Wrocław University of Technology

General Anonymous Key Broadcasting via Lagrangian Interpolation

Łukasz Krzywiecki[1], Mirosław Kutyłowski[1], **Maciej Nikodem**[2]

[1]Institute of Mathematics and Computer Science
[2]Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology

Key Distribution Problem

How to exchange encryption key securely

- one-to-one communication
- many-to-many communication
- **one-to-many communication**

Obvious solutions

- secure communication channel

- public key cryptography

Shortcomings

- one-to-one communication is requried
- to exclude *k* out of *n* users we have to transmit *n*-*k* messages

Challange for Broadcast Systems

Key distribution from the broadcaster to the set of entiltled users over public broadcast channel.

Challenge:

- low communication overhead
- brodcaster determines the set of entiltled users
- **user anonymity**

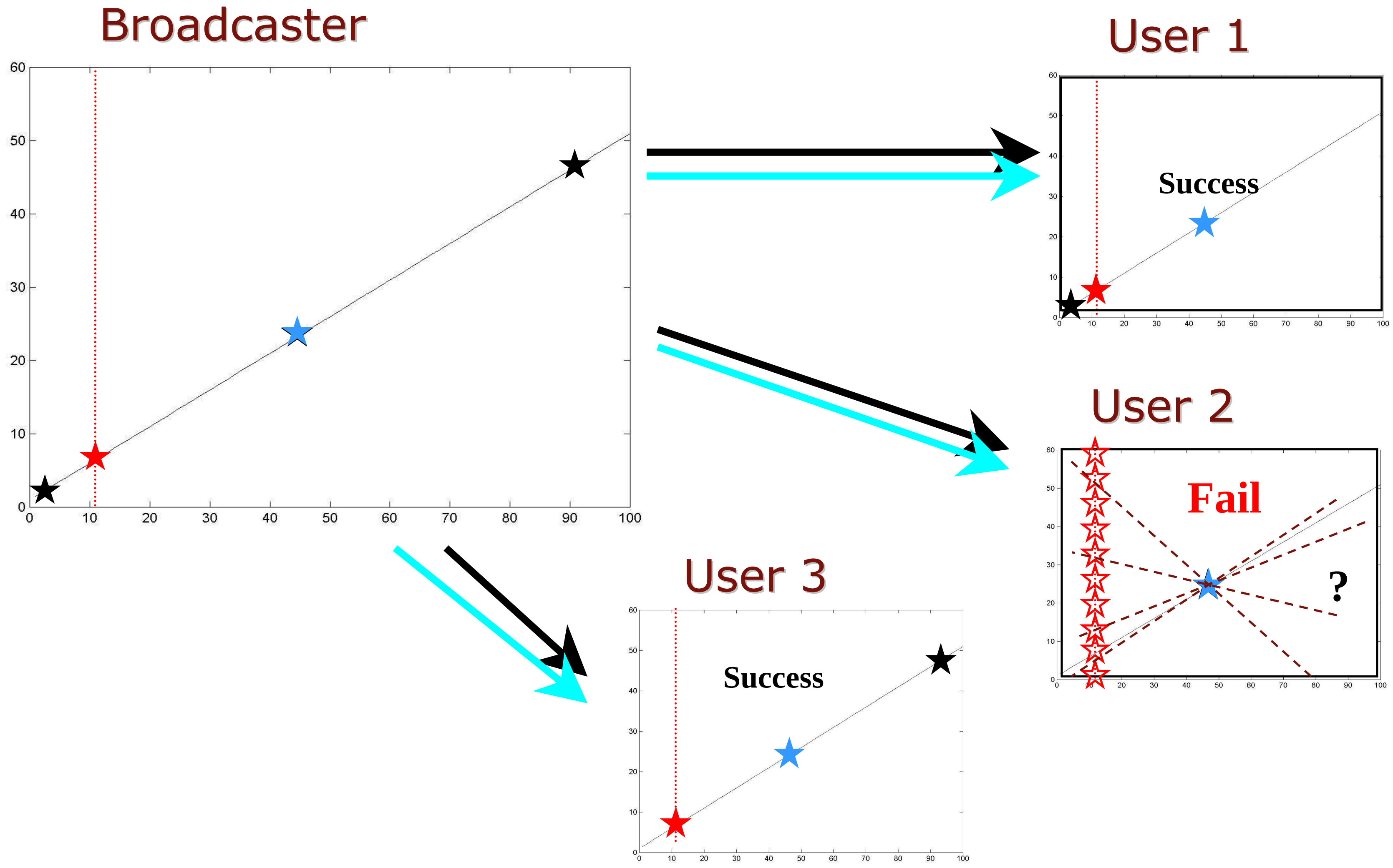
Typical Solution - Broadcast Exclusion

- based on (k,n) secret sharing
    - broadcaster has secret divided into >n shares
    - each user posses one share
    - to get the secret user has to receive k+1 different shares
- communication overhead depends on k
- shares for users are determined by broadcaster
- broadcaster can exclude up to k users
- **no anonymity**

Polynomial Interpolation

- tyically used in broadcast exclusion (BE)
- broadcaster‘s secret polynomial – $w(x)$ such that deg($w(x)$)=t
- each user knows exactly one point (x_u, $w(x_u)$)
- to reconstruct $w(x)$ user requires t additional points (x_j, $w(x_j)$) such that $x_j \# x_u$

Polynomial Interpolation - example



Broadcaster

User 1

Success

User 2

Fail

?

User 3

Success

Broadcast Exclusion (BE)

- based on **polynomial shared by all users**
- broadcaster determines the set of **excluded** users
- broadcaster sends *t* points
  - that belong to the **excluded users**
  - some randomly choosen $(\boldsymbol{x_i}, \boldsymbol{w(x_i)})$
- users can interpolate the polynomial **iff** they recive *t*+1 different points (i.e. they are non-excluded)

Broadcast Selection (BS) 1/2

- based on **random polynomial**
- broadcaster selects the set of **non-excluded** users
- broadcaster selects *t* points
  - that belong to **non-excluded users**
  - some randomly choosen **(x_i, y_i)**
- broadcaster constructs the polynomial $q(x)$

Broadcast Selection (BS) 2/2

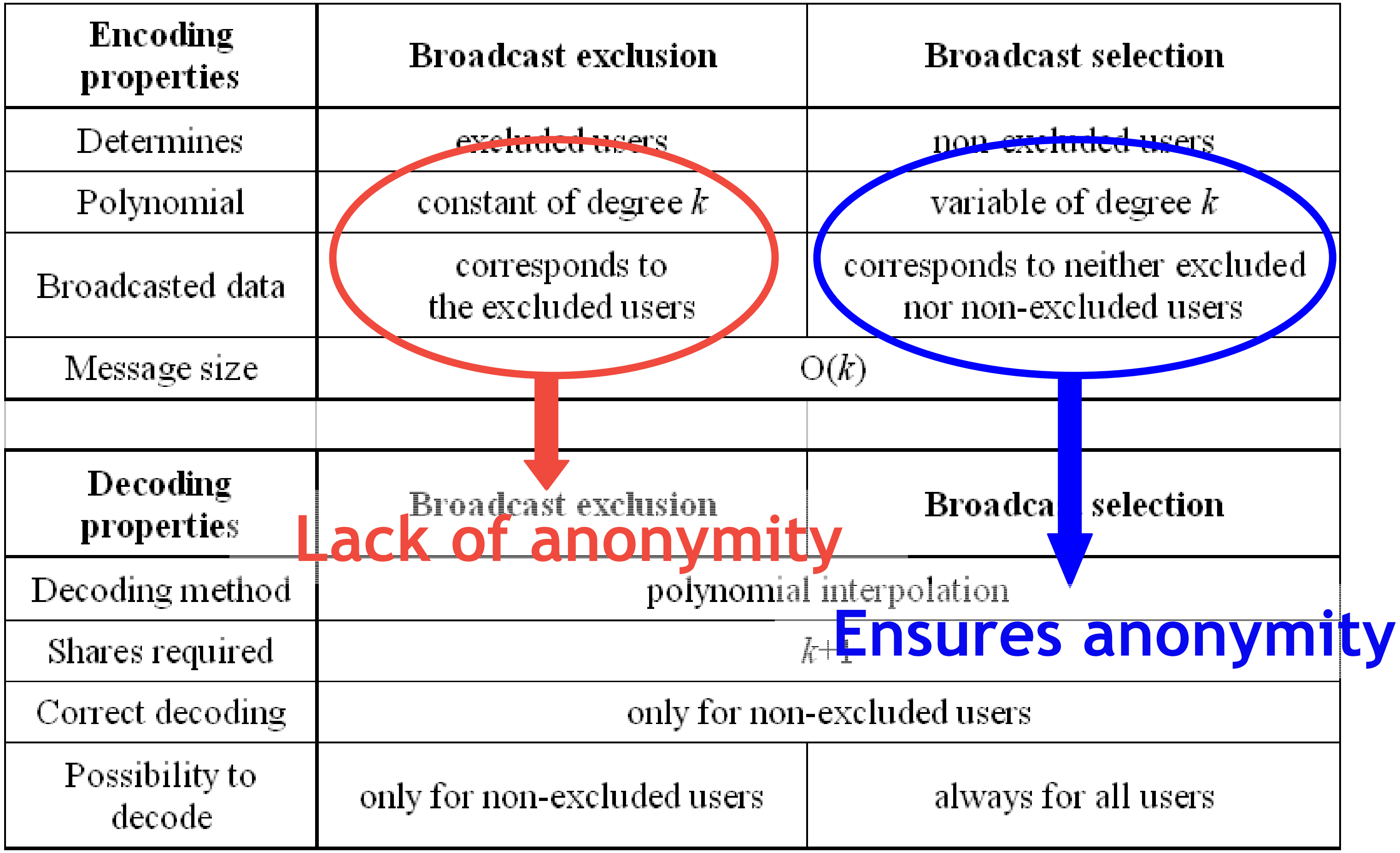
- broadcaster selects *t* points that belong to *q*(*x*), different than points of **non-excluded usres**

- users can **always** interpolate the polynomial
  but only non-excluded users get the polynomial *q*(*x*)

Decoding

- independent of encoding
- based on Lagrangian interpolation
- requries t+1 points from correct polynomial
- yields correct output only for non-excluded users
- unable to decode for excluded users

Broadcast Exclusion vs. Selection



Encoding properties	**Broadcast exclusion**	**Broadcast selection**
Determines	excluded users	non-excluded users
Polynomial	constant of degree k	variable of degree k
Broadcasted data	corresponds to the excluded users	corresponds to neither excluded nor non-excluded users
Message size	O(k)	

Decoding properties	**Broadcast exclusion**	**Broadcast selection**
Decoding method	polynomial interpolation	
Shares required	k+1	
Correct decoding	only for non-excluded users	
Possibility to decode	only for non-excluded users	always for all users

Lack of anonymity

Ensures anonymity

Our Proposal

- encoding
    - BE or BS depending on the number of users to be excluded
- communication
    - broadcast communication over insecure channel
    - *t* points from polynomial $w(x)$
- decoding
    - Lagrangian interpolation – indepedeently of encoding procedure

Security

- user’s shares
  - four shares for each user – assigned through mappings
  - the same share corresponds to different user depending on mapping
- polynomial interpolation
  - user’s shares hidden in the exponent
  - random integer *r* used to mask the polynomial
  - *k*-resilence
- broadcast selection
  - variable polynomial
  - no shares of excluded users send over the broadcast channel
- decoding
  - independent of encryption – no knowlege to the adversary

Security - external adversary

- cannot distingush whether BE or BS was used
- knows that BE and thus shares of excluded users occur with probability ½
- to increase attack difficulty BS use the same shares as BE – so called shadows
- shares denote different users depending on BS/BE and mapping used
- variable polynomial

Security - internal adversary

- can distingush between BE and BS **iff** excluded
- knows when shares of excluded users occur
- cannot trace particular user since shares change

Anonymity

- user’s share is transmited iff BE is used
- shadow of user’s share can be used when BS is used
- external observer doesn’t know if share that occur coresponds to user or its shadow
- internal observer has to determine all user’s shares

Conclusions

- applies to broadcast systems with dynamicly changing number of users
- takes advantage of BE and BS
- assigns different shares to user, and the same share to different users
- ensures security do to well known BE and BS
- ensures anonymity due to BS and the same sheres assigned to different users

Wrocław University of Technology

General Anonymous Key Broadcasting via Lagrangian Interpolation

Łukasz Krzywiecki[1], Mirosław Kutyłowski[1], **Maciej Nikodem**[2]

[1]Institute of Mathematics and Computer Science
[2]Institute of Computer Engineering, Control and Robotics
Wrocław University of Technology