A Comprehensive Survey on ID-Based Cryptography for Wireless Sensor Networks

Constantin GRUMĂZESCU and Victor-Valeriu PATRICIU

Abstract—**Wireless Sensor Networks (WSN) are considered to be the eyes and ears of the Internet of Things (IoT). Whereas sensor boards are becoming cheaper and a lot more diverse, WSN and IoT applications are on a steady upward trend. This leads to an increasing need to ensure the security of data collected and transmitted by these types of applications and networks. Because sensor nodes are still relatively simple, highly constrained devices, security becomes very difficult to implement. While lightweight cryptographic algorithms are still under close supervision by NIST, identity based cryptography (IBC) holds its ground as a viable security approach for WSN based applications. In this paper we are presenting a thorough analysis on identity based cryptographic primitives, techniques, implementation variants and issues. Throughout the paper we are discussing all of these aspects in relation to the specificity of WSN based network infrastructures and applications.**

Index Terms—**distributed, encryption, escrow, hierarchical, identity, revocation, sensor, signature.**

I. Introduction

Network security, in general, has greatly benefited from public key cryptography. The reason why this is not an omnipresent solution is that the Public Key Infrastructure (PKI) itself is relatively difficult to implement and maintain. In order to secure a communication, two users of the same cryptosystem must generate key pairs (for encryption/decryption and/or signing/verification), submit requests in order to receive signed security certificates from a Certificate Authority (CA) which can finally be used to authenticate one another and exchange confidential information.

IBC is a relatively old type of cryptography where, similar to a PKI, data sent over an untrusted channel is secured and authenticated by using a public/private key pair that is centrally managed, for each user in the system, by a third party – the private key generator.

The name itself reveals the great advantage that this cryptographic technique brings – the simplicity of the encryption/signing process is achieved by using the user's identity as his public key.

The efficiency of this concept applied in current applications, the success and maturity that ID-based solutions have reached are proven by the large number of scientific publications, IEEE and IETF working groups dedicated efforts as well as by the published RFCs and fully adopted industry implementations.

For certain applications, some characteristics of ID-based cryptosystems make them highly attractive: central management, ease of use, low overhead, computation requirements and relatively low communications effort. All of these features lead to the idea that this type of cryptosystem is ideal in a network where there is a strong, secure central point that takes the computational burden off of user's side, manages to ensure a secure environment in a fast and simple manner. There isn't a more suitable example of such a network than a WSN.

The purpose of this article is to present a comprehensive survey on IBC, primitives and its applications. The paper is organized as follows. Section II reveals the key characteristics of WSNs, features that make them a perfect candidate for developing ID-based techniques. Section III shows the mathematical tools that IBC is based on and basic operational primitives. Section IV captures some interesting features of IBC. Section V deals with the basic implementation issues and Section VI is a short review of the security assumptions and certainties that IBC are based upon. Section VII is a comparative study between IBC and the classical PKI system. Section VIII is reserved to implementations in terms of algorithms, standards and workgroups, real world applications and WSN specific constructs.

II. WSN – Security and Constraints

WSNs have emerged as a special case of ad-hoc networks. They are composed of a large number of small computing devices, very low processing and wireless communication capabilities and extremely reduced power resources. They are fitted with tiny diverse sensors and are collaborating in order to achieve a wide selection of specific objectives.

WSNs are technical systems consisting of a large number of small computing devices equipped with sensing elements, limited communication, processing capabilities and energy resources, collaborating to achieve specific goals.

Initially, WSN networks developers have tried to solve problems related to limited processing power, battery life and data transmission through adequate protocols and, with the irreversible trend of infiltration in the sphere of industrial applications, aspects regarding the security of data transmissions have occurred.

Current software (symmetric / asymmetric encryption / decryption) and hardware (dedicated components) solutions for data security assurance are resource intensive and especially require high processing power.

This work was supported by a grant of the Romanian Ministry of Research and Innovation, CCCDI – UEFISCDI, project number PN-III-P1-1.2-PCCDI-2017-0272 / Avant-garde Technology Hub for Advanced Security (ATLAS), within PNCDI III.

C. Grumăzescu is with the Cyber Security Advanced Technologies Centre of Excelence, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: cgrumazescu@mta.ro).

Victor-Valeriu Patriciu is with the Doctoral School for Defense and Security Systems Engineering, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: vip@mta.ro).

Digital Object Identifier 10.32754/JMT.2018.1.10

Some of the most important characteristics of WSN nodes and infrastructures are mobility, flexibility, small size, large deployment areas, large number of nodes, minimal planning and maintenance effort, low power consumption, limited lifespan and reduced costs.

When it comes to security, network owners must consider three main aspects of WSN. First, the amount of overhead necessary for communication security should be proportional to the size of usual messages. In order to preserve power, one should reduce transmissions to a minimum. Second, in order to minimize deployment costs, security features must be implemented using as few software/hardware resources as possible. Third, cryptographic keys distribution should be carried out in such way not to risk their disclosure.

In order to prolong battery life, one should also regard: distributing computational costs among sensor nodes, deployment of mobile agents for data collecting and processing, development of new and efficient communication protocols, efficient operating systems and, last but not least, simpler cryptographic algorithms with an acceptable level of security.

PKI based methods are computationally expensive, even if there is an elliptic curve implementation. Also, symmetric key algorithms should be carefully selected so that they wouldn't become a burden for the common network node. Due to the fact that available memory is scarce, having a key for every other neighbor is not a viable solution.

III. Identity Based Cryptography

IBC has achieved a considerable number of implementation solutions developed by using a variety of very different mathematical "hard-to-crack" problems. Thus, Weil pairings are the starting point for the work of Boneh, Boyen, Franklin or Waters [2],[11],[13],[32]. First Cocks [3] and then Boneh, Gentry and Hamburg [33] based their proposed schemes security on the quadratic residues. Finally, Gentry, Peikert and Vaikuntanathan [34-35] have had a completely different approach by using lattices.

But the true pioneer of IBC, Adi Shamir, hasn't benefited from either, thus not being able to complete his work [1]. Starting with the idea of simplifying security measures for email systems, in 1984 Adi Shamir proposed the concept of the very first cryptosystem and signature scheme based on the identity of a user (e.g. name, email, location, etc.).

Shamir's scheme intended for users to communicate in a secure fashion over a public channel without having to exchange public/private keys and, for that, it assumed the existence of a trusted third party – the key generation center or Private Key Generator (PKG). Both encryption/decryption and signing/verification of messages would have been possible in a 4 stage process:

1) setup – the PKG generates its own global system (public) parameters and master (private) key (M_{Key}) based on a security parameter *k*; the parameters set also contains a message and a ciphertext space;

2) extract (smart card deployment) – the PKG calculates (based on its M_{Key}) and hands over, in a secure fashion (additional public/private key pair), the private keys for each user joining the network;

3) encryption / signing – sender signs with his private key and encrypts with the recipient's ID and public parameters;

4) decryption/verification – recipient decrypts with his private key and public parameters and verifies with senders ID.

The whole scheme assumes, as a final request, that the extraction stage is being carried out only if the user requesting a private key has authenticated himself to the PKG, in order to avoid a private key disclosure. The transportation of the private key must also be done via a secure channel.

A. Identity Based Encryption (IBE)

Although a great accomplishment regarding the signature scheme, Shamir's concept lacks in implementation when it comes to the encryption primitive. After years of having it as an open problem, in 2001, Boneh and Franklin's [2] famous Weil pairing on elliptic curves over finite fields based scheme (BF scheme) or Cocks's [3] quadratic residue scheme finally proved that such implementations for the so longed ID-based cryptosystem are possible.

As well as Cocks's proposal [3], both schemes in [2] - *BasicIdent* and *FullIdent* – are developed in a Shamir-similar 4 stage process.

In the first stage, the *setup*, the PKG establishes two public groups of order *q* ($q > 3$, prime factor of $p+1$, prime $p \equiv 2 \bmod 3$) - $\mathbb{G}_1$ (generated by *P*, a point of order *q* on an elliptic curve *E* over $\mathbb{F}_p$) and $\mathbb{G}_2$ (over $\mathbb{G}\mathbb{F}^*_{p^2}$). $\mathbb{G}_2$ is generated by the existence of the bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, with $\mathbb{G}_1$ additive group and $\mathbb{G}_2$ multiplicative, and *q* depending on a security parameter *k*. Then, a random $K_M \in \mathbb{Z}_q^*$ is chosen as the (private) master key and the public $K_{Pub} = K_M P$ is generated. After the two random oracle model hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$ and $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ are chosen and the two spaces – $\mathcal{M} = \{0,1\}^n$ for plaintext and $C = \mathbb{G}_1^* \times \{0,1\}^n$ for ciphertext - the entire set of system parameters $\left(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, K_{Pub}, H_1, H_2\right)$ are made available for all its users.

Any user of this system can execute the *extract* stage through a secure non-ID-based link, by sending his own $ID \in \{0,1\}^*$ to the PKG and gets, in return, his private key $d_{ID} = K_M Q_{ID}$, where $Q_{ID} = H_1(ID)$ (Q_{ID} can be computed by any of the system's users).

The last 2 stages are different in the two variants of the scheme due to a desired countermeasure against chosen ciphertext attacks [2]. The FullIdent requires an additional parameter $\sigma \in \{0,1\}^n$ and two more hashes – $H_3 : \{0,1\}^n \times \{0,1\}^n \in \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ - set and published by the PKG in the initial stage of the scheme.

In order to *encrypt* a message $m \in \mathcal{M}$, the sender must compute the recipient's public key $Q_{ID} = H_1(ID)$, then:

- choose a random $r \in \mathbb{Z}_q^*$ and compute and send the ciphertext $c = (U, V) \in C$, $c = \left(rP, m \oplus H_2\left(g_{ID}^r\right)\right)$, $g_{ID} = \hat{e}\left(Q_{ID}, K_{Pub}\right) \in \mathbb{G}_2^*$ in the BasicIdent variant;

- choose a random $\sigma \in \{0,1\}^n$, set $r = H_3(\sigma, m)$ then compute and send the ciphertext $c = (U, V, W) \in C$, $c = \left(rP, \sigma \oplus H_2\left(g_{ID}^{r}\right), m \oplus H_4(\sigma)\right)$, $g_{ID} = \hat{e}(Q_{ID}, K_{Pub}) \in \mathbb{G}_2$ in FullIdent mode.

For the recipient to be able to decrypt the ciphertext *c*, he must compute:

- $V \oplus H_2\left(\hat{e}(d_{ID}, U)\right) = m$ in BasicIdent

or

- $W \oplus H_4\left(V \oplus H_2\left(\hat{e}(d_{ID}, U)\right)\right) = m$ in FullIdent.

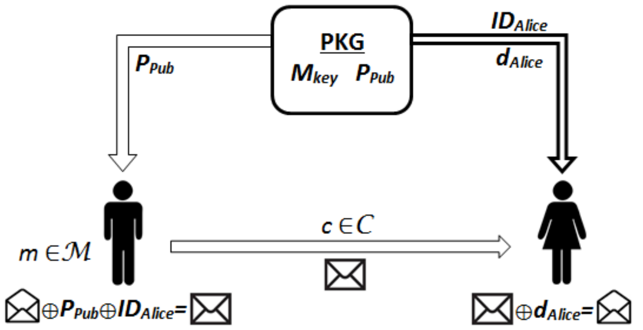

Figure 1. Identity Based Encryption operation

Whereas BasicIdent has the advantage of smaller computations (g is the same for every message sent to a certain user), Fullident is actually proven, at the cost of extensive additional computations, chosen ciphertext secure.

Cocks [3] came up with a different scheme that didn't rely on bilinear pairing but on the hard problem of composite quadratic residues. As it has been proven slightly harder to implement because of the bit-by-bit computationally demanding encryption/decryption process, Cocks's scheme has one very important drawback – it produces long ciphertext. This is definitely undesirable as communication overhead becomes more and more important in today's applications. Security-wise, it's been known as vulnerable to chosen ciphertext attacks. Anyway, its use can be found in a situation where small pieces of information need to be transmitted over the network, like the exchange for session keys.

Regarding Cocks's scheme applicability in the field of WSN we can easily dismiss this just by considering the fact that the sensor's hardware component draining most (around 70-80% for a Mica2 mote [43]) of its battery life is the transceiver unit and thus, communication overhead significantly affects energy consumption.

After some slight variations of these proposals, it was Waters's [32] efficient IBE scheme that was proven to be fully secure in the standard model – no random oracles – under the computational Diffie-Hellman assumption. Based on the Boneh-Boyen [13] construction, Waters also managed to turn it into a signature scheme and propose it as a Hierarchical IBE system for small number of hierarchy levels.

The drawback of this IBE system proposal [32] – the large size of the public parameters set – was solved by Nacache in [38], when he introduced a variant of Waters's scheme with a significantly shorter public key (only a few kB). In order to accomplish this, Nacache reduces the size of the public parameter set by a factor *l*. Hence, the security of the IBE system is reduced by the same factor. This means that the system designer must decide if the parameter size is worth the security risk.

In the context of WSN, the size of the public parameters set is relevant due to the fact that it will occupy a fraction of the already limited available memory. Thus, an equilibrium must be determined between the size of the parameters set and the accepted level of security for a certain deployed network and running application.

The advantages that IBC brings to a WSN based application are quite obvious. The existence of a high capabilities central point – the PKG – fits perfectly into the structure of a WSN, where, in general, there is a sink that gathers and processes data. The sink is the perfect candidate for the actual node to do all the private key generation and distribution operations.

Another important aspect is the fact that the cryptographic operations and the communication overhead that the users of the system – the WSN nodes - must carry out are a lot lighter than with traditional public key cryptosystems. And this could mean only one thing – common nodes can have limited resources (processing capabilities, memory and power).

The reason we have chosen to present the BF scheme [2] in detail is that it has been the foundation for most of the ID-based encryption and key management schemes developed over the years and also became a standard under IEEE. Not only that Boneh and Franklin managed to overcome Shamir's scheme shortcomings, but they have also envisioned several interesting features of IBC based on their solution.

In the following sections, we will present and discus these features with respect to all those special characteristics and constraints of WSNs.

B. *Identity Based Signatures (IBS)*

As authors in [2] stated, any valid asymmetric encryption scheme can be immediately turned into a public key signature scheme, and IBE is no different from that.

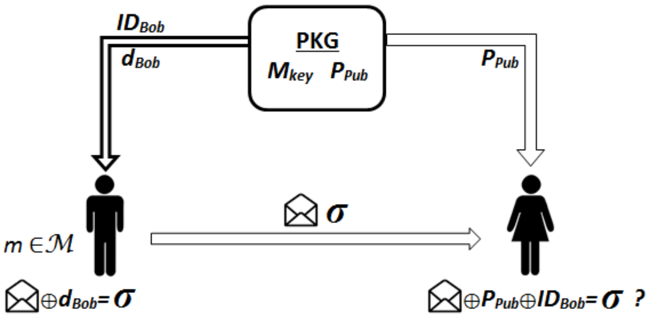

Figure 2. Identity Based Signatures operation

In IBS [2],[12], the first two stages are the same as in the IBE mode:

- the PKG sets up the master key and public parameters;

- the signer of a message first extracts his private key associated with his identity from the PKG;
- next, the sender uses his private key to sign the message and sends it along with the matching signature;
- upon arrival, the recipient verifies the message's authenticity by using the message, the signature, the sender's identity and the PKG public parameters.

The signing and verification operations are somewhat different from one scheme variant to another, but the principle is just as like ([2][11-12][17][24]). We can easily notice that the signing key used by the sender is the IBE corresponding encryption key and the key needed by the recipient for the verification process is nothing else but the sender's identity.

Zhang and Kim proposed an ID-based blind signature scheme and a ring signature scheme in [21]. Both schemes are using bilinear pairings and are based on the work of Chaum in [22] and Rivest-Schaum-Tauman in [23].

Starting from [2], Boneh et al. developed a series of signature schemes leading either to very short signatures [24] - the BLS scheme (154 bits vs. 320-bit DSA) or to faster and more secure ones [11]. Zhang et al. [25] on the other hand proposed a new short signature scheme from bilinear pairings that uses general cryptographic functions and requires less pairing operations than the BLS scheme. The number of required pairing operations is very important due to the fact that these are the most time-consuming operations.

The BLS scheme also influenced [11] where the authors constructed an efficient aggregate signature scheme for reducing the size of certificate chains and message size by using signature aggregation, with significant applicability potential in secure routing protocols.

The ones that finally rounded up Boneh and Franklin's work were Cha and Cheon [36]. They proposed an IBS scheme that shares system wide public parameters with B. and F.'s IBE scheme, using gap Diffie-Hellman groups obtained from bilinear pairings. The four stage scheme is similar to the B. and F. proposal:

- *setup* – choose a generator P of group $\mathbb{G}$ of prime order l, choose a random $K_M \in \mathbb{Z}/l$ as the master key, set $K_{Pub} = K_M P$ and publish the system parameters set (P, K_{Pub}, H_1, H_2), where $H_1 : \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}/l$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$ are two cryptographic hash functions in the random oracle model;
- *extract* – based on a user's *ID*, the PKG computes and transmits to him $d_{ID} = K_M Q_{ID}$, where $Q_{ID} = H_2(ID)$;
- *sign* – based on a message *m* and secret key d_{ID}, choose a random $r \in \mathbb{Z}/l$ and compute the signature $\sigma = (U, V)$, where $U = rQ_{ID}$, $V = (r+h)d_{ID}$ and $h = H_1(m, U)$;
- *verify* – check if $(P,\ K_{Pub},\ U + hQ_{ID},\ V)$ is a valid Diffie-Hellman tuple.

Efficiency-wise, this scheme is quite similar to its complement – the B. and F.'s IBE [2], and it is proven to be secure against existential forgery on adaptively chosen message and ID attacks in the random oracle model.

Combining [36] and [2], we get a complete identity based PKI solution which, when putting aside the random oracle, can be a feasible alternative to a traditional certificate-based PKI.

It was Paterson et al. [37] who finally proposed a fully functional IBS scheme proven to be secure in the standard model. Their work was based on the hardness of the Computational Diffie-Hellman problem (CDH) addressed in [16] and [18] and was inspired by Waters's [32] and Nacache's [38] standard model IBE schemes and by Gentry's [20] observation on the relation between IBE and IBS schemes with focus on hierarchical ones.

While Paterson's scheme produced short signatures, it was also considered computationally efficient, and this is because the signature was composed of 3 group elements, one of which would remain the same for all signatures made by a given user. Also, the signing process is pairing free and verification stage needs 3 pairing operations. The only problem behind this was the relatively large size of the public parameters which, as the authors claim could be reduced with some security costs.

Paterson and Schuldt [37] made a deepened analysis of tradeoffs between keys, signatures and public parameters size, computational effort and proven security of their proposal.

These are key elements when it comes to WSNs. Because of their nodes limited resources, a major objective becomes the key size. Also, a large size parameter set could involve the use of a large area of a node's physical memory. The produced signature size is also very important and not just because it implies more computation, but because it means more overhead and, thus, higher energy requirements. It solely depends on the developer of a WSN based application to decide how much security can be sacrificed in the favor of efficiency.

We notice that, as well as IBE, IBS schemes seem to fit naturally into the world of WSNs. Simplicity of the algorithm, low computation requirements, reduced key and signature size, it all comes together very naturally.

IV. IBC VARIATIONS

A. *Levels of access and delegation*

Boneh and Franklin [2] first suggested their scheme as a way to implement a multi-level user credential system, by generating private keys based on a level of clearance for the user which would be mentioned as part of the public identity (e.g. John-secret).

This could be useful both in civilian (corporate employees) and military specific applications (communications officers), where workstations (nodes) can receive and "read" messages based on the user's clearance on that type of message. Only a subset of messages could be opened with one key.

In WSN application this could be useful for the addition of an extra layer of security. If there were two types of nodes – data harvesting and routing nodes – available in the network, information would be easily received and/or forwarded by any of them, but routing nodes could be prevented from "reading" the actual data.

Taking things to an upper layer and thinking of onboard running applications, if one multiple nodes run applications owned by multiple users, it may be necessary for them to ensure data confidentiality and there is one way to do it.

B. *Distributed Key Generator*

Another interesting feature presented in [2] as a viable variant, fully addressed in papers like [8-10], is the existence of a Distributed Key Generator using threshold cryptography techniques (i.e. a subset of *t-out-of-n* servers can generate a user's private key without the knowing, storing or computing the system "virtual" *master-key*). A successful attack on such a system would imply compromising a number of *t* key-generation servers, which, for an adequate value of $t > n/2$ would be very difficult to achieve. In B. and F.'s vision, a dishonest (forged) server could be easily detected by simply computing two pairings using one's private key, public parameters, a public key and its corresponding identity

$$\hat{e}\left(d_{ID}^2, P\right) = \hat{e}\left(Q_{ID}, K_{Pub}^2\right), \tag{1}$$

where

$$d_{ID}^2 = K_M^2 Q_{ID}, \tag{2}$$

$$K_{Pub}^2 = K_M^2 P, \tag{3}$$

and K_M^2 is part of the master-key K_M.

Some applications that use IBC may very well benefit from this concept, as it brings up a significantly important aspect of the entire security system – failure points. Specifically, a private key generator's availability distributed across many nodes significantly increases the system's overall level of security due to the fact that a single point of failure is no longer the case.

More than that, in order for the entire cryptographic system to be compromised, an attacker would need to successfully attack a minimum of *t* nodes, which makes their attempts a lot more difficult.

When considering WSNs, we realize that the level of security that this type of cryptographic technique has to offer would suit just fine. Having a distributed PKG implies that nodes would have to authenticate and ask for segments of their private key to multiple servers. Even if it is a very powerful security wise approach, in terms of efficiency things are not the same. Having to connect to more than one key servers means that a node would have to work with a lot more traffic, which evidently translates into additional power consumption.

We realize that this could be a solution if and only if the WSN administrator holds information security as the first criteria in running the topology.

Still having B.'s and F.'s [2] concept in mind, issues like synchronized communication, anonymity, possible types of bilinear pairings, security against chosen ciphertext attacks in the random oracle model, all relating to this viable component of IBC have been the subject of many research papers [39-42].

C. *Hierarchical ID-based Systems (HIDS)*

One of the major issues classical PKIs had to face has been the large number of users that had to be serviced at one point. A single, central CA couldn't have been the solution for a worldwide available system. Thus, in the hierarchical PKI model, a handful of root CAs can delegate certificate issuing to multiple intermediate CAs with varying validation requirements.

In the context of IBC, in a flat/single level (single PKG) system, operations executed by the PKG (private key generation, identity verifications, secure channel establishment) would be burdensome for a large number of system users, causing delay in servicing requests, even though certificate validation is no longer the case. Not to mention that once a unique PKG becomes unavailable (after an attack, a failure or exhaustion of the power supply), the entire system would be compromised, existent users not being able to obtain new keys nor new users to join the system.

When applying a flat IBC scheme to a WSN, the PKG could risk power supply depletion for a significant number of nodes. Taking into account the fact that most WSN based applications imply a large number (hundreds, thousands) of sensor nodes (evolution towards IoT), the concept of a Hierachical IDentity-based System fits perfectly, with respect to certain application-specific, physical and security, requirements.

In a HIDS, where a root PKG delegates authority, each subordinated PKG will have an allocated subdomain with a limited number of users and its own subdomain master (private) key. Each user's or subordinated PKG's identity is a tuple of current node's (user or PKG) distinct identity and superior nodes identities. In such a system, the first stage of the cryptographic scheme – the setup, is divided into two phases – setup for the root PKG and setup for the lower levels subordinated PKGs.

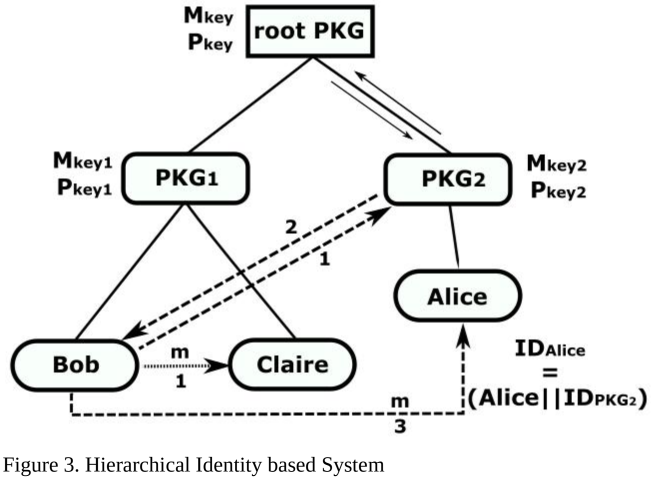

Figure 3. Hierarchical Identity based System

If a user (Bob) wants to transmit a secure message to another (Alice), in order to achieve encryption, Bob will have to obtain the set of public parameters from the subordinated PKG that handles the subdomain which includes Alice. If Bob and Alice belong to the same subdomain, then the communication is limited to that subdomain.

This approach is, clearly, a major benefit for network infrastructures with many nodes that have limited resources as it would certainly reduce network traffic due to distribution of private keys and transmission of the public parameters set. Plus, damage control (limitation of unwanted events) is ensured by the fact that if a subdomain master key is compromised, other subdomains are still secure [31].

We can also imagine a WSN scenario where, after all network nodes that need to securely communicate have their private keys and public parameters sets from respective subordinated PKGs, the root PKG (or higher levels PKGs) may well go offline, in order to save energy or simply to keep them hidden from malicious parties, making them safer from potential attacks.

Boneh and Franklin [2] have also been the first to suggest a cryptographic scheme on more than one level where, an employee that wants an exclusive set of private sub-keys for a short period of time (e.g. a set of ephemeral keys for mobile devices) can generate that for himself based on his private "master" key. There are two reasons for this approach: one – if one of the ephemeral sub-keys is compromised the limited validity would limit prejudice due to the potential security breach; two – if one of the employee's private sub-keys is compromised for one of his mobile devices, other sub-keys could still be used for other devices due to the fact that the sub-keys are generated separately based on the device's identity.

Horwitz and Lynn [31] were the first to propose a practical 2 levels Hierachical Id-Based Encryption (HIBE) scheme, where the root (1st level) PKG delegates key extraction tasks to 2nd level PKGs. This is somewhat similar to a standard Public Key Infrastructure where the root CA is the IBE Master (root) PKG, and is proven secure under the BDH assumption in the random oracle model.

The open problem that remained was the security of the entire system, in the upper as well as in the lower levels, regarding collusion.

Gentry and Silverberg [20] proposed two extension schemes of the B&F [2] principle - Basic HIDE and, one that is CCA secure in the random oracle model, the Full HIDE. Most importantly, based on the same BDH assumption, the schemes are fully scalable and secure regardless of the numbers of levels in the hierarchy.

In the context of proactive system security, where there is the problem of gradual key exposure (the secret key is assumed to be gradually compromised over time), Dodis and Yung [54] showed that G&S's extension [20] brings another big advantage towards security – the natural secret key representation for the HIBE admits a simple and efficient refresh operation, which offers very high level of exposure-resilience, while incurring absolutely no space or time losses for decryption – the above possibility of having a secret refresh from time to time or even from one extraction operation to another.

Another important characteristic present in [20] is the fact that the two schemes are fully secure to collusion attacks (a number of users can collude in order to find out the master secret and then masquerade as the PKG), both in the upper and in the lower layers.

In certain applications where message size and decryption complexity are important due to the fact that they are influencing power consumption, as it is in WSN, a scheme like the ones in [20] is useful because the generated ciphertexts length and the decryption complexity grow at the same rate, having the message recipient level as the constant scale factor. Since most of the energy a mote consumes in a lifecycle goes to the transceiver unit, then every bit of transmitted data (ciphertext) that can be spared translates into energy saving.

For example, if Alice sends messages to the other participants (Bob and Carol), it would take about 30% more time for Carol to decrypt the message than Bob and the ciphertext would be about 30% longer.

Considering the fact that the size of the ciphertext grows linearly with the difference of levels between two nodes, we can conclude that the available fully functional HIDE schemes would not scale well for WSN for to many levels in the hierarchy.

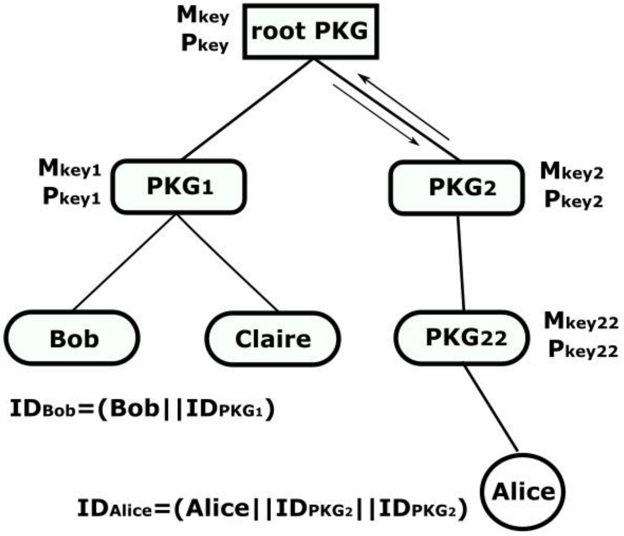

Figure 4. HIDS operational complexity due to infrastructure levels

Based on the Sakai, Ohgishi and Kasahara's concept of a pairing cryptosystem with a dual identity based key sharing scheme which later materialized in [53], Gentry and Silverberg [20] came up with a Dual-HIDE solution. In a pairing based system where the PKG has a secret *s*, the generated private keys for 2 users *Alice* and *Bob* are sP_{Alice} and sP_{Bob} ($P_i = H_1(ID_i)$). It is noticeable that the 2 users now have a shared secret:

$$\hat{e}(sP_{Alice}, P_{Bob}) = \hat{e}(P_{Alice}, P_{Bob})^s = \hat{e}(P_{Alice}, sP_{Bob}) \quad (4)$$

This secret can now easily become a shared symmetric encryption key which can be used to secure their communication.

Gentry and Silverberg showed that the true advantage of this technique comes when put into practice into a hierarchical scheme – the dual-HIDE, and this is because in some situations it can lead to a shorter ciphertext. Also, this scheme reduces the number of pairing operations that must be conducted by the two parties involved in the communication process, which, for some applications like wireless sensor networks is a very important advantage, as pairing operations are some of the most computationally expensive operations conducted by a node. This would lead to significant savings in battery life. Here, there is another important advantage – the common key can be used for the entire domain and it generates a type of domain-limited secure broadcast. Parties above the common PKG of the two users can't decrypt ciphertexts using the common key.

In [15], Boneh, Boyen and Goh proposed a completely different algorithm where the ciphertexts consist of three group elements and decryption only requires computing two bilinear maps, both being independent of the hierarchy depth. For this, the system must be provided with a large parameter set (which can definitely become a major issue if available memory is scarce) and a vector of identities of size *k* for a hierarchy of depth *k* and produces constant size ciphertexts with limited delegation (the private key decreases in size as the depth of the hierarchy grows). This solution can have several applications like efficient forward secure encryption and an efficient mechanism for encrypting to the future.

In [55], Au et al. proposed a somewhat similar scheme which was proven by the authors to be the strongest security model without random oracles. The ciphertexts are of constant size and the parameter set is independent of the depth of the hierarchy but, is relatively large in size.

Based on [15], in [56], Zhang et al., proposed a new scheme that produces constant size ciphertexts and constant size private keys, which eliminates the limiting of delegation.

Even though it is not clear if Identity Based Signatures have an advantage over traditional PKI-based signatures schemes, the authors proposed a fully functional Hierarchical Identity Based Signature Scheme (HIDSS) based on the difficulty of solving the Diffie-Hellman problem, considering that this variant would be much more attractive coming with the corresponding HIDE as a whole package – HIDE & HIDSS cryptosystem.

As it can be seen, much of the research effort in this direction is focused on getting the best performance (number of computationally intensive operations, small public parameter set, small private keys, small ciphertexts) considering a hierarchy of network nodes with respect to the number of levels in the hierarchy.

D. Online/Offline processing

Another interesting characteristic of IBC is the possibility of separating the encryption process into two phases – online and offline encryption. Thus, part of the necessary computing may take place without knowing the message and some even before knowing the recipient's identity.

Going back to B. and F.'s BasicIdent [2], we can easily notice that g ($g_{ID} = \hat{e}\left(Q_{ID}, K_{Pub}\right)$) is message independent and so, it must be computed only for the first plaintext (message); it is still dependent on the recipient's identity. In order to encrypt the message $m \in \mathcal{M}$, the sender must also compute and send $c = \left(rP, m \oplus H_2\left(g_{ID}^{r}\right)\right)$. This means that once r and $H_2\left(g_{ID}{}^{r}\right)$ are pre-computed, it takes very little time to get and send the actual ciphertext.

It was Even, Goldreich and Micali [47] that first launched the idea of an on-line/off-line digital signatures scheme designated for electronic wallets and smart cards. Later on, Guo et al. [48] proposed two very efficient IBE schemes in the online phase based on the Boneh-Boyen [13] (secure in the selective ID model) and Gentry's [19] (secure in the standard model) IBE. Liu and Zhou [49][50] then introduced their own more efficient versions, that generates much shorter ciphertext while being chosen plaintext secure in the random oracle model.

A newer variant is that of Chow, Liu and Zhou [51] which is a lot more efficient, especially when it comes to the online phase, generates even smaller ciphertext and is accompanied by an online/offline key encapsulation method. Wang and Chen [52] came up with an ID-based online/offline signature scheme (IBOOS) without random oracles that has been specially designed for the resource limited environment of a WSN.

When it comes to the energy limitations of WSN nodes, it is very efficient to be able to carry out some cryptographic operations during free time slots, when the node doesn't have any other task and his transceiver being "idle", thus reducing energy consumption due to antenna availability or idle/wake-up transitions. Also, if the PKG and the user securely communicate in order to execute de extract stage, it could also be feasible for the PKG to transmit a reusable offline-part of a user's signature in order to relieve it from the heavy computations. This approach might prove very useful when applied into a hierarchical WSN where, most of the times, a node needs to communicate with the cluster head. If communication is restricted just to that, then the offline phase needs to be carried out only once by the PKG for the node's entire lifespan. Savings in terms of heavy computations translates immediately into significant energy reserves.

V. Implementation Issues

A. Key revocation

IBE is a very powerful, yet controversial, tool when it comes to implementing a key revocation mechanism, and such identity based systems provide the possibility to generate temporary private keys in a simple and natural way.

One of the features present in [2] is a simple, yet effective key revocation method. If the sender would encrypt a message using not only the recipient's identity but also a time and/or date related piece of information, the PKG would have to generate a private key on the same principle and, thus, the ciphertext could only be decrypted within the desired time frame. If the recipient gets a message that has been encrypted outside his private key time frame, it will not be able to decrypt the ciphertext, and so, the sender must not worry about this thing.

Many ([4-7]) have put a lot of effort into creating a system capable of sending/delivering messages "into the future", and this feature of BF's scheme could prove handy when a message must be encrypted, sent and delivered but not decrypted until a certain moment in time. This time frame could also be scheduled according to the availability of the PKG to generate and send private keys.

B. and F.'s key revocation concept [2] could be a valid solution to other issues. In a relatively small network the PKG operations could be done for each node before the deployment phase. In this case an actual persistent on-site PKG would not be required. This translates into a system's lack of key revocation component. But, if the PKG would pre-generate private keys based on specific time frames (ID||year) for each and every node, the revocation component could be accomplished. Moreover, if, in a certain application, a persistent PKG would be necessary for the extraction of additional nodes private keys, these operations could take place at specific time intervals (keys expiration date). Thus, a permanent connectivity to the PKG wouldn't be mandatory, making the actual PKG-node a much more secure and long lasting entity.

For most WSN applications, sink node availability is of the essence. But others rely on mobile nodes in order to "scan" the network and harvest environment data. The key revocation component of an ID-based cryptosystem presented above fits perfectly into such an application. This way, sensor nodes could be preconfigured, security-wise, in the development stage and then deployed. If new nodes are to be deployed or old ones to be replaced, the deployment stage could also involve a private key generation stage executed by the mobile sink responsible for this action. Also, if the sink/PKG node would be static, its lifespan could be dramatically extended if key revocation would be insured indirectly by using well determined time frames – the sink could be saving energy for inter time frames.

The usage of short time frames for key generation (days, ours) is a feasible implementation of an ephemeral keys based system, but for even smaller periods of time the solution isn't scalable anymore due to the fact that the PKG (trusted agent or time server) must issue new private keys at the beginning of each time frame [5]. This translates into large amounts of overhead just for key extractions and, also, due to high computation requirements, the need for a much more powerful and long lasting PKG.

All of these features bring out another critical element of infrastructure, needed not only for security purpose but also for the entire collection and convergence of sensed data in a WSN – system time synchronization [4],[6-7],[10]. While this, obviously, adds a certain degree of complexity to the entire infrastructure, many WSN-based applications depend on it.

B. Key escrow

All classical ID-based cryptographic schemes presented themselves with the problem of key escrow meaning, the PKG, as long as it is the only entity empowered to issue private users keys based on its own master (secret) key, can decrypt and/or sign any messages secured by any of its partisans.

This translates into a matter of trust and physical security of the root PKG. By becoming a single point of failure, the PKG could be the primary target for many types of active attacks.

In wireless (ad-hoc) networks in general, and in WSN in particular, physical security is a serious problem, as devices are not "hard-wired" to the network and any potential attacker can tap the communication media. So, as long as attack prevention is problematic, there are some techniques that can be adopted in order to discourage the attacker.

One of these has been suggested, as we have seen earlier, by B. and F. in [2]. By dividing the PKG's private key generation task between multiple generation servers (a subset of *t-out-of-n* servers can generate a user's private key without the knowing, storing or computing the system "virtual" *master-key*), the attack would prove a lot more difficult to deploy. As simple as it is in theory, as difficult it is to put it into practice, due to the fact that there is a significant amount of overhead added to the system.

As an alternative to this, Gentry came up with a certificate-based proposal [26], where a signature acts as a certificate and also as a decryption key.

C. Key issuing

Gentry's solution [26] also answers a second IBC implementation issue – secure key issuing. The private key for a system user must be serviced over a secure channel or, if not, in a manner not allowing an attacker to intercept and/or compute it. In this case, the PKG would release its public key computed with a master secret key. The user that needs to authenticate would compute his public key based on a secret and its identity. After checking the user's identity, the PKG would release (publish) a certificate computed using the user's public key and the generator's master secret. In order to obtain a decryption key, the user would have to compute it based on its certificate and its secret.

Al-Riyami and Patersen eliminated the need for a public certificate in their proposal [27]. This way, the PKG receives the user's identity and public key and generates and transmits a partial private key. The user would have to compute its permanent private key based on its chosen secret (used when computing the public key) and the partial private key that it received from the PKG. This way, two very important problems are solved – the private key is generated based on a secret kept by the PKG but the actual key is only known by the user. Thus, the PKG can't sign messages in the user's name.

Lee et al. [28] proposed a new secure key issuing scheme which preserves the advantages of IBC, based on pairings, combining the distributed private key generator in B.&F.'s [2] and Al-Riyami & Patersen's [27] blinded partial private key feature. This assumes a single Key Generation Center (KGC) and multiple Key Privacy Authorities (KPA). Communication between a user and KGC/KPAs is secured using a simple blinding technique (users generates and transmits a blinding factor which is used by the key servers to "blind" answers). The fact that it uses a sequential process is very important - assuming that at least one KPA is not compromised, the private key can't be revealed. Only honest users that know the blinding factor can un-blind messages and retrieve the private key. Also, if the situation arises, under the cooperation of all central parties (KGC and KPAs), an encrypted message can be decrypted, while the private key stays safe with the user.

Plus, the current solution solves the key escrow problem of previous proposals.

In WSN-based applications, key issuing is of great importance as wireless communications are free to tap. This is the top factor that leads to a wide variety of attacks known to this day. Although Lee's solution [28] might seem appropriate in order to obtain a high level of security in both key escrow and key issuing aspects, when we analyze all computations that must be carried out by both the users and central authorities (KGC/KPAs) we find that, in addition to B. & F.'s DKG scheme [2], there is a significant amount of extra pairing operations which are proven to be computationally intense.

For example, for the key issuing stage of the process, in [2] only one pairing per private key generator is required to be carried out by the user in order to verify the authority's honesty. For the same key, in [28], every key generator must compute two pairing operations while the user must compute one to verify the correctness of this sequential process. For a WSN this would translate into high energy requirements for the distributed PKGs. If a WSN sink could act as a single system PKG because of its high/inexhaustible energy resource, then, setting up multiple PKGs can't be done in the same way, as it would be trivial. Also, if we consider WSN scenarios where there is only a mobile sink that doesn't always stay attached to the infrastructure (like a UAV), there has to be a decentralized approach regarding privacy and authentication assurance.

VI. IBC Security

A. Mathematical tools

Identity based cryptography is mostly based on mathematical functions called bilinear nondegenerate maps that define pairings of elements from one cyclic group to another of the same prime order, where the discrete logarithm problem is hard in the first group. Initially, pairings represented an attack method on elliptic curve systems. A pairing can be established for a given specially crafted curve and can convert a discrete logarithm problem on the curve into a discrete logarithm problem in a multiplicative subgroup of a field.

Chosen bilinear maps are one considered to be one way functions (easy to compute when a pair of operands is known but hard to calculate the opposite way). This property is known as the Bilinear Diffie-Hellman (BDH) Assumption because the BDH problems (Computational Diffie-Hellman Problem – CDHP or the Decision Bilinear Diffie-Hellman Problem – DBDHP) are reducible to the discrete logarithm problem for these bilinear maps [57].

The basic operation for pairings and, also, the most computationally expensive one is point multiplication on an elliptic curve. Thus, researchers are trying to come up with protocols and cryptographic schemes proposals which lead to as few as possible pairing operations yet without any compromise to security.

According to [58], there still is a series of open problems regarding IBC mathematical tools: curve parameterization attacks, special point attacks and higher-order power attacks.

B. Cryptographic primitives

But, when we consider the security of IBC schemes we can't withhold our analysis just to the strength of the mathematical tools that are being used. Going from the hardness of these tools, every IBC based proposal (encryption, signature, key issuing/management scheme) has to be fully analyzed and proven secure under different types of cryptographic attacks - ciphertext-only attack (COA), brute force attack, known-plaintext attack (KPA), chosen-plaintext attack (CPA), adaptive chosen-plaintext attack (CPA2), chosen-ciphertext attack (CCA), adaptive chosen-ciphertext attack (CCA2).

The resistance of ID-based primitives against these types of attacks has been considered under two different models – the standard model and the random oracle model.

We will give some examples of security proofs for the most important identity based cryptographic algorithms that have been presented so far.

The first cryptographic security analysis has been conducted by Boneh and Franklin [2], also strengthening standard definitions of CPA and CCA and adapting them to identity based primitives. Their BasicIdent scheme is proven to be only semantically secure against CPAs (IND-CPA secure) and is useful just for understanding purpose. FullIdent is IND-ID-CCA secure (i.e. indistinguishably secure against adaptively chosen ciphertext attacks) in the random oracle model, and is also called "fully secure". Boneh and Boyen proposed their ID-based encryption scheme that is selective ID secure without random oracles in [13] and the "fully secure" variant in [14]. Waters also came up with a scheme of its own [32], also proven to be secure in the standard model.

Gentry and Silverberg's HIBE [20] is proven to be CCA secure in the random oracle model, assuming the hardness of the BDH problem. A padding technique is being used in order to obtain a scalable proposal with complete collusion resistance indifferently of the hierarchy depth.

Regarding Cha and Cheon's work [36], the scheme is completely secure against existential forgery under adaptively chosen message and ID attacks in the random oracle model.

The selective identity type of attack was introduced by Canetti et al. in [29] and later improved in [30], which assumes that the adversary must first choose its target. Many researchers consider this security model as being weaker than the B.&F. [2].

Another important issue for IBC, more exactly for the hierarchical schemes, represents collusion. Collusion attack is defined as the cooperation (collusion) of a certain (threshold) percentage of a system's users in order to reproduce the master key for their domain PKG and subsequently masquerade as the PKG. HIBE schemes have been the subject of analysis for such an attack. While some schemes were designed to be secure against collusion in the upper levels of the hierarchy [31], other are completely collusion resistant on a random number of levels [20].

Based on these major models and proofs of security, authors keep proposing both efficient and sufficiently secure identity based cryptographic schemes.

The fact that identity based encryption (BF scheme [2]) has been standardized under IEEE 1363 (the standard body for public key cryptography methods) and multiple RFCs have been issued by the IETF, proves that identity based cryptography itself is reliable, trustworthy and is definitely considered to be very promising for a wide variety of applications.

C. Implementation specific attacks

Besides above analysis on the IBC mathematical problems and cryptographic primitives, there is one important factor that could greatly influence the overall security of a network. It is well known that cryptography itself or even specific security protocols and procedures are not the main point of vulnerability for a system, but, more likely, it is the user and its behavior in a specific context.

In the past years, tremendous efforts have been made for promoting and continuously developing IBC based implementations. This is because IBC is mostly suited to resource limited environments like wireless ad-hoc or sensor networks (fully developing domains).

When we address the field of wireless sensor networks, we must take into consideration previously presented WSN-specific attacks in order to fully analyze the level of security for such a system. There are some specific attacks that could also influence the failure of a cryptographic system. For example, if an attacker needs to analyze a great number of ciphertexts in order to get an advantage from this, he could first conduct a wormhole attack.

The fact that WSN nodes are wireless communication capable devices, mostly isolated and unsupervised, makes them an easy target for physical attacks or, perhaps even worse, side channel attacks. This type of attack is not strictly related to the strength of the cipher itself but, it mainly refers to the usage of other data about encryption or decryption process in order to gain valuable information about messages or parts of an encryption/signature key. Power analysis attacks consist of two phases – data acquisition (the attacker collects information on the power consumption / variations of the encryption device / component) and data analysis.

VII. IBC VS PKI

Since its public acknowledgement in the mid-1990s, PKIs have grown into an important but not so successful business as anticipated. Still, it’s the most renowned asymmetric cryptography based implementation. Even though there were a lot of technical and operational problems that were overcome [44], [45], making PKI schemes fully adoptable, there are some aspects of this type of cryptographic system that makes it undesirable for such an application as a WSN.

In a classical PKI-based application, when node B(ob) wants to securely transmit a message to node A(lice), both parties need to undertake a full 8 stages process: Alice registers with the local RA (Registration Authority) and computes and sends its public key, the RA validates the information and sends it to the nearest CA, the CA binds the public key to a certificate then signs and sends the public key certificate to Alice, Bob asks Alice for its certificate, Alice responds by sending the required certificate, Bob checks the certificate’s validity with Alice’s CA in a 2 step process, and, at last, Bob uses this information to encrypt the message going out to Alice.

As we have seen earlier, there are 3 very important stages that, in the case of IBC, are missing – Bob’s request for Alice’s certificate, the transmission of the actual certificate and the validation operation done by the CA. All these stages add a considerable degree of complexity to the entire system. Plus, if communication must be reduced to a minimum, such as in the case of WSNs, there is the need to cut back on this “secure communication” overhead. By simply using identities (names, network addresses etc.) instead of public certificates, we are eliminating the complexity that PKI brings to the system.

As we have mentioned earlier, an IBC system still relies on a central point (or a few distributed points in case of HIDS) of failure – the PKG. The network sink can play this role in a WSN (as it is more often considered to be more powerful and not so limited in terms of energy resources as other nodes) and this would eliminate the problem of a trusted third party, as the sink would be integrated in the same application and owned/controlled by the same user that deployed the entire network infrastructure. This does not mean that the PKG’s physical security may be neglected [46], on the contrary, supplementary physical measures must be undertaken in order to add an extra layer of security to the sink.

The sink as a CA/PKG may also pose some issues in the case of large scale infrastructures – hundreds or thousands of nodes. Routing messages, needed in the cryptographic scheme, from node to node in order to reach the CA/PKG (sink) might become a real burden and limit even more the lifespan of the infrastructure. In the IBC model, by decreasing the number and dimension of such messages, there is a lot less burdensome transmission of data going on.

In the context of a WSN, the idea of preloading PKI certificates in the node before deployment isn’t necessarily a good one – already limited memory would be occupied with large and potentially unnecessary data.

When it comes to signature schemes, in a PKI-based architecture, the CA links a user’s identity to a digital certificate. IBC approaches provide a simpler architecture for verifying digital signatures by eliminating certificates and just use identities. Traditional PKI certificates also involve some issues regarding information stored in CAs for the owner (organization or person) of the certificate.

A significant difference between Identity Based Cryptosystems and most of the traditional PKIs systems is that the latter doesn’t keep user keys in escrow. In IBC the PKG is the entity that, based on its own secret (master key) can generate all user private keys. Plus, the PKG can encrypt and send messages as if it were a certain user. This could prove useful only in such a situation where the PKG also acts as a gateway and there is the need for automated encryption for certain messages that contain sensitive information, based on policies established by the network owner.

Sure, for the encryption side of IBC, key escrow could pose as a serious problem if there is a problem of trust in the central key generator. When it comes to signatures, things are similar to those of a classical PKI, meaning a CA can produce a fake certificate with a public key for which he knows the private counterpart and can claim that the user tried to register two different public keys.

In applications where key escrow is a concern, IBC-based solutions like certificate-based encryption, secure key issuing (distributed key generators) and certificateless cryptography mentioned above are probably the best answer to this difficulty.

Immediately we can argue that the key escrow problem translates into a much stronger non-repudiation, which is an essential feature of digital signature systems. Even so, if we consider using such an application inside an organization, non-repudiation component loses its importance as it would only be useful in order to retrieve sensitive data when, potentially, the private key is lost.

Conveniently, in an IBC system there is no need for complex and expensive configuration operations, rather users communicate naturally using their own identities. On the server side, there is also no need for a database or a complicated public keys/certificates management system. Plus, this way, high computation operations are practically transferred from the user side to the PKG, thus having an effortless user. For WSN applications this represents a huge advantage because of a node's (user) physical limitations.

In a WSN environment it would be very useful for the PKG to stay in an idle state for as much time as possible for energy saving purpose or just to make it vulnerable to physical attacks for short periods of time. What is interesting in IBC is the fact that once the PKG is offline, secure communications can still be obtained, considering that all users previously got their private keys from the key server. Also, in certain applications where there is no need for a key refreshing/revocation mechanism and the maximum (fixed) number of nodes has been reached, the PKG can be completely taken out of the equation (a mobile/temporary sink also acting as a PKG).

As we have stated earlier, there has been some work on the size of the parameter set. If, for a certain IBC implementation, the parameter set is relatively large, adding a significant communication overhead, it could be hardcoded into each and every network node.

If a user of an IBC-based application only needs to send unsigned encrypted data (gathered information updates), his private key could be kept exclusively within the PKG which, presumably, is a lot safer than the everyday node due to additional security measures.

The key revocation technique that comes along very easily, embedded within an IBC scheme is quite controversial. While it is clear that any resource limited infrastructure can benefit from such a simple technique (generate identities based on names and time frames), some might argue that this actually represents the failure to implement an explicit key revocation mechanism like CRL. Key revocation only works as a damage control method, by limiting private keys to specific, fixed time frames. The explicit revocation itself (in case of a compromised user's private key) can still generate short time frames. During these short periods of time, the network becomes vulnerable.

When considering a single PKG IBC system, the key generator must benefit from supplementary security measures as it can easily become the target for numerous attacks, due to the fact that it is capable of recomputing all user private keys. If the key server is successfully attacked, then the whole system is compromised.

Plus, the connection between the key server and the user trying to extract its private key must be secured by other cryptographic means.

VIII. IBC Implementations

A. Practical algorithms

There are a great number of research papers that come up with theoretical solutions regarding IBC. Putting every proposal into practice proved quite difficult especially if we consider that most algorithms are based on a mathematical abstraction – the random oracle model.

Even though Boneh and Franklin have brought a great contribution to the development of IBC, their work in [2] was failing in implementation. Most of the IBE schemes that followed were also based on security proofs in the random oracle model which may not hold when the oracle is instantiated with concrete hash functions [37]. In the past decade, efforts have been made in order to eliminate this theoretical "black box". Boneh and Boyen then proposed an efficient selective-ID secure ID-based encryption without random oracles [13] and also an inefficient variant that is proven to be IND-CCA secure in the standard model [14]. Based on the work of Waters in [32], Nacache [38] presented a much more efficient version, one that is secure against passive adversaries in the standard model, making it more suitable for practical use.

Regarding IBS, the need for random oracles was first suppressed by Boneh and Boyen [12] and then, based on Waters's [32], by Paterson and Schuldt in [37].

Kate and Goldberg designed a distributed PKG and several key extraction protocols, one of which can be proven selective-ID secure in the standard model [39].

Whereas Bone-Boyen-Goh scheme [15] is only selective-ID secure in the standard model, Ren & Gu's hierarchical ID-based encryption scheme is fully secure regardless of the hash functions implementation.

B. Standards and workgroups

The first secure and practical identity based encryption system that was standardized under IEEE 1363.3 (IEEE P1363.3 is standard for identity-based cryptographic techniques using pairings) is the BF algorithm [2]. 1363-WG is the working group for public-key cryptography. The standard contains pairings-based cryptographic techniques, mathematical primitives for key derivation, public-key encryption and digital signatures.

Also, the IETF S/MIME workgroup issued several drafts regarding identity based cryptographic techniques.

There are also four published RFCs that prove the scientific community's interest and trust in this cryptographic flavor - RFC 1824 (IBC Protocol for Authenticated Key-Exchange), RFC 5091 (IBC Standard #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems), RFC 5408 (IBE Architecture and Supporting Data Structures) and RFC 5409 (Using the BF and BB1 Algorithms with the Cryptographic Message Syntax).

C. Real world applications

The most prodigious author in the field of IBC is arguably Dan Boneh. He is responsible for the Stanford University IBE system - "IBE Secure E-mail". The MIRACL library is another example of an IBE implementation. Both libraries are developed in C/C++ under Debian GNU/Linux and are based on the BF scheme [2].

Ben Lynn is the main author of the PBC (Pairing-Based Cryptography) library, with contributions from Shacham, Goldberg and others. Also written in C language, it was released under the GNU Lesser General Public License and built on the GMP library that performs the mathematical operations underlying pairing-based cryptosystems.

It is clear that successful authors contributed to ID-based applications and industry adoption. Boneh is also co-founder of Voltage Security, company that offers solutions-based on the first secure, practical IBE system , the BF algorithm [2]. According to Voltage, today, the IBE technology protects data for over 100 million users world-wide and is compatible with Outlook, Yahoo!, Gmail or Office365. Voltage employees are also responsible for issuing above mentioned RFCs.

Voltage and Gemalto are responsible for the development of the first smart-card implementation of IBE, based on the BF scheme [2]. Proofpoint Secure Messaging software added Voltage's IBE technology to their existing content-filtering capabilities.

Fortinet's FortiMail provides Identity-Based Encryption, in addition to S/MIME and TLS/SSL, as email encryption options to enforce policy-based encryption for secure content delivery.

Ferris Research conducted a study on Voltage's solutions and concluded that the total cost of ownership for Voltage IBE solutions is one-third of the cost for a classic PKI system and operational costs are even smaller – one-fifth.

D. WSN security solutions

In order to put IBC into service in WSNs, there are a number of key factors that need careful consideration. The first one is the size of the public parameters set which could have a significant impact on the amount of memory that's being used for communication security. In order to reduce power consumption and keep low processing capabilities there is the need to reduce the complexity of the mathematical operations computed for encryption/decryption or signing/verification (the reduction in number of pairing operations, which are the most expensive, has a significant impact). In order to reduce the amount of energy the transceiver unit drains out of the battery, a significant reduction for the size of ciphertexts and signatures is definitely desirable.

There has been a continuous concern in the literature for these problems as IBC was definitely intended to be used in ad-hoc wireless networks. But it was only recently when researchers began to adapt their constructions to the strict resource limitations and tight specifications of WSN.

Watro et al. [59] first started to experiment with public key cryptography in the context of WSN. Similar to the online/offline approach, in their TinyPK scheme, network nodes are efficiently executing RSA public operations while the expensive RSA private operations are being delegated to more powerful nodes ore other infrastructure components. Then, Gura et al. [60] demonstrated that ECC outperforms RSA when tested on the ATmega128L microprocessor that most sensors are fitted with. Malan developed the first known ECC implementation [61] for sensor networks based on the Mica2 architecture running TinyOS, while others have worked on the TelosB mote.

Based on these previous results, Szczechowiak et al. [62] developed NanoECC, an efficient implementation of PBC primitives, based on the MIRACL crypto library and testing their results on the Mica2 and TmoteSky platforms running TinyOS. Other authors have tried to put the famous BF [2] scheme into practice, on a sensor platform, like Yang et al.'s ID-Based Key Agreement and Encryption scheme [63] for WSN, but with no viable results.

Again, Szczechowiak came up with TinyIBE [64], an efficient security bootstrapping protocol for sensor networks that uses IBE and exploits the enhanced capabilities of high-end cluster heads.

Liu and Zhou [65] worked together on two very efficient ID-based proposals for WSNs – an encryption and a signature scheme, both of which are based on the online/offline feature of IBC. They presented a concrete "receiver bound" online/offline scheme with very short ciphertexts compared to other proposals. In [66], authors have presented a MicaZ platform implementation of an online/offline identity-based signature scheme with multi-time usage of the offline storage, a feature that makes it feasible for large scale sensor networks.

Various authentication schemes have been the starting point for several recent identity-based secure routing protocols, even though it has been a major challenge due to node mobility and limited resources.

As it can be seen, the scientific community realized that IBC not only that has a huge potential for usage in WSN, but they actually complete each other very well. A testimony for this is the increasing number of publications in this direction along with recent estimates of great financial potential for the WSN industry.

IX. Conclusion

Despite of the fact that IBC cryptosystems still show some signs of weakness, we must admit that it brings some indisputable advantages for the common user that wishes for a simpler process for setting private, secure communication than classic PKI systems.

More than that, a series of special, key features of IBC (distributed key generator, system hierarchy, key revocation, delegation) are being resolved in a simple and elegant manner.

In applications with limited available system resources, factors regarding overall system performance become much more important. This is the reason why, in certain infrastructures like WSN, where node's lifetime (lifecycle) is a decisive element and computational effort must be limited to a minimum, IBC seems, for the time being, a good solution for system security.

IBC brings obvious advantages when it comes to encryption. Because a user's identity is used as a public key, a message can be transmitted directly, without any certificates or additional verifications. This immediately translates into a massive reduction in communication overhead as well as a more rational usage of bandwidth.

The hierarchical models that can be derived from IBC seem to fit perfectly into the infrastructure of a sensor network. WSN cluster heads and IBC subdomain PKGs could become functionalities available on the same physical device.

Even though there is moderation in technology adoption because of classic key escrow and key revocation issues, there are a number of solutions which prove to be very useful in some real-life scenarios – time synchronization and distributed key generators.

The specific types of applications and limited resources of WSNs are causing massive interest in the scientific community regarding their security assurance. While lightweight cryptography, a relatively new flavor of cryptography, is still under close attention, IBC continues to arouse interest for the research community.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology, CRYPTO 1984, Lecture Notes in Computer Science, vol. 196, pp. 47-53, Springer-Verlag, 1985. doi: 10.1007/3-540-39568-7_5

[2] D. Boneh, M. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology — CRYPTO 2001, CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, pp. 213-229, Springer-Verlag, 2001. doi: 10.1007/3-540-44647-8_13

[3] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," Cryptography and Coding 2001 – Proc. 8th IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science, vol. 2260, pp. 360-363, Springer-Verlag, 2001. doi: 10.1007/3-540-45325-3_32

[4] G. Di Crescenzo, R. Ostrovsky, S. Rajagopalan, "Conditional oblivious transfer and timed-release encryption," in *Advances in Cryptology - EUROCRYPT 1999*, Lecture Notes in Computer Science, vol. 1592, pp. 74-89, Springer-Verlag, 1999. doi: 10.1007/3-540-48910-X_6

[5] J. Cathalo, B. Libert, J. Quisquater, "Efficient and Non-interactive Timed-Release Encryption," *Information and Communications Security - ICICS 2005*, Lecture Notes in Computer Science, vol. 3783, pp. 291-303, Springer-Verlag, 2005. doi: 10.1007/11602897_25

[6] J. H. Cheon, N. Hopper, Y. Kim, I. Osipkov, "Provably secure timed-release public key encryption," ACM Transactions on Information and System Security (TISSEC), vol. 11, no. 2, article no. 4, Mar., 2008. doi: 10.1145/1330332.1330336

[7] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, G. Stephanides, "Pairing Based Timed-Release Cryptography," presented at Identity Based Encryption Workshop, NIST, Thessaloniki, Greece, 2008.

[8] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," *Journal of Cryptology*, vol. 20, pp. 51-83, Springer-Verlag, 2007. doi: 10.1007/s00145-006-0347-3

[9] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," Advances in Cryptology — CRYPTO '91. CRYPTO 1991, Lecture Notes in Computer Science, vol. 576, pp. 129-140, Springer-Verlag, 1991. doi: 10.1007/3-540-46766-1_9

[10] K. Römer, P. Blum, L. Meier, "Time Synchronization and Calibration in Wireless Sensor Networks," in *Handbook of Sensor Networks: Algorithms and Architectures*, I. Stojmenovic, John Wiley & Sons, 2005, pp. 199-237. doi: 10.1002/047174414X.ch7

[11] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," Advances in Cryptology — EUROCRYPT 2003, Lecture Notes in Computer Science, vol. 2656, pp. 416-432, Springer-Verlag, 2003. doi: 10.1007/3-540-39200-9_26

[12] D. Boneh, X. Boyen, "Short Signatures Without Random Oracles," Advances in Cryptology — EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 56-73, Springer-Verlag, 2004. doi: 10.1007/978-3-540-24676-3_4

[13] D. Boneh, X. Boyen, "Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles," Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 223-238, Springer-Verlag, 2004. doi: 10.1007/978-3-540-24676-3_14

[14] D. Boneh, X. Boyen, "Secure Identity Based Encryption Without Random Oracles," Advances in Cryptology – CRYPTO 2004, Lecture Notes in Computer Science, vol. 3152, pp. 443-459, Springer-Verlag, 2004. doi: 10.1007/978-3-540-28628-8_27

[15] D. Boneh, X. Boyen, E.-J. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science, vol. 3494, pp 440-456, Springer-Verlag, 2004. doi: 10.1007/11426639_26

[16] A. Joux, K. Nguyen, "Separating Decision Diffie–Hellman from Computational Diffie–Hellman in Cryptographic Groups," *Journal of Cryptology*, vol. 16, pp. 239-247, Springer-Verlag, 2003. doi: 10.1007/s00145-003-0052-4

[17] D. Boneh, X. Boyen, "Short signatures without random oracles," Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 56-73, Springer-Verlag, 2004. doi: 10.1007/978-3-540-24676-3_4

[18] J. H. Cheon, "Security analysis of the strong Diffie-Hellman problem," Advances in Cryptology - EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 1-11, Springer-Verlag, 2006. doi: 10.1007/11761679_1

[19] C. Gentry, "Practical Identity-Based Encryption without Random Oracles," Advances in Cryptology - EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 445-464, Springer, 2006. doi: 10.1007/11761679_27

[20] C. Gentry, A. Silverberg, "Hierarchical ID-Based Cryptography," Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501, pp. 548-566, Springer-Verlag, 2002. doi: 10.1007/3-540-36178-2_34

[21] F. Zhang, K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501, pp. 533-547, 2002. doi: 10.1007/3-540-36178-2_33

[22] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology, pp.199-203, 1983. doi: 10.1007/978-1-4757-0602-4_18

[23] R. L. Rivest, A. Shamir, Y. Tauman, "How to leak a secret," Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, pp.552-565, Springer-Verlag, 2001. doi: 10.1007/3-540-45682-1_32

[24] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, pp. 514-532, Springer-Verlag, 2001. doi: 10.1007/3-540-45682-1_30

[25] F. Zhang, R. Safavi-Naini, W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," Public Key Cryptography – PKC 2004, Lecture Notes in Computer Science, vol. 2947, pp. 277-290, Springer-Verlag, 2004. doi: 10.1007/978-3-540-24632-9_20

[26] C. Gentry, "Certificate-based encryption and the certificate revocation problem," Advances in Cryptology - EUROCRPYT 2003, Lecture Notes in Computer Science, vol. 2656, pp. 272-293, Springer-Verlag, 2003. doi: 10.1007/3-540-39200-9_17

[27] S. Al-Riyami, K. Paterson, "Certificateless Public Key Cryptography," Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science, vol. 2894, pp. 452-473, Springer-Verlag, 2003. doi: 10.1007/978-3-540-40061-5_29

[28] B. Lee et al., "Secure key issuing in ID-based cryptography," in Proc. 2nd workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - *ACSW Frontiers 2004*, vol. 32, pp. 69-74, 2004.

[29] R. Canetti, S. Halevi, J. Katz, "Chosen-ciphertext security from identity based encryption," Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 207-222, Springer-Verlag, 2004. doi: 10.1007/978-3-540-24676-3_13

[30] D. Boneh, R. Canetti, S. Halevi, J. Katz, "Chosen-ciphertext security from identity based encryption," *SIAM Journal of Computing (SICOMP)*, vol. 36, no. 5, pp. 1301-1328, ACM, 2006. doi: 10.1137/S009753970544713X

[31] J. Horwitz, B. Lynn, "Toward Hierarchical Identity-Based Encryption," Advances in Cryptology - EUROCRYPT 2002, Lecture Notes in Computer Science, vol. 2332, pp. 466-481, Springer-Verlag, 2002. doi:10.1007/3-540-46035-7_31

[32] B. Waters, "Efficient Identity-Based Encryption Without Random Oracles," Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science, vol. 3494, pp. 114-127, Springer-Verlag, 2005. doi: 10.1007/11426639_7

[33] D. Boneh, C. Gentry, M. Hamburg, "Space-Efficient Identity Based Encryption without Pairings," *IACR Cryptology ePrint Archive*, Report 2007/177, 2007. https://eprint.iacr.org/2007/177.pdf

[34] C. Gentry, C. Peikert, V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions," *IACR Cryptology ePrint Archive*, Report 2007/432, 2007. https://eprint.iacr.org/2007/432.pdf

[35] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, H. Wee, "Fuzzy identity based encryption from lattices," *IACR Cryptology ePrint Archive*, Report 2011/414, 2011. https://eprint.iacr.org/2011/414.pdf

[36] J. C. Cha, J. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," Public Key Cryptography - PKC 2003, Lecture Notes in Computer Science, vol. 2567, pp. 18-30, Springer-Verlag, 2002. doi: 10.1007/3-540-36288-6_2

[37] K. Paterson, J. Schuldt, "Efficient Identity-Based Signatures Secure in the Standard Model," Information Security and Privacy - ACISP 2006, Lecture Notes in Computer Science, vol. 4058, pp. 207-222, Springer-Verlag, 2006. doi: 10.1007/11780656_18

[38] D. Naccache, "Secure and practical identity-based encryption," IET Information Security, vol. 1, no. 2, pp. 59-64, IET, 2007. doi: 10.1049/iet-ifs:20055097

[39] A. Kate, I. Goldberg, "Asynchronous Distributed Private-Key Generators for Identity-Based Cryptography," *Cryptology ePrint Archive*, report 2009/355, 2010. https://eprint.iacr.org/2009/355.pdf

[40] A. Kate, I. Goldberg, "Distributed private-key generators for identity-based cryptography," Security and Cryptography for Networks - SCN

2010, Lecture Notes in Computer Science, vol. 6280, pp. 436-453, Springer-Verlag, 2010. doi: 10.1007/978-3-642-15317-4_27

[41] A. Siad, "Anonymous Identity-Based Encryption with Distributed Private-Key Generator and Searchable Encryption," presented at the 5th International Conference on New Technologies, Mobility and Security (NTMS), Istanbul, Turkey, 2012. doi: 10.1109/NTMS.2012.6208695

[42] A.-F. Chan, "Distributed private key generation for identity based cryptosystems in ad hoc networks," *IEEE Wireless Communications Letters*, vol. 1, no. 1, pp. 46-48, 2012. doi: 10.1109/WCL.2012.120211.110130

[43] G. Anastasi, A. Falchi, A. Passarella, M. Conti, E. Gregori, "Performance measurements of motes sensor networks", in Proc. 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems - MSWiM 2004, Venice, Italy, 2004, pp. 174-181. doi: 10.1145/1023663.1023695

[44] C. Ellison, B. Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", in *Public Key Infrastructure: Building Trusted Applications and Web Service*, J. R. Vacca, Eds. CRC Press, 2004, ch. 23, pp. 299-306. doi: 10.1201/9780203498156.ch23

[45] A. Keith, "Common issues in PKI implementations - climbing the <<Slope of Enlightenment>>," SANS Institute InfoSec Reading Room, GSEC Practical v.1.4b, 2003. https://perma.cc/8U2W-QE7S

[46] S. Mohammadi, H. Jadidoleslamy, "A comparison of physical attacks on Wireless Sensor Networks," *International Journal of Peer to Peer Networks (IJP2P)*, vol. 2, no. 2, pp. 24-42, 2011. doi: 10.5121/ijp2p.2011.2203

[47] S. Even, O. Goldreich, S. Micali, "On-line/off-line digital signatures," *Journal of Cryptology*, vol. 9, no. 1, pp. 35-67, Springer-Verlag, 1996. doi: 10.1007/BF02254791

[48] F. Guo, Y. Mu, Z. Chen, "Identity-based online/offline encryption", *Financial Cryptography and Data Security - FC 2008*, Lecture Notes in Computer Science, vol. 5143, pp. 247-261, Springer-Verlag, 2008. doi: 10.1007/978-3-540-85230-8_22

[49] J. K. Liu, J. Zhou, "An efficient identity-based online/offline encryption scheme," in Proc. Applied Cryptography and Network Security - ACNS 2009, vol. 5536, Lecture Notes in Computer Science, pp. 156-167, Springer-Verlag, 2009. doi: 10.1007/978-3-642-01957-9_10

[50] J. K. Liu, J. Baek, J. Zhou, Y. Yang, J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287-296, Springer-Verlag, 2010. doi: 10.1007/s10207-010-0109-y

[51] S. S. M. Chow, J. K. Liu, J. Zhou, "Identity-based online/offline key encapsulation and encryption", in Proc. 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS 2011, Hong Kong, China, 2011, pp. 52-60. doi: 10.1145/1966913.1966922

[52] Z. Wang, W. Chen, "An ID-based online/offline signature scheme without random oracles for wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 837-841, Springer-Verlag, 2013. doi: 10.1007/s00779-012-0534-1

[53] Sakai-Kasahara Key Encryption (SAKKE), RFC 6508, IETF, 2012.

[54] Y. Dodis, M. Yung, "Exposure-resilience for free: The case of hierarchical ID-based encryption," in Proc. 1st International IEEE Security in Storage Workshop, Greenbelt, USA, 2002, pp. 45. doi: 10.1109/IITSI.2010.53

[55] M. Au, J. Liu, T. Yuen, D. Wong, "Practical Hierarchical Identity Based Encryption and Signature schemes without Random Oracles," *IACR Cryptology ePrint Archive*, report 2006/368, 2006. https://eprint.iacr.org/2006/368.pdf

[56] L. Zhang, Q. Wu, Y. Hu, "Hierarchical Identity Based Encryption with Constant-Size Private Keys," *ETRI Journal*, vol. 34, no. 1, pp. 142-145, Wiley Online Library, 2012. doi: 10.4218/etrij.12.0211.0140

[57] Y. Yacobi, "A Note on the Bi-Linear Diffie-Hellman Assumption," *IACR Cryptology ePrint Archive*, report 2002/113, 2002. https://eprint.iacr.org/2002/113.ps

[58] C. Whelan, D. Page, F. Vercauteren, M. Scott, W. Marnane, „Implementation Attacks and Countermeasures," in *Identity Based Cryptography*, Eds. IOS Press, 2009, ch. XIV, pp. 226-243. doi: 10.3233/978-1-58603-947-9-226

[59] R. J. Watro, D. Kong, S. fen Cuti, C. Gardiner, C. Lynn, P. Kruus, "Tinypk: securing sensor networks with public key technology," in Proc. 2nd ACM workshop on Security of ad hoc and sensor networks - SASN 2004, Washington DC, USA, 2004, pp. 59-64. doi: 10.1145/1029102.1029113

[60] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems - CHES 2004*, Lecture Notes in Computer Science, vol. 3156, pp. 119-132, Springer-Verlag, 2004. doi: 10.1007/978-3-540-28632-5_9

[61] D. J. Malan, M. Welsh, M. D. Smith, "A Public-Key Infrastructure for key distribution in TinyOS based on Elliptic Curve Cryptography," *1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks – SECON 2004*, Santa Clara, California, 2004. doi: 10.1109/SAHCN.2004.1381904

[62] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, R. Dahab, "NanoECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks," *European Conference on Wireless Sensor Networks - EWSN 2008*, Lecture Notes in Computer Science, vol. 4913, pp. 305-320, Springer-Verlag, 2008. doi: 10.1007/978-3-540-77690-1_19

[63] G. Yang, C. Rong, C. Veigner, J. Wang, H. Cheng, "Identity-Based Key Agreement and Encryption for Wireless Sensor Networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 13, no. 4, pp. 54-60, 2006. doi: 10.1016/S1005-8885(07)60034-X

[64] P. Szczechowiak, M. Collier, "TinyIBE: Identity-based encryption for heterogeneous sensor networks," in Proc. 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Melbourne, Australia, 2009, pp. 319-354. doi: 10.1109/ISSNIP.2009.5416743

[65] C. Chu, J. Liu, J. Zhou, F. Bao, R. Deng, "Practical ID-based encryption for wireless sensor network", in Proc. 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010, pp. 337-340. doi: 10.1145/1755688.1755734

[66] J. Liu, J. Baek, J. Zhou, Y. Yang, J. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287-296, Springer-Verlag, 2010. doi: 10.1007/s10207-010-0109-y