Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE 2010 27–30 June 2010.

Multi-authority attribute based encryption with honest-but-curious central authority

Vladimir Božović[1], Daniel Socek[2], Rainer Steinwandt[3] and Viktória I. Villányi[4]

[1] *Department of* ***** insert info*****, *University of Montenegro, Montenegro*

[2] *CoreTex Systems LLC, 2851 S Ocean Blvd. 5L, Boca Raton, FL 33432, U.S.A.*

[3] *Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, U.S.A.*

[4] ***** insert info*****, *Keiser University,* ***** insert info*****

emails: `vladobozovic@yahoo.com`, `dsocek@gmail.com`, `rsteinwa@fau.edu`, ***** insert info*****

Abstract

An attribute based encryption scheme capable of handling multiple authorities was recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption scheme presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently capable of decrypting arbitrary ciphertexts created within the system. We present a multi-authority attribute based encryption scheme in which only the set of recipients defined by the encrypting party can decrypt a corresponding ciphertext. The central authority is viewed as "honest-but-curious": on the one hand it honestly follows the protocol, and on the other hand it is curious to decrypt arbitrary ciphertexts thus violating the intent of the encrypting party. The proposed scheme, which like its predecessors relies on the Bilinear Diffie-Hellman assumption, has a complexity comparable to that of Chase's scheme. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority.

Key words: pairing-based cryptography, attribute based encryption
MSC 2000: 94A60

1 Introduction

In both standard *public key encryption* and *identity based encryption* a message is to be transmitted to a single recipient known at the time of encryption. Similarly, *broadcast encryption* addresses scenarios where a sender explicitly specifies a set of receivers (or revoked users) when encrypting a plaintext. In contrast, in an *attribute based encryption* scheme, the sender does not provide an explicit list of recipients or revoked users when encrypting a plaintext, but instead, the recipient of a ciphertext is specified through a set of credentials, also referred to as the *attributes*, which are sufficient to decrypt a ciphertext. Fuzzy identity based encryption proposed by Sahai and Waters [7] can be used to address such a setting, if all attributes are controlled by a single authority.

The starting point of the current paper is a recent proposal of Chase [4] which considers *multi-authority attribute based encryption*, therewith solving an open problem from [7]. Chase's scheme is capable of handling disjoint sets of attributes that are distributed among multiple authorities. In this setting, an encrypting party specifies a set of attributes $\mathcal{A}_C$ with the attributes in $\mathcal{A}_C$ being controlled by several authorities. Let $\mathcal{A}_k$ be the set of attributes controlled by authority k. Then the ciphertext C associated with the attribute set $\mathcal{A}_C$ can only be decrypted by those users u with a set of attributes $\mathcal{A}_u$ for which the cardinality of the intersection $\mathcal{A}_u \cap \mathcal{A}_k \cap \mathcal{A}_C$ exceeds the respective threshold d_k, for each authority k.

As pointed out in [4], one of the primary challenges in implementing such a multi-authority attribute based encryption scheme is the prevention of collusion attacks among users that obtain secret key components from different authorities. Moreover, it is desirable that there be no communication between the individual authorities. To overcome these difficulties, Chase's scheme relies on a trusted central authority. The resulting scheme is capable of tolerating multiple corrupted authorities, but the honesty of the central authority remains of vital importance since, by the constriction from [4], the trusted authority has the capability of decrypting every ciphertext.

Our contribution. Building on Chase's proposal, we construct a threshold scheme for multi-authority attribute based encryption which offers the same security guarantees provided by Chase's construction, but in addition can tolerate an honest-but-curious central authority. Assuming the central authority is honest during the initialization phase, the indistinguishability of encryptions is guaranteed. As in [4], our security analysis is in the selective ID model and builds on the Decisional Bilinear Diffie Hellman assumption.

Related work. Since Shamir posed the problem of identity based encryption [8], various proposals have been made, a very partial list being the work in [6, 9, 10, 2, 5]. Building on the Bilinear Diffie Hellman assumption and the selective ID model [3, 1], at EUROCRYPT 2005 Waters presented an identity based encryption scheme in the standard model [11]. Sahai and Water's proposal for a fuzzy identity based encryption [7] provides an attribute based encryption with a single authority. Here, *fuzzy* refers to an identity id' being able to decrypt a ciphertext encrypted by an identity id if and only if id and id' are close to each other in the "set overlap" distance metric. This is of interest when dealing with noisy inputs, such as biometric templates. Building on the ideas from [7], Chase proposed a solution for multi-authority attribute based encryption, provided that a trusted central authority is available [4]. Our proposal aims at improving Chase's construction by imposing a weaker assumption on the central authority without paying a high cost in terms of efficiency.

2 Notation and preliminaries

As already mentioned, our proposal relies on the Decisional Bilinear Diffie Hellman assumption. For the sake of clarity, the next sections review the relevant terminology related to bilinear maps and multi-authority attribute based encryption. Section 2.3 discusses the security model where, like in [4], we make use of the selective ID model.

2.1 Bilinear maps and the Bilinear Diffie Hellman assumption

Let G_1, G_2 be groups of prime order p, and let P a generator of G_1. We assume p to be superpolynomial in the security parameter ℓ and that all group operations in G_1 and G_2 can be computed efficiently, i. e., in probabilistic polynomial time. We use additive notation for G_1 and multiplicative notation for G_2. By $e : G_1 \times G_1 \longrightarrow G_2$ we denote an admissible bilinear map, i. e., all of the following hold [2]:

- For all $P, Q \in G_1$ and for all $\alpha, \beta \in \mathbb{Z}$ we have $e(\alpha P, \beta Q) = e(P, Q)^{\alpha\beta}$.
- We have $e(P, P) \neq 1$, i. e., $e(P, P)$ is a generator of G_2.
- There is a probabilistic polynomial time algorithm that for arbitrary $P, Q \in G_1$ computes $e(P, Q)$.

In the above setting, the Decisional Bilinear Diffie Hellman ($\mathsf{D\text{-}BDH}$) problem in (G_1, G_2, e) is the problem of distinguishing between the challenger's possible outputs in the following experiment: The challenger chooses $\alpha, \beta, \gamma, \eta \leftarrow \{0, 1, \ldots, p-1\}$ independently and uniformly at random, flips a fair binary coin $\delta \leftarrow \{0, 1\}$, and then outputs the tuple

$$(P, \alpha P, \beta P, \gamma P, e(P, P)^{\delta \cdot \alpha\beta\gamma + (1-\delta)\cdot\eta}).$$

In other words, with probability 1/2 the last component of the challenger's output is $e(P, P)^{\alpha\beta\gamma}$, and with probability 1/2 the last component is a uniformly at random chosen element from G_2. We define the *advantage* of algorithm $\mathcal{A}$ in solving the $\mathsf{D\text{-}BDH}$ problem as

$$\mathrm{Adv}^{\mathsf{bdh}}_{\mathcal{A}}(\ell) := \Pr(\delta' = \delta) - \frac{1}{2}$$

where δ' is the output of $\mathcal{A}$ when trying to guess the value of the fair binary coin δ. We say that an algorithm $\mathcal{A}$ has a *non-negligible advantage* in solving the $\mathsf{D\text{-}BDH}$ problem, if $\mathrm{Adv}^{\mathsf{bdh}}_{\mathcal{A}}$ is not negligible[1] where the probability is over the randomly chosen $\alpha, \beta, \gamma, \eta$ and the random bits consumed by $\mathcal{A}$.

[1] We refer to a function $f : \mathbb{N}_{>0} \longrightarrow \mathbb{R}$ as negligible, if $|f| = |f(\ell)| \in \frac{1}{\ell^{\omega(1)}}$.

Definition 1 (Decisional Bilinear Diffie Hellman assumption) *The Decisional Bilinear Diffie Hellman assumption holds for (G_1, G_2, e) if there exists no probabilistic polynomial time algorithm having non-negligible advantage in solving the above* D-BDH *problem.*

2.2 Authorities, attributes and users

Let $\mathcal{K}$ be the polynomial size set of authorities and $\mathcal{U}$ the polynomial size set of users we consider, and denote by $\mathcal{A}_k$ the polynomial size set of attributes handled by authority $k \in \mathcal{K}$. We impose that the sets $\mathcal{A}_k$ are pairwise disjoint, i.e., the *universal attribute set*

$$\mathcal{A} := \biguplus_{k \in \mathcal{K}} \mathcal{A}_k$$

is the disjoint union of the $\mathcal{A}_k$. In addition to the authorities $k \in \mathcal{K}$, there is one central authority $k_{\mathsf{CA}} \notin \mathcal{K}$ which we will model as honest-but-curious—the central authority k_{CA} honestly follows the protocol, but will try to decrypt ciphertexts sent by users in the system. During an initialization phase we allow communication between k_{CA} and k for each authority $k \in \mathcal{K}$, but thereafter no communication between the central authority and the authorities $k \in \mathcal{K}$ is possible: while the central authority k_{CA} is involved in setting up the system, we do not want to rely on k_{CA} being available throughout the complete lifetime of the system. Also, we do not allow any communication among the authorities in $\mathcal{K}$.

To distinguish different users, we follow [4] and assume that each user $u \in \mathcal{U}$ has a unique identifier. Depending on the application, the identifier could refer to a social security number or a passport number, for instance. We denote the set of those attributes in $\mathcal{A}$ that are available to user $u \in \mathcal{U}$ by $\mathcal{A}_u$. Similarly, we write $\mathcal{A}_C$ for the set of attributes that is associated with a ciphertext C. This set $\mathcal{A}_C$ is chosen by the encrypting party as part of the input to the encryption algorithm, the other part of the input being the plaintext. We associate with each authority $k \in \mathcal{K}$ a threshold $d_k \in \mathbb{N}_{>0}$. The goal is that exactly those users u satisfying

$$|\mathcal{A}_u \cap \mathcal{A}_k \cap \mathcal{A}_C| \geq d_k \text{ for every } k \in \mathcal{K}$$

are able to decrypt the ciphertext C. In other words, for each authority k, user u must have at least d_k of the attributes that have been specified at the time of encryption. To decrypt a ciphertext, user $u \in \mathcal{U}$ uses the secret keys obtained during the initialization phase from the authorities $k \in \mathcal{K}$. Figure 1 lists the main components of a multi-authority attribute based encryption scheme (cf. [4]).

Remark 1 *Unlike [4] we do not make use of a* central key generation algorithm*, run by the central authority k_{CA} to generate secret keys for users u. Without loss of generality, in the security model we therefore will not give the adversary the possibility to query k_{CA} for private user keys. In the scheme we discuss, private user keys are generated by the attribute authorities $k \in \mathcal{K}$ only.*

Setup. A probabilistic polynomial time algorithm[a] that given the security parameter 1^ℓ, a list of pairwise disjoint sets of attributes $[\mathcal{A}_k]_{k\in\mathcal{K}}$ and thresholds $[d_k]_{k\in\mathcal{K}}$ generates

- a (public key, secret key)-pair for each attribute authority $k \in \mathcal{K}$
- public system parameters.

Attribute key generation. A probabilistic polynomial time algorithm that given an attribute authority k's secret key, the corresponding threshold d_k, a (unique identifier of a) user u and a subset $\mathcal{A}_u \subseteq \mathcal{A}_k$ outputs decryption keys for user u.

Encryption. A probabilistic polynomial time algorithm that given a plaintext, attributes $\mathcal{A}_C \subseteq \mathcal{A}$ and the public system parameters, outputs a ciphertext C.

Decryption. A deterministic polynomial time algorithm that given a set of decryption keys for a set of attributes $\mathcal{A}_u$ and a ciphertext C encrypted with attribute set $\mathcal{A}_C$, outputs the corresponding plaintext M if $|\mathcal{A}_u \cap \mathcal{A}_k \cap \mathcal{A}_C| \geq d_k$ for all attribute authorities $k \in \mathcal{K}$; otherwise it outputs an error symbol $\perp$.

[a] It may be preferable to realize this computation in a distributed fashion, involving individual attribute authorities and some central authority. Below we will use such a distributed realization.

Figure 1: Algorithms in a multi-authority attribute based encryption scheme.

A crucial feature of a multi-authority attribute based encryption scheme is the prevention of collusions among users: we want to prevent that any set of users, each of which is not able to decrypt a ciphertext C, can combine their information to decrypt C. The security definition discussed next tries to capture this design goal.

2.3 Security model

Like [4], we use a selective ID model for the security analysis. The adversary $\mathcal{H}$ has to specify the set of attributes that he wants to attack before receiving any public keys of the system. Figure 2 shows the game an adversary has to win to defeat the security of our scheme. As in [4], for our security analysis we impose the technical restriction that the adversary does not query the same attribute authority twice for private keys of the same user.

For a multi-authority attribute based encryption scheme to be secure, we require that there is no efficient algorithm achieving a non-negligible advantage in the game in Figure 2. More specifically, we define the advantage of an adversary $\mathcal{H}$ in the game in Figure 2 as

$$\mathrm{Adv}^{\mathsf{sid}}_{\mathcal{H}}(\ell) := \Pr(\delta' = \delta) - \frac{1}{2}$$

and make the following definition.

Setup. 1. Given the security parameter 1^ℓ, the adversary $\mathcal{H}$ outputs

- a non-empty list $\mathcal{U}$ of (unique identifiers of) users
- a non-empty list $\mathcal{K}$ of (unique identifiers of) attribute authorities
- a list $[(\mathcal{A}_k, \mathsf{corrupted}, d_k)]_{k\in\mathcal{K}}$ of non-empty, pairwise disjoint attribute sets, each along with a threshold $d_k \in \mathbb{N}_{>0}$ and a flag indicating if the respective authority is corrupted. There must be at least one uncorrupted authority.[a]
- a non-empty set of attributes $\mathcal{A}_C \subseteq \biguplus_{k\in\mathcal{K}} \mathcal{A}_k$ that will be associated with the challenge ciphertext.

2. The public and secret keys are generated, and $\mathcal{H}$ learns

- the public keys of all attribute authorities
- the public system parameters
- the complete history of all those authorities $k \in \mathcal{K}$ that are corrupted.

Secret key queries. The adversary can query the authorities $k \in \mathcal{K}$ for private user keys for attributes in $\mathcal{A}_k$ for user u. Whenever the adversary queries k for a secret key for attribute $a \in \mathcal{A}_k$ for user u, the attribute a is added to the (initially empty) set $\mathcal{A}_u$. The only restrictions for secret key queries are the following:

- at any time, for each user u there is at least one uncorrupted authority $\hat{k} = \hat{k}(u)$ with $|\mathcal{A}_u \cap \mathcal{A}_{\hat{k}} \cap \mathcal{A}_C| < d_{\hat{k}}$[b]
- for each user u, no authority $k \in \mathcal{K}$ is queried more than once for private keys of u.

Challenge. 1. The adversary $\mathcal{H}$ outputs two equal length messages M_0, M_1.

2. The challenger flips a fair binary coin $\delta \leftarrow \{0,1\}$ and then applies the encryption algorithm to M_δ and the attribute set $\mathcal{A}_C$.
3. The resulting ciphertext C is given to the adversary $\mathcal{H}$.

Further secret key queries. The adversary can query for further private keys of users, subject to the same restrictions as before: for each user u there is at least one uncorrupted authority $\hat{k} = \hat{k}(u)$ with $|\mathcal{A}_u \cap \mathcal{A}_{\hat{k}} \cap \mathcal{A}_C| < d_{\hat{k}}$, and for each user u, no authority $k \in \mathcal{K}$ is queried more than once for private keys of u.

Guess. The adversary $\mathcal{H}$ outputs a guess δ' for the challenger's secret coin δ.

[a] Note that the central authority k_{CA} is not included in this list and in particular cannot be corrupted.

[b] The uncorrupted authority $\hat{k} = \hat{k}(u)$ may be different for each user u.

Figure 2: Attacking multi-authority attribute based encryption in the selective ID model.

Definition 2 (Security in the selective ID model) *A scheme for multi-authority attribute based encryption is* secure in the selective ID model*, if for all probabilistic polynomial time adversaries $\mathcal{H}$, the advantage* $\mathrm{Adv}^{\mathsf{sid}}_{\mathcal{H}}(\ell)$ *is negligible.*

The security requirement in Definition 2 does not address the question which information is available to the central authority. Specifically, in Chase's scheme [4], the central authority has the capability of reading arbitrary ciphertexts constructed by the users within the system. To express a requirement that limits the possibilities of an honest-but-curious central authority, we take a more detailed look at the setup phase, which is combined into a single algorithm in Figure 1. More precisely, this step can be seen as a simple protocol where the central authority k_{CA} securely communicates with the attribute authorities.

Remark 2 *From a practical perspective, it is desirable to have no communication among attribute authorities, and only very limited interaction of the central authority with each attribute authority. In the protocol in Section 3.1, the central authority sends one message to each attribute authority and derives the public system parameters from the replies.*

The game in Figure 3 captures a setting where an honest-but-curious central authority tries to violate the indistinguishability of ciphertexts. We introduce a "curious" algorithm $\mathcal{B}$ which, similarly as the "outside adversary" $\mathcal{H}$ in Figure 2, fixes the attribute sets and their distribution among the attribute authorities. Further on, $\mathcal{B}$ specifies the set of attributes that will be associated with the challenge ciphertext. At the end of the setup phase, $\mathcal{B}$ learns the complete state of the central authority, and based on this knowledge then tries to violate the indistinguishability of ciphertexts.
For an algorithm $\mathcal{B}$, we define the advantage in the game in Figure 3 as

$$\mathrm{Adv}^{\mathsf{ca}}_{\mathcal{B}}(\ell) := \left| \Pr(\delta' = \delta) - \frac{1}{2} \right| .$$

Definition 3 (Tolerating an honest-but-curious central authority) *A scheme for multi-authority attribute based encryption* can tolerate an honest-but-curious central authority*, if for all probabilistic time algorithms $\mathcal{B}$, the advantage* $\mathrm{Adv}^{\mathsf{ca}}_{\mathcal{B}}(\ell)$ *is negligible.*

Remark 3 *Unlike for the adversary $\mathcal{H}$ in Figure 2, we do not require that an honest-but-curious central authority specifies the challenge attributes $\mathcal{A}_C$ in advance: algorithm $\mathcal{B}$ in Figure 3 does not have to provide this set before the challenge phase.*

We are now in the position to describe our suggestion for a multi-authority attribute based encryption scheme and to discuss its security in the sense of both Definition 2 and Definition 3.

Setup

1. Given the security parameter 1^ℓ, the algorithm $\mathcal{B}$ outputs
   - a non-empty list $\mathcal{U}$ of (unique identifiers of) users
   - a non-empty list $\mathcal{K}$ of (unique identifiers of) attribute authorities
   - a list $[(\mathcal{A}_k, \mathsf{corrupted}, d_k)]_{k\in\mathcal{K}}$ of non-empty, pairwise disjoint attribute sets, each along with a threshold $d_k \in \mathbb{N}_{>0}$ and a flag indicating if the respective authority is corrupted. There must be at least one uncorrupted authority.[a]
2. The public and secret keys of all authorities $k \in \mathcal{K}$ are generated, and $\mathcal{B}$ learns
   - all public keys
   - the public system parameters
   - the complete history of all those authorities $k \in \mathcal{K}$ that are corrupted
   - the complete history of the central authority k_{CA}.

Challenge

1. The algorithm $\mathcal{B}$ outputs two equal length messages M_0, M_1 and a non-empty set of attributes $\mathcal{A}_C \subseteq \biguplus_{k\in\mathcal{K}} \mathcal{A}_k$.
2. The challenger flips a fair binary coin binary $\delta \leftarrow \{0, 1\}$ and then applies the encryption algorithm to M_δ and the attribute set $\mathcal{A}_C$.
3. The resulting ciphertext C is given to $\mathcal{B}$.

Guess

The algorithm $\mathcal{B}$ outputs a guess δ' for the challenger's secret coin δ.

[a]Note that the central authority k_{CA} is not included in this list and in particular cannot be corrupted.

Figure 3: Dealing with an honest-but-curious central authority.

3 Proposed protocol

We adopt the notation from Section 2 with G_1, G_2 being groups of prime order p, P a generator of G_1 and $e : G_1 \times G_1 \longrightarrow G_2$ an admissible bilinear map. We assume the unique identifiers for users u and for the attribute authorities $k \in \mathcal{K}$ to be public. Similarly, we assume the sets of attributes $\mathcal{A}_k$ and the corresponding threshold d_k to be public—in particular, all these values are known to the central authority k_{CA}, which we invoke (only) in the setup phase. In order to generate secret keys for users, we assume that each attribute $a \in \mathcal{A}$ can be identified with a number $\iota(a) \in \{1, \ldots, p-1\}$—for practical purposes, $\iota(a)$ could be based on a hash value, for instance.

3.1 The proposed protocol

3.1.1 Setup.

The setup phase requires one message to be sent from the central authority to each of the attribute authorities. It is assumed that the adversary has no possibility to interfere with or to access this communication:

The central authority k_{CA} chooses, for each pair $(k,u) \in \mathcal{K} \times \mathcal{U}$, uniformly at random a secret value $s_{k,u} \leftarrow \{0,\dots,p-1\}$. In additon, k_{CA} chooses $\sigma \in \{0,\dots p-1\}$ uniformly at random, and for each $u \in \mathcal{U}$ computes a "dummy secret" $s_{k_{\mathsf{CA}},u} := \sigma - \sum_{k\in\mathcal{K}} s_{k,u}$. The sequence

$$[\underbrace{s_{k,u} \cdot P}_{=:S_{k,u}}]_{u\in\mathcal{U}}$$

is sent to attribute authority k ($k \in \mathcal{K}$), and k_{CA} publishes the public system parameters

$$\Big([s_{k_{\mathsf{CA}},u} \cdot P]_{u\in\mathcal{U}}, \underbrace{e(P,P)^{\sigma}}_{=:\mathsf{pk}}\Big).$$

Remark 4 *The value $s_{k_{\mathsf{CA}},u} \cdot P$ is only needed by user u. To decrease the size of the public parameters, instead of publishing the sequence $[s_{k_{\mathsf{CA}},u} \cdot P]_{u\in\mathcal{U}}$, alternatively a scenario could be considered where $s_{k_{\mathsf{CA}},u} \cdot P$ is transmitted to u (only).*

Attribute authority $k \in \mathcal{K}$ receives the corresponding sequence of $S_{k,u}$-values from k_{CA} and chooses a value $r_k \leftarrow \{0,\dots,p-1\}$ uniformly at random. Moreover, for each of its attributes $a \in \mathcal{A}_k$, a secret value $t_{k,a} \leftarrow (\mathbb{Z}/p\mathbb{Z})^*$ is chosen uniformly at random by k, and the pair

$$\Big(e(P,P)^{r_k}, [\underbrace{t_{k,a} \cdot P}_{=:T_{k,a}}]_{a\in\mathcal{A}_k}\Big)$$

forms k's public key. The secret key of k contains the aforementioned values r_k, $[S_{k,u}]_{u\in\mathcal{U}}$, and $[t_{k,a}]_{a\in\mathcal{A}_k}$. Finally, for each user $u \in \mathcal{U}$, attribute authority k chooses uniformly at random a secret polynomial $f_{k,u} \in \mathbb{F}_p[X]$ of degree $< d_k$.

Remark 5 *The value $e(P,P)^{r_k}$ is only used during encryption and decryption to compute the product $\mathsf{pk} \cdot \prod_{k\in\mathcal{K}} e(P,P)^{r_k}$—which is ciphertext-independent. If one allows the attribute authorities to contribute to the generation of the public system parameters, the $e(P,P)^{r_k}$-component in the attribute authorities' public keys can be omitted. To do so, the public system parameter $\mathsf{pk} = e(P,P)^{\sigma}$ can be replaced with $e(P,P)^{\sigma+\sum_{k\in\mathcal{K}} r_k}$.*

3.1.2 Attribute key generation.

To extract the secret decryption key associated with an attribute $a \in \mathcal{A}_k \cap \mathcal{A}_u$ for a user $u \in \mathcal{U}$, attribute authority k proceeds as follows:

- The secret value $X_{k,u} := S_{k,u} + (r_k - f_{k,u}(0)) \cdot P$, which depends on k and u, but not the specific attribute a, is computed and given to u.
- The attribute-specific value $D_{k,u,a} := \frac{f_{k,u}(\iota(a))}{t_{k,a}} \cdot P$ is computed and given to u.

3.1.3 Encryption.

To encrypt a plaintext $M \in G_2$ with associated attribute set $\mathcal{A}_C \subseteq \mathcal{A}$, the encrypting party chooses $s \leftarrow \{0, \ldots, p-1\}$ uniformly at random and computes the ciphertext

$$\left(\left(\mathsf{pk} \cdot \prod\nolimits_{k \in \mathcal{K}} e(P,P)^{r_k}\right)^s \cdot M, s \cdot P, [s \cdot T_{k,a}]_{a \in \mathcal{A}_C}\right).$$

3.1.4 Decryption.

Let $C = ((\mathsf{pk} \cdot \prod_{k \in \mathcal{K}} e(P,P)^{r_k})^s \cdot M, s \cdot P, [s \cdot T_{k,a}]_{a \in \mathcal{A}_C})$ be a ciphertext with associated attribute set $\mathcal{A}_C$, and suppose that user u's attribute set $\mathcal{A}_u$ satisfies $|\mathcal{A}_u \cap \mathcal{A}_k| \geq d_k$ for all $k \in \mathcal{K}$. Then u can recover the plaintext M as follows.

1. For each $k \in \mathcal{K}$, he chooses d_k attributes $a \in \mathcal{A}_u \cap \mathcal{A}_k$, and computes
$$e(s \cdot T_{k,a}, D_{k,u,a}) = e(P,P)^{f_{k,u}(\iota(a)) \cdot s}.$$
Then, using Lagrange polynomial interpolation, u computes
$$e(P,P)^{f_{k,u}(0) \cdot s}.$$
2. Further on, for each $k \in \mathcal{K}$, user u can use the $X_{k,u}$-component of his secret key to compute $e(X_{k,u}, s \cdot P) = e(P,P)^{(s_{k,u} + r_k - f_{k,u}(0)) \cdot s}$.
3. Multiplying $e(s \cdot P, s_{k_{\mathsf{CA}},u} \cdot P)$ with all of the above values yields
$$\begin{aligned} & e(s \cdot P, s_{k_{\mathsf{CA}},u} \cdot P) \cdot \prod_{k \in \mathcal{K}} e(P,P)^{f_{k,u}(0) \cdot s} \cdot e(P,P)^{(s_{k,u} + r_k - f_{k,u}(0)) \cdot s} \\ = \; & e(P,P)^{s \cdot s_{k_{\mathsf{CA}},u}} \cdot e(P,P)^{s \cdot \sum_{k \in \mathcal{K}} (s_{k,u} + r_k)} \\ = \; & e(P,P)^{s \cdot (\sigma + \sum_{k \in \mathcal{K}} r_k)} \\ = \; & \left(\mathsf{pk} \cdot \prod_{k \in \mathcal{K}} e(P,P)^{r_k}\right)^s. \end{aligned}$$
By inverting this element and multiplying the result with the first component of the ciphertext, the plaintext M can be recovered.

3.2 Adding new authorities

The "dummy secrets" $s_{k_{\mathsf{CA}},u}$ facilitate the introduction of new authorities to a previously established protocol. To add a new authority k^*, the central authority k_{CA} replaces the old value σ with a new uniformly at random chosen σ', and replaces each $s_{k_{\mathsf{CA}},u}$ with $\sigma' - \sum_{k \in \mathcal{K} \cup \{k^*\}} s_{k,u}$. Then the updated "dummy public keys" $s_{k_{\mathsf{CA}},u} \cdot P$ have to be communicated to the users, and the new authority k^* can compute its secret and public key as before.

4 Security analysis

The protocol proposed in Section 3 can be shown to be secure both both in the sense of Definition 2 and Definition 3. Proofs for the subsequent two theorems are given in the extended version of this paper.

Theorem 1 *Suppose there exists a probabilistic polynomial time adversary $\mathcal{H}$ against the protocol in Section 3.1 having a non-negligible advantage in the game in Figure 2. Then there is a probabilistic polynomial time algorithm $\mathcal{S}$ having a non-negligible advantage in solving the* D-BDH*-problem.*

Our proof of Theorem 1 builds on the analysis of Chase's scheme in [4], and it is worth noting that the reduction to a D-BDH adversary $\mathcal{S}$ in the proof is tight: Essentially, the advantage of the adversary $\mathcal{H}$ violating security in the selective ID model is only halved at the cost of simulating the attribute authorities k and the central authority k_{CA}.

Theorem 2 *Let $\mathcal{B}$ be a probabilistic polynomial time adversary against the protocol in Section 3.1 having a non-negligible advantage in the game in Figure 3. Then there is a probabilistic polynomial time algorithm $\mathcal{S}$ having a non-negligible advantage in solving the* D-BDH*-problem.*

To prove Theorem 2, i. e., that the proposed scheme can tolerate an honest-but-curious central authority in the sense of Definition 3, a similar argument as in the proof of Theorem 1 can be used. It turns out that again there is a tight security reduction: Essentially, for the price of simulating the central authority and the attribute authorities, from an adversary $\mathcal{B}$ described in the game from Figure 3, we obtain a D-BDH adversary whose advantage is half the advantage of $\mathcal{B}$.

5 Conclusion

Building on the proposal for multi-authority based attribute based encryption from [4], we constructed a scheme where the central authority is no longer capable of decrypting arbitrary ciphertexts created within the system. In addition to providing security in the selective ID model, the proposed system can tolerate an honest-but-curious central authority. Since both Chase's scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase's construction. However, since only the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is recommended in applications where security against such a central authority is required.

References

[1] D. Boneh and X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2004.

[2] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001.

[3] R. Canetti, S. Halevi, and J. Katz. A Forward-Secure Public-Key Encryption Scheme. In E. Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 255–271. Springer-Verlag, 2003.

[4] M. Chase. Multi-authority Attribute Based Encryption. In S.P. Vadhan, editor, *Theory of Cryptography – TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 515–534. Springer-Verlag, 2007.

[5] C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In B. Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer-Verlag, 2001.

[6] Y. Desmedt and J-J. Quisquater. Public-key Systems Based on the Difficulty of Tampering (Is there a difference between DES and RSA?). In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 111–117. Springer-Verlag, 1987.

[7] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer-Verlag, 2005.

[8] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology – CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1985.

[9] H. Tanaka. A Realization Scheme for the Identity-Based Cryptosystem. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 340–349. Springer-Verlag, 1988.

[10] S. Tsujii and T. Itoh. An ID-Based Cryptosystem Based on the Discrete Logarithm Problem. *IEEE Journal on Selected Areas in Communications*, 7(4), May 1989.

[11] B. Waters. Efficient Identity-Based Encryption Without Random Oracles. In R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer-Verlag, 2005.