

An efficient attribute based broadcast scheme

David Lubicz, Thomas Sirvent
david.lubicz@univ-rennes1.fr
thomas.sirvent@m4x.org

CELAR - IRMAR

Plan of the talk

1 Context

- Broadcast encryption
- Efficiency of standard schemes
- Attributes

2 The scheme

- Introduction
- Principles
- Performance

Plan of the talk

1 Context

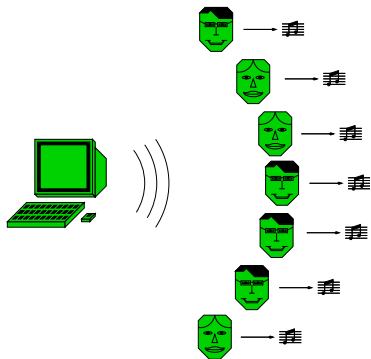
- Broadcast encryption
- Efficiency of standard schemes
- Attributes

2 The scheme

- Introduction
- Principles
- Performance

Broadcast

A **emitter** intends to send securely and efficiently the **same message** to a large number of receivers:



Wide range of scenarios and performances requirements

Security requirements:

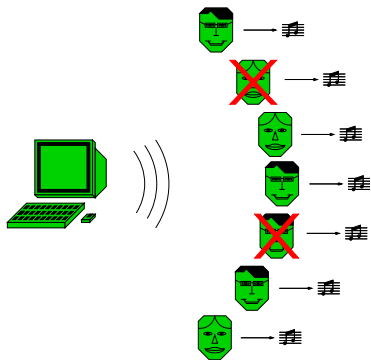
- users can be added or removed securely and efficiently;
- dropped users can not read subsequent traffic even if they share their secret information.

Performance requirements:

- time for setup;
- storage space for each user;
- number of transmissions required for setup, rekey and maintenance.

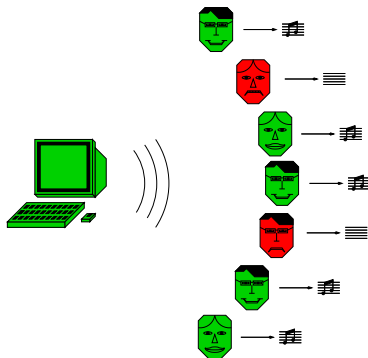
Revocation

In the case of a revocation, some users are **removed** from the set of receivers (for example when their decryption keys are compromised):



Permanent revocation

In the case of a **permanent revocation**, the decryption keys are updated. The revoked users are not able anymore to obtain the messages sent by the emitter:



Temporary revocation

When permanent revocations are used ([stateful schemes](#)),

- receivers must remain [online](#),
- receivers must [store](#) and use new decryption keys.

To avoid these limitations, it is possible to use [stateless schemes](#), where revocations are [temporary](#):

- in the encryption process, the emitter chooses the set of receivers,
- only members of this set may decrypt the message.

Description of a broadcast scheme

A broadcast scheme is given by :

- an **initialisation** function (for key generation),
- a **encryption** mechanism,
- a **decryption** mechanism.

→ Permanent revocation: a mechanism to add or remove users need to be provided.

→ Temporary revocation: the encryption scheme have to take into account of a set of revoked users.

Security of a broadcast scheme: Is an adversary controlling revoked users able to distinguish two ciphertexts obtains from two different chosen plaintext?

Description of a broadcast scheme

A broadcast scheme is given by :

- an **initialisation** function (for key generation),
- a **encryption** mechanism,
- a **decryption** mechanism.

→ Permanent revocation: a mechanism to add or remove users need to be provided.

→ Temporary revocation: the encryption scheme have to take into account of a set of revoked users.

Security of a broadcast scheme: Is an adversary controlling revoked users able to distinguish two ciphertexts obtains from two different chosen plaintext?

Description of a broadcast scheme

A broadcast scheme is given by :

- an **initialisation** function (for key generation),
- a **encryption** mechanism,
- a **decryption** mechanism.

→ Permanent revocation: a mechanism to add or remove users need to be provided.

→ Temporary revocation: the encryption scheme have to take into account of a set of revoked users.

Security of a broadcast scheme: Is an adversary controlling revoked users able to distinguish two ciphertexts obtains from two different chosen plaintext?

Description of a broadcast scheme

A broadcast scheme is given by :

- an **initialisation** function (for key generation),
- a **encryption** mechanism,
- a **decryption** mechanism.

→ Permanent revocation: a mechanism to add or remove users need to be provided.

→ Temporary revocation: the encryption scheme have to take into account of a set of revoked users.

Security of a broadcast scheme: Is an adversary controlling revoked users able to distinguish two ciphertexts obtains from two different chosen plaintext?

Permanent revocation broadcast scheme

With permanent revocation, we have to maintain a key shared by all the privileged users. A **particular structure** is used **on the set of receivers** so that adding or the revocation of a user is efficient.

In term of bandwidth,

- sending a message is efficient,
- adding or revoking a user is difficult.

A broadcast encryption scheme with permanent revocation is well adapted for a small **small** set of receivers, **stable** enough in the time.

Permanent revocation broadcast scheme

With permanent revocation, we have to maintain a key shared by all the privileged users. A **particular structure** is used **on the set of receivers** so that adding or the revocation of a user is efficient.

In term of bandwidth,

- sending a message is efficient,
- adding or revoking a user is difficult.

A broadcast encryption scheme with permanent revocation is well adapted for a small **small** set of receivers, **stable** enough in the time.

Permanent revocation broadcast scheme

With permanent revocation, we have to maintain a key shared by all the privileged users. A **particular structure** is used **on the set of receivers** so that adding or the revocation of a user is efficient.

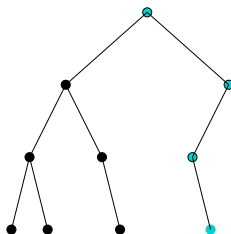
In term of bandwidth,

- sending a message is efficient,
- adding or revoking a user is difficult.

A broadcast encryption scheme with permanent revocation is well adapted for a small **small** set of receivers, **stable** enough in the time.

Permanent revocation broadcast scheme

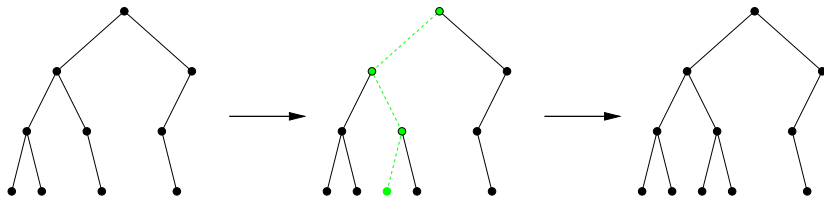
All the users are placed at leaves of a tree.



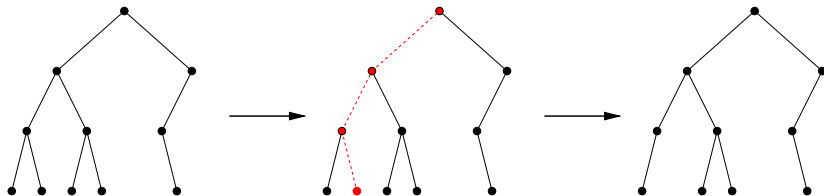
Each node correspond to a specific key: a user knows the keys corresponding to the nodes between its leaf and the root.

Permanent revocation broadcast scheme

Adding a user:



Revocation of a user:



Temporary revocation broadcast scheme

With a temporary revocation, a **particular structure** is used for **the set of all users** so as to allow an efficient encryption.

In term of bandwidth,

- sending a message is expensive,
- a variation of the set of privileged users is free.

Temporary broadcast encryption is well adapted for a **small** set of receivers or a **small** set of revoked users, with **frequent modification** of the set of privileged users.

Temporary revocation broadcast scheme

With a temporary revocation, a **particular structure** is used for **the set of all users** so as to allow an efficient encryption.

In term of bandwidth,

- sending a message is expensive,
- a variation of the set of privileged users is free.

Temporary broadcast encryption is well adapted for a **small** set of receivers or a **small** set of revoked users, with **frequent modification** of the set of privileged users.

Temporary revocation broadcast scheme

With a temporary revocation, a **particular structure** is used for **the set of all users** so as to allow an efficient encryption.

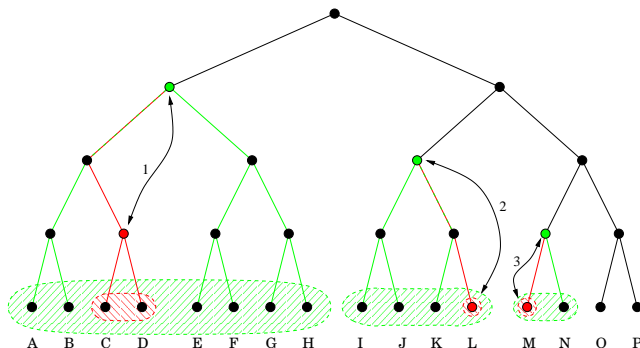
In term of bandwidth,

- sending a message is expensive,
- a variation of the set of privileged users is free.

Temporary broadcast encryption is well adapted for a **small** set of receivers or a **small** set of revoked users, with **frequent modification** of the set of privileged users.

Temporary revocation broadcast scheme

All the users are placed on the leaves of a tree.



In this structure a key corresponds to a couple of nodes of the tree: it is known from the users descending from the first node which are not descendant of the second node.

Users and attributes

In concrete applications of broadcast encryption schemes, users have particular characteristics (called attributes) which could be used:

Id	Name	Subscription		Town
1	Alice	Cinema	Jan 2008	Paris
2	Bob	Sports	Aug 2009	Rennes
3	Charlie	Series	May 2008	Limoge
4	Dan	Information/Cinma	May 2008	Bordeaux
5	Eve	Sports	Jan 2008	Lyon

One can also consider different content providers using the same receivers. The users have their attributes dedicated to their provider.

Attribute based broadcast scheme

We would like to **select or revoke simultaneously** users corresponding to certain attributes:

Film broadcasted in June 2008 $\left\{ \begin{array}{l} \text{Select the users with the cinema package} \\ \text{Exclude the expired subscriptions} \end{array} \right.$

The goal is to be able to **send efficiently** messages to a set of receivers **defined by their attributes**. The choice a any set of receivers have to be possible.

Plan of the talk

1 Context

- Broadcast encryption
- Efficiency of standard schemes
- Attributes

2 The scheme

- Introduction
- Principles
- Performance

The scheme is based upon the use of perfect pairings, that is a map $e : G_1 \times G_1 \rightarrow G_2$ such that :

- (G_1, g_1) and (G_2, g_2) are cyclic groups of prime order p ,
- $e(g_1, g_1) = g_2$,
- e is bilinear.

Full scheme - key generation

- We randomly choose a secret 4-uple $(\alpha, \beta, \gamma, \delta) \in ((\mathbb{Z}/p\mathbb{Z})^*)^4$,
- Each user u is associated with a secret $s_u \in (\mathbb{Z}/p\mathbb{Z})$,
- Each attribute is associated with a public $\mu_i \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\alpha\}$.

$$\text{EK} = \left(g_1, \beta \gamma \delta g_1, (\mu_i, \alpha^i g_1, \alpha^i \gamma g_1, \alpha^i \delta g_1)_{0 \leq i \leq l} \right).$$

$$\text{dk}_u = \left(\Omega(u), (\beta + s_u) \delta g_1, \gamma s_u \Pi(u) g_1, (\alpha^i \gamma \delta s_u g_1)_{0 \leq i < l(u)} \right),$$

$$\text{where } \begin{cases} \Omega(u) = \{\mu_i \in (\mathbb{Z}/p\mathbb{Z}) / \mu_i \text{ attribute of } u\}, \\ l(u) = |\Omega(u)| \text{ is the number of attributes of } u, \\ \Pi(u) = \prod_{\mu \in \Omega(u)} (\alpha - \mu). \end{cases}$$

Full scheme - encryption

- Let Ω^N be the set of needed attributes.
- Let $\Omega^R \neq \emptyset$ be the set of revoked attributes.
- A user u is valid for these sets if: $\Omega^N \subset \Omega(u)$ and $\Omega^R \cap \Omega(u) = \emptyset$.

The encryption for these sets (Ω^N, Ω^R) gives :

$$\text{hdr} = \left(\Omega^N, \Omega^R, z \prod^{NR} g_1, \gamma z \prod^N g_1, (\alpha^i \delta z g_1)_{0 \leq i < I^R} \right),$$
$$K = \beta \gamma \delta z \prod^N g_2.$$

where

$$\begin{cases} z \text{ is randomly chosen in } (\mathbb{Z}/p\mathbb{Z})^*, \\ I^R = |\Omega^R|, \\ \prod^N = \prod_{\mu \in \Omega^N} (\alpha - \mu), \\ \prod^{NR} = \prod^N \prod_{\mu \in \Omega^R} (\alpha - \mu). \end{cases}$$

Full scheme - decryption

The decryption is based on a decryption key dk_u and a header hdr :

$$\begin{cases} dk_u = (\Omega(u), dk_1, dk_2, dk_{3,0}, \dots, dk_{3,l(u)-1}), \\ hdr = (\Omega^N, \Omega^R, hdr_1, hdr_2, hdr_{3,0}, \dots, hdr_{3,l^R-1}). \end{cases}$$

If u is a valid receiver, extended Euclide's algorithm gives two polynomials

$V(X) = \sum_{i=0}^{l(u)-1} v_i X^i$ and $W(X) = \sum_{i=0}^{l^R-1} w_i X^i$ such that:

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

The key is obtained by:

$$e(dk_1, hdr_2) - e\left(\sum_{i=0}^{l(u)-1} v_i dk_{3,i}, hdr_1\right) - e\left(dk_2, \sum_{i=0}^{l^R-1} w_i hdr_{3,i}\right).$$

$$V(\alpha)\Pi^{NR} + W(\alpha)\Pi(u) = \Pi^N.$$

$$V(\alpha) = \sum_{i=0}^{l(u)-1} v_i \alpha^i$$

$$W(\alpha) = \sum_{i=0}^{l^R-1} w_i \alpha^i$$

$$dk_1 = (\beta + s_u) \delta g_1$$

$$hdr_1 = z \Pi^{NR} g_1$$

$$dk_2 = \gamma s_u \Pi(u) g_1$$

$$hdr_2 = \gamma z \Pi^N g_1$$

$$dk_{3,i} = \alpha^i \gamma \delta s_u g_1$$

$$hdr_{3,i} = \alpha^i \delta z g_1$$

$$e(dk_1, hdr_2) = e\left(\sum_{i=0}^{l(u)-1} v_i dk_{3,i}, hdr_1\right) = e\left(dk_2, \sum_{i=0}^{l^R-1} w_i hdr_{3,i}\right)$$

$$\hookrightarrow K = \beta \gamma \delta z \Pi^N g_2.$$

Construction principles

- User u is associated to $\Pi(u)$, which is the evaluation in α of $\prod_{\mu \in \Omega(u)} (X - \mu)$,
- the header hdr is associated to Π^{NR} , which is the evaluation in α of $\prod_{\mu \in \Omega^N \cup \Omega^R} (X - \mu)$,
- the key K is associated to Π^N , which is the evaluation of $\prod_{\mu \in \Omega^N} (X - \mu)$ in α .

α is **secret**, the used operation must be valid **on the polynomial**, and not only on the values in α (following the *generic group model*).

The operation are constrained

- group operation correspond to **linear combination**,
- pairings correspond to a **unique product** of polynomials.

Construction principles

- User u is associated to $\Pi(u)$, which is the evaluation in α of $\prod_{\mu \in \Omega(u)} (X - \mu)$,
- the header hdr is associated to Π^{NR} , which is the evaluation in α of $\prod_{\mu \in \Omega^N \cup \Omega^R} (X - \mu)$,
- the key K is associated to Π^N , which is the evaluation of $\prod_{\mu \in \Omega^N} (X - \mu)$ in α .

α is **secret**, the used operation must be valid **on the polynomial**, and not only on the values in α (following the *generic group model*).

The operation are constrained

- group operation correspond to **linear combination**,
- pairings correspond to a **unique product** of polynomials.

Construction principles

- User u is associated to $\Pi(u)$, which is the evaluation in α of $\prod_{\mu \in \Omega(u)} (X - \mu)$,
- the header hdr is associated to Π^{NR} , which is the evaluation in α of $\prod_{\mu \in \Omega^N \cup \Omega^R} (X - \mu)$,
- the key K is associated to Π^N , which is the evaluation of $\prod_{\mu \in \Omega^N} (X - \mu)$ in α .

α is **secret**, the used operation must be valid **on the polynomial**, and not only on the values in α (following the *generic group model*).

The operation are constrained

- group operation correspond to **linear combination**,
- pairings correspond to a **unique product** of polynomials.

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

→ Si $\Omega(u) \cap \Omega^R \neq \emptyset$, such a relation is **formally impossible**.

→ If $\Omega^N \not\subset \Omega(u)$, such a relation is possible. But the degrees of $V(X)$ and $W(X)$ are bounded (by $l(u) - 1$ and $l^R - 1$), this relation becomes **statistically improbable**.

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

→ Si $\Omega(u) \cap \Omega^R \neq \emptyset$, such a relation is **formally impossible**.

→ If $\Omega^N \not\subset \Omega(u)$, such a relation is possible. But the degrees of $V(X)$ and $W(X)$ are bounded (by $I(u) - 1$ and $I^R - 1$), this relation becomes **statistically improbable**.

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

→ Si $\Omega(u) \cap \Omega^R \neq \emptyset$, such a relation is **formally impossible**.

→ If $\Omega^N \not\subset \Omega(u)$, such a relation is possible. But the degrees of $V(X)$ and $W(X)$ are bounded (by $l(u) - 1$ and $l^R - 1$), this relation becomes **statistically improbable**.

Construction principle

risk 1 : Recombination of the headers ?

↔ **Randomisation of the headers** of decryption (via z)

risk 2 : Recombination of the encryption keys ?

↔ **Randomisation of the encryption keys** (via s_u)

risk 3 : None expected arithmetic operations ?

↔ Strict limitation of the authorized products (via γ and δ)

Construction principle

risk 1 : Recombination of the headers ?

↪ Randomisation of the headers of decryption (via z)

risk 2 : Recombination of the encryption keys ?

↪ Randomisation of the encryption keys (via s_u)

risk 3 : None expected arithmetic operations ?

↪ Strict limitation of the authorized products (via γ and δ)

Construction principle

risk 1 : Recombination of the headers ?

↪ Randomisation of the headers of decryption (via z)

risk 2 : Recombination of the encryption keys ?

↪ Randomisation of the encryption keys (via s_u)

risk 3 : None expected arithmetic operations ?

↪ Strict limitation of the authorized products (via γ and δ)

Size of the ciphertexts: hdr linear in $|\Omega^N| + |\Omega^R|$.

Computations :

- Decryption: 3 pairings,
- Encryption: 1 pairing.

Size of the keys:

- EK linear in l ,
- dk_u linear in $l(u)$.

Other features:

- possible to add new users (or key renewal).

Complex logic formulas can not be implemented (“or”, threshold).

Performance

Size of the ciphertexts: hdr linear in $|\Omega^N| + |\Omega^R|$.

Computations :

- Decryption: 3 pairings,
- Encryption: 1 pairing.

Size of the keys:

- EK linear in l ,
- dk_u linear in $l(u)$.

Other features:

- possible to add new users (or key renewal).

Complex logic formulas can not be implemented (“or”, threshold).

Size of the ciphertexts: hdr linear in $|\Omega^N| + |\Omega^R|$.

Computations :

- Decryption: 3 pairings,
- Encryption: 1 pairing.

Size of the keys:

- EK linear in l ,
- dk_u linear in $l(u)$.

Other features:

- possible to add new users (or key renewal).

Complex logic formulas can not be implemented (“or”, threshold).

Size of the ciphertexts: hdr linear in $|\Omega^N| + |\Omega^R|$.

Computations :

- Decryption: 3 pairings,
- Encryption: 1 pairing.

Size of the keys:

- EK linear in l ,
- dk_u linear in $l(u)$.

Other features:

- possible to add new users (or key renewal).

Complex logic formulas can not be implemented (“or”, threshold).

Size of the ciphertexts: hdr linear in $|\Omega^N| + |\Omega^R|$.

Computations :

- Decryption: 3 pairings,
- Encryption: 1 pairing.

Size of the keys:

- EK linear in l ,
- dk_u linear in $l(u)$.

Other features:

- possible to add new users (or key renewal).

Complex logic formulas can not be implemented (“or”, threshold).

The End.