南京大學
NANJING UNIVERSITY

Eingerprint: Robust Energy-related Fingerprinting for Passive RFID Tags

Xingyu Chen*, Jia Liu*, Xia Wang, Haisong Liu,
Dong Jiang, Lijun Chen

Motivation

Anti-counterfeiting

Passport

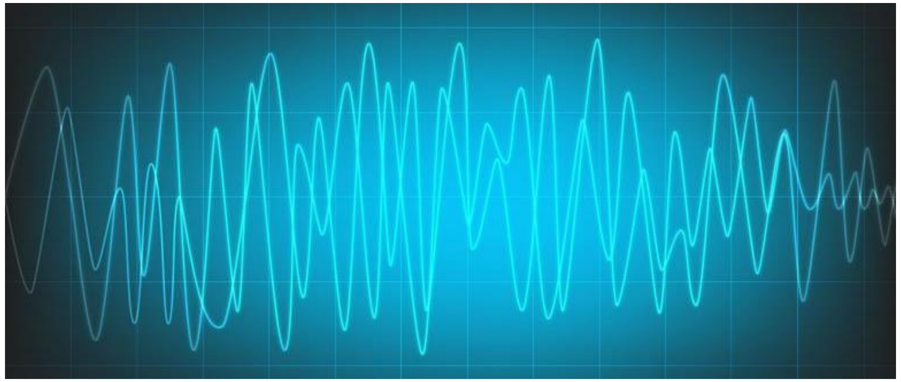
Infant security

RFID authentication is becoming increasingly important

Existing Work

Cryptographic methods

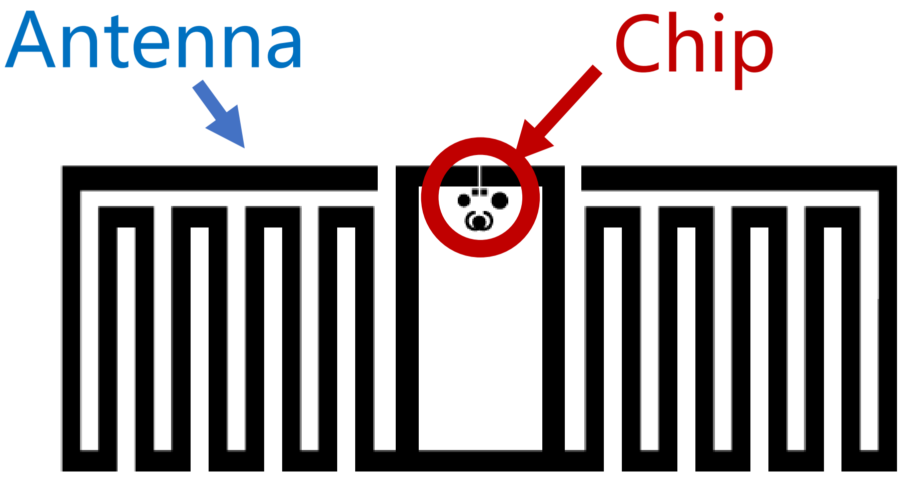
- ➢ Increase the cost of the passive tag
- ➢ Reduce the communication range



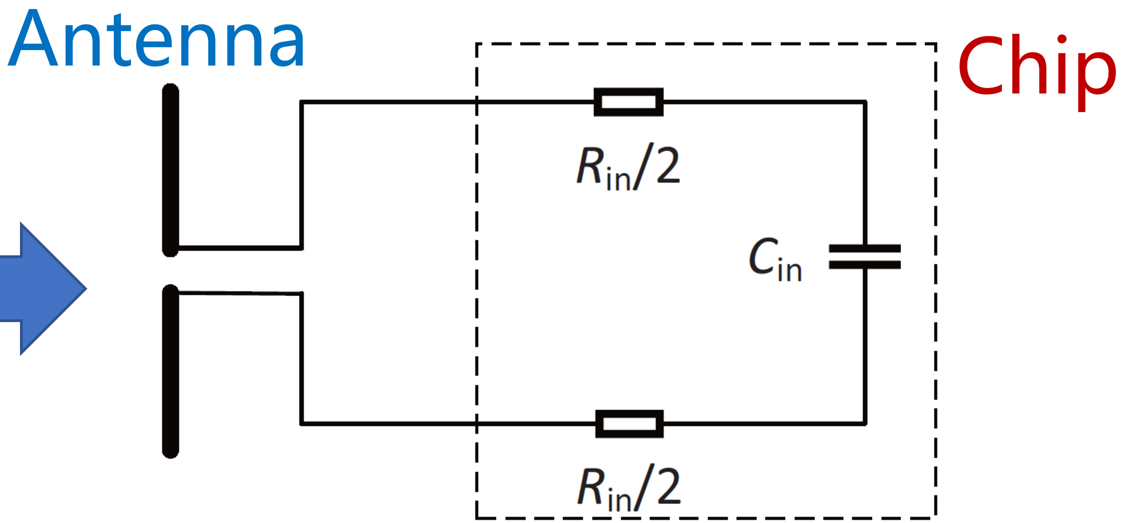
Physical-layer Identification

- ➢ Require a purpose-built device
- ➢ Sensitive to environmental conditions (Phase)

Our Solution: Energy-related Fingerprint



RFID tag



Equivalent resistor-capacitor (RC) circuit

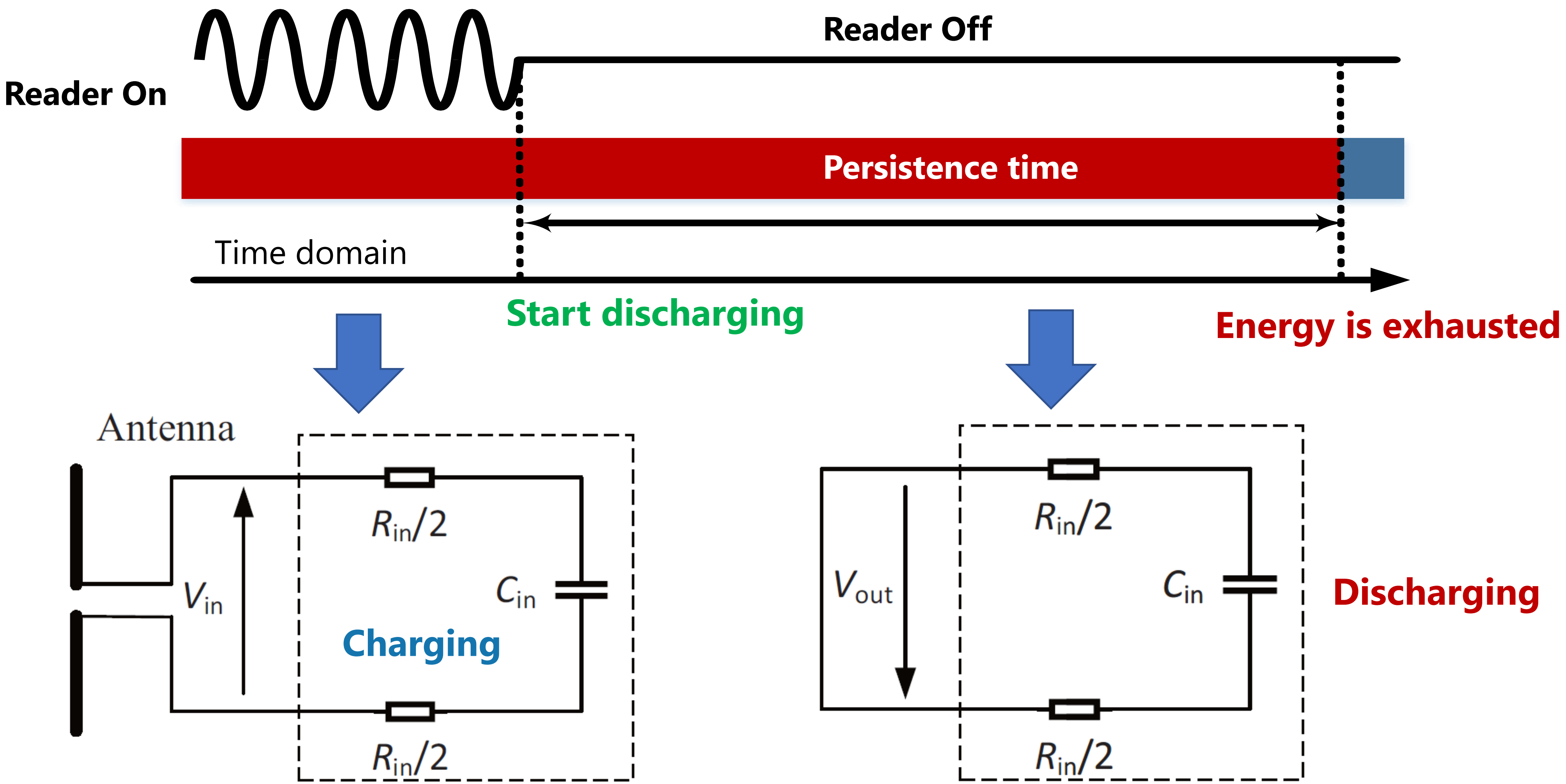
Basic idea:

- Use the electronic energy stored in the chip circuit to fingerprint a tag

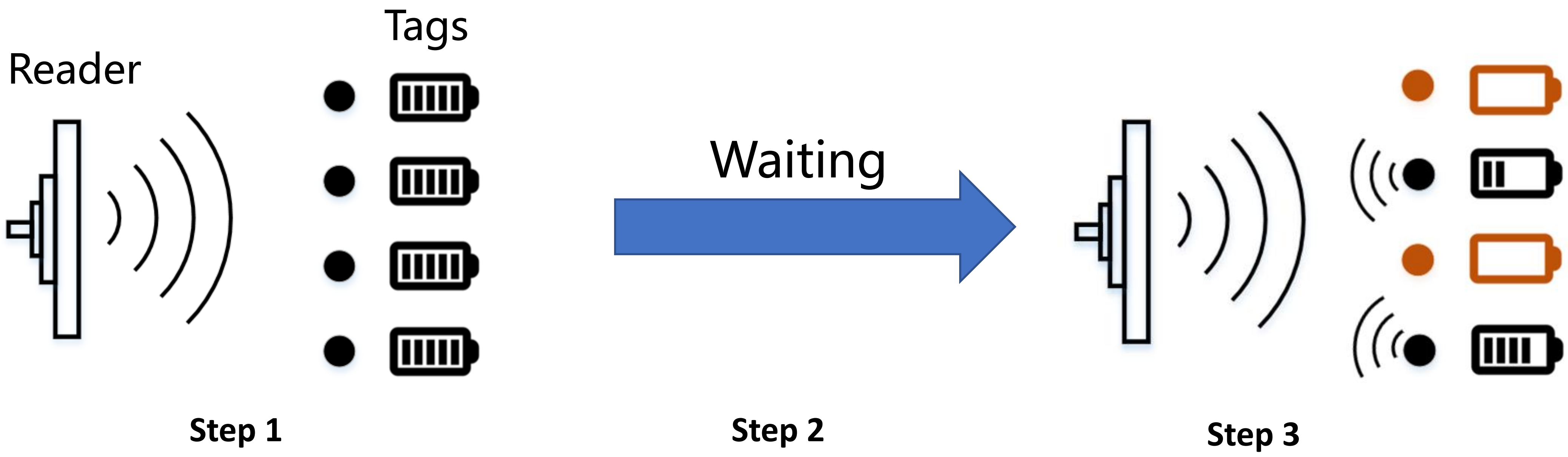
Challenges:

- Physically measuring the circuit is impractical
  - Needs a purpose-built test platform
  - Destroys the tag's structure and function

Our Solution: Persistence Time



Our Solution

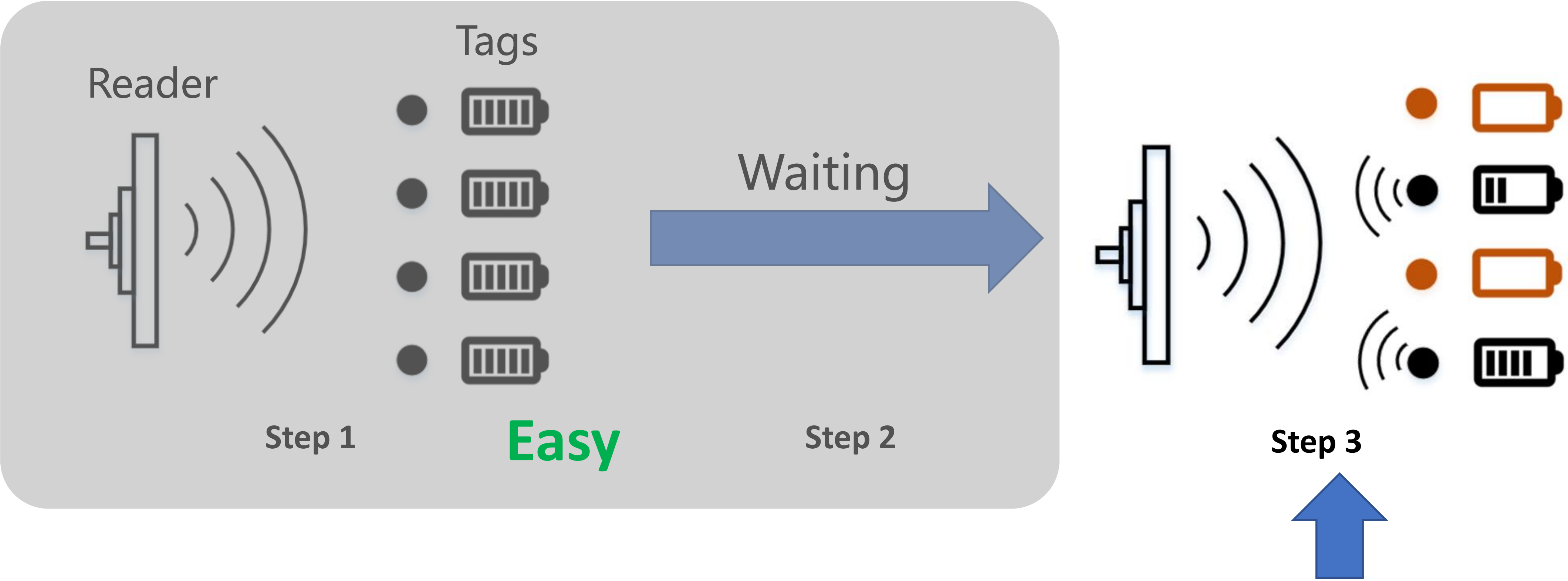


Step 1: Turn on the reader to energize the tags until they are fully charged

Step 2: Turn off the reader and wait for a period of time

Step 3: Check each tag whether its energy is exhausted or not. If yes, the waiting time is treated as the persistence time of the tag.

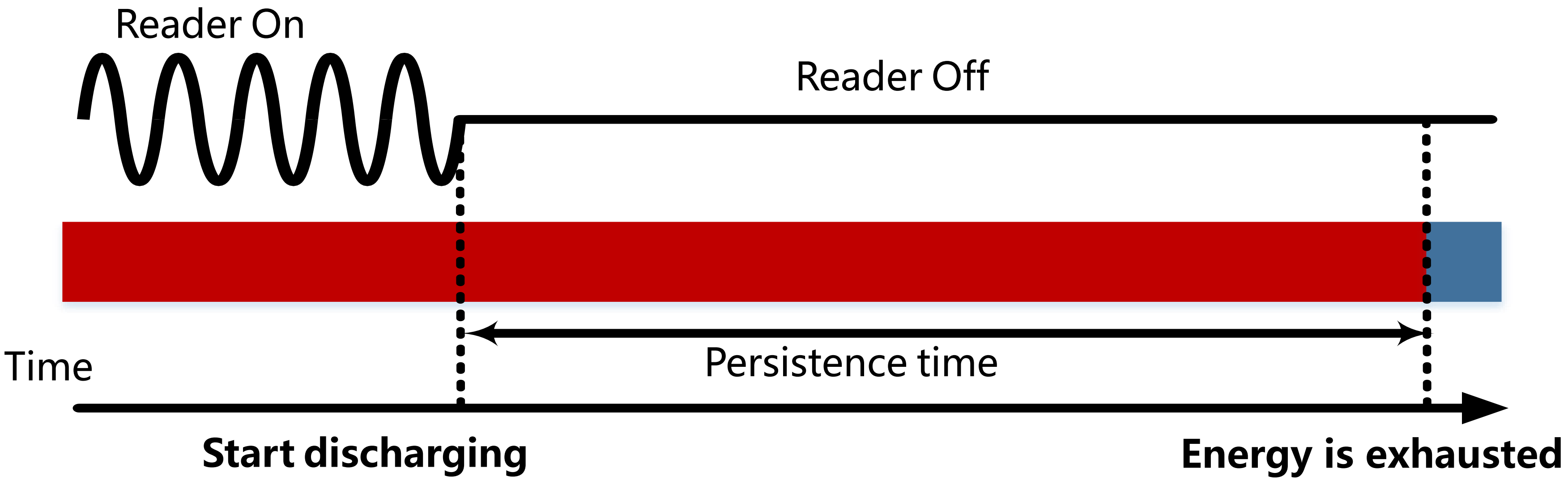
Our Solution

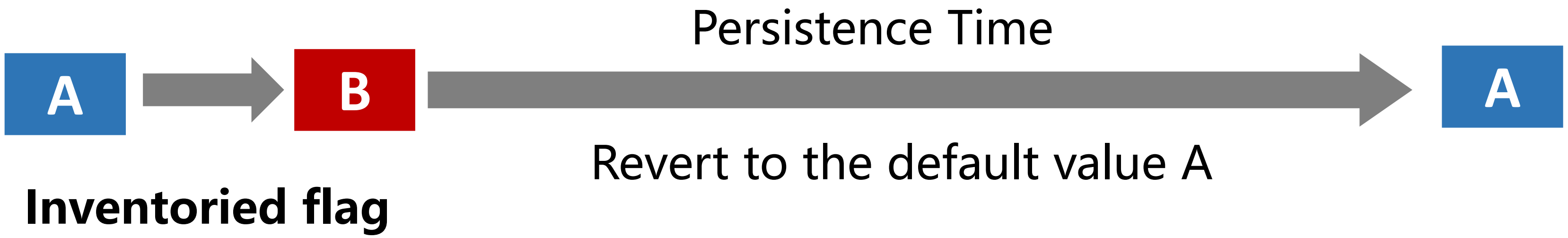


Whether a tag’s energy is exhausted?

Volatile Memory: Inventoried Flag

- Inventoried flag (**Volatile memory**)





Fingerprint Extraction

- **Related functions in EPCglobal Gen2 standard (Gen2) [1] :**

- F1: Sessions and inventory flag
- F2: Select Command.
- F3: Query Command.

[1] GS1 EPCglobal. EPC radio-frequency identity protocols generation-2 UHF RFID version 2.0.1, 2015.

Session and Inventoried Flag

4 inventoried flags → **3 persistence times**

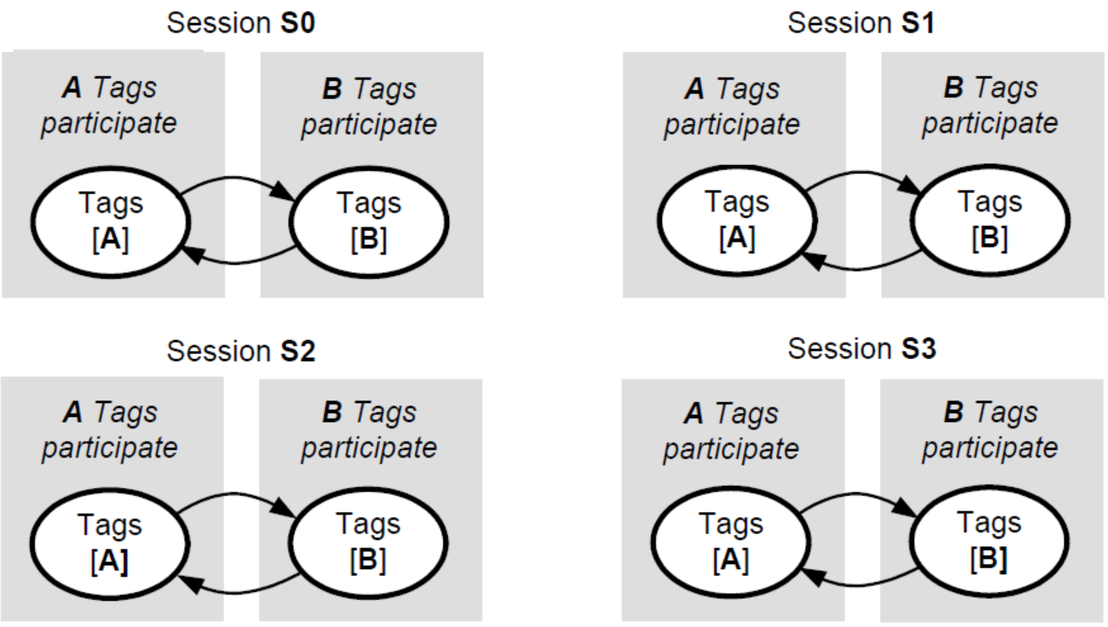
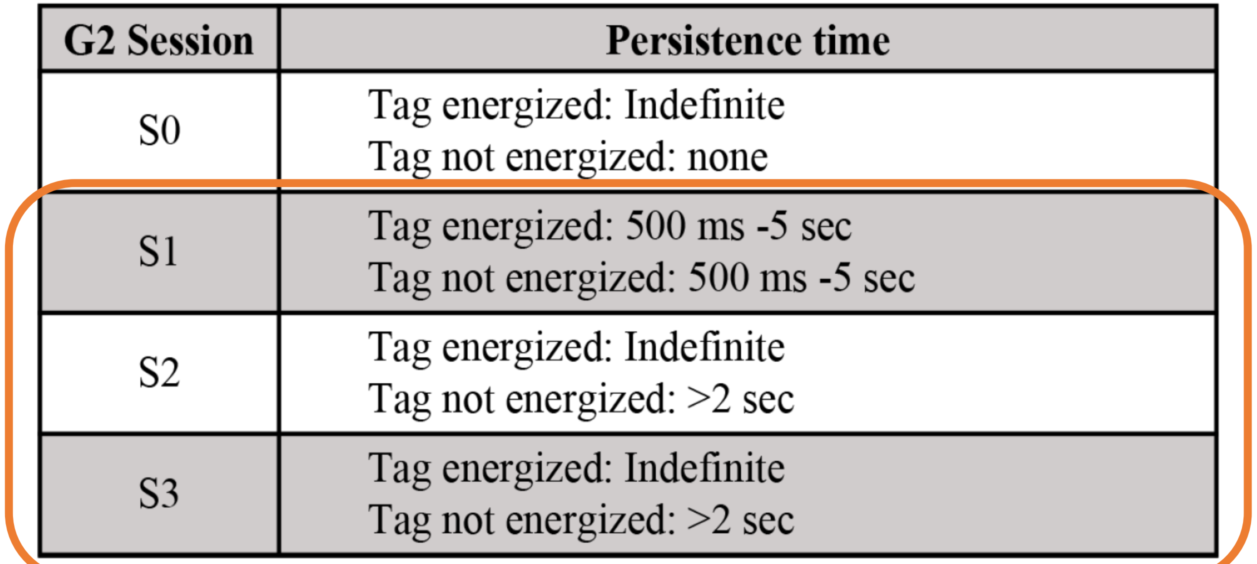

Session **S0**
A *Tags participate*
B *Tags participate*
Tags [A]
Tags [B]
Session **S1**
A *Tags participate*
B *Tags participate*
Tags [A]
Tags [B]
Session **S2**
A *Tags participate*
B *Tags participate*
Tags [A]
Tags [B]
Session **S3**
A *Tags participate*
B *Tags participate*
Tags [A]
Tags [B]

Table 1: Persistence time



G2 Session	Persistence time
S0	Tag energized: Indefinite Tag not energized: none
S1	Tag energized: 500 ms -5 sec Tag not energized: 500 ms -5 sec
S2	Tag energized: Indefinite Tag not energized: >2 sec
S3	Tag energized: Indefinite Tag not energized: >2 sec

Observations:

- The flag will flip to A when the tag is exhausted
- A tag has three fingerprints

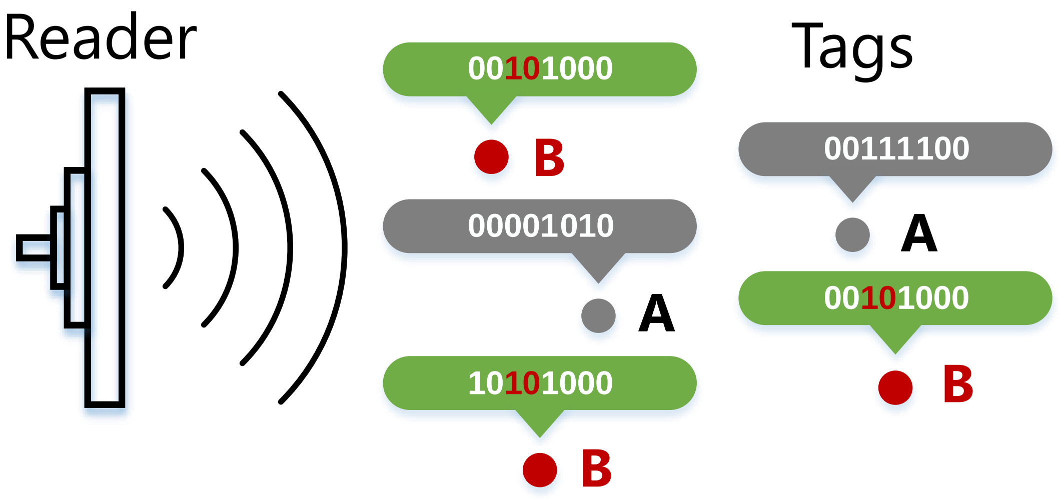
Select Command

- Fields of Select command:

Cmd Code	Target	Action	Membank	Pointer	Length	Mask
	Session	Action	Bit mask			

Select

Target = 1
Action = 0
MemBank = 1
Pointer = 2
Length = 2
Mask = **10**



Set **inventoried flags** to either **A or B**
or set **SL flag** to either **SL or ~SL**

Query Command

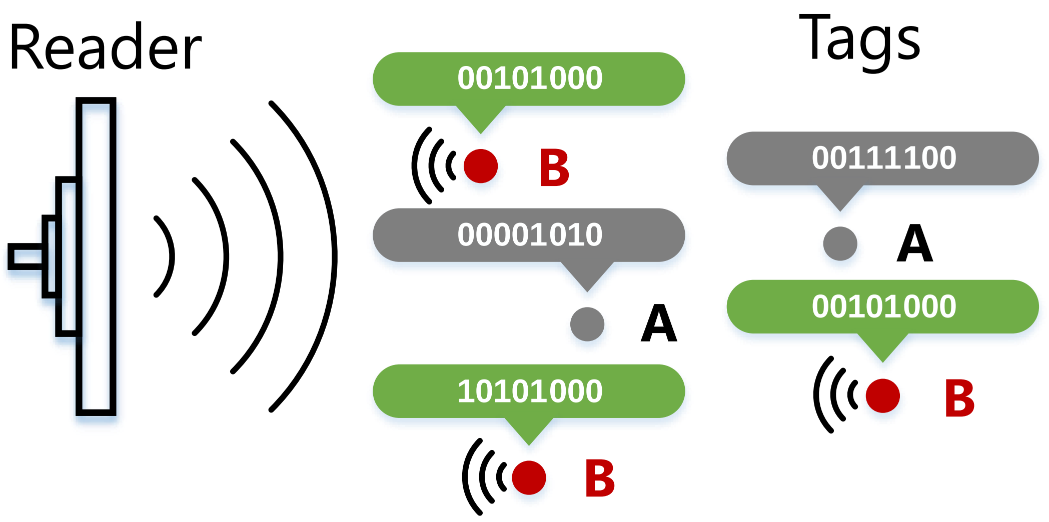
- ➢ Fields of Query command:

Cmd Code	Target	Sel	Session

Inventoried flag **A (0)** or **B (1)**

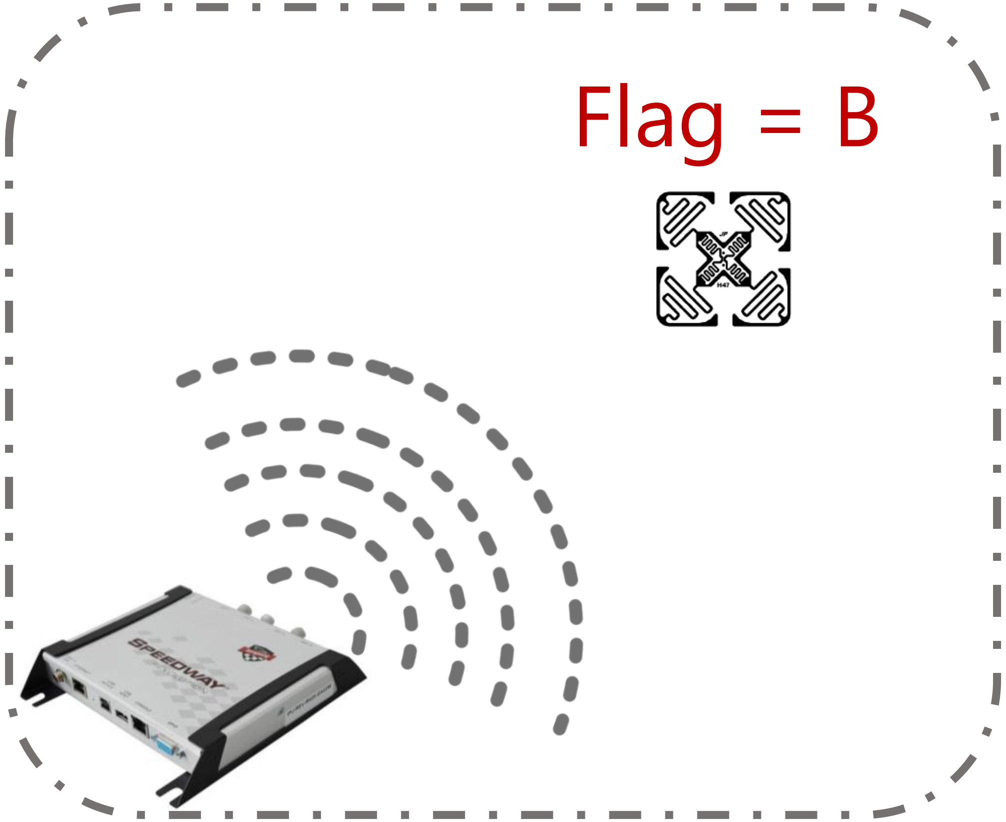
Query

Target = 1
Session = 1
Sel = 0



The tags with Target state B will reply to the reader

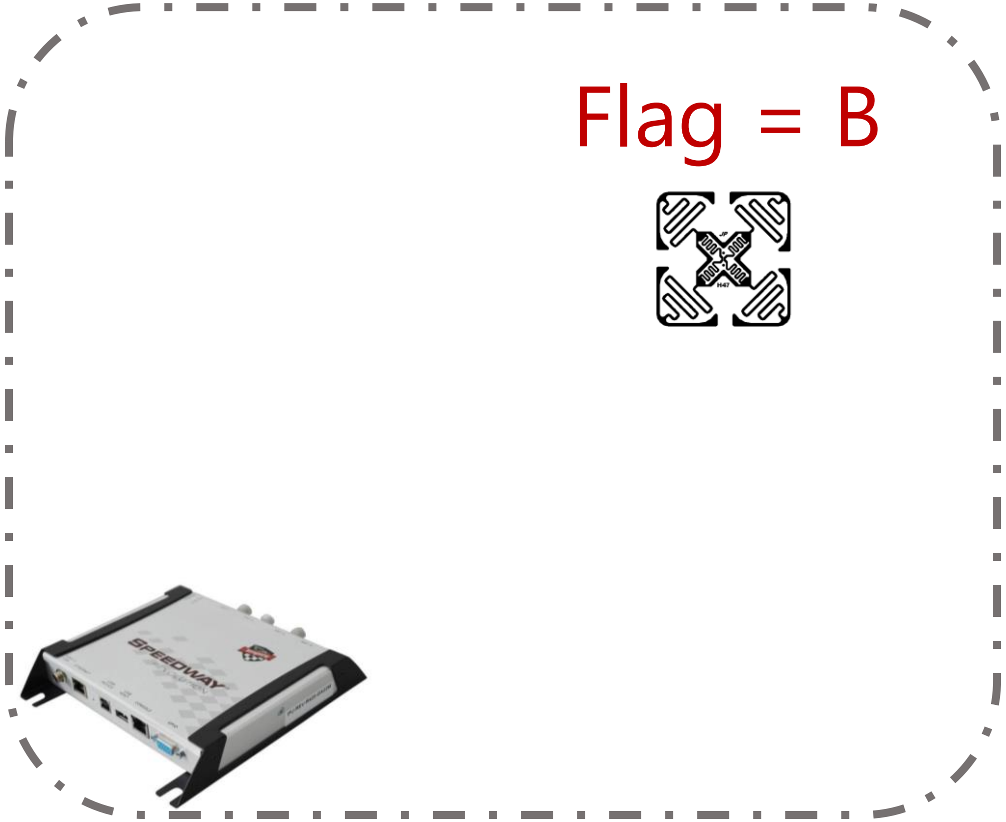
Select and Query Measurement (SQM)



1. Set a tag's flag to B.

Select $\text{Flag} \leftarrow \text{BA}\text{: } S(1,4,1,32,96,id)$

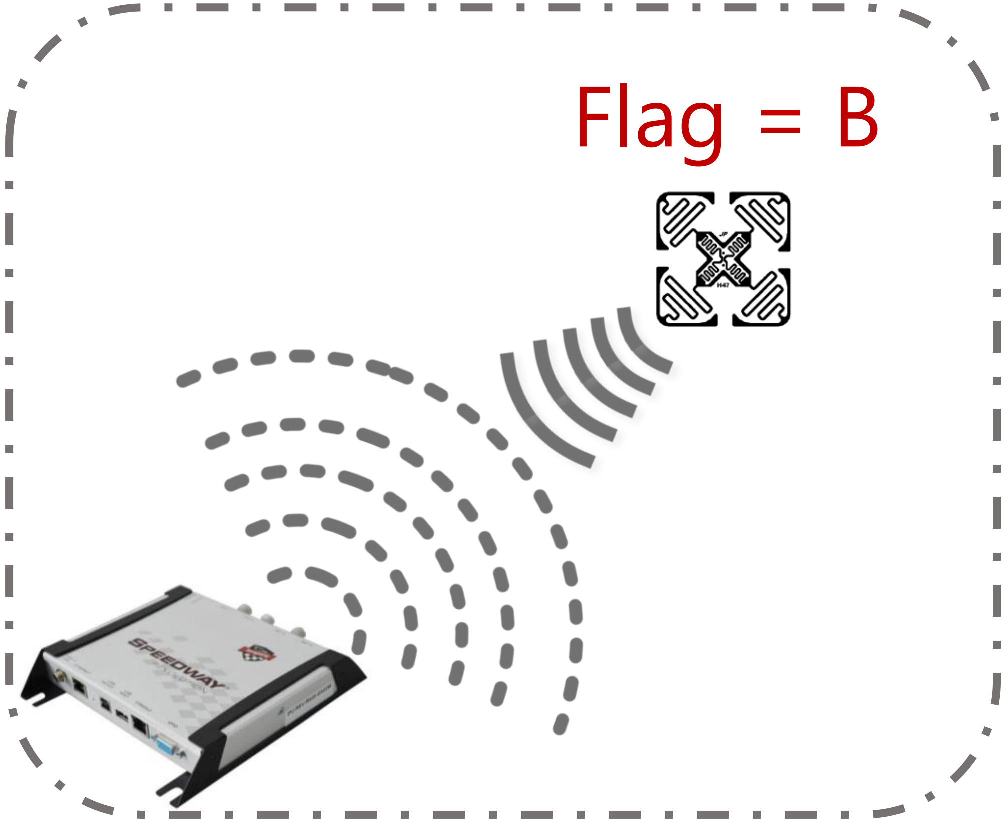
Select and Query Measurement (SQM)



1. Set a tag's flag to B.

2. Turn off the reader and wait for a period of time.

Select and Query Measurement (SQM)



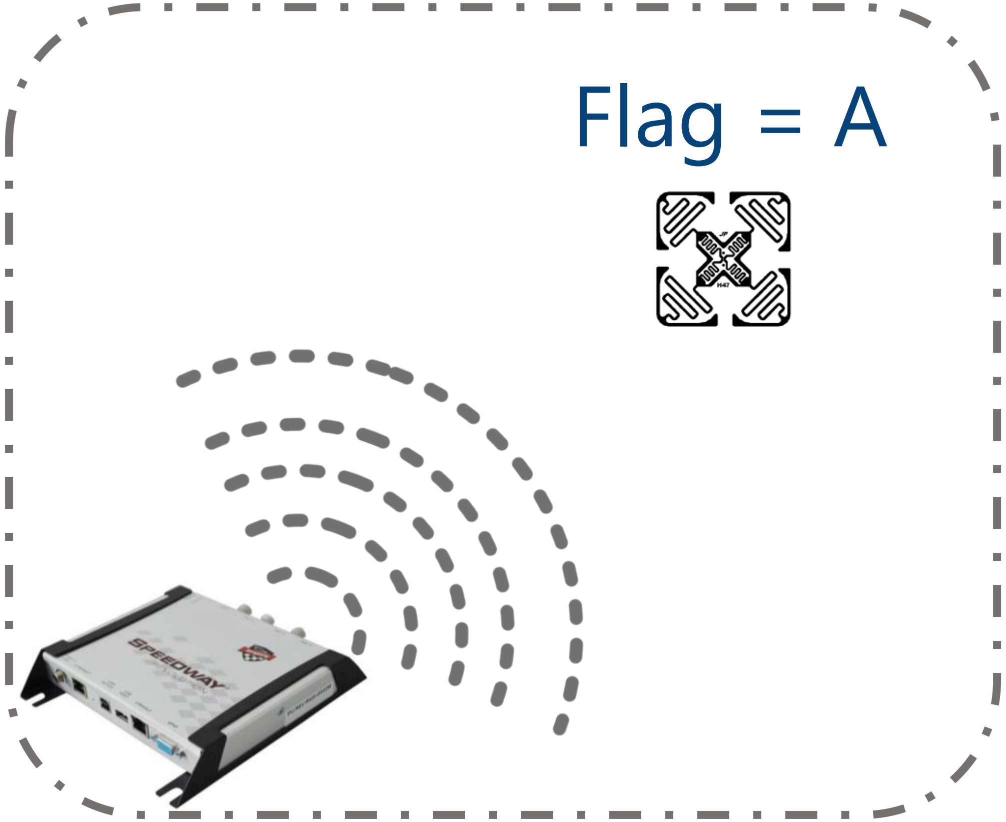
1. Set a tag's flag to B.

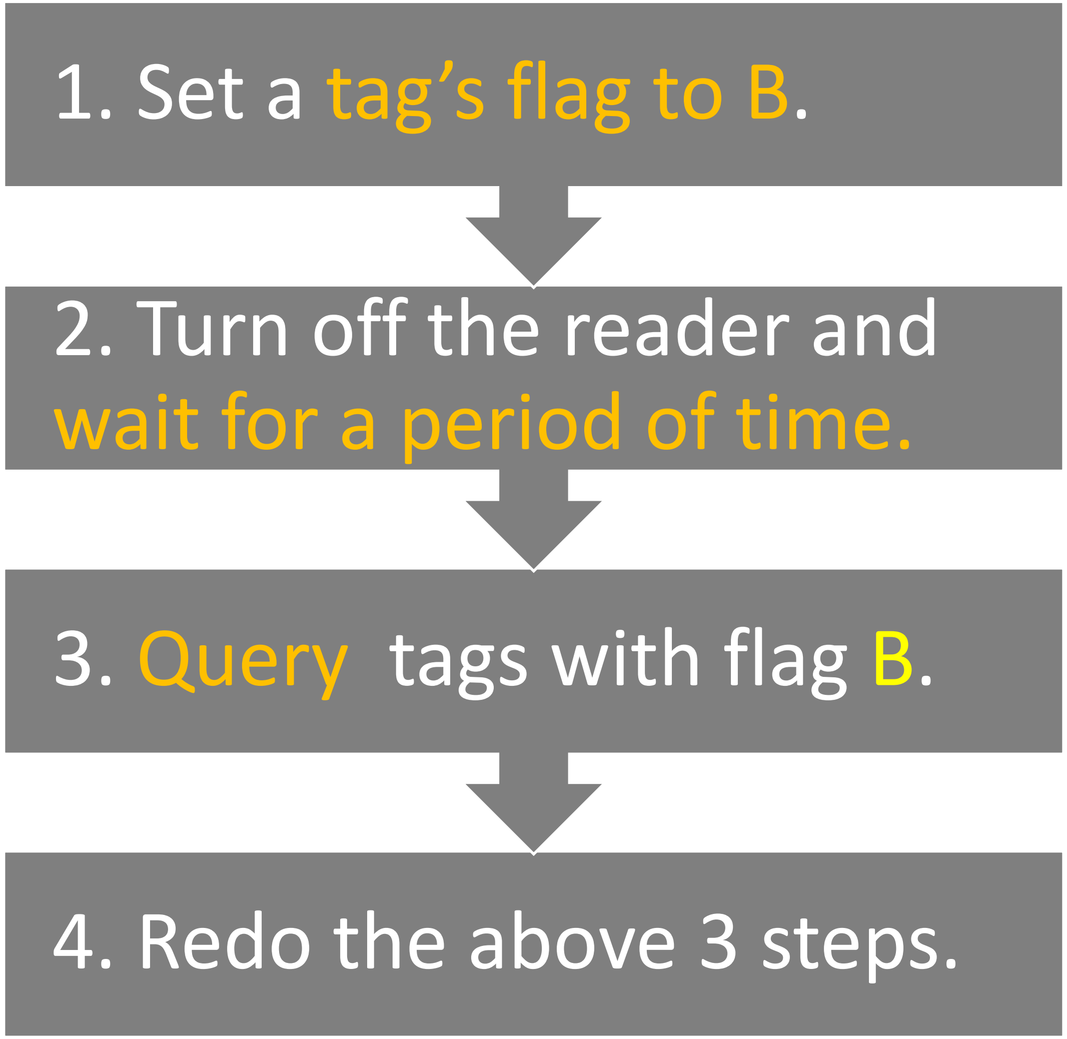
2. Turn off the reader and wait for a period of time.

3. Query tags with flag B.

$$\text{Query } B: \ Q(Session = 1, Taget = 1, Sel = 0)$$

Select and Query Measurement (SQM)





1. Set a tag’s flag to B.

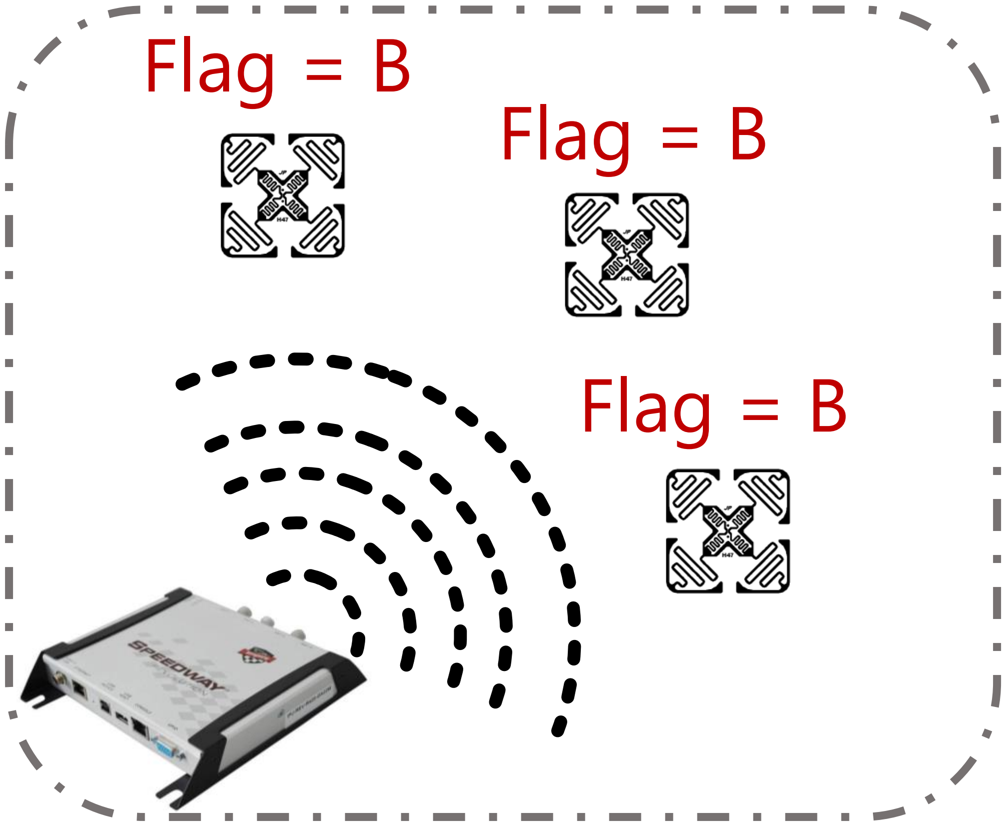
2. Turn off the reader and wait for a period of time.

3. Query tags with flag B.

4. Redo the above 3 steps.

Minimal period makes no reply.

Multiple Tags



1. Set target tags’ flags to B.

2. Turn off the reader and wait for a period of time.

3. Query tags with flag B.

Select Commands

$$\textcircled{1}\ t_1 \leftarrow BA : S(2, a = 4, 1, 32, 96, id_1)$$

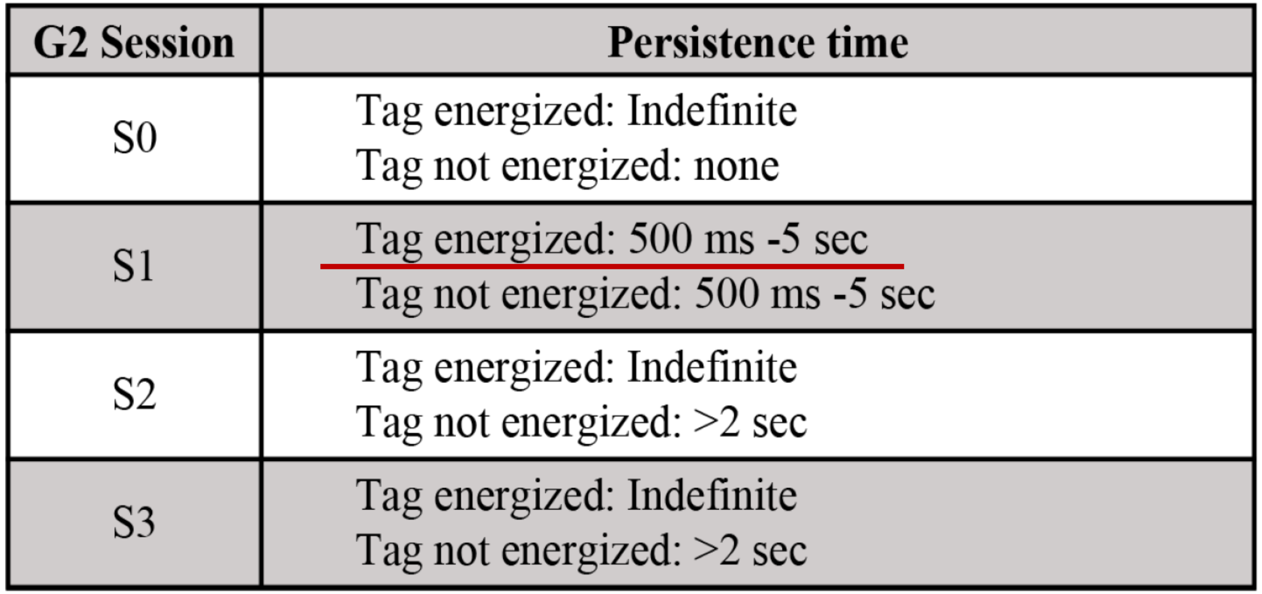
$$\textcircled{i}\ t_i \leftarrow B- : S(2, a = 5, 1, 32, 96, id_i),\ \ i \in [2, m]$$

Enhanced SQM (ESQM)

- SQM is still time-consuming

  e.g., Measuring a tag with 3 s persistence time requires 0.5+0.6+ …… +3 = **45.5 s.**

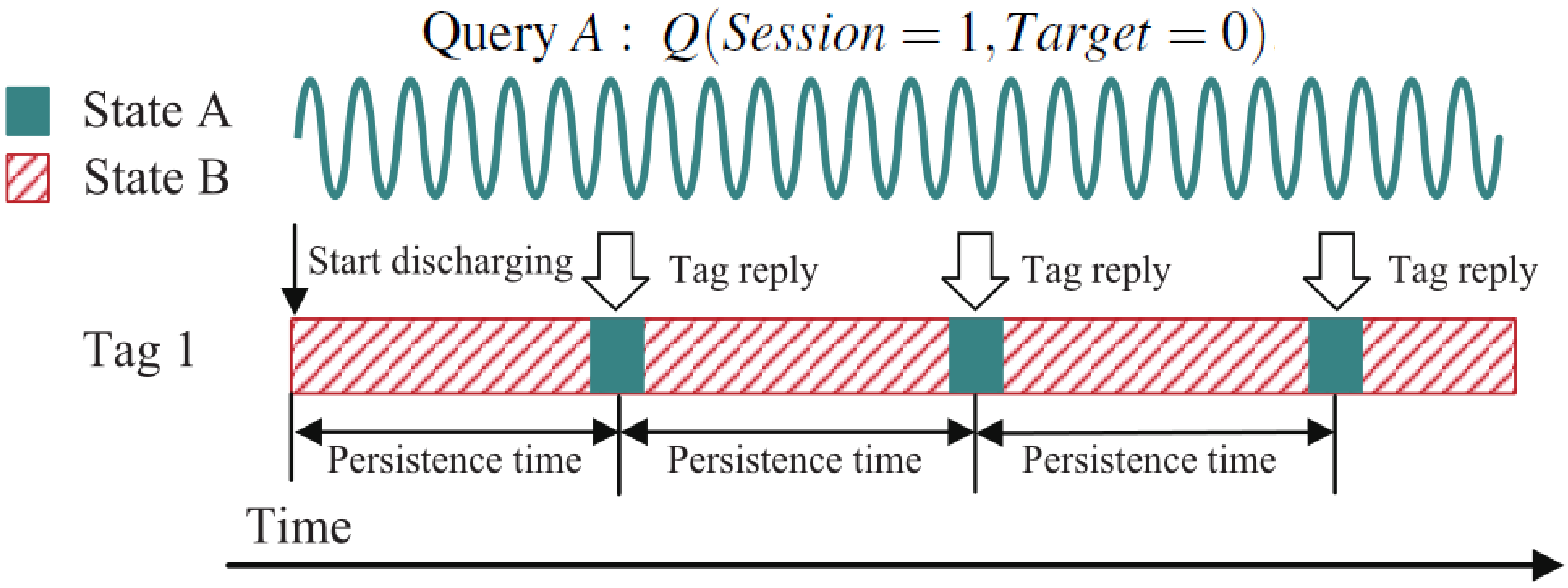
- **The persistence time of S1 can be measured when reader is on**



G2 Session	Persistence time
S0	Tag energized: Indefinite Tag not energized: none
S1	Tag energized: 500 ms -5 sec Tag not energized: 500 ms -5 sec
S2	Tag energized: Indefinite Tag not energized: >2 sec
S3	Tag energized: Indefinite Tag not energized: >2 sec

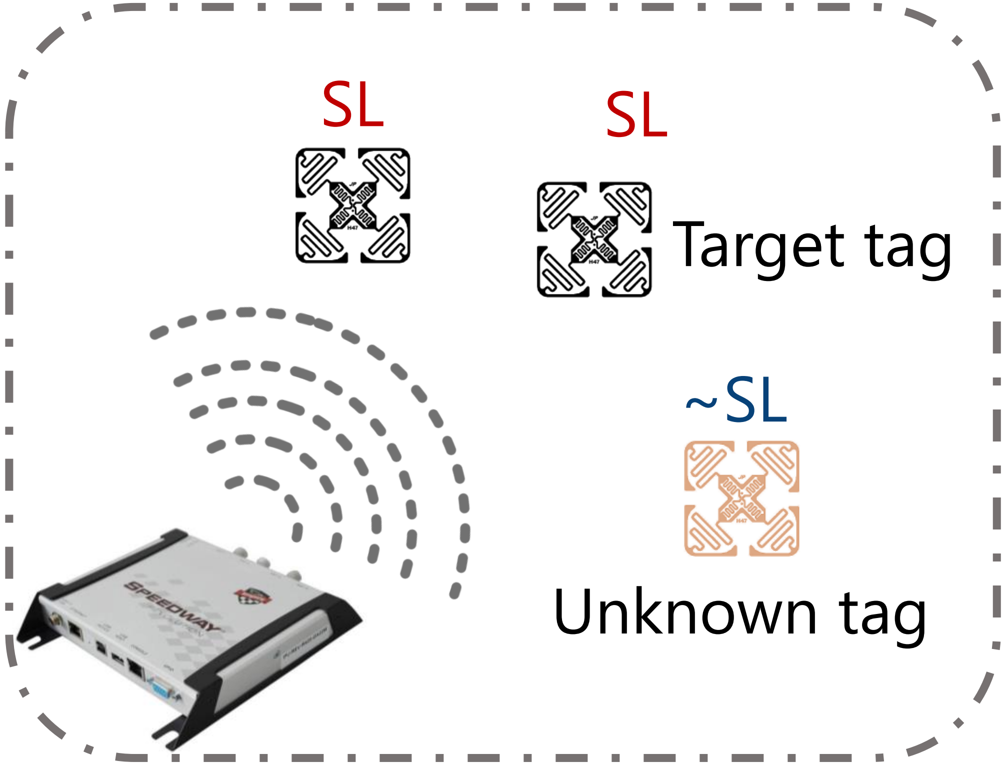
Enhanced SQM (ESQM)

- ➢ Quickly measure the persistence time of session 1

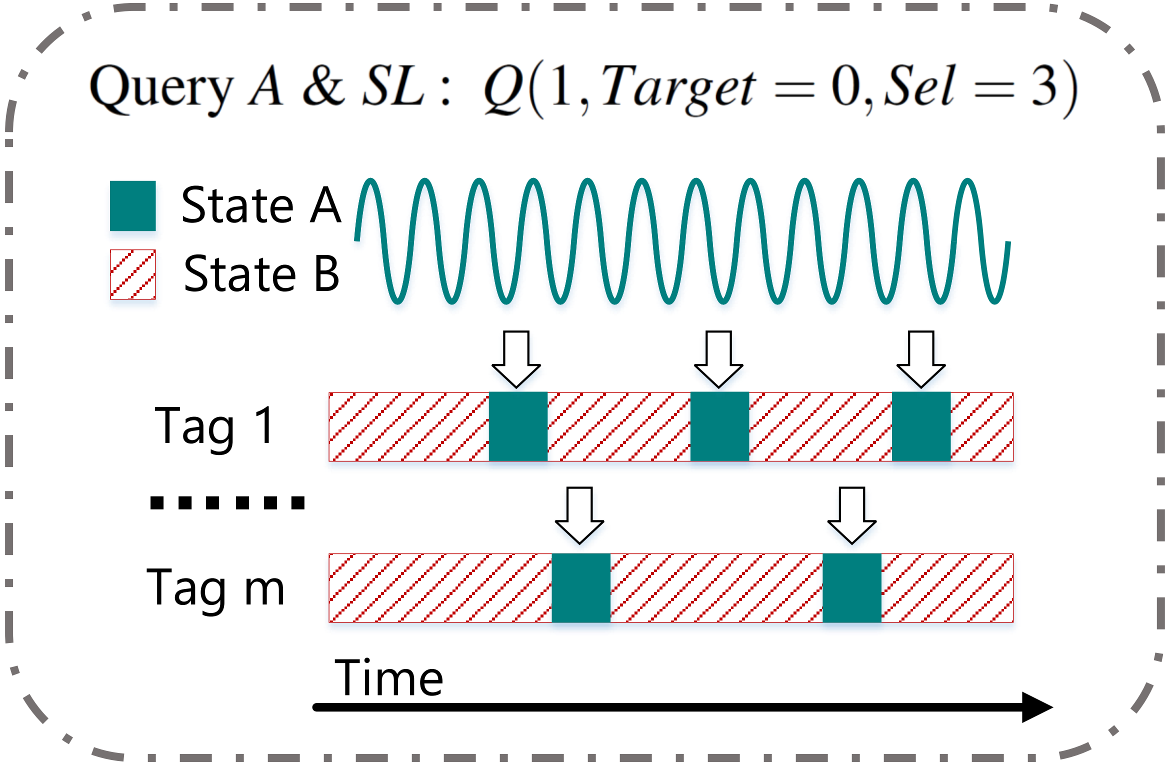


Tips: According to Gen2, the tag will flip its inventory flag after replying to the reader. (**A->B** in this case)

ESQM--Multiple Tags



Query



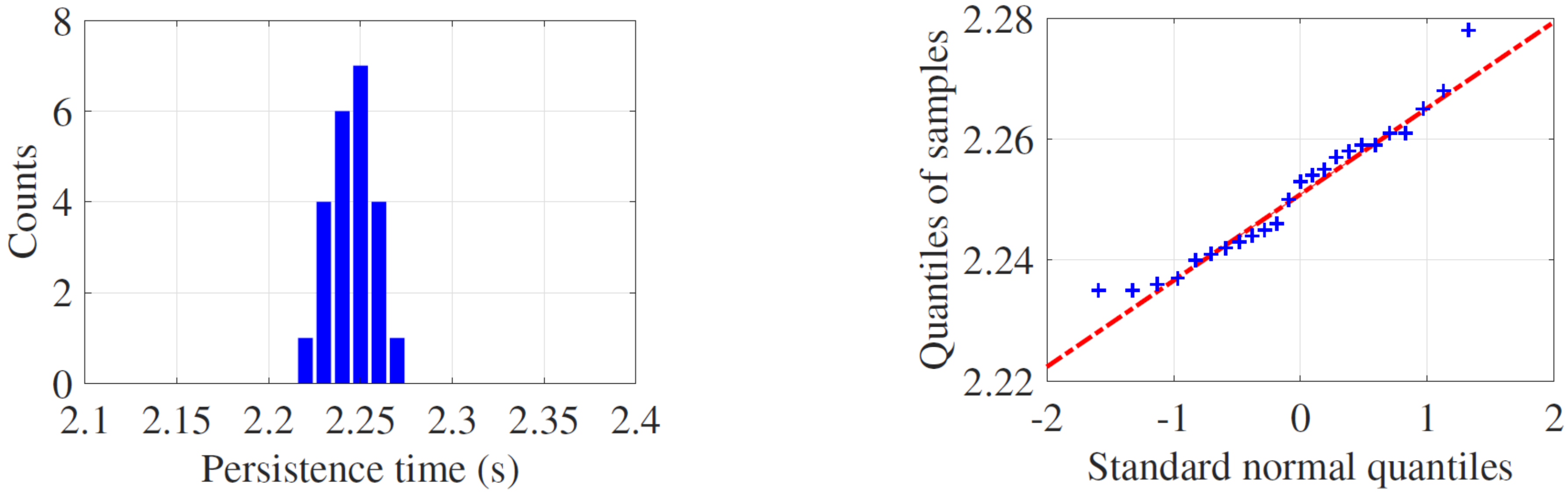
Query A & SL : $Q(1, Target = 0, Sel = 3)$

Select

① $t_1 \leftarrow AB : S(t = 4, 0, 1, 32, 96, id_1)$, Set target tags to SL

ⓘ $t_i \leftarrow A- : S(t = 4, 1, 1, 32, 96, id_i)$, $i \in [2, m]$

Genuineness Validation



(a) Sample data.

(b) Q-Q plot.

Observation:

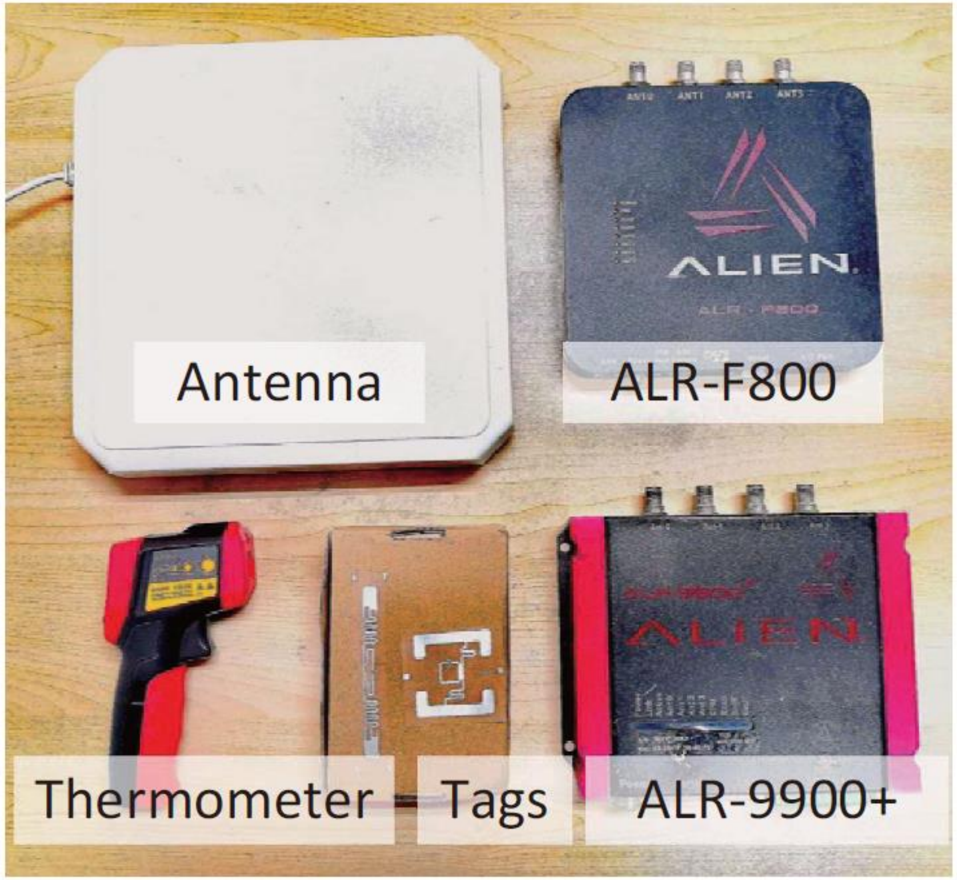
- Persistence time follows **Gaussian distribution**.

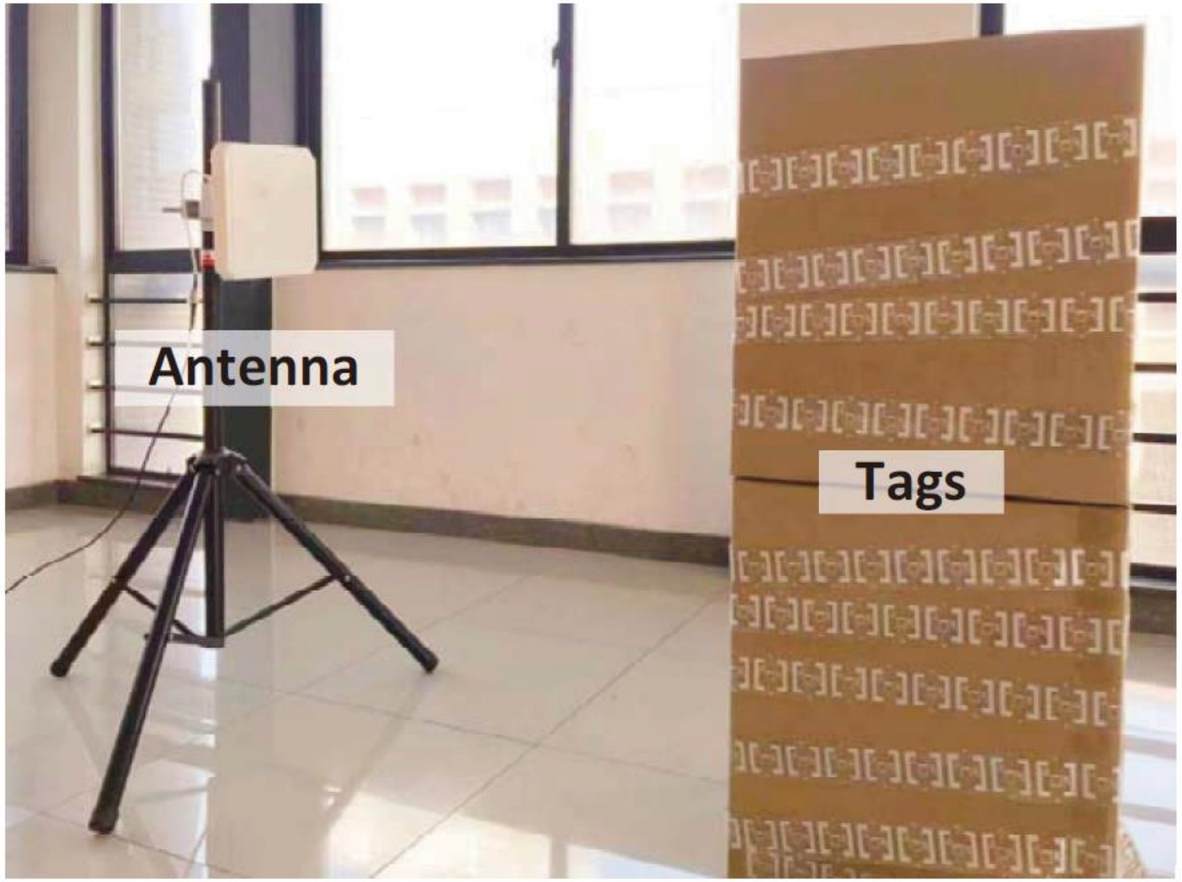
Solution:

- We use **t-test** to check whether the test data and the genuine data follow the same distribution.

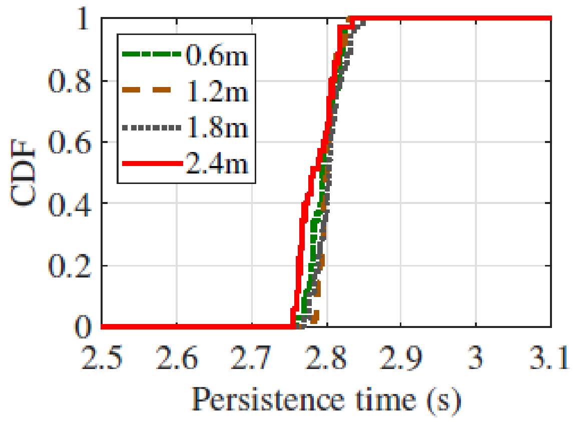
Evaluation

- **1000 tags + 4 readers**

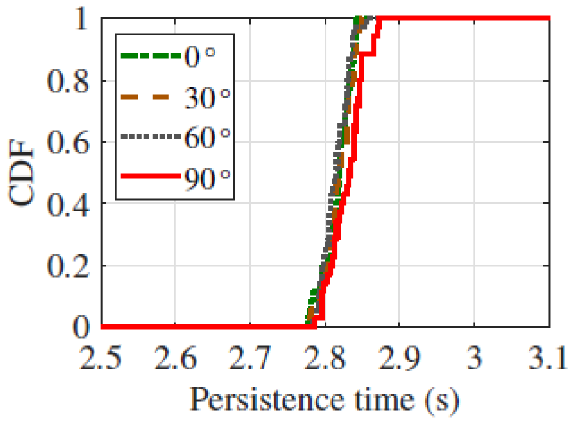




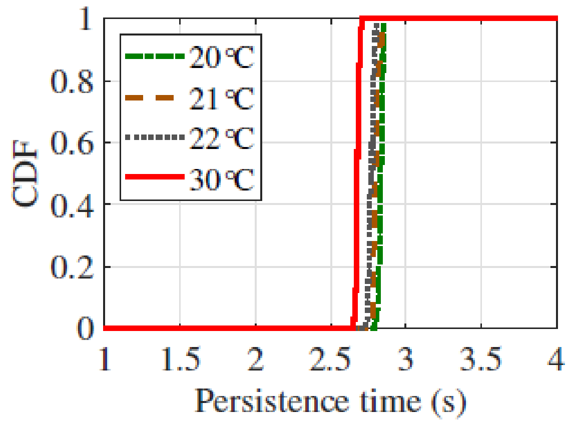
Evaluation



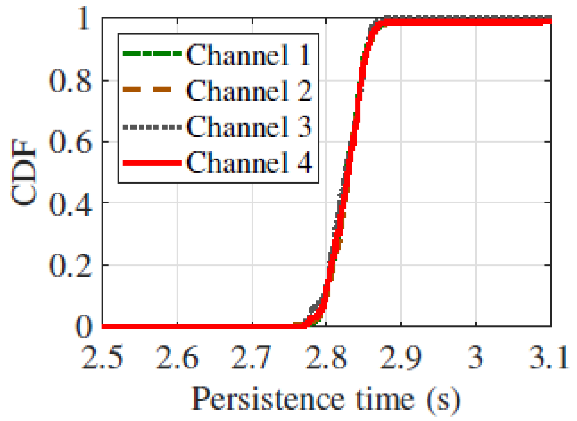
Communication distance



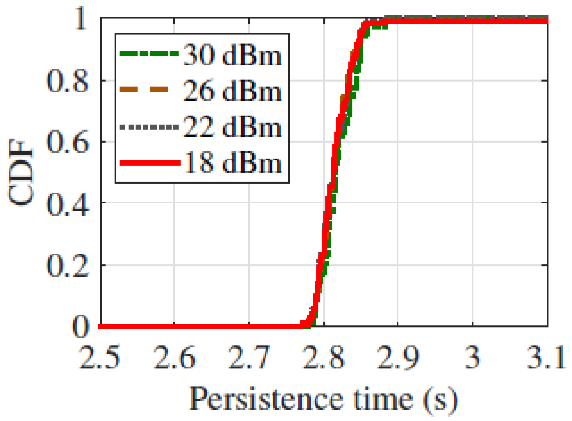
Tag direction



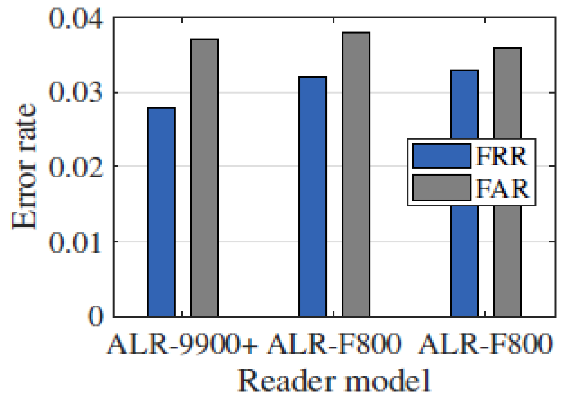
Temperature



RF channel



Transmit power

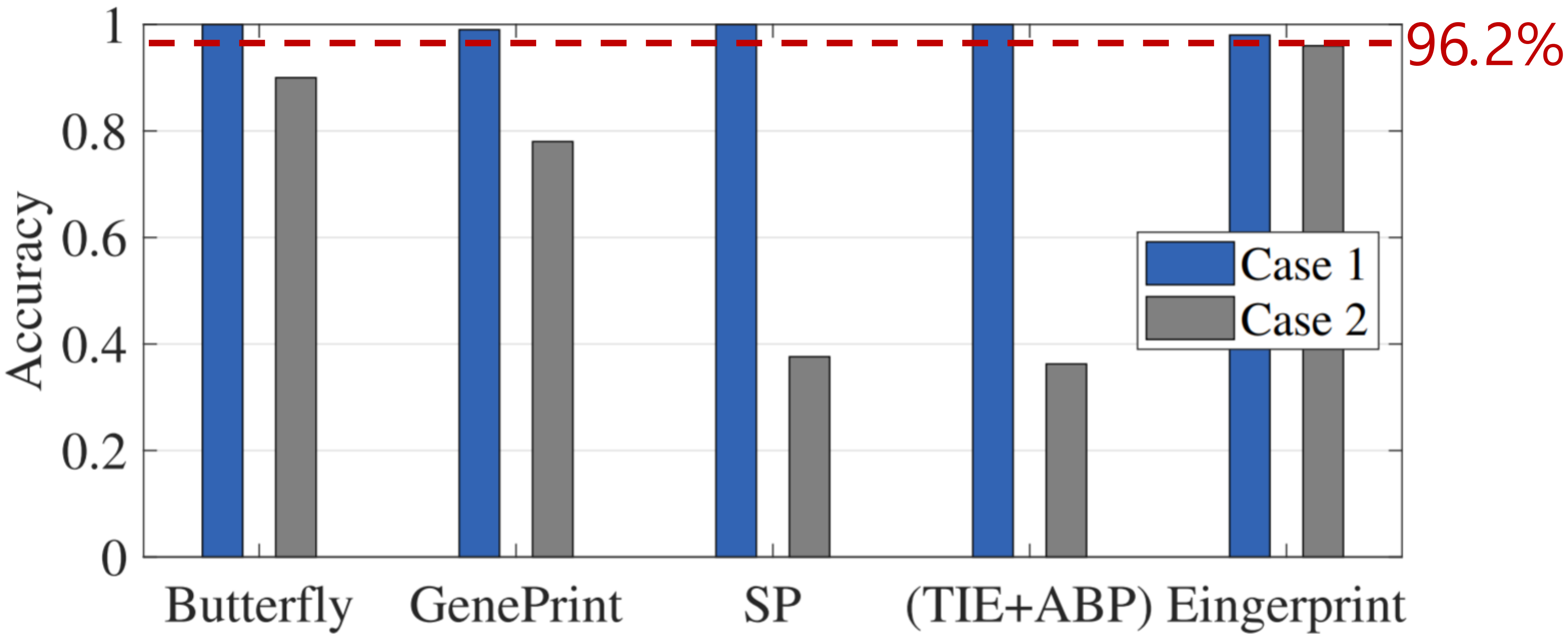


Device diversity

- **Eingerprint is robust to environmental factors**

Evaluation

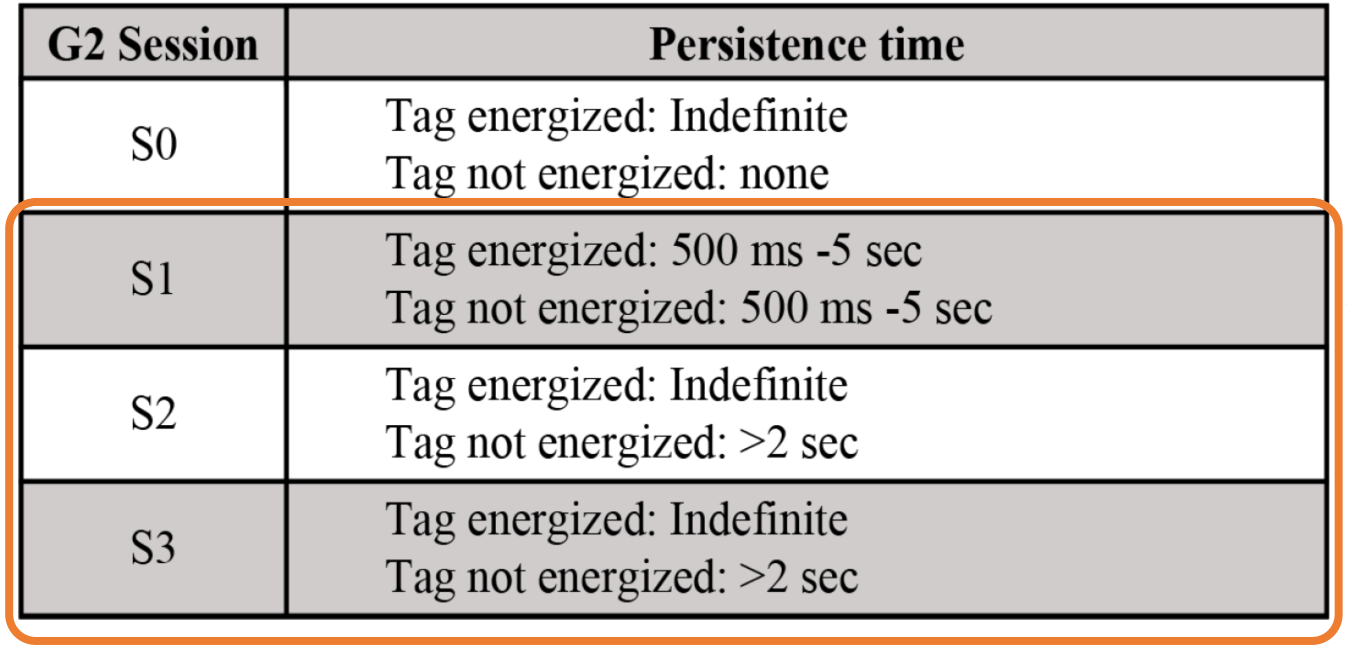
Authentication Accuracy



Case 1 : Same position. **Case 2 : Different rooms.**

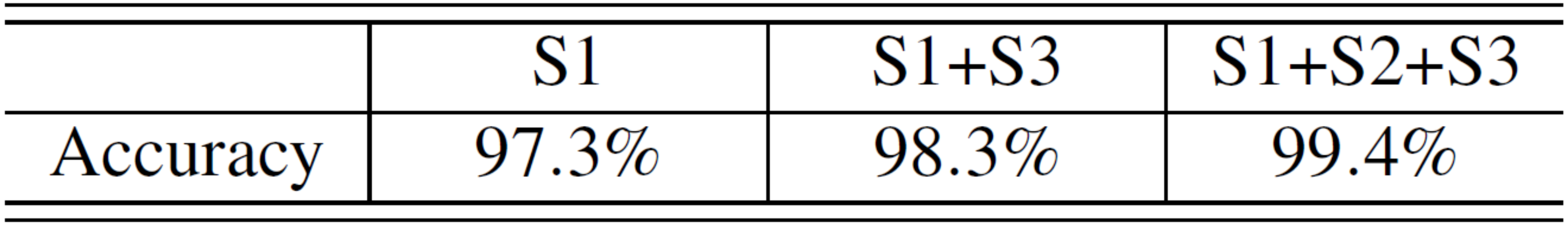
Evaluation

Performance with different sessions



G2 Session	Persistence time
S0	Tag energized: Indefinite Tag not energized: none
S1	Tag energized: 500 ms -5 sec Tag not energized: 500 ms -5 sec
S2	Tag energized: Indefinite Tag not energized: >2 sec
S3	Tag energized: Indefinite Tag not energized: >2 sec

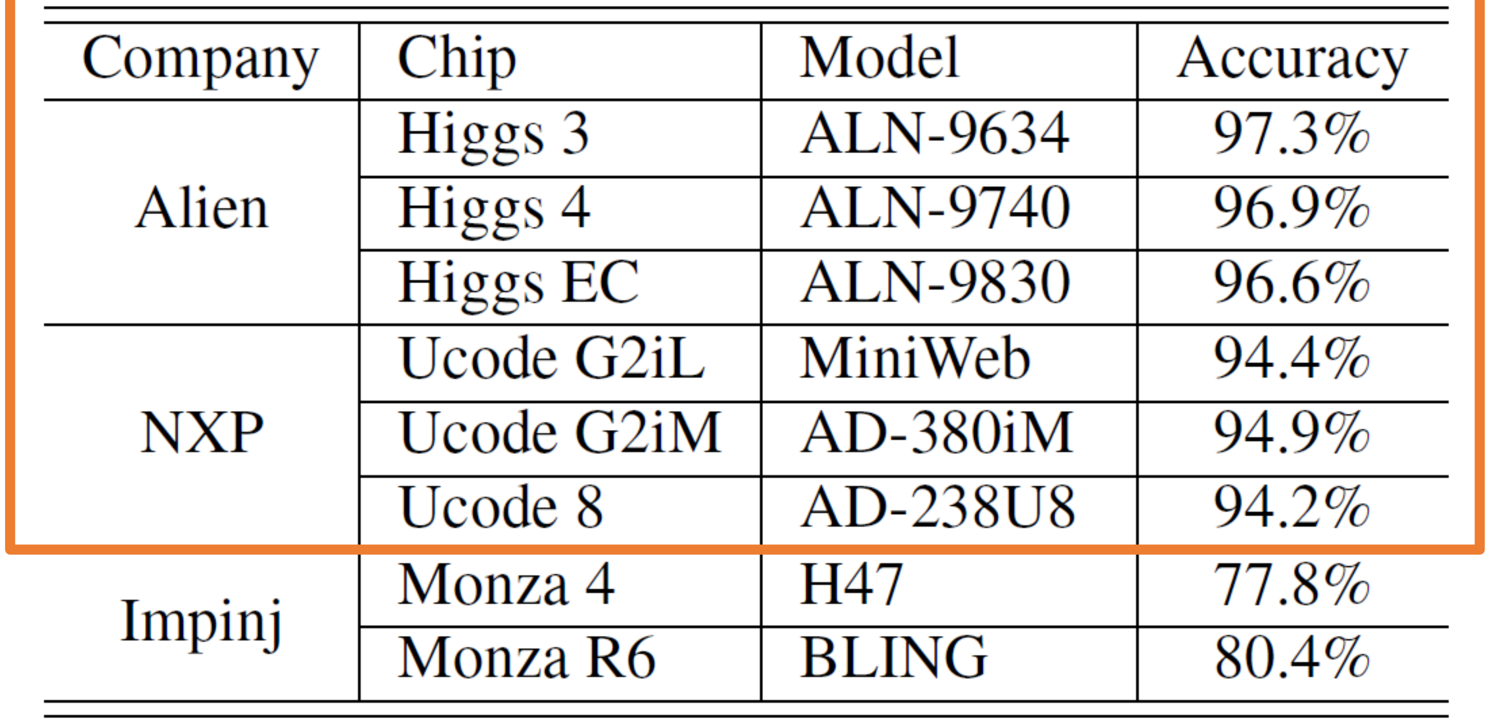
Accuracy = 99.4%



	S1	S1+S3	S1+S2+S3
Accuracy	97.3%	98.3%	99.4%

Evaluation

Performance on different tag models



Company	Chip	Model	Accuracy
Alien	Higgs 3	ALN-9634	97.3%
	Higgs 4	ALN-9740	96.9%
	Higgs EC	ALN-9830	96.6%
NXP	Ucode G2iL	MiniWeb	94.4%
	Ucode G2iM	AD-380iM	94.9%
	Ucode 8	AD-238U8	94.2%
Impinj	Monza 4	H47	77.8%
	Monza R6	BLING	80.4%

Accuracy > 94%

Conclusion

01

We propose a new **energy-related fingerprint** called Eingerprint to authenticate passive tags. The competitive advantage of Eingerprint is that it is **fully compatible with the RFID standard**.

02

We use a new metric called **persistence time** to indicate the energy level stored in a tag's RC circuit. A flag-based solution is designed to measure the time.

03

We implement a prototype of Eingerprint in a commercial RFID system. Experiments show that our method is able to **achieve a high accuracy** and also **robust to the environmental factors.**

THANKS