Intactness Verification in Anonymous RFID Systems

Kai Bu[1], Jia Liu[2], Bin Xiao[3], Xuan Liu[3], Shigeng Zhang[4]
Zhejiang University[1], Nanjing University[2]
Hong Kong Polytechnic University[3]
Central South University[4]

Anonymous RFID

unknown tag identifiers (IDs)

Anonymous RFID Missing Tag Detection

unknown tag identifiers (IDs)

any missing tags?

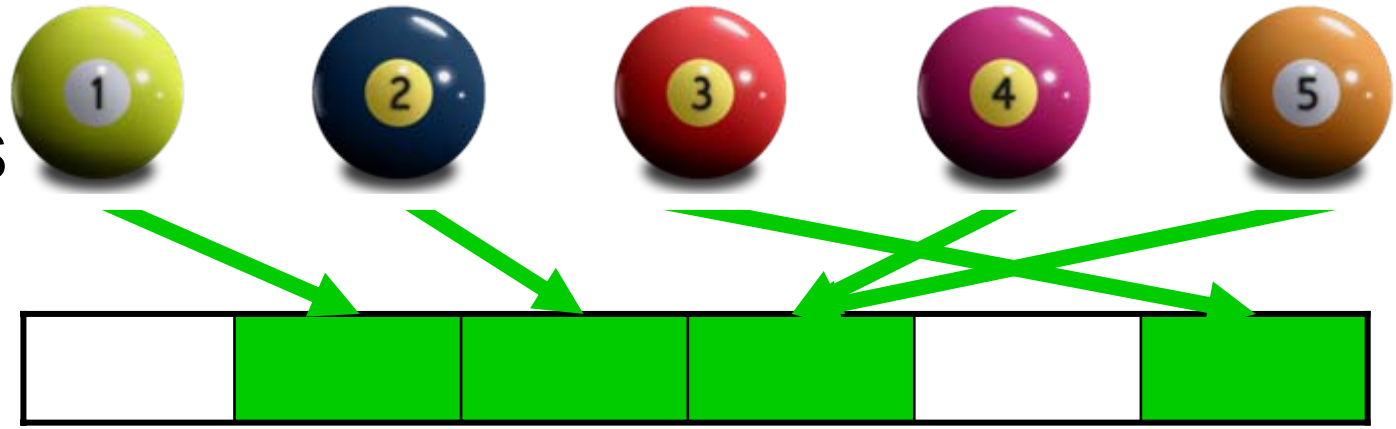
Is everyone here?

Things were easier with known tag IDs

Known Tag IDs

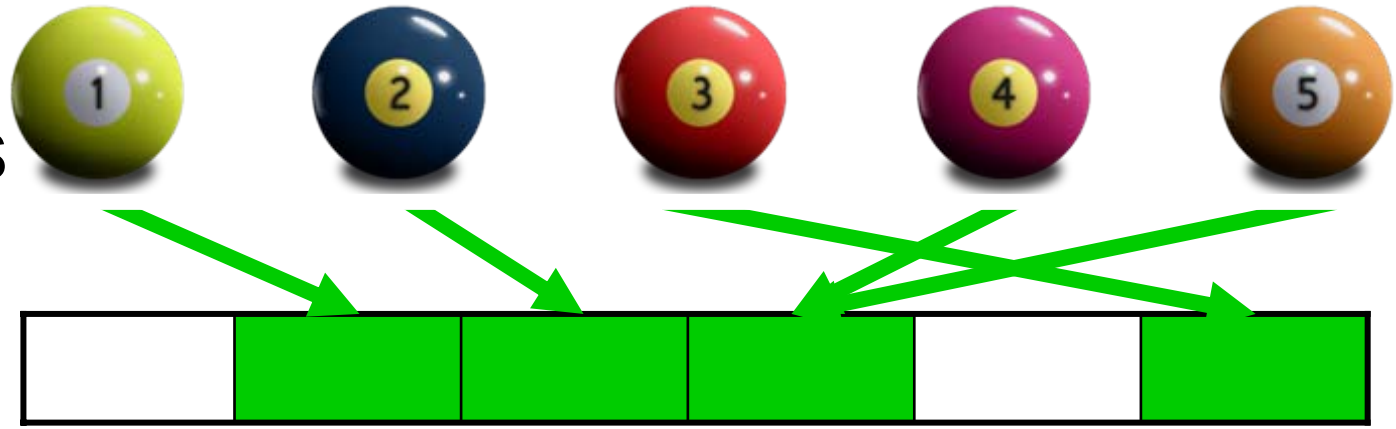
Things were easier with known tag IDs

Known Tag IDs



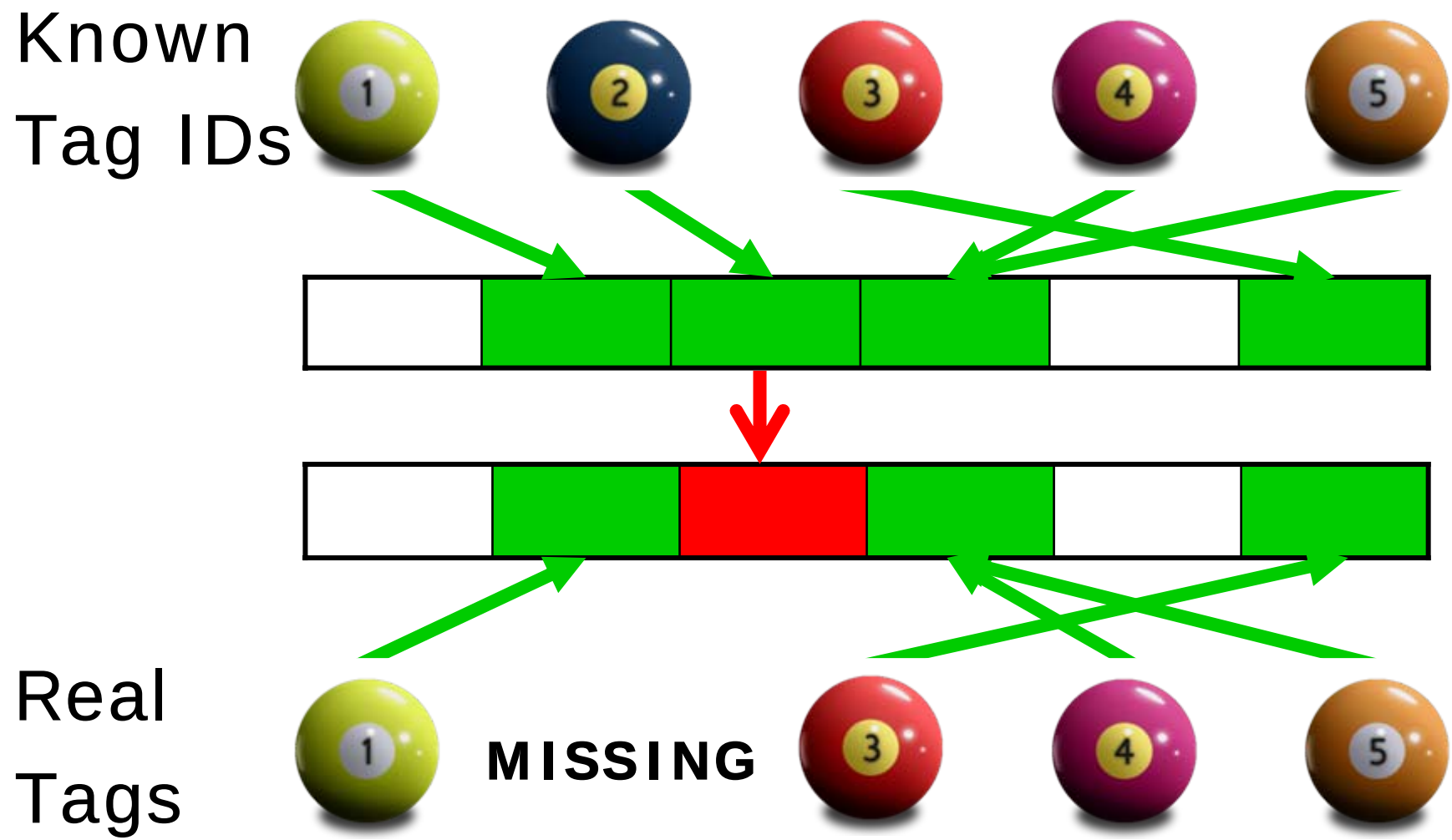
Things were easier with known tag IDs

Known Tag IDs

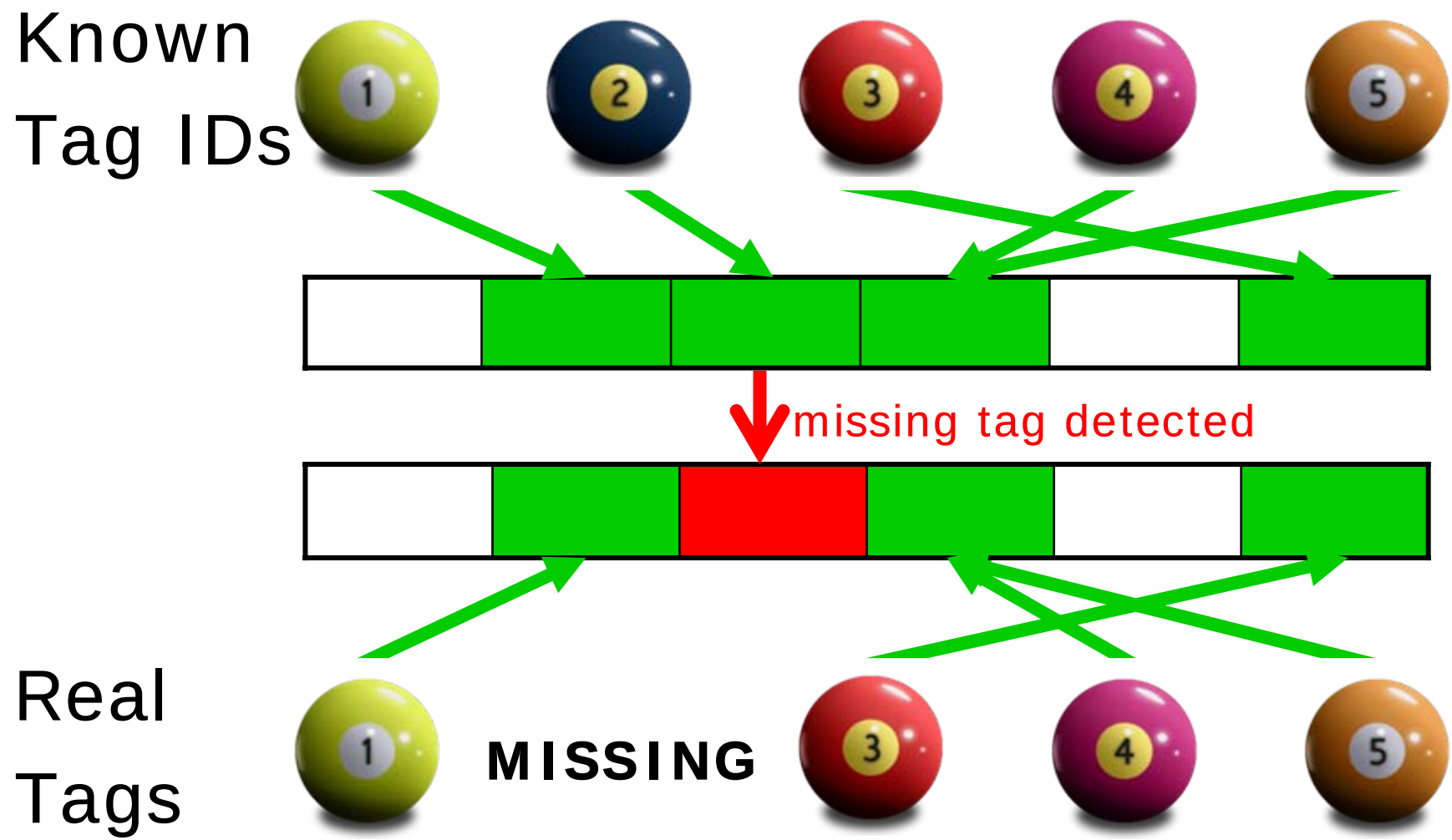


Real Tags

Things were easier with known tag IDs



Things were easier with known tag IDs



But more challenging without known tag IDs

Solution Goals

- Anonymity Preservation
- Deterministic Detection
- Fast Detection

Design Choices

- Anonymity Preservation

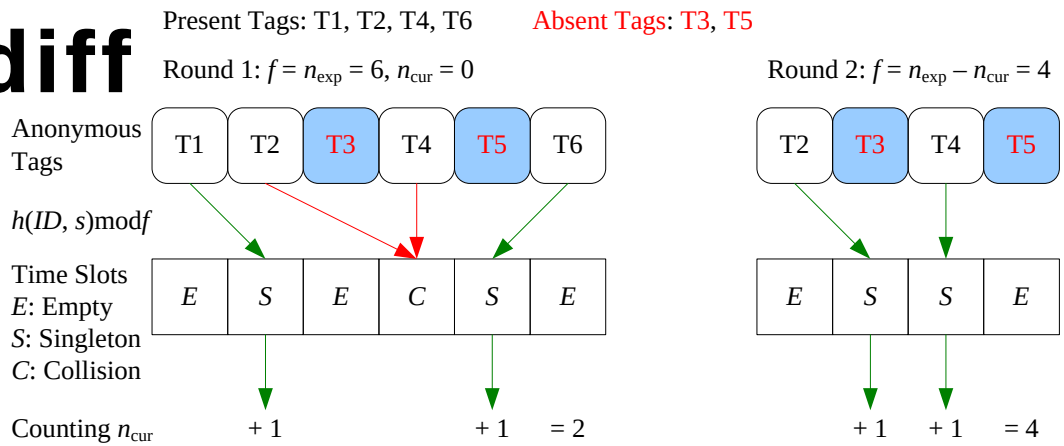
  isolate ID from protocol design
- Deterministic Detection

  verify tag absence via cardinality variation
- Fast Detection

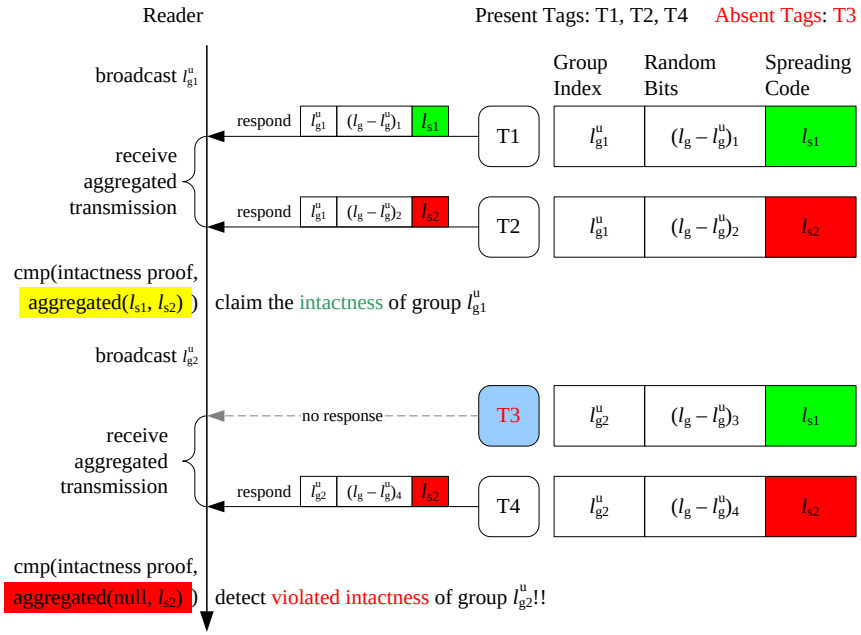
  adapt DSSS technique for scalable protocol design

Fast & Deterministic Protocols

Cardiff



Divar

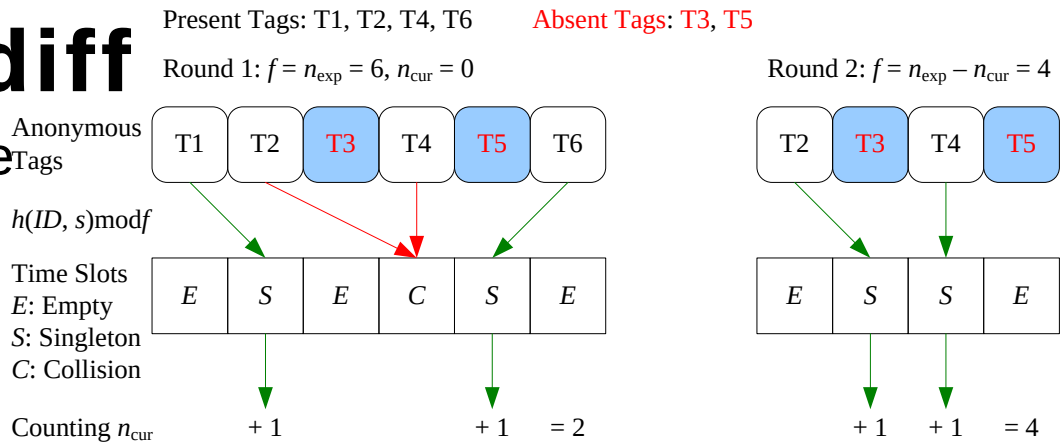


Anonymous Missing Tag Detection

Fast & Deterministic Protocols

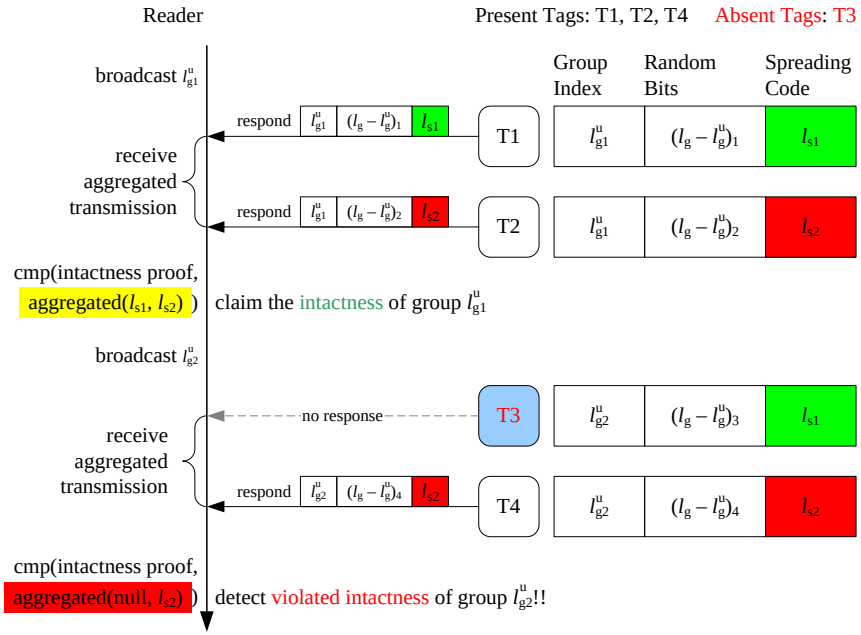
Cardiff

using cardinality difference



Divar

leveraging adapted DSSS

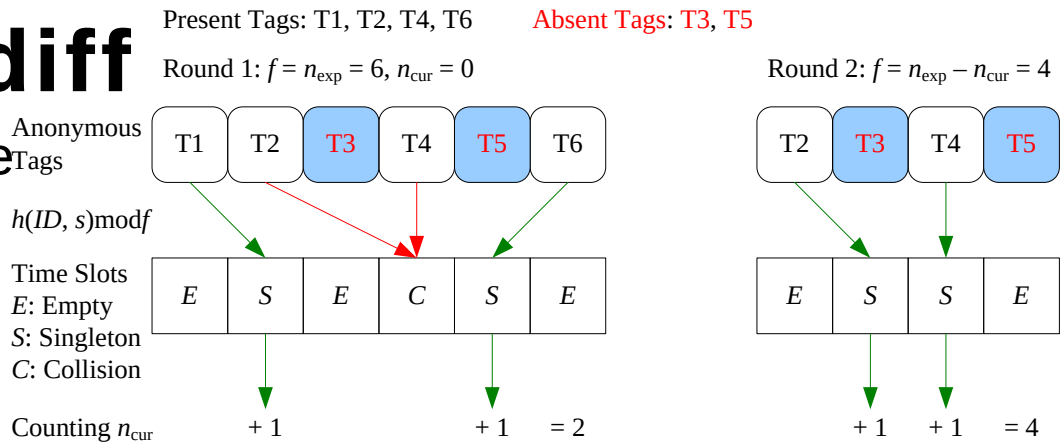


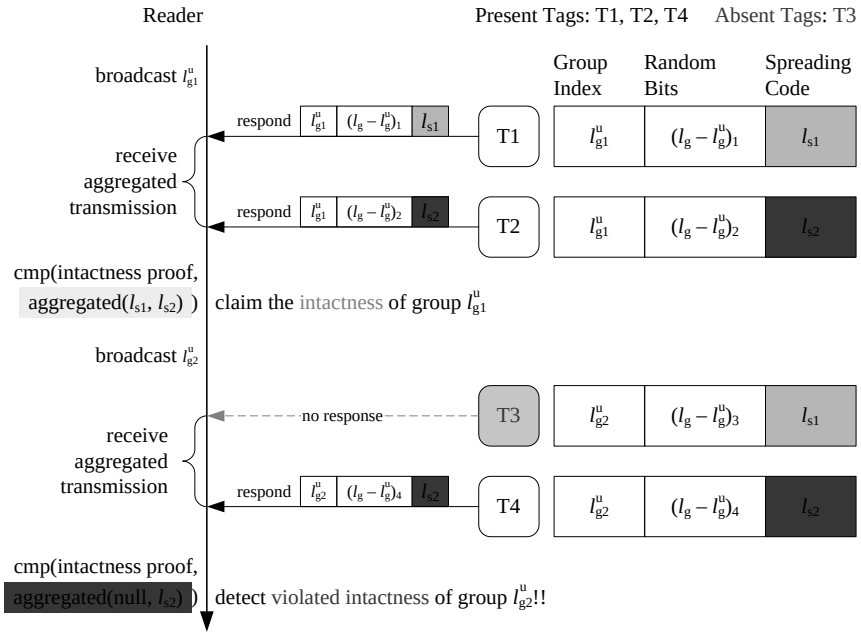
Anonymous Missing Tag Detection

Fast & Deterministic Protocols

Cardiff

using cardinality difference





Divar

leveraging adapted DSSS

Anonymous Missing Tag Detection

Cardiff

- Motivation

  missing tags make

  tag cardinality < ID cardinality

Cardiff

- Motivation

  missing tags make

  tag cardinality < ID cardinality

$N_{id} = 5$

Cardiff

- Motivation

  missing tags make

  tag cardinality < ID cardinality

$N_{tag} = 4 \longleftarrow N_{id} = 5$

cardinality difference

Cardiff

- Design

  Count tags using slotted Aloha;

  Require tag responses short yet sufficient for the reader detecting singleton and collision;

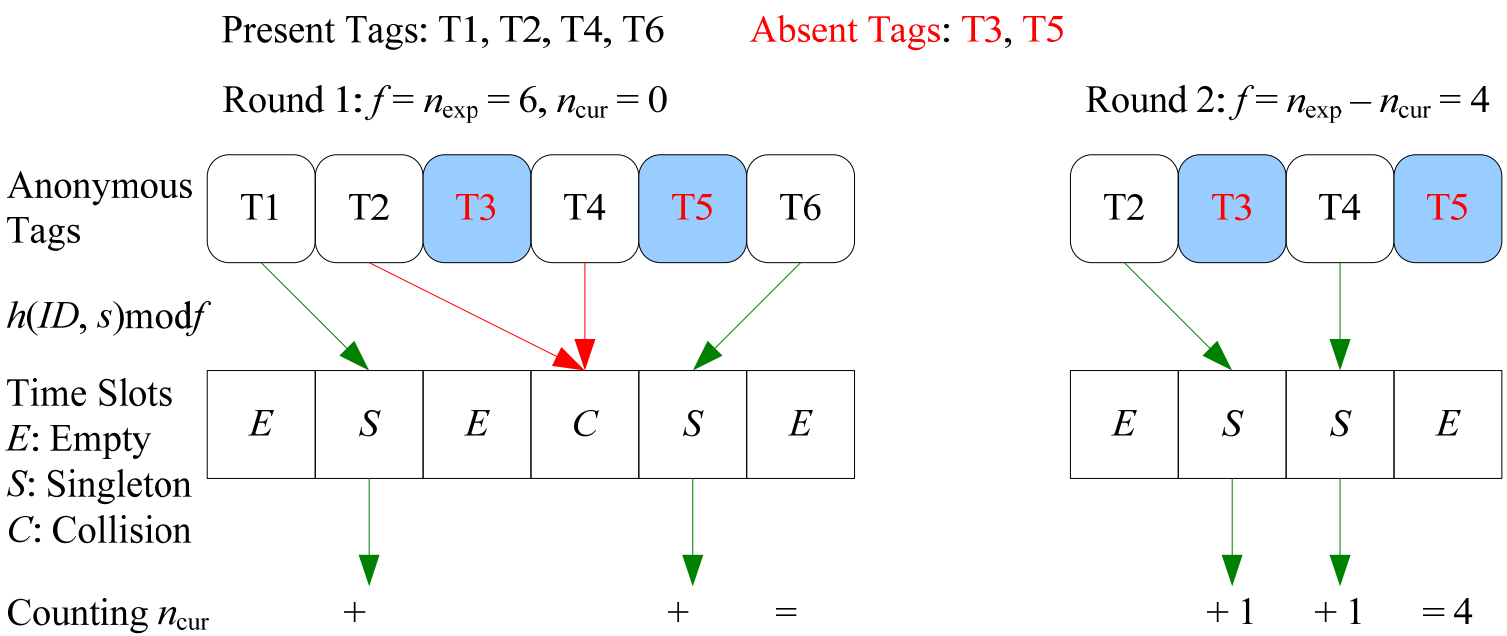
  Increase tag count by one upon singleton;

  Detect violated intactness if tag cardinality < ID cardinality.

Cardiff

- Example

  tag cardinality = 4 < ID cardinality = 6

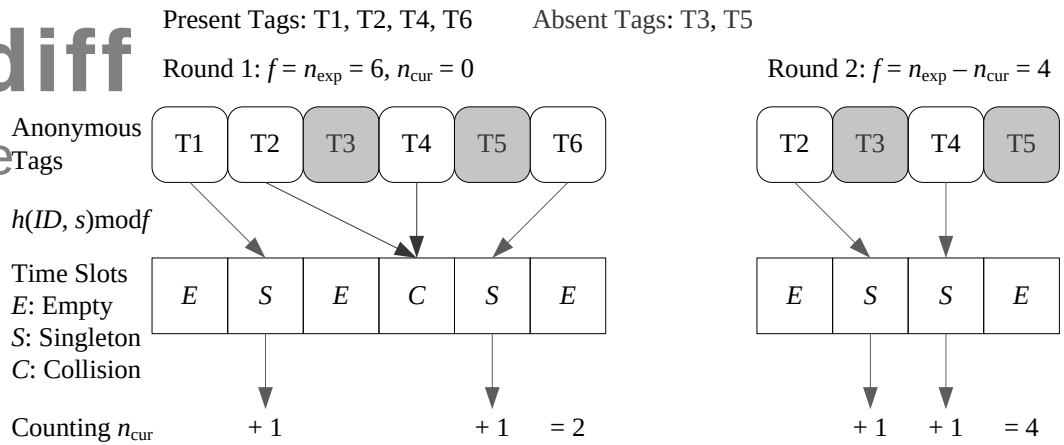


tags may respond times

Fast & Deterministic Protocols

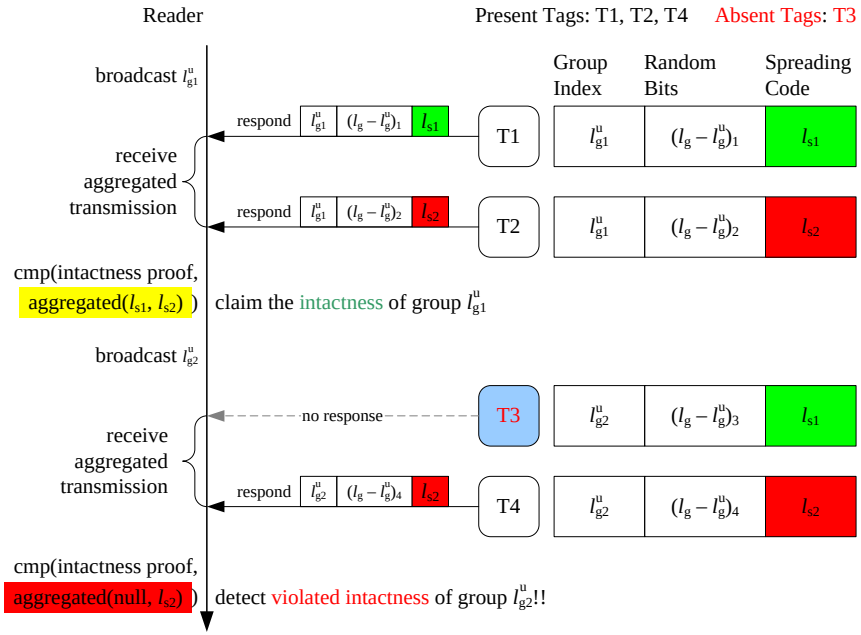
Cardiff

using cardinality difference



Divar

leveraging adapted DSSS



Anonymous Missing Tag Detection

Divar

- Motivation

  Direct-Sequence Spread Spectrum (**DSSS**) technique can extract each participant's transmission from aggregated signal;

  Recent advances implement DSSS-enabled RFID.

Divar

- Motivation
  DSSS-enabled RFID comm. example:

Tag	Spreading Code	0	1	0	1	1	1	0	0								
	Bipolar Notation	-1	1	-1	1	1	1	-1	-1								
	Binary Data	Bit 1								Bit 0							
	Encoded Data	0	1	0	1	1	1	0	0	1	0	1	0	0	0	1	1
	Modulated Transmission	-1	1	-1	1	1	1	-1	-1	1	-1	1	-1	-1	-1	1	1
Reader	Received Transmission	-1	1	-1	1	1	1	-1	-1	1	-1	1	-1	-1	-1	1	1
	Normalized Inner Product*	1								-1							
	Extracted Data	Bit 1								Bit 0							
	Bipolar Notation**	-1	1	-1	1	1	1	-1	-1								
	Spreading Code**	0	1	0	1	1	1	0	0								

*: Normalized inner product of received transmission and bipolar notation. Take the case of bit 1 for example,

$$\frac{(-1, 1, -1, 1, 1, 1, -1, -1) \cdot (-1, 1, -1, 1, 1, 1, -1, -1)}{8} = 1.$$

**: The reader shares the same spreading code (and its bipolar notation) with the tag.

L-bit spreading code supports at most l tags for simultaneous transmission.

Divar

- Design: *pre-load each tag l-bit string*

  Spreading code reuse

  $l = l_g + l_s$

  l_g-bit group index

  l_s-bit *reusable* spreading code

  support up to $2^{l_g} \times l_s$ *tags*

Divar

- Design

  Tag cardinality disguise

  $l_g = l_g^u + (l_g - l_g^u)$

  l_g^u-bit used group index

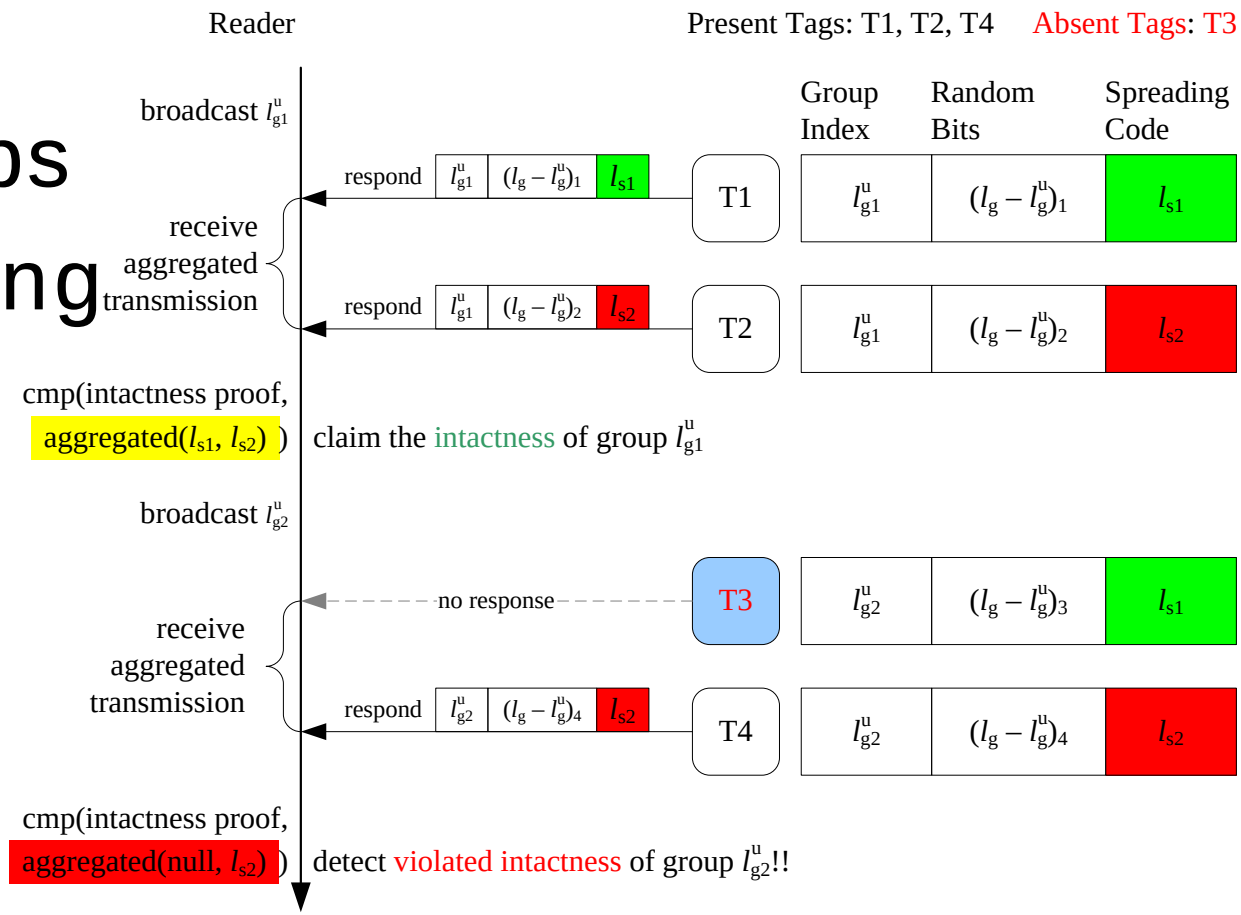
  support up to $2^{l_g^u} \times (l - l_g)$ *tags*

  eavesdropper's inferred tag cardinality:

  $$2^{l_g^u} \times (l - l_g^u)$$

Divar

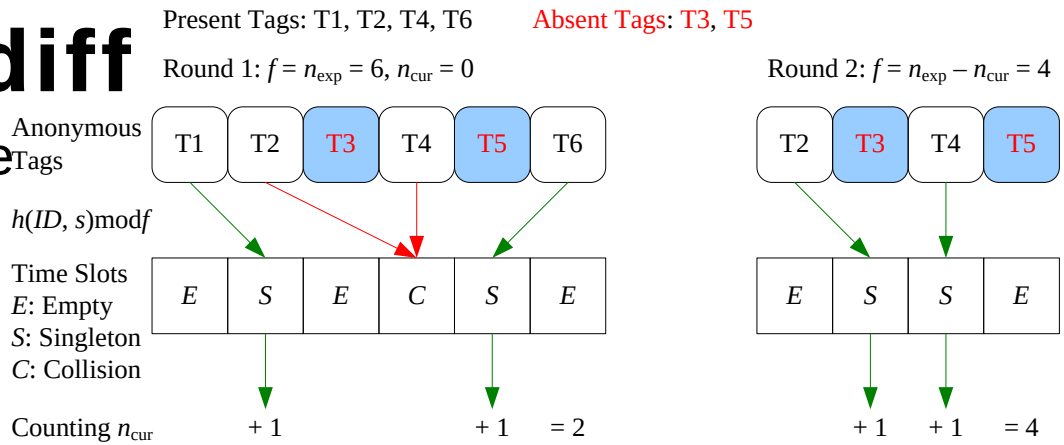
- Example
  four tags
  two groups
  one missing



Fast & Deterministic Protocols

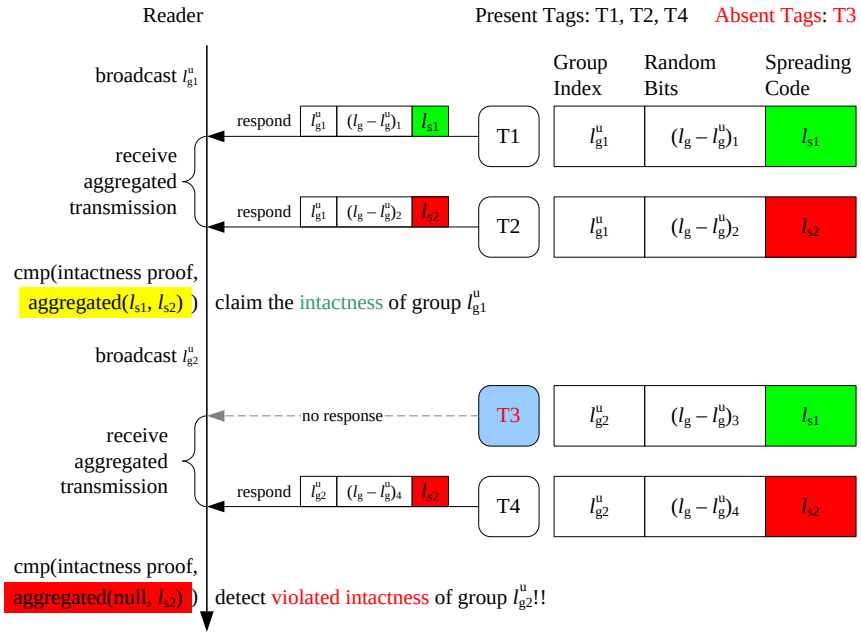
Cardiff

using cardinality difference



Divar

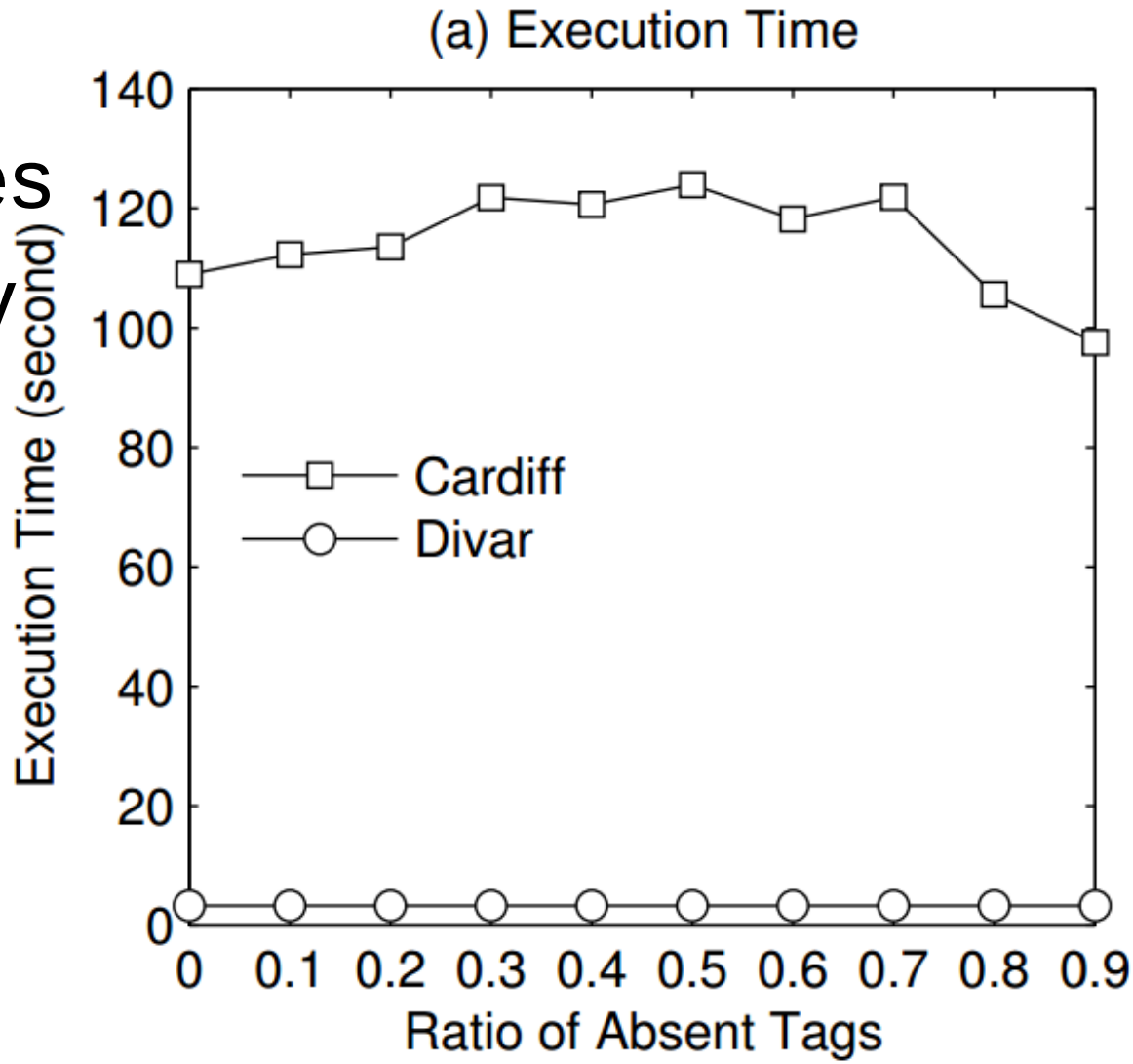
leveraging adapted DSSS



Anonymous Missing Tag Detection

Evaluation

50,000 tags;
Divar increases time efficiency over Cardiff by 96%



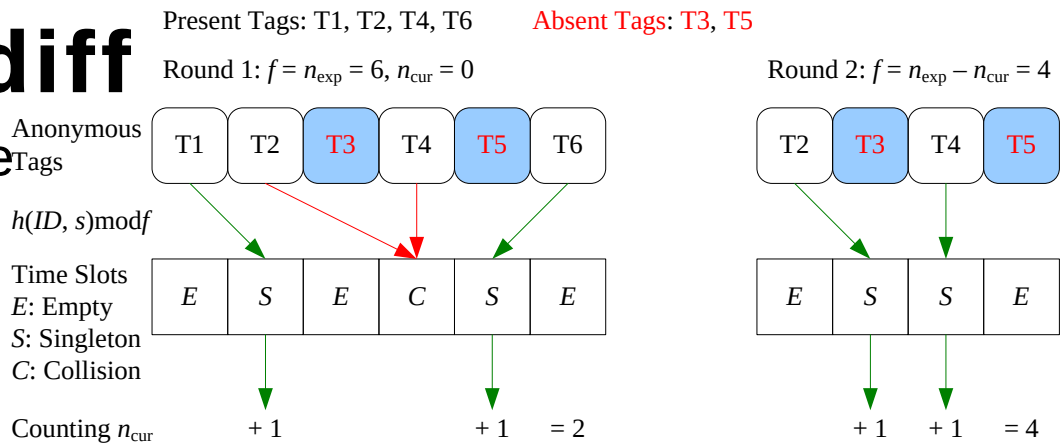
CONCLUSION

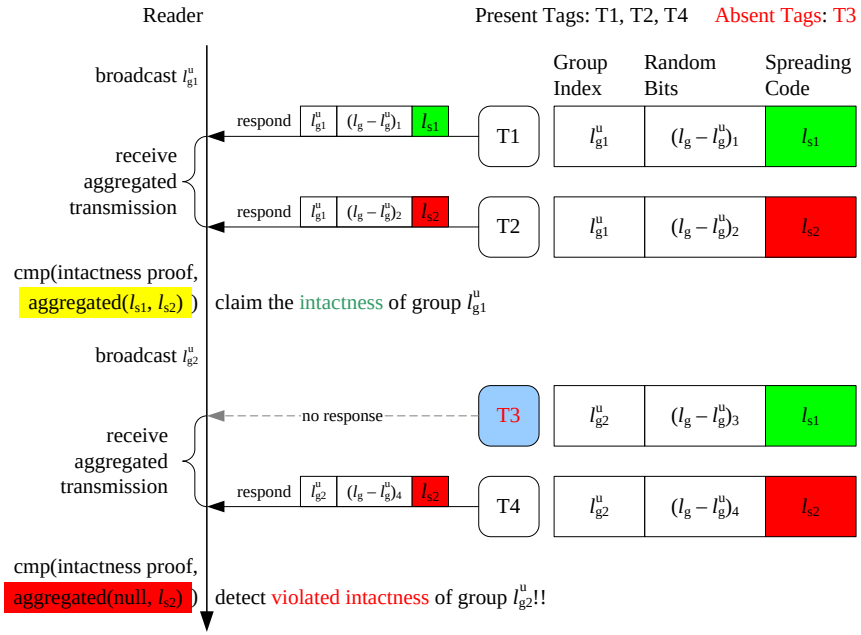
Fast & Deterministic Protocols

Cardiff

using cardinality difference

apply to off-the-shelf tags





Divar

leveraging adapted DSSS

apply to DSSS-enabled tags

faster than Cardiff

Thank You

kaibu@zju.edu.cn

Thank You

kaibu@zju.edu.cn