudonyms, and the public keys. This phase is executed in a secure channel.

D2D Discovery: Assume there are $\{UE_i\}_{i=1\sim n}$ with pseudonyms $\{PID_i\}_{i=1\sim n}$ establish group session keys and perform the D2D discovery phase. For the details of the D2D discovery process, interested readers are referred to [28].

Group Session Request: To request for a secure group D2D communication, each UE_i belongs to $\{UE_i\}_{i=1\sim n}$ randomly chooses $a_i, b_i \in Z_q^*$, and computes $m_i = b_i + x_i \bmod q$ and $V_i = \alpha_i P$. It applies our CLAS to generate its signature for m_i as $\delta_i = (V_i, X_i)$.

UE_i prepares its group session request M_i^{req} as follows. It sends M_i^{req} to the SN, where the pseudonyms listed in the request M_i^{req} do not define the ordering.

$$M_i^{req} := \{PID_i, PID_1, ..., PID_{i-1}, PID_{i+1}, ..., PID_n\}, m_i, \delta_i\}.$$

Upon receiving the requests from $\{UE_i\}_{i=1\sim n}$, the SN first validates each PID_i and then verifies the signature δ_i for m_i. If a signature is verified, then the SN computes M_i as follows.

$$M_i = m_i \cdot P - X_i = (b_i + x_i)P - x_i P = b_i P. \quad \textbf{(5)}$$

For those verified *UEs*, the SN chooses a group session identity *SID*, and forms a ring structure $R_{SID} = (PID_1, ..., PID_{n'})$, where $n' \le n$ and $PID_i \in R_{SID}$ if and only if $UE_i's$ signature satisfies the SN's verification. The listing in R_{SID} specifies the ordering; that is, PID_{i-1} and PID_{i+1} are respectively the left and right neighbors of PID_i for $1 \le i \le n'$, $PID_0 = PID_{n'}$, and $PID_1 = PID_{n'+1}$.

Then the SN prepares its response $M^{res} := (R_{SID}, \{M_i\}_{i=1\sim n'})$, and generates its signature $Sign_{SN}(M^{res})$. It broadcasts $(M^{res}, Sign_{SN}(M^{res}))$ to all the nearby UE_s.

Here, we note the differences between Wang-Yan's group session request phase and ours. (1) The SN in Wang-Yan's group session request phase would reject all the requests if any UE discovered in the D2D discovery phase fails to send its request or does not pass the verification, but our SN checks the requests and lets those verified UEs continue the rest of the process. (2) UEs in Wang-Yan's scheme only send their intentions in this phase, but our UEs send their intentions and their keying materials for the SN to verify. (3) The keying material in this phase is in the form of $m_i = b_i + x_i \bmod q$. These designs will have three improvements. First, our scheme reduces 1 message round. Second, our scheme achieves stronger fault-tolerance as it lets those verified UEs continue the rest of the process. Third, our application of the MCDHP lets each UE reduce one scalar multiplication in ECC. In a summary, it improves the fault tolerance, the communication overhead, and the computational performance.

Session Establishment: Contrary to the two-round process in the session establishment phase of Wang-Yan's PPKA schemes, our session establishment phase only needs one round. Upon receiving $(M^{res}, Sign_{SN}(M^{res}))$ from the SN, each UE_i belonging to R_{SID} performs the following tasks.

Compute a left key K_i^L, a right key K_i^R, and a $\overline{K_i}$ as follows.

$$K_i^L = b_i M_{i-1} = (b_{i-1} b_i)P, \quad K_i^R = b_i M_{i+1} = (b_i b_{i+1})P,$$
$$\overline{K_i} = K_i^R K_i^L = (b_i b_{i+1} - b_{i-1} b_i)P \quad \textbf{(6)}$$

Prepare $M_i' = SID \,||\, PID_i \,||\, \overline{K_i}$, and computes its CLAS-SG for M_i' as $\delta_i' = (V_i', S_i')$. Broadcast (M_i', δ_i') to all nearby *UEs*.

Group Key Generation: Upon receiving all messages $\tilde{M}_i := \{M_j', \delta_j'\}_{PID_j \in RID,\ PID_j \ne PID_i}$, UE_i performs the following tasks.

Aggregate the signatures $\delta_j's$ in $\tilde{M}_i$, and perform the CLAS-ASV on the aggregated signature.

After verifying the aggregated signature, UE_i calculates

$$\begin{aligned}
\widehat{K_{l+1}^R} &= \overline{K}_{i+1} + K_i^R \\
&= (b_{i+1} b_{i+2} - b_i b_{i+1})P + (b_i b_{i+1})P \\
&= (b_{i+1} b_{i+2})P \\
\widehat{K_{l+2}^R} &= \overline{K}_{i+2} + \widehat{K_{l+1}^R} \\
&= (b_{i+2} b_{i+3} - b_{i+1} b_{i+2})P + (b_{i+1} b_{i+2})P \\
&= (b_{i+2} b_{i+3})P \\
&\cdots
\end{aligned}$$

$$\begin{aligned}\widehat{K^R_{l+(n'-1)}} &= \widehat{K_{i+(n'-1)}} + \widehat{K^R_{l+(n'-2)}} \\ &= (b_{i+(n'-1)}b_{i+n'} - b_{i+(n'-2)}b_{i+(n'-1)}P \\ &\quad + (b_{i+(n'-2)}b_{i+(n'-1)}P \\ &= (b_{i+(n'-1)}b_{i+n'})P = (b_{i-1}b_i)P\end{aligned} \quad (7)$$

Verify whether $\widehat{K^R_{1+(n'-1)}}$ equals its own $K^L_i = (b_{i-1}b_i)P$.

If all the verifications succeed, then it computes the session key SK_i^{SID} as follows.

$$\begin{aligned}SK_i^{SID} &= \widehat{K^R_1} + \widehat{K^R_2} + \cdots + \widehat{K^R_{n'}} \\ &= (b_1b_2)P + (b_2b_3)P + \cdots + (b_n, b_1)P\end{aligned} \quad (8)$$

Group Session Activation: Each $UE_i \in R_{SID}$ can sign a signature on its hashed session key $h(h(SK_i^{SID}))$ and broadcasts the signature to notify other members and the SN its knowledge of the session key. The SN monitors and maintains the membership of the group.

When Wang-Yan's scheme needs the SN to verify all the confirmation messages and to notify the UEs, our scheme facilitates UEs notify other members directly. This arrangement reduces one message round and reduces the burden of the SN.

Key Update: There are several scenarios that cause the membership change or continue a will-expire session. For all such cases, the SN maintains the membership of a group, and securely deliver a random number r' to still-stay old members and new joining members (if any). If there are any new joining members, then the SN also *securely* delivers the hashed old session key $h(SK_i^{SID})$ to the new members. After that, any legitimate UE_i computes the new-$SK_i^{SID} := h(r', h(SK_i^{SID}))$ and signs $h(h($(new-SK_i^{SID})) to activate the new session key.

5 Security Analysis

We respectively analyze the security of our proposed CLAS scheme and that of the proposed PPAKA-CLAS.

5.1 The Security of the Proposed CLAS Scheme

We first prove that the proposed CLAS scheme is unforgeable for a single signature. Since the security of many digital signature schemes have been well studied, we will prove the security of our CLAS scheme by reducing it to that of Elgamal signature with certificateless public key in the ECC setting, to save the lengthy and tedious paragraphs.

Theorem 2. The private key (x_i, y_i) and the public key (X_i, Y_i) that satisfies $(x_i, y_i)P = X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}$ is secure as long as the DLP in ECC is hard.

Proof: The form of $(x_i + y_i)P = X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}$ is equivalent to the discrete logarithm problem in the ECC setting. To derive (x_i, y_i) that satisfies $(x_i + y_i)P = X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}$ should break the DLP problem unless he owns the private key s or he can compromise P_{pub}. As long as the DLP in ECC is hard, the private key setting is secure.

Theorem 3. The individual signature generation and verification of our CLAS scheme is equivalent to Harn's Elgamal signature [29] with the public key $X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}$.

Proof: We first denote $Pub_{PID_i} := X_i + Y_i + H_1(PID_i, X_i, Y_i)P_{pub}$ be the public key of PID_i. Then, the signature generation in (2) and the verification equation in (3) can be re-written respectively as follows.

$$\begin{aligned}V_i = \alpha_i P,\ S_i &= \alpha_i + (x_i + y_i)h_{i2} \\ &= \alpha_i + (x_i + y_i)H_2(PID_i \mid m_i, V_i) \bmod q\end{aligned} \quad (9)$$

$$\begin{aligned}S_iP ? &= v_i + h_{i2}(X_i + Y_i + h_{i1}P_{pub}) \\ &= V_i + H_2(PID_i \mid m_i, V_i)Pub_{PID_i}\end{aligned} \quad (10)$$

In 1994, Harn [29] has proposed a secure variant of Elgamal-like signature. The scheme has the signature generation and verification equations as follows.

$$V = g^k \bmod p, s = k + x_A h(m, V) \bmod q, \quad (11)$$

where x_A is the private key.

$$g^s ? = Y_A^{h(m,V)} \cdot V \bmod p, \quad (12)$$

where Y_A is the public key.

From (9-12), we can see that our scheme is equivalent to Harn's Elgamal-like signature in ECC setting.

Theorem 4. Our CLAS signature and verification is unforgeable as long as the DLP in ECC is secure.

Proof: Harn has proved the security of their scheme in [29]. Hoster et al. [page 9, 30] studied a series of Elgamal-like signatures and proved that Harn's version is secure, as long as the DLP is hard. Following the result of Theorem 3, our CLAS individual signature and verification is secure.

Theorem 5. The aggregate signature and verification of our CLAS is secure (unforgeable).

Proof: We prove this by contradiction.

We first examine the case of $n' = 2$ (say two signers PID_1 and PID_2). We assume that attackers $\mathcal{A}$ and $\mathcal{A}'$ can forge aggregate signatures for the case $n' = 2$, and $\mathcal{A}'$ can further get the co-operation of PID_1.

In the first step, $\mathcal{A}'$ outputs a valid aggregate signature $\delta = <(m_1, V_1), (m_2, V_2), S>$ that satisfies

$SP? = \Sigma_{i=1\sim2}(V_i + h_{i2}(X_i + Y_i + h_{i1}P_{pub}))$.

Next, $\mathcal{A}'$ asks for $PID_1's$ support to output a valid signature (m_2, V_1, S_1). With that, $\mathcal{A}'$ lets $S_2 = S - S_1 \bmod q$, and then (m_2, V_2, S_2) is a valid signature for PID_2. That is, with the support of PID_1, $\mathcal{A}'$ can forge signatures for another un-compromised user PID_2. This contradicts the result of Theorem 4. So $\mathcal{A}'$ cannot forge any aggregate signature for PID_1 and PID_2. Since $\mathcal{A}$ is not more powerful than $\mathcal{A}'$, we conclude that $\mathcal{A}$ cannot forge any aggregate signature for the case $n' = 2$.

It is easy to extend the above result for the cases $n' > 2$. So we have our theorem.

5.2 The Security of the Proposed PPAKA-CLAS Scheme

Before analyzing the security properties, we first prove the correctness of the group key generation.

Theorem 6. After the successful execution of our PPAKA-CLAS, the legitimate *UE*s can securely share a common session key $SK_i^{SID} = (b_1b_2)P + (b_2b_3)P + \cdots + (b_n, b_1)P$.

Proof: The correctness of the group key generation follows two facts: (1) the authenticity of several key materials respectively signed UEs and the SN; (2) the correctness of the equations. We examine them one by one as follows.

In the Group Session Request phase, each $UE_i's$ $m_i = b_i + x_i \bmod q$ is signed by UE_i. Based on the verified m_i, the SN derives and signs on $M_i = b_iP$.

In the Session Establishment phase, UE_i, based on its private value b_i (in (5) and the broadcast and signed $\{M_j s\}$, computes and signs $\overline{K_i} = (b_ib_{i+1} - b_{i-1}b_i)P$ (in (6)).

In the Group Key Generation phase, UE_i, based on the broadcast and signed $\{\overline{K}_j s\}$, follows (7) to calculate and verify $\widehat{K_{1+(n'-1)}^R}$, and then follows (8) to derive $SK_i^{SID} = (b_1b_2)P + (b_2b_3)P + \cdots + (b_n, b_1)P$.

Finally, in the Group Session Key Activation phase, each $UE_i \in R_{SID}$ signs $h(h(SK_i^{SID}))$ and broadcasts the signature.

In all the phases, each key material is signed and verified; therefore, the keying materials are securely signed as long as the CLAS signature scheme is unforgeable. The security of $K_i^L = M_{i-1}^{b_i} = (b_{i-1}b_i)P$ and $K_i^R = M_{i+1}^{b_i} = (b_ib_{i+1})P$ is based on the CDHP hardness. Based on all the above facts, we can conclude that our group key SK_i^{SID} is securely and privately shared among those legitimate $UE_i s$.

Theorem 7. Our PPAKA-CLAS scheme can protect the device identity privacy.

Proof: In our scheme, each key material is signed using our CLAS, where the public keys are linked to $UE_i's$ pseudonyms $PID_i s$ and each PID_i has the specified valid period. This protects the privacy of UEs.

Theorem 8. The proposed PPAKA-CLAS scheme satisfies group forward/backward secrecy.

Proof: If there are any membership changes, then the new key will be updated as new- $SK_i^{SID} := h(r', h(SK_i^{SID}))$. In our scheme, only still-stay members and will-be members can securely receive the r' from the SN, and the SN only deliver the hashed old key $h(SK_i^{SID})$ to the will-be members. These protocols ensure that only legitimate group members can compute the new keys. Any new UEs cannot derive old keys from $h(SK_i^{SID})$. Any leaving UEs cannot get r' from the SN and cannot compute $SK_i^{SID} := h(r', h(SK_i^{SID}))$.

Table 3 sorts out the rationales that facilitate the security goals of the proposed scheme.

Table 3. The rationales facilitating the security goals

Security property	Rationales
Authentication	In the group session request phase, the session establishment phase, the group session activation phase, and the key update phase, each entity applies digital signature on the sending messages; all the signatures should be properly verified; this ensures the authentication of the messages.
Identity privacy	During the whole process, only the pseudonyms are used to specify each entity; this ensures the identity privacy. Note that this does not provide unlinkability if the pseudonyms are not frequently update. We will study unlinkability in the future work.
Group session key privacy	The computation of the group session key is based on the CDHP problem. This has been proved in Theorem 6. During the group session activation phase, only $h(h(SK^{SID}))$ the double-hash value of the session key is released. These mechanisms ensure the group key privacy.
Group forward/ backward secrecy	The new key is updated as new- $SK_i^{SID} := h(r', h(SK_i^{SID}))$. Because the SN only delivers the *r'* to those legitimate entities and only delivers the hashed old key $h(SK_i^{SID})$ to the will-be members. These two designs well protect the Group forward/backward secrecy.

6 Performance Evaluation

We compare the computational performance and the communication performance of our scheme with the related works in Section VI.A and Section VI.B respectively. Finally, we give a short summary of all the performance (security, computation, and communication).

The D2D schemes like SeDS [14] are pairwise D2D key agreement. Even though they might be iteratively applied to establish group communications among n UEs, it is very costly in terms of computations and communications because the complexity is $O(n^2)$. On the contrary, the complexities of our scheme are $O(n)$. Considering Wang-Yan's PPAKA-HMAC only considers external attackers, which is impractical as many UEs are prone to various attacks. Therefore, in the rest of this section, we will focus on the comparison of our PPAKA-CLAS with Wang-Yan's PPAKA-IBS.

6.1 The Computational Performance

We neglect those lightweight operations like modular addition, XOR, etc, as their contributions to the overhead are insignificant. We skip those initialization phases of all related works in the comparison, as they are very similar and do not demand lots of overhead. Let $T_{\text{ECC\_PM}}$ denotes the time complexity of one elliptic curve point multiplication, $T_{\text{ECC\_PA}}$ denotes that of one elliptic curve point addition, T_h denotes that of one hash operation, T_{GF_MM} denotes that for one modular multiplication in GF(p), T_{GF_ME} denotes that for one modular exponentiation in GF(p), T_{pair} denotes that for one pairing operation, and T_{mp} denotes that for one map-to-point function.

The signature generation of our CLAS scheme, the CLAS-AS, needs $1\ T_{\text{ECC\_PA}} + 1\ T_h + 1\ T_{GF\_MM}$. The individual signature verification of our CLAS, the CLAS-ISV, demands $3T_{\text{ECC\_PM}} + 3T_{\text{ECC\_PA}} + 2T_h$. The signature aggregation, the CLAS-SA, takes $(n\text{-}1)\ T_{\text{ECC\_PA}}$. The aggregate signature verification, the CLAS-ASV, demands $n*(\ 2T_{\text{ECC\_PM}} + 3T_{\text{ECC\_PA}} + 2T_h\ ) + 1T_{\text{ECC\_PM}} = (2n+1)\ T_{\text{ECC\_PM}} + 3n\ T_{\text{ECC\_PA}} + 2n\ T_h$.

Now we analyze the computational cost of our PPAKA-CLAS. Here, we assume the SN uses the same CLAS scheme to simplify the evaluation. In the Group Session Request phase, each UE performs one CLAS signature and one CLAS verification, which totally demands $1\ T_{GF\_MM} + 3\ T_{\text{ECC\_PM}} + 4\ T_{\text{ECC\_PA}} + 3\ T_h$. The SN needs to calculate one CLAS-ASV and n M_i, which totally takes $(3n+1)\ T_{\text{ECC\_PM}} + (5n\text{-}1)\ T_{\text{ECC\_PA}} + 2n\ T_h$.

In the Session Establishment phase, a UE compute 3 keying materials and one CLAS-SG, which demands $2\ T_{\text{ECC\_PA}} + 1\ T_h + 1\ T_{GF\_MM} + 2\ T_{\text{ECC\_PM}}$. In the Group Key Generation phase, each UE performs one signature aggregation, one aggregate signature verification, and the session key derivation. The total cost is $(2n\text{-}1)\ T_{\text{ECC\_PM}} + (6n\text{–}7)\ T_{\text{ECC\_PA}} + 2(n\text{-}1)\ T_h$. In the Group Session Activation phase, each UE just needs $1\ T_{\text{ECC\_PA}} + 2\ T_h + 1\ T_{GF\_MM}$.

Table 4 summarizes the computational complexities and the communication overhead. The computational complexities are marked in green color, the communication overheads are marked in yellow color, and the fault tolerance is marked pink.

Table 4. Performance comparison of computation, communication, and fault tolerance

Phase[1]	PPAKA-CLAS		PPAKA-IBS [17]	
	UE	SN	UE	SN
GSR Comp.	$1T_{GF_{MM}} + 3T_{ECC_{PM}} + 4T_{ECC_{PA}} + 3T_h$	$(3n+1)T_{ECC_{PM}} + (5n-1)T_{ECC_{PA}} + 2nT_h$	0^{Note2}	$0^{\text{note 2}}$
GSR Comm.	$nL_{PID} + 2L_q + L_P$ (broadcast)	$nL_{PID} + L_q + (n+1)L_P$ (broadcast)	nL_{PID} note2 (1 UE-SN)	$n(n+1)L_{PID}$ $(nUE - SN)$
GSR Fault Tol.	S Verified UEs continue the process		If any UE discovered in D2D discovery phase does not commit their request in this phase, then SN rejects all requests	
SE Comp.	$2T_{ECC_{PA}} + 1T_h + T_{GF_{MM}} + 2T_{ECC_{PM}}$	0	$4T_h + 2T_{mp} + T_{GF_{MM}} + 10T_{ECC_{PM}} + 6T_{ECC_{PA}} + 3T_{pair}$	0
SE Comm.	$2nL_{PID} + L_q + 2L_P$ (broadcast)	0	$6L_{PID} + 5L_P$ (broadcast: 2 rounds)	0

Table 4. Performance comparison of computation, communication, and fault tolerance (continue)

Phase[1]	PPAKA-CLAS		PPAKA-IBS [17]	
	UE	SN	UE	SN
GKG Comp.	$(6n-7)T_{ECC\_PA}$ $+2(n-1)T_h$ $+2(n-1)T_{ECC\_PM}$	0	$(4n-5)T_{ECC_{PA}}$ $+(n-1)T_h$ $+(n-1)T_{mp}$ $+(n-1)T_{GF_{MM}}$ $+(n-1)T_{ECC_{PM}}+nT_{pair}$	0
GKG Comm.	0	0	0	0
GSA Comp.	$T_{ECC\_PA}+2T_h+T_{GF\_MM}$	0	$1T_h$	nT_h
GSA Comm.	L_q (broadcast)	0	L_q [note 3] (1 UE-SN)	nL_q $(nUE-SN)$
Total Comp.	$3T_{GF\_MM}+6nT_{ECC\_PA}$ $+(2n+4)T_h$ $+(2n+4)T_{ECC\_PM}$	$(5n-1)T_{ECC_{PA}}$ $+2nT_h$ $+(3n+1)T_{ECC\_PM}$	$(n+1)T_{mp}$ $+(4n+1)T_{ECC\_PA}$ $+(n+4)T_h$ $+(n+9)T_{ECC\_PM}$ $+(n+3)T_{pair}$	nT_h
Total Comm.	$(n+2)L_{PID}+4L_q+3L_P$	$nL_{PID}+L_q+(n+1)L_P$	$(n+6)L_{PID}+L_q+5L_P$	$n(n+1)L_{PID}+nL_q$
KUComp.	$T_{ECC\_PA}+2T_h+T_{GF\_MM}$	0	$1T_h$	nT_h
KUcomm.	L_q (broadcast)	L_q	L_q [note 3] (1 UE-SN)	nL_q $(nUE-SN)$

1. GSR: Group Session Request; SE: Session Establishment; GKG: Group Key Generation; GSA: Group Session Activation; Comp.: computation; Comm.: Communication; KU: Key Update.
2. In Wang-Yan's scheme, each UE needs to establish a secure UE-SN channel to send its request to the VN. Therefore, there are *n* UE-SN connections.
3. In Wang-Yan's scheme, each UE needs to establish a secure UE-SN channel to send its $h(SK_i^{SID})$ to the SN. Therefore, there are there are *n* UE-SN connections.

Here, we note that the computational complexities listed in Wang-Yan's publication [17] are wrong: they wrongly confuse some computation notations, and, therefore, have the wrong calculations in their comparison table. One obvious example is discussed and corrected here. The group G in their scheme is an additive cyclic group based on elliptic curves, and g is a generator for G. Therefore, even though g^{x_i} and $PK_i^{x_i}$ with $PK_i = H_2(PID_i) \in G$ have the form of exponentiation, they are point multiplications in ECC. In their comparison, they wrongly mix these notations. Because the difference is significant, we should correct it in the comparison. One another is $PK_i = H_2(PID_i) \in G$, which has the form of normal hash, but it is a mapping to point (mapping input to a point in ECC). Fortunately, normal hashing and a map- to-point function are quite lightweight, compared to other computations. We, therefore, can ignore these two computations.

Among the computations listed in Table 2, T_{pair}, T_{mp}, $T_{\text{ECC\_PM}}$, and $T_{\text{ECC\_PA}}$ are the most expensive computations, and their actual timing costs depend on the parameters, the software environment, the hardware and the implementations [5, 9, 26-27, 30]. To have a fair comparison, we refer to the same setting and platforms as [2, 5], where the bit length of Galois field is 1024 bits, and the ECC group G with order $|q|$=160. In such an setting and the algebra equations of ECC from [9], we have $T_{\text{ECC\_PM}} \sim = 241\, T_{\text{ECC\_PA}}$, where "~=" means "roughly equal". We list the figures for the setting in Table 5. Applying these figures, a UE in our scheme spends 2.41 ms, and a UE in Wang-Yan's scheme takes 71.6 ms for the case n=2 (only two devices in a group); for the case n=1000, a UE in our scheme takes 606.158 ms, and Wang-Yan's scheme spends 14023 ms. We can see that even in a very small group of n=2, our scheme has much better computational performance. Figure 3 shows how a UE computational cost varies as the number of members changes. From Figure 3, we can see that our

computational performance improvement amplifies more significantly as n increases.

Table 5. Time cost for referring operations

Symbol	Time (ms)	Symbol	Time (ms)
T_{pair}	13.6736	T_{ECC_PM}	0.2986
T_{GF_ME}	0.3418	T_{ECC_PA}	0.001239
T_{GF_MM}	0.0019	T_{SSL}	45.1

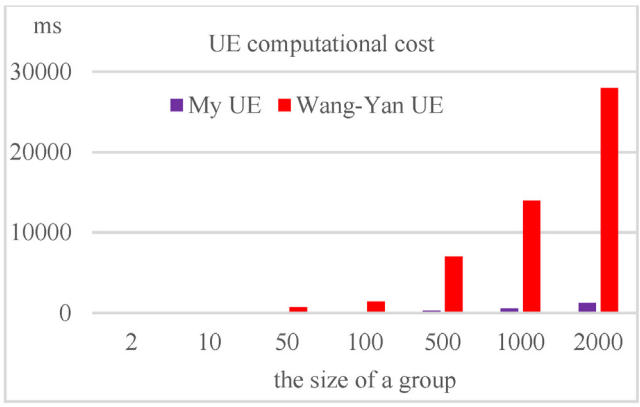


Figure 3. The computational costs of a UE

6.2 The Communication Performance

Here, we concern two communication overhead metrics: one is the message length and the other is the number of message rounds. Let L_{PID} denote the bit length of one identity (like one pseudonym, or one group session identity). L_q denotes the bit length of the order q and the output length of one hash. L_Q denotes the bit length of one ECC point representation. The total communication overhead for each UE in our scheme is $(n+2)L_{PID}+4L_q+3L_P$ while that for Wang-Yan's scheme being $(n+6)L_{PID}+L_q+5L_P$. We can see that there is no significant difference between these two schemes. The total communication overhead of SN in our scheme $nL_{PID}+L_q+(n+1)L_P$ while that for Wang-Yan's scheme being $n(n+1)L_{PID}+nL_q$; we can see that the overhead of SN in Wang-Yan's scheme ($O(n^2)$) is much larger than ours $O(n)$. This is because Wang-Yan's scheme needs n pairwise UE-SN connections (each of the UE-SN connection demands $O(n)$ overhead) in both the group session request phase and the group session activation phase. Additionally, Wang-Yan's session establishment phase needs two rounds while ours requiring only one round. At the first glance on the green part of our Table 4, it might seem that the SN in Wang-Yan' scheme requires less computational overheads than ours. But, we should note that in Wang-Yan's scheme, the SN need $O(n)$ UE-SN connections (each of the UE-SN connection demands $O(n)$ communication overheads) while our scheme requiring only simple broadcasting. Because Wang and Yan did not describe how the authenticated UE-SN connections are implemented, we, therefore, do not include the computational overheads in the Table. But, we should note that these UE-SN connections would require some overheads on the SN.

To simplify the simulation without losing its semantics, we let the transmission time of the broadcast channel in both schemes (our scheme and Wang-Yan's scheme) being zero, as the broadcast channel does not need session connection time. In the simulation, we also let the total connection time of n SSL connections be the square root(n) times of one SSL connection. We let the UE-SN SSL connection time be 45.1 ms. Figure 4 shows the simulation time of each phase, where the Y-axis is in $\log_2$(time in ms). Both Wang-Yan's GKG and Wang-Yan's GSA are the two longest phases. Wang-Yan's GKG involve the costly pairing computations, and Wang-Yan's GSA involves the costly UE-SN SSL connections; on the contrary, our scheme uses simple broadcast channels, and involves only lighter ECC computations. Figure 5 shows the simulation time of the whole process, where the Y-axis is in ms. From Figure 5, we can see that the whole process latency of Wang-Yan's scheme is longer than ours, and the difference becomes more and more significant as the size of the group increases.

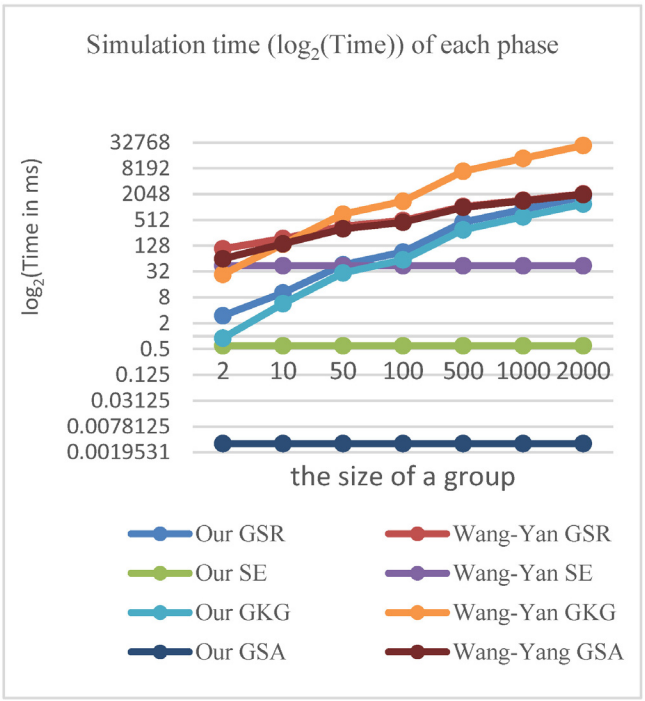


Figure 4. Simulation time in $\log_2$(ms) of each phase (refer to Table 4 for the symbols)

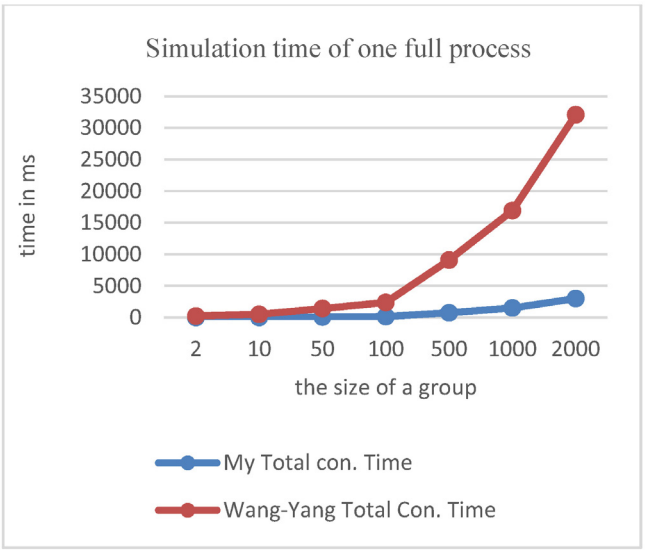


Figure 5. The simulation of the whole process

In a short summary, our scheme shows much better performance than Wang-Yan's scheme in terms of computations, communications, and fault tolerance. Table 6 summaries the rationales behind each improvement.

7 Conclusions

This paper has proposed a certificateless aggregate signature scheme, called the CLAS. Based on our CLAS and the technique of applying the MCDHP, we have proposed our privacy-preserving authenticated key agreement scheme for the D2D group communications. The security properties of the proposed scheme have been proved. The performance analysis and evaluations show that our scheme owns significant improvements over Wang-Yan's scheme in terms of computations, communications, and fault tolerance. The computational performance is so obvious that even if the group is very small (only two devices), our computational cost is only 4% the computational cost of Wang-Yan's scheme. And, the improvement is greatly amplified when the group size increases. These improvements make our scheme much more attractive and practical, considering many devices are resource-limited and are prone to various attacks. Three future works are interesting. One is to reduce the involvement of service networks to avoid the possible bottleneck at the service networks. Another is to enhance the fault tolerance in the latter phases of the process to cope with possible hostile attacks in IoT environments. The third one is providing un-linkability of IoT devices; an attacker can still link the transmissions from the same device in our scheme, if the pseudonyms are not changed very frequently.

Table 6. Detailed rationales behind each improvement

Metrics	Detailed rationales
Computation improvements	In the group session request phase, each entity only need to ensure the authenticity of others' ephemeral public keys; there is no requirement of encrypting the public keys. Therefore, we design our new CerftificateLess Aggregate Signature as a building block, instead of using existent CertificateLess Aggregate SignCryption (CLASC). Our CLAS is based on efficient Elliptic Curve Cryptography (ECC); But, Wang-Yan' scheme applied Identity-Based Signature which requires computationally expensive pairing operations. Furthermore, our MCDHP-based key computation is more efficient than the conventional CDHP-based key agreement. The new building blocks are far more efficient.
Communication improvements	Merge two message rounds into one when it is feasible in the session establishment phase. Replace O(n) UE-SN SSL interactions with O(n) UE broadcast in the group session request phase, in the group session activation phase, and in the key update phase.
Fault tolerance	We let UEs commit their ephemeral public keys in the group session request phase. And, we let SN verify UEs' commitment of ephemeral public keys as soon as possible so that, when UEs enter the session establishment phase, they can continue their session establishment and group key computation. This arrangement not only enhances fault tolerance but also reduce message rounds.

Acknowledgments

This project is partially supported by the Ministry of Science and Technology of Taiwan, under the grant no. MOST 108-2221-E-260-009-MY3.

References

[1] C. L. I, M. A. Uusitalo, K. Moessner, The 5G Huddle: from the guest editors, *IEEE Vehicular Technology Magazine*, Vol. 10, No. 1, pp. 28-31, March, 2015.

[2] X. Li, S. P. Liu, F. Wu, S. Kumari, J. J. P. C. Rodrigues, Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications, *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 4755-4763, June, 2019.

[3] 3GPP, 3GPP TS 33.401 *3GPP System Architecture Evolution (SAE)*; Security architecture, 3GPP, ed, 2015.

[4] 3GPP, *Standards for the IoT*, 2016. https://www.3gpp.org/news-events/1805-iot_r14.

[5] F. Wu, X. Li, L. Xu, A. K. Sangaiah, J. J. P. C. Rodrigues, Authentication Protocol for Distributed Cloud Computing: An Explanation of the Security Situations for Internet-of-Things-Enabled Devices, *IEEE Consumer Electronics Magazine*, Vol. 7, No. 6, pp. 38-44, November, 2018.

[6] S. Kim, J. Y. Choi, J. Jeong, On Authentication Signaling Costs in Hierarchical LTE Networks, *2014 7th International Conference on Ubi-Media Computing and Workshops*, Ulaanbaatar, Mongolia, 2014, pp. 11-16.

[7] F. B. Degefa, D. H. Lee, J. Y. Kim, Y. S. Choi, D. H. Won, Performance and security enhanced authentication and key agreement protocol for SAE/LTE network, *Computer Networks*, Vol. 94, pp. 145-163, January, 2016.

[8] H. Y. Chien, Group-Oriented Range-Bound Key Agreement for Internet-of-Things Scenarios, *IEEE Internet of Things Journal*, Vol. 5, No. 3, pp. 1890-1903, June, 2018.

[9] M. Scott, On the Efficient Implementation of Pairing-Based Protocols, in: L. Chen (Eds.), *IMA International Conference on Cryptography and Coding*, LNCS 7089, Springer, 2011, pp. 296-308.

[10] M. Wang, Z. Yan, A survey on security in D2D communications, *Mobile Networks and Applications*, Vol. 22, No. 2, pp. 195-208, April, 2017.

[11] M. Wang, Z. Yan, V. Niemi, UAKA-D2D: Universal authentication and key agreement protocol in D2D communications, *Mobile Networks and Applications*, Vol. 22, No. 3, pp. 510-525, June, 2017.

[12] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, Y. Cheng, Secure key establishment for device-to-device communications, *Proc. IEEE Global Communications Conference*, Austin, TX, USA, 2014, pp. 336-340.

[13] H. Kwon, C. Hahn, D. Kim, K. Kang, J. Hur, Secure device-to-device authentication in mobile multi-hop networks, *International Conference on Wireless Algorithms, Systems, and Applications*, Harbin, China, 2014, 267-278.

[14] A. Zhang, J. Chen, R. Q. Hu, Y. Qian, SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks, *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 4, pp. 2659-2672, April, 2016.

[15] A. Zhang, L. Wang, X. Ye, X. Lin, Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 3, pp. 662-675, March, 2017.

[16] R. Hsu, J. Lee, T. Q. S. Quek, J. Chen, GRAAD: Group Anonymous and Accountable D2D Communication in Mobile Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 2, pp. 449-464, February, 2018.

[17] M. Wang, Z. Yan, Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3637-3647, August, 2018.

[18] W. Diffie, M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-654, November, 1976.

[19] T. F. Lee, T. Hwang, C. L. Lin, Enhanced three-party encrypted key exchange without server public keys, *Computers and Security*, Vol. 23, No. 7, pp. 571-577, October, 2004.

[20] H. Y. Chien, A Generic Approach to Improving Diffie-Hellman Key Agreement Efficiency for Thin Clients, *The Computer Journal*, Vol. 59, No. 4, pp. 592-601, April, 2016.

[21] H. Y. Chien, Using The Modified Diffie-Hellman Problem to Enhance Client Computational Performance in a Three-Party Authenticated Key Agreement, *Arabian Journal for Science and Engineering*, Vol. 43, No. 2, pp. 637-644, February, 2018.

[22] M. S. Wang, Z. H. Qi, A Certificateless Aggregate Signcryption Scheme without Bilinear Pairing, *Computer Technology and Development*, Vol. 27, No. 8, pp. 1-5, August, 2017.

[23] J. Cao, P. Yu, M. Ma, W. Gao, Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network, *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 1561-1575, April, 2019.

[24] J. Cui, J. Zhang, H. Zhong, R. H. Shi, Y. Xu, An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks, *Information Sciences*, Vol. 451-452, pp. 1-15, July, 2018.

[25] I. A. Kamil, S. O. Ogundoyin, An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks, *Journal of Information Security and Applications*, Vol. 44, pp. 184-200, February, 2019.

[26] S. Al-Riyami, K. Paterson, Certificateless public key cryptography, *Proc. of Asiacrypt*, Taipei, Taiwan, 2003, pp. 452-473.

[27] S. Chung, J. Lee, H. Chang, C. Lee, A high-performance elliptic curve cryptographic processor over GF(p) with SPA resistance, *2012 IEEE International Symposium on Circuits and Systems*, Seoul, Korea (South), 2012, pp. 1456-1459.

[28] 3GPP, Study on architecture enhancements to support proximity-based services (ProSe), Stage 2, 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects*; 3GPP TS 23.3034, V15.0.0, June, 2017.

[29] L. Harn, New digital signature scheme based on discrete logarithm, *Electronics Letters*, Vol. 30, No. 5, pp. 396-398, March, 1994.

[30] P. Horster, H. Petersen, M. Michels, Meta-ElGamal signature schemes, *Proc. of the 2nd ACM Conference on Computer and communications security*, Fairfax, Virginia, USA, 1994, pp. 96-107.

[31] H. Y. Chien, Y. J. Chen, G. H. Qiu, J. F. Liao, R. W. Hung, P. C. Lin, X. A. Kou, M. L. Chiang, C. H. Su, A MQTT-API-Compatible IoT Security-Enhanced Platform, *International Journal of Sensor Networks*, Vol. 32, No. 1, pp. 54-68, January, 2020.

[32] S. Kumari, X. Li, F. Wu, A. K. Das, K. K. R. Choo, J. Shen, Design of a provably secure biometrics-based multi-cloud-server authentication scheme, *Future Generation Computer Systems*, Vol. 68, pp. 320-330, March, 2017.

[33] S. Kumari, M. K. Khan, M. Atiquzzaman, User Authentication Schemes for Wireless Sensor Networks: A Review, *Ad Hoc Networks*, Vol. 27, pp. 159-194, April, 2015.

Biography

Hung-Yu Chien received the B.S. degree from NCTU, Taiwan, 1988, the M.S. degree from NTU, Taiwan, 1990, and the doctoral degree in applied mathematics at NCHU 2002. He is a professor of National Chi Nan University since 199808 His research interests include cryptography, networking, network security, ontology, and Internet-of-Things.