Authentication in dynamic groups using identity-based signatures

Nils gentschen Felde, Sophia Grundner-Culemann, Tobias Guggemos
MNM-Team, Ludwig-Maximilians-Universität München, Munich, Germany
Email: {felde, grundner-culemann, guggemos}@nm.ifi.lmu.de

***Abstract*—Group communication in constrained networks lately sparked broader interest as it allows dealing more efficiently with the few available resources. Both sender authentication and membership verification are serious issues to be tackled despite the lack of resources. Identity-based signatures (IBS) offer an alternative to certificate-based authentication by mathematically binding a user's public key to its identity. To utilize the consequently smaller network load, this paper proposes an IBS-based lightweight solution to achieve authentication and membership verification for group communication in constrained environments. An infrastructure for managing IBS-based authentication is introduced together with a taxonomy for the selection of suitable IBS schemes. An implementation and practical evaluation on basis of an IoT-lab completes this, demonstrating that IBS is a viable option for very constrained devices. To the best of our knowledge, this is the first fully operational implementation and proof of applicability of IBS in such a scenario.**

***Keywords*-IoT; Multicast; Security; Group Communication; Authentication; Identity-Based Signatures**

I. Introduction

In modern Internet of Things (IoT) scenarios like Wireless Sensor Networks (WSN), Industrial IoT or simply home automation, a multitude of small ("constrained") devices form a group and enable higher level services. The constraints of participating devices range from limited computational power over little (local) storage and energy supply to reduced network capabilities and data rates as well as any combination thereof. Efficient communication among a given group of such devices is vital to provide any other service. Multicasting for example reduces networking overhead and thus minimizes energy consumption [1]. In wireless, mobile, and ad-hoc networks, communication groups can form and change frequently, making security and especially individual authentication of clients within the group a challenging task.

This work introduces a lightweight architecture for sender authentication in constrained group communication using identity-based signatures (IBS). Characteristically for IBS, the term "lightweight" refers to efficiency in regard to network load at the expense of CPU use, which proves useful for certain use cases. As a by-product, IBS provides mathematically sound means for access control via the use of a master secret key (msk) and thus avoids the necessity of distributing and managing revocation lists. More details about IBS can be found in Sections II-A and IV.

A major advantage of IBS over regular PKIs (public key infrastructures) is found in highly dynamic scenarios, in this case meaning frequently changing group settings, for which IBS is second to none in terms of messages to be exchanged. Even though X.509 certificate compression has already been addressed by the IETF [2], access management is typically enforced using costly revocation lists. Frameworks such as SAML (Security Assertion Markup Language) or OAuth (Open Authorization) offer optimizations based on so-called access tokens. They can also be used to grant both group access and group authentication. However, individual sender authentication is not covered.

Talking about IBS and its use for authenticated group communication, it is inevitable to define the term authenticity in the scope of group communication. A well-suited definition is given in an earlier publication [3]: "*A message is authentic, if the message originates from its stated sender. Similar to message integrity, in group communication scenarios one can differentiate two types of message authenticity: a) a message can be proven to originate from within the communication group (group authentication) or b) a message can be verified being sent by a certain sender (sender authentication). Sender authentication implies group authentication, if and only if additional and validated knowledge of group memberships is available.*"

Usually, individual sender authentication (also in group communication scenarios) is realized using individually generated public / private key pairs in combination with a variety of cryptographic signature algorithms. However, it is challenging to reliably prove a sender's "ownership" of a certain key pair.

A. Contribution of this paper

In summary, IBS promises the following advantages over conventional signing methods in IoT group communication settings:

1) Messages do not need to contain certificates but can be authenticated with comparably very little overhead. This reduces the network load significantly.
2) Private key revocation is done mathematically by issuing new key material. In this new configuration, the old keys are invalid and can not be used for signing anymore. Management of revocation lists is therefore not necessary. This is of special interest in dynamic networks such as wireless / mobile networks, where group membership changes frequently.

On the downside, a strong trust relationship with a key server is needed, which is why this work studies the possibility of integrating IBS features into a typical architecture for security management in group settings, namely with GCKS (RFC 4046 [4]).

The main contributions of this paper consist in 1) the proposal of a taxonomy that allows a (visual) comparison of various IBS schemes with respect to the four key components of identity-based signatures, 2) the discussion and formalization of re-keying as a means of key revocation in IBS and 3) the first implementation and measurements for IBS in a group communication testbed consisting of constrained devices.

B. Goal and prerequisites

The scope of this work is the application of IBS to grant authenticity (sender and group) in group communication settings among constrained devices in a lightweight fashion with respect to memory usage, network load, and storage demands. Please note that confidentiality is not targeted by this paper, but that due to its nature, IBS will be able to grant message integrity.

As a prerequisite, the management of communication groups themselves and an identification service are assumed to be available:

Reliable group management:
This service must be able to reliably add devices to and remove them from a communication group as well as prove the group membership status of a given device based on its identity. The technical access to a group on the other hand will be handled by cryptographic means using IBS.

Identification service:
As identification of devices is not in the scope of this work, we assume an identification service to be available. It has to realize at least the following functions:

1) Arbitrary entities must be able to register with the service and a unique ID will be issued.
2) It must be possible to prove a given ID's validity and link it to its owner.
3) Optionally, it comes in handy if an ID can be revoked.

Technically speaking, Trusted Platform Modules (TPM) can be used as a basis to assign IDs (among others).

C. Structure of the paper

The remainder of the paper is structured as follows: Firstly, Section II introduces IBS and surveys related work. Section III discusses criteria for the choice of a well-suited IBS scheme depending on the use case in form of a taxonomy. After that, Section IV presents an IBS-based authentication structure including mathematically sound means to ensure access control using IBS. An evaluation of the findings follows in Section V. To conclude, Section VI summarizes the paper and gives an outlook on future work.

II. Background and Related Work

Lightweight authentication infrastructures for IoT are a controversially discussed topic among researchers. This paper evaluates one possible solution, namely IBS. In the following, Section II-A will give a short introduction to the concepts behind IBS, before Section II-B discusses related work in the area of lightweight authentication.

A. Identity-Based Signatures

Usually, a user's key material is chosen at random and some external infrastructure (like a certificate) is used to prove ownership. In 1984, Adi Shamir [5] proposed an asymmetric key system in which the public key is specifically chosen in order to be mathematically linked to some information about its owner. Typically, an identity approved by a trusted authority is used for this, leading to the name *identity-based signatures / encryption* (IBS / IBE). A Trusted Third Party (TTP) is required to compute user secret keys (*usk*) with a master secret key (*msk*). As in other asymmetric systems, signatures are created using the user secret key, while encryption is performed with the public key. Only the intended recipient's identity and the *mpk* need to be known to send an encrypted message. Similarly, given the *mpk*, a signature, and the stated signer's identity, any recipient can verify the signature. This makes additional infrastructure for managing individual public keys unnecessary. Thus, IBS offers minimal network overhead during communication and a lightweight management infrastructure at the expense of a very strict trust relationship between client and TTP.

This paper focuses on signing messages, which works as follows:

Setup: The TTP chooses an *msk*, computes the *mpk* and chooses / computes other relevant public parameters (*pub params*), e. g. random group generators, hash and pairing functions, and elliptic curve parameters.

Extract: Given a new member's ID, the TTP creates its *usk* using the *msk* and sends it to the member over a secure channel, together with the *mpk* and *pub params*.

Sign: A user signs a message with its *usk*.

Verify: Given the stated sender's ID, a signed message, and the group's *mpk* and *pub params*, a recipient verifies / falsifies the signature.

Table I presents the mathematics of these four phases for two exemplary IBS schemes and shows the mathematical link between a signature and the *mpk*. Both schemes use special maps on elliptic curves called pairings.

B. Related Work

Most related literature focuses on building lightweight infrastructures (minimizing management and / or network overhead with the key-server(s)), which are often based on (D)TLS (e.g. [6], [7]). Our solution is a more generic approach which could be built in any IP based infrastructure. There are also approaches using compression (minimizing signatures / certificates during communication), implying the necessity of pre-installed knowledge which is often difficult to update. Other works define lightweight cryptographic algorithms (minimizing computation and / or key-sizes), but they are usually barely evaluated. This section will focus on related work with IBS in constrained environments and other cryptographic primitives allowing lightweight sender authentication.

TABLE I: The phases of IBS in Hess and BLMQ

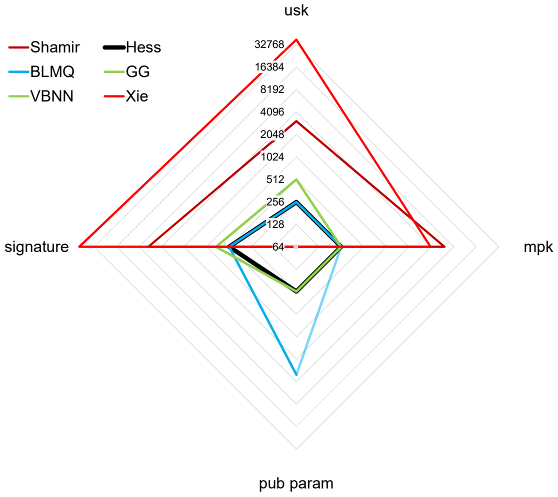
Hess	BLMQ
Setup:	
1) $msk \leftarrow \mathbb{Z}_p^*$ 2) $mpk = msk * P$	1) $msk \leftarrow \mathbb{Z}_p^*$ 2) $mpk = msk * P$
Extract:	
$usk = msk * H_1(ID)$	$usk = \frac{1}{msk+h_1(ID)} P$
Sign:	
1) $x \leftarrow \mathbb{Z}_p^*,\ Q \leftarrow \mathbb{G}^*$ 2) $r = e(Q, P)^x$ 3) $h = h_2(M, r)$ 4) $S = h * usk \oplus x * Q$	1) $x \leftarrow \mathbb{Z}_p^*$ 2) $r = \mathbf{e}(\mathbf{P}, \mathbf{P})^x$ 3) $h = h_2(M, r)$ 4) $S = (x + h) * usk$
Verify:	
$\tilde{r} = e(S, P)e(H_1(ID), -mpk)^h$ $h \overset{?}{=} h_2(M, \tilde{r})$	$\tilde{r} = e(S, h_1(ID) * P \oplus mpk) \cdot \mathbf{e}(\mathbf{P}, \mathbf{P})^{-h}$ $h \overset{?}{=} h_2(M, \tilde{r})$

M message P point on ell. curve $\mathbb{G}$ cyclic group generated by P
$h_i()$ hash function in $\mathbb{Z}_p$ $H_i()$ hash function in $\mathbb{G}$ $e()$ pairing
S signature $\mathbb{Z}_p^*, \mathbb{G}^*$ groups without identity ($\mathbb{1}$) element

1) IBS in constrained environments: Some work to apply IBS in constrained environments, such as in Baek et al. [8], or on top of mobile networks [9] has already been carried out, but both mainly focus on the applicability and advantages of IBS in specific cases. Yasmin et al. [10] applied IBS in Wireless Sensor Networks for authenticated broadcast using constrained devices, which yielded measurements very similar to those presented in this paper. However, they did not discuss the implications of dynamic group structures. Also, instead of classic IBS they implemented and tested so-called online / offline signatures which allow for pre-computation of some signature parts on more resourceful devices. Lin et al. [11] were among the first to show the potential of IBS for vehicular ad-hoc networks and thus for dynamic groups. They mainly focus on the reduction of network traffic overhead and the possibility to dynamically form groups. The work was a very welcome source of discussions, but left out the adaption for inter-domain scenarios such as IoT or Industry 4.0. To the best of our knowledge, IBS has not been discussed very actively in the context of group communication ever since.

2) Cryptographic Primitives: There have been a number of proposals for cryptography in multicast scenarios, but not necessarily in constrained group communication. A popular idea came from Perrig et al. [12] who proposed the use of symmetric cryptography and introducing time-asymmetry for individual sender authentication. Both schemes from the paper – EMSS and Tesla – were proposed and standardized by the IETF Multicast Security WG[1]. Lately, Tesla gained more attention. Some optimizations for wireless sensor network were developed, resulting in the so-called μTesla [13]. The major drawback is the authentication being delayed by one packet, which results in serious DoS vulnerabilities [14]. Also, as a symmetric key needs to be distributed for every sender it does not scale well.

Another approach are one-time signatures, which usually optimize computation with the drawback of high communication overhead. BiBa [14] is one example, which Yao et al. [15] tried to optimize for the needs of wireless sensor networks.



Scheme	Shamir	Hess	BLMQ	GG	VBNN	Xie
usk	3,072	254	254	508	508	37,975
mpk	6,144	254	254	254	254	4,001
pub param	64	254	3,302	254	254	64
signature	6,144	508	508	762	762	51,677

Fig. 1: Taxonomy to evaluate IBS schemes (all sizes in bits)

IBS has a sibling called Attribute Based Signatures (ABS) [16], which has to deal with a more difficult management of not only IDs, but also attributes. However, ABS could allow for additional features in comparison to IBS – for example group authentication (n:1), where the recipient is not part of the group.

III. Taxonomy for lightweight IBS schemes

For a comprehensive comparison and as a guideline for choosing a suitable IBS scheme in a given use case, this paper proposes a taxonomy based on the memory requirements and network load per scheme, with the following four parameters:

1) *Size of the usk*: The usk is re-computed during every re-keying action and communicated privately with the user.
2) *Size of the mpk*: The mpk is re-computed during every re-keying action and then broadcasted.
3) *Size of the pub params*: Public parameters need to be calculated and communicated only once.
4) *Signature size*: As the infrastructure is meant for authentication, signatures are usually exchanged frequently and should be as small as possible.

The sizes are given as the absolute values in bits required to grant a security equivalent to 128 Bit AES. In all schemes, the parameters only vary with the security level and do not depend on message- or ID-size. The measurements include pre-computed values as part of the public parameters. They can be represented in a spider chart where smaller (and therefore preferable) results are plotted closer to the center.

Please note that the size of the *pub params* needs to be weighted on a per scenario basis, as pre-computed values

[1] https://datatracker.ietf.org/wg/msec

might heavily decrease the computation overhead. A prominent example is given by comparing the two pairing-based schemes BLMQ and Hess. In BLMQ, the pairing function (see $e(P,P)$ in Table I) can be precomputed, which results in larger *pub params*. It can, however, significantly reduce the computation time for signing and verifying.

Figure 1 shows the comparison of six IBS-schemes on a logarithmic scale. Most of them are based on the Elliptic Curves Discrete Logarithm Problem (ECDLP), as they currently provide the best trade-off between key-length and security [17]. The comparison includes two of the best-known pairing-based IBS-schemes designed by F. Hess [18] and by Barreto et al. (BLMQ [19]). Two non-pairing based ECDLP schemes are also considered (GG [20], VBNN [21]). For comparison, the original scheme [5] proposed by Shamir, which is based on the hard problem of prime factorization is included along with the work of Xie et al. which discusses a lattice-based IBS Scheme (Xie [22]).

As expected, elliptic curve based schemes turn out to perform best in the chosen taxonomy, mostly due to their low resource consumption. The bad result of Xie does not surprise either as lattices are known for heavy resource requirements. However, they might become unavoidable with the emergence of quantum computers.

IV. An IBS based Authentication Infrastructure

A. System Design

With IBS, an authentication infrastructure can be modeled very closely to a group key infrastructure as standardized in RFC 4046 [4]. Adapting this model to IBS, the system design looks as depicted in Figure 2.

The *Group Member* (GM) is a (constrained) device which is willing to participate in a communication group, while the *Group Controller Key Server* (GCKS) acts as the TTP in the system. The GCKS generates a master key pair (see *setup* phase in Section II-A), consisting of a master public and secret key (*mpk* and *msk*) and the public parameters (*pub params*). The GCKS uses the *msk* to *extract* a private key for the identity of the GM – the user secret key (*usk*) – and sends it to the GM.

The latter is a security critical step during the setup of a communication group, as the secret key is sent over a potentially public link. Thus, the GM and GCKS need to set up a secure channel for the exchange, which demands an a priori exchange of credentials – typically in form of public keys. The credentials also need to prove that the given identity matches the cryptographic one. At first sight, it might seem odd for an authentication infrastructure to require another external public key infrastructure in order to work securely. However, this also holds true for any other authentication infrastructure (e.g. X.509, which requires an identity check by a national authority).

In addition to creating the *usk*, the GCKS also controls access to the group and authorizes potential group members. Thus, the same credentials can be used for the *Controller*. The components *Controller* and *Credentials* can be outsourced to an external service (e. g. X.509 for *Credentials* and LDAP for *Controller*).

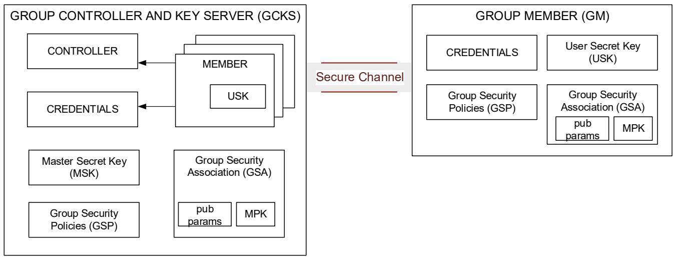

GROUP CONTROLLER AND KEY SERVER (GCKS)
CONTROLLER
MEMBER
USK
CREDENTIALS
Master Secret Key (MSK)
Group Security Association (GSA)
pub params
MPK
Group Security Policies (GSP)
Secure Channel
GROUP MEMBER (GM)
CREDENTIALS
User Secret Key (USK)
Group Security Policies (GSP)
Group Security Association (GSA)
pub params
MPK

Fig. 2: System design of GCKS and GM

The GCKS also stores so-called *Group Security Associations* (GSAs), which are distributed to all group members and include the *mpk* and the chosen IBS scheme's public parameters. In typical group systems, these GSAs also specify symmetric keys (e. g. for traffic encryption). They are therefore usually distributed using secure channels. That is not necessary if only the *mpk* is meant to be given out. In order to establish secure channels, well-known techniques from *Group Key Management* (GKM) can be used. A comparison of different techniques suitable for constrained environments can be found in [23].

Having received all parameters, the GMs can use their *usk* to *sign* messages and send them out with their signature and identity. Any recipient in possession of the *mpk* can use the sender's identity to generate the *upk* and *verify* the message. As long as the identity can be verified by the *Controller*, it can be anything (e. g. global IPv6 address). This IBS-specialty can be important to minimize traffic overhead.

In special scenarios, some devices might not be allowed to send but only to receive information, which is also covered by the given design. The *Controller* specifies which identities are suitable for *extracting* keys, but the *mpk* can still be distributed to other participants.

B. Access control with IBS

If group memberships change (e. g. a device entering or leaving the group) it can be necessary to replace the key material in order to ensure forward and backward secrecy. All GKM systems offer a re-key mechanism which (in a nutshell) uses the well-established secure channels to provide all GMs with new keys. Using IBS, re-keying can be a means to enforce group management actions, especially membership revocation. Please note that *joining* a group without backward secrecy is already covered by the *extract* functionality of IBS. Re-keying is not yet explicitly included in IBS-schemes and thus specified as follows:

Re-key: The GCKS renews its own key-pair (*msk* and *mpk*), *extracts* a new *usk* for each registered GM and distributes them through the secure channel. Additionally, the *mpk* is distributed globally. Unless explicitly changed, *pub params* remain untouched.

This function is applicable to any IBS scheme by design, as distributing new key material is equivalent to forming a

TABLE II: Memory required of the test setup

Feature	BLMQ	VBNN
RIOT kernel (incl. stack)	1,536 Byte	
RIOT 6LoWPAN cache	1,024 Byte	
RIOT IPv6 stack	1,024 Byte	
RIOT UDP stack	1,024 Byte	
RIOT net cache	1,216 Byte	
RIOT packet buffer	6,144 Byte	
∑ RIOT	11,968 Byte	
Relic cryptographic suite	10,772 Byte	5,060 Byte
IBS stack	18,432 Byte	12,288 Byte
∑ IBS	29,204 Byte	17,348 Byte
∑ Test Setup	41,172 Byte	29,316 Byte

new group. In case of a revocation, it is possible to indirectly exclude GMs by denying them access to a new *usk* corresponding to the new msk. Former members can then not sign messages, but may still have access to the publicly distributed *mpk* allowing them to verify messages. Revocation is thus solved simply and elegantly in IBS. The overhead expected from distributing key material during each re-keying action can be reduced using hierarchical IBS schemes, which is not subject of this work, but will be addressed in future research.

V. Evaluation

The tests were performed utilizing the *IoT-Lab*[2], in particular three M3 Nodes (72 Mhz ARM Cortex M3, 64 KB RAM) as constrained GMs in a multicast domain and one A8 Node (600 Mhz ARM Cortex A8, 256 MB RAM) acting as the GCKS. The firmware for the GMs is a RIOT-OS[3] with Relic[4] as the cryptographic library.

A. Measurements

The IBS implementation requires a maximum of ~41 KB of RAM (for BLQM, see Table II) and thus fits the 64 KB RAM of the IOT-Lab M3 nodes easily. There are two major RAM consumers, namely the Relic library and the memory required to store cryptographic material during IBS calculations. As BLMQ requires more cryptographic functionality, the memory consumption for the relic library is doubled in comparison to VBNN. Additionally, VBNN requires fewer parameters, which decreases the memory use.

Besides the memory requirements, the time for signing and verifying messages is tested, as well as the power consumption. In order to evaluate IBS for different scenarios, typical MTU sizes are chosen as message size (SigFox, Lora, IEEE 802.15.4, default BLE, Ethernet, typical Wifi) in addition to some larger cases of 4 and 8 KB (see Figure 3). The ID length is chosen according to typical address or name lengths (IPv4 address, MAC address, IPv6 address and 256 Byte URI as an extreme case). Every measurement represents the arithmetic mean of a set of 100 independent measurements.

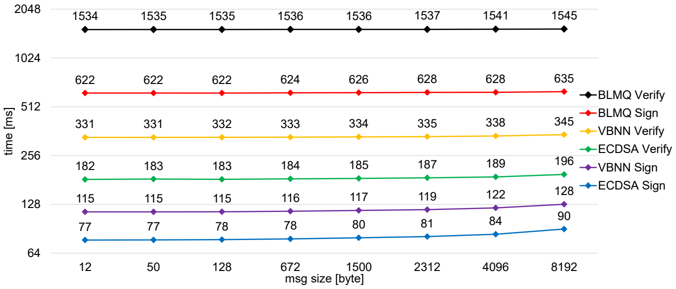


Fig. 3: Time (in milliseconds) for signing and verifying with BLMQ, VBNN and ECDSA for different message

It is worth noting that the relative standard deviation[5] ranges between 3.5 and 4.5 %.

The size of the ID only comes into play during the verification process when the public key needs to be calculated from the ID. The experiment showed that ID length has no significant influence on the required time for both signing and verifying. With the largest ID in the setup (here 256 Byte) the computation took ~1 ms longer than using shorter IDs, which is within the standard deviation. Increasing the size of the message increases the time for signing and verifying, which is due to the fact that hash calculations are more expensive for longer messages (see Figure 3).

The measurements confirm the expected behavior of IBS, but the most valuable result is the comparison of the two schemes. On average, VBNN is 5 times faster than BLMQ. This can be explained by the fact that BLMQ requires pairing, which is by far the heaviest operation, even though precomputation is enabled. In [19] the computational overhead of pairings was even calculated as up to 21 times. As a comparison, ECDSA using the same elliptic curve (BN-254) and hash function (SHA-256) is evaluated, which shows that VBNN has an overhead of around 50 % for signing and 75 % for verifying. This result shows that IBS fits best for scenarios where lower networking overhead is preferred over computation time.

The power consumption observed during computation of VBNN and BLMQ showed an overhead of ~70 mW to idling for both schemes. Figure 4 shows the consumption while signing and verifying one configuration set of Figure 3, proving that signing and verifying do not have different power requirements. Obviously, the higher computation time of BLMQ results in a higher energy consumption, which is an important information to be considered when running IBS with constrained power resources.

VI. Summary and Future Work

This work proposes the use of IBS for group communication in constrained scenarios. The theoretical analysis of IBS shows benefits over traditional authentication infrastructures, especially in terms of traffic overhead and group access control.

[2] `https://www.iot-lab.info`

[3] `https://riot-os.org`

[4] `https://github.com/relic-toolkit/relic`

[5] Given a set $\{x_1,..,x_n\}$ of n elements. Let $\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ be the arithmetic mean and $s = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2}$ be the standard deviation. The relative standard deviation is then defined as $s_{rel} = s/\overline{x}$.

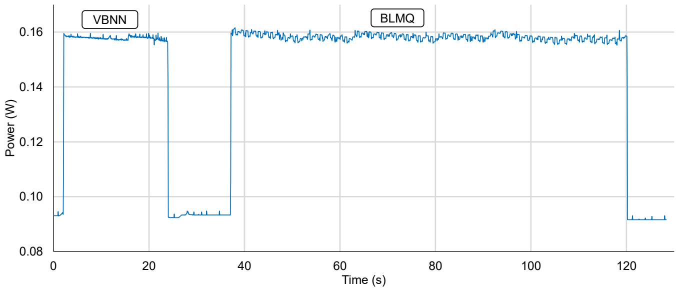


Fig. 4: Power consumption of BLMQ and VBNN.

However, IBS requires a very strong trust relationship to the key server; the suitability of this needs to be judged on a per scenario basis. With a strong focus on constrained environments, a taxonomy for easily choosing an IBS scheme is presented and a practical evaluation proves that especially VBNN could be a valuable tool, even for time-critical scenarios. The real strength of IBS comes into play in dynamic scenarios, where client participation varies frequently. This is why this paper introduced an integration of IBS in a typical group key management architecture that allows re-keying. To the best of our knowledge, this is the first analysis of IBS for group setups with actually constrained hardware.

Future Work

Our analysis only considers non-hierarchical schemes. As hierarchical schemes seem promising in order to reduce computational overhead even further, they will be subject of further research. The same holds for online / offline signature schemes which promise more economic computation of signatures. Efforts to solve key-revocation more efficiently in IBS are also underway. Additionally, efforts towards a more detailed evaluation will be made and a proposal for the inclusion of IBS into standardized key exchange protocols such as IKEv2, HIP or (D)TLS is planned.

Acknowledgment

The authors would like to thank Andrian Melnikov for his extraordinary work implementing and setting up the environment, which was necessary to perform the evaluation of the proposed architecture with some real-world IBS schemes. We also thank the MNM-Team for their valuable comments and especially Dr. David Schmitz for his initial idea on using IBS in group communication.

References

[1] R. Silva, J. S. Silva, M. Simek, and F. Boavida, “Why should multicast be used in WSNs,” in *IEEE International Symposium on Wireless Communication Systems 2008*, G. Qu, Ed. IEEE, 2008, pp. 598–602.

[2] D. D. A. McGrew and M. Pritikin, “The Compressed X.509 Certificate Format,” Internet Engineering Task Force, Internet-Draft draft-pritikin-comp-x509-00, May 2010, work in Progress (expired Nov. 2010). [Online]. Available: https://datatracker.ietf.org/doc/html/draft-pritikin-comp-x509-00

[3] N. gentschen Felde, T. Guggemos, and D. Kranzlmüller, “Secure Group Communication in Constrained Networks – A Gap Analysis,” in *Proceedings of the 1st IEEE Global IoT Summit*, vol. 2017, IEEE. Geneva, Switzerland: IEEE Xplore, Jun. 2017.

[4] R. Canetti, L. R. Dondeti, F. Lindholm, and M. Baugher, “Multicast Security (MSEC) Group Key Management Architecture,” RFC 4046, May 2005. [Online]. Available: https://rfc-editor.org/rfc/rfc4046.txt

[5] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer Berlin Heidelberg, 1984, pp. 47–53.

[6] M. Tiloca, K. Nikitin, and S. Raza, “Axiom: DTLS-Based Secure IoT Group Communication,” *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, pp. 66:1–66:29, Apr. 2017. [Online]. Available: http://doi.acm.org/10.1145/3047413

[7] W. Werner, A. Somaraju, S. S. Kumar, and H. Tschofenig, “Security for Low-Latency Group Communication,” Internet Engineering Task Force, Internet-Draft draft-somaraju-ace-multicast-02, Oct. 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-somaraju-ace-multicast-02

[8] J. Baek, Y.-J. Byon, E. Hableel, and M. Al-Qutayri, “An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature,” in *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2013, pp. 358–363.

[9] D. Wang, B. Da, J. Li, and R. Li, “IBS enabled authentication for IoT in ION framework,” in *Proceedings of the 1st IEEE Global IoT Summit*. Piscataway, NJ and Piscataway, NJ: IEEE, 2017, pp. 1–6.

[10] R. Yasmin, E. Ritter, and G. Wang, “An authentication framework for wireless sensor networks using identity-based signatures: Implementation and evaluation,” vol. 95-D, pp. 126–133, 01 2012.

[11] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,” *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” in *Proceedings*. IEEE Computer Society, 2000, pp. 56–73.

[13] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security protocols for sensor networks,” *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[14] A. Perrig, “The BiBa One-time Signature and Broadcast Authentication Protocol,” in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, ser. CCS ’01. New York, NY, USA: ACM, 2001, pp. 28–37.

[15] X. Yao, X. Han, X. Du, and X. Zhou, “A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693–3701, 2013.

[16] X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the Internet of Things,” *Future Generation Computer Systems*, vol. 49, pp. 104–112, 2015.

[17] M. Sethi, J. Arkko, A. Keränen, and H.-M. Back, “Practical Considerations and Implementation Experiences in Securing Smart Object Networks,” Internet Engineering Task Force, Internet-Draft draft-ietf-lwig-crypto-sensors-05, Dec. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lwig-crypto-sensors-05

[18] F. Hess, “Efficient Identity Based Signature Schemes Based on Pairings,” in *Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 310–324.

[19] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, “Efficient and provably-secure identity-based signatures and signcryption from bilinear maps,” in *Advances in Cryptology- Asiacrypt 2005*. New York: Springer, Jan. 2006, vol. 3788, pp. 515–532.

[20] D. Galindo and F. D. Garcia, “A Schnorr-Like Lightweight Identity-Based Signature Scheme,” in *Progress in Cryptology – AFRICACRYPT 2009: Second International Conference on Cryptology*, B. Preneel, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 135–148.

[21] X. Cao, W. Kou, L. Dang, and B. Zhao, “IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks,” *Computer Communications*, vol. 31, no. 4, pp. 659–667, 2008.

[22] J. Xie, Y. Hu, J. Gao, and W. Gao, “Efficient identity-based signature over NTRU lattice,” *Frontiers of Information Technology & Electronic Engineering*, vol. 17, pp. 135–142, 2016.

[23] N. gentschen Felde, T. Guggemos, T. Heider, and D. Kranzlmüller, “Secure Group Key Distribution in Constrained Environments with IKEv2,” in *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, Taiwan, 2017.