Designing a Hybrid Attribute-Based Encryption Scheme Supporting Dynamic Attributes

Stefan G. Weber

StefanGeorgWeber@gmail.com

Abstract. This article presents the design of a novel hybrid attribute-based encryption scheme. The scheme is attribute-based, as it allows encrypting under logical combinations of attributes, i.e. properties that users satisfy. It is hybrid, as it combines ciphertext-policy attribute-based encryption (CP-ABE) with location-based encryption (LBE) on the level of symmetric keys. It can efficiently handle dynamic attributes with continuous values, like location, even in resource-constrained settings.

Key words: Based Encryption, Cryptography, Secure Communication

1 Introduction

Recently introduced, attribute-based encryption (ABE) schemes [10, 9, 2] have drawn attention for realizing secure communication and decentralized access control in large and dynamic networks and ubiquitous computing environments, in particular with mobile and unknown interaction partners [8, 19, 14, 15].

ABE provides means for a decentralized enforcement of security and access control policies by cryptographically binding the policies to data objects, e.g. messages in transmission. It is designed to harness properties of users, by generalizing the traditional concepts of public and private keys towards attributes. More generally, encryption operations can be based on logical combinations of attributes, forming so called attribute policies, which in turn allow making users addressable according to their properties.

In this article, we introduce and describe a novel attribute-based hybrid encryption scheme that is able to handle even more expressive policies. In particular, the notion of an expressive policy refers to the capability to efficiently support static attributes as well as continuous dynamic attributes in combination in conjunctive encryption policies. Conceptually, we propose to combine ciphertext-policy attribute-based encryption (CP-ABE) [2] and location-based encryption (LBE) [11, 7], which allows realizing expressive encryption policies, while we leverage symmetric AES encryption [6] to efficiently encrypt the payload. Current state-of-the-art encryption schemes are unable to support such encryption capabilities which consider continuous dynamic attributes that may change in an unpredictable manner.

The remainder of this article is structured as follows: The following section discusses existing encryption schemes. Then, we introduce the construction principle of our novel proposal, followed by a description of the main primitives. The protocols and mechanisms are explained in detail afterwards. After a discussion of the security properties, this article is concluded.

2 A Primer to Encryption Schemes

In this section, we review existing schemes that can potentially be used to implement an expressive end-to-end encryption for messaging applications and secure communication. Basically, a secure communication channel can be implemented based on

- Symmetric Encryption
- Asymmetric Encryption
- Identity-based Encryption
- Attribute-based Encryption

We discuss existing approaches next. In a large-scale or distributed setting, traditional cryptographic constructions suffer from key distribution problems (symmetric encryption) or problems related to the efficiency of encryption operations (asymmetric encryption). Figure 1 depicts the basic approach how symmetric encryption can be applied to achieve secure communication. The main drawback is that a symmetric key has to be distributed between any relevant combination of senders and recipients. In case the group of recipients is not known when a message is sent out, this approach is not applicable.

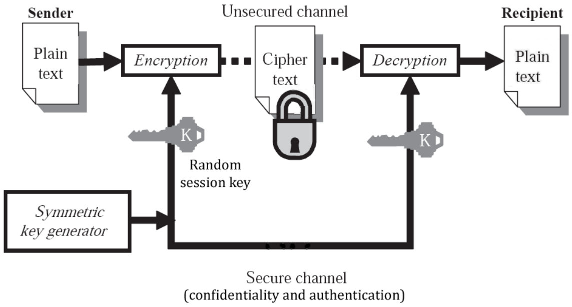

Fig. 1. Symmetric Encryption

Figure 2 illustrates how public key encryption can solve the key distribution problem of symmetric encryption. Here, instead of using a single symmetric key for both encryption and decryption, a pair of keys is used. It consists of a public key and a private key. By publishing the public keys of all possible recipients, a sender can send encrypted messages. Yet, this approach does not consider one-to-many settings. Also, operations of asymmetric encryption are more resource demanding than symmetric ones. Therefore, both concepts alone do not fit well in dynamic and mobile settings.

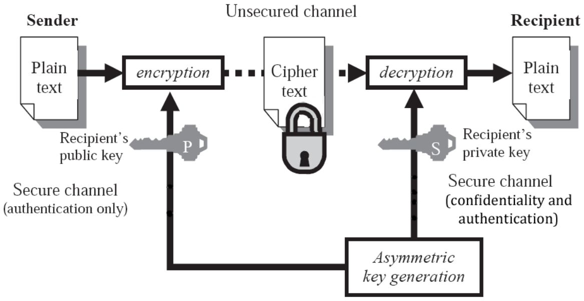

Fig. 2. Public Key Encryption

Identity-based encryption (IBE) [3], which is a certificateless alternative to public key encryption, allows encrypting messages under textual strings, instead of public keys. Such a string originally refers to the identity of a recipient. This principle is also shown in Figure 3.

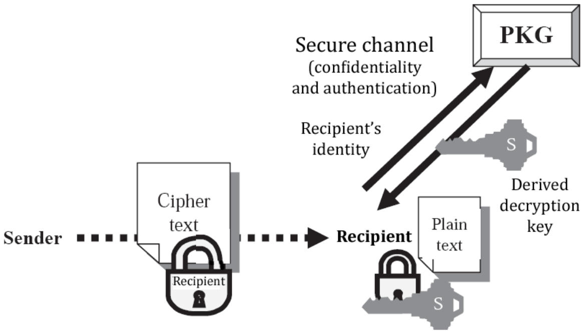

Fig. 3. Identity-Based Encryption

However, this identity-based approach requires the availability of a complete list of all intended recipients. Yet, it allows realizing encryption that is partly suitable for one-to many settings, by describing a group by a single textual string. Differently, we seek to devise an encryption scheme that is able to handle more expressive policies.

Attribute-based encryption (ABE) is a natural candidate building block for dynamic settings: here, groups of recipients can be selected in an elegant way, by specifying combinations of descriptive attributes. Especially, ABE is a generalization of IBE. In fact, the first variant was described as fuzzy identity-based encryption [10]. Yet, current ABE proposals lack an efficient way of handling dynamic attributes. One common way is to add an expiration date to attributes as revocation mechanism, as proposed by [2]. A different approach is to change the values of attributes according to a pre-determined temporal function [5]. Yet, both approaches are not applicable to dynamic attributes that change in an unpredictable manner, as in the case of location attributes, where attributes additionally have a continuous range of values.

3 Our Construction Principle

In the last section, we argued that realizing end-to-end encryption in dynamic and distributed settings and systems is a challenging task: traditional asymmetric encryption schemes are not practical for securing communication with dynamic groups or unknown recipients, since unknown entities cannot be addressed and also certificate verification is a huge obstacle. Dealing with these issues, more recent asymmetric encryption techniques proposed to generalize the role of the recipients' identities [10] and thus can enable a more flexible specification of recipients and content. As a consequence, in this approach, the key-related concepts refer to attributes, which can represent properties of recipients and/or messages.

Yet, handling continuous dynamic attributes is thus far only possible among the unpractical assumption of an online key generator, which we want to avoid in our design. Also, due to the inherent use of computationally demanding pairing-based cryptography (cf. [3]), the practical applicability of existing techniques remains highly challenging in scenarios with mobile and resource-constrained devices.

To overcome these issues, we propose to leverage ciphertext-policy attribute-based encryption (CP-ABE) [2] in combination with location-based encryption (LBE) [11, 7] and symmetric AES encryption [6]. Especially, we propose to make use of CP-ABE to handle static attributes within an encryption policy, while the principle of location-based encryption is employed to derive a symmetric key from a dynamic attribute, e.g. a GPS position. In order to save the computation of pairings, we leverage CP-ABE in a hybrid mode, this means, we split the encryption of the payload from the encryption of the session key. The session key is then additionally bound to the location-based encryption.

Thus, in order to decrypt, both the CP-ABE policy (static attributes) and the LBE constraint (a dynamic attribute) have to be satisfied. Figure 4 shows this construction principle in overview. Practically, this approach means that we combine an offline key generation for static attributes with a light-weight online key generation for dynamic attributes. Together with relying on AES encryption for the payload, the approach is rendered suitable even for mobile and resource-

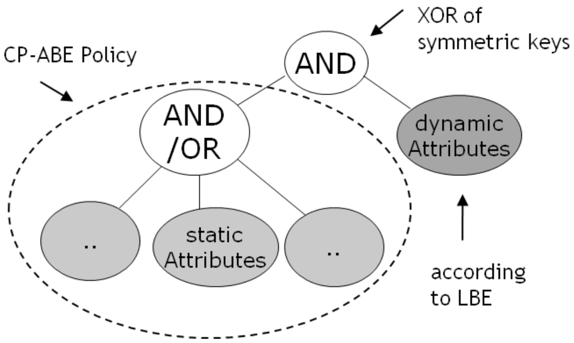

Fig. 4. Construction Principle

constrained devices which represent the end point of an end-to-end encrypted communication.

Please note that the following descriptions mostly abstract from the concrete (pairing-related) algorithms of CP-ABE. For simplicity reasons, our descriptions thus consider attribute-based encryption mostly as a black box.

3.1 Main Primitives

In this section, we describe the two main building blocks that contribute to the design of the presented hybrid encryption scheme supporting dynamic attributes.

Ciphertext-Policy Attribute-Based Encryption Attribute-based encryption (ABE) [10] is an encryption scheme that generalizes the functional role of identities and keys. In traditional asymmetric encryption schemes, identities relate to distinct public key / private key tuples. In ABE, the concepts of public and private keys are replaced by sets of attributes, which abstract from actual user properties. (In the following, we denote the concept that replaces a private key as private attribute set.) Moreover, ABE is certificateless and the cryptographic credentials are issued by a central trusted party called attribute authority, which is in possession of a global master key for key generation. Since users are associated with sets of attributes, they might try to trade some attributes and related private key components to gain more decryption powers. However, ABE systems are collusion resistant [2], i.e. keys of different users are incompatible due to the cryptographic construction.

Like identity-based encryption [3], ABE cryptographically builds upon pairings, i.e. bilinear maps that provide an extra structure on special elliptic curves. While pairings enable attribute-based encryption, they are very computationally demanding. From a practical point of view, the goal is to minimize pairing-related operations, in order to enable use even on resource-constrained devices.

Ciphertext-policy attribute-based encryption (CP-ABE) [2] is a special form of attribute-based encryption, which associates a set of attributes used in the encryption process with logical access structures, also called attribute policies.

Due to the use of secret sharing [12], the access structures are trees with nodes that represent t-out-of-n combinations of attribute child nodes, naturally including conjunctions (AND) as well as disjunctions (OR). In CP-ABE, the encryption algorithm takes as input a message and an attribute policy. The algorithm encrypts the message and produces a ciphertext, such that only a recipient possessing a set of attributes that satisfies the attribute policy is able to decrypt that message. In order to avoid the computation of parings and thus enable more practical applications, CP-ABE can be used in hybrid mode: a message itself is encrypted with a random symmetric secret key. Only this session key is then CP-AB encrypted under a policy. In the following, we assume that the ciphertext also encodes the policy.

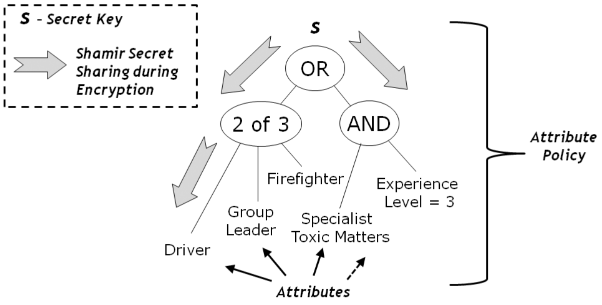

Fig. 5. SamplePolicy

An example of a CP-ABE policy and its application to encryption in hybrid mode is given in Figure 5. The figure shows an attribute policy containing attributes that are exemplarily taken from the first response domain [14]. During the encryption under the policy, the session key S is Shamir secret shared according to the operation specified in the nodes of the policy, from the root node down to the leafs. Given an AND node, the key or the share of the key is distributed to child nodes according to a n-out-of-n secret sharing.

For the decryption operation, this effectively means that all the shares associated to child nodes have to be available, for the reconstruction to succeed. Given an OR node, the key or the share of the key is distributed according to a 1-out-of-n secret sharing; i.e. only one share is required to reconstruct the secret in the level above. During the encryption process, shares of S are thus consecutively dealt out from the root node down to the leaf nodes. Every leaf node is associated to an attribute. The share dealt out to a leaf node is finally encrypted according to attribute-based encryption principles. Thus, for the decryption to succeed, a user requires a set of attributes that at least satisfies the policy. With-out at least this set, the shares at the leaf nodes cannot be decrypted. Thus, the secret key S cannot be reconstructed, and consecutively, the message cannot be decrypted.

For the purpose of symmetric encryption, we propose to make use of the advanced encryption standard (AES) [6]. AES supports key sizes of 128, 192 and 256 bits. This key size is a parameter that has to be chosen in accordance to the intended security level.

Location-Based Encryption The concept of location-based encryption (LBE) was proposed by [11, 7]. It aims at securing mobile communication by limiting the area inside which the intended recipient can decrypt a message.

In order to implement this location-based security constraint, LBE adds a layer of security to a symmetric encryption of a message: the targeted recipient's geographic location L is combined with the session key, in order to produce a location-locked key. This location-locked key is then sent along with the encrypted message. As a result, the ciphertext can only be decrypted if the session key can be recovered from the location-locked key. In turn, LBE requires that this decryption is only possible if the recipient's device is physically presented at location L, or respectively inside a geographic area associated with L. This process is called location verification, it hinges on a tamper-resistant GPS receiver inside the recipient's mobile device. In LBE, the sender has to transmit parameters which define the area where decryption is permitted and may specify further dynamic constraints like time periods or even velocity that have to be verified upon decryption [1].

In general, a location-based encryption scheme requires an efficient mapping from location areas to symmetric keys, which is called a location lock. The location lock is secured by including an additional key as an input parameter in order to derive symmetric keys.

4 Setting and Main Mechanisms of Hybrid Encryption Scheme

Having described the background, this section introduces the basic protocols of the novel hybrid encryption scheme. In particular, we describe the encryption and the decryption scheme. Also, we provide details of the underlying key management approach.

4.1 Parties

The parties relevant to the setting of the hybrid encryption scheme are derived from the underlying CP-ABE and LBE concepts. For brevity of presentation, we only consider the following two authorities and entities explicitly in our setting:

- Attribute authority AA: the AA is responsible for creating the private credentials (attributes) used for decryption. Especially, it issues a private attribute set $\{A\}_R$ to every possible recipient.

- Recipient R: this entity receives encrypted messages on her communication device. The device is initialized for decryption with the recipient's private attribute set $\{A\}_R$ and K_{LL}, the key for the location lock function. Also, the device has a tamper-resistant GPS receiver that is leveraged in the following schemes.

4.2 Encryption and Decryption Protocols

This section introduces the main protocols of the novel hybrid encryption scheme. In the following description, we particularly refer to location attributes as dynamic attributes.

We use the following notation:

- $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. In the following, we also denote $L^{(P_1,P_2)}$ simply as L.
- $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$.
- $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$.

In the given approach, it is possible that one of the two main parts of a policy remains undefined:

- in case the CP-ABE part AP is not specified, encryption is reduced to location-based encryption;
- in case the LBE location area attribute $L^{(P_1,P_2)}$ is not specified, encryption is reduced to ciphertext-policy attribute-based encryption.

We now introduce the complete approach. Here, decryption succeeds if R's attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. Figure **??** shows the basic operations of the encryption schemee in overview.

Our hybrid encryption employs a keyed *location lock mapping* that we denote as $f_{LL}(L^{(P_1,P_2)}, K_{LL})$, according to the following principle: GPS coordinates P_1, P_2 and K_{LL} are concatenated. Then, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2||K_{LL}$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a bit string that matches the chosen key size, in order to produce the location lock value[1].

Protocol for Hybrid Encryption The *hybrid encryption protocol* works as follows (cf. Figure 6):

[1] In this operation an appropriate collision resistant hash function has to be employed. Assuming e.g. a level of 160 bit security for symmetric keys, then SHA-1 is a hash function of choice.

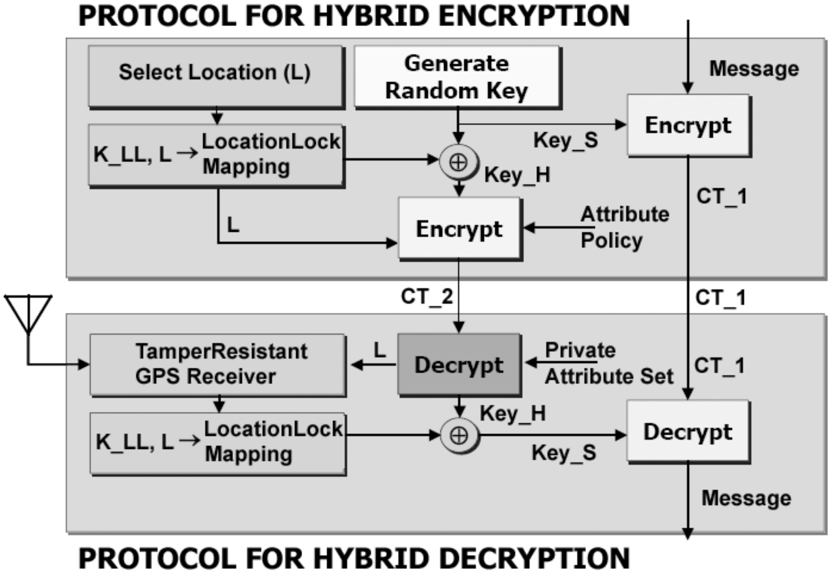

Fig. 6. Hybrid Encryption in Overview

1. A random session key Key_S is generated.
2. The message is symmetrically encrypted under Key_S, producing ciphertext CT_1.
3. The location lock value is computed from the selected location area L and key K_{LL}.
4. Key_S is XORed with the location lock value, generating a hybrid key Key_H.
5. Key_H is concatenated with an encoding of the location area L, producing the string $L||Key_H$. This string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2
6. CT_1 concatenated with CT_2 represent the ciphertext CT. CT is transferred to a receiver R.

Protocol for Hybrid Decryption The *protocol for hybrid decryption* works as follows (cf. Figure 6):

1. After reception of $CT = CT_1||CT_2$, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. On successful decryption, the location area L and Key_H are recovered.
2. R's current GPS position P_R is computed by means of a tamper-resistant GPS receiver and verified to be inside the location area L. On success, the location lock value is computed, taking L and key K_{LL} as input parameters.

3. The location lock value is then XORed with the recovered Key_H, in order to reconstruct Key_S.
4. Key_S is used to symmetrically decrypt CT_1 to M.

5 Management and Generation of Private Keys

The proposed hybrid encryption scheme entails an important design aspect: key management, including the generation of private keys. Since the present approach combines two existing encryption techniques, it inherits properties from CP-ABE, other characteristics derive from LBE. Especially, the hybrid encryption scheme hinges on a tamper-resistant GPS receiver. The GPS receiver triggers the creation of keys that need to satisfy location-depended constraints in the encryption process. Figure 7 summarizes the design space of the generation of private keys as well as the chosen approach.

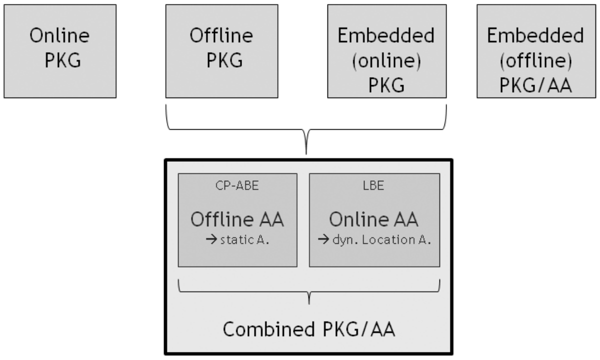

Fig. 7. Key Management Design Space

Basically, in our setting, private key generation (PKG) is possible online, offline and embedded in tamper-resistant hardware (TR06). An online PKG refers to a server that is permanently reachable and produces and communicates private keys or attributes on request. In the offline mode, all keys are generated in a preceding phase and handed out to the recipient.

An embedded (online) generation of private keys refers to a local implementation of the key provisioning mechanisms based on tamper-resistant hardware integrated in the recipient's device. In this case, a device itself creates a private key required for message decryption. CP-ABE requires a master key for private key generation, which is, among practical considerations, of high risk, since this global trapdoor is then highly distributed.

Furthermore, in an embedded (offline) key generation mode, all possible keys/attributes are generated in a preceding phase, and registered in a tamper-resistant storage module of the recipient's device. If a particular key/attribute is required for decryption, the tamper-resistant hardware can temporarily provide the key to the execution environment of the decryption operation (cf. [14, 4, 18]).

In this article, we propose to realize the hybrid encryption scheme with the following combination of online and offline key generation mechanisms: static attributes are generated offline by an CP-ABE attribute authority (AA) and distributed to recipients before use, dynamic location attributes are generated by an embedded online LBE key generator which is realized on the device. Practically, this approach means that a global secret, i.e. K_{LL}, the key for the location lock, is required for securing one-to-many encryptions. Even though a global secret is distributed on every device, it can only be used to generate dynamic attributes. Static attributes cannot be generated on the device. Since the decryption based on static attributes is executed in the first step, a maliciously generated dynamic attribute cannot allow decrypting additional ciphertexts in case that insufficient static attributes are available. Yet, K_{LL} also provides protection against outside adversaries in case that only location attributes are used for encryption. Thus, the chosen approach reconciles a low misuse potential and secure functionality under practical assumptions.

The chosen approach moves a major part of trust into the organizational level of using security mechanisms, i.e. the offline issuing of private attributes and K_{LL}.

6 Security Discussion

In this section, we discuss the security provided by our novel hybrid encryption scheme. The proposed design of the hybrid encryption technique followed two main goals: achieving efficiency in handling continuous dynamic attributes and minimizing trust requirements in attribute authorities at the same time. We recap the design decisions and discuss the resulting level of security.

At first, handling dynamic attributes requires means for providing keys on mobile devices. An online AA (or online PKG) could principally solve the problem, but does not scale. An offline AA only allows handling dynamic attributes by pre-registering all possible attributes to a local trusted activator. This is inefficient for continuous attributes. An embedded AA could be implemented locally on tamper-resistant hardware. However, it locally requires the master key and could generate all attributes of all users, such that the key escrow risk associated to a compromise is extremely high. Within our approach, we propose to conceptually split the role of the single AA (cf. Figure 7): an offline CP-ABE AA issues all static attributes in a registration phase, while an embedded LBE AA handles dynamic location attributes, based on tamper-resistant hardware.

Regarding encryption security, the hybrid scheme is designed such that the location-based encryption (LBE) parts adds a further level of security to the symmetric session key that is used for message encryption. In our approach, the XOR operation encrypts the initially generated session key comparable to a one-time pad [13]. Hence, decryption is only possible if the required CP-ABE attributes are available to decrypt the outer asymmetric encryption layer and the location lock value can be generated correctly in order to recover the session key. In most cases, policies will include a conjunction of location and further CP-ABE attributes. The approach retains encryption of messages even in case the embedded LBE AA is compromised.

Moreover, in case the CP-ABE attributes are compromised, a message is still protected by the additional location-dependent encryption layer. Thus, the hybrid encryption scheme allows realizing end-to-end encryption while being able to handle expressive policies.

In addition, our proposal minimizes the use of pairings in the end-to-end encryption. This design broadens the applicability of the encryption scheme to a range of mobile devices. In particular, the session key decryption requires one XOR operation for the LBE part. To decrypt the CP-ABE part of the policy, two pairing operations for every attribute that is matched by one of R's attributes are required. For policies with additional internal AND-/OR-levels, one exponentiation operation is required for each internal node from an attribute in the leaf to the root node of the CP-ABE policy part.

In [16], we describe additional runtime experiments, which are beyond the scope of this article, confirming the recent statements that attribute-based encryption techniques have become applicable to resource-constrained settings (cf. [8, 19]).

As a consequence of the chosen design approach, the hybrid encryption scheme looses full cryptographic collusion resistance with respect to the expressive policy. Yet, collusion between recipients or adversaries that try trading CP-ABE attributes, e.g. in order to gain access to messages of further organizations, fails. The hybrid encryption assumes tamper-resistant hardware, especially a tamper-resistant GPS receiver. In several contexts, this assumption is practically fulfilled. The application logic required for implementing the location lock mapping and the location verification procedure is small, such that means to guarantee correctness based on certification procedures can easily be applied. Together with a secure software stack, e.g. supported by a TPM chip of a mobile device (cf. [4]), additional practical security guarantees can be given.

In some cases, a device may be unable to compute its current GPS position, e.g. inside closed buildings. To circumvent functional problems, we propose to internally rely on the last computed (and thus computable) GPS position in such cases.

7 Conclusion

This article proposed a novel hybrid attribute-based encryption scheme, which allows encrypting under expressive policies, including dynamic attributes. The proposal is build on an efficient combination of ciphertext-policy attribute-based encryption, location-based encryption and symmetric AES encryption.

Being able to efficiently handle dynamic attributes, the proposal has applications to end-to-end secure attribute-based messaging schemes [17], identity management [18] as well as enables secure location-based collaboration [16].

References

1. Al-Fuqaha, A., Al-Ibrahim, O.: Geo-Encryption Protocol for Mobile Networks. Computer Communications 30(11-12), 2510–2517 (2007)
2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (SP '07). pp. 321–334. IEEE CS (2007)
3. Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing 32(3), 586–615 (2003)
4. Brucker, A.D., Petritsch, H., Weber, S.G.: Attribute-Based Encryption with Break-Glass. In: Workshop in Information Security Theory and Practice (WISTP'10). pp. 237–244. Springer (2010)
5. Chen, N., Gerla, M., Huang, D., Hong, X.: Secure, Selective Group Broadcast in Vehicular Networks using Dynamic Attribute Based Encryption. In: IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net). pp. 1 – 8 (2010)
6. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer (2002)
7. Denning, D.E., Scott, L.: Geo-Encryption - Using GPS to Enhance Data Security. GPS World (2003)
8. Huang, D., Verma, M.: ASPE: Attribute-Based Secure Policy Enforcement in Vehicular Ad Hoc Networks. Ad Hoc Networks 7(8), 1526–1535 (2009)
9. Piretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure Attribute-Based Systems. In: ACM Conference on Computer and Communications Security (CCS '06). pp. 99–112. ACM Press (2006)
10. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Advances in Cryptology - EUROCRYPT '05. pp. 457–473. Springer (2005)
11. Scott, L., Denning, D.E.: A Location Based Encryption Technique and Some of Its Applications. In: ION National Technical Meeting 2003. pp. 730–740 (2003)
12. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
13. Shannon, C.E.: Communication Theory of Secrecy Systems. The Bell System Technical Journal 28, 656–715 (1949)
14. Weber, S.G.: Securing First Response Coordination with Dynamic Attribute-Based Encryption. In: Conference on Privacy, Security and Trust (PST '09) in conjunction with World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09). pp. 58 – 69. IEEE CS (2009)
15. Weber, S.G.: A Hybrid Attribute-Based Encryption Technique Supporting Expressive Policies and Dynamic Attributes. Information Security Journal: A Global Perspective 21(6), 297–305 (2012)
16. Weber, S.G.: Multilaterally Secure Pervasive Cooperation - Privacy Protection, Accountability and Secure Communication for the Age of Pervasive Computing. IOS Press (2012)
17. Weber, S.G., Kalev, Y., Ries, S., Mühlhäuser, M.: MundoMessage: Enabling Trustworthy Ubiquitous Emergency Communication. In: Conference on Ubiquitous Information Management and Communication (ICUIMC '11). pp. 29:1–29:10. ACM Press (2011)
18. Weber, S.G., Martucci, L.A., Ries, S., Mühlhäuser, M.: Towards Trustworthy Identity and Access Management for the Future Internet. In: Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS '10) (2010)

19. Yu, S., Ren, K., Lou, W.: FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks. In: IEEE INFOCOM 2009. pp. 963–971. IEEE CS (2009)