# The Cost of Maintaining Keys in Dynamic Groups with Applications to Multicast Encryption and Group Messaging

Michael Anastos, Benedikt Auerbach, Mirza Ahad Baig, **Miguel Cueto Noval**, Matthew Kwan, Guillermo Pascual-Perez, Krzysztof Pietrzak

ISTA, Austria

TCC 2024

Institute of Science and Technology Austria

# Maintaining Keys in Dynamic Groups

- Round 1: group of users agree on a key.

# Maintaining Keys in Dynamic Groups

- Round 1: group of users agree on a key.

# Maintaining Keys in Dynamic Groups

- Round 1: group of users agree on a key.
- Round 2: replace operation.

# Maintaining Keys in Dynamic Groups

- Round 1: group of users agree on a key.

- Round 2: replace operation.

# Maintaining Keys in Dynamic Groups

- Round 1: group of users agree on a key.

- Round 2: replace operation.

- Security: ‘only current group members know the group key’.

# Maintaining Keys in Dynamic Groups

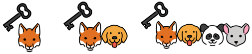
- Round 1: group of users agree on a key.

- Round 2: replace operation.

- Security: ‘only current group members know the group key’.
- Examples: Multicast Encryption (ME), Group Messaging.

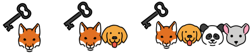
# Multicast Encryption

- In ME there is a central authority and each user maintains a private state:



# Multicast Encryption

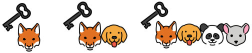
- In ME there is a central authority and each user maintains a private state:



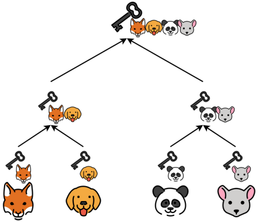
- Example: key trees as in Logical Key Hierarchies (LKH).

# Multicast Encryption

- In ME there is a central authority and each user maintains a private state:



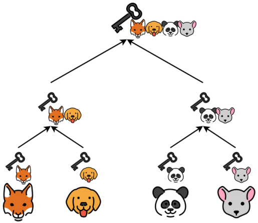
- Example: key trees as in Logical Key Hierarchies (LKH).

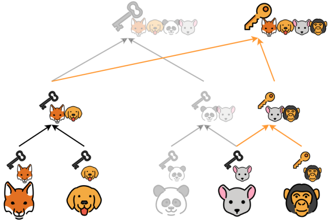


# Multicast Encryption

- In ME there is a central authority and each user maintains a private state:

- Example: key trees as in Logical Key Hierarchies (LKH).

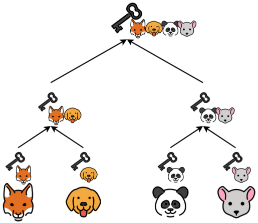


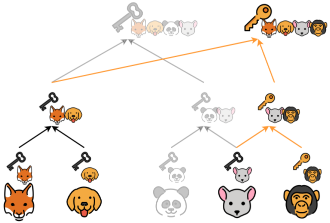


# Multicast Encryption

- In ME there is a central authority and each user maintains a private state:

- Example: key trees as in Logical Key Hierarchies (LKH).





- Cost per round of replacing $d$ users: $O(d(1 + \log_2(n/d)))$.

# Communication Cost in Multicast Encryption

**Question:** How many messages does the CA have to send per round in order to communicate a new key?

# Communication Cost in Multicast Encryption

**Question:** How many messages does the CA have to send per round in order to communicate a new key?
**Upper Bound:** Cost per round of replacing $d$ users is $O(d(1 + \log_2(n/d)))$ [NNL01, LYGL01, SM03].

# Communication Cost in Multicast Encryption

**Question:** How many messages does the CA have to send per round in order to communicate a new key?
**Upper Bound:** Cost per round of replacing $d$ users is $O(d(1 + \log_2(n/d)))$ [NNL01, LYGL01, SM03].

| **Lower Bounds for** $d = 1$ | | |
|---|---|---|
| [MP04] | $\Omega(\log_2 n)$ | Worst case |
| [AAB+21] | $\Omega(\log_2 n)$ | Average Case |

# Communication Cost in Multicast Encryption

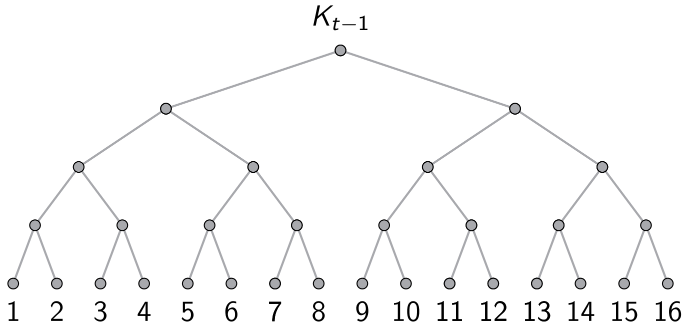
**Question:** How many messages does the CA have to send per round in order to communicate a new key?

**Upper Bound:** Cost per round of replacing $d$ users is $O(d(1 + \log_2(n/d)))$ [NNL01, LYGL01, SM03].

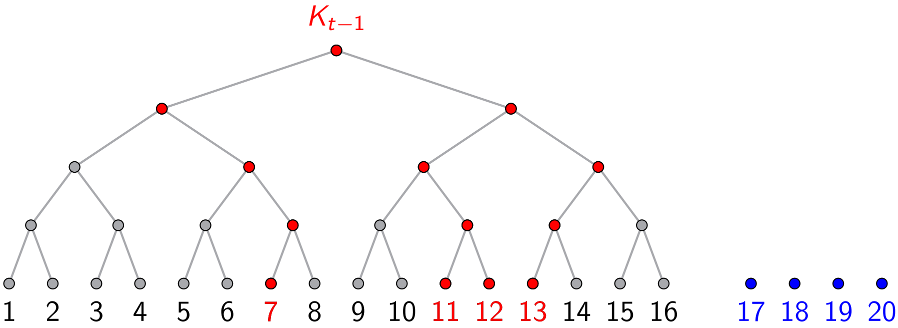
| **Lower Bounds for $d = 1$** | | |
|---|---|---|
| [MP04] | $\Omega(\log_2 n)$ | Worst case |
| [AAB+21] | $\Omega(\log_2 n)$ | Average Case |

**This Work:** A lower bound for arbitrary $d$ of $\Omega(d \cdot \log_2(n/d))$ (Average Case).

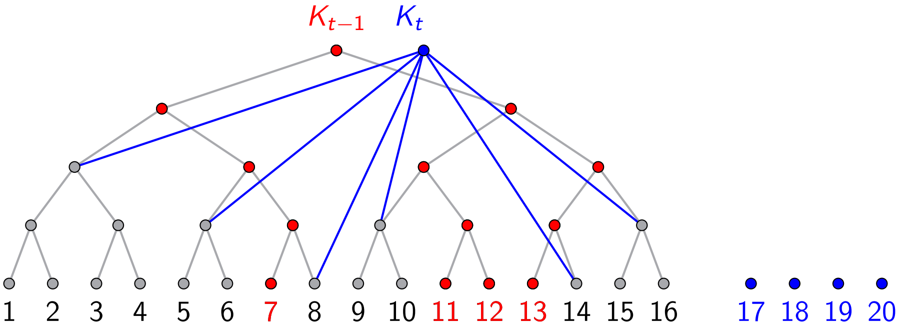
# Combinatorial Model: The Cost Function



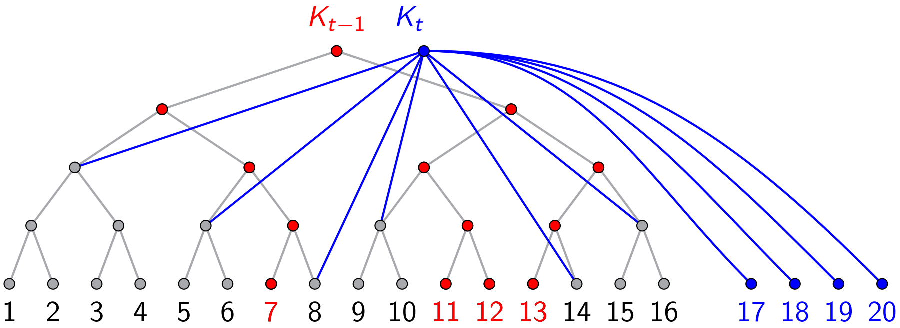
# Combinatorial Model: The Cost Function



# Combinatorial Model: The Cost Function



# Combinatorial Model: The Cost Function




$\mathrm{Cost}(t) =$ red nodes + blue edges

# Combinatorial Lower Bound

**Theorem**

*In every round $t$*

$$\mathbb{E}[\mathrm{Cost}(t)] \geq d \ln\left(\frac{n}{d}\right),$$

*where $d$ denotes the number of users replaced in round $t$ and the set of users removed is sampled uniformly at random in every round.*

$$\mathrm{Cost}(t) = \text{red nodes} + \text{blue edges}$$

Consequence of Bollobás Set Pairs Inequality.

# Lower Bound for Multicast Encryption

**Lemma**

*For any correct and secure ME scheme built using PRGs, PRFs, dual PRFs, symmetric encryption and secret sharing in the symbolic model:* $\sum_{t=0}^{t_{\max}} |\mathtt{M}_t| \geq 1/3 \cdot \sum_{t=0}^{t_{\max}} \mathrm{Cost}(t)$, *where* $|\mathtt{M}_t| =$ *number of messages sent by CA in round* $t$.

# Lower Bound for Multicast Encryption

**Lemma**

*For any correct and secure ME scheme built using PRGs, PRFs, dual PRFs, symmetric encryption and secret sharing in the symbolic model:* $\sum_{t=0}^{t_{\max}} |\mathtt{M}_t| \geq 1/3 \cdot \sum_{t=0}^{t_{\max}} \mathrm{Cost}(t)$, *where* $|\mathtt{M}_t|$ = *number of messages sent by CA in round* $t$.

**Theorem**

*Thus it must hold that*

$$\frac{1}{t_{\max}} \mathbb{E}\left[\sum_{t=0}^{t_{\max}} |\mathtt{M}_t|\right] \geq \frac{1}{3} d \ln\left(\frac{n}{d}\right),$$

*where* $d$ *denotes the amount of users replaced per round and the set of users replaced is sampled uniformly at random in every round.*

# Thanks!

https://ia.cr/2024/1097