

# Advantages of Layered Subset Difference over Subset Difference Broadcast Encryption

Bochum, December 1, 2004

# AGENDA

- 
- Overview
  - Subset difference broadcast encryption (BE)
  - Layered subset difference BE
-

# AGENDA

---

- **Overview**

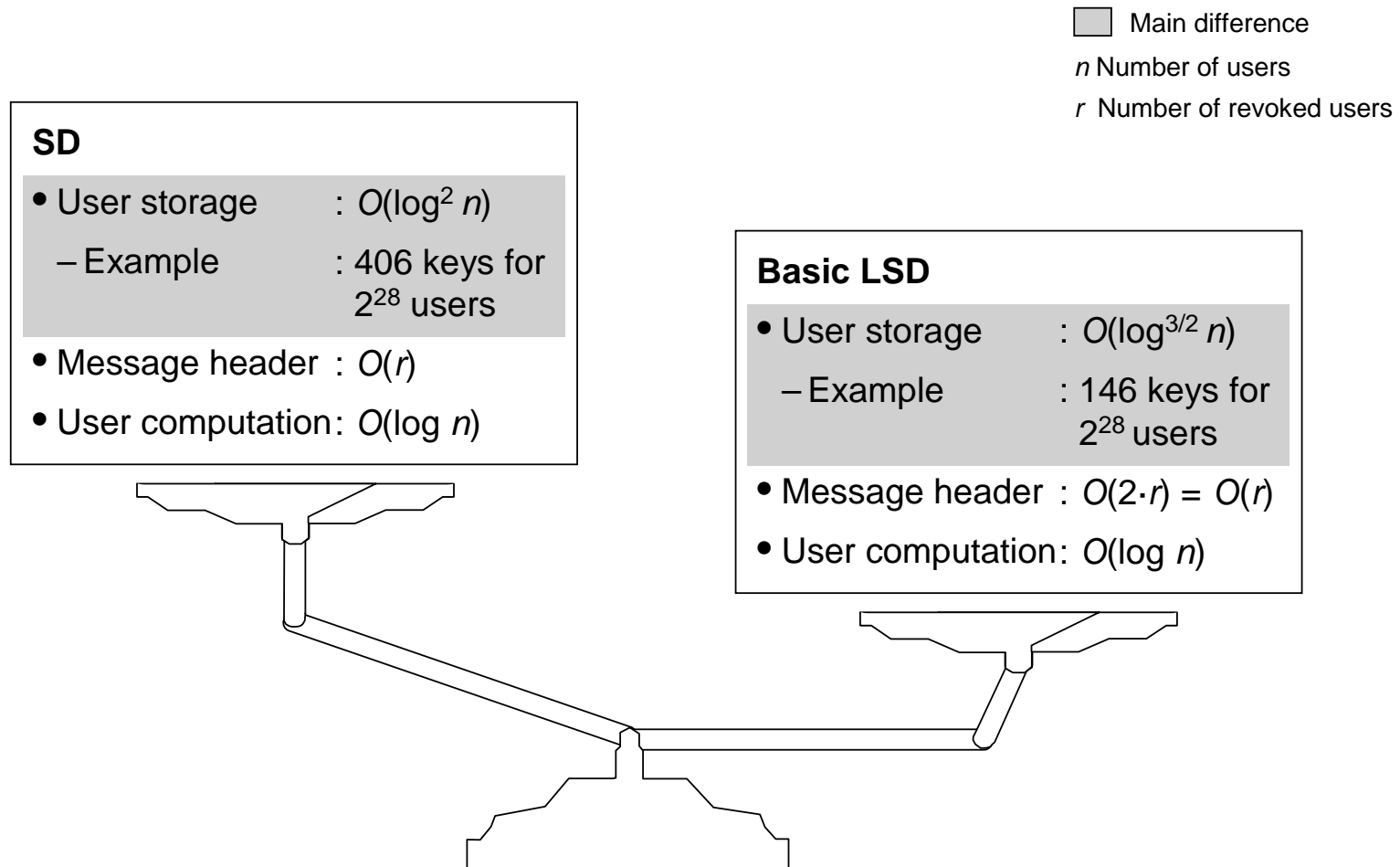
- Subset difference broadcast encryption (BE)

- Layered subset difference BE

---

Compared to SD\*, the basic LSD\*\* scheme significantly reduces the storage requirements of the users by slightly increasing the message header length

## COMPARISON OF SD\* AND BASIC LSD\*\* PERFORMANCE PARAMETERS



\* Subset difference

\*\* Layered subset difference, not lysergic acid diethylamide

Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60

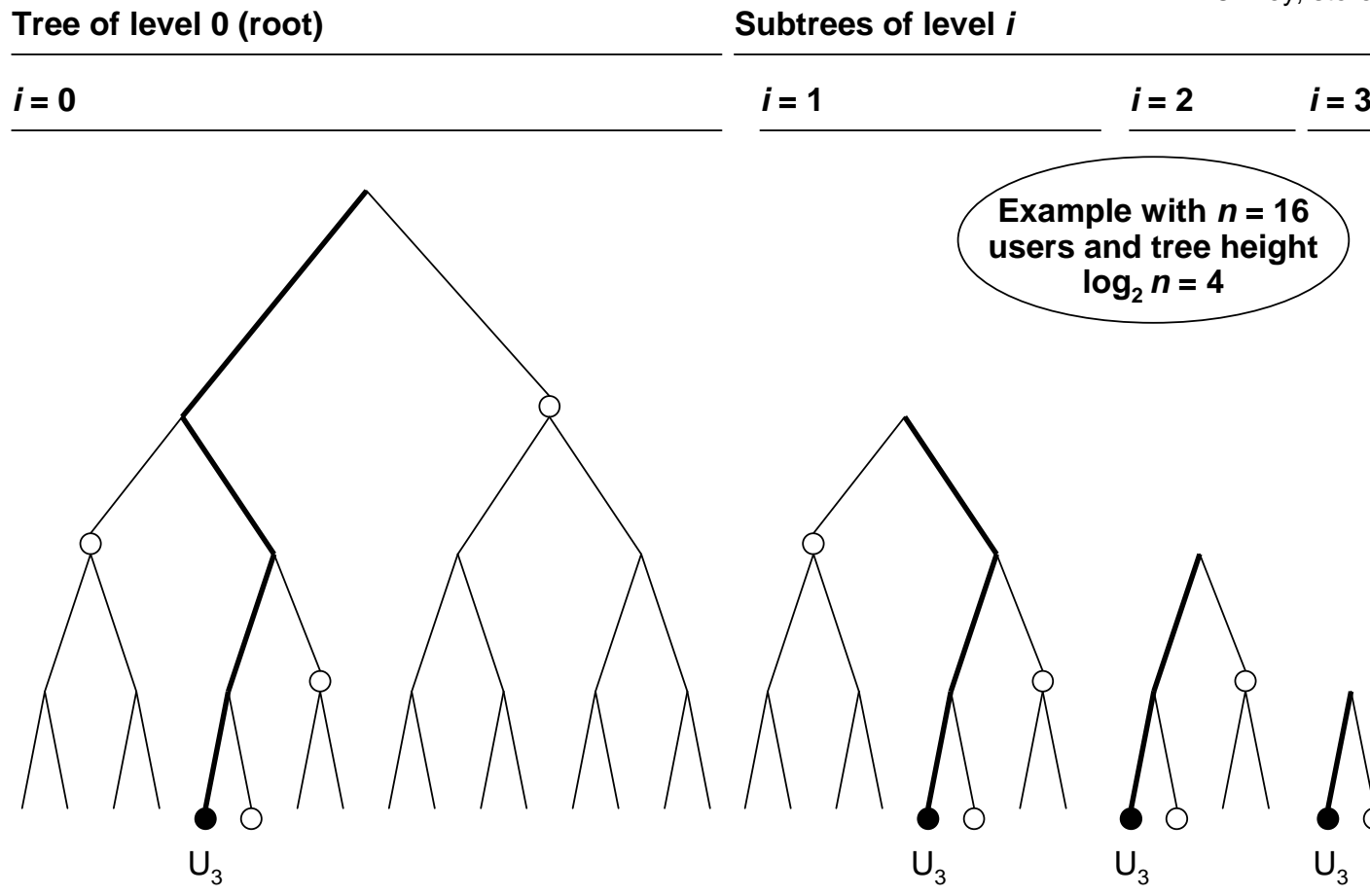
# AGENDA

- 
- Overview
  - **Subset difference broadcast encryption (BE)**
  - Layered subset difference BE
-

In the SD scheme, each receiver obtains the keys just off his key path within each subtree

### KEYS OF AN EXEMPLARY USER IN THE SD SCHEME

● Exemplary user  $U_3$   
○ Key, stored by  $U_3$



No. of stored keys

4

3

2

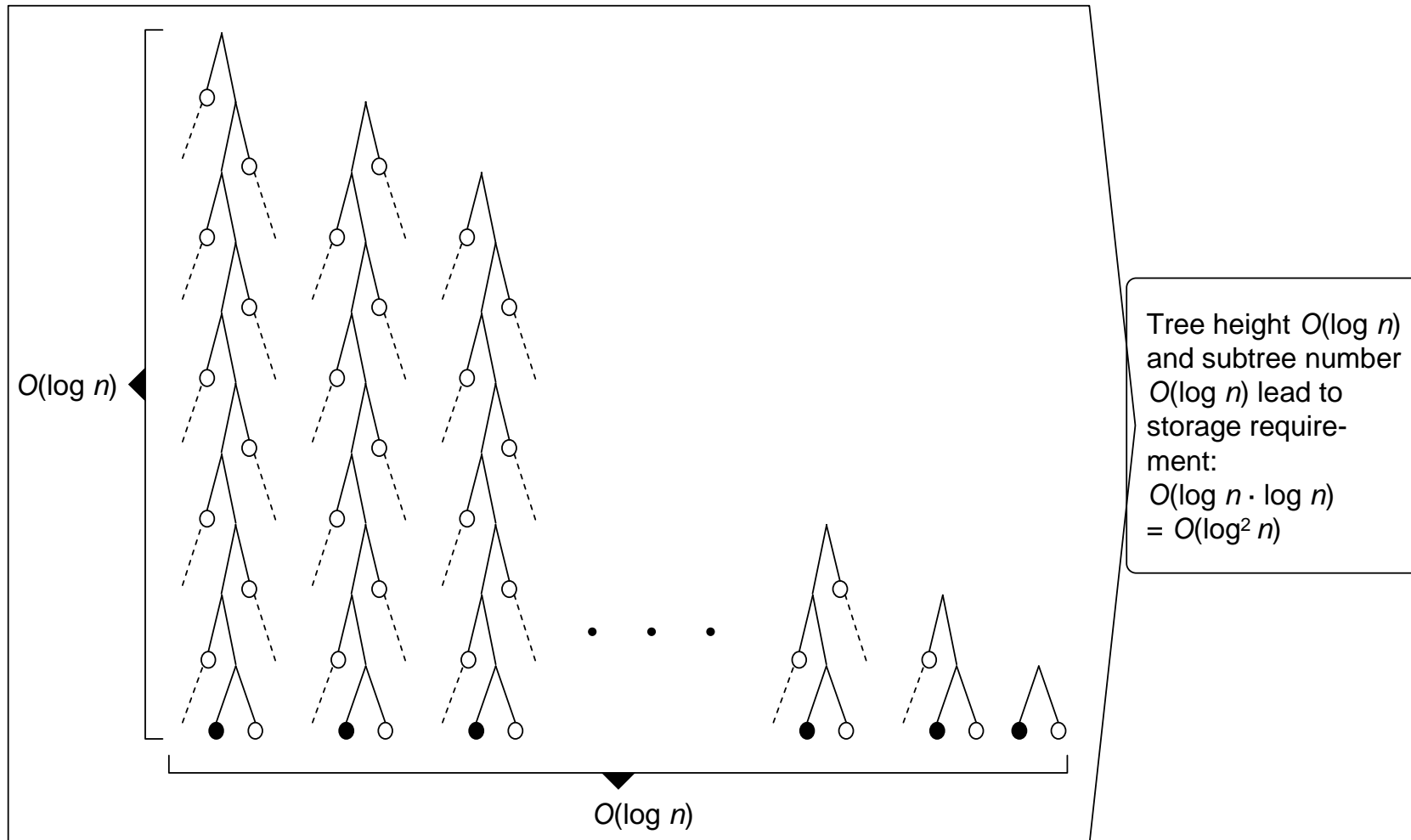
1

$\Sigma 10$

In a deep tree, each receiver of the SD scheme has to store many keys, especially for the uppermost subtrees

## STORAGE REQUIREMENT OF SD SCHEME

- Exemplary user
- Key stored by this user
- ⋯ Tree continuation

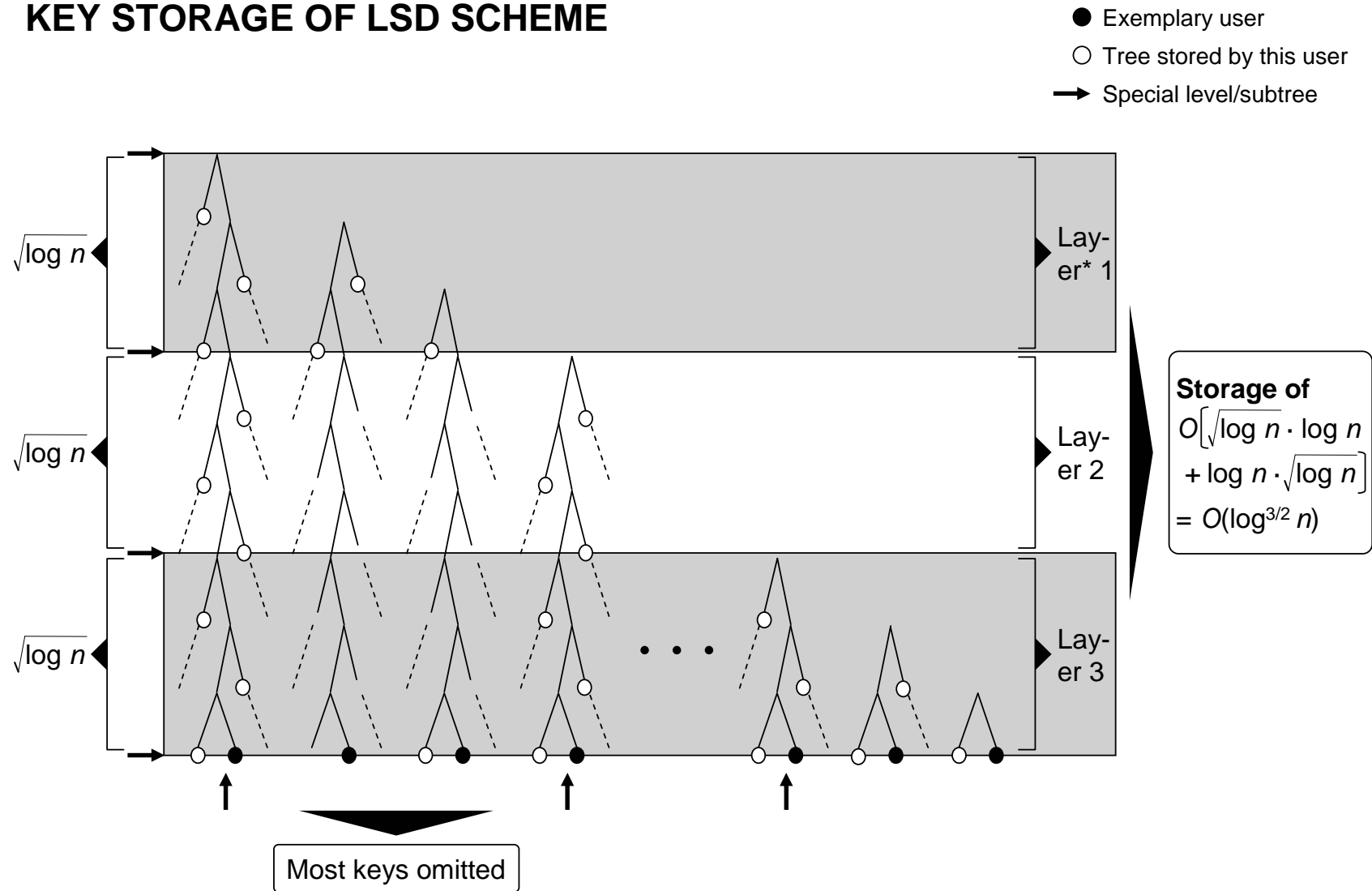


# AGENDA

- 
- Overview
  - Subset difference broadcast encryption (BE)
  - **Layered subset difference BE**

In the LSD scheme, a receiver still stores all keys of so called "special" subtrees, but omits most keys of non-special subtrees

## KEY STORAGE OF LSD SCHEME

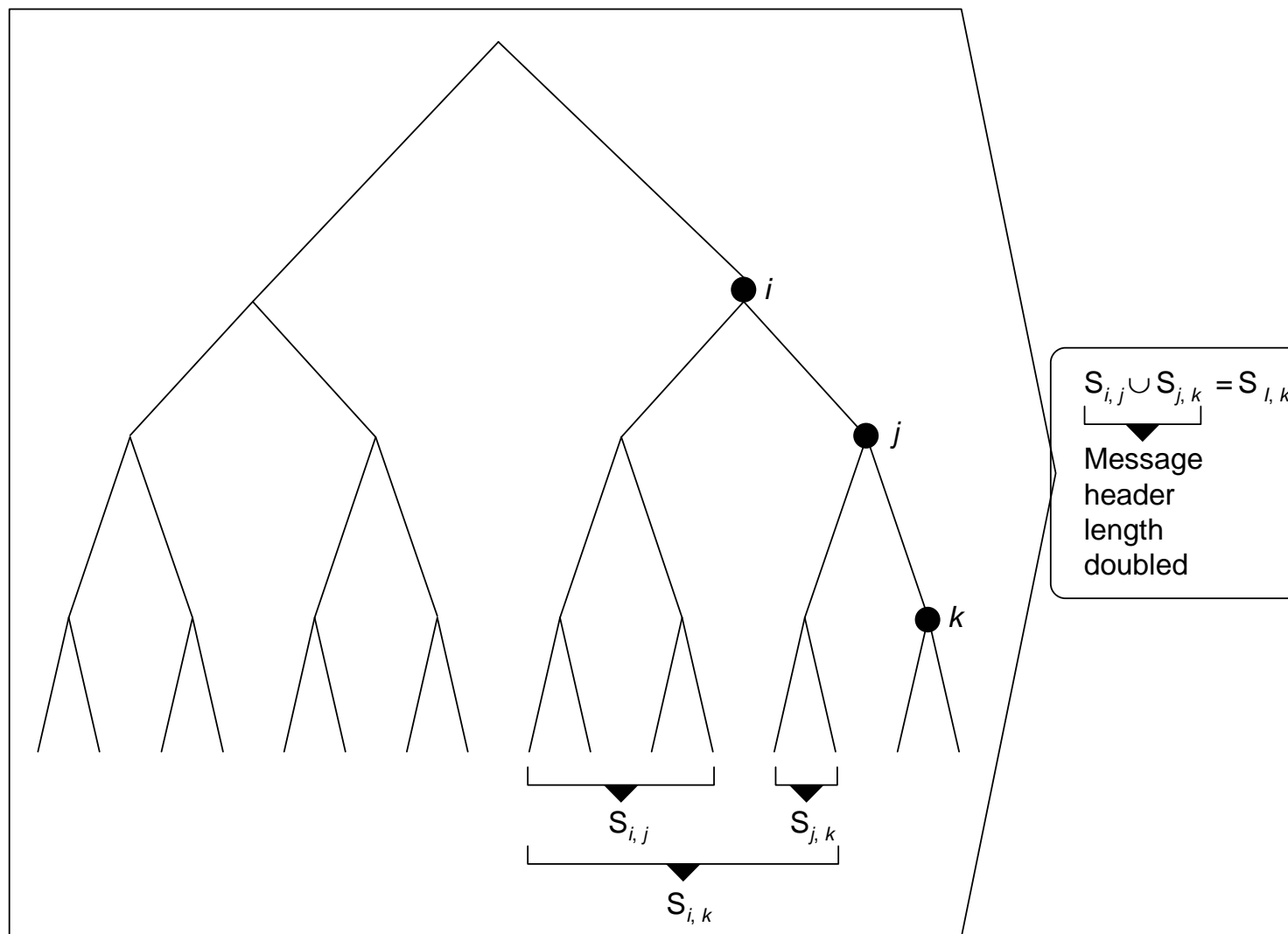


\* Each layer includes both adjacent special levels

Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60

**A trivial property of the LSD subsets allows to reconstruct the SD subsets with an increased message header length**

## **RECONSTRUCTION OF SD SUBSETS WITH LSD SUBSETS**



The trivial property is applicable for each relevant receiver because he has exactly one of the two necessary keys

## RECONSTRUCTION AS SEEN BY A PARTICULAR USER

