Anonymity and unlinkability in ring signature-based discussion boards

Oriol Alàs, Francesc Sebé, Sergi Simón

Dept. Matemàtica

Universitat de Lleida

Ring signatures

- Digital signature

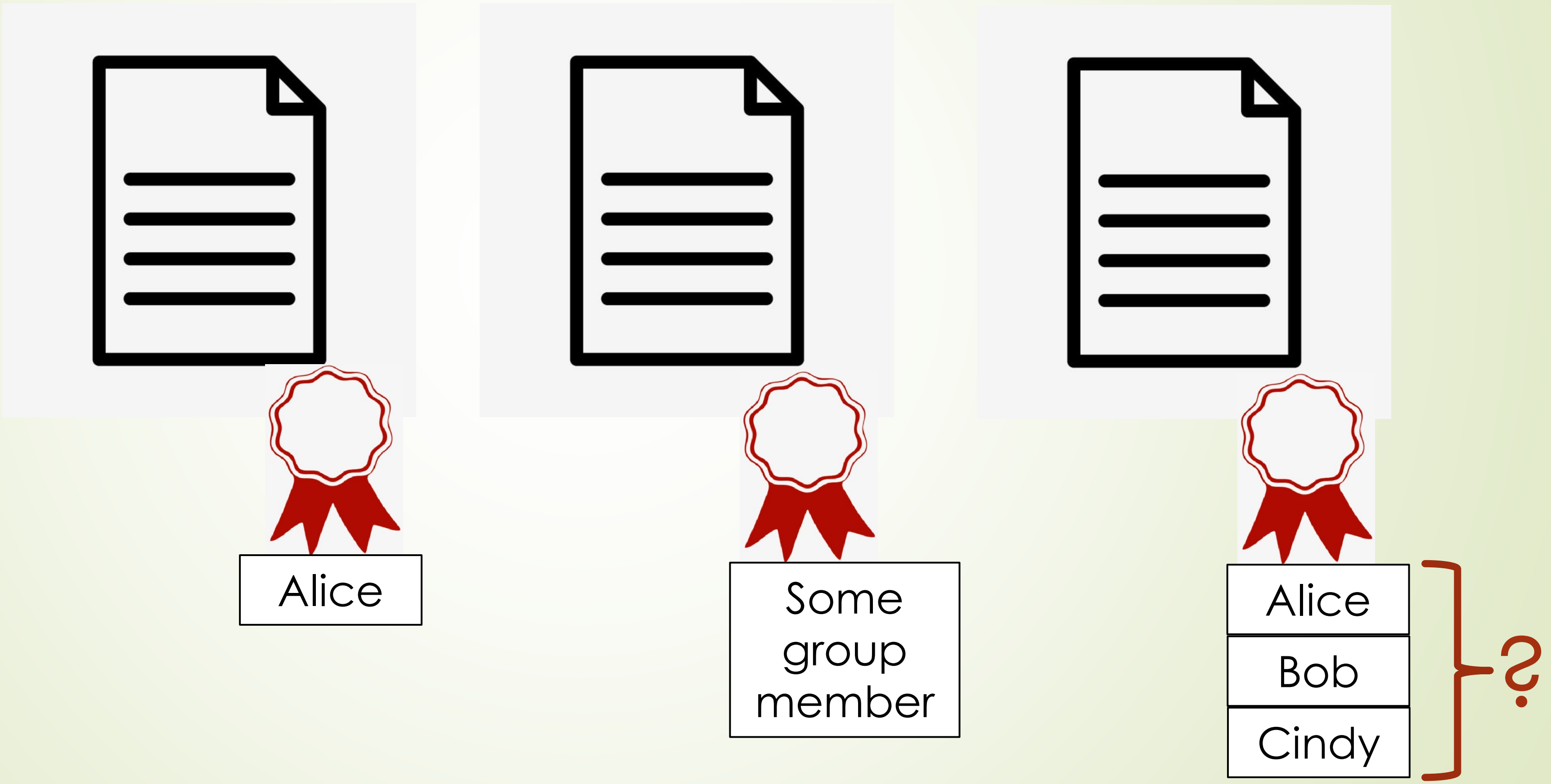
Ring signatures

- Digital signature

- Group signature

Ring signatures

- Digital signature
- Group signature
- Ring signature



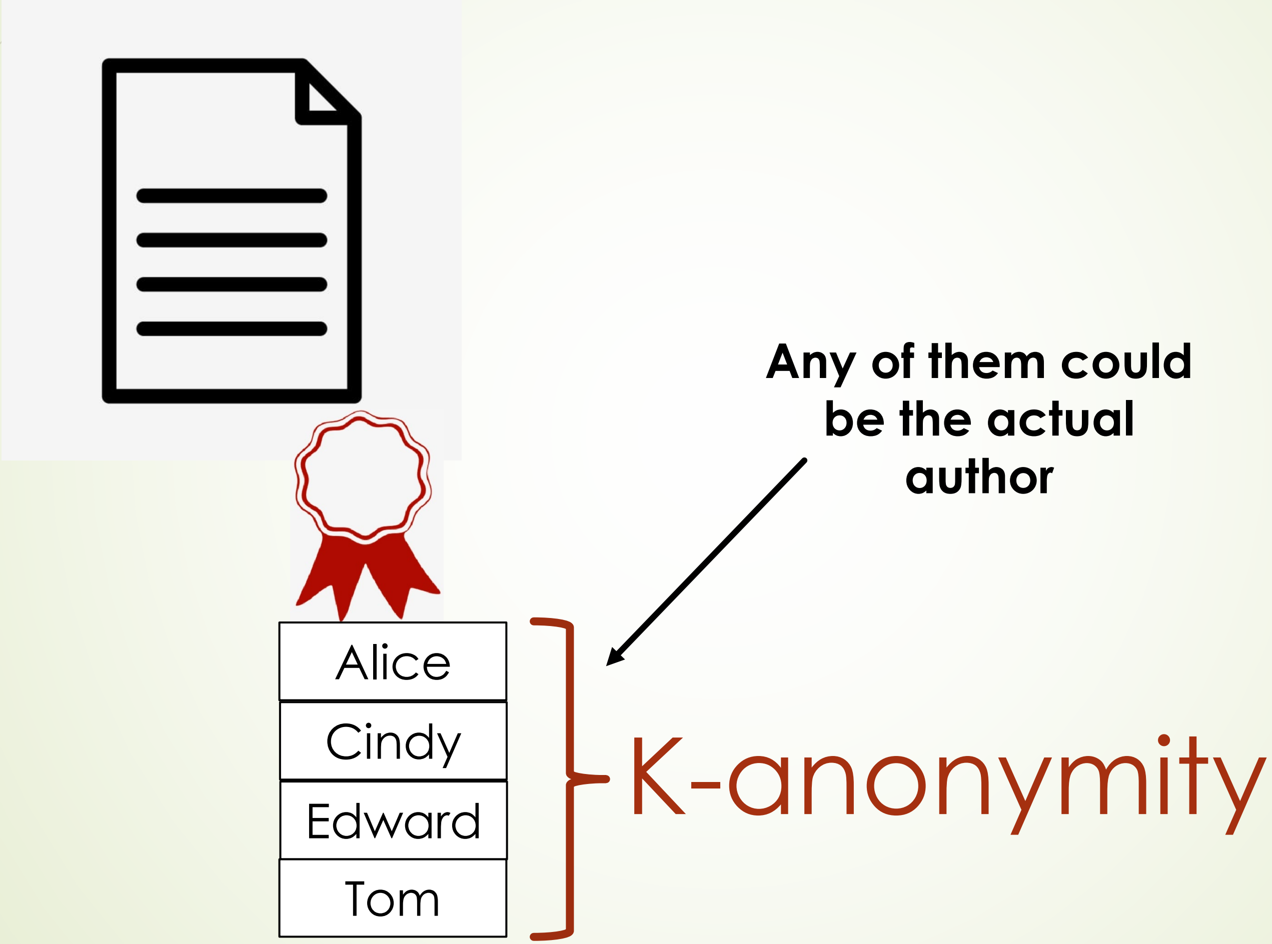
Scenario

- Discussion board
  - Only registered users can post messages
  - Anonymous and unlinkable messages
- Group signatures attain these requirements
  - There exists a group manager who can lift anonymity of messages
- What about ring signatures?
  - Objective of our research

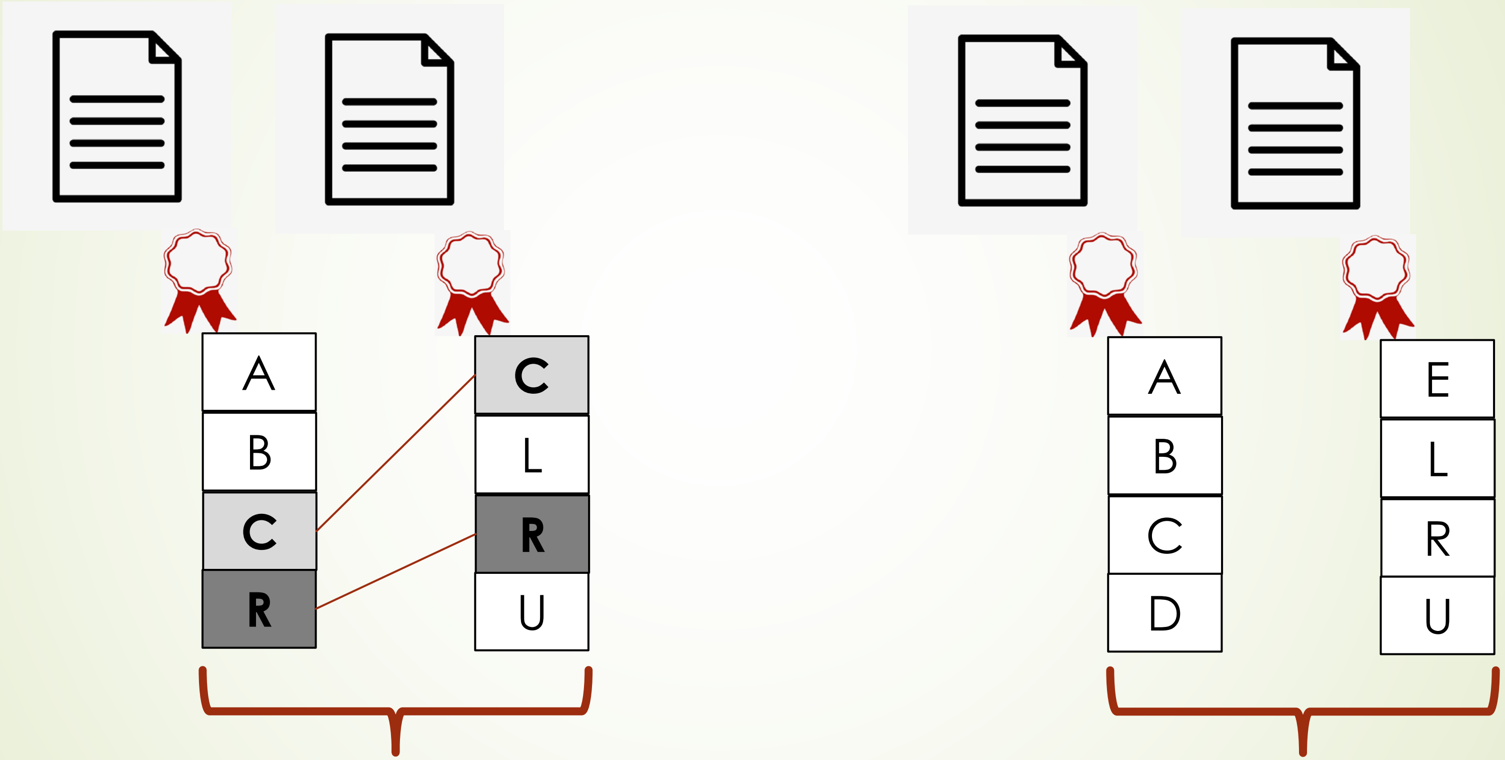
Forum operation

- Users enabled to post messages
  - Have a certified public key
- Posting a message
  - Write your message
  - Choose (K-1) forum members at random and take their public keys
  - Include your public key in that set
  - Compute the ring signature
  - Post the ring-signed message

Message anonymity



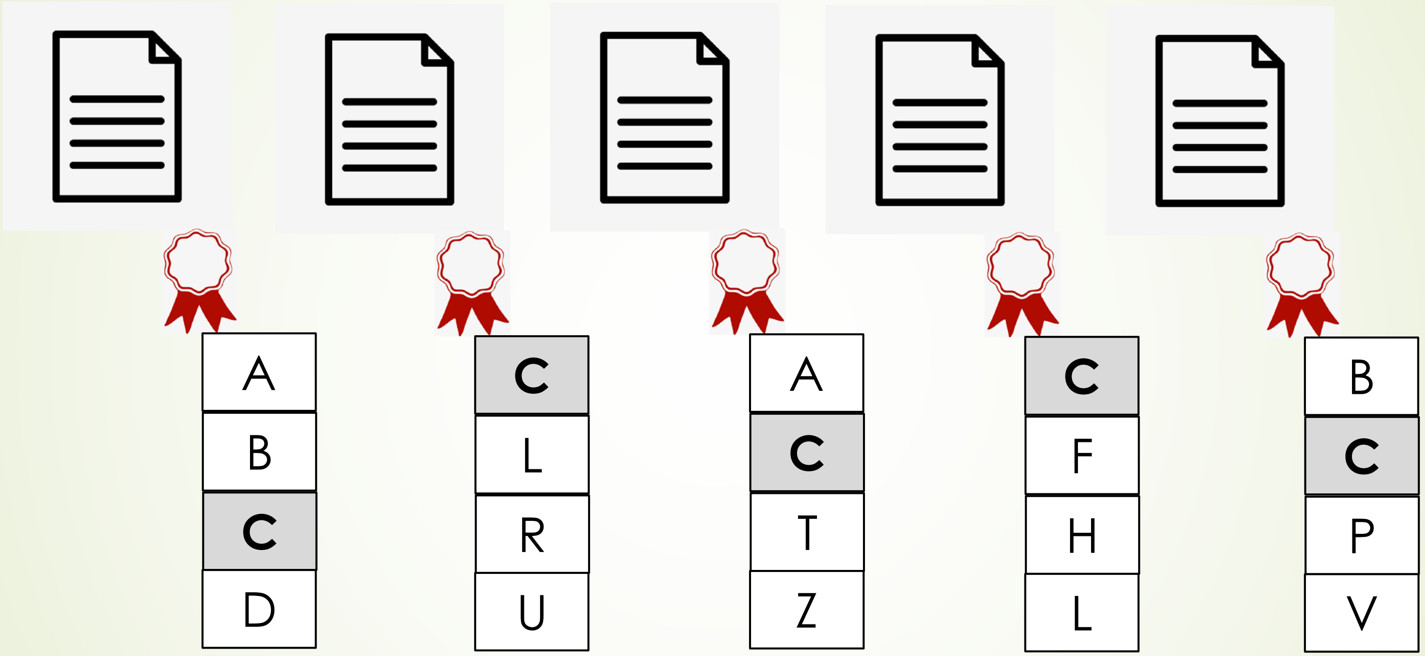
Message linkability



<u>May</u> have been written by the same person

<u>Cannot</u> have been written by the same person

Message linkability



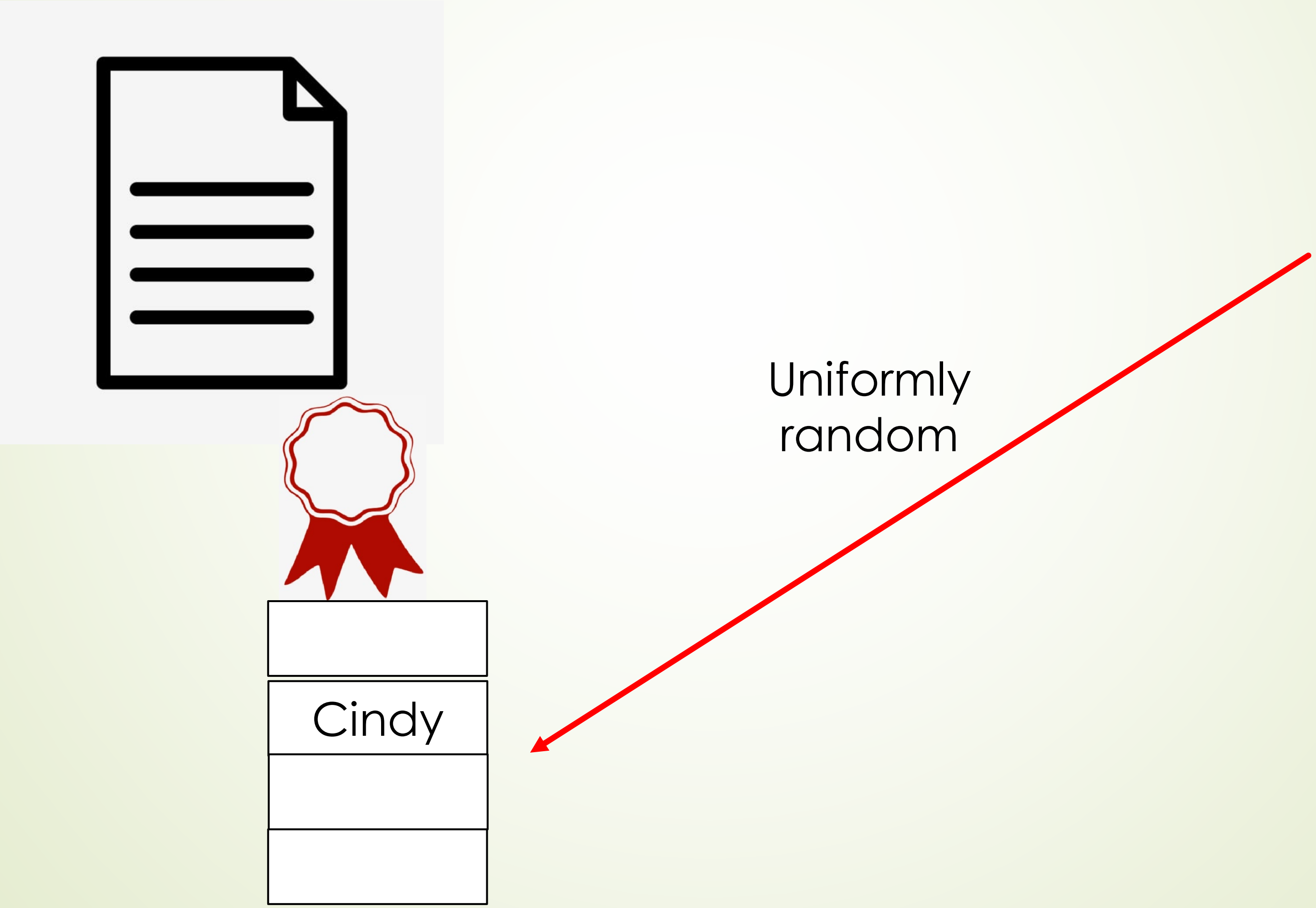
Which of these messages were really authored by C?

- Ratio $K_C = \frac{N_C}{n_C}$
- N_C : # Messages including C in its ring
- n_C : # Messages really authored by C

Message linkability

- $K_C = \frac{N_C}{n_C}$
  - Random variable
  - Its distribution depends on the strategy to compose rings

Uniformly random choice of ring members



Forum members
Alice
Bob
Cindy
David
Edward
$(\cdots)$

Each member has a $\frac{K-1}{M-1}$ probability of being chosen

Uniformly random choice of ring members

- The number of times you are chosen to be part of a ring follows a binomial random model
  - $r_C \approx Bin\left(\hat{N}; \frac{K-1}{\hat{M}}\right)$
- It does not depend on your activity
  - Highly active forum members (n_C ↑↑) are less protected
  - $K_C = \frac{N_C}{n_C} = \frac{n_C + r_C}{n_C}$
- For $p[K_C \leq \mathcal{K}] \leq e^{-\varepsilon}$ $\rightarrow$ K=$O\left(\frac{\mathcal{K} n_C + \varepsilon}{\frac{\hat{N}}{\hat{M}}}\right)$
- Whatever the choice is
  - It will underprotect highly active members, or,
  - It will overprotect less active members

Preferential attachment strategy

- Probability of being chosen
  - Grows with the number of times you are in a ring
  - Constant term (w_i) + Proportional term (w_m)
- Highly active members
  - Always belong to the ring of their messages

Simulation results (w_i=3, w_m=10)

K	$User_1$	$User_5$	$User_{10}$	$User_{15}$
8	26.4	6.0	3.5	2.6
12	40.2	8.8	4.9	3.6
16	54.1	11.7	6.3	4.5

Privacy ($K_C = \frac{N_C}{n_C} = \frac{n_C + r_C}{n_C}$) using <u>uniform</u> strategy

Simulation results (w_i=3, w_m=10)

K	$User_1$	$User_5$	$User_{10}$	$User_{15}$
8	26.4	6.0	3.5	2.6
12	40.2	8.8	4.9	3.6
16	54.1	11.7	6.3	4.5

Privacy ($K_C = \frac{N_C}{n_C} = \frac{n_C+r_C}{n_C}$) using <u>uniform</u> strategy

K	$User_1$	$User_5$	$User_{10}$	$User_{15}$
8	20.7	6.3	4.8	4.4
12	33.3	9.6	6.7	6.0
16	50.1	13.6	8.7	6.5

Privacy ($K_C = \frac{N_C}{n_C} = \frac{n_C+r_C}{n_C}$) using <u>preferential attachment</u> strategy

Anonymity and unlinkability in ring signature-based discussion boards

Oriol Alàs, Francesc Sebé, Sergi Simón

Dept. Matemàtica

Universitat de Lleida