Top-k Queries for Multi-category RFID Systems

Xiulong Liu, Keqiu Li, Jie Wu, Alex X. Liu, et al.

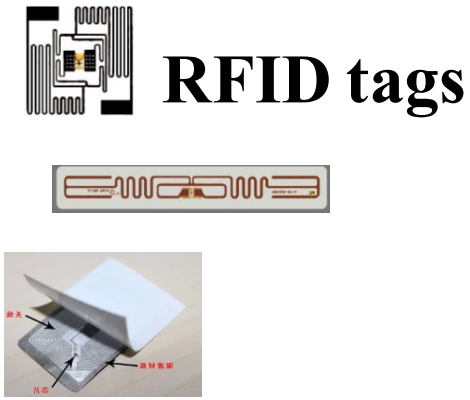
Speaker: **Xiulong Liu**
Dalian University of Technology
xiulongliudut@gmail.com

Outline

1. Background & Motivation
2. Problem Formulation
3. RFID Estimation scheme with Blocker tags (REB)
4. Theoretical Analysis
5. Performance Evaluation
6. Conclusion

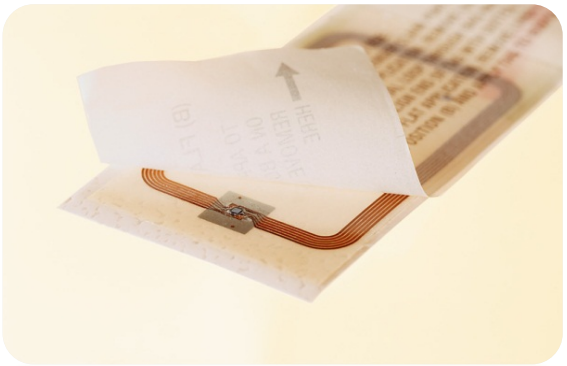
Background & Motivation

- Radio Frequency Identification.
- An identification system that consists of chip-based tags, readers and a back-end server.
- Each tag has a unique 96-bit ID to identify the tagged object.

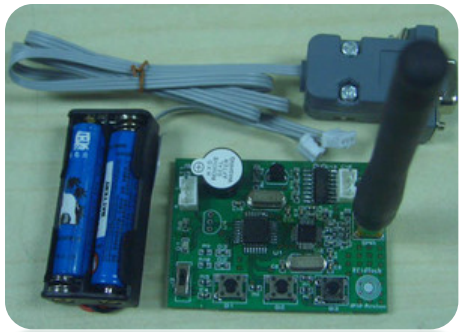


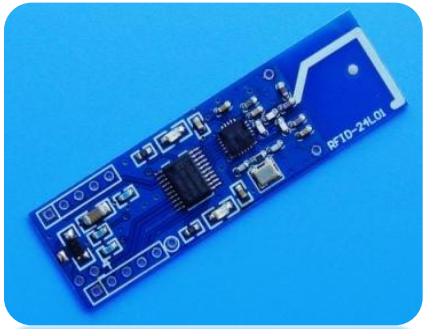
Background & Motivation

- Two types of RFID tags:
  - Passive tags and Active tags

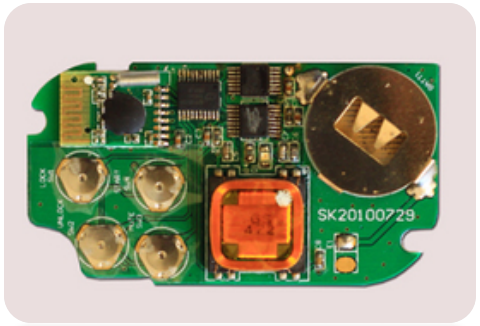


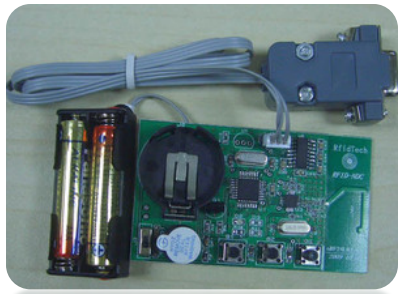
Passive tags



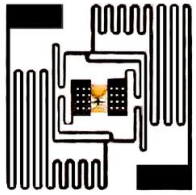


Active tags

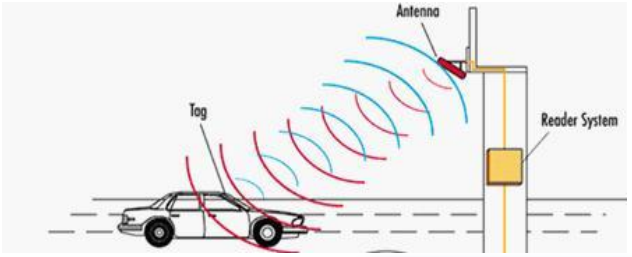




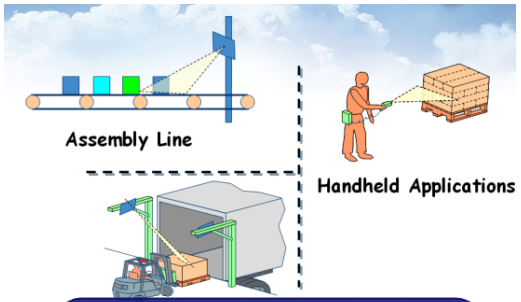
Background & Motivation

RFID  *vs.*  Bar-code

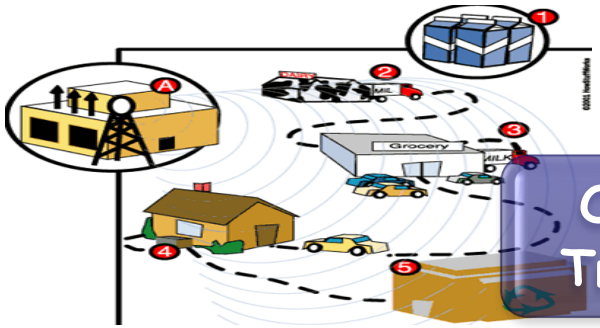
- Advantages of RFID over bar-code:
  - remote access
  - non-line-of-sight reading
  - multiple simultaneous accesses
  - large rewritable memory



Background & Motivation



Supply Chain Management

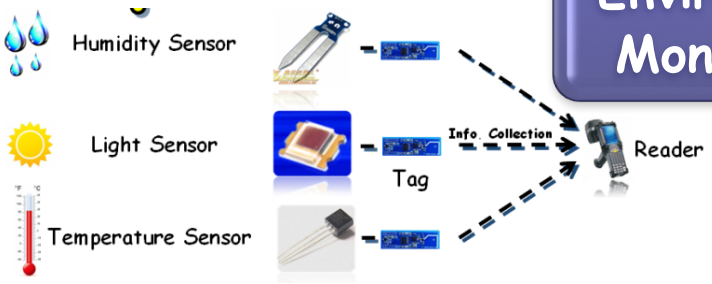


Object Tracking

Anti-Counterfeit

Environment Monitoring

Pets Management

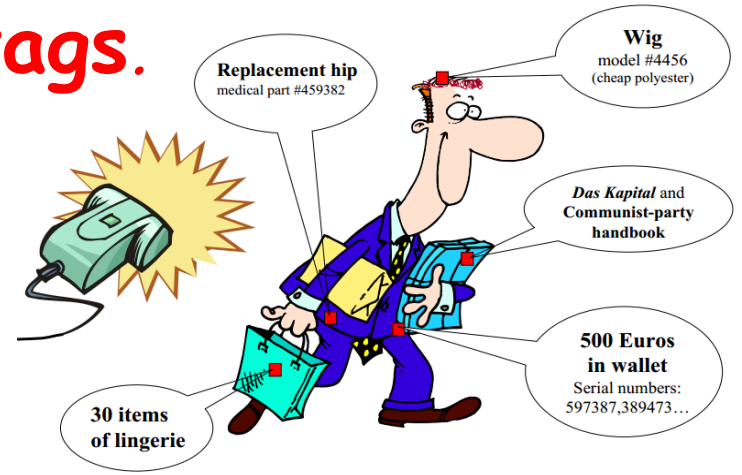


Privacy Concerns

- The widely used RFID tags impose serious **privacy concerns**.
- **Reason:** When C1G2 tags are interrogated by an RFID reader, **no matter the reader is authorized or not**, they blindly respond their IDs and other stored information (such as manufacturer, product type, and price) in a broadcast fashion.

Background & Motivation

- **What woman** wants her dress size to be publicly readable by any nearby scanner?
- **Who** wants the medications and other contents of a purse to be scannable?
- **Who** wants his or her location to be tracked and recorded based on the unique ID number in shoes or other clothing?
- An effective solution to this privacy issue is to use commercially available **blocker tags**.



What is the blocker tags?

- A blocker tag is an RFID device that is preconfigured with a set of known RFID tag IDs, which we call blocking IDs. The blocker tag behaves as if all tags with its blocking IDs are present.

How blocker tags protect the privacy?

Framed Slotted Aloha Protocol in C1G2-RFID Systems

Specify the blocking tag IDs on the Blocker tag device.

(1)

Manager

The blocker tag device behaves as if the tags with the blocking IDs are present.

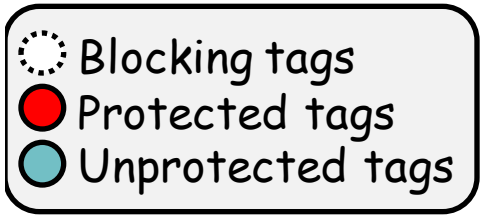
(2)

(3)

Blocking tags respond with RN16 as noise.

The response from a protected tag is always coupled with the simultaneous response from the blocking tag.

(4)

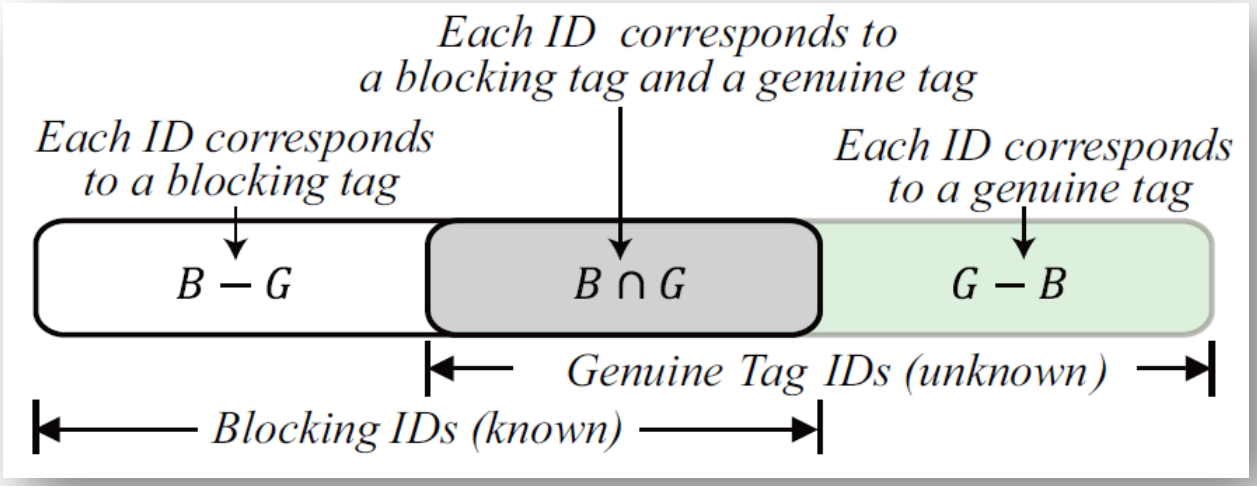


$H(ID,R)\%f$

Malicious Query

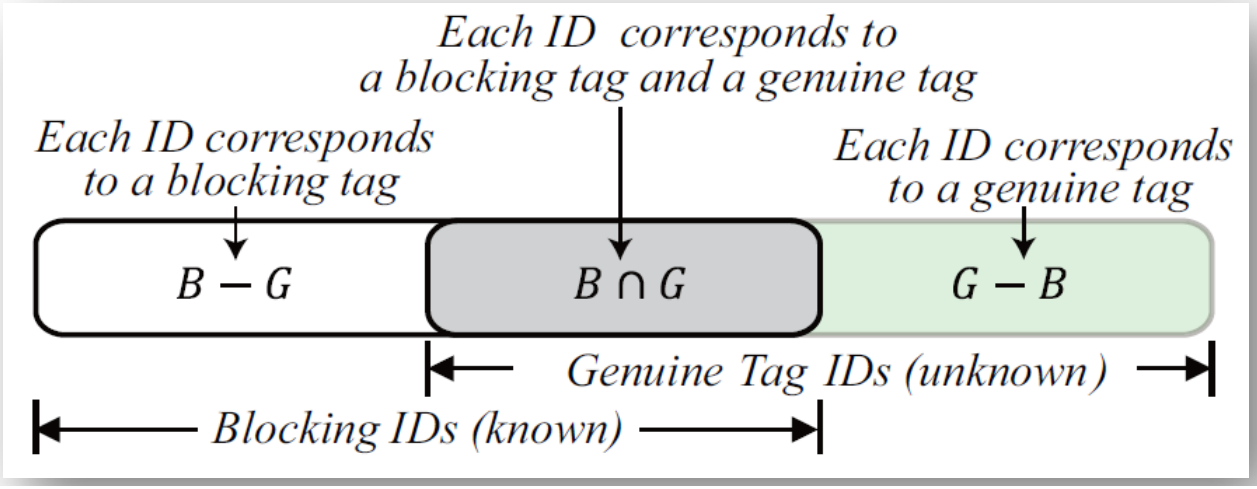
Revisit the Estimation Problem with Blocker Tags

- Consider an anonymous set of tags that may contain privacy-sensitive tags, e.g., pricey jewelries.
- To ensure the protection of all privacy-sensitive tags, we specify a relatively large Blocking tag set $\boldsymbol{B}$ that covers all the possible privacy-sensitive tag IDs, e.g., all the possible IDs of jewelry category.



Problem Formulation

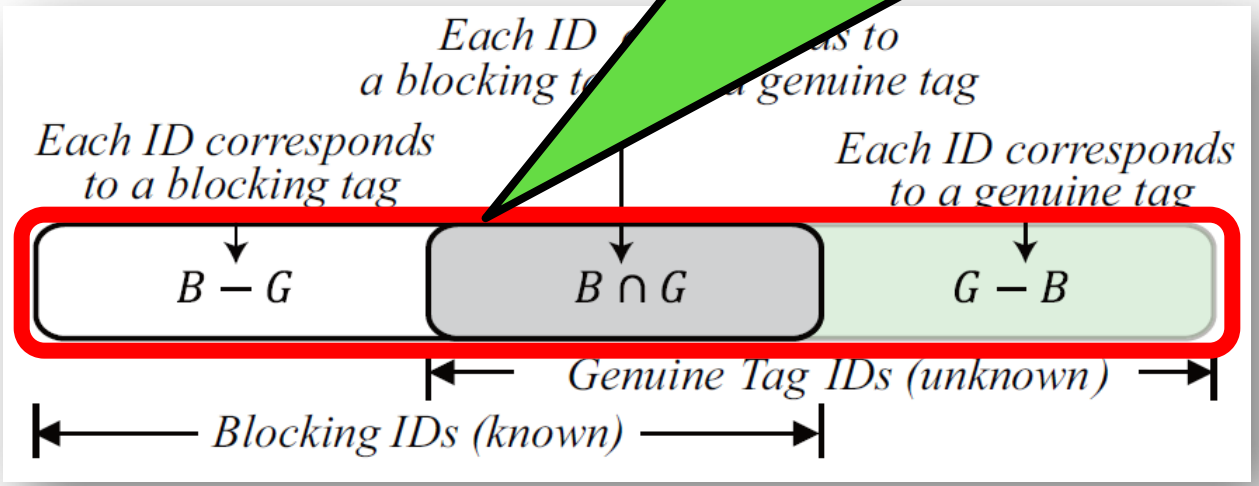
- We concern with the problem of **RFID (population size) estimation with the presence of blocker tags.**
- **Problem Definition:** given (1) a set of unknown genuine tags G of unknown size g, (2) a blocker tag with a set of known blocking IDs B, (3) a required confidence interval $\alpha \in (0,1]$, and a required reliability $\beta \in [0,1)$, we want to use one or more readers to estimate the number of genuine tags in G, denoted as $\hat{g}$, so that $P\{|\hat{g} - g| \leq g\alpha\} \geq \beta$



From Traditional Solution

The existing estimation protocols **can only estimate the tag population of the universal tag set $|B \cup G|$**, which is not what we want.

Tag Estimation:



Tag Identification:

The identification protocols **slow** to solve the tag estimation problem.

From Traditional Solution

- How about turning off the blocker tag and then using prior RFID estimation schemes to estimate the number of genuine tags?

- Not the best solution
  - a time window to breach privacy, especially for the scenarios that RFID estimation schemes are being continuously performed for monitoring purpose.

REB Protocol

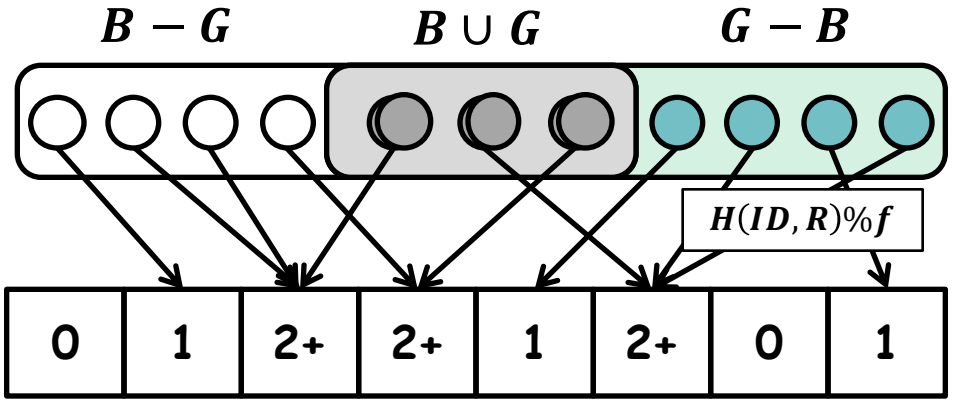
- **R**FID **E**stimation scheme with **B**locker tags
- The communication protocol used by REB is the standard *framed slotted Aloha protocol*.

REB Protocol

- Detailed Steps:
- **Step1:** the reader broadcasts a value f and a random number R to query all tags (including blocker tags), where f is the number of slots in the forthcoming frame. Then, each tag computes a hash $H(ID, R)\%f$ to select a slot to respond.

REB Protocol

- Detailed Steps:
- **Step1:** the reader broadcasts a value f and a random number R to query all tags (including blocker tags), where f is the number of slots in the forthcoming frame. Then, each tag computes a hash $H(ID,R)\%f$ to select a slot to respond.



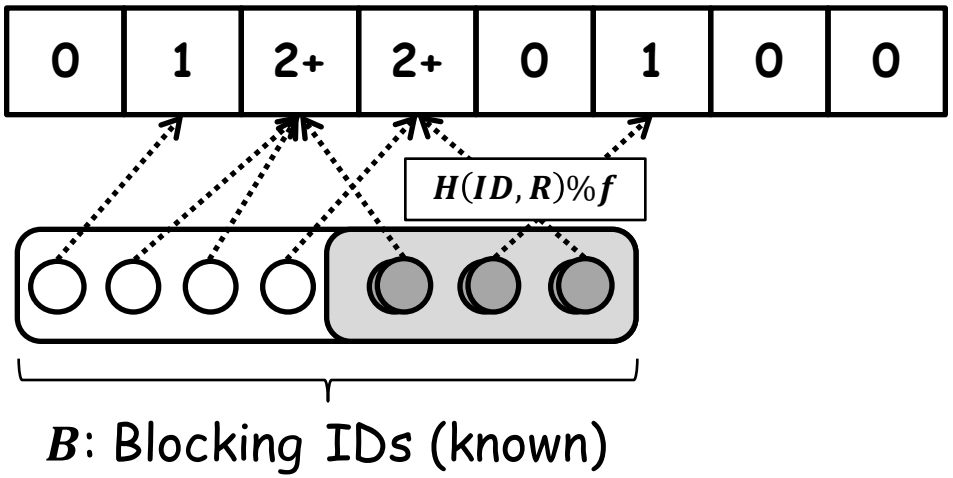
- 0: empty slot
- 1: singleton slot
- 2+ : collision slot

REB Protocol

- **Step2**: As we know the blocking IDs, we can virtually execute the framed slotted Aloha protocol using the same frame size f and random number R for the blocking IDs; thus, we get another vector.

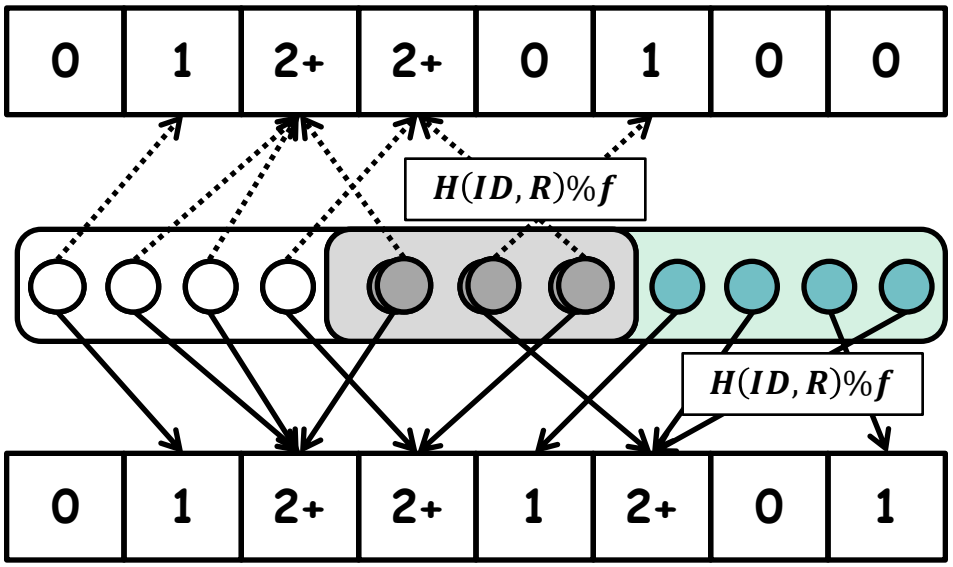
REB Protocol

- **Step2**: As we know the blocking IDs, we can virtually execute the framed slotted Aloha protocol using the same frame size f and random number R for the blocking IDs; thus, we get another vector.



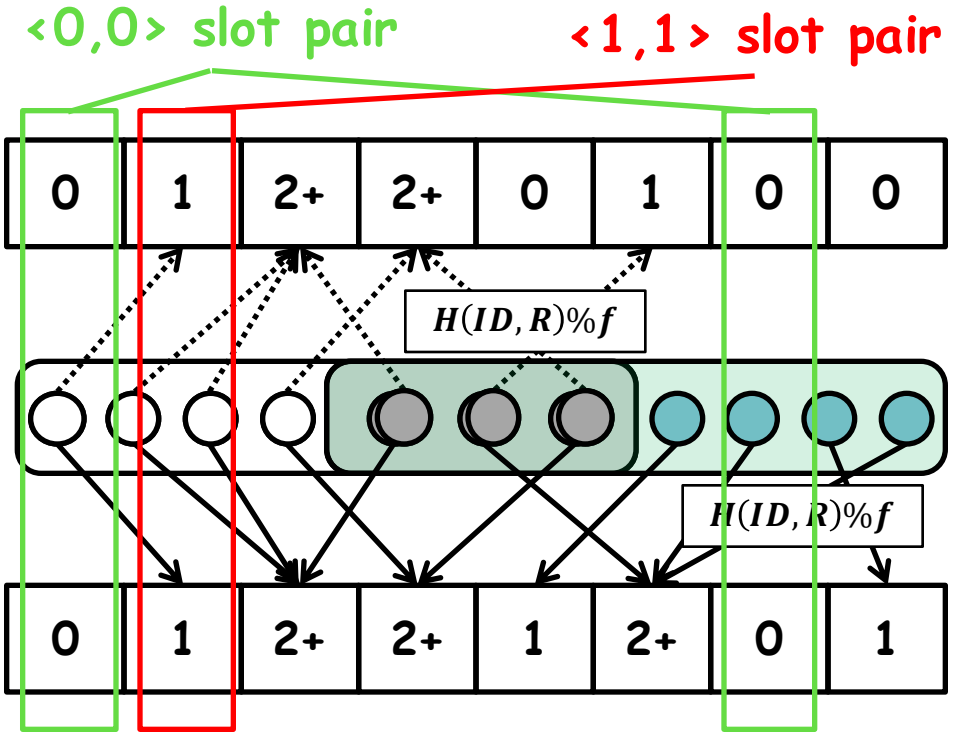
REB Protocol

- **Step3**: we count two numbers: N_{00}, which is the number of <0,0> slot pair, and N_{11}, which is the number of <1,1> slot pair.



REB Protocol

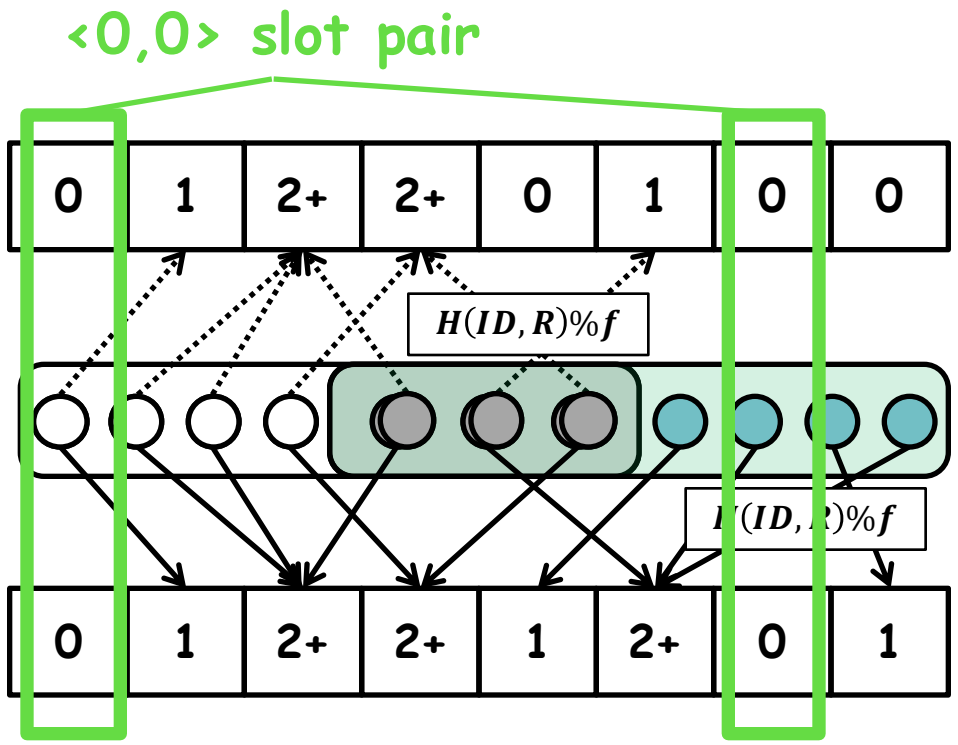
- **Step3**: we count two numbers: N_{00}, which is the number of <0,0> slot pair, and N_{11}, which is the number of <1,1> slot pair.

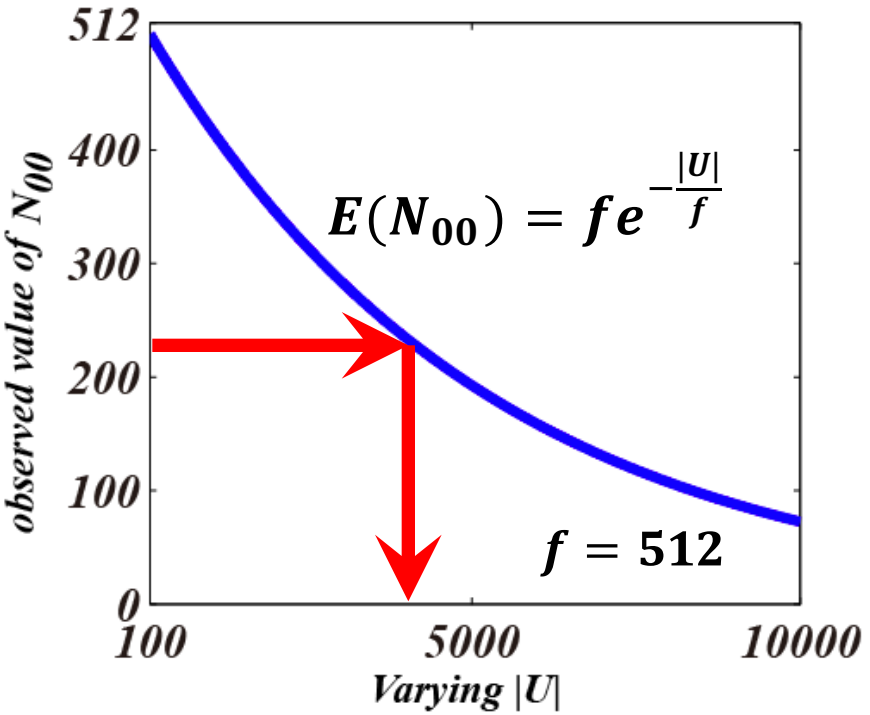


- $N_{00} = 2$
- $N_{11} = 1$

Key Insights

- 1. **Since <0,0> slot pair should not be selected by any tag in U, the observed N_{00} is closely related to $|U|$.**
- We propose a monotonous relationship between N_{00} and $|U|$: $E(N_{00}) = fe^{-\frac{|U|}{f}}$.





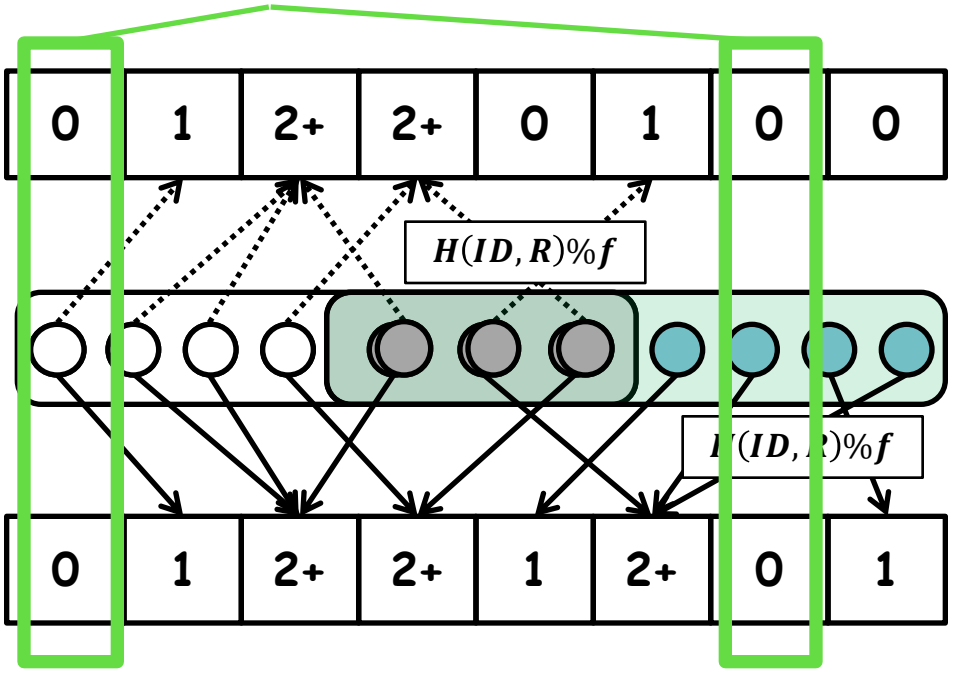
Key Insights

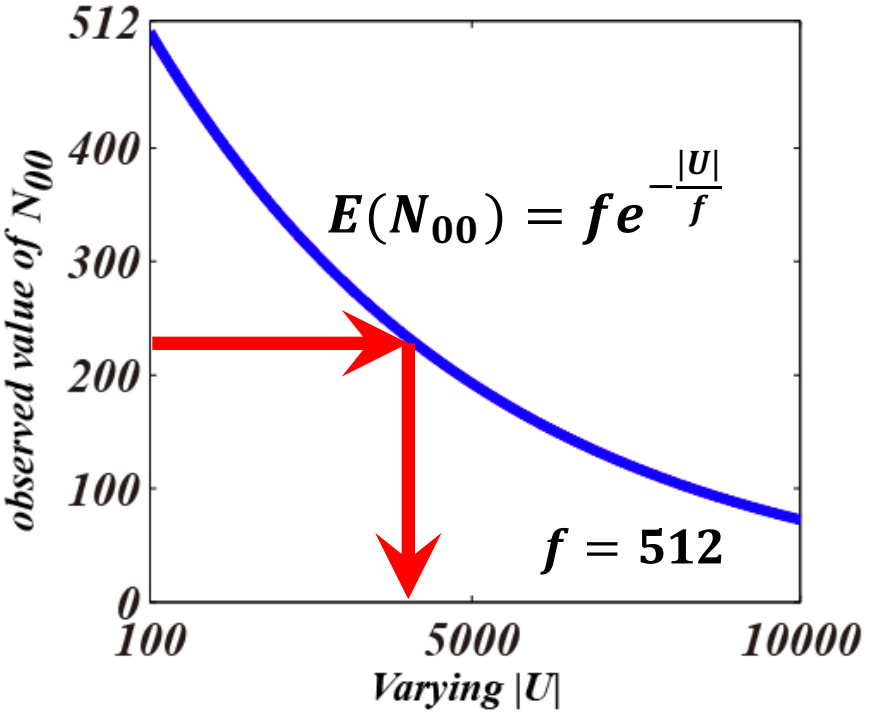
- 1. **Since <0,0> slot pair should not be selected by any tag in U, the observed N_{00} is closely related to $|U|$.**
- We propose a monotonous relationship between N_{00} and $|U|$: $E(N_{00}) = fe^{-\frac{|U|}{f}}$

close to actual val. **11**

- $N_{00} = 2 \rightarrow \widehat{|U|} = -f \ln\left(\frac{N_{00}}{f}\right) = -8 * \ln\left(\frac{2}{8}\right) = 11.0904$

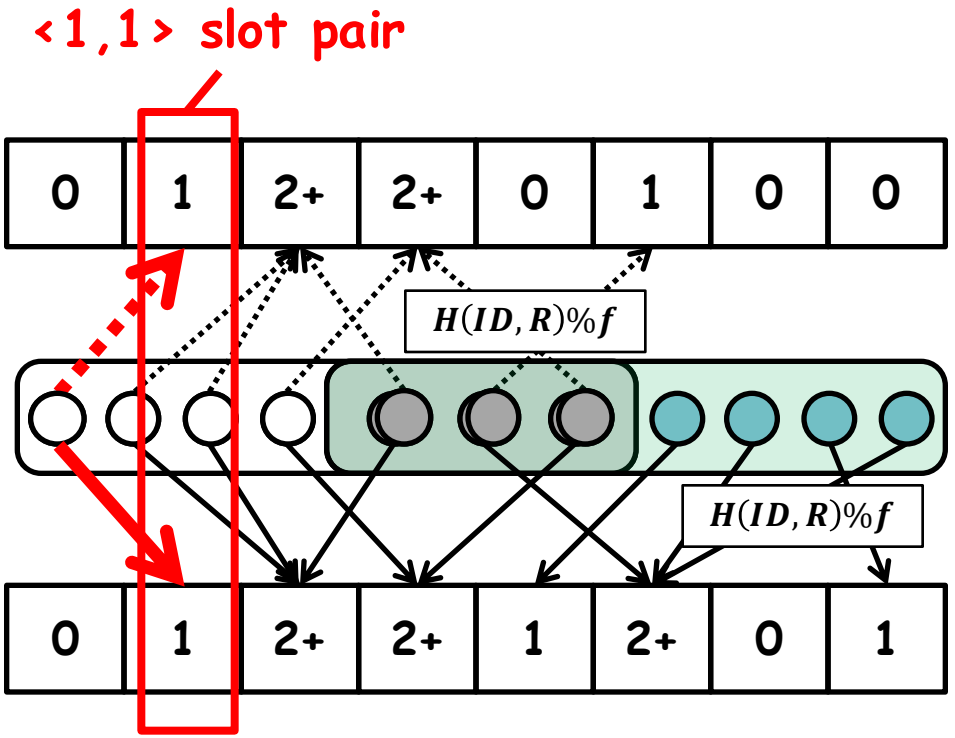
<0,0> slot pair

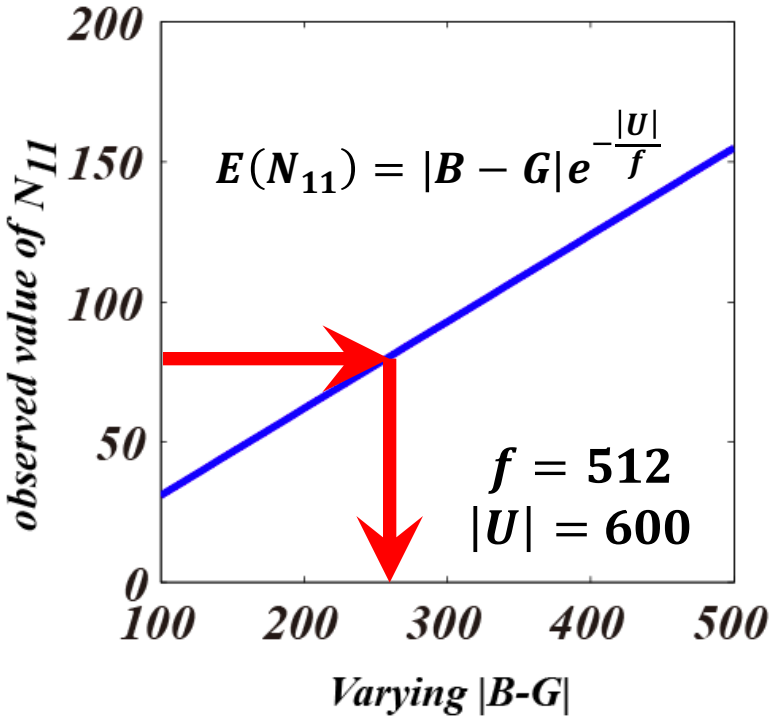




Key Insights

- 2. **Since <1,1> slot pair is contributed by only tags in $B-G$, N_{11} is closely related to $|B-G|$.**
- We propose a monotonous relationship between N_{11} and $|B-G|$: $E(N_{11}) = |B-G|e^{-\frac{|U|}{f}}$.



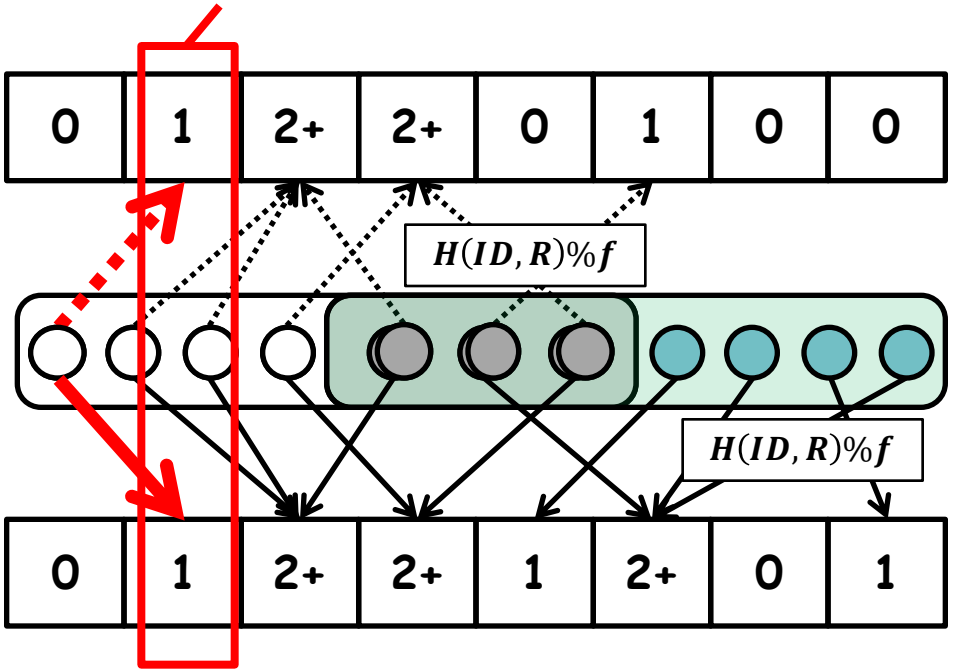


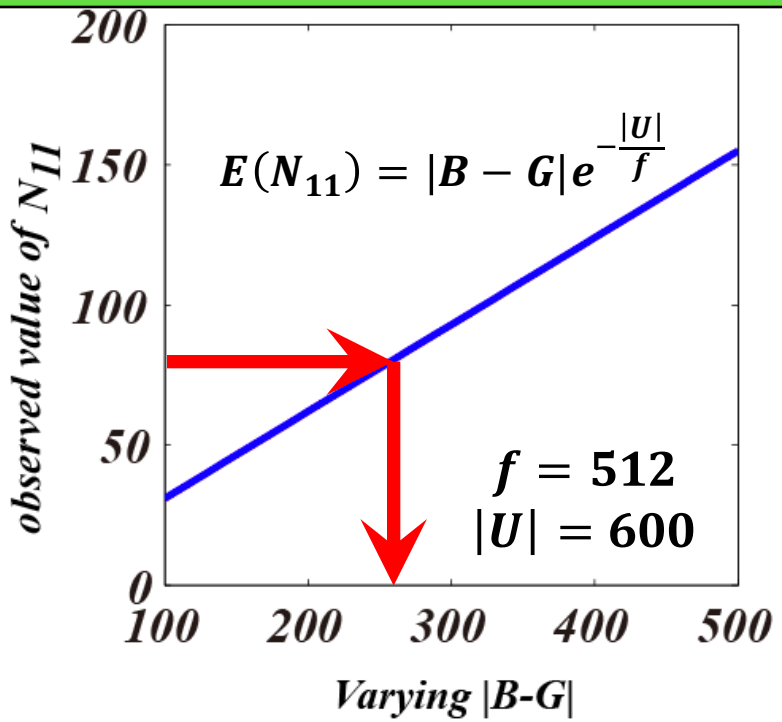
Key Insights

- 2. **Since <1,1> slot pair is contributed by only tags in $B-G$, N_{11} is closely related to $|B-G|$.**
- We propose a monotonous relationship between N_{11} and $|B-G|$: $E(N_{11}) = |B-G|e^{-\frac{|U|}{f}}$.

$$N_{11} = 1 \rightarrow \widehat{|B-G|} = N_{11}e^{\frac{|U|}{f}} = 1 * e^{\frac{11.0904}{8}} = 4$$

<1,1> slot pair



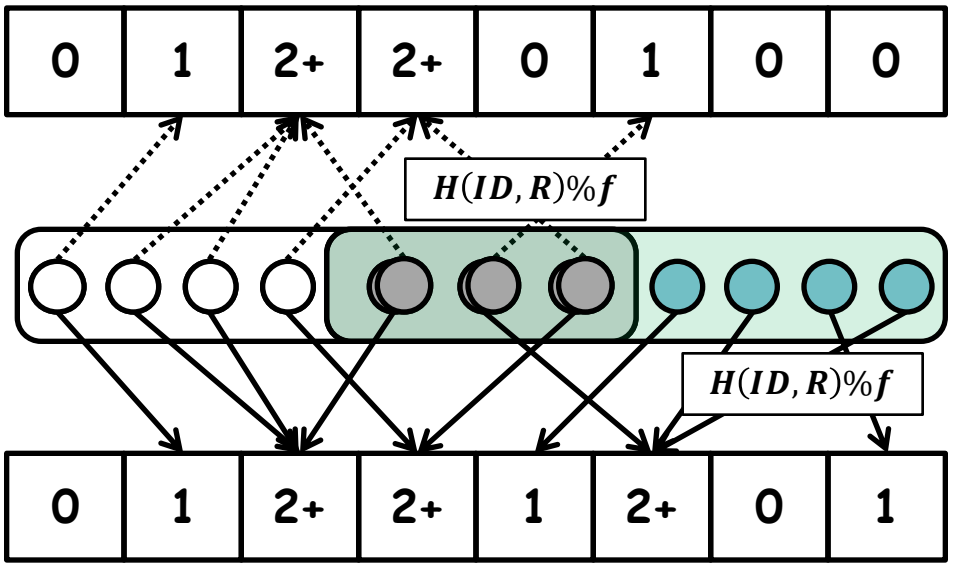


Key Insights

$$N_{00} = 2 \rightarrow \widehat{|U|} = -f \ln\left(\frac{N_{00}}{f}\right) = -8 * \ln\left(\frac{2}{8}\right) = 11.0904$$

$$N_{11} = 1 \rightarrow \widehat{|B-G|} = N_{11} e^{\frac{|U|}{f}} = 1 * e^{\frac{11.0904}{8}} = 4$$

$$\widehat{|G|} = \widehat{|U|} - \widehat{|B-G|} = 11.0904 - 4 = 7.0904 \text{ (actual val. is 7)}$$



Scale to large tag population

- To scale to a large tag population, the reader uses a persistence probability $p \in (0, 1]$ to virtually extends the frame size f to f/p, but actually terminates the frame after the first f slots.
- **Each tag participate in the frame with a probability p.**

Theoretical Analysis

- **Functional Estimator:**
- $\hat{g} = -\frac{f}{p}\ln\left(\frac{N_{00}}{f}\right) - \frac{fN_{11}}{pN_{00}}$, where f is the observed frame size, p is the persistence probability, N_{00} is the number of persistent empty slots, N_{11} is the number of persistent singleton slots.

Theoretical Analysis

- **Variance of the Estimator:**
- $\boldsymbol{Var(\hat{g}) = \frac{1}{fp^2} e^{\frac{up}{f}} \left(b'^2 p^2 + f^2 - b' fp\right) - \frac{f}{p^2}}$, where f is the observed frame size, p is the persistence probability, $u = |B \cup G|$, and $b' = |B - G|$.

Theoretical Analysis

- **How many frame are required?**
- If the frame number k satisfies: $k \geq$

$$\frac{Z_\beta}{g\alpha}\sqrt{\sum_{j\in[1,k]}\left[\frac{1}{f_j p_j^2}e^{\frac{up_j}{f_j}}\left(b'^2p_j^2+f_j^2-b'f_jp_j\right)-\frac{f_j}{p_j^2}\right]},$$

where f_j and p_j are the frame size and persistence probability used in the j-th frame.

Performance Evaluation

- 1. Verifying the Optimized f and p.

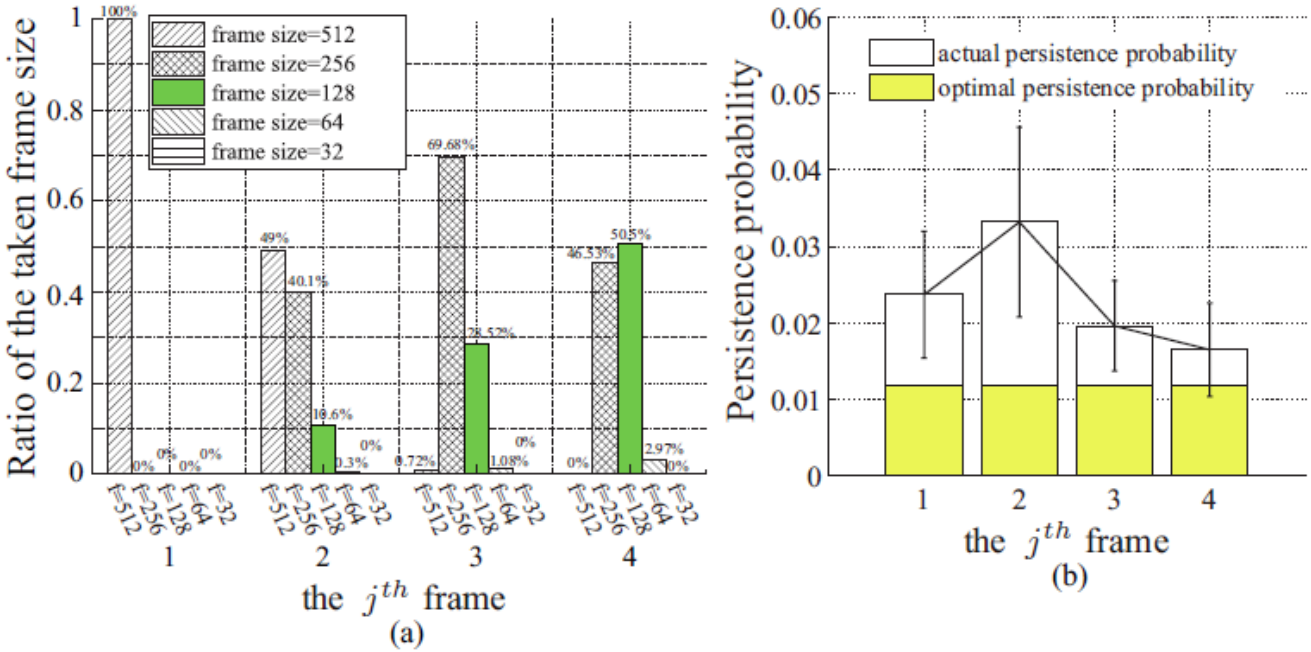


Fig. 3. Verifying the optimized settings of f and p. $|B - G| = 5000$, $|B \cap G| = 5000$, $|G - B| = 5000$. $\alpha = 10\%$, $\beta = 90\%$. (a) Verifying the optimized f. (b) Verifying the optimized p.

The values of f and p approach their overall optimal values after a few frames.

Performance Evaluation

- 2. Estimation Reliability.

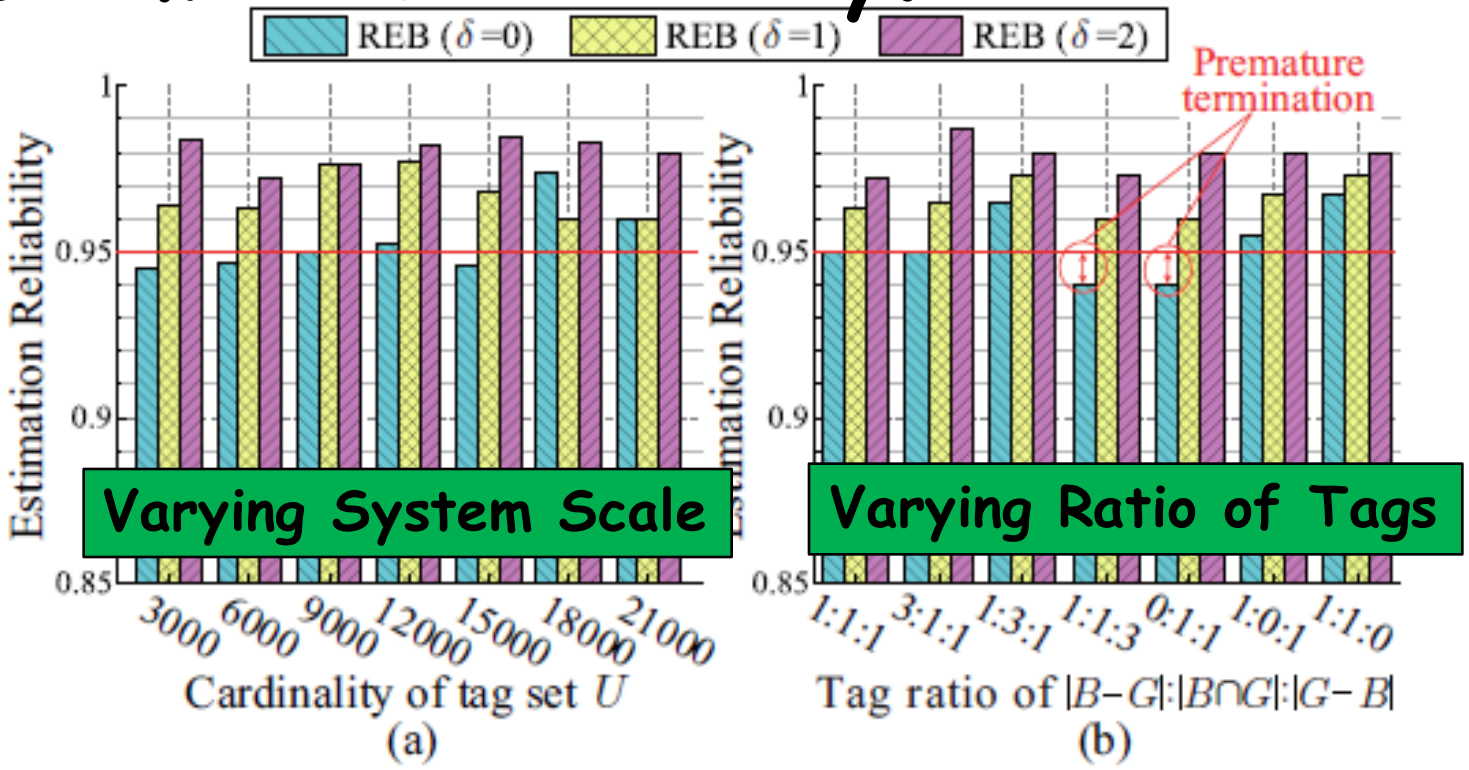
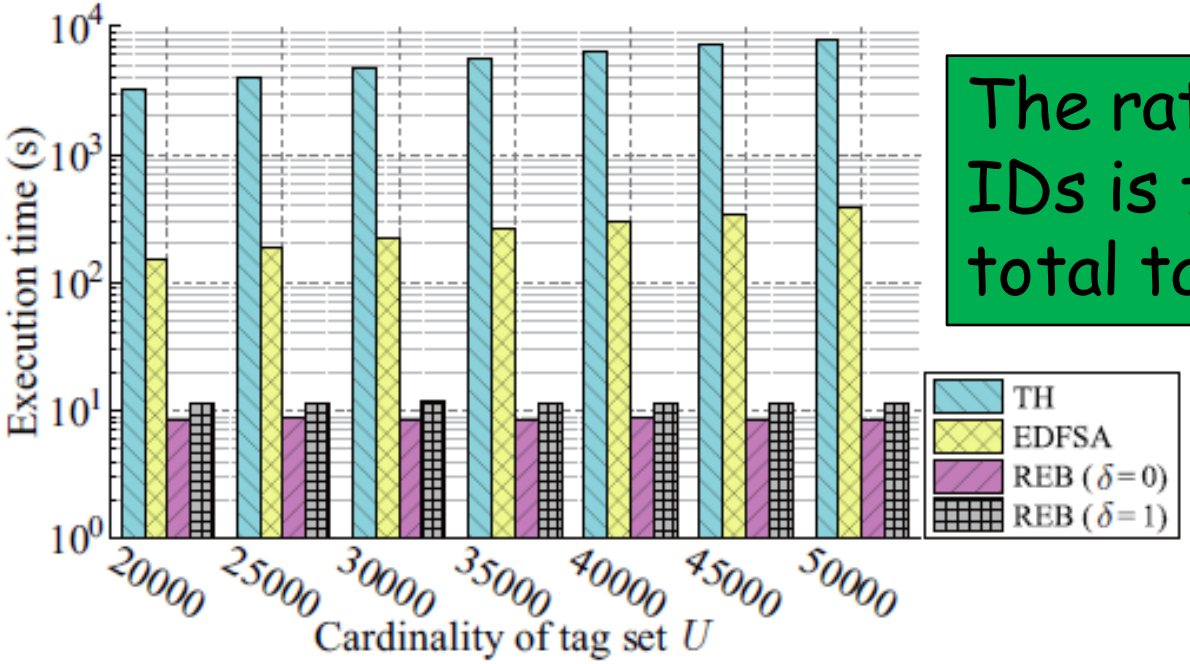


Fig. 4. Evaluating the reliability of REB. $\alpha = 5\%$, $\beta = 95\%$. (a) Tag ratio $|B - G|:|B \cap G|:|G - B|$ is fixed to $1 : 1 : 1$, and u varies from 3000 to 21000. (b) u is fixed to 9000, and tag ratio varies.

Our REB ($\delta = 1$) can meet the required accuracy under different simulation settings

Performance Evaluation

- 3. Time Efficiency: Impact of $|U|$



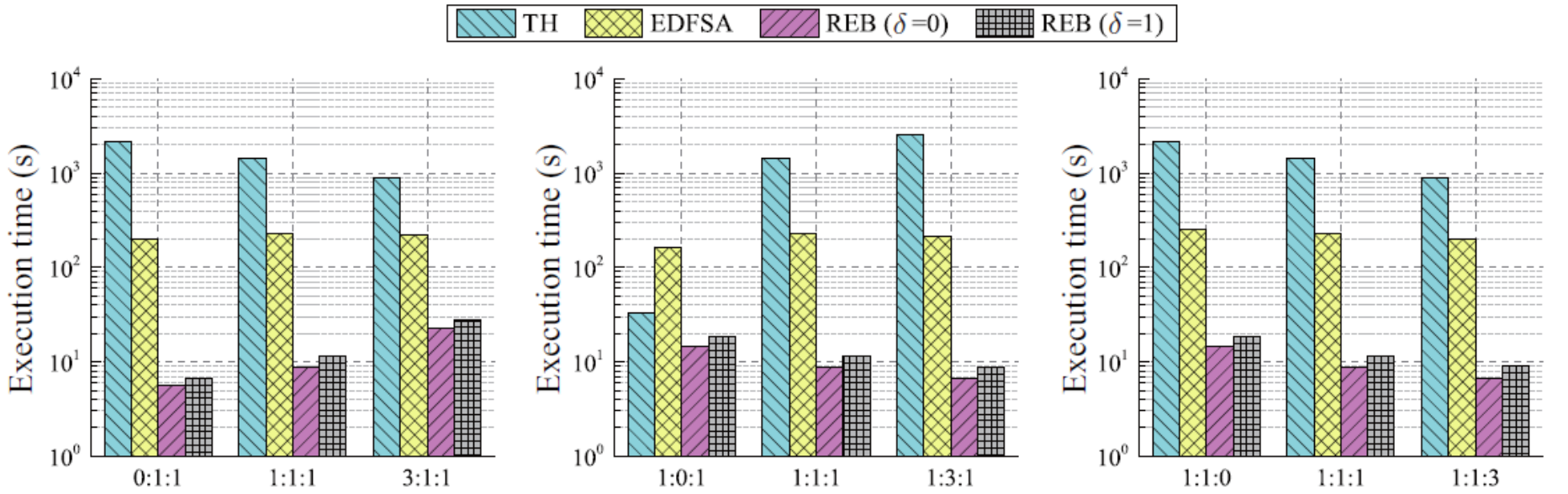
The ratio of three types of IDs is fixed to 1:1:1. The total tag number $|U|$ varies.

Fig. 5. Evaluating the time-efficiency of protocols with varying u. Tag ratio of $|B - G|:|B \cap G|:|G - B|$ is fixed to $1 : 1 : 1$ and $\alpha = 5\%$, $\beta = 95\%$.

When $|U|$=50000, our REB runs 33x faster than the fastest tag identification protocol.

Performance Evaluation

- 4. Time Efficiency: Impact of Tag Ratio



Varying the ratio of $|B - G|$

Varying the ratio of $|B \cap G|$

Varying the ratio of $|G - B|$

Our REB persistently runs tens of times faster than the existing protocols.

Conclusion

- We take the first step to address the problem of RFID estimation with Blocker tags.
- The propose REB protocol is compliant with the commodity EPC C1G2 standard and does not require any modifications to off the-shelf RFID tags.
- REB can guarantee any degree of estimation accuracy specified by the users.
- Extensive simulation results reveal that REB is tens of times faster than the fastest identification protocol with the same accuracy requirement.

Thanks for your attention!

Q & A