MundoMessage: Enabling Trustworthy Ubiquitous Emergency Communication

Stefan G. Weber
CASED
Mornewegstraße 32
64293 Darmstadt, Germany
stefan.weber@cased.de

Yulian Kalev
CASED
Mornewegstraße 32
64293 Darmstadt, Germany
yulian.kalev@cased.de

Sebastian Ries
CASED
Mornewegstraße 32
64293 Darmstadt, Germany
sebastian.ries@cased.de

Max Mühlhäuser
CASED
Mornewegstraße 32
64293 Darmstadt, Germany
max.muehlhaeuser@cased.de

ABSTRACT

Efficient emergency communication is of high practical importance, but has specific challenges: unpredictable local emergency situations harden the establishment of communication structures, legal requirements dictate the use of end-to-end secure and documentable approaches, while users demand ease-of-use and privacy protection. Dealing with these challenges, the contribution of this paper is four-fold: first, together with emergency practioners we define realistic security requirements and patterns for ubiquitous emergency communication. Second, we devise techniques for privacy-respecting re-identificaton of pseudonymous receivers. Third, we propose a new hybrid encryption technique for expressive policies, which combines ciphertext-policy attribute-based encryption with location-based encryption. Fourth, building on the new techniques, we introduce MundoMessage, our approach to multilaterally end-to-end secure, user-friendly attribute-based messaging for emergency communication. Finally, we analyze our approach.

1. INTRODUCTION

Mobile communication has become an integral part of our modern information society. Personal communication devices enable locally distributed users to participate in communication contexts of everyday's life and work. In some application scenarios, communication technologies even constitute a critical service: considering e.g. the case of a sudden emergency, efficient communication support can mean the difference between success and failure of rescue missions, possibly between life and death of affected persons and between the loss and safeguard of infrastructure and property. Thus, communication mechanisms that allow for reaching the right actors at the right time are of highest practical importance for emergency management. Currently, in Europe, dedicated digital communication networks for emergency communications are under establishment. They are designed according to the *TE*rrestrial *T*runked *RA*dio (TETRA) standard[1] and promise to reliably connect organizations, parties and individuals involved in rescue efforts. Yet, such networks require adequate security mechanisms, but their final realization and secure use still raise a number of major research challenges. Two of these challenges are the implementation of *multilaterally secure* and *user-friendly* communication mechanisms. The first objective accentuates that secure systems need to consider the security goals of all involved parties [1], in and along with legal and individual usage contexts. The latter one points out that "the goal is not to build systems that are theoretically securable, but to build systems that are actually secure" [2] when real users deal with them in real application scenarios. We resort to these issues, stating that the realization of a (mostly ideal) system for trustworthy mobile and ubiquitous one-to-many communication does not only require paying attention to several explicit security requirements like mutual authentication and end-to-end confidentiality, but also to the more implicit security requirements of user-friendliness of the mechanisms as well as privacy protection of receivers. In this paper, we answer the challenging research question, whether and how it is possible to design and realize a multilaterally end-to-end secure yet practical approach that enables ubiquitous communication in dynamic situations *at ease* - as required for handling emergencies.

1.1 Our Approach and Contributions

We follow the approach that designing user-friendly security mechanisms in this application context requires *first* identifying human-adequate levels of abstraction and communication patterns and *second* realizing them in an end-to-end secure and efficient manner. Thus, in the first part of this work, we derive realistic use cases and security requirements for emergency one-to-many communication, by taking into account experiences with real users as well as legally implied security requirements. Based on these findings, we

ICUIMC '11, February 21-23, 2011, Seoul, Korea
Copyright 2011 ACM 978-1-4503-0571-6 ...$10.00.

[1] Cf. WWW.TETRAMOU.COM

propose MundoMessage, a novel approach to multilaterally end-to-end secure, yet user-friendly attribute-based messaging (ABM). As main building blocks, we introduce a new technique for re-identifying selected attributes of pseudonymous receivers, which is based on semantically secure ElGamal encryption, and a novel hybrid encryption technique for expressive logical policies. This encryption technique efficiently combines ciphertext-policy attribute-based encryption and location-based encryption. Applying it on the end-to-end encryption layer of the TETRA security infrastructure allows to enforce end-to-end secure attribute-based messaging. Overall, the proposed concepts enable the realization of communication mechanisms that are *user-friendly*, i.e. supporting easy-to-use, intuitive communication with dynamic groups of mobile and pseudonymous receivers, by introducing location as a human-adequate level of abstraction into the selection of receivers; *multilaterally end-to-end secure*, i.e. combining end-to-end confidential messaging with documentation and accountability means as they are required in the emergency communication domain, while also handling replay attacks on the end-to-end-encryption layer, and providing privacy protection for mobile users via pseudonyms; *practical*, i.e. complying with identified real emergency communication patterns, while being efficient for the use with a wide range of mobile devices. In sum, this is what we consider trustworthy ubiquitous emergency communication, since MundoMessage allows for a seamless integration of emergency communication services and facilities into everyday's life and work. We note that traditionally, end-to-end encryption layers only protect user data against confidentiality threats. Within our MundoMessage approach, the end-to-end encryption layer is also used as a *key management and identity abstraction layer.* While this work advances the study of secure attribute-based messaging systems, it also details practical methods for cryptographic key and end-to-end access control management in large-scale ubiquitous communication systems.

1.2 Outline

The remainder of this paper is structured as follows. Section 2 describes related work. Section 3 analyses emergency communication and sets up requirements. Afterwards, we sketch our overall approach in section 4. In section 5, main building blocks are presented. Then, a novel hybrid encryption technique as well as a new technique for selective attribute re-identification are introduced in section 6. Our complete ABM approach MundoMessage is described in detail in section 7. The proposed concepts are discussed and evaluated in section 8. Finally, the paper is concluded in section 9.

2. RELATED WORK

Previous related work on secure one-to-many messaging started with the introduction of secure role-based messaging [3, 4]. The scheme [3] allows specifying the recipients of a message based on a single organizational role. It employs traditional public key infrastructure (PKI) [5] and role-based access control (RBAC) [6] authorization concepts, but does not provide end-to-end encryption, since a trusted entity is required for each message decryption. The proposal [4] allows to combine several roles to form a logical policy for recipient selection. The scheme builds on identity-based encryption [7], such that logical policies are mapped to single cryptographic keys. Furthermore as a main drawback, it requires frequent interactions with an online trust authority in order to receive message decryption keys. In [8], the concept of attribute-based messaging was first presented. ABM allows to logically specify the group of receivers of a message in form of a flexible combination of attributes. ABM is a natural generalization of role-based messaging. The approach builds on attribute-based access control (ABAC) [9] as main security mechanism and does not provide end-to-end encryption. After the introduction of attribute-based encryption (ABE) techniques [10, 11], end-to-end encrypted attribute-based messaging schemes [12, 13] were proposed. Both schemes employ ciphertext-policy attribute-based encryption (CP-ABE) [14], which allows for a flexible cryptographic encoding of logical policies. Especially, [13] extends [8], by integrating encryption into ABAC mechanisms, but did not address handling of dynamic attributes and mobile receivers. Generally, the application of ABE enables a flexible specification of receivers and content. Yet, due to the inherent use of computationally demanding pairing-based cryptography, the practical applicability of ABE concepts in scenarios with mobile and resource-constrained devices remains highly challenging. We presented our first proposal of an attribute-based messaging scheme and system for emergency communication in [12]. While it was limited w.r.t. handling continuous dynamic attributes as selectors, handling replay attacks and issues related to ease-of-use, a prototype was used to initiate discussions with real users, enabling a cognitive walkthrough[2][15] of typical emergency communication scenarios. This paper presents a major revision, extension and follow up work on [12]. To the best of our knowledge, we are the first to address the complex issue of enabling multilaterally end-to-end secure yet user-friendly one-to-many communication through attribute-based messaging in a realistic scenario under practical assumptions.

3. ANALYSIS OF COMMUNICATION IN EMERGENCY SITUATIONS

From experiences and discussions with real users (first responders, decision makers and trainers from police and fire departments as well as relief organizations), we extracted the characteristics of emergency communications. A basic finding is that messages are the preferred communication mechanism in emergency management work [16]. Messages are also used to organize, inform and document any progress and internal actions. In this paper, we focus on the communication between the staff in operational headquarters and the outside world via messaging. The following lists give the main identified communication patterns (`CPs`) as well as a set of security requirements (`SReqs`) relevant to this communication.

3.1 Identified Communication Patterns

- `CP1: Communication by location addressing:` Fast participation in a disaster response fundamentally depends on both the nature and location of a disaster.

[2] A cognitive walkthrough, an usability evaluation method, builds on practical user experiments with a system. This helped to understand how real users interact by and with an emergency communication system. Findings contributed to section 3.

In order to handle large-scale disasters, several parties and organizations need to collaborate and communicate based on location. Some rescue efforts require the participation of local relief agencies, while others require local specialists to participate, rendering location both as a comfortable and necessary mean to select receivers.

- `CP2: Requests to unknown entities:` Some parties, like fire and police departments, are involved in most responses. But since the geographical scope of a disaster cannot be pre-determined before it actually happens, the real identities of responsible people are not directly clear. Yet, support for efficient communication with unknow entities is required.
- `CP3: Communication with dynamic groups of entities:` On lower hierarchical levels, when decision makers need to communicate with local groups of first responders, the actual identities are also not known beforehand, or groups are even dynamically formed. These groups need to be addressable comfortably.
- `CP4: Deposition of information for future use:` In many cases, information has to be deposited for entities that are known to join operations in future.

3.2 Security Requirements

- `SReq1: Basic security:` In emergency communication, mutual authentication, message integrity, availability and revocation of devices are basic requirements, detailed by the TETRA standard.
- `SReq2: End-to-end confidentiality:` Beyond that, preserving end-to-end confidentiality through encryption is legally implied for public security reasons.
- `SReq3: Protection against replay attacks:` Means that protect against replay attacks are required, in order to prevent an attacker from injecting a valid message a further time.
- `SReq4: Accountability of senders:` Emergency communication legally requires to document who sent which messages.
- `SReq5: Documentation of readers:` Also, the parties and entities who read received messages, requests and commands need to be documented for post-hoc audit purposes.
- `SReq6: Efficiency of security mechanisms:` Employed security mechanisms need to be suitable for resource-constrained mobile devices that are widely used in emergency communications.
- `SReq7: User-friendliness:` In order to foster end user acceptance, security mechanisms must be user-friendly [17]. For senders of messages, this implies minimum learning efforts as well as an intuitive use.
- `SReq8: Privacy protection of receivers:` Many participants involved in responses, like specialists, doctors or volunteers, are only available on requests sent to their mobile communication devices. Yet, receiver participation depends on a seamless integratability into personal lives, i.e. especially receivers prefer not to be traceable and demand privacy protection as far as possible. Even more, in some cases, organizational rules demand that senders may not know individual receivers by identity, e.g. in case a critical decision in a rescue mission has to be assigned to responders out in the field.

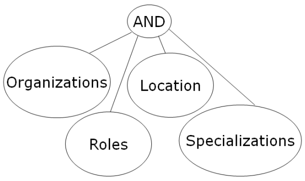

Figure 1: Structure of Logical Messaging Policy

4. SKETCH OF APPROACH

The last section detailed the central research question: how to enable a sender to securely and comfortably communicate with receivers unknown by identity, that may locally form dynamic groups? This section sketches our proposed solution called MundoMessage. For a sender in a certain messaging task, it is not immediately known with which actual parties and entities to communicate, but the sender can elaborate *which kind* of organizations, roles and specializations are appropriate and *where* they should be present, to allow for a fast engagement. Thus, we propose that a sender may specify the group of intended receivers of a message on a high level of abstraction. Especially, we propose to use the *logical attributes* as depicted in figure 1 in conjunction. Such a combination is what we call a *logical messaging policy*. It is used to specify the group of receivers in the messaging. Communication mechanisms that allow for a flexible highlevel specification of receivers in form of an attribute-based description are known as attribute-based messaging (ABM) [8, 12, 13]. ABM concepts potentially allow to implement a combined approach that may handle all major communication patterns, thus minimizing learning efforts. Also, it may combine location selectors with further attributes. In order to realize a secure ABM functionality, on the one hand, we can make use of the existing TETRA security infrastructure, which provides basic security services for emergency communication and also implies the existence of secure mobile devices on the receiver side. However, realizing the required end-to-end security leads to new challenges: traditional asymmetric encryption schemes and PKI concepts are not practical for communication with dynamic groups of unknown receivers. Even more, existing encryption techniques do not provide the required flexibility and means for expressing complex policies. To overcome these issues, we propose to leverage ciphertext-policy attribute-based encryption (CP-ABE) [14] in combination with location-based encrytion (LBE) [18]. CP-ABE is a recent asymmetric certificate-less encryption technique, that supports a cryptographic realization of flexible *cryptographic attribute*[3] *policies* to a certain degree. Yet, CP-ABE has

[3] Note that the cryptographic attributes of CP-ABE techniques are not necessarily equal to the logical attributes used

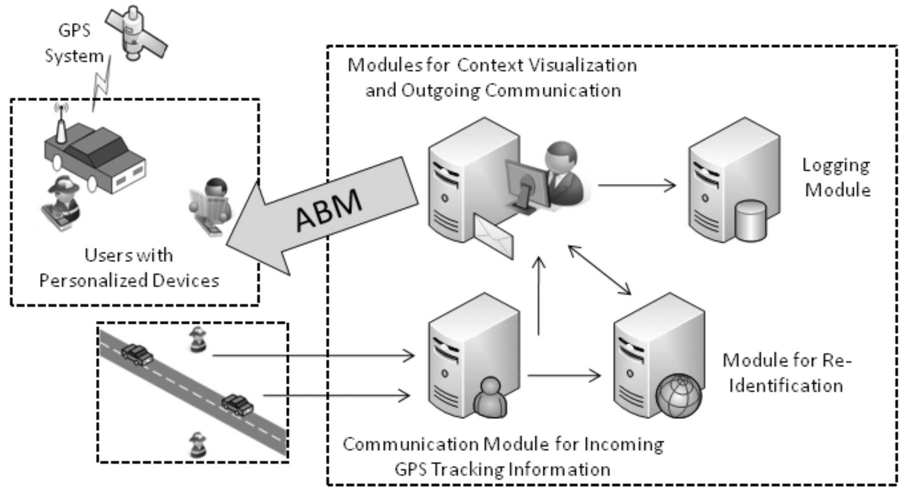
GPS System
Modules for Context Visualization and Outgoing Communication
Logging Module
ABM
Users with Personalized Devices
Module for Re-Identification
Communication Module for Incoming GPS Tracking Information

Figure 3: System Architecture of MundoMessage

practical limitations w.r.t. the handling of dynamic and continuous attributes. In emergency management, the use of augmented digital maps is inherent [19]. An integration of location selection into a digital map, illustrated in figure 2, was proposed by real users as a basic mean for intuitive use, but requires more expressive encryption support. Also, we assume that potential receivers of messages continuously provide location information to the system. In order to deal with the inherent privacy issues [20, 21] of this situation, we propose that location tracking proceeds under transaction pseudonyms. Yet, we also provide a technique for re-identification of role or specialization attributes implicitly attached to pseudonyms. Thus, we allow to selectively read out only non-sensitive information from pseudonyms, in order to reconcile privacy protection with an effective use of location addressing in the messaging. A short overview on the system architecture of MundoMessage is given in figure 3. As depicted, each mobile user (first responders and further registered specialists) provides GPS-based location information. A sender may communicate with the outside world via ABM mechanisms. In order to assess the current need for action, he is supported by an annotated digital map, which also may contain the spatial distribution of mobile users (supported by a *context visualization module*). In case of additional information needs, he may request role or specialization attributes of a pseudonymous user from the *module for re-identification.* Each message and re-identification request is logged (by a *logging module*), to enable post-hoc auditing. In the following, we introduce our concepts that enable to practically and securely incorporate location into receiver selection, while additional privacy protection of receivers is granted. In a later section, these concepts are used to devise and implement MundoMessage, our novel attribute-based messaging scheme and system.

5. BUILDING BLOCKS

In this section, we describe important building blocks of our work, namely the TETRA security architecture and employed encryption techniques.

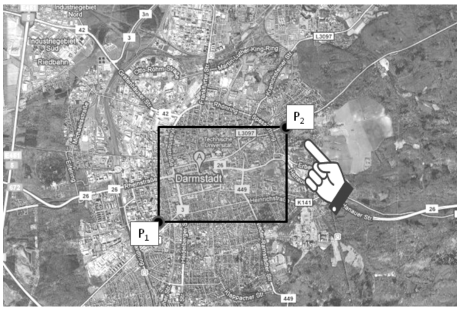

Figure 2: Location Selection on Digital Map

5.1 TETRA Security Architecture

TETRA is an open standard for digital radio [22]. It has been adopted in emergency communications by a number of national European administrations. This terrestrial trunked radio system was especially designed with data security mechanisms as principal features, including mutual authentication, air interface encryption and disabling of mobile devices. However, in its basic form, it only protects the air interface layer. Thus, additional, end-to-end encryption mechanisms are required for application contexts with end-to-end confidentiality requirements. The end-to-end encryption key management is in the user domain, especially, the underlying TETRA key management infrastructure is unable to decode end-to-end encrypted messages or access the end-to-end keys. For the receivers, we assume that they are equipped with mobile communication devices, that provide a digital communication channel to operational headquarters by means of TETRA. The mobile devices are uniquely identifiable and equipped with dedicated smart cards including TPM chips, rendering them tamper-resistant. End-to-end encryption keys are individually issued, e.g. along with the distribution of these devices. In the following, w.r.t. outgoing communication, we focus on broadcast-based one-

in ABM schemes, but belong to different conceptual layers of the messaging system.

to-many communication between a sender in an operational headquarter and mobile receivers. Since the TETRA communication infrastructure does not provide confidential point-to-point channels, end-to-end security of outgoing broadcasted messages is guaranteed by means of end-to-end encryption layer security mechanisms.

5.2 Semantically Secure ElGamal Encryption

The ElGamal cryptosystem [23], over subgroups $\mathbb{G}_q$ of order q of the multiplicative group $\mathbb{Z}_p^*$, for large primes $p = 2q+1$ provides the basis for pseudonym creation [24] and the novel attribute re-identification technique. The primes p, q and a primitive element g of $\mathbb{G}_q$ are common system parameters. More specifically, we build upon a threshold variant of it [25, 26]. In this setting, an ElGamal private key $s \in_R \mathbb{Z}_q$ is generated via a distributed key generation protocol [25], and consequently it is secret shared [27] among all participating authorities. The authorities share a single public key, $h = g^s \bmod p$, that is made available together with the system parameters. Since the private key is distributed, no single authority is able to decrypt. ElGamal incorporates random factors into the encryption process and is known to be semantically secure in $\mathbb{G}_q$, under certain complexity assumptions [28]. Practically, semantic security means that no partial information about a plaintext is leaking from the corresponding ciphertext. Later, we exploit the features of ElGamal encryption in the design of re-identification mechanisms. Especially, we build on the possibility to manipulate ElGamal ciphertexts via certain algebraic operations [26].

5.3 Attribute-Based Encryption

Attribute-based encryption (ABE) [10] is an encryption technique which generalizes the functional role of identities and keys. In traditional asymmetric encryption schemes, identities relate to distinct public key / private key tuples. In ABE, both public key and private key concepts are replaced by *sets of attributes*, which abstract from actual user properties. 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* [14], i.e. keys of different users are incompatible due to the cryptographic construction. Like identity-based encryption, ABE cryptographically builds upon pairings [29], 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-constraint devices. Ciphertext-policy attribute-based encryption (CP-ABE) [14] is a special form, which associates a set of attributes used in the encryption process with logical access structures[4], also called *attribute policies.* Thus, 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 receiver possessing a set of attributes that satisfies the attribute policy is able to decrypt that message. In the following, we assume that the ciphertext implicitly contains the policy. In practical applications, CP-ABE is used as *hybrid encryption*: a message itself is encrypted with a random symmetric secret key. Only this *session key* is then CP-AB encrypted under a policy. CP-ABE concepts can be the basis to realize a combined cryptographic *key management and identity abstraction layer*, which makes them interesting for the use in messaging applications.

5.4 Location-Based Encryption

The concept of location-based encryption (LBE) according to [18, 30] aims at securing mobile communication by limiting the area inside which the intended recipient can actually decrypt a message. In order to implement this, it adds a layer of security to the symmetric encryption of a message: the session key is combined with the targeted recipient's geographic location L, producing a location-locked key, which 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 is only possible if the receiver's device is physically present at location L, or respectively inside an geographic area associated with L. Location verification 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 receiver velocity that have to verified upon decryption [31]. In general, location-based encryption techniques require an efficient mapping from location areas to symmetric keys, which is called *location lock* in the following.

6. MAIN TECHNIQUES

In this section, we introduce the main support techniques for MundoMessage. These are, first, a novel hybrid encryption technique for expressive policies and, second, a novel technique for attribute re-identification.

6.1 Hybrid Encryption Technique

We next introduce a new efficient hybrid encryption technique for expressive policies. The technique is hybrid, as it combines CP-ABE with LBE on the level of symmetric keys. It enables to encrypt under expressive policies, since it can efficiently handle logical attributes with continuous values, like location[5]. We use the following notation: $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$. Hereby, $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ (cp. figure 2). Finally, $D_{\{A\}_R}^{P_R}(CT)$ 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 $P_R = (x_R, y_R)$. 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 4 depicts the basic operations of

[4] Due to the use of secret sharing [27], the access structures are trees with nodes that represent t-out-of-n combinations of attribute child nodes, naturally including conjunctions (n-out-of-n) and disjunctions (1-out-of-n).

[5] We restrict the description to location, however, further continuous attributes can be handled analogously.

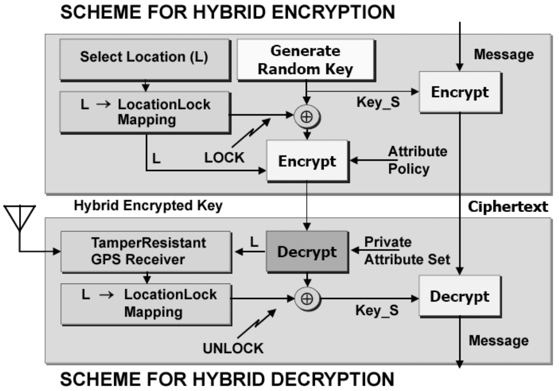

Figure 4: Overview of Hybrid Encryption Technique for Expressive Policies

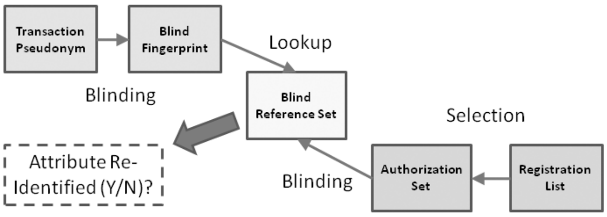

Figure 5: Main Steps of Re-Identification Technique

the encryption technique. It employs a *location lock mapping* $f_{LL}(L^{(P_1,P_2)})$, according to the following principle: GPS coordinates P_1, P_2 are concatenated. Then, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a 128 bit string[6], the location lock value. The *hybrid encryption scheme* works as follows: first, a random session key Key_S is generated. Second, the message is symmetrically encrypted under Key_S, producing ciphertext CT_1. Third, Key_S is XORed with the location lock value, generating a hybrid key Key_H. Fourth, the output is concatenated with an encoding of the location area. Fifth, the resulting string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2. CT_1 concatenated with CT_2 form the ciphertext CT. CT is transferred to a receiver R. The *scheme for hydrid decryption* works as follows: first, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. Second, on successful decryption, the location area $s_{LL^{(P_1,P_2)}}$ is extracted. Third, R's current GPS position P_R is verified to be inside the location area by means of a tamper-resistant GPS receiver. On success, the location lock value is be computed. It is then XORed with the recovered Key_H, in order to reconstruct Key_S. Finally, Key_S is used to symmetrically decrypt CT_1 to M.

6.2 Technique for Re-Identification

In this section, we introduce a novel technique for partial re-identification of pseudonyms. Within the MundoMessage system, we propose to make use of transaction pseudonyms in the location tracking. Such pseudonyms change with every single transaction, i.e. every location update that is sent by a mobile user to the headquarter is unlinkable to previous ones. Thus, the use of pseudonyms implements a basic privacy protection for mobile users, since their real identities are replaced by pseudo-random identifiers and are thus not traceable by unauthorized users. Next, we describe a techniques that yet enables to read out selected information that is implicitly attached to any transaction pseudonym. Such information is useful in the specification of a messaging policy, e.g. a sender may check before sending a message, whether a required specialist is nearby an emergency location by reading out information from selected, geographically displayed pseudonyms. This supports elaboration on adequate messaging contents as well as on which geographic areas to chose as selectors. First, in order to *generate transaction pseudonyms*, a base pseudonym $P_{U_i,B}$ of a user U_i is initially created as an ElGamal encryption of an algebraic representation of the unique base identifier ID_i (cp. [20, 21]). Thus, $ID \in \mathbb{G}_q$ is non-deterministically encrypted by choosing $r \in_R \mathbb{Z}_q$ and by computing $(g^r, h^r ID_i)$. Afterwards, transaction pseudonyms can be derived from the base pseudonym by iterative re-encryption (where $k \in \mathbb{N}$ refers to the k^{th} transaction pseudonym and $\otimes$ denotes algebraic multiplication): $P_{U_i,k+1} = P_{U_i,k} \otimes g^{r_{k+1}} = (g^{r+r_{k+1}}, h^{r+r_{k+1}} ID_i)$. In this process, the encrypted base identifier remains unchanged, and no private key is required. The base identifiers have implicit meanings, due to their creation in a registration process. A responsible authority sets up a registration list containing base pseudonyms and associated organizational roles and specializations. For example, the user with ID *John Doe*, a doctor registering to the system, may be recognized as a *specialist for toxic matters*. Thus, when a transaction pseudonym of *John Doe* is sent to the operational headquarter together with his current location, the implicitly attached information on the mentioned specialization can be read out in order to support the receiver selection process. For such a re-identification of role or specialization attributes[7], two entities within the system have to cooperate: a linkability broker (LB) as well as an authority for re-identification[8]. Additionally, we assume that the LB interacts with the authorities carrying the ElGamal private key s in a trustworthy manner. In the following, every step involving this key could be passed on to them, or the LB would play the same role[9], if chosen so in the system setup. The main steps of the re-identification techniques are given in figure 5. The linkability broker creates a fingerprinting key $z \in_R \mathbb{Z}_q$ in a setup phase. This key is comparable to the private key s, since it will be used for manipulation of ciphertexts. Then, the LB selects all base pseudonyms in the registration list that match the semantic of a given attribute, e.g. it selects all base pseudonyms belonging to the

[6] We assume 128 bit symmetric keys.

[7] Note that these attributes have the same semantics as the logical attributes used in logical messaging policies, i.e. the value can be used as part of the messaging policy. Yet, they have a different cryptographic implementation within the re-identification functionality.

[8] In the architecture displayed in figure 3, this authority is represented by the re-identification module.

[9] A distributed implementation of the LB is also possible using techniques presented in [21]. For simplicity, we describe the single authority version.

attribute *specialist for X*, in order to set up an *authorization set.* Then, the authorization set is blinded as follows, in order to produce the *blind reference set*:

- First, by raising the first component of each pseudonym $((g^r), (h^r ID_i))$ within the authorization set to the power of z: $(g^r)^z = (g^{rz})$, in order to derive a partly processed pseudonym $((g^{rz}), (h^r ID_i))$.
- Second, by decrypting each of the partly processed pseudonyms (using s) to blind deterministic fingerprints $g^{-z} ID_i$. This succeeds, since $(g^{rz})^s = g^{rsz} = g^{rs} \otimes g^z = h^r \otimes g^z$, which can be used to cancel out the first factor of $(h^r ID_i)$ via an algebraic division, hereby computing $g^{-z} ID_i$.

The blind reference sets together with the attached semantic in terms of a logical attribute are both provided to the authority for re-identification. Also, this authority receives $zs \in \mathbb{Z}_q$, which acts as a *blinded* fingerprinting key. Note that the re-identification authority learns nothing about z or s due to this. All these operations can be executed in a prior preparation phase, thus those are offline operations. The next steps can be performed online, i.e. in real time during the operation of MundoMessage. For the re-identification of an attribute of a chosen transaction pseudonym $(g^r, h^r ID_?)$, i.e. to test whether the information encoded in the pseudonym is implicitly attached to the semantics of the attribute in question or not, the authority

- raises the first component of the pseudonym to the power of zs: $(g^r)^{zs} = (g^{rzs})$,
- performs an algebraic division in order to produce a blind fingerprint: $(h^r ID_?)/(g^{rzs}) = g^{-z} ID_?$,
- executes a fingerprint lookup on the chosen blind reference set, i.e. it compares whether the produced blind deterministic fingerprint is part of this set.
- On success, i.e. if the fingerprint is part of the set, the transaction pseudonym has been re-identified with the logical attribute in question. Otherwise, the authority may proceed with a lookup on a different reference set.

7. OUR APPROACH TO ATTRIBUTE-BASED MESSAGING

Having introduced the basic building blocks and techniques, in this section we detail MundoMessage, our overall ABM approach, in a conceptual as well as schematic view.

7.1 Conceptual View

MundoMessage has two main conceptual layers: on the *logical messaging policy layer*, senders specify logical messaging policies, in order to select receivers in the communication via an ABM system. The *access control layer* provides security mechanisms that enforce the logical constraints specified by the messaging policies, by employing encryption techniques and tamper-resistant access control support mechanisms.

7.1.1 Logical Messaging Policy Layer:

When using the ABM system, in any messaging act, a sender selects attributes representing organizations (e.g. police), roles (e.g. group leader) and specializations (e.g. specialist for toxic matters), from a central attribute database.

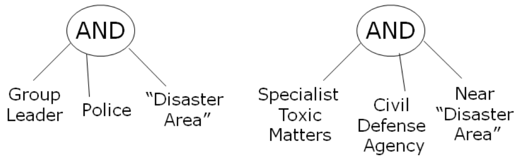

Figure 6: Simple Messaging Policies

The sender also selects a location area (cf. figure 2) or a specific location, e.g. a city by name, as a logical attribute. The sender has in principle flexibility[10] in combining the logical attributes.

Due to space restrictions, we omit further implementation details here, yet, we set up the basic construction rule for messaging policies, that a location attribute shall always be used in conjunction with at least one further attribute. Also, the sender has to select one communication pattern from `CP1,..,CP4` (cf. section 3.1).

7.1.2 Access Control Layer:

Dependent on the selection of the communication pattern, the access control layer chooses an enforcement method: direct communications (`CP1,CP3`) and requests (`CP2`) are secured using the hybrid encryption technique (cf. section 6.1), depositions (`CP4`) are handled with CP-ABE[11] alone (cf. section 5.3). The following descriptions focus on the realization of `CP1-CP3`.

7.2 Schematic View

We next detail registration and messaging phases of MundoMessage[12]. We denote the entities in the scheme: AA, a central attribute authority, RIA, a re-identification authority, S, a sender, R, a receiver. Beyond that, the following system components are involved: DM, a digital map, $RegL$, a registration list, ML, a message log and RL, a readers list. Log and lists are append-only.

7.2.1 Registration Phase:

In this phase, each relevant receiver interacts with the AA in order to receive keying material. This consists of a private attribute set $\{A\}_R$ to be addressable via ABM, as well as a base pseudonym $P_{R,B}$, to enable pseudonymous location tracking. In the registration process, upon proof of eligibility, the AA creates cryptographic attributes according to organization and role memberships as well as specializations that R actually satisfies. $\{A\}_R$ is transferred to R's personal mobile device for emergency communication. In turn, R's distinct mobile subscriber identity ($IMSI_R$) is added to the registration list $RegL$, along with the real world identity and assigned attributes. Also, the base pseudonym is added to that list, to enable specification of authorization sets for

[10] Logical disjunctions as root node are also possible. MundoMessage resolves this into several messaging acts with the same message content.

[11] In this case, location attributes are not necessarily continuous, enabling direct mapping to CP-ABE policies, even as combined attributes, e.g. PoliceDarmstadt.

[12] For space and simplicity reasons, we omit setup, preparation and auditing phases relevant to the system. Thus, entities that are involved only in these phases are also omitted in what follows.

pseudonym re-identification. In this phase, R additionally receives a key for symmetric encryption of replys, K_{Ack}^{RS}, and registers two keys for mutual message authentication with S, denoted K_{MAC}^{R} and K_{MAC}^{S}.

7.2.2 *Messaging Phase:*

The messaging phase consists of two main steps: a *re-identification step* and a *sending step*. First, in the optional re-identification step, S may request the RIA to re-identify selected attributes of pseudonymous receivers (according to section 6.2) that are displayed on DM, in order to derive additional information that is relevant to the specification of a logical messaging policy. Next, in the sending act, S selects a communication pattern, specificies the messaging policies by selecting attributes and a location area on the DM, and composes the message content. The underlying protocol of the sending act is depicted in figure 7. Basically, it consists of a broadcast of an end-to-end encrypted message M_{E2E} and answer back steps. Messages and acknowledged readers are documented on ML and RL. The end-to-end encryption incorporates a unique message ID, ID_M, to prevent replay attacks, symmetric accountability is supported by MACs. Optionally, readers can reply and answer a read messages.

8. SECURITY ANALYSIS

This section sketches the security analysis of the proposed concepts.

8.1 Discussion of Hybrid Encryption Technique

The design of the hybrid encryption technique follows two main goals: efficiency in handling continuous attributes and minimizing trust in attribute authorities. First, handling dynamic attributes requires means for providing keys on mobile devices. An *online AA* 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: 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.

W.r.t. to encryption security, the hybrid technique is designed such that the LBE parts adds a further level of security to the symmetric session key that is used for message encryption. Here, the XOR operation encrypts the initially generated session key comparable to an one-time pad [32]. Thus, 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. Since messaging policies always include conjunctions of location and further CP-ABE attributes, this approach retains encryption of messages even in case the *embedded LBE AA* is compromised. In case the CP-ABE attributes are compromised, the message is still protected by the additional location-dependent encryption layer. Thus, the hybrid encryption technique allows to realize end-to-end encryption while being able to handle expressive policies.

Also, this approach minimizes the use of pairings in the end-to-end encryption, which broadens the applicability of the encryption technique to a broad range of mobile devices. In turn, the hybrid encryption technique looses full cryptographic collusion resistance w.r.t. the expressive policy. Yet, collusion between receivers or attackers 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 tamper-resistant GPS receivers. In the emergency domain, this assumption is practically fulfilled by all given TETRA mobile communication devices. The application logic required to implement 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 the secure software stack due to the TPM chip of the device [33], additional practical security guarantees can be given.

8.2 Discussion of Re-Identification Technique

The re-identification technique harnesses algebraic operations on pseudonyms. This is possible, since pseudonyms are created via ElGamal encryption in our approach. The operations presented are minimal knowledge under the Decision Diffie-Hellman (DDH) assumption, since ElGamal is semantically secure under the DDH assumption [34, 26]. Practically, minimal knowledge means that the re-identificator learns nothing beyond whether the requested attribute is implicitly attached to a transaction pseudonym or not. A blind reference set could also be defined by a single base pseudonym, thus carrying the semantics of the involved user ID. Yet, the linkability broker can restrict this kind of readout by defining only larger authorization sets that comply with data protection regulations of the emergency management organization.

8.3 Fullfillment of Security Requirements

- `SReq1`: The basic security mechanisms of mutual authentication, message integrity and availability are implemented by the TETRA security architecture. Since the ABM scheme is realized on the TETRA end-to-end encryption layer, they apply to it, too. Especially, device revocation is possible by means of TETRA, without relying on cryptographic application level mechanisms.
- `SReq2`: End-to-end encryption in the messaging is given due to and implemented by the use of the proposed hybrid encryption scheme on the end-to-end encryption layer. Computation security reduces to the same computational assumptions as in CP-ABE. Collusion resistance is given as discussed in section 8.1.
- `SReq3`: Replay attacks are handled on the end-to-end encryption layer: after decryption, the receiver verifies the freshness of the included message ID, ID_m. The receiver rejects messages that contain an ID_m that he already decrypted.
- `SReq4`: Accountability of senders is assured due to two mechanisms: first, each message sent is added to ML, for additional security digitally signed by S. This record can later be audited. Second, messages include a MAC, such that it can be linked to the sender, given that registration is trustworthy.

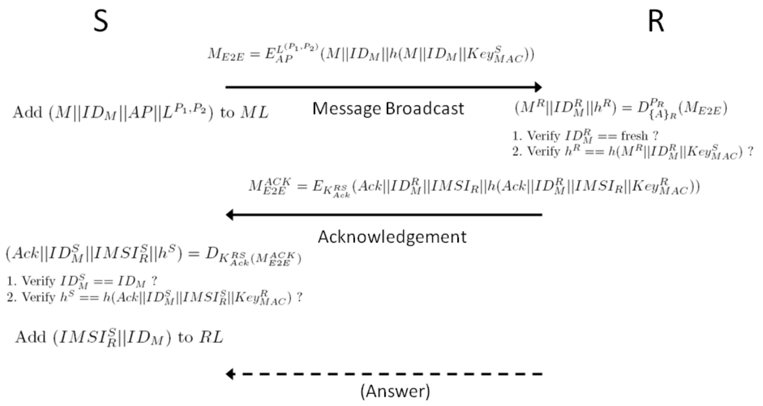
S
R
$M_{E2E} = E_{AP}^{L^{(P_1,P_2)}}(M||ID_M||h(M||ID_M||Key^S_{MAC}))$
Message Broadcast
Add $(M||ID_M||AP||L^{P_1,P_2})$ to ML
$(M^R||ID^R_M||h^R) = D^{P_R}_{\{A\}_R}(M_{E2E})$
1. Verify $ID^R_M ==$ fresh ?
2. Verify $h^R == h(M^R||ID^R_M||Key^S_{MAC})$?
$M^{ACK}_{E2E} = E_{K^{RS}_{Ack}}(Ack||ID^R_M||IMSI_R||h(Ack||ID^R_M||IMSI_R||Key^R_{MAC}))$
Acknowledgement
$(Ack||ID^S_M||IMSI^S_R||h^S) = D_{K^{RS}_{Ack}(M^{ACK}_{E2E})}$
1. Verify $ID^S_M == ID_M$?
2. Verify $h^S == h(Ack||ID^S_M||IMSI^S_R||Key^R_{MAC})$?
Add $(IMSI^S_R||ID_M)$ to RL
(Answer)

Figure 7: Protocol for Sending Step

- `SReq5`: Readers, i.e. the subset of all receivers of a message that satisfied the logical messaging policy, are documented via RL. Unique mobile subscriber identities, $IMSI_R$, can be resolved to real world identities of readers, via linking to information present on $RegL$.

- `SReq6`: Efficiency of the ABM scheme has computational and organizational factors. Regarding computational efficiency, our approach has a low pairing complexity[13] due to the hybrid policy encryption, which renders decryption practically on resource-constraint devices. From the organizational perspective, no online AA is required, such that the interactions in end-to-end key management are reduced to a registration phase.

- `SReq7`: User-friendliness for senders is given in the sense that MundoMessage allows for a single, combined realization of all necessary communication patterns `CP1-CP4`, thus minimizing learning efforts. Further, our approach integrates continuous location attributes into the selection of receivers, which are intuitive selectors for senders.

- `SReq8`: From the receivers' perspective, MundoMessage allows for a seamless integration into personal lives, since privacy protection via transaction pseudonyms is given. Yet, registered specialists and volunteers can be efficiently contacted and requested via location addressing without requiring them to disclose identities along with location information, since re-identification is restricted to a high level of abstraction, as the specification of messaging policies. Also, restrictions on authorization and reference set can directly be imposed in terms of anonymity, since set cardinality directly translates to the degree of anonymity.

9. CONCLUSION

This paper dealt with security issues inherent to ubiquitous one-to-many communication. We used the context of emergency communication as a descriptive real world application scenario. First, we contributed to this domain by elicitating requirements of emergency practioners. Second, we introduced techniques for privacy-respecting re-identificaton of pseudonymous receivers. Third, we proposed a hybrid encryption technique for expressive policies that enables to devise end-to-end secure communication mechanisms which may make use of continuous dynamic location attributes as selectors. Fourth, we introduced and analyzed MundoMessage, our approach to multilaterally end-to-end secure, user-friendly attribute-based messaging.

We believe that ABM concepts have the potential to become an important communication paradigm in mobile and ubiquitous computing scenarios, due to inherent user-friendliness, practicality and flexibility. As next steps, further efficiency evaluations and user trials of our work will follow. Moreover, the novel hybrid encryption technique will be extended to efficiently enable information theoretically secure storage of messages. We will also evaluate the applicability of multi-authority ABE techniques [35] to our setting.

Acknowledgment

This work was supported by CASED (www.cased.de). The authors are responsible for the content of this publication.

10. REFERENCES

[1] K. Rannenberg, "Multilateral Security - a Concept and Examples for Balanced Security," in *Workshop on New Security Paradigms (NSPW '00)*. ACM, 2000, pp. 151–162.

[2] B. Tognazzini, "Design for Usability," in *Security and Usability: Designing Secure Systems That People Can Use*, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, pp. 31–96.

[3] D. Chadwick, G. Lunt, and G. Zhao, "Secure Role Based Messaging," in *IFIP Conference on Communications and Multimedia Security (CMS '04)*, 2004, pp. 303–316.

[13] 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.

[4] M. C. Mont, P. Bramhall, and K. Harrison, "A Flexible Role-Based Secure Messaging Service: Exploiting IBE technology for Privacy in Health Care," in *Workshop on Database and Expert Systems Applications (DEXA '03)*. IEEE CS, 2003, pp. 432–437.

[5] U. M. Maurer, "Modelling a Public-Key Infrastructure," in *ESORICS*, 1996, pp. 325–350.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[7] C. Gentry, "IBE (Identity-Based Encryption)," in *Handbook of Information Security - Volume 2*, H. Bidgoli, Ed. John Wiley and Sons, 2006, pp. 575–592.

[8] R. Bobba, O. Fatemieh, F. Khan, C. A. Gunter, and H. Khurana, "Using Attribute-Based Access Control to Enable Attribute-Based Messaging," in *Annual Computer Security Applications Conference (ACSAC '06)*. IEEE CS, 2006, pp. 403–413.

[9] E. Yuan and J. Tong, "Attribute Based Access Control (ABAC) for Web Services," in *Conference on Web Services (ICWS'05)*. IEEE CS, 2005, pp. 561 – 569.

[10] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology: EUROCRYPT '05*. Springer, 2005, pp. 457–473.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in *ACM Conference on Computer and Communications Security (CCS '06)*. ACM, 2006, pp. 89–98.

[12] S. G. Weber, "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)*. IEEE CS, 2009, pp. 58 – 69.

[13] R. Bobba, O. Fatemieh, F. Khan, A. Khan, C. A. Gunter, H. Khurana, and P. Manoj, "Attribute-Based Messaging: Access Control and Confidentiality," *ACM Trans. Inf. Syst. Secur. (TISSEC)*, vol. 14, 2010.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *IEEE Symposium on Security and Privacy (SP '07)*. IEEE CS, 2007, pp. 321–334.

[15] M. H. Blackmon, "Cognitive Walkthrough," in *Encyclopedia of Human-Computer Interaction - Volume 1*, W. S. Bainbridge, Ed. Berkshire Publishing Group, 2004, pp. 104–107.

[16] C. Endres, A. Wurz, M. Hoffmann, and A. Behring, "A Task-Based Messaging Approach to Facilitate Staff Work," in *International Conference on Information Systems for Crisis Response and Management (ISCRAM 2010)*, 2010.

[17] F. Flentge, S. G. Weber, A. Behring, and T. Ziegert, "Designing Context-Aware HCI for Collaborative Emergency Management," in *Int'l Workshop on HCI for Emergencies in conjunction with CHI '08*, 2008.

[18] L. Scott and D. E. Denning, "A Location Based Encryption Technique and Some of Its Applications," in *ION National Technical Meeting 2003*, 2003, pp. 730–740.

[19] Committee on Planning for Catastrophe, Ed., *Successful Response Starts With A Map: Improving Geospatial Support for Disaster Management*. National Academy Press, 2007.

[20] S. G. Weber, "Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis," in *Conference on Intelligent Networking and Collaborative Systems (INCoS '09)*. IEEE Computer Society, 2009, pp. 119 – 126.

[21] S. G. Weber and M. Mühlhäuser, "Multilaterally Secure Ubiquitous Auditing," in *Intelligent Networking and Collaborative Systems and Applications, SCI 329*. Springer, 2010, pp. 207–233.

[22] B. W. Murgatroyd, "End to End Encryption in Public Safety TETRA Networks," *IE Seminar on Secure GSM and Beyond: End to End Security for mobile Communication*, no. Digest No. 2003/10059, 2003.

[23] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[24] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," in *Financial Cryptography*. Springer, 2003, pp. 103–121.

[25] T. P. Pedersen, "A Threshold Cryptosystem without a Trusted Party (Extended Abstract)," in *Advances in Cryptology: EUROCRYPT '91*. Springer, 1991, pp. 522–526.

[26] M. Jakobsson and A. Juels, "Mix and Match: Secure Function Evaluation via Ciphertexts," in *Advances in Cryptology: ASIACRYPT '00*. Springer, 2000, pp. 162–177.

[27] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[28] Y. Tsiounis and M. Yung, "On the Security of ElGamal Based Encryption," in *Workshop on Practice and Theory in Public Key Cryptography (PKC '98)*. Springer, 1998, pp. 117–134.

[29] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[30] D. E. Denning and L. Scott, "Geo-Encryption - Using GPS to Enhance Data Security," GPS World, 2003.

[31] A. Al-Fuqaha and O. Al-Ibrahim, "Geo-Encryption Protocol for Mobile Networks," *Comput. Commun.*, vol. 30, no. 11-12, pp. 2510–2517, 2007.

[32] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[33] A. D. Brucker, H. Petritsch, and S. G. Weber, "Attribute-Based Encryption with Break-Glass," in *Workshop in Information Security Theory and Practice (WISTP'10)*. Springer, 2010, pp. 237–244.

[34] D. Boneh, "The Decision Diffie-Hellman Problem," in *ANTS-III*, ser. Lecture Notes in Computer Science, vol. 1423. Springer, 1998, pp. 48–63.

[35] S. Müller, S. Katzenbeisser, and C. Eckert, "Distributed Attribute-Based Encryption," in *International Conference on Information Security and Cryptology (ICISC'08)*. Springer, 2008, pp. 20–36.