Towards a Cryptography Benchmark: A View on Attribute Based Encryption Schemes

Thomas Prantl†, Timo Zeck†, Lukas Iffländer†, Lukas Beierlieb†, Alexandra Dmitrenko†,
Christian Krupitzer‡ and Samuel Kounev†
†{firstname.lastname}@uni-wuerzburg.de, University of Würzburg
‡{christian.krupitzer}@uni-hohenheim.de, University of Hohenheim

2022 5th Conference on Cloud and Internet of Things (CIoT) | 978-1-6654-7964-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/CIOT53061.2022.9766494

***Abstract*—In many Internet-of-Things (IoT) scenarios — such as smart home, or intelligent traffic systems — groups of devices interact with each other. Such scenarios no longer require encryption for individual recipients but for groups of recipients, i.e., this is a shift towards 1-to-n and n-to-n encryption schemes. Developers must select the scheme that (1) offers the required functional encryption features, (2) has the non-functional requirements best fitting the specific use case, and (3) is the most performant in the specific group setting. In other research domains, benchmarks help to support researchers, but also practitioners, in the choice of the best technology for a specific use case. However, there is no benchmark for encryption schemes available that covers all different types of encryption schemes, like 1-to-n and n-to-n encryption. In this paper, we provide such a benchmark for the category of attribute-based encryption schemes (ABE), especially focusing on the workloads, measurement setup, metrics, requirements, and features for an attribute based 1-to-n encryption scheme benchmark. Additionally, we describe how to include n-to-n encryption schemes. Lastly, we apply the benchmark to compare attribute-based encryption schemes among and with n-to-n group encryption schemes. Our result indicate that (1) our benchmark is suitable for evaluating ABE schemes as 1-to-n and n-to-n ciphers, (2) there is no single scheme that performs best in all scenarios and (3) with ABE schemes extended to n-to-n encryption schemes, a combination of constant computation times and an efficient use of broadcast is possible, which is not the case with traditional n-to-n encryption schemes.**

***Index Terms*—Attribute-based Encryption, Performance**

I. Introduction

In today's era of digital transformation, we are seeing the emergence of new services and a revolution of user experience through new technologies like 5G. For example, online platforms such as Spotify or Netflix make films and music digitally accessible to their millions of users [1], [2]. Similar platforms also exist in the gaming industry, for example, where Steam or Battle.net provide video games digitally to an audience of millions [3], [4]. Alongside this boom in cloud applications, we are seeing the synergy of the physical and digital worlds through the integration of billions of low-cost Internet-of-Things (IoT) devices into physical objects. Through these billions of IoT devices, smart applications, such as autonomous driving cars, autonomously forming so-called platoons exploiting slipstream effects to save energy, enhance our everyday lives.

978-1-7281-8688-7/22/31.00 ©2022$IEEE$

It is essential for all these new applications that operators can control data provision and access privileges. Otherwise. Game developers, for example, lose money when users access their games without paying. In addition to such financial losses, however, lives could also be endangered if, for the example of self-driving cars, hackers inject false data into the system and thereby provoke car accidents.

These services implement this form of access control using encryption techniques. As the previous examples show, data no longer needs to be encrypted for individual recipients but for groups of recipients. For example, control instructions encryption for cars driving independently in a platoon must work not only for one platoon member but for the entire platoon. A wide variety of 1-to-n and n-to-n encryption schemes emerged over the years to avoid having to encrypt the message individually for each member (1-to-1 encryption). From this multitude of encryption schemes, developers must select the scheme that (1) offers all the features — such as hiding the identity of the recipient of an encrypted message [5] — required by the specific use case, (2) whose requirements — such as the efficient use of broadcast [6] — fit the specific use case, and (3) is the most performant choice for the specific use case. This choice ideal relies on the base of a benchmark covering all types of encryption (1-to-1 [7], 1-to-n and n-to-n) and considering not only performance but also the features and requirements of the schemes.

However, no such all-encompassing benchmark exists in the literature, since there are already three completely different implementation types — centralized, decentralized, hybrid — for the n-to-n encryption methods alone, for which no common benchmark exists [6]. Considering the fact that encryption schemes originally developed, for example, for 1-to-n encryption can also suit the demands for n-to-n encryption schemes further complicates the creation of an all-encompassing benchmark. We envision such a benchmark and want to contribute a first step towards its realization by creating a sub-benchmark for the category of attribute-based encryption schemes (ABE), which originally belong to the centralized 1-to-n encryption schemes. Our ABE benchmark should also allow the comparison with centralized n-to-n encryption schemes and be compatible with our existing benchmark for centralized n-to-n encryption schemes [6]. More specifically, our contributions are:

- the description of workloads, measurement setup, metrics,

requirements, and features for an attribute-based 1-to-n encryption scheme benchmark;
- extension of the attribute-based encryption scheme benchmark for 1-to-n encryption to n-to-n encryption;
- the benchmarking and comparison of attribute-based 1-to-n encryption schemes with each other and n-to-n group encryption schemes.

The remainder of this paper is structured as follows. In Section II, we show how 1-to-n encryption schemes can be extended to n-to-n encryption schemes and introduce the concept of ABE schemes. We then present our benchmark for ABE schemes in Section III and apply it to state-of-the-art ABE schemes in Section IV. We then extend our ABE benchmark with respect to n-to-n encryption schemes in Section V and use our extended benchmark to compare ABE schemes with n-to-n group encryption schemes in Section VI. Finally, we highlight the novelties of our contributions by comparing them with related work in Section VII and summarize our paper in Section VIII.

II. Background

In this section, we introduce the basic concept of ABE schemes and we show how 1-to-n encryption can be extended to n-to-n encryption.

A. Concept of ABE Schemes

Figure 1 illustrate the concept of ABE schemes involving four different entities, namely a cloud, an authority, a data owner (DO) and a data user (DU) [8]. The cloud is there only as a means of communication between the DO and DUs. Each DU has a set of attributes, for example, in Figure 1 Bob is a computer science student, Carl is a civil engineering student and Alice is a teacher. Based on these attributes, the authority creates the public and secret keys for the DO and the DUs. The goal of ABE schemes is to enable the DO to share its encrypted data only with DUs who have certain attributes. In the example illustrated in Figure 1, for example, the DO wants to share its data only with Alice and Bob, but not with Carl. To achieve this, an access policy must allow Alice and Bob to decrypt the data, but must not allow Carl to decrypt the data. There are different ways for ABE schemes how to specify such an access policy — e.g., threshold policies, AND policies, tree policies, and the linear secret sharing scheme matrix [8]–[10]. However, all access policies represent boolean formulas. For our example, an access policy could math the following boolean formula: `((Name: Alice) OR (Name: Bob))`. Either the Authority must encode the policy into the secret key of the DOs, or the DOs must encode it into the ciphertext.

In addition to the terms introduced so far, we still need to introduce the terms attribute universe, CI, and group member in the context of ABE schemes for the understanding of the later sections. By *attribute universe*, we mean the set of existing attributes. In our example, this set would be {Role, Name, Degree Program}. Furthermore, we assume in the following that the authority and the data owner are the same entity, and we again call this entity the Central Instance,

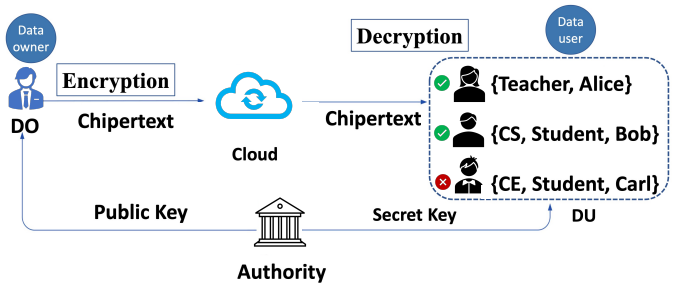

Fig. 1: Concept of ABE schemes, illustrated in the style of [11].

or short CI. For later comparability of ABE schemes with n-to-n group encryption schemes, we also refer to the DOs as group members in the following.

B. Extension from 1-to-n encryption to n-to-n encryption

In the case of 1-to-n encryption, we have n+1 communication participants. One of these participants, which we denote as the CI, can encrypt messages in such a way that only the remaining n participants can decrypt them. Thus, the other n group members can receive messages from the CI, but they can not send encrypted messages to the other participants themselves. However, the CI can easily change this through generating a symmetric key and sending it encrypted to the n other participants. This way, all n+1 participants have the same symmetric key, which they can use to send encrypted messages to the other participants, who in turn can decrypt them. Thus, a 1-to-n encryption becomes an n-to-n encryption. Literature calls this approach the Simple Key Distribution Center [12].

III. ABE Benchmark for 1-to-n Encryption

We propose in this section a benchmark for ABE schemes used for 1-to-n encryption schemes to approach an all-encompassing cryptography benchmark for encryption schemes. Since we want to extend the ABE benchmark for 1-to-n encryption schemes to n-to-n encryption schemes in the following sections, it is important to keep the ABE benchmark compatible to the already existing benchmark [6], which was specifically designed for centralized n-to-n encryption schemes and has already proven its suitability in benchmarking centralized post-quantum n-to-n encryption schemes ([13], [14]). Accordingly, analogous to [6], we proceed in this section in presenting the ABE benchmark for 1-to-n encryption schemes and (i) first define requirements and features of ABE schemes and then present (ii) workload patterns, (iii) measurement environments, and (iv) metrics for ABE schemes.

A. Requirements and Features

Requirements: In order to be able to extend our ABE benchmark for 1-to-n encryption schemes to n-to-n encryption schemes later on in such a way that it is compatible with the benchmark for centralized n-to-n encryption schemes [6] and and since the requirements for n-to-n encryption schemes also

apply to 1-to-n encryption schemes, we adopt the requirements from [6]. The requirements from [6] are namely topology and confidentiality. Topology describes whether unicast is required or whether broadcast is sufficient, and confidentiality whether the content of the respective communication is confidential or not.

Features: Analogous to the requirements, we adopt the following features from the benchmark for n-to-n encryption schemes [6]: group size limit, group backward, and forward secrecy. Group size limit describes whether it is possible for the participants of the 1-to-n communication to calculate the corresponding parameters for groups of any size in order to participate in this communication in encrypted form. Backward/Forward secrecy describes, if members, added to or removed from the group, do have access to data transmitted before joining or after leaving the group. We assume that backward/forward secrecy is present when the addition/revocation of participants triggers an immediate corresponding adjustment of the used keys.

To these four features we add receiver anonymity and accountability, determined by our analysis of multiple ABE schemes [15]–[19]. A scheme fulfills receiver anonymity if it prohibits retrieving the recipient from an encrypted message. For example, the scheme in [15] offers this feature, whereas the scheme in [16] does not. Accountability describes if an ABE scheme includes user accountability and tractability. For example, in the ABE scheme [16], the actions of the CI are traceable, and in the ABE scheme [17], the actions of the users are traceable. However, there are also ABE schemes that offer no traceability at all [16]. These two new properties are not only interesting for 1-to-n encryption ABE encryption schemes, but also for n-to-n encryption schemes. Even for n-to-n encryption schemes it can be important that attackers can not identify group members which would allow an attacker, for example, to selectively shield individual group members from group communication. The traceability of actions is also important for n-to-n encryption, since traitors in the group who pass on group messages to unauthorized persons can be identified and removed from the group.

B. Workload Pattern

Analogous to the benchmark for n-to-n encryption schemes [6], our workload patterns for ABE schemes also describe group management operations (comprising group creation and member addition/revocation) and the actual group communication. We define them using the same notation as in [6]. Regarding group communication, we distinguish the CI workload patterns (see Definition 1) and member patterns (see Definition 2).

Definition 1. *$WP_{CI,enc}(N, B, A, U)$: The CI encrypts a message N times, which initially consists of B Bytes, for group members with the access policy A from the attribute universe U using the corresponding public key.*

Definition 2. *$WP_{group\ member,dec}(N, B, A, U)$: A group member, with the access policy A from the attribute universe U, decrypts a message N times, which initially consists of B Bytes, using its private key.*

Regarding group management operations, we additionally distinguish in which phase they take place. Thus, we call the phase in which the CI generates the public key and the secret private keys the operational and deployment phase. Beside group creation, we also consider the subsequent member addition and removal. We describe the associated workloads from the point of view of the corresponding actor, which is in the case of ABE schemes only the CI. The reason we do not define workloads for group members is that their only task in group management operations is storing secret keys during the deployment phase. This storage operation is negligible in our opinion. Definition 3 and 4 define the CI workloads for the initial creation of a group in the deployment and operational phase. Furthermore, Definition 5 and 6 give CI's workloads for the subsequent member addition/removal in the deployment and operational phases.

Definition 3. *$WP_{CI,creation,deployment}(N, S, A, U)$: The CI creates a group with S members having the same access policy A from the attribute universe U by computing the corresponding S secret keys N times in a row.*

Definition 4. *$WP_{CI,creation,operational}(N, S, A, U)$: The CI creates a group with S members having the same access policy A from the attribute universe U by computing the corresponding public key N times in a row.*

Definition 5. *$WP_{CI,addition/revocation,operational}(N, S, A, U)$: The CI adds/revoked a group member with access policy A from the attribute universe U to/from a group with S members having the same access policy A from the attribute universe U by updating the corresponding public key N times in a row.*

Definition 6. *$WP_{CI,addition/revocation,deployment}(N, S, A, U)$: The CI adds/revoked a member with access policy A from the attribute universe U to a group with S members having the same access policy A from the attribute universe U by updating/calculating the corresponding secret keys N times in a row.*

C. Measurement Testbed

Since (i) IoT scenarios typically consist of many devices communicating in a group, (ii) IoT devices are typically resource-constrained resulting in the need to benchmark ABE schemes on such devices as well, and (3) we want to be compatible with the benchmark for n-to-n encryption [6], we adopt the IoT measurement environment from [6].

The measurement setup from [6] comprises an ESP32, a 32-bit microcontroller, to implement a group member. To measure the power consumption of the ESP32, we recommend the use of a Yokogawa WT310 power meter [6] because of its accuracy in the appropriate measurement range $\pm$(0.1% of reading + 0.0006 watts) [20] which fits IoT devices. The recommended CI in [6] is a commercially available laptop,

more specifically the Lenovo B50-50 80S2004AGE with an Intel® Core™ i3-5005U 2x 2.00 GHz, Intel® HD Graphics 5500 shared memory, 4 GB RAM and 500 GB HDD running Ubuntu 16.04.4 LTS, which we also use.

D. Metrics

Since the metrics from [6] for n-to-n encryption schemes also apply to 1-to-n encryption schemes, we adopt them and thus are also compatible with [6]. We adopt the metrics storage requirements, computation times, and energy efficiency and present them briefly in the following.

Storage Requirements: The average memory required for keys to be stored permanently or data to be stored temporarily for updating keys or decrypting messages.

Computation Times: The computation time $\bar{t}_A$ for an action A is the average time required to execute action A n times in a row, see Equation 1. The accuracy of $\bar{t}_A$ is $\Delta\bar{t}_A$ from Equation 2, in which $\Delta t_{A,i}$ stands for the accuracy of the measured time required to perform the i-th action A.

$$\bar{t}_A = \frac{1}{n}\sum_{i=1}^{n} t_{A,i} \quad (1) \qquad \Delta\bar{t}_A = \frac{1}{n}\sqrt{\sum_{i=1}^{n}\Delta t_{A,i}^2} \quad (2)$$

Energy Efficiency: The energy efficiency E is the throughput T_A to power consumption W ratio from Equation 3. Equation 4 defines The accuracy of E as ΔE in.

$$E = \frac{\text{Throughput}}{\text{Power Consumption}} = \frac{T_A}{W} \quad (3)$$

$$\Delta E = \sqrt{\frac{\Delta T_A^2}{W^2} + \frac{T_A^2 * \Delta W^2}{W^4}} \quad (4)$$

For the calculation of the energy efficiency we require the parameters average power consumption W, its accuracy ΔW, the throughput T_A for an action A and its accuracy ΔT_A. Equations 6 and 7 give the corresponding formulas. Thereby, ΔW_i is the accuracy of the measured power consumption during the i-th second. T_A from Equation 7 is the weighted number of performed actions A during a period t_p. Thereby the parameter W_A in Equation 7 computes as follows: W_A is the number of decrypted or encrypted bits for decryption and encryption actions. For all other actions, we set W_A to the value 1. Equation 8 gives the accuracy of T_A as ΔT_A.

$$W = \frac{1}{n}\sum_{i=1}^{n} W_i \quad (5)$$

$$\Delta W = \frac{1}{n}\sqrt{\sum_{i=1}^{n}(0.1\% * W_i + 0.0006 * W)^2} \quad (6)$$

$$T_A = \frac{W_A * |A|}{t_p} \quad (7) \qquad \Delta T_A = \frac{W_A * |A| * \Delta t_p}{t_p^2} \quad (8)$$

We augment the metrics of the benchmark for n-to-n encryption from [6] with the aspect of how many groups the CI can create using the information distributed in Deployment Phase. We denote these metrics as *Parallel group amount*, and the value range of this metric consists of the natural numbers.

IV. Benchmarking of ABE schemes used for 1-to-n encryption

To analyze the suitability of our ABE benchmark, we apply it to the three exemplary selected ABE schemes [19], [18] and [17]. Due to space limitations, we cannot discuss all aspects of our ABE benchmark and, therefore, focus on the analysis of features, requirements, computation times, memory requirements, and the number of parallel groups. Regarding group management operations, we focus on group creation and group message encryption and decryption. We begin by analyzing the features and requirements of the ABE schemes under consideration, followed by a performance analysis from (i) the group member's perspective and (ii) the CI's perspective. A discussion of the comparison of the three considered ABE schemes concludes this section.

A. Feature and Requirement Analysis

Table Ia lists the requirements of the various group management operations of the considered ABE schemes. Based on this table, the following conclusions result: 1) the schemes have the same requirements regarding group creation and adding members, and 2) only the scheme [18] has requirements for removing members, since only the scheme in [18] supports this operation. Table IIa lists the features of the considered schemes and shows that all schemes have the same features except for accountability. Schemes [19] and [17] provide user accountability, while scheme [18] does not.

B. Group Member Performance

Figure 2 presents the duration required by a group member to decrypt a message from the CI. Thereby the message consists of 128 bytes since most messages in the IoT are small and often comprise less than 40 bytes [22]. The power of the attribute universe has been varied from one attribute to 50 attributes, and there are always as many group members as attributes. Our used exemplary access policy is a connection of all attributes using the logical AND operator. Figure 2 allows the following statements about the considered schemes and measurement range, 1) all schemes increase linearly with the number of attributes of the universe and 2) the schemes rank ascending bei their computation times as follows: [19], [17], [18]. And 3) that ABE schemes can be used on IoT devices with complex access policies. However, conventional methods are significantly faster if you consider that a message encrypted using AES256 takes the ESP only a few hundred milliseconds to decrypt, whereas ABE schemes need more than 50 seconds for a universe with 50 attributes. In order for group members to decrypt messages at all, they must permanently store a secret key and temporarily store a cipher text. The memory required for this is shown in Figure 3 and 4 respectively, where Figure 3 illustrates the memory requirement for the secret keys and Figure 4 illustrates the

TABLE I: Requirements of the group management operations of the ABE schemes [19], [18] and [17] and the n-to-n group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$.

		[19]				[18]				[17]			
		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential	
		uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no
Group Creation	Deployment	✓		✓		✓		✓		✓		✓	
	Operational		✓		✓	✓			✓	✓			✓
Member revocation		n.d	n.d	n.d	n.d		✓		✓	n.d.	n.d.	n.d.	n.d.
Member Addition	old		✓		✓		✓		✓		✓		✓
	new		✓		✓		✓		✓		✓		✓

(a) Requirements of ABE schemes [19], [18], [17]. (If a schema does not support a group management operation, we mark the respective requirements with "not defined" or abbreviated n.d.)

		$BASE$ [12]				$Nishat$ [21]				$Boneh{+}_{\text{Fat Client}}$				$Boneh{+}_{\text{Thin Client}}$			
		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential	
		uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no
Group Creation	Deployment	✓		✓		✓		✓		✓		✓		✓		✓	
	Operational	✓			✓		✓		✓		✓		✓	✓			✓
Member revocation		✓			✓		✓		✓		✓		✓	✓			✓
Member Addition	old	✓			✓		✓		✓		✓		✓	✓			✓
	new	✓			✓		✓		✓		✓		✓	✓			✓

(b) Requirements of the n-to-n group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$.

TABLE II: Features of pre- and post-quantum group encryption schemes.

Schemes / Features	[19]	[18]	[17]
unlimited group size	depending on universe size	depending on universe size	depending on universe size
backward secrecy	✓	✓	✓
forward secrecy	✓	✓	✓
anonymity	✗	✗	✗
accountability	user	✗	user

(a) Features of ABE schemes [19], [18] and [17]

Schemes / Features	$Base$ [12]	$Nishat$ [21]	$Boneh$ Thin Client	$Boneh$ Fat Client
unlimited group size	✓	✗	✓	✗
backward secrecy	✓	✓	✓	✓
forward secrecy	✓	✓	✓	✓
anonymity	✓	✓	✓	✓
accountability	✗	✗	✗	✗

(b) Features of n-to-n group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$

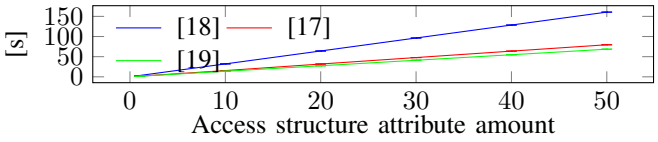

Fig. 2: Message from the CI decryption time for different sized attribute universes of the ABE schemes [19], [18] and [17]

memory requirement for the cipher text. On the basis of these two figures, the following statements can be made for the used measurement range and ABE schemes under consideration:

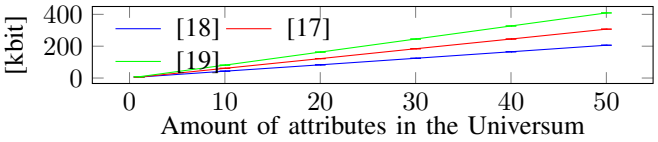

Fig. 3: Size of the secret keys of the ABE schemes [19], [18] and [17] for diffrent sized attribute universes

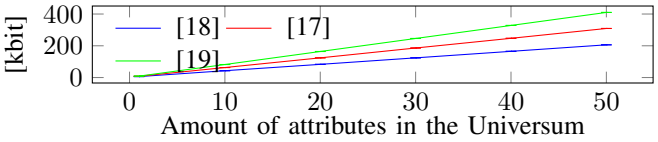

Fig. 4: Cipher text key sizes of the ABE schemes [19], [18] and [17] for different sized attribute universes

1) both the secret keys and the cipher texts increase linearly with the size of the universe, and 2) the methods can be arranged in ascending order with respect to both the size of the secret keys and cipher text sizes as follows: [18], [17], [19].

C. CI Performance

The CI must first compute the corresponding secret keys for all group members for the CI to send encrypted messages to all group members, In addition, the CI must compute a public key for itself that he uses to encrypt messages for the group members so that they can decrypt the message using their secret keys. Figure 5 shows the required time for the

key computation in the deployment and operational phase[1]. Figure 5 allows for the considered schemes and measurement range the statements that 1) the time for the deployment and operational phase increases linearly with the size of the universe and that 2) the schemes can be listed in ascending order by their computation times as follows: [18], [17], [19].

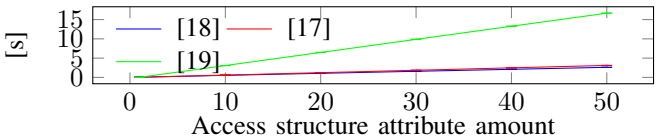

Fig. 5: Time needed by the ABE schemes [19], [18] and [17] for the Deployment and Operational Phase for different access structures

Figure 6 illustrates the time required by the CI to encrypt a message using the public key generated in the operational phase. Also, for encrypting messages it is true that 1) the required time increases with the size of the universe and 2) that the schemes can be unambiguously ordered with respect to the required time as follows: [18], [17], [19].

As a last metric, we consider the amount of parallel groups the CI can create using the keys created in the deployment phase. For an attribute universe U, the CI can generate $2^{|U|}$, $2^{|2U|}$, or $2^{|2U|}$ groups, respectively, if it uses the scheme [19], [18], and [17], respectively.

D. Interpretation of the Results

Our evaluations show that none of the ABE schemes performs best everywhere in the measurement range considered. The scheme [18] is always the fastest in terms of computation times, apart from when decrypting messages, and allows for the most parallel groups. However, it has the highest memory requirements and does not offer the feature accountability. But [18] is also the only scheme that supports removing group members. The following statements can be made about the two schemes [19] and [17] that provide accountability, but can't remove group members: (1) with respect to storage requirements, encryption, deployment, and operational times, [17] performs better than [19], (2) with regard to decryption times and the number of possible parallel groups, [19] outperforms [17].

[1]Note: (1) For space reasons we evaluate the deployment and operational phase together and not separately. (2) Again we assume that there are as many users as attributes.

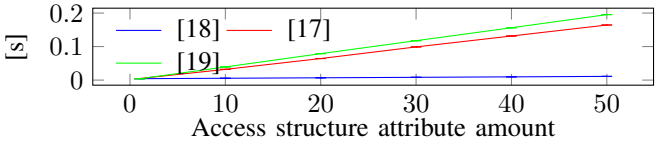

Fig. 6: Required time of the CI for encrypting a message to the group members for ABE schemes [19], [18] and [17] for different sized attribute universes.

V. ABE Benchmark for n-to-n Encryption Schemes

After presenting and applying our benchmark for ABE schemes as 1-to-n encryption schemes, we extend this benchmark for ABE schemes used as n-to-n encryption schemes. For the ABE benchmark for n-to-n encryption schemes, we extended the ABE schemes originally developed for 1-to-n encryption to n-to-n encryption according to Section II.A. Based on this assumption, our benchmark for ABE schemes used for n-to-n encryption is mostly equivalent to our ABE benchmark for 1-to-n encryption. The only differences are in the workload definitions, both in terms of communication among group members and group management operations. We explain them in the following.

The new workloads with regard to group communication correspond to our previous Definitions 1 and 2, except that encryption and decryption are now each performed with the symmetric group key. Regarding the group management workloads, the workloads change in the operational phase, see Definitions 4 and 5. They change in that the CI additionally encrypts a newly generated symmetric key N times using the new generated public key. Furthermore, there is an additional workload for the group members, since they do not just have to store keys. They now have to decrypt the symmetric key, which they need to communicate with the other group members, in the operational phase after it has been encrypted by the CI, using their secret key. This corresponds to the workload from Definition 1, where B is the length of the symmetric key in this case.

VI. Comparison of ABE schemes with group encryption schemes

In this section, we compare the considered ABE from Section IV with group encryption schemes, using the extended ABE benchmark from Section V. As group encryption schemes we use the three schemes $BASE$, $Boneh$, and $Nishat$ which we also used in the n-to-n group encryption scheme benchmark [6]. For $Boneh$, the work in [6] considers two different implementation options, which distributes the main computational burden to either the CI or the group members. We designate the first variant as $Boneh{+}_{\text{Thin Client}}$ and the second as $Boneh{+}_{\text{Fat Client}}$.

Due to space limitations, we can again not discuss all aspects of our extended benchmark. Therefore, we focus on the creation of groups and the analysis of features, requirements, computation times, memory requirements and the number of parallel groups from a group member's perspective.

A. Feature and Requirement Analysis

Tables Ia and Ib list the group encryption and ABE scheme requirements. These two tables show that ABE schemes have lower requirements regarding their environment. Thus, broadcast is sufficient for all ABE schemes considered, while only $Nishat$ and $Boneh{+}_{\text{Fat Client}}$ can manage with broadcast and both $Boneh{+}_{\text{Thin Client}}$ and $Base$ require unicast. However, all considered group encryption schemes support the removal of members, while [18] is the only ABE scheme to support it.

Tables IIa and IIb list the features of the ABE and group encryption schemes. The tables show that none of the group encryption schemes provides the accountability feature, but all ABE schemes do so. On the other hand, the two group encryption schemes $Nishat$ and $Boneh+_{\text{Fat Client}}$ allow group members to join groups of arbitrary size, which is not the case with the ABE schemes. In the considered ABE scheme, joining a group is independent of the number of group members but depends on the number of attributes in the universe. In addition, all group encryption schemes provide feature anonymity.

B. Group Member Performance

A group member must first compute the symmetric group key from the CI's message to join a group. Figures 2 and 7 show the times required by ABE and group encryption schemes. Please note that for the ABE schemes, the calculation of the group key consists of decrypting a message from the CI. Comparing these two figures leads to a remarkable conclusion. The group key calculation time of ABE schemes is independent of the group size and depends only on the size of the universe and the used access policy. Considering a universe of size 1 and an access policy that presupposes this one attribute, the ABE schemes under consideration take around 1.5 seconds to compute the group key. Almost in the same order of magnitude as the group encryption schemes. On the group encryption scheme side, only the schemes $BASE$ and $Boneh_{\text{Thin Client}}$ provide this independence from the group size. The calculation times of $Nishat$ and $Boneh_{\text{Fat Client}}$ increase linearly with group size, albeit very slowly. However, the schemes $BASE$ and $Boneh_{\text{Thin Client}}$ provide this property by requiring their CI to send individualized messages to their group members, which prevents them from using broadcast efficiently. The ABE schemes, on the other hand, can all use broadcast. Thus, ABE schemes are the only way to have group key calculation times independent of the group size and at the same time be able to use broadcast efficiently. This combination is especially interesting for IoT use cases, since IoT communication typically relies on broadcast protocols like MQTT. Another advantage of ABE schemes is that they not only allow the CI to create multiple groups using the keys distributed in the deployment phase, but also allow group members to be in more than one group using these keys.

A similar picture emerges for the permanently required memory with regard to the secret keys. Figures 3 and 8 show the storage requirements for ABE and group encryption schemes. Again, for ABE schemes, the memory requirement depends only on the size of the universe, but not on the group size, as it is the case with group encryption schemes. On the group encryption scheme side, only the $Nishat$ and $Base$ schemes have costs independent of the group size, while the memory requirements of the schemes $Boneh_{\text{Thin Client}}$ and $Boneh_{\text{Fat Client}}$ increase linearly with the group size. Considering again a universe of 1, the memory requirement of the ABE schemes is less than 10 kBit, which is in the same order of magnitude as for the group encryption schemes $Nishat$ and $Base$.

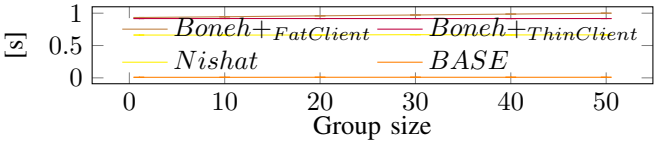

Fig. 7: Time needed by group members to calculate the group key during group creation for group encryption schemes [21], [12] and $Boneh+$ for different group sizes

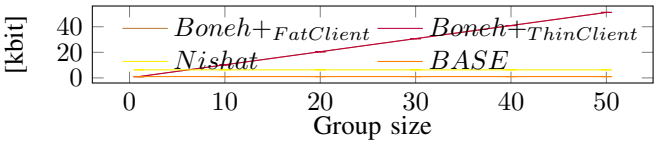

Fig. 8: Size of the secret keys of the group encryption schemes [21], [12] and $Boneh+$ for diffrent sized attribute universes (Note: Only $Boneh+_{\text{Thin Client}}$ can be seen in the graphic, as this covers $Boneh+_{\text{Fat Client}}$)

VII. Related Work

In this section, we present related work and highlight the innovations of our contributions. Related work can be divided into the following two groups: (1) theoretical comparisons and (2) practical comparisons. In the following, we first present the theoretical and then the practical performance comparisons.

Theoretical comparisons of ABE schemes take place in corresponding surveys [8], [10], [23] evaluating performance using the Landau notation. These estimations give first performance reference points for developers. However, they make no precise statements about, e.g., necessary computation times or the memory requirement.

In [24], the authors compared the practical performance in terms of storage space requirements, energy efficiency, and the computation times of the encryption and decryption process and key generation. For the performance measurements, they considered different attribute universes sizes. We, on the other hand, determine the performance for our metrics not only for different sized attribute universes but also for different access policies. Furthermore, we introduced the metric Parallel Group Amount and considered — besides pure performance — also the features and requirements of the ABE Schemes. However, our biggest novelty is that we make ABE schemes and n-to-n schemes comparable.

The authors of [25] consider the practical performance of ABE schemes in terms of the memory requirements of the cipher text and the time required for encryption depending on the attribute universe's size. We additionally consider the memory requirements for the corresponding keys, and the computation times for decrypting and generating the keys. Furthermore, we consider not only different sized attribute universes but also different access policies and introduce the metric *Parallel Group Amount*. We also consider the features and requirements

of ABE schemes, and establish comparability of ABE schemes and n-to-n group encryption schemes ciphers.

In [26], the authors consider the computation times and energy efficiencies of the encryption and decryption process of ABE schemes for different attribute universe sizes in practice. We additionally consider different access policies and also take the memory requirements for chip texts and keys into account. Additionally, [26] misses the comparison of ABE schemes to n-to-n group encryption schemes which is a part of this paper.

The authors of [27] consider the practical performance of ABE schemes regarding computation times and cipher text size for a fixed-sized attribute universe and fixed access policy. We, on the other hand, also consider the encryption process and the key generation. Furthermore, we consider different attributes and access policies.

VIII. Conclusion

In this work, we presented a benchmark for group encryption schemes for attribute-based encryption schemes (ABE), especially focusing on the workload definition, measurement setup, metrics, requirements, and required features. Additionally, we describe how to include n-to-n encryption. We applied the benchmark to compare attribute-based encryption schemes among and with n-to-n group encryption schemes to show the applicability of the benchmark. Our results indicate that our benchmarks enable the comparison between different categories and help to identify the best working scheme. E.g., ABE n-to-n encryption schemes can offer constant calculation times for group creation and efficient broadcast usage, while none of the original schemes provides this combination.

As future work, we plan to extend our benchmark and measure further aspects, such as energy efficiency or more complicated access policies. In addition, we want to evaluate other ABE schemes, consider different network situations using the tools [28] and [29] and generalize the results to other domains besides IoT systems. Further, as the benchmark showed that there is no scheme superior in all situation, we plan to integrate situation-awareness. Such a situation-aware mechanism can switch the encryption scheme based on the current system situation based on self-learning decision-making, e.g., following a self-aware computing systems approach [30].

Acknowledgment

This research has been funded by the Federal Ministry of Education and Research of Germany in the framework KMU-innovativ — Verbundprojekt: Secure Internet of Things Management Platform - SIMPL (project number 16KIS0852) [31].

References

[1] S. R. Department, "Anzahl der zahlenden Streaming-Abonnenten von Netflix weltweit vom 3. Quartal 2011 bis zum 1. Quartal 2021," online available under https://de.statista.com/statistik/daten/studie/196642/umfrage/abonnenten-von-netflix-quartalszahlen/.

[2] M. Brandt, "155 Millionen Premium-Kunden," online available under https://de.statista.com/infografik/13769/monatlich-aktive-nutzer-und-zahlende-abonnenten-von-spotify-weltweit/.

[3] Steam, "STEAM- & SPIELSTATISTIKEN," online available under https://store.steampowered.com/stats/?l=german.

[4] I. Activision Blizzard, "Activision Blizzard Announces Third-Quarter 2019 Financial Results ," online available under https://investor.activision.com/static-files/594047f5-10b9-4fbf-b43b-45c8552cbd79.

[5] T. Nishide, K. Yoneyama, and K. Ohta, "Abe with partially hidden encryptor-specified sccess structure," in *ACNS*, 2008, pp. 111–129.

[6] T. Prantl *et al.*, *Towards a Group Encryption Scheme Benchmark: A View on Centralized Schemes with Focus on IoT*. ICPE, 2021.

[7] ——, "Performance impact analysis of securing mqtt using tls," in *2021 ACM/SPEC International Conference on Performance Engineering (ICPE)*, ser. ICPE'21, April 2021.

[8] P. Kumar *et al.*, "Attribute based encryption in cloud computing: A survey, gap analysis, and future directions," *Journal of Network and Computer Applications*, vol. 108, 2018.

[9] C. Lee, P.-S. Chung, and M. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *Int. J. Netw. Secur.*, vol. 15, pp. 231–240, 2013.

[10] G. Bordogna *et al.*, "A survey of research progress and development tendency of attribute-based encryption," *The Scientific World Journal*, p. 193426.

[11] Y. Zhang *et al.*, "Attribute-based encryption for cloud computing access control: A survey," *ACM Comput. Surv.*, Aug. 2020.

[12] S.-Q. Li *et al.*, "A survey on key management for multicast," in *ICCSIT 2010*.

[13] T. Prantl *et al.*, "Benchmarking of pre- and post-quantum group encryption schemes with focus on iot," in *IPCCC*, 2021.

[14] ——, "Performance evaluation of a post-quantum public-key cryptosystem," in *2021 IEEE 40th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2021.

[15] T. Phuong *et al.*, "Hidden ciphertext policy attribute-based encryption under standard assumptions," in *Trans. Inf. Forens. Sec.11*, 2016.

[16] K. Xue *et al.*, "Robust and auditable access control with multiple attribute authorities for public cloud storage," in *Trans. Inf. Forens*, 2017.

[17] K. Zhang *et al.*, "Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability," in *Sci. China Inf.*, vol. 3, 2018.

[18] P. Yu *et al.*, "Decentralized, revocable and verifiable attribute-based encryption in hybrid cloud system," *Wirel. Pers. Commun.*, 2019.

[19] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," vol. 2009, 09 2009, p. 284.

[20] Y. T. . M. Corporation, "WT300 Serie Digitale Leistungsmessgeräte," online available under https://tmi.yokogawa.com/de/solutions/products/power-analyzers/digital-power-meter-wt300/#Details.

[21] T. Prantl *et al.*, "Evaluating the Performance of a State-of-the-Art Group-oriented Encryption Scheme for Dynamic Groups in an IoT Scenario," in *MASCOTS*, ser. MASCOTS '20, November 2020.

[22] I. Management Association, *The Internet of Things: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice*. IGI Global.

[23] C.-C. Lee *et al.*, "A survey on attribute-based encryption schemes of access control in cloud environments." *Int. J. Netw. Secur.*, 2013.

[24] X. Wang *et al.*, "Performance evaluation of attribute-based encryption: Toward data privacy in the iot," in *ICC*. IEEE, 2014.

[25] M. Fischer *et al.*, "Using attribute-based encryption on iot devices with instant key revocation," in *2019 PerCom Workshops*. IEEE, 2019.

[26] B. Girgenti *et al.*, "On the feasibility of attribute-based encryption on constrained iot devices for smart systems," in *SMARTCOMP*, 2019.

[27] M. La Manna *et al.*, "Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update," *Sensors*, vol. 21, 2021.

[28] S. Herrnleben *et al.*, "An IoT Network Emulator for Analyzing the Influence of Varying Network Quality," in *Simulation Tools and Techniques*. Cham: Springer International Publishing, 2021, pp. 580–599.

[29] S. Herrnleben, M. Leidinger *et al.*, "ComBench: A Benchmarking Framework for Publish/Subscribe Communication Protocols under Network Limitations," ser. VALUETOOLS '21, 2021.

[30] C. Krupitzer *et al.*, "An Overview of Design Patterns for Self-Adaptive Systems in the Context of the Internet of Things," *IEEE Access*, vol. 8, pp. 187 384–187 399, 2020.

[31] T. Prantl *et al.*, "Simpl: Secure iot management platform," in *ITG Workshop on IT Security (ITSec)*, 2020.