




Article

A Homomorphic Digital Signature Scheme for the Internet of Things

Mohamed Hamdi ^{1,*}, Sandeep Pirbhulal ^{2,*} and Habtamu Abie ^{2,*}

¹ University of Carthage Higher School of Communication of Tunis (SUPCOM) Tunisia; hamdi.mm@gmail.com

² Norwegian Computing Center, P.O. Box 114, Blindern, 0314 Oslo, Norway; sandeep@nr.no, habtamu.abie@nr.no

* Correspondence: hamdi.mm@gmail.com (M.H.), sandeep@nr.no (S.P.), habtamu.abie@nr.no (H.A.)

Abstract: In this paper, we address the problem of compatibility between digital signature schemes and in-network aggregation approaches. In the IoT world, the gateways alter the signed network flows when performing in-network aggregation. Therefore, existing conventional approaches are not suitable for verifying the authenticity of the original flows. This raises the need for energy-effective and secure schemes that enable the destination to validate aggregated network flows. In this regard, a lightweight homomorphic signature scheme is proposed which supports the implementation of aggregation procedures without affecting the verification process. We demonstrate the unforgeability and the privacy of our scheme. We also perform an analytical study of its energy-efficiency. The results suggest that the proposed scheme considerably decreases the processing overhead of the existing set-homomorphic signature schemes. Moreover, it does not add any communication overhead to traditional (non-homomorphic) signature schemes. This, in turn, improves the energy consumption by 30% compared to existing homomorphic signature techniques.

Keywords: Homomorphic; Digital Signature; IoT; Authentication

1. Introduction

IoT-based healthcare systems are exposed to numerous security challenges. These are mainly due to the wireless connectivity of IoT devices, and their network topologies. At the same time, many IoT medical devices are tiny and have limited power support. Therefore, it is essential that their security framework offers a balance between security and energy efficiency. As a matter of fact, Wireless Body Area Networks (WBANs) consist of resource-constrained devices that monitor various parameters, including body temperature, blood pressure, and Electromyography. The patient monitoring system proposed in the ASSET project illustrates the role of WBANs in the eHealth system (Figure 1) using smart things such as sensors and actuators [1]. The ASSET project developed adaptive security approaches for healthcare using IoT, specifically lightweight mechanisms that will allow it to adapt to a dynamic changing context of threats, diversity, and processing capability. This allows the mechanisms to detect, respond and adapt in real-time to future security and privacy threats. It is essential to consider efficient utilization of resources in IoT, since sensor nodes used in these networks are tiny and have a limited battery. Thus, lightweight schemes need to be used for implementing security in IoT systems.

The main challenge for applying cryptographic approaches is their high consumption of computing resources. These usually need various iterations to perform encryption and decryption. Thus it is unfeasible to implement them within low-powered medical devices. In WBANs, the resources are needed during data processing, storing, and transmission. In fact, healthcare systems encourage reducing the amount of data that is processed in order to save both energy and cost. Therefore, aggregation has often been considered an optimal approach for computing and storage abilities of the local node, as it eliminates excessive data within the system flow. Figure 1 demonstrates an architecture in which the WBAN gateways are used to gather bio-signals acquired from patients using sensor nodes.

In the last decade, numerous methods have been developed to perform data and network aggregation [2–4]. They have been useful in saving the energy resources of the

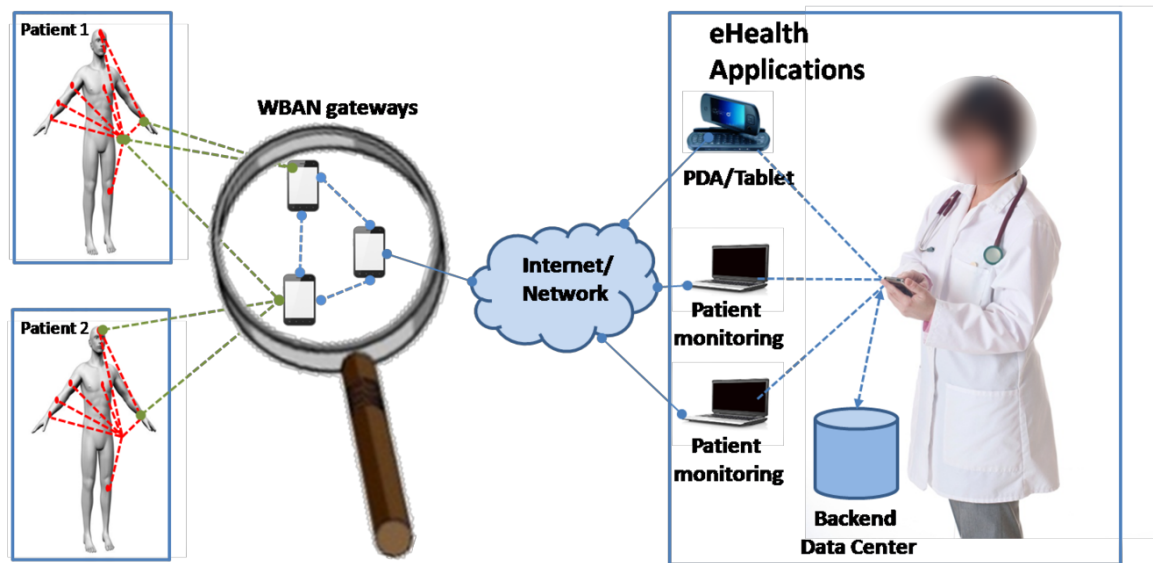


Figure 1. Architecture of an IoT-based eHealth system.

gateways, thereby extending the lifetime of the WBAN. Unfortunately, such aggregation mechanisms can also impact the system's security properties. For example, if few packets are dropped, the destination node will not be able to correctly validate the signed stream's authenticity. Many homomorphic signature techniques have been proposed to solve this problem. Nonetheless, they exhibit severe short-comings making them inapplicable in our context. In fact, most of them only focus on the cases where the aggregated message is obtained through the application of addition, multiplication, or polynomial functions on the original messages [22,24,25]. However, these techniques do not apply to the contexts where subsets of the original messages are eliminated during the aggregation process to minimize redundancy or to preserve anonymity. This property is only fulfilled by "redactable" signature schemes [26,27] and "sanitizable" signature schemes [20].

These schemes allow a party to remove parts of a signed document without affecting its digital signature. Also a third party would be able to redact the signed document without the use of private keys while the verifier is able to verify the validity and authenticity of the remaining documents. The techniques that have been proposed in the literature to implement this concept do not scale with the length of the message. This constitutes a severe limitation in our application since the transmission of large digital signatures considerably increases the communication overhead and reduces the lifetime of the smart things.

This research work addresses the problem associated with designing digital signatures schemes that are compatible with in-network aggregation. The redactable property is required for the WBAN gateways to perform efficient aggregation operations on the traffic transmitted by the smart things deployed on the patient body without affecting the digital signatures of these traffics. Since aggregation is not limited to the removal of subsets of messages, we introduce the set-homomorphism property, which extends redactability to other set operations such as union and intersection. A set-homomorphic signature approach allows signing sets so that the signature can be computed on the union of signed sets or the subset of a signed set [16].

We show that the signature scheme used to guarantee the authenticity of the medical data needs to be set-homomorphic and follow a definition of the before-mentioned signature procedure. After that, a set-homomorphic scheme is proposed using Elliptic Curve Cryptography (ECC) for healthcare applications. The main characteristic of our research is that it supports the application of basic set theoretic operations (i.e., union, intersection) on a digitally signed system flow without altering the verifying mechanism. The unforgeability and privacy properties of our scheme are also proved. An analytical

study is conducted to assess its energy effectiveness. An experimental study is presented to evaluate the overhead introduced by our set-homomorphic signature scheme in terms of bandwidth, delay, and energy consumption.

Our main contributions are as follows:

1. A new set-homomorphic signature scheme is proposed. It allows the computation of a signature on a set of aggregated packets (computed as the union of the sets of the original packets) without requiring the private keys used to compute the original signatures.
2. The unforgeability, privacy, and length-efficiency of the proposed signature algorithm are studied. We found that the complexity of computing forged signatures is equivalent to the Computational Diffie-Hellman (CDH) problem, and the length of the signature is substantially reduced compared to existing schemes.
3. A prototype of our signature technique is implemented on T-mote Sky sensors and O2 smartphones. The results that have been obtained through experiments corroborate the analytical study and show that our scheme outperforms the existing candidate approaches for implementing set-homomorphic signature schemes for the IoT.

The paper is organized as follows: The requirements analysis and related approaches are presented in Section 2. Section 3 discusses proposed set-homomorphic scheme to compute aggregate signatures in the IoT. The properties of our technique are mathematically studied in Section 4. Section 5 describes the experiments that have been performed to prototype the proposed solution and evaluates the performance of this solution with respect to existing techniques. Finally, Section 6 concludes the paper and gives future prospects.

2. Digital Signature Schemes for IoT in eHealth

IoT is important in modern healthcare systems because doctors, families, and insurance companies can assess medical records to follow up on the treatment plans of patients. However, care needs to be taken to mitigate potential threats on these intelligent networks and guarantee that medical information is only accessed by authorized users. The tiny medical devices used in healthcare have limited power, processing, memory, and communication resources. Thus, using strong cryptographic algorithms and protocols is not an optimal solution. This section addresses the requirements related to the computation of aggregate signatures in an IoT environment. Then, existing approaches to address aggregate signatures and underline their limitations in our context are discussed.

2.1. Requirement analysis

In Figure 1, it is assumed that the WBAN gateways perform the aggregation procedure so to save resources by reducing communication overhead which is the performance bottleneck of the patient monitoring system. For instance, through practical experiments realized on a T-mote Sky sensor, we found that the energy consumption for the calculation of the SHA-1 hash value is $14.7\mu J$ while transmitting the hash value costs $30\mu J$. This illustrates the processing and communication overhead impact related to security algorithms and protocols on power consumption.

A critical problem related to the implementation of aggregate signatures that save battery life is addressed in this work. Figure 2 presents an illustration medical gateway aggregates packet flows originating from different smart things deployed on the patient body. The authenticity of the origin of these packets is guaranteed through the digital signature. The two main rationales to support the aggregation process are:

1. Reducing redundancy between the packet flows to minimize energy consumption and communication latency.
2. Preserving the patient's privacy by hiding information related to his/her identity, sex, or location, etc.

Figure 2 demonstrates that the WBAN gateway will aggregate the traffic from all incoming packets and only forward one green and one violet packets. The available options for aggregating signatures along with packet flow are stated as follows:

- Naive forwarding: The gateway sends the signatures associated with the input packet flows. The verifier will not verify signatures because the verifying procedure is altered since the partial original signed content utilized to form these signatures was omitted.
- Naive computing: For each aggregate flow, the gateway recalculates a new signature. The major drawback of this method, it creates processing overhead. Another shortcoming is that it destroys any connection to the originators of the signed packets
- Aggregate signature: The WBAN gateway generates a digital signature to aggregate packet flow without using private keys. This results in reducing the processing overhead. However, the length of the new signature is longer, which needs more energy during the computation process.

In this paper we develop a new aggregate signature scheme. In the following, we discuss the basic properties that should be fulfilled by such a scheme.

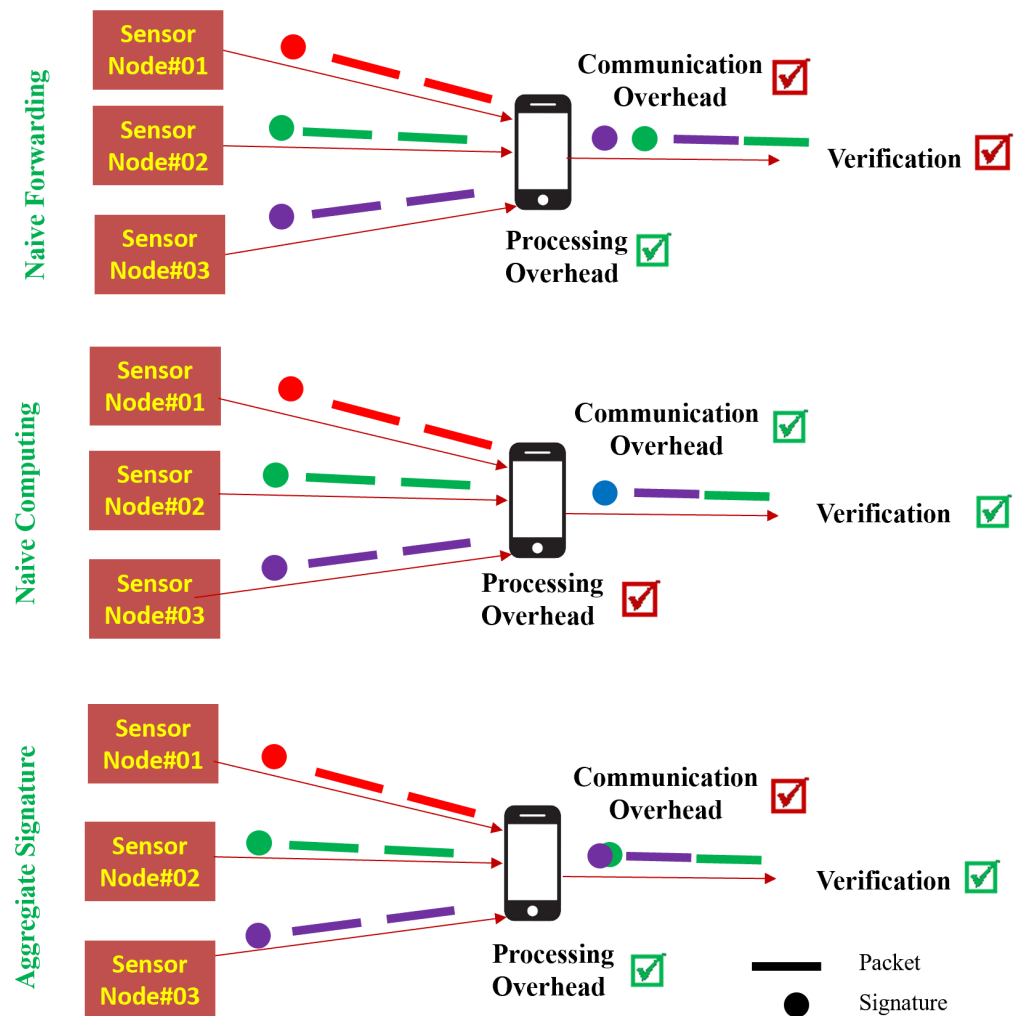


Figure 2. Options for the computation of aggregate signatures.

Definition 1. Set-based signature scheme

We consider a message space \mathcal{M} , a signature space \mathcal{S} , a private key space \mathcal{K}_{pr} , and a public key space \mathcal{K}_{pub} . A Set-Based Signature Scheme (SBSS) consists of the following three algorithms.

- A key generation algorithm $\text{gen} : \{1\}^\lambda \rightarrow \mathcal{K}_{\text{pr}} \times \mathcal{K}_{\text{pub}}$, where λ is the length of the public and private keys
- A signature generation algorithm $\text{sig} : \mathcal{K}_{\text{pr}} \times 2^{\mathcal{M}} \rightarrow 2^{\mathcal{M}} \times \mathcal{S}$, where $2^{\mathcal{M}}$ is the power set of \mathcal{M}
- A signature verification algorithm $\text{ver} : \mathcal{K}_{\text{pub}} \times 2^{\mathcal{M}} \times \mathcal{S} \rightarrow \{0, 1\}$

such that, for every $M \in 2^{\mathcal{M}}$, $\text{ver}(k_{\text{pub}}, \text{sig}(k_{\text{pr}}, M)) = 1$ if and only if, k_{pub} is the public key associated to k_{pr} .

In the rest of the paper, the algorithm that computes the digital signature is denoted by sig_0 . The mathematical relation between sig and sig_0 is given in Equation 1.

$$\text{sig}(k_{\text{pr}}, M) = \{M, \text{sig}_0(k_{\text{pr}}, M)\}. \quad (1)$$

A slight difference to the traditional signature schemes is that the function sig operates on sets of messages in $2^{\mathcal{M}}$ instead of operating on individual messages in \mathcal{M} . This is to make the signature scheme applicable to sets of packets issued by the smart things.

To illustrate the need for set-homomorphic signature schemes, we consider the simple case where a WBAN gateway receives two signed sets of packets originating from the sensor nodes s_1 and s_2 . The WBAN gateway receives $\text{sig}(k_{\text{pr},1}, \Pi_1)$ and $\text{sig}(k_{\text{pr},2}, \Pi_2)$ from s_1 and s_2 , respectively. The packet sets are represented by $\Pi_1 = \{\pi_{1,1}, \dots, \pi_{1,n_1}\}$ and $\Pi_2 = \{\pi_{2,1}, \dots, \pi_{2,n_2}\}$, where $p_{i,j} \in 2^{\mathcal{M}}$ for $i = 1, 2, 1 \leq j \leq n_i$, and n_i is the number of packets in the set Π_i . Having removed the redundancy from these sets, the WBAN gateway is supposed to forward $\Pi_1 \cup \Pi_2$. To guarantee the authenticity of the new set while avoiding the shortcuts of the naive forwarding and naive computing approaches described above, we propose to develop an implementation of aggregate signatures using set-homomorphic signature schemes.

Definition 2. Set-homomorphic signature scheme A set-based signature scheme $\text{SBSS} = \{\text{gen}, \text{sig}, \text{ver}\}$ is called set-homomorphic if there exist three operations $\diamond : \mathcal{K}_{\text{pr}} \times \mathcal{K}_{\text{pr}} \rightarrow \mathcal{K}_{\text{pr}}$, $\nabla : \mathcal{K}_{\text{pub}} \times \mathcal{K}_{\text{pub}} \rightarrow \mathcal{K}_{\text{pub}}$, and $\bullet : \mathcal{S} \times \mathcal{S} \rightarrow \mathcal{S}$ that satisfy the two following properties for a set operation \star and for any Π_1 and Π_2 in $2^{\mathcal{M}}$, any $k_{\text{pr},1}$ and $k_{\text{pr},2}$ in \mathcal{K}_{pr} , and any $k_{\text{pub},1}$ and $k_{\text{pub},2}$ in \mathcal{K}_{pub} .

- **Homomorphism**

$$\text{sig}_0(k_{\text{pr},1} \diamond k_{\text{pr},2}, \Pi_1 \star \Pi_2) = \text{sig}_0(k_{\text{pr},1}, \Pi_1) \bullet \text{sig}_0(k_{\text{pr},2}, \Pi_2). \quad (2)$$

- **Correctness**

$$\begin{aligned} &\text{ver}(k_{\text{pub},1} \nabla k_{\text{pub},2}, \text{sig}(k_{\text{pr},1} \diamond k_{\text{pr},2}, \Pi_1 \star \Pi_2)) = \\ &\text{ver}(k_{\text{pub},1}, \text{sig}(k_{\text{pr},1}, \Pi_1)) \wedge \text{ver}(k_{\text{pub},2}, \text{sig}(k_{\text{pr},2}, \Pi_2)), \end{aligned} \quad (3)$$

where \wedge is the logical AND operator.

Therefore, a Set-Homomorphic Signature Scheme (SHSS) consists of four algorithms and four operators. It is represented as follows.

$$\text{SHSS} = \{\{\text{gen}, \text{sig}, \text{ver}, \text{agg}\}, \{\diamond, \nabla, \bullet, \star\}\}, \quad (4)$$

where the algorithm $\text{agg} : \mathcal{S} \times \mathcal{S} \rightarrow \mathcal{S} \times \mathcal{A}$ returns an aggregate signature with a set of parameters in \mathcal{A} . \mathcal{A} is the set of parameters needed to compute the operation ∇ .

$$\begin{aligned} &\text{agg}(\text{sig}_0(k_{\text{pr},1}, \Pi_1), \text{sig}_0(k_{\text{pr},2}, \Pi_2)) = \\ &\{\text{sig}_0(k_{\text{pr},1}, \Pi_1) \bullet \text{sig}_0(k_{\text{pr},2}, \Pi_2), A\}, \end{aligned} \quad (5)$$

where $A \in \mathcal{A}$. For instance in the case where ∇ is a polynomial function, A would represent the coefficients of this polynomial, which have to be known by the verifier to compute $k_{\text{pub},1} \nabla k_{\text{pub},2}$ in Equation 3.

Since we are interested in the design of set-homomorphic signature schemes that are compatible with in-network aggregation, in the rest of the paper we mainly focus on the case where \star is the union operator. In this case, the set-homomorphic properties given in Equations 2 and 3 improve the energy-efficiency when the processing and communication overhead of \bullet is less than the processing and communication overhead for the computation of two digital signatures using the algorithm sig_0 . We also investigate two other set operations, which are set difference and intersection.

Additionally, the proposed signature scheme needs to fulfill other requirements also such as unforgeability, low process overhead, support of multiple signers, anti-reply, low communication overhead, privacy.

2.2. Literature review

Table 1. Summary of homomorphic signature schemes.

Ref./year	Underlying problem	Homomorphic property	Processing overhead	Communication overhead	Support of multiple signers
BF [22] / (2011)	SIS	Polynomial	$R \log(p+1)L$	$O(p \log(l.p))$	\times
N [24] / (2008)	RSA	Transitive	E	$2 \log(p) + 2l \log(l)$	\checkmark
BJ [25] / (2010)	RSA	Multiplication	$2.E$	$O(\log(p)) + \log(l)$	\checkmark
LLP [26] / (2012)	DLP	Set operations	$7.M$	$3l \log(q)$	\checkmark
SPBPM [27] / (2012)	CDH	Set operations	$2P$	$\log(q).O(l^2)$	\checkmark
HA / (2013)	CDH	Set operations	M	$\log(q)$	\checkmark

There are different types of homomorphic signatures present in the literature. These include prefix aggregation signatures [15], redactable signatures [16,19], sanitizable signatures [20], set-based signatures [21], verifiably encrypted signatures [13], multisignatures [17], transitive signatures (a special case of homomorphic signatures) [14], and linearly homomorphic signatures [22]. From these schemes ours is closely-related to set-based and redactable signature schemes.

A redactable (or sanitizable) signature scheme allows the removal of messages from the original message without affecting the verification process and without the redacted message and signature revealing anything about the content of the redacted message [20,23]. Hiding the amount and positions of redacted data is an important privacy requirement since one is able to derive the lengths or positions of the redacted (sanitized) data. Several authors address different properties of redactable signatures including immutability, signer accountability, sanitizer accountability, transparency, and unlinkability. In the literature, it is mentioned that such signatures are applicable in a number of relevant application scenarios, including medical applications, secure routing, multicast and database applications, privacy-preserving billing system, military and governmental applications just to mention few.

According to Definition 2, a set-homomorphic signature scheme signs sets that a third party can compute the signature on the output of set operators on the original sets. In our work, we focus on the union and subset operators since the WBAN uses them to aggregate the traffic coming from the smart things.

Table 1 reviews the homomorphic signature schemes that are most closely-related to our context. To evaluate the complexity of the signing and the verification operations as well as the length of the aggregate signatures, we suppose that integer exponentiation is performed in \mathbb{Z}_p^* , scalar point multiplication is performed in $E(\mathbb{F}_q)$, and R is the rank of the private basis used in lattice-based signature. Depending on the signature scheme, the complexity is evaluated in terms of number of exponentiations (E), number of scalar point

multiplications (M), number of pairing operations (P), number of lattice multiplications (M'), and number of lattice additions (L). Moreover, l denotes the number of digital signatures used to generate the aggregate signature.

We notice that the first three approaches [22,24,25] are limited with regard to the supported homomorphic operation. They do not allow the computation of aggregate signatures for packets flows to which simple set operations have been applied. In addition, the first approach [22] does not extend to the case where multiple private keys are used. The authors in [26,27] develop "redactable" signatures that have the property that given a signature on a message, a signature on the subsets of the message can be generated without using the private key.

Authors in [36] presented innovative, strictly more robust notions with supplementary use-cases for sanitizable Signatures schemes. In their research, notions of strong unforgeability and sanitizer accountability are focused that have great significance for security aspects in different applications. However, their study did not focus on resource efficiency, which is the main limitation for its implementation in medical scenarios. In [37], authors claim that the developed approach efficiently verifies aggregated data collected from different IoT devices using a homomorphic signature mechanism. The efficiency parameter was merely focused on authentication parameters, such as detecting forged signatures or proper signature generation. However, their re-search did not highlight the significance of energy efficiency for implementing the signature scheme in IoT. Furthermore, the developed approach is theoretical, the results and implementation scenarios are not provided to support their claim. Our previous research [38] highlighted the significance of the approach, which offers a balance between resource efficiency and security, but for supply-chain management. Here in this research work, we will be developing an energy-efficient security scheme for IoT-based healthcare.

Researchers have developed several other homomorphic cryptographic techniques for different applications in the modern era [39–42]. In [39], multi-signatures based approach is proposed based on signing multiple signature with key aggregation mechanism. Their proposed method does not require further public-key model assumptions and is build from three-round protocols. In [40], a framework is proposed integrating redactable signature scheme (RSS) with non-interactive zero-knowledge proof systems. It is claimed that their framework can play key role to comprehend privacy enhancing approach. However, the main limitation of [39,40] is that they only provided the theoretical model; there is no real-time verification or deployment of the developed approach. It is reported in [41] that RSSs are vulnerable to dishonest redactors or illegal redaction detection. To overcome this issue, authors in [41] proposed two distinct RSSs with flexible release control. It is also claimed that the proposed method has better performance in terms of security, and efficiency. However, it is not demonstrated how the issue with the efficiency of processing overhead of the existing schemes is solved. In [42], a certificateless aggregate signature approach is developed. Authors claim that the developed approach decreases the network bandwidth and also offers high confidentiality.

The major drawback of these techniques is that they generate long signatures that are not suitable to the scarcity of energy and communication bandwidth. The approach introduced in [27] covers this limitation but the size of the generated signature is equivalent to $\frac{n(n-1)}{2}$ normal signatures, where n is the number of private keys used to sign the message, while the signature generated by the algorithm proposed in [26] is of size $3n \log(q)$. Our scheme therefore outperforms existing schemes in terms of length efficiency as depicted in Table 1. Another point that should be underlined is that most of the prior work on homomorphic signature studies the security aspects in a theoretical framework and overlooks the issues related to the applicability of the proposed schemes in resource-constrained networks. In our case, we provide experimental results to assess the improvement resulting from the application of our set-homomorphic signature scheme in terms of communication, delay, processing, and energy overhead.

3. Proposed Set-Homomorphic Signature Scheme

Let G and G_T be two cyclic multiplicative groups and $\hat{e} : G \times G \rightarrow G_T$ be a bilinear map, which is a function that has the following properties [9]:

- **Computability:** There exists an efficiently-computable algorithm for computing $\hat{e}(x, y)$, for every x and y in G .

- **Bilinearity:**

$$\forall x, y \in G, \forall z_1, z_2 \in \mathbb{Z} \quad \hat{e}(x^{z_1}, y^{z_2}) = \hat{e}(x, y)^{z_1 z_2}. \quad (6)$$

- **Non-degeneracy:**

$$\forall x \in G, x \neq 0 \Rightarrow \langle \hat{e}(x, x) \rangle = G_T. \quad (7)$$

This is also equivalent to

$$\forall x \in G, x \neq 0 \Rightarrow \hat{e}(x, x) = 1. \quad (8)$$

The reader should refer to [9] for a detailed definition of bilinear maps.

We also consider a generator g of G . The set of sensor nodes is denoted by $S = \{s_1, \dots, s_n\}$. We also consider a hash function h on \mathcal{M} (meaning that h operates on packets). A function ψ is introduced to associate the transmitted packets with their sequence numbers defined by the communication protocol used at the layer 2 of the communication protocol stack. In our work, ψ reads the value of the sequence number field from the header of the packet to which it is applied.

Algorithm 0 in Figure 3 shows how the keys used to sign and verify the digital signatures are generated. The private key of a sensor s_i consists of a random integer $k_i \in \mathbb{Z}_q^*$, where q is the order of G . An algorithm PRNG is used to generate k_i using a security parameter κ . The corresponding public key is $\hat{k}_i = g^{k_i}$.

Algorithms 1 and 2 in Figure 3 illustrate how s_i generates the signature of a set of packets $\Pi_i \in 2^{\mathcal{M}}$ and how the eHealth applications verify this signature, respectively. In these algorithms, the concatenation operation is represented by the symbol \parallel . For every packet $\pi_{i,j}$ in Π_i , the hash function h is applied to the result of the concatenation of the packet with its sequence number. The product of these hashed packets is denoted by $H(\Pi_i)$. The algorithm sig returns the set Π_i along with $H(\Pi_i)^{-k_i}$, which is the digital signature of Π_i using the private key k_i . The verification algorithm relies on a function ext, which parses the received $\text{sig}(k_i, \Pi_i)$ and extracts the set of packets Π and the digital signature σ . To check the authenticity of Π , the function H , used by the signer, is applied to Π . Then, the verifier states that the received set of packets is authentic if and only if, $\hat{e}(\sigma, g) = \hat{e}(H(\Pi), g^{\hat{k}_i})$.

Lemma 3. *The algorithms gen, sig, and ver define a set-based signature scheme SBSS = {gen, sig, ver}.*

Proof. We show that SBSS fulfills the property of Definition 1. The correctness of the verification process is easy to check using the property of the bilinear map. In fact, the bilinearity feature implies that

$$\hat{e}(g^{H(\Pi_i)^{-1}}, g^{k_i}) = \hat{e}(g^{k_i H(\Pi_i)^{-1}}, g). \quad (9)$$

As a result, using the non-degeneracy property of the bilinear map \hat{e} , the SBSS scheme satisfies that

$$\text{ver}(\hat{k}, \text{sig}(k_i, \Pi_i)) = 1, \quad (10)$$

if, and only if, $\hat{k} = \hat{k}_i = g^{k_i}$. This proves that Algorithm 2 states that Π_i is authentic if, and only if, the public key used by the algorithm corresponds to the private key used to generate the signature of Π_i . Hence, according to Definition 1 SBSS is a set-based signature scheme. \square

Algorithm 0 Key generation
Require: g s.t. $G = \langle g \rangle$
Ensure: $\text{gen}(\kappa)$
1: $k_i := \text{PRNG}(\kappa);$
2: $\hat{k}_i := g^{k_i};$
3: $\text{gen}(\kappa) := \{k_i, \hat{k}_i\};$
Return: $\text{gen}(\kappa)$
Algorithm 1 Set-homomorphic signature
Require: $G = \langle g \rangle, k_i \in \mathbb{Z}_q^*, \Pi_i \in 2^{\mathcal{M}}$
Ensure: $\text{sig}(k_i, \Pi_i)$
1: $H(\Pi_i) := \prod_{\pi_{i,j} \in \Pi_i} h(\pi_{i,j} \psi(\pi_{i,j}))$
2: $\text{sig}(k_i, \Pi_i) := \{\Pi_i, g^{H(\Pi_i) \cdot k_i}\}$
Return: $\text{sig}(k_i, \Pi_i)$
Algorithm 2 Signature verification
Require: $\text{sig}(k_i, \Pi_i), g, \hat{k}_i$
Ensure: 0 or 1
1: $\{\Pi, \sigma\} = \text{ext}(\text{sig}(k_i, \Pi_i))$
2: $V := \prod_{\pi_j \in \Pi} h(\pi_j \psi(\pi_j))^{-1}$
3: if $\hat{e}(\sigma, g) = \hat{e}(g^V, \hat{k}_i)$ then
$\text{ver}(\hat{k}_i, \text{sig}(k_i, \Pi_i)) := 1$
else
$\text{ver}(\hat{k}_i, \text{sig}(k_i, \Pi_i)) := 0$
Return: $\text{ver}(\hat{k}_i, \text{sig}(k_i, \Pi_i))$

Figure 3. Algorithms 0, 1, and 2

Figure 4 illustrates the sequence of operations performed by the smart things to generate the signature for $\Pi \in 2^{\mathcal{M}}$ (Figure 4(a)) and the sequence of operations performed by the verifier to check the authenticity of a signature $\text{sig}(k_i, \Pi_i)$ (Figure 4(b)). In this figure, $|\Pi_i|$ is the number of packets in the set Π_i . Obviously, the figure does not model the real execution of the algorithms on the smart things because it does not take into consideration the way the multiplication, concatenation, and inversion operations are effectively executed.

The computational complexity of our signature algorithm is evaluated in terms of the following operations:

- $|\Pi_i|$ computations of h
- $|\Pi_i| - 1$ multiplications in \mathcal{M}
- 1 inversion in \mathcal{K}_{pr}
- 1 exponentiation in G

In practice, the cost of an exponentiation in multiplicative fields is much more significant than the computation of h , the multiplication in \mathcal{M} , or the inversion in \mathcal{K}_{pr} . For example, for one packet formatted according to the IEEE 802.15 protocol, if h is implemented using the SHA-1 algorithm and G is an elliptic curve group in \mathbb{Z}_{128} , then the energy costs of the aforementioned operations on a T-Mote Sky sensor are given in Table 2. Using these experimental values, if the proposed signature algorithm is applied to 10 packets, the energy spent for the three first rows does not exceed 5% of the energy spent for the exponentiation operation in G .

The computational complexity of the signature verification algorithm is evaluated in terms of the following parameters:

- $|\Pi_i| - 1$ computations of h
- $|\Pi_i|$ multiplications in \mathcal{M}
- 2 computations of the bilinear function \hat{e} (including two exponentiations in G for each computation of \hat{e}).

Table 2. Energy costs of elementary cryptographic computations on a T-Mote Sky sensor.

Operation	Energy cost
Execution of h	14.71 μ J
Multiplication in \mathcal{M}	1.5 μ J
Inversion in \mathcal{K}_{pr}	10.33 μ J
Exponentiation in G	6.93 mJ

This computational cost is comparable to the cost of existing signature schemes such as the Elliptic Curve Digital Signature Algorithm (ECDSA) [8]. In the context of our work, the computational cost on the verifier side is less crucial than the computational cost of the signature generation algorithm. This is mainly because the verifier is assumed to be part of the eHealth applications of Figure 1, where enough resources are available to perform standard cryptographic operations. For this reason, the communication, processing, delay, and power overhead on the verifier side are not experimentally studied in Section 5.

Another feature of our algorithm is that it does not add size overhead compared to existing signature schemes based on exponentiation in cyclic groups. In fact, as for traditional signature schemes, the length of the digital signature generated by our algorithm equals the order of the cyclic group G .

In proposed scheme, we used the sequence number which offers anti-replay security having less overhead, this property plays key role to provide robustness to our approach for IoT based healthcare.

4. Properties and Proofs

The proposed research applies ECC since it offers an energy-efficient performance. Let \mathbb{F}_q be a prime finite field and $a, b \in \mathbb{F}_q$ satisfying $4a^3 + 27b^2 \neq 0$. An elliptic curve group $E(\mathbb{F}_q)$ is defined by the set of points (x, y) satisfying $y^2 \equiv x^3 + ax + b \pmod{q}$, together with an extra point O called the point at infinity. In the following, we consider that G is a subgroup of $E(\mathbb{F}_q)$. We also use the Weil pairing function that has been shown in [10] to define a bilinear map where G_T is a subgroup of \mathbb{F}_{q^α} (α is a security multiplier depending on the group G). Hereafter, the operations of Algorithms 1 and 2 are assumed to be executed in G . Hence, g is considered as a point in $E(\mathbb{F}_q)$ and the exponentiation operation used in Algorithms 1 and 2 is replaced by scalar multiplication. For $x \in \mathbb{F}_q$ and $y \in G$, the scalar multiplication of y by x is represented by $x.y$.

In this section, we investigate the properties of the signature scheme introduced in this paper. We first prove that our scheme is set-homomorphic with respect to the union, subset, and intersection operators. Then, we analytically study its security and energy-effectiveness features.

4.1. Set-homomorphic properties of the proposed signature scheme

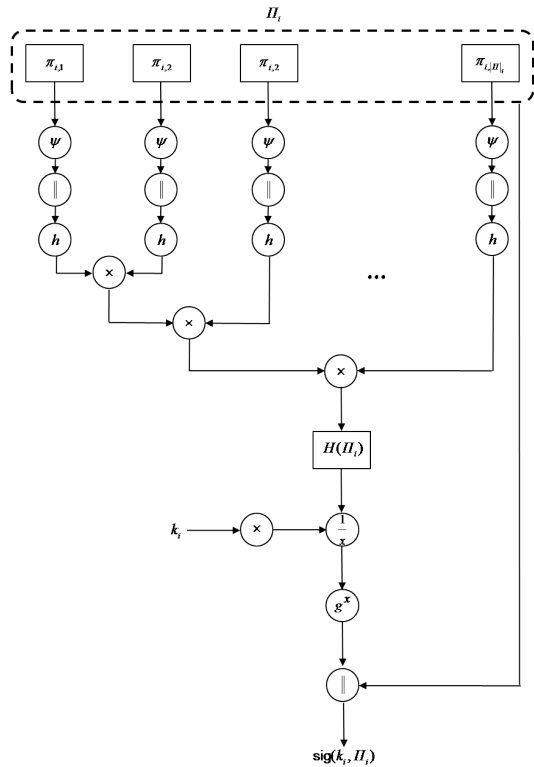
Our first objective is to demonstrate that our signature scheme is set-homomorphic with regard to the union operator. To this purpose, we express $H(\Pi_i \cup \Pi_j)$ using $H(\Pi_i)$ and $H(\Pi_j)$. The following lemma provides this expression.

Lemma 4. For every Π_i, Π_j in $2^{\mathcal{M}}$ and given the function H used in Algorithms 1 and 2, there exist unique integers u, v such that

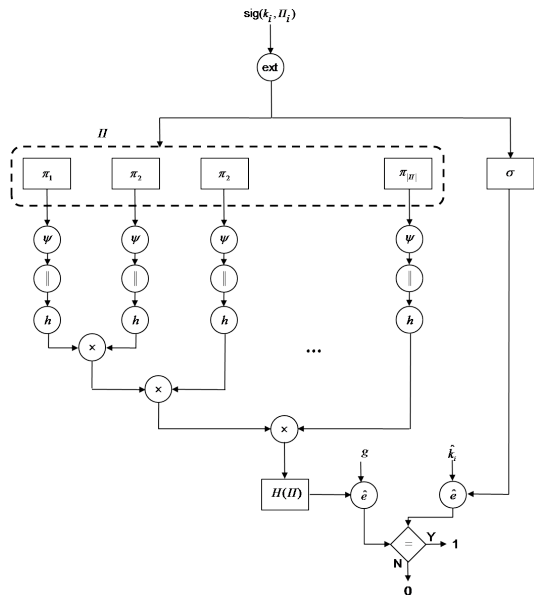
$$u.H(\Pi_i)^{-1} + v.H(\Pi_j)^{-1} = H(\Pi_i \cup \Pi_j)^{-1}. \quad (11)$$

Proof. Using the Bézout's identity [28], we can apply the Euclidean algorithm to find u, v such that

$$v.H(\Pi_i) + u.H(\Pi_j) = \gcd(H(\Pi_i), H(\Pi_j)). \quad (12)$$



(a) Signature generation.



(b) Signature verification.

Figure 4. Our set-homomorphic signature scheme (graphical illustration of Algorithms 1 and 2).

In other terms, the gcd and lcm satisfy the following property.

$$\gcd(H(\Pi_i), H(\Pi_j)).\text{lcm}(H(\Pi_i), H(\Pi_j)) = H(\Pi_i).H(\Pi_j). \quad (13)$$

Consequently, using Equations 12 and 13, we find the following expression of $\text{lcm}(H(\Pi_i), H(\Pi_j))^{-1}$.

$$\text{lcm}(H(\Pi_i), H(\Pi_j))^{-1} = u.H(\Pi_i)^{-1} + v.H(\Pi_j)^{-1}. \quad (14)$$

Given the construction of $H(\cdot)$, the computation of $H(\Pi_i \cup \Pi_j)$ is performed as follows:

$$\begin{aligned} H(\Pi_i \cup \Pi_j) &= \prod_{\pi_{k,l} \in \Pi_i \cup \Pi_j} h(\pi_{k,l} || \psi(\pi_{k,l})), \\ &= \text{lcm} \left(\prod_{\pi_{i,k} \in \Pi_i} h(\pi_{i,k} || \psi(\pi_{i,k})), \prod_{\pi_{j,l} \in \Pi_j} h(\pi_{j,l} || \psi(\pi_{j,l})) \right), \\ &= \text{lcm}(H(\Pi_i), H(\Pi_j)). \end{aligned} \quad (15)$$

As a result, by replacing $\text{lcm}(H(\Pi_i), H(\Pi_j))$ in Equation 14 by $H(\Pi_i \cup \Pi_j)$, we obtain the proof of the lemma. \square

We now use the property of Lemma 4 to prove the set-homomorphism property of our signature scheme with respect to the union operator.

Theorem 5. Set-homomorphism property 1 – Union operator

Consider the algorithms *gen*, *sig*, and *ver* defined in Algorithms 0, 1, and 2. Let *agg* be the algorithm of Equation 5 such $A = \emptyset$ and the \bullet operator is defined as follows.

$$\text{sig}_0(k_i, \Pi_i) \bullet \text{sig}_0(k_j, \Pi_j) = u' \text{sig}_0(k_i, \Pi_i) - v' \text{sig}_0(k_j, \Pi_j), \quad (16)$$

where

$$u' = u + vH(\Pi_i)H(\Pi_j)^{-1}, v' = v + uH(\Pi_j)H(\Pi_i)^{-1},$$

and u and v satisfy

$$v.H(\Pi_i) + u.H(\Pi_j) = \gcd(H(\Pi_i), H(\Pi_j)). \quad (17)$$

The signature scheme defined in the following equation is set-homomorphic.

$$\text{SHSS}_1 = \{\{\text{gen}, \text{sig}, \text{ver}, \text{agg}\}, \{\diamond, \nabla, \bullet, \cup\}\}, \quad (18)$$

where $k_i \diamond k_j = (k_i - k_j)$ and $\hat{k}_i \nabla \hat{k}_j = \hat{k}_i - \hat{k}_j$.

Proof. We demonstrate that SHSS_1 fulfills the homomorphism and correctness properties of Definition 2.

Proof of Homomorphism.

By expanding the expressions of $\text{sig}_0(k_i, \Pi_i)$ and $\text{sig}_0(k_j, \Pi_j)$, we demonstrate the following property.

$$\begin{aligned} &u \text{sig}_0(k_i, \Pi_i) + v \text{sig}_0(k_j, \Pi_j) \\ &= uk_i H(\Pi_i)^{-1}.g + vk_j H(\Pi_j)^{-1}.g \\ &= (uk_i H(\Pi_i)^{-1} + vk_j H(\Pi_j)^{-1}).g + v(k_j - k_i)H(\Pi_j)^{-1}.g \\ &= k_i(uH(\Pi_i)^{-1} + vH(\Pi_j)^{-1}).g + v(k_j - k_i)H(\Pi_j)^{-1}.g \\ &= \text{sig}_0(k_i, \Pi_i \cup \Pi_j) + v(k_j - k_i)H(\Pi_j)^{-1}.g. \end{aligned} \quad (19)$$

Similarly, we can write that

$$\begin{aligned} & u\text{sig}_0(k_i, \Pi_i) + v\text{sig}_0(k_j, \Pi_j) \\ &= \text{sig}_0(k_j, \Pi_i \cup \Pi_j) + u(k_i - k_j)H(\Pi_i)^{-1}.g. \end{aligned} \quad (20)$$

In addition, we have the following property for our signature algorithm.

$$\begin{aligned} & \text{sig}_0(k_i - k_j, \Pi_i \cup \Pi_j) \\ &= \text{sig}_0(k_i, \Pi_i \cup \Pi_j) - \text{sig}_0(k_j, \Pi_i \cup \Pi_j). \end{aligned} \quad (21)$$

Consequently, by subtracting Equation 19 from 20, we obtain the following result.

$$\begin{aligned} & \text{sig}_0(k_i - k_j, \Pi_i \cup \Pi_j) \\ &= u\text{sig}_0(k_i, \Pi_i) - v\text{sig}_0(k_j, \Pi_j) \\ &\quad - vk_iH(\Pi_j)^{-1} + uk_jH(\Pi_i)^{-1}. \end{aligned} \quad (22)$$

Noticing that

$k_iH(\Pi_j)^{-1} = H(\Pi_i)H(\Pi_j)^{-1}\text{sig}_0(k_i, \Pi_i)$ and $k_jH(\Pi_i)^{-1} = H(\Pi_j)H(\Pi_i)^{-1}\text{sig}_0(k_j, \Pi_j)$, we replace these terms in Equation 22.

$$\begin{aligned} & \text{sig}_0(k_i - k_j, \Pi_i \cup \Pi_j) \\ &= (u + vH(\Pi_i)H(\Pi_j)^{-1})\text{sig}_0(k_i, \Pi_i) \\ &\quad - (v + uH(\Pi_j)H(\Pi_i)^{-1})\text{sig}_0(k_j, \Pi_j) \end{aligned} \quad (23)$$

This proves that our signature scheme fulfills the homomorphism property of Definition 2 for the operators $\text{sig}_0(k_i, \Pi_i) \bullet \text{sig}_0(k_j, \Pi_j)$ defined in Equation 16 and $k_i \diamond k_j = k_i - k_j$. 365
366

Proof of Correctness. 367

We show how the verifier can rely on the aggregate signature $u'\text{sig}_0(k_i, \Pi_i) + v'\text{sig}_0(k_j, \Pi_j)$ to verify the authenticity of the aggregate traffic $\Pi_i \cup \Pi_j$. Using the properties of the bilinear function \hat{e} , we can write

$$\begin{aligned} & \hat{e}(u'\text{sig}_0(k_i, \Pi_i) + v'\text{sig}_0(k_j, \Pi_j), g) \\ &= \hat{e}(\text{sig}(k_i - k_j, \Pi_i \cup \Pi_j), g) \\ &= \hat{e}(H(\Pi_i \cup \Pi_j)^{-1}, (k_i - k_j)g). \end{aligned} \quad (24)$$

Consequently, given that $\hat{k}_i \nabla \hat{k}_j = \hat{k}_i - \hat{k}_j$, and using the ver algorithm, we have the following property.

$$\begin{aligned} & \text{ver}(k_i \nabla k_j, \text{sig}(k_i \diamond k_j, \Pi_1 \cup \Pi_2)) = 1 \quad \text{iff.} \\ & \hat{e}(k_iH(\Pi_i)^{-1}.g, g) = \hat{e}(H(\Pi_i)^{-1}, k_i.g), \quad \text{and} \\ & \hat{e}(k_jH(\Pi_j)^{-1}.g, g) = \hat{e}(H(\Pi_j)^{-1}, k_j.g). \end{aligned} \quad (25)$$

This proves the correctness of SHSS₁ according to Definition 2. □ 368
369

The set-homomorphism property proved in Theorem 5 is useful in practice to generate an aggregate signature for $\Pi_i \cup \Pi_j$ without the need for the private keys of the smart things. It allows an efficient implementation of the scenario depicted in Figure 2(c). Another interesting feature for the use of IoT in eHealth is the compatibility between our signature and privacy algorithms that guarantee k -anonymity [31]. These algorithms basically delete some parts of the healthcare data for the sake of pseudonymizing. To study the compatibility of our signature scheme to such techniques, we investigate whether it is possible for the WBAN gateway to generate a signature for a subset of the traffic sent by the smart things 370
371
372
373
374
375
376
377

without using the private keys of these things [30,31]. The following theorem proves that our signature scheme is homomorphic with respect to the subset operator.

Theorem 6. Set-homomorphism property 2 - Subset operator

Consider the algorithms gen , sig , and ver defined in Algorithms 0, 1, and 2. Let agg be the algorithm of Equation 5 such $A = \emptyset$ and the \bullet operator is defined as follows.

$$\begin{aligned} \text{sig}_0(k_i, \Pi_i) \bullet \text{sig}_0(k_j, \Pi_j) \\ = H(\Pi_j) \text{sig}_0(k_i, \Pi_i) - H(\Pi_j)^2 H(\Pi_i)^{-1} \text{sig}_0(k_j, \Pi_j). \end{aligned} \quad (26)$$

The signature scheme defined in the following equation is set-homomorphic.

$$\text{SHSS}_2 = \{\{\text{gen}, \text{sig}, \text{ver}, \text{agg}\}, \{\diamond, \nabla, \bullet, \setminus\}\}, \quad (27)$$

where $k_i \diamond k_j = k_i - k_j$ and $\hat{k}_i \nabla \hat{k}_j = \hat{k}_i - \hat{k}_j$.

Proof. As for the previous theorem, we prove the homomorphism and the correctness of SHSS_2 .

Proof of homomorphism.

Let Π_i and Π_j be two elements of $2^{\mathcal{M}}$ such that $\Pi_j \subset \Pi_i$. The function H used in Algorithms 1 and 2 satisfies the following property for every $k_i \in \mathbb{Z}_q^*$.

$$\begin{aligned} H(\Pi_i)^{-k_i} &= \prod_{\pi_{i,k} \in \Pi_i} h(\pi_{i,k})^{-k_i}, \\ &= \prod_{\pi_{i,k} \in \Pi_i \setminus \Pi_j} h(\pi_{i,k})^{-k_i} \cdot \prod_{\pi_{i,k} \in \Pi_j} h(\pi_{i,k})^{-k_i}. \end{aligned} \quad (28)$$

As a result, $H(\Pi_i \setminus \Pi_j)^{-k_i}$ can be written as follows.

$$H(\Pi_i \setminus \Pi_j)^{-k_i} = H(\Pi_i)^{-k_i} \cdot H(\Pi_j)^{k_i}. \quad (29)$$

Using the result of Equation 29, we expand the expression of $\text{sig}_0(k_i - k_j, \Pi_i \setminus \Pi_j)$.

$$\begin{aligned} \text{sig}_0(k_i - k_j, \Pi_i \setminus \Pi_j) \\ &= (k_i - k_j) H(\Pi_i)^{-1} H(\Pi_j).g \\ &= k_i H(\Pi_i)^{-1} H(\Pi_j).g - k_j H(\Pi_i)^{-1} H(\Pi_j).g \\ &= H(\Pi_j) \text{sig}_0(k_i, \Pi_i) - H(\Pi_j)^2 H(\Pi_i)^{-1} \text{sig}_0(k_j, \Pi_j). \end{aligned} \quad (30)$$

This proves that SHSS_2 is homomorphic with respect to the subset operation.

Proof of correctness.

Taking into consideration that $\hat{k}_i \nabla \hat{k}_j = \hat{k}_i - \hat{k}_j$, the application of the ver algorithm to the aggregate signature gives that

$$\begin{aligned} \hat{e}(\text{sig}_0(k_i - k_j, \Pi_i \setminus \Pi_j), g) \\ = \hat{e}(\text{sig}_0(k_i, \Pi_i))^{H(\Pi_j)} \hat{e}(\text{sig}_0(k_j, \Pi_j))^{H(\Pi_j)^2 H(\Pi_i)^{-1}}. \end{aligned} \quad (31)$$

Therefore, we have proved the correctness of SHSS_2 since

$$\begin{aligned} \text{ver}(k_i \nabla k_j, \text{sig}(k_i \diamond k_j, \Pi_1 \setminus \Pi_2)) &= \mathbf{1} \quad \text{iff.} \\ \hat{e}(k_i H(\Pi_i)^{-1}.g, g) &= \hat{e}(H(\Pi_i)^{-1}, k_i.g), \quad \text{and} \\ \hat{e}(k_j H(\Pi_j)^{-1}.g, g) &= \hat{e}(H(\Pi_j)^{-1}, k_j.g). \end{aligned} \quad (32)$$

□

This theorem is particularly interesting when $k_j = 0$. In this case, the result of Theorem 6 can be written as follows:

$$\text{sig}_0(k_i, \Pi_i \setminus \Pi_j) = H(\Pi_j) \text{sig}_0(k_j, \Pi_i). \quad (33)$$

This property can be used by the WBAN gateway to issue a digital signature for $\Pi_i \setminus \Pi_j$ without needing the private key k_i . Hence, private patient data such as the identity, race, and birth date can be hidden (by dropping the packets carrying this data) without the signature process being affected.

Having proved that our scheme allows the generation of aggregate signatures which are compatible with union and subset operations, it is possible to extend the homomorphic properties using the relations between set operations. For instance, using the results of Theorems 5 and 6, the following corollary establishes the set-homomorphism of our signature scheme with respect to set intersection.

Corollary 7. Set-homomorphism property 3 - Intersection operator

Consider the algorithms *gen*, *sig*, and *ver* defined in Algorithms 0, 1, and 2. Let *agg* be the algorithm of Equation 5 such $A = \emptyset$ and the \bullet operator is defined as follows.

$$\begin{aligned} \text{sig}_0(k_i, \Pi_i) \bullet \text{sig}_0(k_j, \Pi_j) \\ = vH(\Pi_i)H(\Pi_j)^{-1}\text{sig}_0(k_i, \Pi_i) \\ + uH(\Pi_j)H(\Pi_i)^{-1}\text{sig}_0(k_j, \Pi_j). \end{aligned} \quad (34)$$

The signature scheme defined in the following equation is set-homomorphic.

$$\text{SHSS}_2 = \{\{\text{gen}, \text{sig}, \text{ver}, \text{agg}\}, \{\diamond, \nabla, \bullet, \cap\}\}, \quad (35)$$

where $k_i \diamond k_j = k_i + k_j$ and $\hat{k}_i \nabla \hat{k}_j = \hat{k}_i + \hat{k}_j$.

This corollary can be proved using the fact that intersection can be expressed in terms of union and set difference:

$$\Pi_i \cap \Pi_j = ((\Pi_i \cup \Pi_j) \setminus (\Pi_i \setminus \Pi_j)) \setminus (\Pi_j \setminus \Pi_i). \quad (36)$$

We have shown through this corollary how the homomorphic properties of our signature scheme can be extended based on the union and subset operators depending on the need of the application in which the signature is used. In the IoT, the homomorphism property with respect to union operator is the most important because it allows the implementation of digital signature mechanisms that are compatible with in-network packet aggregation. In the following sections, we only focus on this scheme and conduct analytical and experimental analyses to assess the tradeoff between its security-effectiveness and energy-efficiency.

4.2. Security and energy-efficiency properties of the proposed signature scheme

We now study the security properties of our signature scheme. We first assess its resistance to forgery attacks. Goldwasser et al. [32] defined the unforgeability property as a game between an intruder \mathcal{I} and a challenger \mathcal{C} . The challenger is a user that makes a legitimate use of the cryptographic credentials of the signature algorithm. In our context, the challenger \mathcal{C} stands for a legitimate smart thing deployed on the patient's body and sending signed sets of packets to the WBAN gateway. The intruder \mathcal{I} is an eavesdropper located within the radio range of the WBAN and performing various non-legitimate actions. A digital signature scheme is unforgeable if no Probabilistic Polynomial-Time (PPT) intruder

\mathcal{I} , issuing a polynomial number of queries, is able to achieve a non-negligible advantage over the challenger \mathcal{C} in the following game (called the Forg game):

1. Given a security parameter κ , the challenger \mathcal{C} runs the key generation algorithm gen to obtain a key pair (k, \hat{k}) . The intruder \mathcal{I} is given the public key \hat{k} while the challenger \mathcal{C} keeps the private key k secret.
2. \mathcal{I} is given access to a signature oracle \mathcal{O}_k which, given two sets of packets Π and Π' in $2^{\mathcal{M}}$, executes one of the following queries:
 - Generate signature: The oracle \mathcal{O}_k returns the signature of Π_i using the algorithm sig and private key k .
 - Generate aggregate signature: The challenger runs the agg algorithm and the oracle \mathcal{O}_k returns an aggregate signature on $\Pi \cup \Pi'$.
3. \mathcal{I} outputs a pair composed of a message X and a signature σ_X . It wins the game if the verification algorithm ver returns 1 for the pair (X, σ_X) and Π was never the input of a signing query during the game. The advantage of the intruder after time t , denoted by $\text{Adv}_{\text{Forg}}(\mathcal{I}, t)$, is defined as the probability of winning the game given his queries as well as the responses of the challenger (given through the oracle).

We prove the security of the SHSS₁ signature scheme against forgery assuming that the Computational Diffie-Hellman (CDH) assumption is valid in G . Given two random g_1 and g_2 in G , and for a random $a \in \mathbb{Z}_q^*$, the CDH assumption states that, for a PPT intruder \mathcal{I} , the following probability is negligible in κ (the security parameter).

$$\text{Adv}_{\text{CDH}}(\mathcal{I}, t) = \Pr \left[\mathcal{A}(g_1, a \cdot g_1, g_2) = a \cdot g_2 : a \xleftarrow{R} \mathbb{Z}_q, g_1, g_2 \xleftarrow{R} G \right], \quad (37)$$

where $\text{Adv}_{\text{CDH}}(\mathcal{I}, t)$ is the advantage of the intruder \mathcal{I} after time t and \xleftarrow{R} stands for the uniform random choice on sets. The complexity of the CDH problem has been studied in [29] and it has been demonstrated to be hard to solve. A (t, ϵ) -CDH group is a group for which $\text{Adv}_{\text{CDH}}(\mathcal{I}, t) \leq \epsilon$ for every PPT adversary running in a time t .

Theorem 8. Unforgeability We assume that G is a (t, ϵ) -CDH group, h is a collision-free hash function, and PRNG is a secure pseudo-random generator. Then, for a PPT intruder \mathcal{I} performing ζ_h hash queries and ζ_s signature queries using the signature scheme SHSS₁ defined in Theorem 5, for all t' and ϵ' such that $\epsilon' \geq e(\zeta_s + 1)\epsilon$ and $t' \leq t - \rho(\zeta_h + \zeta_s)$, we have $\text{Adv}_{\text{Forg}}(\mathcal{I}, t') < \epsilon'$.

Proof. We prove the result of the theorem using a *reductio ad absurdum* reasoning. We suppose that an intruder \mathcal{I} can violate the statement of the theorem by reaching an advantage $\text{Adv}_{\text{Forg}}(\mathcal{I}, t') \geq \epsilon'$ and show that this leads to the existence of an intruder \mathcal{I}' that can reach $\text{Adv}_{\text{CDH}}(\mathcal{I}, t) \geq \epsilon$. Intuitively, \mathcal{I}' relies on the capabilities of \mathcal{I} to forge the signatures generated by the oracle in order to violate the assumption. Since the \mathcal{I} and \mathcal{I}' algorithms are based on coin tosses. The first condition for \mathcal{I}' to succeed is that it does not abort the game before \mathcal{I} . In [34], this probability has been show to be $\frac{1}{e}$ if the probability for the coin to be 0 is $\frac{1}{\zeta_s + 1}$. The other condition is that the intruder \mathcal{I}' is able to identify the value of H for which the signature has been forged by \mathcal{I} . After a time $t' \leq t - \rho(\zeta_h + \zeta_s)$, this probability is $\frac{1}{\zeta_s + 1}$. This shows that \mathcal{I}' can violate the CDH probability with a probability equal to $\frac{\epsilon}{e(\zeta_s + 1)}$, which conflicts with the fact that G is a (t, ϵ) -CDH group. \square

Another desirable feature for our set-homomorphic signature scheme is anti-replay, which consists in preventing the intruder from re-injecting valid signatures that have been generated by the smart things during past sessions.

Corollary 9. Anti-replay We assume that G is a (t, ϵ) -CDH group, h is a collision-free hash function, and PRNG is a secure pseudo-random generator. Then, for a PPT intruder \mathcal{I} performing

ξ_h hash queries and ξ_s signature queries using the signature scheme SHSS₁ defined in Theorem 5, for all t' and ϵ' such that $\epsilon' \geq e(\xi_s + 1)\epsilon$ and $t' \leq t - \rho(\xi_h + \xi_s)$, we have $\mathbf{Adv}_{\text{Rep}}(\mathcal{A}, t') < \epsilon'$.

Proof. The proof directly stems from the unforgeability property. In fact, inserting the sequence numbers in the hashed packets will prevent the attacker from winning the Rep game. The boundaries on $\mathbf{Adv}_{\text{Rep}}(\mathcal{I}, t) \geq \epsilon$ will be identical to those defined in Theorem 8 because the signatures generated for two different packets holding the same information in their payloads are statistically independent. \square

A signature scheme fulfills the privacy property if the generated signatures reveal nothing more than the message being signed. More precisely, for two sets of packets Π_i and Π_j in $2^{\mathcal{M}}$, if σ is a signature on $\Pi_i \cup \Pi_j$, an adversary should not be able to infer from σ any information about Π_i and Π_j which is not in $\Pi_i \cup \Pi_j$. In other terms, a set-homomorphic scheme according to Definition 2 fulfills the privacy property if the following distributions, defined on an oracle \mathcal{O}_{k_i, k_j} , are

$$\begin{aligned} &\{k_i, k_j, \sigma, \sigma' \leftarrow \text{sig}(k_i, \Pi_i), \text{sig}(k_j, \Pi_j), \\ &\text{sig}(k_i - k_j, \Pi_j \cup \Pi_i)\} \\ &\{k_i, k_j, \sigma, \sigma' \leftarrow \text{sig}(k_i, \Pi_i), \text{sig}(k_j, \Pi_j), \\ &\text{sig}(k_i, \Pi_j) \bullet \text{sig}(k_j, \Pi_j)\} \end{aligned} \quad (38)$$

statistically close. This definition is equivalent to those proposed in [13,22]. The fact that these two distributions are statistically close means that the aggregate signature $\text{sig}(k_i \diamond k_j, \Pi_i \cup \Pi_j)$, derived from two valid signatures $\text{sig}(k_i, \Pi_i)$ and $\text{sig}(k_j, \Pi_j)$, is statistically indistinguishable from a new signature on $\Pi_i \cup \Pi_j$ generated using k_i or k_j . The following theorem proves that our set-signature scheme fulfills the privacy requirement. The proof follows from the hardness of the CDH problem in $G \subset E(\mathbb{F}_q)$.

Theorem 10. Privacy *Supposing that h is a collision-free hash function, the signature scheme SHSS₁ defined in Theorem 5 is private.*

Proof. Our scheme is private because the union of the aggregated sets of packets is completely removed from the signature and the message. Supposing the initial sequence numbers for each session are uniformly generated, the application of the hash function h to the concatenation of the packets and their sequence numbers generates a uniformly distributed sequence. Removing random numbers from a uniformly distributed sequence leads to another uniformly distributed sequence. Hence, the aggregate signature does not convey any information about the packets that have been removed during the aggregation process. \square

To evaluate the energy-efficiency of the proposed signature scheme, we compare it to the case where the WBAN gateway computes a new signature for the aggregate set of packets $\Pi_i \cup \Pi_j$. This is referred to as 'Naive Computing' in Figure 2. Nonetheless, as it has been noticed in Section 2, 'Naive Computing' destroys any link between the verifier and the originators of the network flow since only the signature of the WBAN gateway will be used to verify the authenticity of the received traffic. In fact, 'Naive Computing' allows a potentially compromised WBAN gateway to transmit sets of packets to the medical applications as if they were transmitted from the smart things. Therefore, we assess the communication and processing overhead that have to be spent to guarantee the aforementioned security properties.

The following theorem evaluates the processing and communication costs of SHSS₁ compared to NC (Naive Computing). To this purpose, we define the following costs:

- γ_h : cost of computing the hash function h

- $\gamma_{+, \mathbb{Z}_q^*}$: cost of an addition in \mathbb{Z}_q^*
- $\gamma_{\times, \mathbb{Z}_q^*}$: cost of a multiplication in \mathbb{Z}_q^*
- $\gamma_{\text{inv}, \mathbb{Z}_q^*}$: cost of an inversion in \mathbb{Z}_q^*
- $\gamma_{+, E(\mathbb{F}_q^*)}$: cost of an addition in $E(\mathbb{F}_q^*)$
- $\gamma_{\cdot, E(\mathbb{F}_q^*)}$: cost of a scalar multiplication in $E(\mathbb{F}_q^*)$

The alert reader would have noticed that all of these costs relate to the processing overhead. This is because our approach does not add a communication overhead to the normal signature generated using the gen algorithm. This is one of the most important advantages of our signature scheme.

Theorem 11. Energy-efficiency Let Π_i and Π_j be two sets of packets in $2^{\mathcal{M}}$ and $\Pi_i \cup \Pi_j$ the aggregate set of packets. The processing overheads of SHSS₁ and NC satisfy the following equation

$$\gamma_{\text{SHSS}_1} - \gamma_{\text{NC}} = |\Pi_i \cap \Pi_j|(\gamma_h + \gamma_{\times, \mathbb{Z}_q^*}) + 5 \log(q) \gamma_{+, \mathbb{Z}_q^*} + (5 \log(q) + 1) \gamma_{\text{inv}, \mathbb{Z}_q^*} + \gamma_{\cdot, E(\mathbb{F}_q^*)} + \gamma_{+, E(\mathbb{F}_q^*)}, \quad (39)$$

where γ_{SHSS_1} and γ_{NC} are the processing overheads of signing $\Pi_i \cup \Pi_j$ using SHSS₁ and NC, respectively.

Proof. To generate the aggregate signature defined in Theorem 5, the WBAN gateway first computes $H(\Pi_i)$ and $H(\Pi_j)$. The cost of this computation is $(|\Pi_i| + |\Pi_j|)(\gamma_h + \gamma_{\times, \mathbb{Z}_q^*})$. Moreover, two inversions in \mathbb{Z}_q^* are needed to compute $H(\Pi_i)^{-1}$ and $H(\Pi_j)^{-1}$. Then, to compute u' and v' , the WBAN gateway performs two sums and two products in \mathbb{Z}_q^* . For that, the integers u and v of the Bézout's identity are also needed. These integers can be found using the Euclidean algorithm. The maximum number of steps to execute the Euclidean algorithm on two integers in \mathbb{Z}_q^* is $5 \log(q)$ [33]. Each of these steps requires one inversion and one addition in \mathbb{A}_q^* . Consequently, the total number of operations to generate the aggregate signature of SHSS₁ is given by the following expression.

$$\begin{aligned} \gamma_{\text{SHSS}_1} = & |\Pi_i \cup \Pi_j| \gamma_h + (|\Pi_i \cup \Pi_j| + 2) \gamma_{\times, \mathbb{Z}_q^*} + 2 \gamma_{\cdot, E(\mathbb{F}_q^*)} \\ & + (5 \log(q) + 2) \gamma_{\text{inv}, \mathbb{Z}_q^*} + 5 \log(q) \gamma_{+, \mathbb{Z}_q^*} \\ & + 3 \gamma_{+, E(\mathbb{F}_q^*)}. \end{aligned} \quad (40)$$

The 'Naive Computing' approach consists in computing a signature on $\Pi_i \cup \Pi_j$. Using the results of Section 3, the number of operations needed for this computation is expressed as follows.

$$\gamma_{\text{NC}} = |\Pi_i \cup \Pi_j|(\gamma_h + \gamma_{\times, \mathbb{Z}_q^*}) + \gamma_{\text{inv}, \mathbb{Z}_q^*} + \gamma_{\cdot, E(\mathbb{F}_q^*)}. \quad (41)$$

Consequently, subtracting Equation 41 from Equation 40 and using the fact that $|\Pi_i| + |\Pi_j| - |\Pi_i \cup \Pi_j| = |\Pi_i \cap \Pi_j|$, we obtain the proof of the theorem. \square

5. Experimental Study

To evaluate the energy-efficiency of the proposed signature scheme, we implemented a prototype where: (a) the aggregation is done by an O2 smartphone (XDA Comet) and (b) the patient data are transmitted by five T-mote Sky sensors. The ECC scalar multiplication on the sensor node have been implemented using TinyECC 2.0 (2011 release) on TinyOS. TinyECC is a library providing public key cryptography operations in elliptic curve groups. It includes a number of optimization switches that can be flexibly activated based on the context of the application. For the smartphone, these operations have been implemented in Pocket GCC. For the sake of energy-efficiency, we use the SPONGENT hash function introduced in [35].

Table 3. Performance of the set-homomorphic signature scheme at the sensor level.

Curve param.	Execution time (ms)			
	LLP	SPBPM	ECDSA	HA
128	2492	2774	3638	2003
160	2825	3031	4486	2317
192	3925	3855	4558	3629
	Memory consumption (bytes)			
	LLP	SPBPM	ECDSA	HA
128	2671	2913	776	776
160	3009	3631	892	892
192	3917	4028	1008	1008
	Energy consumption (mJ)			
	LLP	SPBPM	ECDSA	HA
128	26	38	23	21
160	35	42	29	27
192	41	46	37	33

First, we analyze the performance of our technique at the sensor node level. To this end, the time, CPU, and energy needed to generate a digital signature are estimated. The proposed scheme is experimentally compared to ECDSA [8] as well as two recently proposed homomorphic digital signature schemes for WSNs [26,27]. The results of the experiments conducted for different ECC parameters are given in Table 3. One of the key findings is that the proposed homomorphic signature technique outperforms the existing schemes in terms of execution time, memory requirement, and consumed power. With respect to storage requirements, our scheme is similar to ECDSA because the public and private keys are generated using the same process.

To evaluate the amount of energy necessary to perform the secure aggregation process at the WBAN level, we consider four experiment scenarios:

1. 10 sensor nodes, 100 packets, 5% of the traffic is dropped due to aggregation
2. 20 sensor nodes, 100 packets, 5% of the traffic is dropped due to aggregation
3. 20 sensor nodes, 100 packets, 10% of the traffic is dropped due to aggregation
4. 30 sensor nodes, 100 packets, 10% of the traffic is dropped due to aggregation

Figure 5 shows that our approach requires much less power to produce aggregate signatures than the LLP and SPBPM schemes. The figure depicts the total energy needed to *compute* the aggregate signature and *transmit* it across the network. ECDSA has not been represented in this figure because the energy consumption is at least 1500mJ, which cannot be depicted at the scale of the graph. We notice that our approach reduces the energy consumption by 30 to 78%, which is an important achievement allowing substantial lifetime extension at the WBAN gateway level. It is also important to notice that the number of source sensor nodes has a more significant impact on the consumed energy than the packet dropping rate.

6. Conclusion

We introduced a novel set-homomorphic aggregate signature scheme for the IoT in eHealth. Our approach allows important energy savings thanks to its compatibility to in-network aggregation. Moreover, it can conceal private patient data without altering the verification process at the final destination. We proved that our signature scheme fulfills important set-homomorphic properties including the support of union and subset operators. We also proved that our set-homomorphic signature scheme is secure against forging, privacy, and replay attacks. From the experiments that were conducted in the frame of this work, we found that, compared to the existing techniques, our implementation reduces the energy consumption by 30% to 78% in the WBAN gateway. It is also noteworthy that the proposed approach can be used in other contexts where constrained devices are deployed and networked. Moreover, a future extension of our scheme to support dynamic

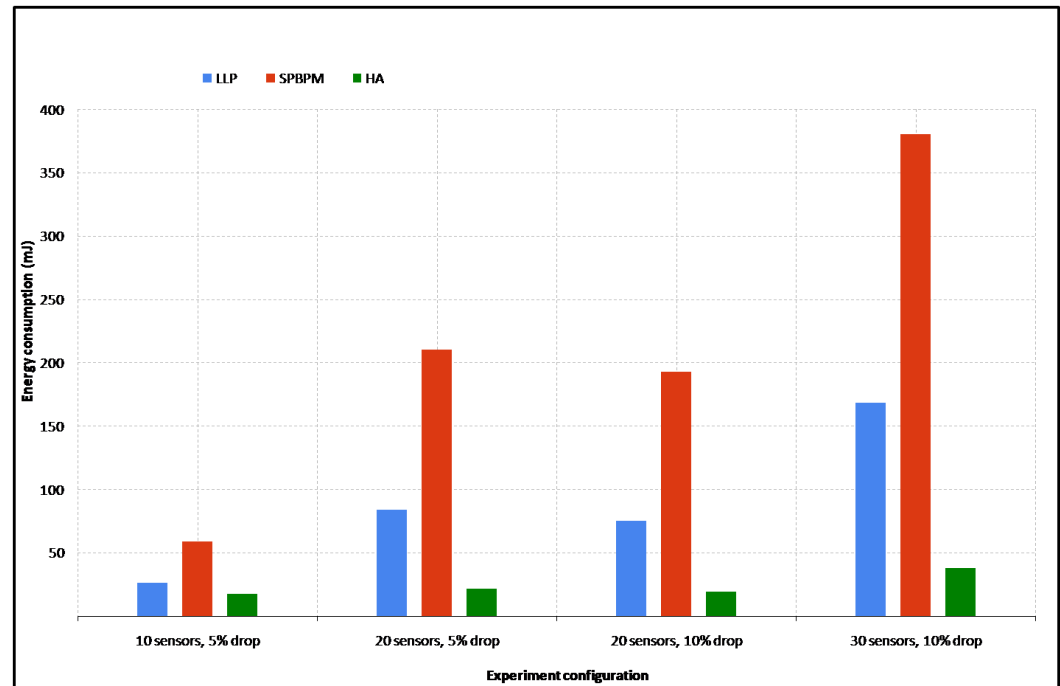


Figure 5. Energy performance at the WBAN level.

context-awareness is worthwhile to be investigated. We posit that the size of the set of packets as well as the size of the keys used to sign the packets can be adapted to the evolution of the dynamic resources available at the smart things and the WBAN gateways.

7. Acknowledgment

The work presented in this paper has been carried out as part of the ASSET research project (grant number: 213131), Adaptive Security for Smart Internet of Things in eHealth, which was funded by the Research Council of Norway from 2012 to 2015.

The authors would like to thank Prof. Adi Shamir (Weizman Institute, Israel), Dr. Sigrid Guergens (Fraunhofer Institute, Germany), Dr. Wolfgang Leister (Norwegian Computing Center, Norway) and Dr. Ijlal Loutfi (Norwegian Computing Center, Norway) for their helpful suggestions, comments and proof-read.

References

1. Y. B. Woldegeorgis, H. Abie, M. Hamdi. A Testbed for Adaptive Security for IoT in eHealth, Proc. ACM ASPI Workshop, Zurich, Switzerland, 2013.
2. X. Sun, R.F. Yu, P. Zhang, W. Xie, and X. Peng. A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks, *Sensors*, Vol. 20, Issue 15, pp. 1-31, 2020.
3. H. Tan, P. Kim, and I. Chung. Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pan-demic Control, *Electronics*, Vol. 9, Issue 10, pp. 1-21, 2020
4. B. Alaya, L. Laouamer and N. Msilini. Homomorphic encryption systems statement: Trends and challenges, *Computer Science Review*, Vol. 36, 100235, 2020.
5. L. Wang, L. Wang, Y. Pan, Z. Zhang, and Y. Yang. Discrete logarithm based additively homomorphic encryption and secure data aggregation, *Elsevier Information Sciences*, Vol. 181, Issue 16, pp. 3308-3322, 2011.
6. C. Castelluccia, A. Chan, E. Meykletun, and G. Tsudik. Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks, *ACM Transactions on Sensor Networks*, Vol. 5, Issue 3, May 2009.
7. Seung-Hoon Lee. Performance Evaluation of Secure Network Coding Using Homomorphic Signature, *IEEE International Symposium on Network Coding*, pp. 1-6, Beijing, 2011.

8. D. Hankerson, A. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography, Springer, ISBN 0-387-95273-X, 2004.
9. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, Proceedings of Eurocrypt 2003, LNCS 2656, pp. 416-432, 2003.
10. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers, Discrete Applied Mathematics, 156(16):3113-3121, 2008.
11. S. Agrawal and D. Boneh. Homomorphic MACs: MAC-Based Integrity for Network Coding, M. Abdalla et al. (Eds.): ACNS 2009, LNCS 5536, pp. 292-305, 2009.
12. Agrawal, S., Kumar, S., Shareef, A., Rangan, C.P. Sanitizable Signatures with Strong Transparency in the Standard Model. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Inscrypt 2009. LNCS, Vol. 6151, pp. 93-107. Springer, Heidelberg, 2010.
13. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, Advances in Cryptology - EUROCRYPT 2003, Vol. 2656 of LNCS, pp. 416-432, Warsaw, Poland, May 4-8, Springer-Verlag, Berlin, Germany, 2003.
14. P. Camacho and A. Hevia. Short Transitive Signatures for Directed Trees. In the Proceedings of Cryptographers Track at the RSA Conference 2012 (CT-RSA 2012), San Francisco, CA, USA, February 27 – March 2, 2012.
15. S. Chari, T. Rabin, and R. Rivest. An efficient signature scheme for route aggregation. Unpublished manuscript, 2002.
16. R. Johnson, D. Molnar, D. X. Song, and D. Wagner. Homomorphic signature schemes. In Bart Preneel, editor, Topics in Cryptology - CT-RSA 2002, Vol. 2271, pp. 244-262, LNCS, San Jose, CA, USA, February 18-22, 2002. Springer-Verlag, Berlin, Germany.
17. S. Micali, K. Ohta, and L. Reyzin. Accountables-subgroup multisignatures (extended abstract). In Proceedings of CCS 2001, pp. 245-54. ACM Press, 2001.
18. S. Micali and R. L. Rivest. Transitive signature schemes. In Bart Preneel, editor, Topics in Cryptology - CT-RSA 2002, LNCS, Vol. 2271, pp. 236-243, San Jose, CA, USA, February 18-22, 2002. Springer-Verlag, Berlin, Germany
19. K. Samelin, H. C. Pohls, A. Bilzhause, J. Posegga, and H. D. Meer. Redactable Signatures for Independent Removal of Structure and Content (Extended), In Proc. of the 8th Int'l Conf. on Information Security Practice and Experience (ISPEC 2012), Vol. 7232 LNCS, Springer-Verlag, 2012.
20. G. Ateniese, D. Chou, B. Medeiros, G. Tsudik. Sanitizable signatures. In ESORICS, pp. 159-177, 2005.
21. A. Hevia and D. Micciancio. The provable security of graph-based onetime signatures and extensions to algebraic signature schemes. In Yuliang Zheng, editor, Advances in Cryptology - ASIACRYPT 2002, Vol. 2501 LNCS, pp. 379-396, Queenstown, New Zealand, December 1-5, 2002.
22. D. Boneh and D.M. Freeman. Homomorphic Signatures for Polynomial Functions, Advances in Cryptology, EUROCRYPT'11, Springer LNCS 6632, pp. 149-168, 2011.
23. S. Canard, A. Jambert, and R. Lescuyer. Sanitizable Signatures with Several Signers and Sanitizers, Progress in Cryptology - AFRICACRYPT 2012, LNCS Vol. 7374, pp. 35-52, 2012.
24. G. Neven. A simple transitive signature scheme for directed trees, Theoretical Computer Science, 396:277-282, 2008.
25. A. Bagherzandi and S. Jarecki. Identity-Based Aggregate and Multi-Signature Schemes Based on RSA, Public Key Cryptography, LNCS 6056:480-498, 2010.
26. S. Lim, E. Lee, and C-M. Park. A Short Redactable Signature Scheme Using Pairing, Security and Communication Networks, 5(6):523-534, 2012.
27. K. Samelin, H. C. Pohls, A. Bilzhause, J. Posegga, H. de Meer. Redactable Signatures for Independent Removal of Structure and Content, Information Security Practice and Experience, LNCS, 7232:17-33, 2012.
28. V. Shoup. A Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2012.
29. D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing, Proceedings of AsiaCrypt, LNCS, 2248:514-532, 2001.
30. S. Haber, Y. Hatano, Y. Honda, W. Horne, K. Miyazaki, T. Sander, S. Tezokuy, and D. Yao. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification," Proc. ASIACCS, pp. 353-362, Japan, 2008.
31. L. Sweeny. Achieving k -Anonymity Privacy Protection Using Generalization and Suppression, Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, Issue 5, pp. 571-588, 2002.

32. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen message attacks, *SIAM Journal of Computing*, Vol. 17, Issue 2, pp. 281-308, 1988.
33. R.A. Mollin. *Fundamental Number Theory with Applications*, 2nd Edition, Boca Raton: Chapman & Hall/CRC, 2008.
34. J. H. Ahn, D. Boneh, J. Camenish, S. Hohenbeger, A. Shelat, and B. Waters. Computing on Authenticated Data, 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012.
35. A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede. Spongnet: A Lightweight Hash Function, *Proc. CHES*, pp. 312-325, Japan, 2011.
36. S. Krenn, K. Samelin, and D. Sommer. Stronger security for sanitizable signatures. In *Data Privacy Management, and Security Assurance*, LNCS series, Springer, Cham, Vol. 9481, pp. 100-117, 2015.
37. N. Kaaniche, E. Jung, and A. Gehani. Efficiently validating aggregated IoT data integrity, *IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*, pp. 260-265, 2018.
38. M. Chamekh, M. Hamdi, and S. E. Asmi. A new architecture for supply-chain management, 14th *IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 77-82, 2017.
39. R. Kojima, D. Yamamoto, T. Shimoyama, K. Yasaki, and K. Nimura. A New Schnorr Multi-Signatures to Support Both Multiple Messages Signing and Key Aggregation, *Journal of Information Processing*, Vol. 29, pp. 525-536, 2021
40. D. Derler, H. C. Pöhls, K. Samelin, and D. Slamanig. A general framework for redactable signatures and new constructions, *Information Security and Cryptology (ICISC)*, Vol.9558, pp. 3-15, Springer, Cham, 2015
41. J. Liu, J. Ma, Y. Xiang, W. Zhou, and X. Huang. Authenticated medical documents releasing with privacy protection and release control, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, pp. 448-459, 2021
42. J. Kar, X. Liu, and F. Li. An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks, *Journal of Information Security and Applications*, Vol. 61, pp. 1-14, 2021.