Multicast Security Project

Alain Pannetrat, Refik Molva
Melek Önen

Institut EURECOM
Sophia Antipolis - France

Multicast security issues

- **Multicast Confidentiality and key distribution**
  - **A Scalable key distribution scheme**
  - **A Multi-Layer Encryption scheme**

- **Multicast Authentication**
  - **An Efficient Multicast Packet Authentication**

Multicast Authentication

Basic Multicast Requirement: Scalability

- **1 Source (Generator) – N Recipients (Verifier)**
- **Generator ^{1} Verifier**

$\Rightarrow$ Requirement for an Asymmetric Solution

Real-time Streaming

Streams of Packets vs Application Messages

- **Authentication of Individual Packets**
- **Loss-tolerant Authentication**
- **Space constraints**

Pre-recorded data

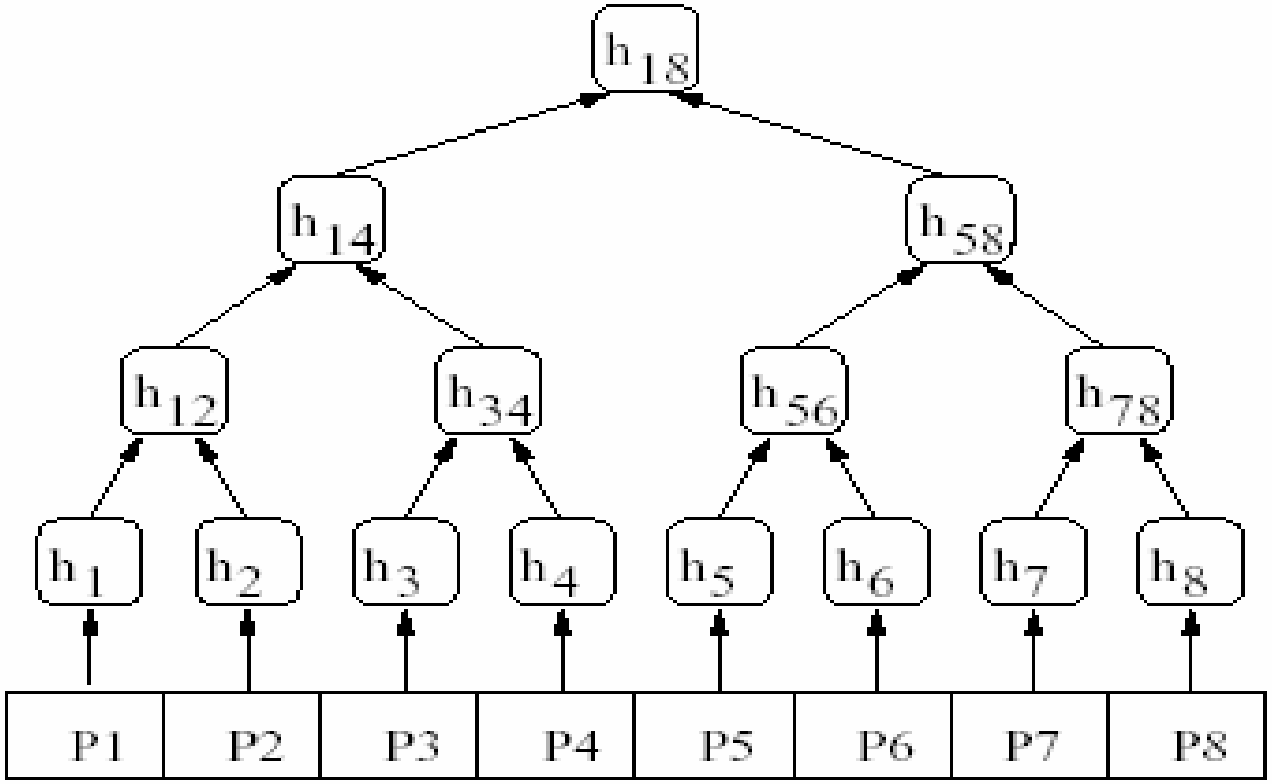
- **Time-constrained Play back Þ Fast Verification**

Real-time data

- **Fast Generation and Fast Verification**

Þ Requirement for Symmetric Algorithms

Hash Trees



- **[Wong&Lam 99]**

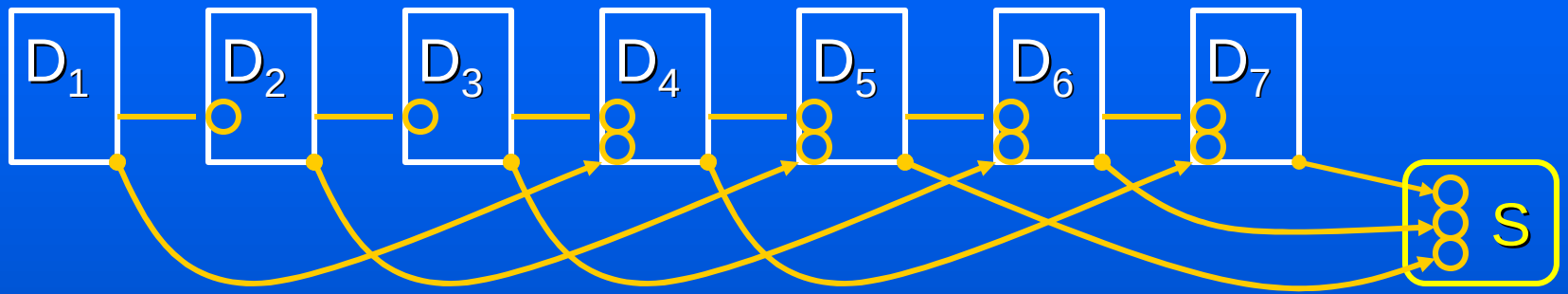
Approaches

Requirement Summary for packet authentication :
Scalable, Asymmetric, Fast, Bandwidth Efficient, Loss Resilient

- **MAC extensions**
  [Canetti et al 99]
  TESLA [Perrig et al 00]

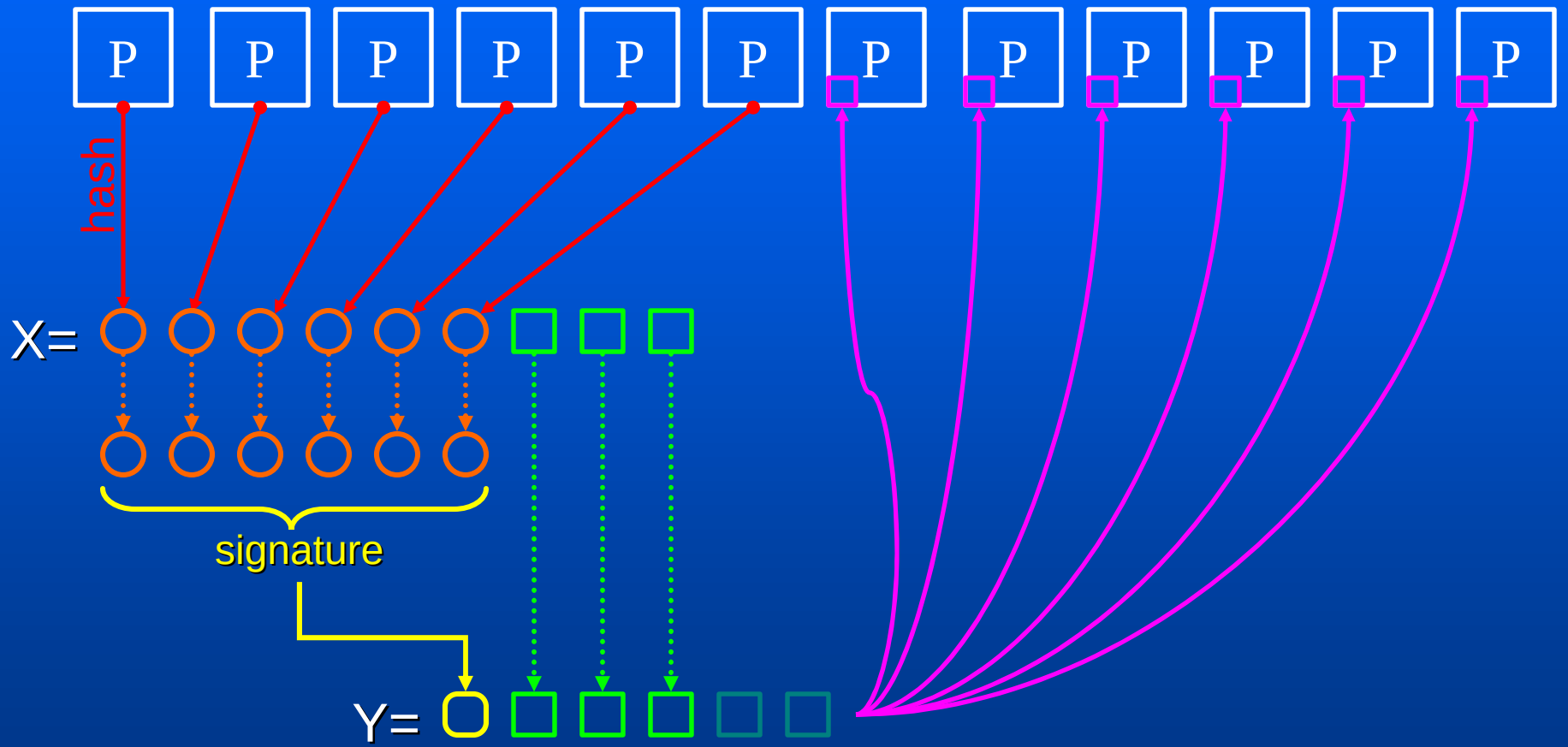
- **Digital Signature**
  - **Fast signature: [Rohatgi 99], BiBa [Perrig 01], [Reyzin 02]**
  - **Signature Amortizing:**
    - Hash trees
    - Hash chains
    - FEC

Hash Chains

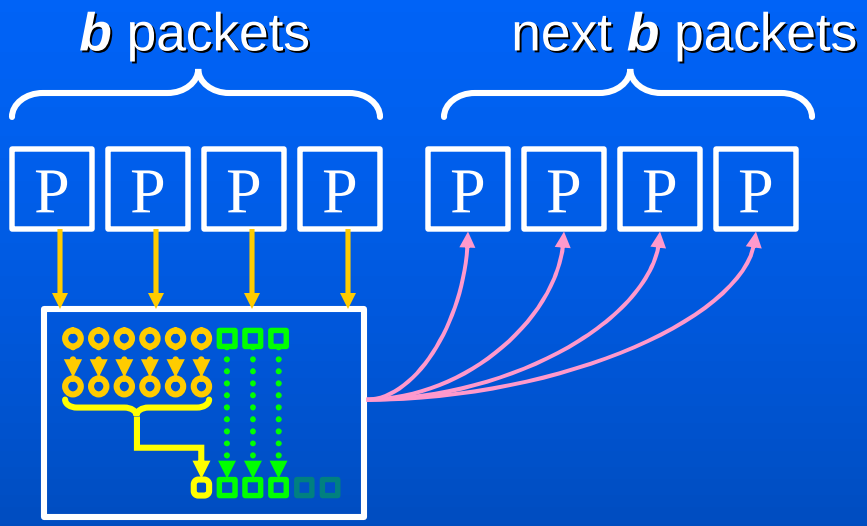


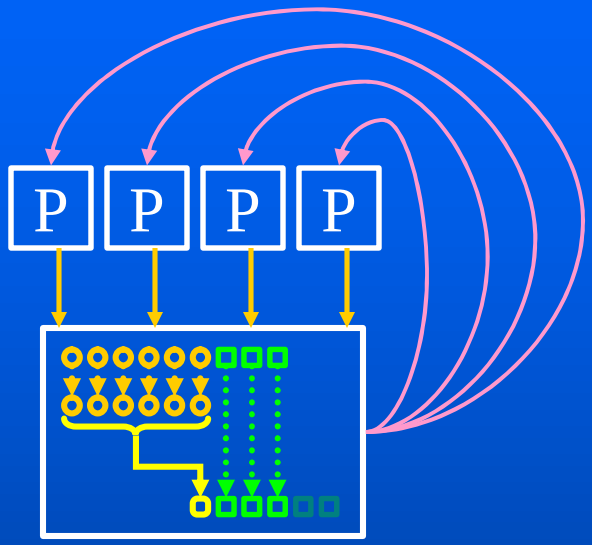
- **[Gennaro & Rohatgi 97]**
- **EMSS [Perrig et al 00]**
- **[Golle & Mogadugu NDSS'01]**
- **[Miner & Staddon 01]**

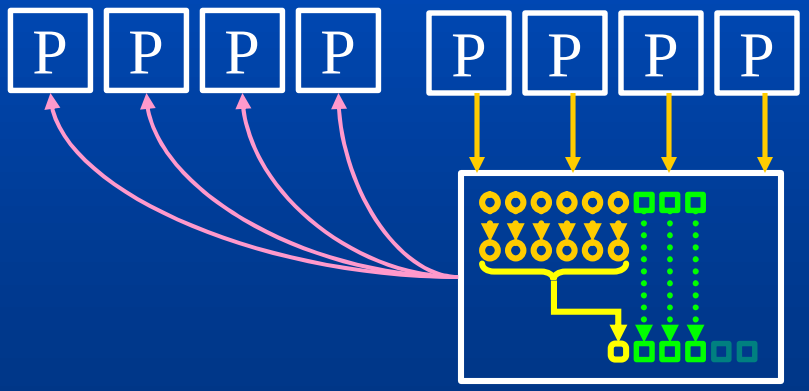
Our Solution : Use of erasure codes



3 Modes







Parameters

- **The block size: *b***
  - **When *b* ↗ , latency (buffering) ↗**
  - **When *b* ↘ , computational cost ↗**
  - **Choose *b* as large as possible within application constraints**

- **Maximum acceptable loss rate *p***
  - **Defines the redundancy generated by the Erasure Code.**
  - **Use Gilbert model to simulate losses (2-state Markov chain).**

Comparison

- **Case 1: Sensors**
  - 10 Kbps (20 pkt/s, 64 B/pkt)
  - Max. verification delay : 10 s
  - Packet loss rate : **5%**
  - Average burst size: **5 packets**
    - tags on the next block
    - b = 100 packets
    - p = 0.27
- **Case 2: Video broadcast**
  - 2 Mbps(512 pkt/s, 512 B/pkt)
  - Max. verification delay : 1 s
  - Packet loss rate : **60%**
  - Average burst size: **10 packets**
    - tags on the same block
    - b = 512 packets
    - p = 0.73

Overhead (bytes/packet)

	Case 1	Case 2
Hash chains	38	58
EMSS	34	84
Our Solution	8	45

Conclusion

- **Solution with lowest overhead**
- **Key points:**
  - **FEC over packets vs. FEC over authentication data**
  - **Minimal redundancy (no transmission of hash values)**

Multicast Confidentiality

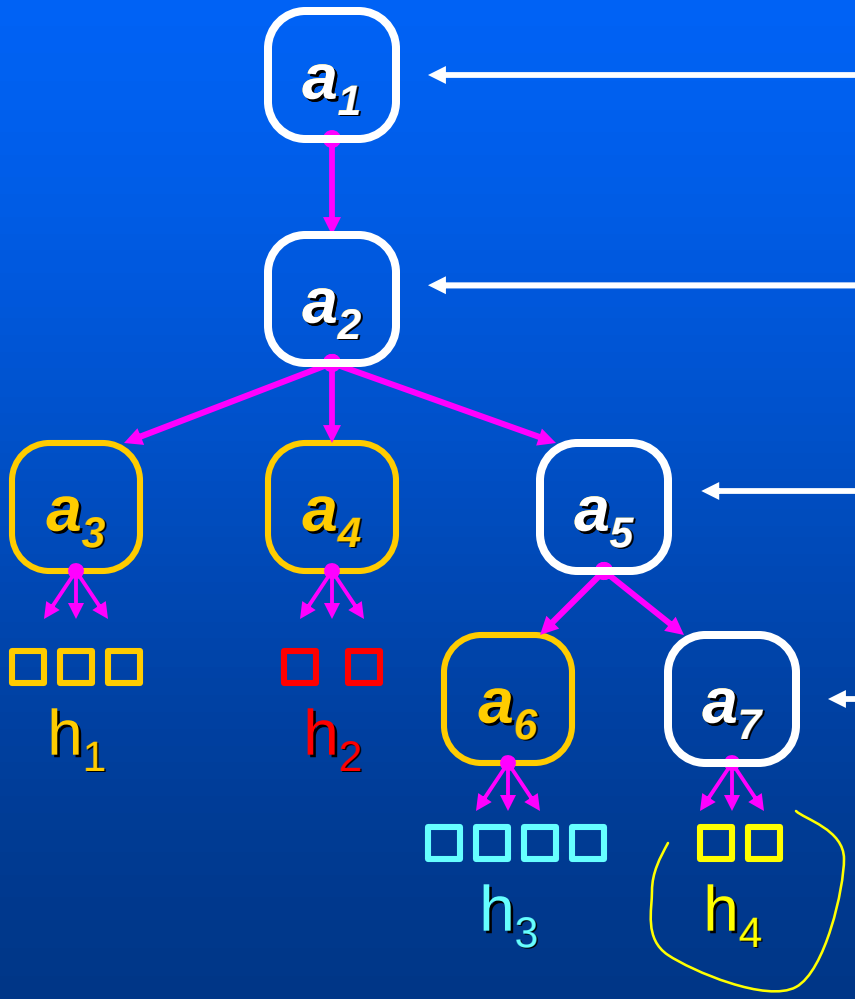
- **Security**
  - **Membership**
  - **Containment**
- **Scalability**
  - **Processing cost**
  - **Membership dynamics**
    - No group-wide re-key message
- **2 solutions :**
  - **A Scalable key distribution scheme**
  - **A Multi-Layer encryption scheme**

} **Use intermediate nodes**

Parametric Sequences : Properties

- **Limited trust in the intermediate elements**
  - **They don’t access the multicast data**
  - **They perform blind transformations**
- **Containment trough limited key scope**
  - **Security: key exposure is limited to a subgroup**
  - **Scalability: join/leave operations only impact a subgroup**

Parametric sequences



Source sends :

$$S_1 = (S_0)^{a_1} \bmod N$$

Node sends :

$$S_2 = (S_0)^{a_1 a_2} \bmod N$$

Node sends

$$S_3 = (S_0)^{a_1 a_2 a_5} \bmod N$$

Node sends:

$$S_4 = (S_0)^{a_1 a_2 a_5 a_7} \bmod N$$

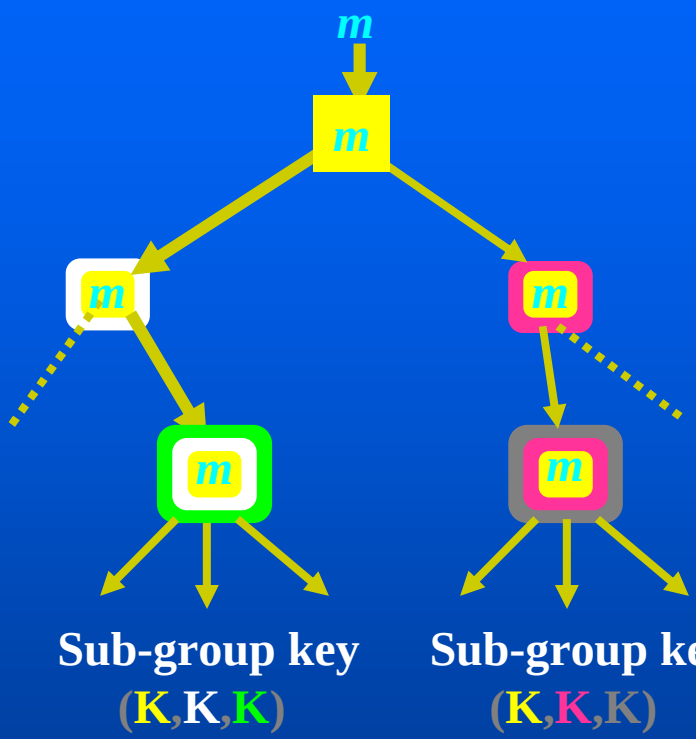
$$h_4(x) = x^B \bmod N,$$

$$B = 1/(a_1.a_2.a_5.a_7) \bmod j\,(N)$$

$$h_4(S_4) = S_0$$

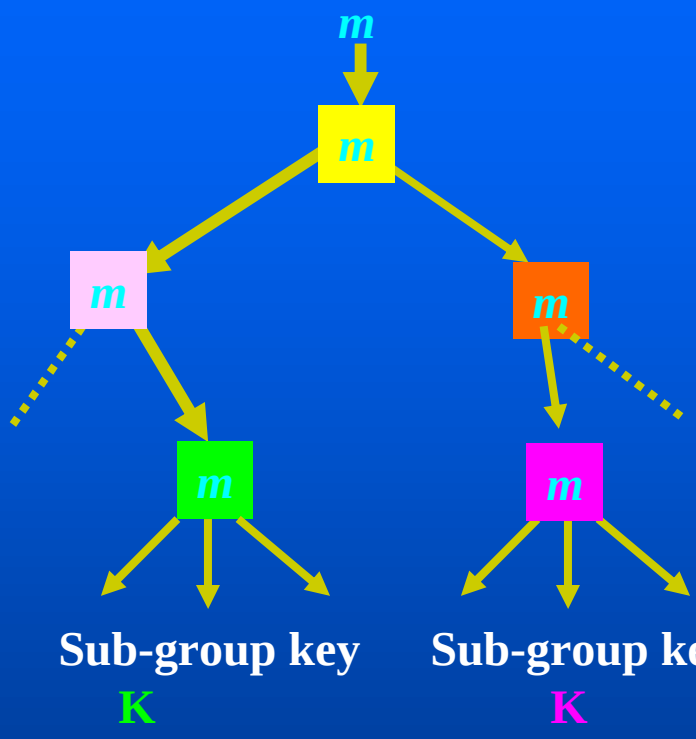
Using Intermediate Elements

Parametric Sequences



- **Pros: no trust in IE**
- **Cons: asymmetric algorithms not suitable for bulk data encryption**

Iolus

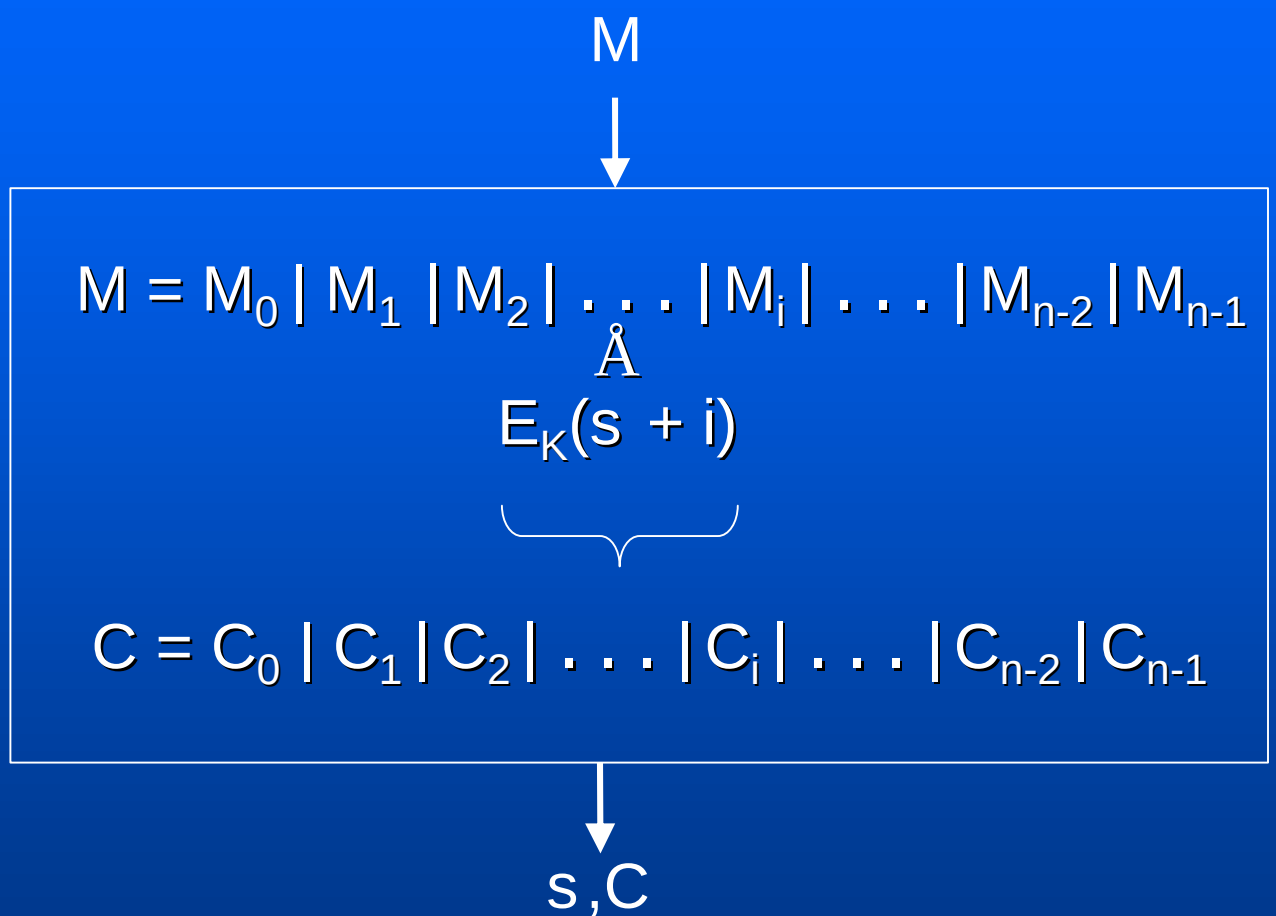


- **Pros: symmetric encryption**
- **Cons: IE must be trusted**

Multi-layer Encryption

- **Goal: Combine advantages of Iolus and Parametric Sequences to get fast bulk data encryption with containment**
- **Solution: Use symmetric encryption in XOR-Counter mode.**
  - **Apply several layers of encryption at the source and recipients.**
  - **Only two operations in the intermediate elements.**
    - One symmetric decryption
    - One symmetric encryption

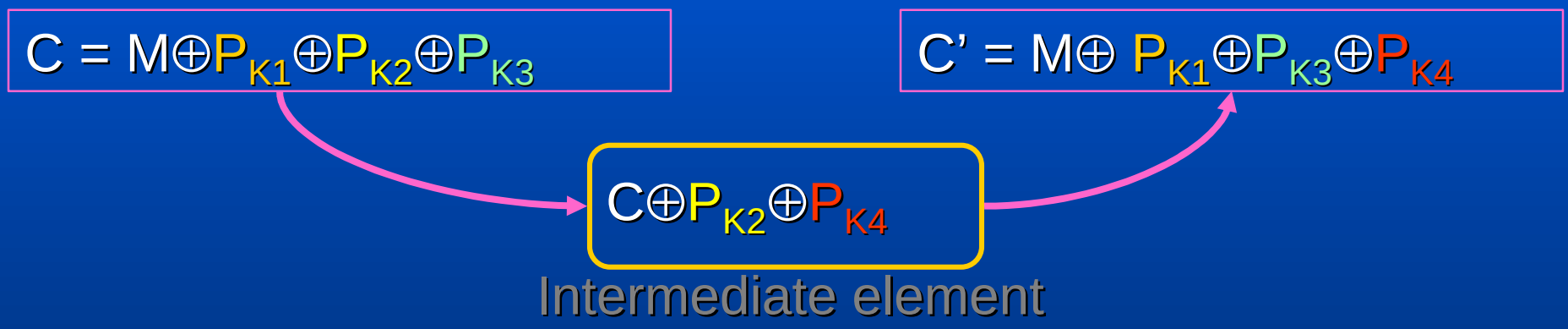
Counter Mode (CTRM) Encryption



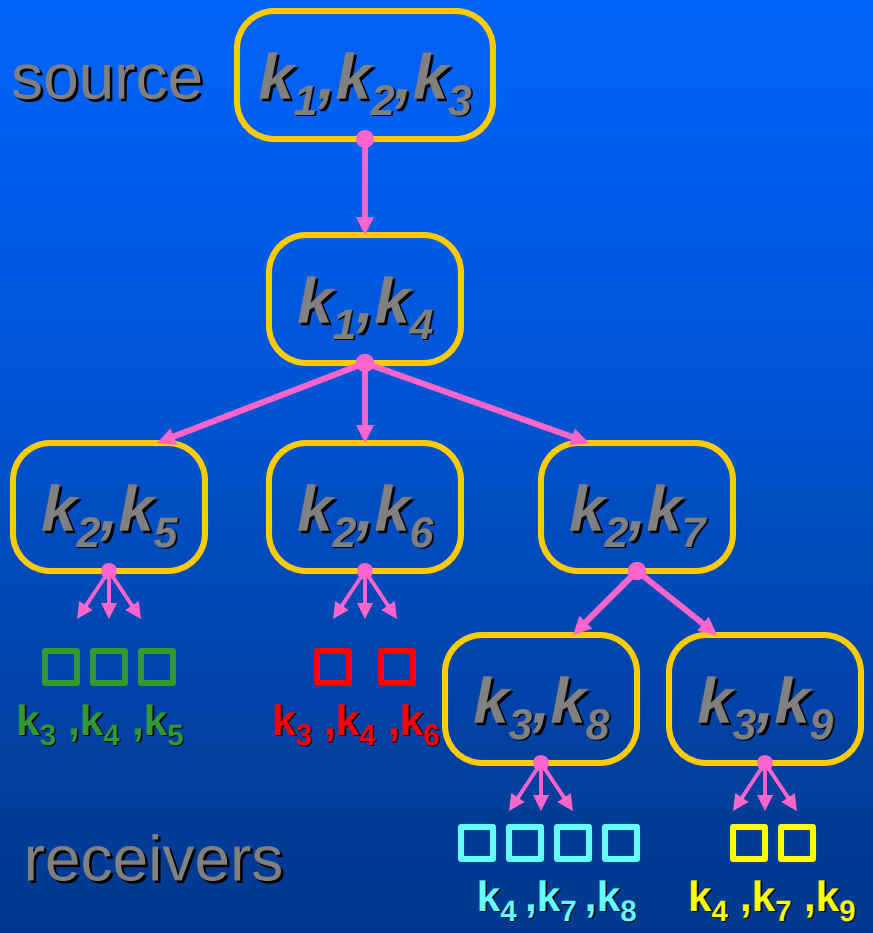
- **[Bellare et al] Security Equivalent to PRF E**

Multi-layer CTRM

- **Thanks to the commutativity of X-OR**
- **Intermediate elements can add and remove encryption layers**
- **Without accesing the cleartext information**

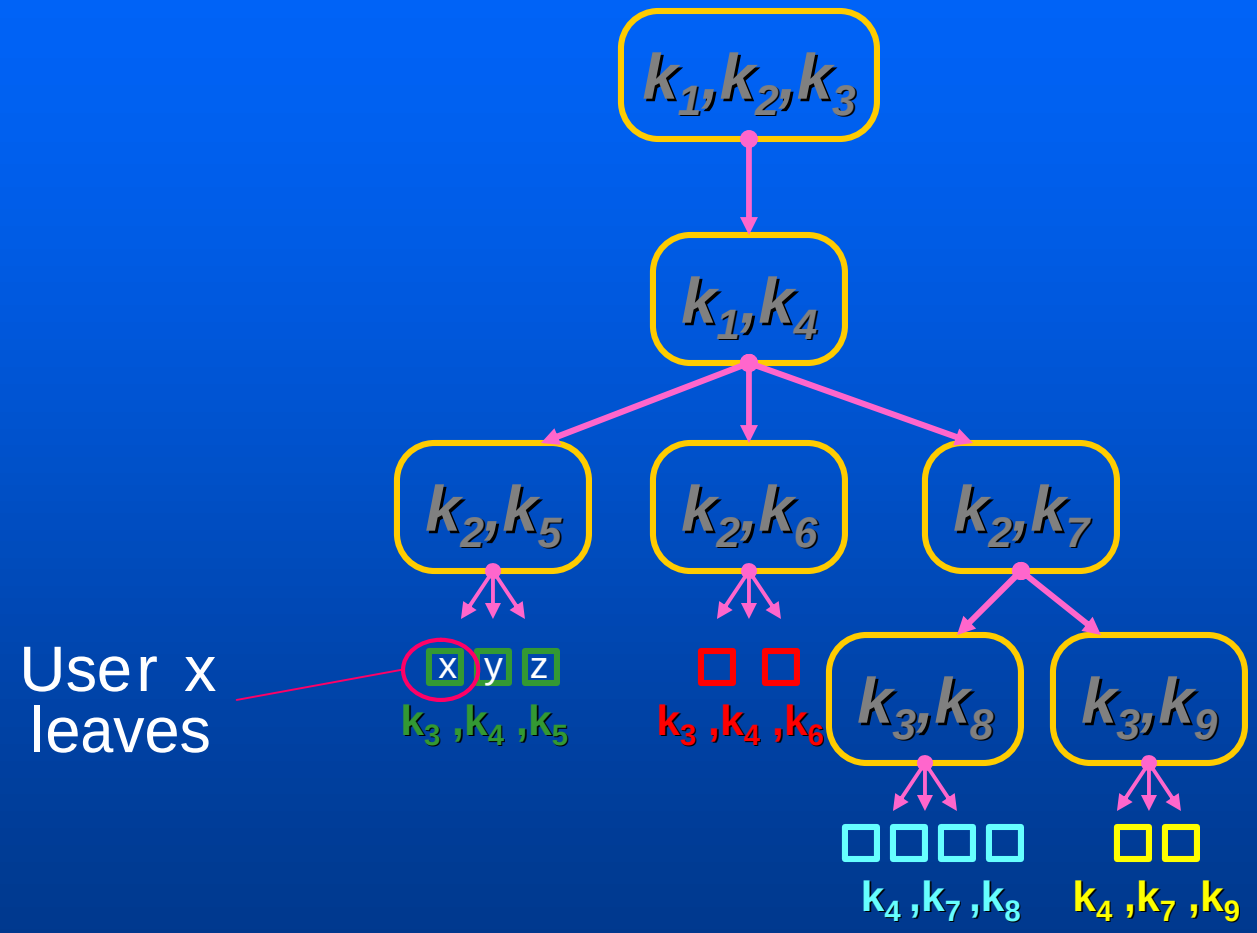


M-layer Data encryption Tree

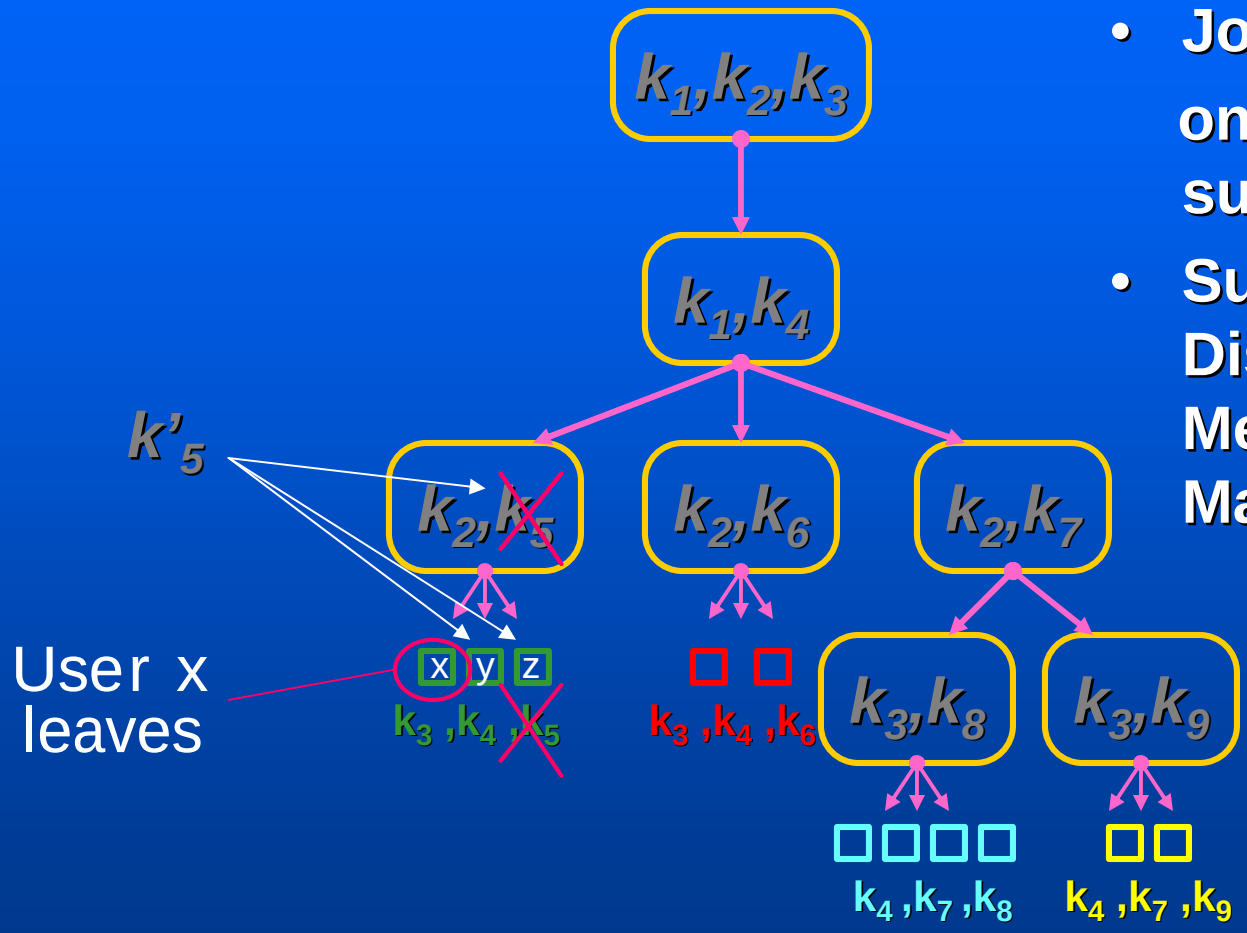


- **Cost**
  - **Source: M operations**
  - **Recievers: M operations**
  - **Intermediate Nodes: 2 operations**
  - **Linear (M) increase w.r. to bulk data encryption with a shared group key**

Membership Management



Membership Management



- **Join & leave only affect the sub-group**
- **Suitable for Distributed Membership Management**

Conclusion

- **Our approach**
  - **Based on the same principle as multicast protocols to achieve scalability: *use intermediate elements***
  - **No trust in intermediate elements ([1] Iolus)**
- **A new concept: Containment and location-dependent group keys**

Unique solution offering

- Scalability
- containment
- bulk data encryption

References

- **A. Pannetrat, R. Molva.** ***Efficient Multicast Authentication (NDSS'03)***
- **A. Pannetrat, R. Molva.** ***Multiple Layer Encryption For Multicast Groups (6th IFIP Communications and Multimedia Security Conference'02)***
- **R. Molva, A. Pannetrat.** ***Scalable Multicast Security in Dynamic Groups (ACM CCS'99)***

THANK YOU