Revocable Broadcast Encryption

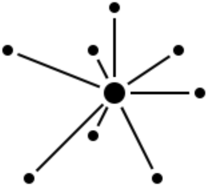
Sima Nerush

Reed College

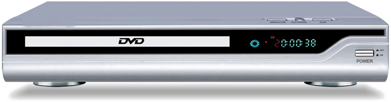
February 14, 2023

General Idea

We will explore the problem of **broadcasting** confidential information to a collection of n devices.



Examples

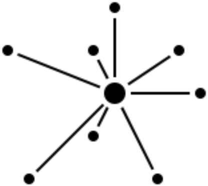


The Problem

Every device has its own key k_d to decipher information. Once the key is extracted, it can be used to decipher and distribute any information! Thus, we need to be able to **revoke** keys.

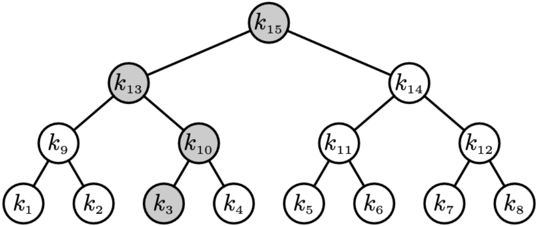
Revocable Broadcast Encryption

We will explore the problem of **broadcasting** confidential information to a collection of n devices while providing the ability to **revoke** an arbitrary subset of those devices. [3]



Constructions

We organize the set of *n* devices in a tree structure, associating each device with a different leaf in the tree. [3]



Setup

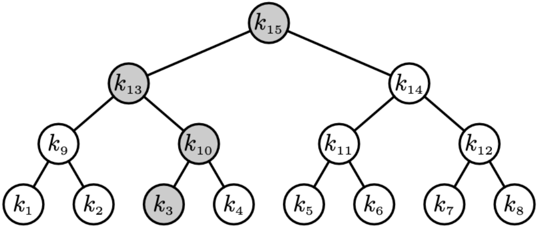
1. KeyGen, the *key generation algorithm*, is a probabilistic algorithm used by the Center to generate keys for the devices and the secret key. Takes into consideration the maximum number of revoked users.
2. Reg, the registration algorithm, is a probabilistic algorithm used by the Center to compute the secret initialization data to be delivered to a new user when they subscribe to the system. [2]

Setup

1. `Enc`, the encryption algorithm, is a probabilistic algorithm used to encapsulate a given session key k in such a way that the revoked users cannot recover it. `Enc` takes as input the public key PK, the session key k and a set $\mathcal{R}$ of revoked users and returns the ciphertext to be broadcast.
2. `Dec`, the decryption algorithm, is a deterministic algorithm that takes as input the secret data of a user u and the ciphertext broadcast by the center and returns the session key k that was sent if u was not in the set $\mathcal{R}$ when the ciphertext was constructed. [2]

Tree

Device 3 is initialized with keys {3, 10, 13, 15}. [1]



Before revocation

Encryption of some content (a movie) before any devices are revoked [1]:

$$c_m := \{k \xleftarrow{R} \mathcal{K},\ c_1 \leftarrow E(k_{root}, k),\ c \leftarrow E'(k,\ m),\ \text{output } (c1,\ c)\}$$

After Revocation

Suppose all keys of device 3 are revoked. Recall:

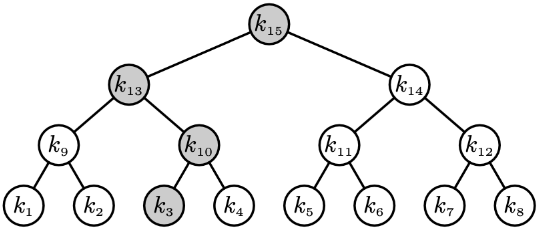


Figure: Device 3 has keys $\{3, 10, 13, 15\}$

After Revocation

Now, all content will be encrypted using the keys associated with the siblings of the $\log n$ nodes on the path from leaf 3 to the root.

$$c_{\mathrm{m}} := \left\{ \begin{array}{l} k \xleftarrow{\mathrm{R}} \mathcal{K} \\ c_1 \xleftarrow{\mathrm{R}} E(k_4,\ k), \quad c_2 \xleftarrow{\mathrm{R}} E(k_9,\ k), \quad c_3 \xleftarrow{\mathrm{R}} E(k_{14},\ k) \\ c \xleftarrow{\mathrm{R}} E'(k, m) \\ \text{output } (c_1, c_2, c_3, c) \end{array} \right\}$$

Now, device 3 cannot decrypt the header.

Cover problem

What's the minimum amount of keys that we need for the scheme to work for some number of revoked devices?

Theorem

Let T be a complete binary tree with n leaves, where n is a power of two. Let $S \subseteq \{1, \ldots, n\}$ be a set of leaves. We say that a set of nodes $W \subseteq \{1, \ldots, 2n-1\}$ covers the set S if every leaf in S is a descendant of some node in W, and leaves outside of S are **not**. *We use $cover(S)$ to denote the smallest set of nodes that covers S.[1]*

Example cover

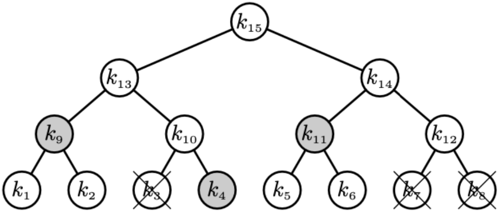


Figure: The three shaded nodes are the minimal cover for leaves $\{1, 2, 4, 5, 6\}$

Observation

The more devices are revoked, the larger the header of c_m becomes.

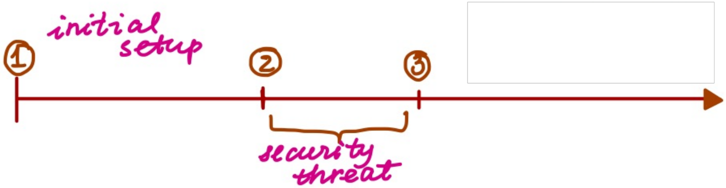
Theorem

Let T be a complete binary tree with n leaves, where n is a power of two. For every $1 \leq r \leq n$, and every set S of $n - r$ leaves, we have

$$|cover(S)| \leq r \cdot log_2(n/r)$$

This theorem can be proven by induction. [1]

Timeline



1. All information is encoded with a pair of keys.
2. Device is corrupted, adversary can use its key to decrypt all of the upcoming information.
3. The device is revoked, the keys are updated.

Security Issues

1. The problem of always growing keys, any of which can decrypt the master key.
2. How fast are keys updated poses a security threat, since adversary can decrypt any information until the corrupted device is revoked.

Further Work

Naor's Subset Difference representation [4]

References

Boneh, D., & Shoup, V. (2023). *A graduate course in applied cryptography*. Stanford University.

Dodis, Y., & Fazio, N. (2003). Public key broadcast encryption for stateless receivers. *DRM 2002.*

Goodrich, M. T., Sun, J. Z., & Tamassia, R. (2004). Efficient tree-based revocation in groups of low-state devices. *CRYPTO 2004.*

Naor, D., Naor, M., & Lotspiech, J. (2001). Revocation and tracing schemes for stateless receivers. *CRYPTO 2001.*