A Tunable Broadcast Encryption Scheme

David Lubicz, Thomas Sirvent

David Lubicz
david.lubicz@univ-rennes1.fr

Thomas Sirvent
thomas.sirvent@m4x.org

CELAR
BP 57419 35174 Bruz Cedex
France

Abstract. In this paper, we describe yet another broadcast encryption scheme for stateless receivers. The main difference between our scheme and the classical schemes derived from the complete subtree and its subsequent improvements is that in our scheme the group management is based upon a more adaptable data structure. In these classical schemes, users must be spread on a tree structure where each level of the tree is associated to some distinguishing property of the users. The fact that the underlying data structure is a fixed tree is a strong limitation for some applications where an operator wants to select users very dynamically following criterions with changing levels of priority. Our scheme may be thought as if in the complete subtree it would be possible to exchange the different level of the tree in order to make it very efficient to revoke or select a class of users. It is also very efficient in the cases where there exists very unbalanced groups of users.
This scheme allows one to select or revoke users by sending ciphertexts of linear size with respect to the number of groups which is in general far less than the number of users. Moreover, by using a specific group repartition, it is possible to recover a tree structure in order to apply the classical methods which guarantee that our scheme is in general as efficient as a usual ones.
We prove that our scheme is fully collusion secure in the generic group with pairing model.

Keywords: Public-key broadcast encryption, Group management, Generic model of groups with pairing

1 Introduction

A broadcast scheme is used whenever an emitter wants to send messages to several recipients using an unsecured channel. Such a scheme actually allows the broadcaster to choose dynamically a subset of privileged users inside the set of all possible recipients and to send a ciphertext, readable only by the privileged users. This kind of schemes is helpful in numerous commercial applications such as the broadcast of multimedia content or pay-per-view television. This problematic was first described in [FN93].

We are interested in broadcast systems where one can specify some groups of users. These groups, possibly with a non-empty intersection, contain users that the broadcaster wants to treat in uniform manner, in order to select or exclude them together by sending some well-formatted messages.

Such setting exists in numerous applications of broadcast systems. Actually, if one considers a big system of pay-per-view television, one can group the users

by considering some useful criterion such as the kind of subscription, the period of subscription, if they have or have not access to some kind of content.

Take for instance the case of a family which is a client of such a system: this family, call it "A", has a subscription on some satellite television channels but it does not have access to specific channels with recent contents, which are only accessible on a pay per view basis. This family "A"'s subscription begins the 8th of August 2007 and runs for one year. Moreover, this family "A" has two receivers (called "A1" and "A2"), with one of them restricted to children's programs. A family "B" has also two receivers ("B1" and "B2") but with a different kind of subscription package: the subscription starts from the 19th of May 2007 and runs for 18 months, it contains only music channels and the receiver "B1" is offline from 11pm to 7am.

In a system with such numerous constraints, the broadcaster must grant or ban the access to the receivers, with quick and important changes in the set of privileged users.

In this paper, we construct a fully collusion secure public-key broadcast encryption system which allows the broadcaster to easily manage predetermined groups of users. This property contrasts from the usual SD family of broadcast encryption schemes where the underlying binary structure imposes strong constraints on group management as explained later on. Our construction is based upon the intractability of a problem defined for cyclic groups together with a pairing: such kind of problems were introduced in cryptographic schemes in [Jou00] for tripartite Diffie-Hellman.

In this scheme, each group is associated with a characteristic, i.e. an element of $(\mathbb{Z}/p\mathbb{Z})$. Each user u is described by the set $\Omega(u)$, containing the characteristics associated to the groups he belongs to. We present a way to efficiently encrypt messages for the users u such that $\Omega(u)$ contains Ω^N (set of required characteristics), and $\Omega(u)$ has an empty intersection with Ω^R (set of revoked characteristics). In this way, a broadcaster can choose two sets of groups, and encrypt messages for members of all groups in the first set, but excluding members of any group in the second set. These encryptions are called basic encryptions, and the size of a basic ciphertext is linear in the number of groups involved in this encryption ($|\Omega^N| + |\Omega^R|$). A ciphertext is built nearly like in the subset-cover paradigm, presented by Naor et al. in [NNL01], by considering a sequence of basic encryptions addressed to subsets of users, whose union is exactly the privileged set.

1.1 Related Work

The first broadcast schemes were based upon stateful receivers, which means that the receivers have a memory that can store some information about the past messages. Such receivers have the possibility to refresh their decryption key using information given in broadcasted messages. This is the case of "Logical Key hierarchy" (LKH) presented independently in [WGL98] and in [WHA99], where the users have assigned positions as leaves in a tree, and have keys corresponding to nodes on the path from user's leaf to the root. The key corresponding to the root is used to encrypt messages to users, and a rekey occurs, using

keys corresponding to internal nodes, when users are revoked or when a new user joins. These techniques have been later improved in [CGI+99,CMN99,PST01].

These schemes are aimed at practical applications where the set of privileged users is updated rarely and in a marginal way. The ciphertexts are very short and are computed from a key known by all current users. In return, changing the set of privileged users (add or exclude a user) costs a lot and must be done on a per user basis: each change entails the distribution of a new global key to privileged users. Moreover, this can only be done if all users are on-line which is a strong limitation in some applications.

Broadcast schemes of a different kind have been later introduced: the goal is to avoid frequent rekeys. In [KRS99,GSW00], users have different decryption keys, and these decryption keys are known by well-chosen sets of users. When the broadcaster wants to exclude a given set of users, it builds ciphertexts corresponding to decryption keys that these specific users do not know. Rekey occurs only after large permanent modifications of the privileged set of users, but the ciphertexts are longer than with the previous method.

Stateless receivers extend this last case: in [NNL01], the broadcaster can choose any set of privileged users without any rekey, i.e. the receivers can keep the same decryption keys during the whole life of the broadcast system. Theses schemes, called Complete Subtree (CS) and Subset Difference (SD) are based on a binary tree structure, where users are placed in the leaves. They have subsequently been improved in [HS02,GST04], and an efficient extension to the public-key case based on hierarchical identity-based encryption has been proposed in [DF02]. This extension has been confirmed in [BBG05] with the first hierarchical identity-based encryption with constant-size ciphertexts.

New public-key schemes have been proposed in [BGW05], where it is claimed that the first described scheme has constant-size decryption keys and ciphertexts, with an encryption key linear in the number of users, while the second one has ciphertexts and public key with a size linear in the square root of the number of users. In these schemes, the knowledge of the decryption key is however not sufficient to decrypt a ciphertext: the public key is used and this means a large storage capacity in the first scheme. A new scheme has then be proposed in [DPP07] by Delerablee et al.: it is dynamic, achieves constant-size ciphertexts, has an encryption key linear in the number of users, and has the property that a constant-size decryption key, together with public information concerning only revoked users, allows the decryption of a ciphertext. A variation of this last scheme gives rise to a public-key broadcast scheme for stateful receivers, with constant-size ciphertexts, where one user can be permanently revoked in each ciphertext.

1.2 Efficiency in Group Management

Even these broadcast encryption schemes for stateless receivers are not really meant to perform well in realistic situations where large groups of users must be excluded or added to the set of privileged users: their performance is evaluated by considering the number of users and the number of permanent or temporary excluded users, which are very large in these situations. The only scheme with

an attractive analysis are the first schemes suggested in [BGW05,DPP07], where the ciphertexts have a constant size. A receiver in these schemes needs however the exact knowledge of the set of privileged users, which means the transmission of an information at least linear in the number of revoked users, or the number of selected users, or the number of users with a different status from a predefined situation, when a large modification of the set of privileged users is made.

Is group management really not possible in previous schemes ? In fact, the binary tree structure presented in [NNL01] and its following improvements allows efficient selection or revocation of large sets of users: users are placed in the leaves of the tree, and the SD scheme can for example select or revoke the subtree starting from an internal node in a constant-size ciphertext. So, one can hope to benefit from this structure by positioning the users in a clever manner in the tree. But then, it is necessary to choose which criterions are important and which ones are not. For instance a criterion which is used at the root of the tree will be associated to an efficient revocation mechanism while a criterion near the base of the tree will entail very long ciphertexts. Tree systems seem at first sight well adapted but they can only perform well in the case where there is only a small set of criterions to classify the users.

Group management can be performed by the combination of [DF02] with a hierarchical identity-based encryption scheme with wildcards, like presented in [ACD+06,BDNS06]. The resulting scheme would allow the selection of users with given characteristics, i.e. build ciphertexts addressed to intersections of groups. The revocation of all users with a fixed characteristic from the SD technique is unclear, and its use is not efficient since the size of the ciphertexts is not constant in the hierarchical identity based encryption (see [BBG05]).

2 Preliminaries

We give a formal definition of groups of users, and an associated definition of broadcast encryption schemes with group management, deduced from the definition given in [BGW05].

2.1 Bilinear Maps

In the following definitions, we consider the symmetric setting of bilinear maps, like in [Jou00,BF01]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order p. The group laws in $\mathbb{G}_1$ and $\mathbb{G}_2$ are noted additively. Let g_1 be a generator of $\mathbb{G}_1$. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a non-degenerate pairing:

- for all $a, b \in (\mathbb{Z}/p\mathbb{Z})$, $e(a\, g_1, b\, g_1) = ab.e(g_1, g_1)$,
- let $g_2 = e(g_1, g_1)$, g_2 is a generator of $\mathbb{G}_2$.

We make the assumption that the group laws in $\mathbb{G}_1$ and $\mathbb{G}_2$, and the bilinear map e can be computed efficiently.

2.2 Groups of Users

In our applications, we have a large number of users, and a large number of groups (in practice, we need for each user a group containing this single user). Each user belongs to only a few groups of users. We choose a description which takes advantage of this fact.

We represent the set of all users, called $\mathcal{U}$, by the list of integers $\{1, \ldots, n\}$. A group of users is a subset $\mathcal{G}$ of $\mathcal{U}$. From the inverse point of view, for a fixed number l of groups of users, we can associate to a user $u \in \mathcal{U}$ the set of groups he belongs to: $\mathcal{B}(u) = \{i \in \{1, \ldots, l\} \,/\, u \in \mathcal{G}_i\} \subset \{1, \ldots, l\}$.

2.3 Broadcast Encryption with Group Management

The model does not take into account the fact that the scheme could be dynamic, i.e. that new users could join without changing the decryption key given to other users, like in [DPP07], even if our scheme seems to allow such behavior. We concentrate on groups of users, and the following definitions are just a slight adaptation of [BGW05]. A public-key broadcast encryption scheme with group management with security parameter λ is a tuple of three randomized algorithms:

- ***Setup***$(\lambda, n, (\mathcal{B}(u))_{1 \leq u \leq n})$: takes as input the security parameter λ, the number of users n, and groups of users. It outputs an encryption key EK, and n decryption keys $(\mathrm{dk}_u)_{1 \leq u \leq n}$.
- ***Encrypt***$(\mathrm{EK}, \mathcal{B}^N, \mathcal{B}^R)$: takes as input the encryption key EK and two sets of groups $\mathcal{B}^N$ and $\mathcal{B}^R$. It outputs a header hdr and a message encryption key K in a finite set $\mathcal{K}$ of keys.
- ***Decrypt***$(\mathrm{dk}_u, \mathrm{hdr})$: takes as input a decryption key given to a user u and a header hdr. If the header hdr comes from an encryption using $(\mathcal{B}^N, \mathcal{B}^R)$ such that $\mathcal{B}^N \subset \mathcal{B}(u)$ and $\mathcal{B}(u) \cap \mathcal{B}^R = \emptyset$, then it outputs a message encryption key $K \in \mathcal{K}$.

In the encryption process a message M is encrypted with a key K and the resulting ciphertext C is sent together with the header hdr. Users in all groups mentioned in $\mathcal{B}^N$ (needed groups) and outside all groups mentioned in $\mathcal{B}^R$ (revoked groups) can obtain K from the header hdr and their decryption key dk_u. Using the key K a user recovers M from C.

Note that in these definitions, the decryption key and the header are the only elements that a user needs in order to compute the key K. The encryption key and the knowledge of the set of privileged users is not necessary for decryption. In fact, in our scheme, the knowledge of the set of privileged users is implicitly included in the header, using the characteristics corresponding to the required groups, and to the revoked groups. The header corresponds then exactly to the cost of the broadcast scheme in terms of transmission.

In this description, we do not allow an encryption for an arbitrary set of privileged users, which is the usual definition of a broadcast encryption scheme. Any set of privileged users can however be represented by an union of sets used in this "basic encryption" for well-chosen groups of users (in fact, it is enough

that each user belongs to a group containing only this single user). Different basic encryptions are then used to encrypt a common key, instead of a message. The full message can then be sent, using this common key.

2.4 Security Model

We consider semantic security of broadcast encryption schemes with group management. The adversary is assumed static, as in previous models: the only difference with standard definitions is that the groups of users are given to the adversary before the beginning of the game between the challenger and the adversary $\mathcal{A}$:

- The challenger and the adversary are given l fixed groups of users, defined by $(\mathcal{B}(u))_{1\leq u\leq n}$.
- The adversary $\mathcal{A}$ outputs two sets of groups $\mathcal{B}^N$ and $\mathcal{B}^R$ corresponding to an encryption it intends to attack.
- The challenger runs *Setup*$(\lambda, n, (\mathcal{B}(u))_{1\leq u\leq n})$ and gives to $\mathcal{A}$ the encryption key EK, and the decryption keys dk_u corresponding to users that the adversary may control, i.e. such that $\mathcal{B}^N \cap \mathcal{B}(u) \neq \mathcal{B}^N$ or $\mathcal{B}^R \cap \mathcal{B}(u) \neq \emptyset$.
- The challenger runs *Encrypt*$(\mathrm{EK}, \mathcal{B}^N, \mathcal{B}^R)$, and obtains a header hdr and a key $K \in \mathcal{K}$. Next, the challenger picks a random bit b, sets $K_b = K$, picks a random $K_{1-b} \in \mathcal{K}$, and gives (hdr, K_0, K_1) to the adversary $\mathcal{A}$.
- The adversary $\mathcal{A}$ outputs a bit b'.

The adversary $\mathcal{A}$ wins the previous game when $b' = b$. The advantage of $\mathcal{A}$ in this game, with parameters $(\lambda, n, (\mathcal{B}(u))_{1\leq u\leq n})$, is:

$$\mathrm{Adv}^{\mathrm{ind}}(\lambda, n, (\mathcal{B}(u)), \mathcal{A}) = |2\Pr[b' = b] - 1|.$$

A broadcast encryption scheme with group management is (n, l)-semantically secure against full static collusions if for all randomized polynomial-time (in λ) adversary $\mathcal{A}$ and for all groups of users $(\mathcal{B}(u))_{1\leq u\leq n}$ with at most l groups, $\mathrm{Adv}^{\mathrm{ind}}(\lambda, n, (\mathcal{B}(u)), \mathcal{A})$ is a negligible function in λ when n and l are at most polynomials in λ.

From such semantically secure scheme, we can build schemes secure in a stronger model: the use of generic transformations like the ones presented in [FO99a,FO99b,OP01] has a negligible cost, and we obtain chosen-ciphertext security in the random oracle model. This explains why our security model is limited to chosen-plaintexts attacks.

2.5 Well-Chosen Groups of Users

Groups of users can be defined from a data structure, in order to place in a same group users with a given property. These groups are however not fully adequate, since they may not allow the revocation of a single user, for example.

In the definition of a broadcast encryption scheme with group management, we proposed to add groups containing single users. With such groups, any choice

of the set of privileged users is possible even if the ciphertexts could be quite long.

Adding more groups of users may ensure that ciphertexts will have a reasonable length, even in the worse case: independently of groups defined from a data structure, we place users in the leaves of a binary tree. Each subtree corresponds to a new group of users, containing users placed in the leaves in this subtree: at most $2n$ new groups of users are added.

With these new groups, basic encryption with privileged users corresponding to the members of one group, excluding members of another group give at least the same sets as in the SD-method presented in [NNL01]. The efficiency of the broadcast encryption scheme with group management is then at least as good as in the SD-method, for any set of privileged users.

3 Construction

In this section, we describe a public-key broadcast encryption scheme with group management.

3.1 The Setup algorithm

From the security parameter λ, the first step consists in constructing a tuple $(\mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, p)$, where:

- $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic groups of prime order p,
- e is a non-degenerate pairing from $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$,
- g_1 is a generator of $\mathbb{G}_1$ and $g_2 = e(g_1, g_1)$,
- the length of p is equal to λ.

Four elements (α, β, γ and δ) are randomly chosen in $(\mathbb{Z}/p\mathbb{Z})^*$.

Each group of users $\mathcal{G}_i$, mentioned in $(\mathcal{B}(u))_{1 \leq u \leq n}$ is then associated to a characteristic μ_i randomly chosen in $(\mathbb{Z}/p\mathbb{Z})$, such that all these characteristics are pairwise different and different from α. Another characteristic μ_0 is randomly chosen with the same constraints, corresponding to a virtual group containing no users.

The encryption key is:

$$\mathrm{EK} = \left\{ g_1, \frac{1}{\gamma}\, g_1 \right\} \cup \left\{ \left(\mu_i, \frac{1}{\alpha - \mu_i}\, g_1, \frac{\delta}{\alpha - \mu_i}\, g_1, \frac{\beta}{\alpha - \mu_i}\, g_2 \right) / \, i \in \{0, \ldots, l\} \right\}.$$

For each user $u \in \mathcal{U}$, s_u is randomly chosen in $(\mathbb{Z}/p\mathbb{Z})^*$. Let $\Omega(u)$ be the set of characteristics corresponding to the groups he belongs to: $\Omega(u) = \{\mu_i \in (\mathbb{Z}/p\mathbb{Z}) \,/\, i \in \mathcal{B}(u)\}$. Let $l(u)$ be the size of $\Omega(u)$, i.e. the number of groups containing u. Let $\Pi(u) = \prod_{\mu \in \Omega(u)} (\alpha - \mu)$. The decryption key of u is:

$$\mathrm{dk}_u = \left(\Omega(u), s_u\, g_1, \left(\frac{\beta}{\delta} + \frac{s_u}{\delta\, \Pi(u)} \right) g_1, \frac{\gamma\, s_u}{\Pi(u)}\, g_1, \ldots, \frac{\gamma\, s_u\, \alpha^{l(u)-1}}{\Pi(u)}\, g_1 \right).$$

3.2 Encryption

If $\mathcal{B}^N \cap \mathcal{B}^R \neq \emptyset$, the encryption aborts, since a user can not be simultaneously inside and outside a given group of users.

Otherwise, let $\Omega^N = \{\mu_i \,/\, i \in \mathcal{B}^N\}$ and $\Omega^R = \{\mu_i \,/\, i \in \mathcal{B}^R\}$. Let $l^N = |\mathcal{B}^N|$ be the number of required groups and $l^R = |\mathcal{B}^R|$ be the number of revoked groups[1]. Let $\Pi^N = \prod_{\mu\in\Omega^N}(\alpha - \mu)$, let $\Pi^R = \prod_{\mu\in\Omega^R}(\alpha - \mu)$ and let $\Pi^{NR} = \Pi^N\Pi^R$. Let r be a randomly chosen element of $(\mathbb{Z}/p\mathbb{Z})^*$. The result of the encryption is:

$$\text{hdr} = \left(\Omega^N, \Omega^R, \frac{r}{\gamma}\, g_1, \frac{\delta\, r}{\Pi^R}\, g_1, \frac{r}{\Pi^{NR}}\, g_1, \ldots, \frac{r\,\alpha^{l^R-1}}{\Pi^{NR}}\, g_1\right) \quad \text{and} \quad K = \frac{\beta\, r}{\Pi^R}\, g_2.$$

All these elements can be computed by a sender, using only EK. This is a simple consequence of the fact that for ν_1, ν_2 in $\mathbb{Z}/p\mathbb{Z}$, when μ_t and μ_s are two different characteristics in $\mathbb{Z}/p\mathbb{Z}$, we have

$$\nu_1 \frac{1}{\alpha - \mu_t} + \nu_2 \frac{1}{\alpha - \mu_s} = \frac{(\nu_1 + \nu_2)\alpha - \nu_1\mu_s - \nu_2\mu_t}{(\alpha - \mu_s)(\alpha - \mu_t)}.$$

From this equality, for any $\Omega \subset \{\mu_1, \ldots, \mu_l\}$, for any $c \in \{1, \ldots, |\Omega| - 1\}$, with the knowledge of $\left\{\frac{\alpha^j}{\prod_{\mu\in\omega}(\alpha-\mu)}\, g_1 \,/\, 0 \leq j < c,\, \omega \subset \Omega,\, |\omega| = c\right\}$, we can compute $\left\{\frac{\alpha^j}{\prod_{\mu\in\omega}(\alpha-\mu)}\, g_1 \,/\, 0 \leq j < c+1,\, \omega \subset \Omega,\, |\omega| = c+1\right\}$. We can then recursively compute $\left\{\frac{\alpha^j}{\prod_{\mu\in\Omega}(\alpha-\mu)}\, g_1 \,/\, 0 \leq j < |\Omega|\right\}$ for any $\Omega \subset \{\mu_1, \ldots, \mu_l\}$.

3.3 Decryption

We consider here the decryption of a header hdr with a decryption key dk_u:

$$\begin{cases} \text{dk}_u = (\Omega(u), \text{dk}_1, \text{dk}_2, \text{dk}_{3,0}, \ldots, \text{dk}_{3,l(u)-1})\,, \\ \text{hdr} = (\Omega^N, \Omega^R, \text{hdr}_1, \text{hdr}_2, \text{hdr}_{3,0}, \ldots, \text{hdr}_{3,l^R-1})\,. \end{cases}$$

The receiver u is valid for this header if Ω^N is contained in $\Omega(u)$ and if $\Omega^R \cap \Omega(u)$ is empty. To decrypt the header, the valid receiver u uses first the extended Euclidian algorithm over the polynomials $\prod_{\mu\in(\Omega^N\cup\Omega^R)}(X - \mu)$ and $\prod_{\mu\in\Omega(u)}(X - \mu)$. It obtains two unitary polynomials, $V(X) = \sum_{0\leq j<l(u)} v_j X^j$ and $W(X) = \sum_{0\leq j<l^R} w_j X^j$, in $(\mathbb{Z}/p\mathbb{Z})[X]$, such that:

$$V(X) \prod_{\mu\in(\Omega^N\cup\Omega^R)} (X - \mu) + W(X) \prod_{\mu\in\Omega(u)} (X - \mu) = \prod_{\mu\in\Omega^N} (X - \mu).$$

From these polynomials, the receiver computes the key:

$$K(\text{dk}_u, \text{hdr}) = e(\text{dk}_2, \text{hdr}_2) - \left(\sum_{j=0}^{l(u)-1} v_j\, \text{dk}_{3,j}\,,\, \text{hdr}_1\right) - e\left(\text{dk}_1\,,\, \sum_{j=0}^{l^R-1} w_j\, \text{hdr}_{3,j}\right).$$

[1] A slight modification occurs when $\mathcal{B}^R$ is empty: in such case, the encryption considers that the virtual group containing no users is revoked and then $\Omega^R = \{\mu_0\}$, $l^R = 1$.

3.4 Proof of correctness

If dk_u is the valid decryption key given to a user u, if hdr is a header built using the encryption and if u is a valid user for hdr, then the decryption gives:

$$K(\mathrm{dk}_u, \mathrm{hdr}) = \left(\frac{\beta\, r}{\Pi^R} + \frac{r\, s_u}{\Pi^R\, \Pi(u)}\right) g_2 \; - \; \frac{r\, s_u\, V(\alpha)}{\Pi(u)}\, g_2 \; - \; \frac{r\, s_u\, W(\alpha)}{\Pi^{NR}}\, g_2.$$

By definition of V and W, we have: $V(\alpha)\, \Pi^{NR} + W(\alpha)\Pi(u) = \Pi^N$. The computed key is then exactly the key associated to the header in the encryption:

$$K(\mathrm{dk}_u, \mathrm{hdr}) = \left(\frac{\beta\, r}{\Pi^R} + \frac{r\, s_u}{\Pi^R\, \Pi(u)}\right) g_2 \; - \; \frac{r\, s_u}{\Pi^R\, \Pi(u)}\, g_2 = \frac{\beta\, r}{\Pi^R}\, g_2.$$

4 Security of the Protocol

The previous scheme can be proved in different ways. The usual strategy is first to define some security assumption and to prove this assumption in the generic model of groups with pairing. The reduction of the security of the scheme to this assumption concludes the proof.

Following this strategy, we need a new security assumption which is a extension of the decisional version of the General Diffie-Hellman Exponent (GDHE) problem, precisely studied in the full version of [BBG05]: we need rational functions instead of polynomials in the definition of the problem.

We prefer here a direct proof in the generic model of groups with pairing. Such direct proof provides the same guarantee as in the previous method and it is not clear how an intermediate security assumption would provide more security than the generic model. Some criticisms of the model of generic groups are moreover irrelevant, as explained in [KM07].

In this section, we define the decisional problem upon which our broadcast encryption mechanism is built. We assess its security in the framework of the generic model of groups with pairing.

4.1 A Decisional Problem

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order p and e be a non-degenerate pairing from $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$. Let g_1 be a generator of $\mathbb{G}_1$ and $g_2 = e(g_1, g_1)$. Let α, β, γ, δ, r be elements of $(\mathbb{Z}/p\mathbb{Z})^*$. For all $i \in \{0, \ldots, l\}$, let μ_i be an element of $(\mathbb{Z}/p\mathbb{Z})$ different from α and from μ_j where $j < i$.

The encryption key is:

$$\mathrm{EK} = \left\{ g_1, \frac{1}{\gamma}\, g_1 \right\} \cup \left\{ \left(\mu_i, \frac{1}{\alpha - \mu_i}\, g_1, \frac{\delta}{\alpha - \mu_i}\, g_1, \frac{\beta}{\alpha - \mu_i}\, g_2 \right) / \, i \in \{0, \ldots, l\} \right\}.$$

For each user $u \in \mathcal{U}$, $\Omega(u)$ is a subset of $\{\mu_1, \ldots, \mu_l\}$. Let $l(u) = |\Omega(u)|$ and let $\Pi(u) = \prod_{\mu \in \Omega(u)} (\alpha - \mu)$. The decryption key dk_u of the user u is:

$$\mathrm{dk}_u = \left(\Omega(u), s_u\, g_1, \left(\frac{\beta}{\delta} + \frac{s_u}{\delta\, \Pi(u)} \right) g_1, \frac{\gamma\, s_u}{\Pi(u)}\, g_1, \ldots, \frac{\gamma\, s_u\, \alpha^{l(u)-1}}{\Pi(u)}\, g_1 \right).$$

Let Ω^N be a subset of $\{\mu_1, \ldots, \mu_l\}$, let Ω^R be a non-empty subset of $\{\mu_0, \ldots, \mu_l\}$ such that $\Omega^N \cap \Omega^R = \emptyset$, let $l^R = |\Omega^R|$. Let $\mathcal{R}$ be the set of revoked users for these sets:

$$\mathcal{R} = \left\{ u \in \mathcal{U} \,/\, \Omega(u) \cap \Omega^N \neq \Omega^N \text{ or } \Omega(u) \cap \Omega^R \neq \emptyset \right\}.$$

Let $\Pi^N = \prod_{\mu \in \Omega^N} (\alpha - \mu)$, let $\Pi^R = \prod_{\mu \in \Omega^R} (\alpha - \mu)$ and let $\Pi^{NR} = \Pi^N \Pi^R$. The header hdr and the key K are defined by:

$$\text{hdr} = \left(\Omega^N, \Omega^R, \frac{r}{\gamma}\, g_1, \frac{\delta\, r}{\Pi^R}\, g_1, \frac{r}{\Pi^{NR}}\, g_1, \ldots, \frac{r\, \alpha^{l^R - 1}}{\Pi^{NR}}\, g_1 \right) \quad \text{and} \quad K = \frac{\beta\, r}{\Pi^R}\, g_2.$$

Let b be a bit, let K_{1-b} be an element of $(\mathbb{Z}/p\mathbb{Z})^*$, let $K_b = K$. The decisional problem is the following: guess b from the knowledge of EK, hdr, K_0, K_1 and all the dk_u, where $u \in \mathcal{R}$.

4.2 Interpretation in the Generic Model

In this section, we use the notations of the full version of [BBG05] in order to assess the difficulty of the preceding decisional problem in the generic model of groups with pairing model. This extends the classical model of generic groups presented in [Nec93,Sho97].

The first part of the proof consists in showing that there exists no formula giving the key from the header, the encryption key, and the decryption keys corresponding to revoked users. The second part details why an adversary can not distinguish the key from a random element in the generic model of groups with pairing.

No Formula Denote by $\mathcal{F}$ the field of rational functions in the variables $A, B, C, D, R, \{S_u, u \in \mathcal{R}\}$.

Let P be the tuple of elements in $\mathcal{F}$, corresponding to the exponents of elements in $\mathbb{G}_1$ given to an adversary in the problem. The tuple P contains 1, $1/C$, R/C, $D\,R/\Pi^R(A)$ and the following rational functions:

- $\dfrac{1}{A - \mu_i}$ and $\dfrac{D}{A - \mu_i}$ for all $i \in \{0, \ldots, l\}$,
- S_u, $\dfrac{B}{D} + \dfrac{S_u}{D\,\Pi_u(A)}$, $\dfrac{C\,S_u}{\Pi_u(A)}$, $\ldots$, $\dfrac{C\,S_u\,A^{l(u)-1}}{\Pi_u(A)}$ for all $u \in \mathcal{R}$,
- $\dfrac{R}{\Pi^{NR}(A)}$, $\ldots$, $\dfrac{R\,A^{l^R-1}}{\Pi^{NR}(A)}$,

where

$$\Pi^N(X) = \prod_{\mu \in \Omega^N} (X - \mu), \quad \Pi^R(X) = \prod_{\mu \in \Omega^R} (X - \mu),$$

$$\Pi_u(X) = \prod_{\mu \in \Omega(u)} (X - \mu), \quad \Pi^{NR} = \Pi^N(X)\Pi^R(X).$$

Let Q be the tuple of elements in $\mathcal{F}$, corresponding to the exponents of elements in $\mathbb{G}_2$ given to an adversary in the problem. The tuple Q contains 1 and the rational functions $B/(A - \mu_i)$ where $i \in \{0, \ldots, l\}$.

Lemma 1. *Let W_1 be the sub-$\mathbb{Z}$-module of $\mathcal{F}$ generated by elements of P. Let W_2 be the sub-$\mathbb{Z}$-module of $\mathcal{F}$ generated by elements of Q, and all products of elements of W_1. We have that W_2 contains the element $\left(B\,R/\Pi^R(A)\right)$ with probability less than $\frac{1}{p}$, the probability being taken over all possible choices of the characteristics μ_i in $(\mathbb{Z}/p\mathbb{Z})$.*

Proof. This lemma is proved in appendix A.1.

Indistinguishability in the Generic Model In the generic model of groups with pairing, we consider two injective maps ξ_1 and ξ_2 from $(\mathbb{Z}/p\mathbb{Z})$ into $\{0,1\}^*$, also known as encoding functions. The additive law on $(\mathbb{Z}/p\mathbb{Z})$ induces a group law over $\xi_1(\mathbb{Z}/p\mathbb{Z})$ and $\xi_2(\mathbb{Z}/p\mathbb{Z})$, respectively denoted by $\mathbb{G}_1$ and $\mathbb{G}_2$. Oracles corresponding to the group law and the inverse law of each group are provided. A new law, corresponding to the pairing, is also given as an oracle: for all $y, z \in \mathbb{G}_1, e(y,z) = \xi_2({\xi_1}^{-1}(y) \times {\xi_1}^{-1}(z)) \in \mathbb{G}_2$. An algorithm computing in this model has only access to these 5 oracles, and has no information about ξ_1 and ξ_2: its computations are based on queries to these oracles.

In our case, this model means that a challenger will use randomly chosen encoding functions from $(\mathbb{Z}/p\mathbb{Z})$ into a set of p binary strings. The challenger randomly chooses α, β, γ, δ, r, $(\mu_i)_{0\leq i\leq l}$, $(s_u)_{u\in\mathcal{U}}$ following their constraints, and gives to the adversary:

- all values $\xi_1\left(f(\alpha,\beta,\gamma,\delta,r,s_1,\ldots,s_n)\right)$, where f is in the tuple P,
- all values $\xi_2\left(f(\alpha,\beta,\gamma,\delta,r,s_1,\ldots,s_n)\right)$, where f is in the tuple Q,
- $\xi_1(z_0)$ and $\xi_1(z_1)$, where $z_b = \beta\, r/\Pi^R$ and z_{1-b} is chosen randomly in $(\mathbb{Z}/p\mathbb{Z})^*$.

The adversary makes queries to oracles and outputs its guess b'.

Some results have already been proved over this kind of problems, but only with polynomials instead of rational functions. Considering a change of basis, the rational functions can be "transformed" into polynomials. We define the two following elements:

$$g_1' = \frac{1}{\gamma\,\prod_{i=0}^{l}(\alpha-\mu_i)}\,g_1, \quad g_2' = \frac{1}{\gamma^2\,\prod_{i=0}^{l}(\alpha-\mu_i)^2}\,g_2.$$

The change of basis from g_1 to g_1' in $\mathbb{G}_1$ means that all rational functions in P are multiplied by $C\prod_{i=0}^{l}(X-\mu_i)$, and become polynomials of degree at most $l+4$. In the same way, the change of basis from g_2 to g_2' in $\mathbb{G}_2$ means that all rational functions in Q are multiplied by $C^2\prod_{i=0}^{l}(X-\mu_i)^2$, and become polynomials of degree at most $2l+2$. The rational function corresponding to the key becomes a polynomial of degree at most $2l+3$.

We now use the following theorem, proposed and proved in the full version of [BBG05] (theorem A.2):

Theorem 1. *Let $P, Q \in (\mathbb{Z}/p\mathbb{Z})[A,B,C,D,R,S_1,\ldots,S_n]^\ell$ be two ℓ-tuples of $(n+6)$-variate polynomials over $(\mathbb{Z}/p\mathbb{Z})$ and let f be another $(n+6)$-variate polynomials over $(\mathbb{Z}/p\mathbb{Z})$. Let d_P be the maximum of degrees of polynomials in P, d_Q*

be the maximum of degrees of polynomials in Q, and $d = \max(2d_P, d_Q, \deg(f))$. If f is not in the sub-$\mathbb{Z}$-module generated by elements of Q and products of elements of P, then for any adversary $\mathcal{A}$ that makes at most q queries to oracles computing the group operations and the bilinear pairing we have:

$$\left| Pr[b' = b] - \frac{1}{2} \right| \leq \frac{d\,(q + 2\ell + 2)^2}{2p}.$$

The tuple P contains at most $2nl+2n+3l+6$ elements, the tuple Q contains at most $l+2$ elements. We define then $\ell = 2nl+2n+3l+6$, and $d = 2l+8$. As a result, with probability $1-1/p$ (from the first part of the proof), the advantage of an adversary that makes q queries is bounded by:

$$\frac{(2l+8)(q+4nl+4n+6l+14)^2}{p}.$$

Putting all probabilities together, we obtain the following advantage for an adversary that makes q queries in the generic model of groups with pairing:

$$\frac{(2l+9)(q+4nl+4n+6l+14)^2}{p}.$$

As q, n and l are at most polynomial in λ, when $|p| = \lambda$, this advantage is negligible. This ends the security proof.

5 Conclusion

In this paper, we built a new public-key broadcast encryption scheme. This scheme is specifically interesting when a data structure categorizes the users in groups depending on their properties. In this case, our broadcast scheme can easily implement this data structure in order to efficiently send message to sets of users defined by the groups they belong to. We proved the security of this scheme in the generic model of groups with pairing.

References

[ACD+06] Michel Abdalla, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, and Nigel P. Smart. Identity-based encryption gone wild. In *Proc. of ICALP'06*, pages ?–?, 2006.

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In *Proc. of Advances in Cryptology – Eurocrypt'05*, pages 440–456, 2005.

[BDNS06] James Birkett, Alexander W. Dent, Gregory Neven, and Jacob Schuldt. Efficient chosen-ciphertext secure identity-based encryption with wildcards. Technical Report 377, Cryptology ePrint Archive, 2006.

[BF01] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. In *Proc. of Advances in Cryptology – Crypto'01*, pages 213–229, 2001.

[BGW05] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proc. of Advances in Cryptology – Crypto'05*, pages 258–275, 2005.

[CGI+99] Ran Canetti, Juan Garay, Gene Itkis, Daniele Micciancio, Moni Naor, and Benny Pinkas. Multicast security: A taxonomy and efficient constructions. volume 2, pages 708–716, 1999.

[CMN99] Ran Canetti, Tal Malkin, and Kobbi Nissim. Efficient communication-storage tradeoffs for multicast encryption. In *Proc. of Advances in Cryptology – Eurocrypt'99*, pages 459–474, 1999.

[DF02] Yevgeniy Dodis and Nelly Fazio. Public key broadcast encryption for stateless receivers. In *Proc. of Security and Privacy in Digital Right Management (DRM'02)*, pages 61–80, 2002.

[DPP07] Cecile Delerablee, Pascal Paillier, and David Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. To appear in *Proc. of Pairing'07*.

[FN93] Amos Fiat and Moni Naor. Broadcast encryption. In *Proc. of Advances in Cryptology – Crypto'93*, pages 480–491, 1993.

[FO99a] Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In *Proc. of Advances in Cryptology – PKC'99*, pages 53–68, 1999.

[FO99b] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proc. of Advances in Cryptology – Crypto'99*, pages 537–554, 1999.

[GST04] Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia. Efficient tree-based revocation in groups of low-state devices. In *Proc. of Advances in Cryptology – Crypto'04*, pages 511–527, 2004.

[GSW00] Juan A. Garay, Jessica Staddon, and Avishai Wool. Long-lived broadcast encryption. In *Proc. of Advances in Cryptology – Crypto'00*, pages 333–352, 2000.

[HS02] Dani Halevy and Adi Shamir. The lsd broadcast encryption scheme. In *Proc. of Advances in Cryptology – Crypto'02*, pages 47–60, 2002.

[Jou00] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *Lectures Notes in Computer Science*, 1838:385–393, 2000.

[KM07] Neal Koblitz and Alfred Menezes. Another look at generic groups. *Advances in Mathematics of Communications*, 1:13–28, 2007.

[KRS99] Ravi Kumar, Sridhar Rajagopalan, and Amit Sahai. Coding constructions for blacklisting problems without computational assumptions. In *Proc. of Advances in Cryptology – Crypto'99*, pages 609–623, 1999.

[Nec93] V. I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematicheskie Zametki*, 55(2):91–101, 1993.

[NNL01] Dalit Naor, Moni Naor, and Lotspiech. Revocation and tracing schemes for stateless receivers. In *Proc. of Advances in Cryptology – Crypto'01*, pages 41–62, 2001.

[OP01] Tatsuaki Okamoto and David Pointcheval. React: Rapid enhanced-security asymmetric cryptosystem transform. In *Proc. of Cryptographers' Track, RSA Conference – CT-RSA'01*, pages 159–175, 2001.

[PST01] Adrian Perrig, Dawn Song, and J. D. Tygar. Elk, a new protocol for efficient large-group key distribution. In *Proc. of IEEE Symposium on Security and Privacy*, pages 247–262, 2001.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4):701–717, 1980.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *Proc. of Advances in Cryptology – Eurocrypt'97*, pages 256–266, 1997.

[WGL98] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam. Secure group communications using key graphs. In *Proc. of ACM-SIGCOMM'98*, pages 68–79, 1998.

[WHA99] Debby. M. Wallner, Eric J. Harder, and Ryan C. Agee. Key management for multicast: Issues and architectures, rfc 2627, 1999.

A Proof of Lemma 1

A.1 Lemma 1

Lemma 1. *Let W_1 be the sub-$\mathbb{Z}$-module of $\mathcal{F}$ generated by elements of P. Let W_2 be the sub-$\mathbb{Z}$-module of $\mathcal{F}$ generated by elements of Q, and all products*

of elements of W_1. We have that W_2 contains the element $\left(B\,R/\Pi^R(A)\right)$ with probability less than $\frac{1}{p}$, the probability being taken over all possible choices of the characteristics μ_i in $(\mathbb{Z}/p\mathbb{Z})$.

Proof. Let $\mathcal{L}$ be the set of elements of $\mathcal{F}$ which in Q or products of pairs of elements of P. By definition $\mathcal{L}$ generates W_2.

Suppose that $B\,R/\Pi^R(A) \in W_2$. Then it is a linear combination with coefficients in $\mathbb{Z}$ of elements of $\mathcal{L}$. Considering the elements of W_2 as polynomials with respect to the variable R, we see that $B\,R/\Pi^R(A)$ can only be obtained as a linear combination of linear terms in R. In the same way, we see that it can only be obtained as a linear combination of constant terms in the variables C and D.

These terms of $\mathcal{L}$ which are linear in R and constant in C and D are listed in the followings sets:

$$T_1 = \left\{ \frac{R\,A^j}{(A-\mu_i)\,\Pi^{NR}(A)} / j \in \{0,\ldots,l^R-1\}, i \in \{0,\ldots,l\} \right\},$$

$$T_2 = \left\{ \frac{S_u\,R\,A^j}{\Pi_u(A)} / u \in \mathcal{R}, j \in \{0,\ldots,l(u)-1\} \right\},$$

$$T_3 = \left\{ \frac{S_u\,R\,A^j}{\Pi^{NR}(A)} / u \in \mathcal{R}, j \in \{0,\ldots,l^R-1\} \right\},$$

$$T_4 = \left\{ \frac{B\,R}{\Pi^R(A)} + \frac{S_u\,R}{\Pi_u(A)\,\Pi^R(A)} / u \in \mathcal{R} \right\},$$

$$T_5 = \left\{ \frac{R\,A^j}{\Pi^{NR}(A)} / j \in \{0,\ldots,l^R-1\} \right\}.$$

The elements of T_4 are linearly independent because of the presence of the independent variables S_u. As B only appears in these terms, at least one of these must be involved in the linear combination of elements of $\mathcal{L}$ which is equal to $B\,R/\Pi^R(A)$.

In order to cancel the terms of the form $\frac{S_u R}{\Pi_u(A)\Pi^R(A)}$ appearing in the elements of T_4 by a linear combination of elements of T_1, T_2, T_3 and T_4, by considering only linear terms in this specific S_u, one can see that it is necessary to build a relation of the form

$$\frac{1}{\Pi_u(A)\,\Pi^R(A)} = \sum_{j=0}^{l(u)-1} \frac{\lambda_j A^j}{\Pi_u(A)} + \sum_{j=0}^{l^R-1} \frac{\lambda'_j A^j}{\Pi^{NR}(A)}. \tag{1}$$

We have two cases:

- if $\Omega(u) \cap \Omega^R \neq \emptyset$ then left term of this equation is a rational function with a pole of order 2 while all elements of the right hand linear combination have only simple poles in A. Such a relation can not exist.

– if Ω^N is not included in $\Omega(u)$, we can rewrite equation (1) as

$$\Pi^N(A) = \Big(\sum_{j=0}^{l(u)-1} \lambda_j A^j \Big)\, \Pi^{NR}(A) + \Big(\sum_{j=0}^{l^R-1} \lambda'_j A^j \Big)\, \Pi_u(A).$$

As $\Pi^N(A)$ divides $\Pi^{NR}(A)$, it also divides $(\sum_{j=0}^{l^R-1} \lambda'_j A^j)\, \Pi_u(A)$. But, by hypothesis, $\Pi^N(A)$ does not divide $\Pi_u(A)$. It means that we have:

$$\Big(\sum_{j=0}^{l^R-1} \lambda'_j A^j \Big)\, \Pi_u(A) = \Pi^N(A)\; Q(A)\; \pi_u(A),$$

where $Q(A)$ is a strict divisor of $\sum_{j=0}^{l^R-1} \lambda'_j A^j$. So equation (1) is equivalent to equation

$$1 = \Big(\sum_{j=0}^{l(u)-1} \lambda_j A^j \Big)\, \Pi^R(A) + Q(A)\, \pi_u(A),$$

with $\deg(Q) < \deg(\Pi^R) - 1$. According to lemma 2 given in next section of the appendix such a relation does happen with probability less than $\frac{1}{p}$.

These two cases complete the proof of the lemma.

A.2 Lemma 2

Consider A and B two elements of the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[X]$ with $\deg A = a$ and $\deg B = b$. We suppose that A and B are relatively prime. By Bezout's theorem, there exists U, V in $(\mathbb{Z}/p\mathbb{Z})[X]$ unitary such that

$$AU + BV = 1, \tag{2}$$

with $\deg U < b$ and $\deg V < a$. This last condition determines uniquely U and V satisfying (2). We are interested here in computing the probability that $\deg U < b - 1$. We have the

Lemma 2. *The probability taken over all polynomials $A, B \in (\mathbb{Z}/p\mathbb{Z})[X]$ such that $\deg A = a$ and $\deg B = b$ and A, B relatively prime, that there exists $U, V \in (\mathbb{Z}/p\mathbb{Z})[X]$ with $AU + BV = 1$ and $\deg U < b - 1$ is bounded by*

$$\frac{a+b}{p^{a+b}}.$$

Proof. Suppose that there exists $U, V \in (\mathbb{Z}/p\mathbb{Z})[X]$ such that $AU + BV = 1$ and $\deg U < \deg B - 1$ and $\deg V < \deg A - 1$. This means that the family

$$\Big(1, \{AX^k \,/\, k \in \{0, \ldots, b-2\}\}, \{BX^k \,/\, k \in \{0, \ldots a-2\}\}\Big)$$

is not free. We can rephrase it by saying that

$$\det \begin{bmatrix} 1 & \alpha_0 & 0 & \cdots & 0 & \beta_0 & 0 & \cdots & 0 \\ 0 & \alpha_1 & \alpha_0 & \ddots & \vdots & \vdots & \beta_0 & \ddots & \vdots \\ \vdots & \vdots & \alpha_1 & \ddots & 0 & \vdots & \vdots & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \alpha_0 & \vdots & \vdots & & \beta_0 \\ \vdots & \alpha_a & \vdots & & \alpha_1 & \beta_b & \vdots & & \vdots \\ \vdots & 0 & \alpha_a & & \vdots & 0 & \beta_b & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \alpha_a & 0 & \cdots & 0 & \beta_b \end{bmatrix} = 0.$$

Developing this determinant, we obtain an element of degree $a+b$ in a polynomial ring of $a+b$ variables over $\mathbb{F}_p$. By [Sch80] lemma 1, the probability that such a polynomial is 0 is $\frac{a+b}{p^{a+b}}$. Actually, we have to take this probability over all the polynomials A and B such that A and B are relatively primes but this is a generic condition given by the cancellation of the polynomial provided by the Sylvester determinant which does not change asymptotically the above mentioned probability.