Improved Key Management for Fiat-Tassa Dynamic Traitor Tracing

Tzong-Chen Wu, **Yen-Ching Lin**, and Ming-Chin Lee

Department of Information Management
National Taiwan University of Science & Technology
Taipei, Taiwan

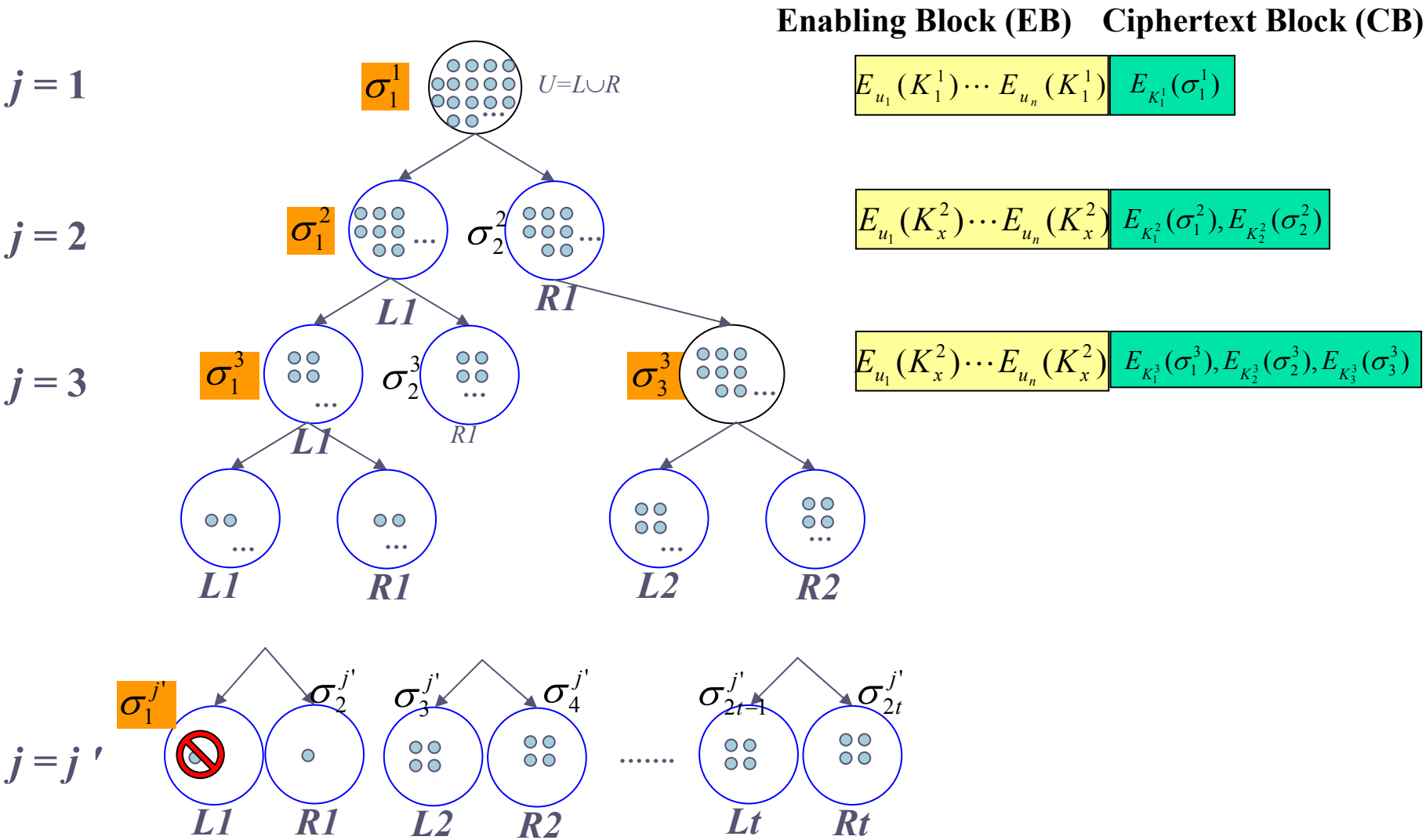
Introduction

- Fiat and Tassa (CRYPTO 1999) proposed a new traitor tracing mechanism by using fingerprinting techniques that guarantee to identify at least one traitor when subscribers collude to construct a pirate decoder
- In the Fiat-Tassa scheme, each subscriber has only one personal key initially, but the broadcaster should need to construct an enabling block that contains $O(n)$ encrypted keys used for recovering the session key

Introduction (cont.)

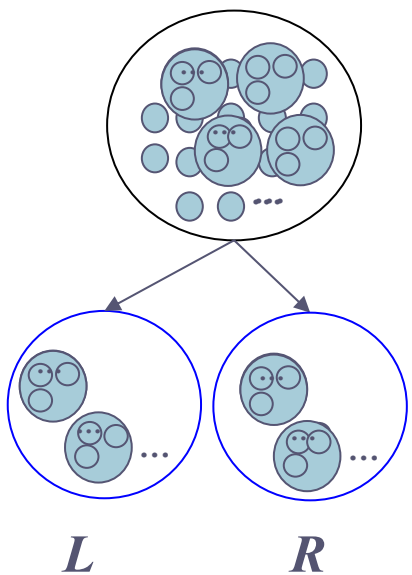
- The Fiat-Tassa scheme requires a large amount of transmission bandwidth and computational overhead for broadcast encryption
- Our proposal uses the Subset-Difference method proposed by Naor et al . (CRYPTO 2001) to construct a key tree hierarchy formed by the personal keys for the subscribers
- The improved key management mechanism preserves the security properties provided by the original Fiat-Tassa scheme
- The size of the enabling block produced by our proposal is reduced significantly from our experimental results

Tracing Process in Fiat-Tassa Scheme



Main Idea of Our Proposal

- Divide the set of n subscribers into smaller disjoint subsets
- All subscribers in the same subset share a set of secret keys



subscriber

subscriber subset s_{x_i, y_i}

Enabling Block (EB)

$$\underbrace{\boxed{E_{u_1}(K_1^1)\cdots \qquad E_{u_n}(K_1^1)}}_{n}$$

Fiat-Tsaas

$$\underbrace{\boxed{E_{s_{x,y}}(K_1^1)\cdots E_{s_{x',y'}}(K_1^1)}}_{c}$$

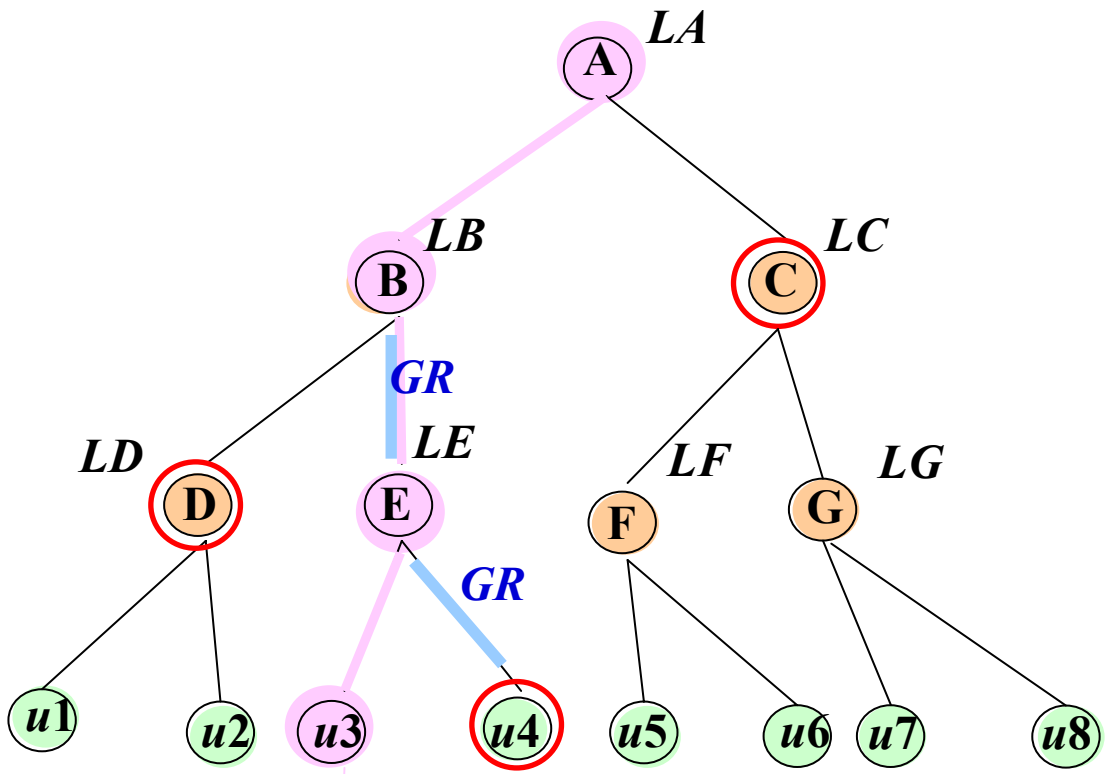
Our proposal

$c = F(t, spt)$

t: # of traitors could be detected

spt: pre-defined size of subset

Key Hierarchy of Our Proposal using Subset-Difference method



$L_{A,C}$, $L_{A,D}$, $L_{A,u4}$,
$L_{B,D}$, $L_{B,u4}$,
$L_{E,u4}$,
initial

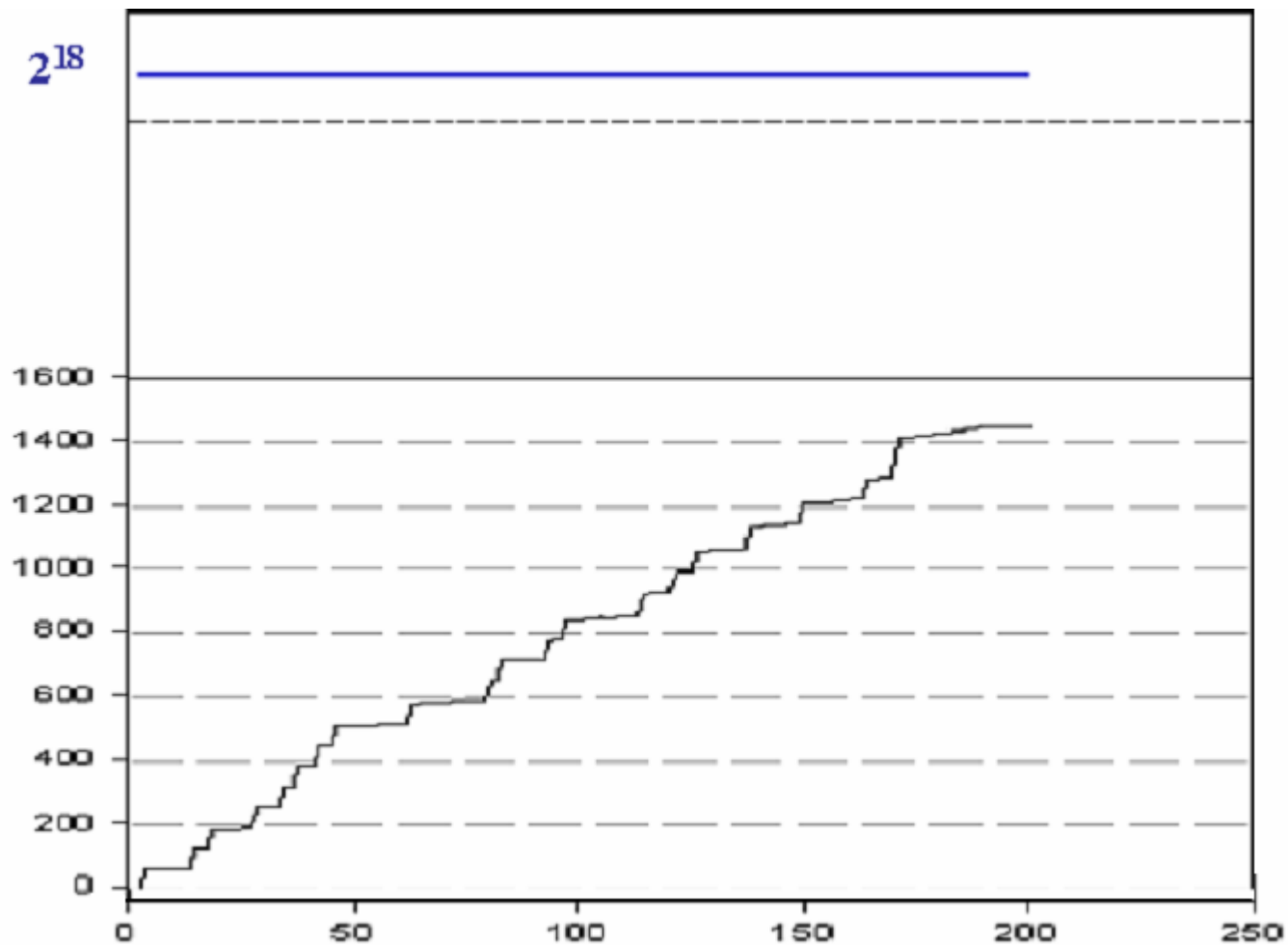
GR: key generation function

$L_{B,u4} = GR\,(GR\,(LB))$

$L_{E,u4} = GR\,(LE)$

Experimental Result of Our Proposal with $n=2^{18}$, $spt=64$

EB size c



Fiat-Tassa scheme

Our proposal

j-th broadcast/tracing run

The First Glimpse of Comparison

	Fiat-Tassa	**Our Proposal**
Personal keys	1	$\log^2 n$
Enabling block size	n	$c = F(t, spt)$
Rounds for detecting traitor	$\log(n)$	$\log(n/spt)$

Notes:

t: # traitors could be detected in each round

spt: pre-defined size of subset

Thank you

for your attention