THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RF-DNA: Large-Scale Physical-layer Identifications of RFIDs via Dual Natural Attributes

Qingrui Pan, Zhenlin An, Xueyuan Yang,

Xiaopeng Zhao, Lei Yang

RFID becomes Increasingly Important

Supply Chain

Electronic Passport

Mobile Payment

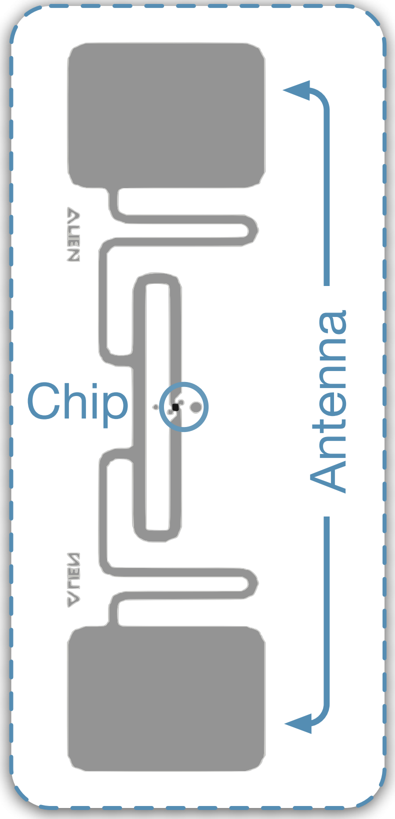
- **Radio Frequency IDentification** **(RFID) tags** are becoming in

Security of RFIDs attract more attention.

- According to the report, **17.5 billion** RFID tags are sold in 2018

Protocol-based Solutions are NOT Practical

- **Authentication Protocols**
  - Checking stored data and identifying tags
  - **Limitation: vulnerable** to counterfeiting attacks
- **Cryptographic Protocols**
  - Sending cipher-text instead of plaintext
  - **Limitation:** demanding **extra power** and **computation**



Previous Fingerprints only on a Small-Scale

Solution	Fingerprint(s)	Components	Scale (#)	Accuracy	Time
ETH	TIE+ABP	Antenna+IC	**50**	98.7%	20ms
Geneprint	ExTIE+PSD	Antenna+IC	**150**	99.68%	20ms
TagPrint	Phase	Antenna	**2,000**	80.39%	20ms
Eingerprint	Persistence Time	IC	**200**	91.60%	60s

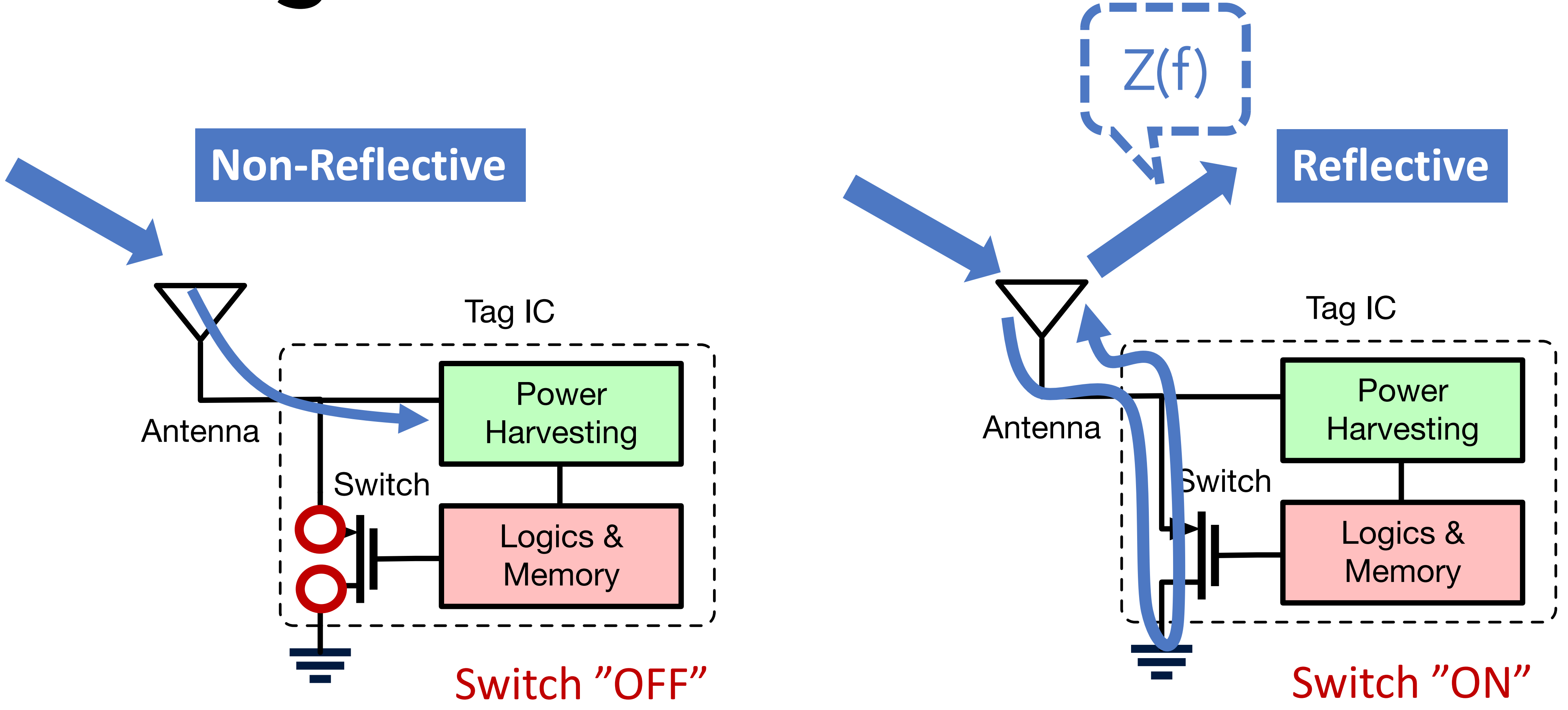
Previous Fingerprints only on a Small-Scale

Solution	Fingerprint(s)	Components	Scale (#)	Accuracy	Time
ETH	TIE+ABP	Antenna+IC	50	98.7%→**26.08%**	20ms
Geneprint	ExTIE+PSD	Antenna+IC	150	99.68%→**56.08%**	20ms
TagPrint	Phase	Antenna	2,000	80.39%→**24.93%**	20ms
Eingerprint	Persistence Time	IC	200	91.60%→**77.80%**	60s
Ours	**RF-DNA**	Antenna+IC	**16,000**	**95.98%**	20ms

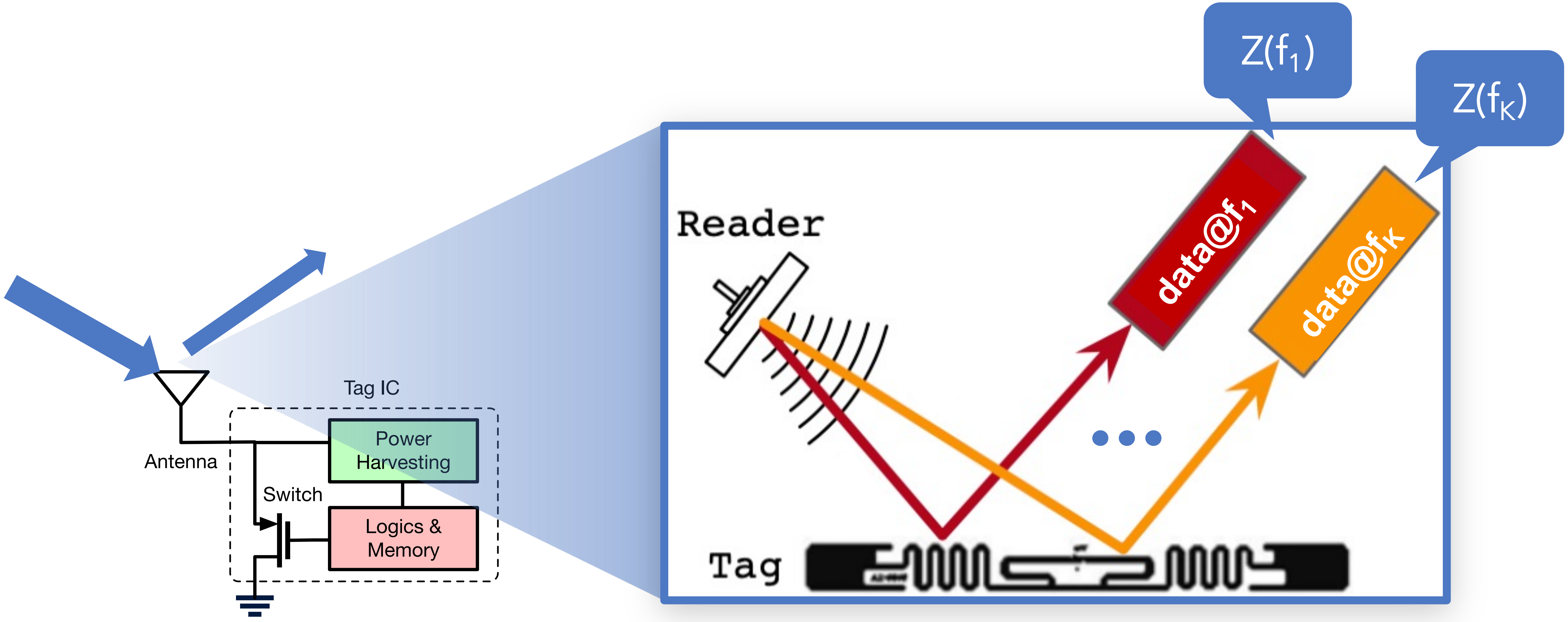
Our fingerprint (RF-DNA) works in a large-scale dataset with high accuracy.

Why our fingerprint works?

RFID Tag Backscatters in Two States



Intrinsic Response Chain is Extendable



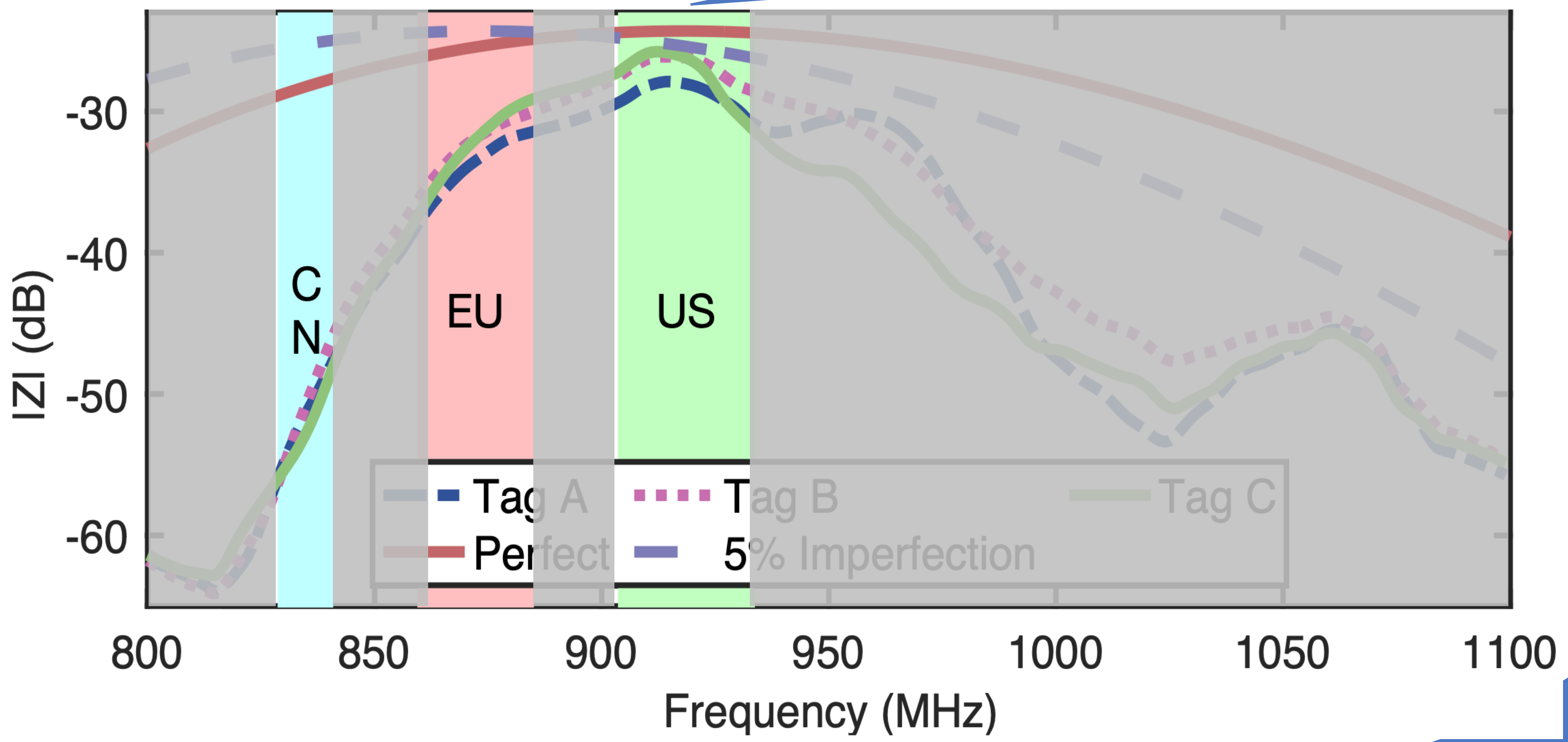
$\{f_1, f_2, f_3, f_4, \ldots f_K\}$ $\xrightarrow{\text{Tag}}$ $\{Z(f_1), Z(f_2), Z(f_3), Z(f_4), \ldots Z(f_K)\}$

Chain of response can be **extended** by utilizing more frequencies.

RFID working frequency bands are narrow

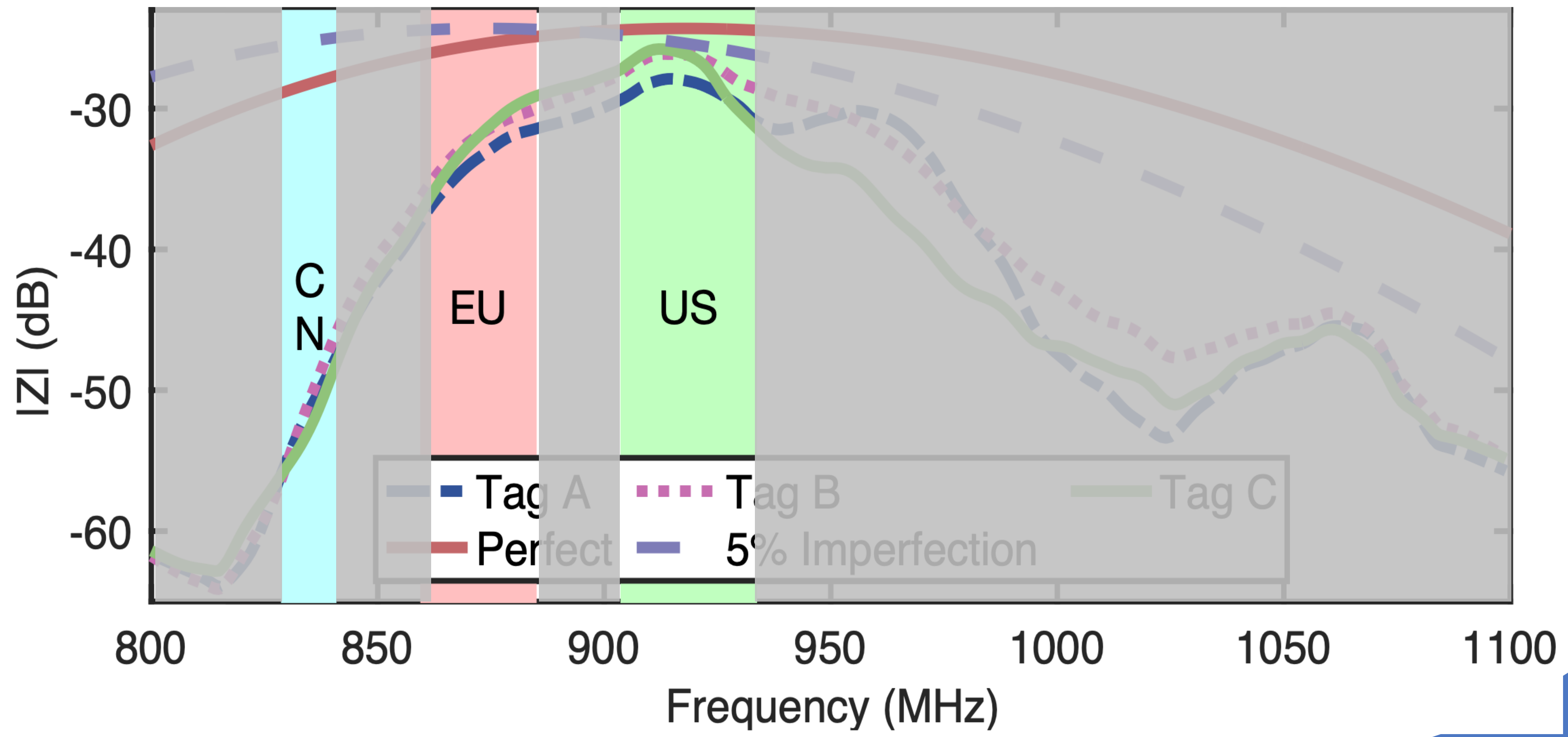
Previously proposed fingerprints are exploited at **in-band frequencies** assigned to an RFID system.

Previous Fingerprints Work Here!



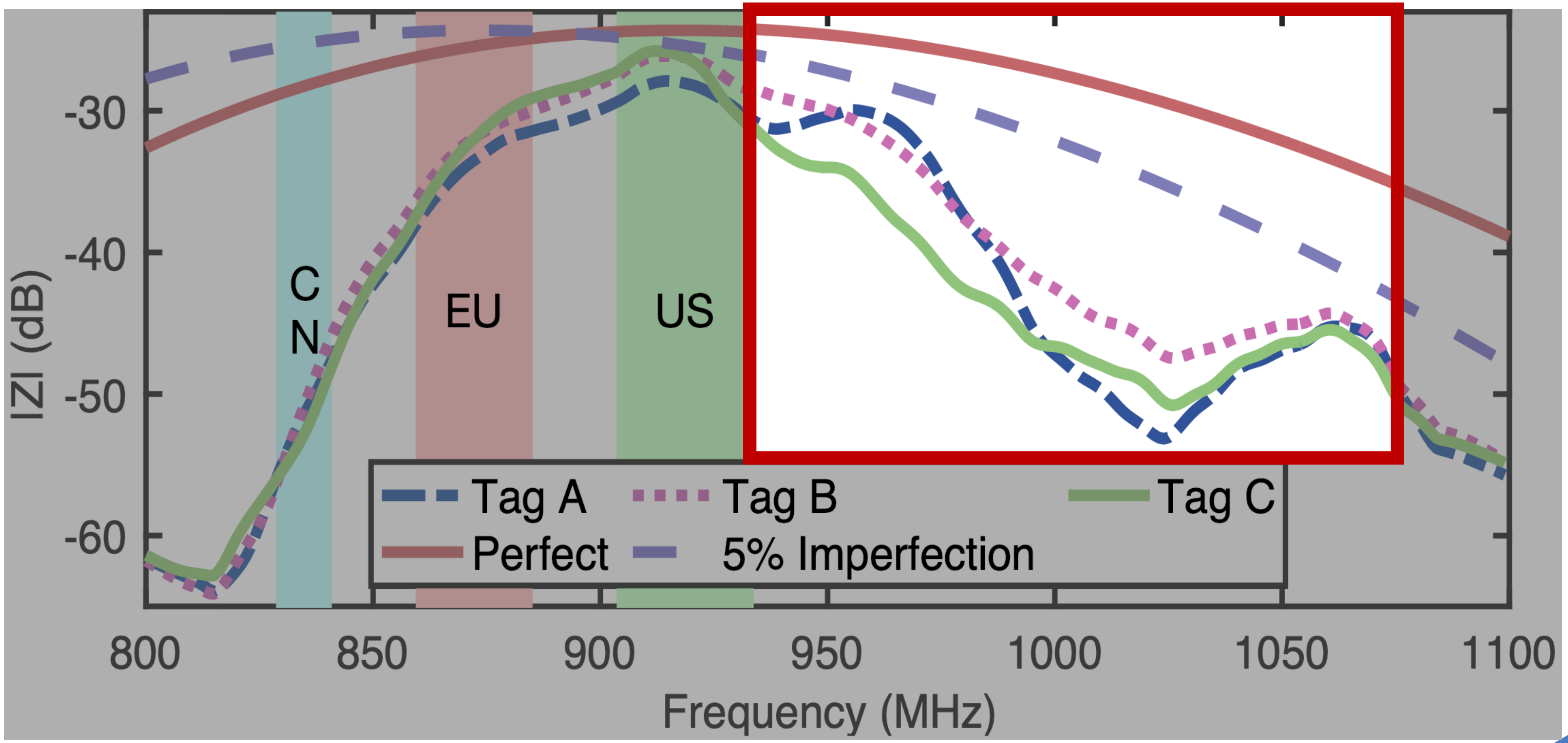
Frequency Agnostic Phenomenon

RFID Tags backscatter in both **in-band** frequencies and **out-of-band** frequencies



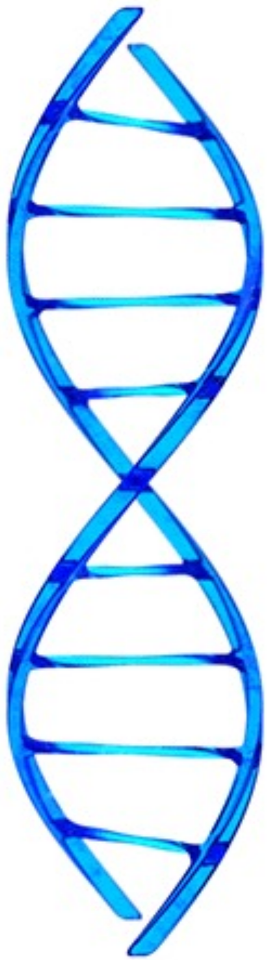
Frequency Agnostic Phenomenon

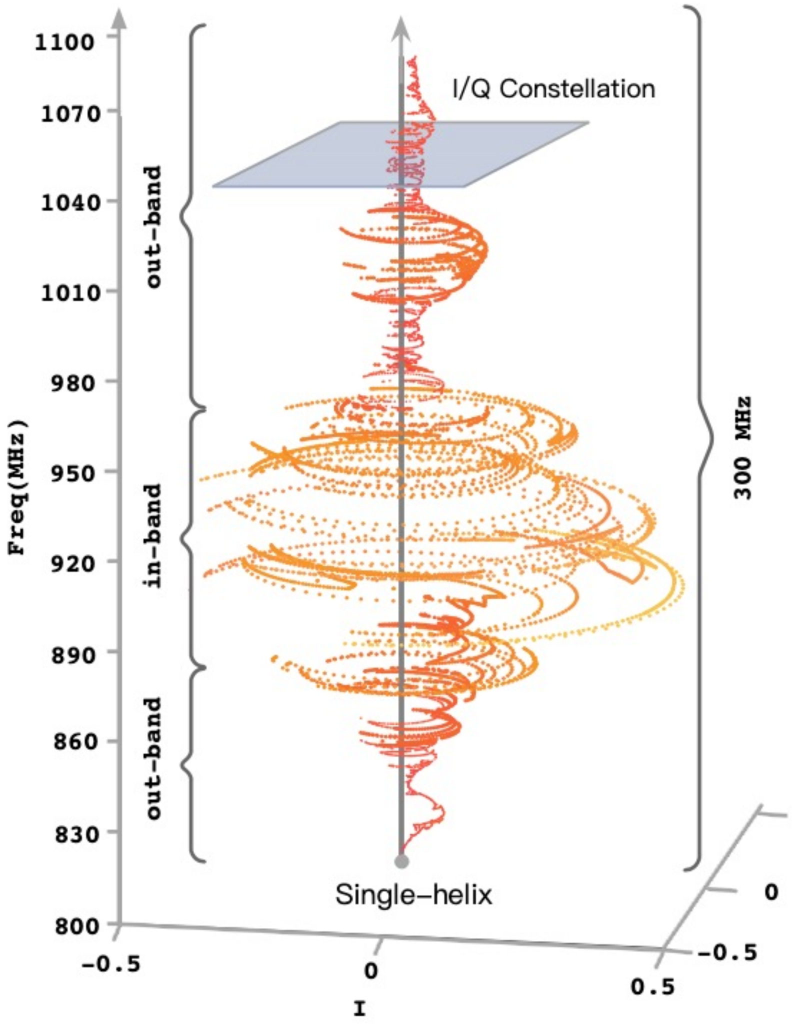
Out-of-band intrinsic responses are more **distinguishable** than intrinsic In-band responses.



RF-DNA

Bio-DNA

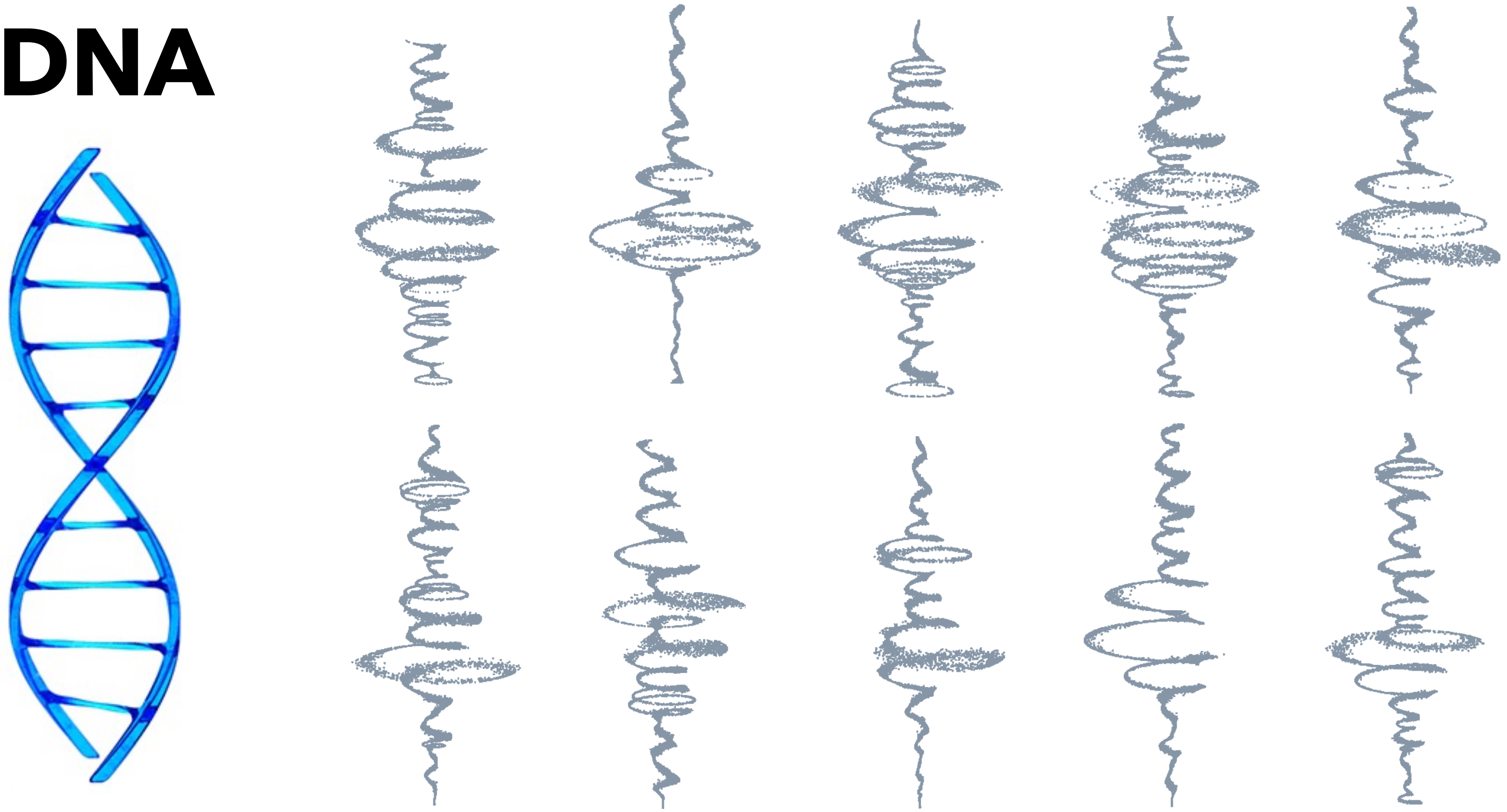




RF-DNA

RF-DNA: a chain of pairs of I and Q components of a tag's **intrinsic responses** challenged at 300 MHz wide band.

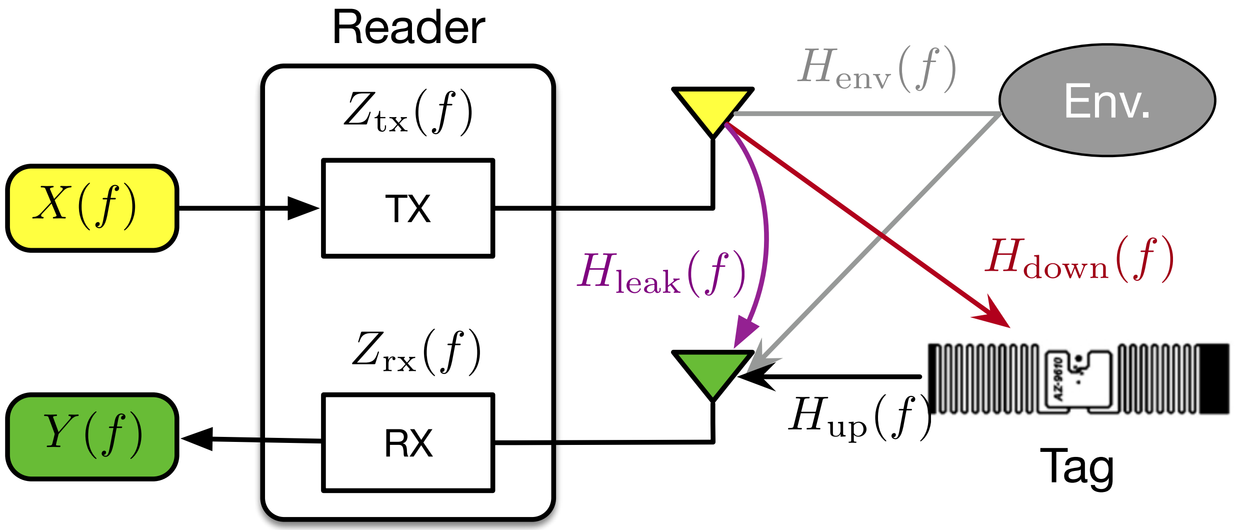
RF-DNA



Ten RF-DNA examples profiled from ten RFID tags with different models

Challenge 1: how to extract context-free intrinsic response?

Problem: tag response is NOT context-free!



Context involves:

- surrounding response
- distance
- transmission power
- self interference
- ……

Non-reflective: $Y_0(f) = X(f)Z_{tx}(f)\left(H_{leak}(f) + H_{env}(f)\right)Z_{rx}(f)$

Reflective: $Y_1(f) = Y_0(f) + X(f)Z_{tx}(f)H_{up}(f)Z_{tag}(f)H_{down}(f)Z_{rx}(f)$

Solution: Context-free DNA Extraction

Step 1

Eliminating impact of CW and reader

$$\xi(f) = \frac{Y_1(f) - Y_0(f)}{Y_0(f)} = \frac{\cancel{X(f)Z_{tx}(f)Z_{rx}(f)}H_{up}(f)Z_{tag}(f)H_{down}(f)}{\cancel{X(f)Z_{tx}(f)Z_{rx}(f)}(H_{leak}(f) + H_{env}(f))}$$
$$= \frac{H_{up}(f)H_{down}(f)}{H_{leak}(f) + H_{env}(f)} Z_{tag}(f)$$

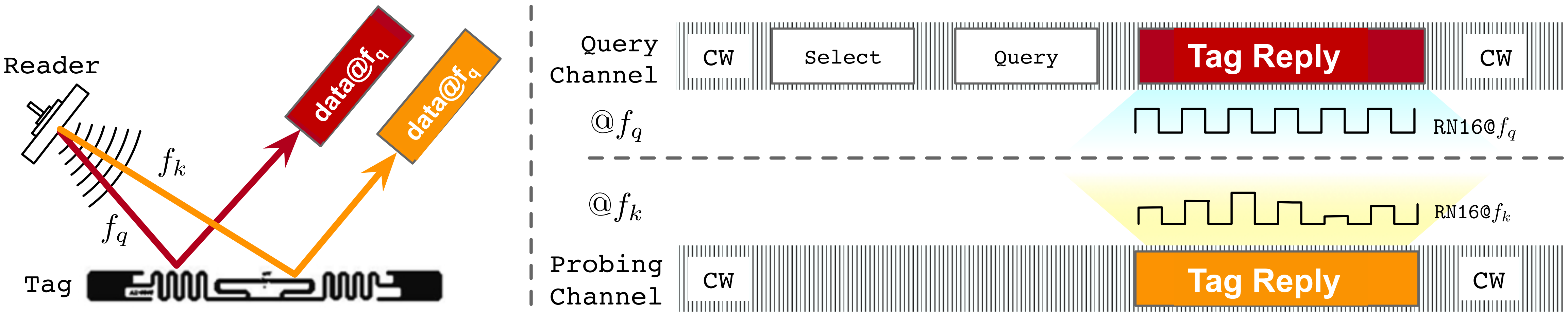
Step 2

Eliminating impact of path-related variables

$$\eta(f_k) = \frac{\xi(f_k)}{\xi(f_{k-1})} = \frac{Y_1(f_k) - Y_0(f_k)}{Y_1(f_{k-1}) - Y_0(f_{k-1})} \cdot \frac{Y_0(f_{k-1})}{Y_0(f_k)}$$
$$= \cancel{\frac{H_{up}(f_k)H_{down}(f_k)}{H_{leak}(f_k) + H_{env}(f_k)}} \cdot \cancel{\frac{H_{leak}(f_{k-1}) + H_{env}(f_{k-1})}{H_{up}(f_{k-1})H_{down}(f_{k-1})}} \cdot \frac{Z_{tag}(f_k)}{Z_{tag}(f_{k-1})}$$
$$\approx \frac{Z_{tag}(f_k)}{Z_{tag}(f_{k-1})}$$

Challenge 2: how to profile large-scale RF-DNAs instantly?

Problem: Single-tone Profiling is Time-consuming!

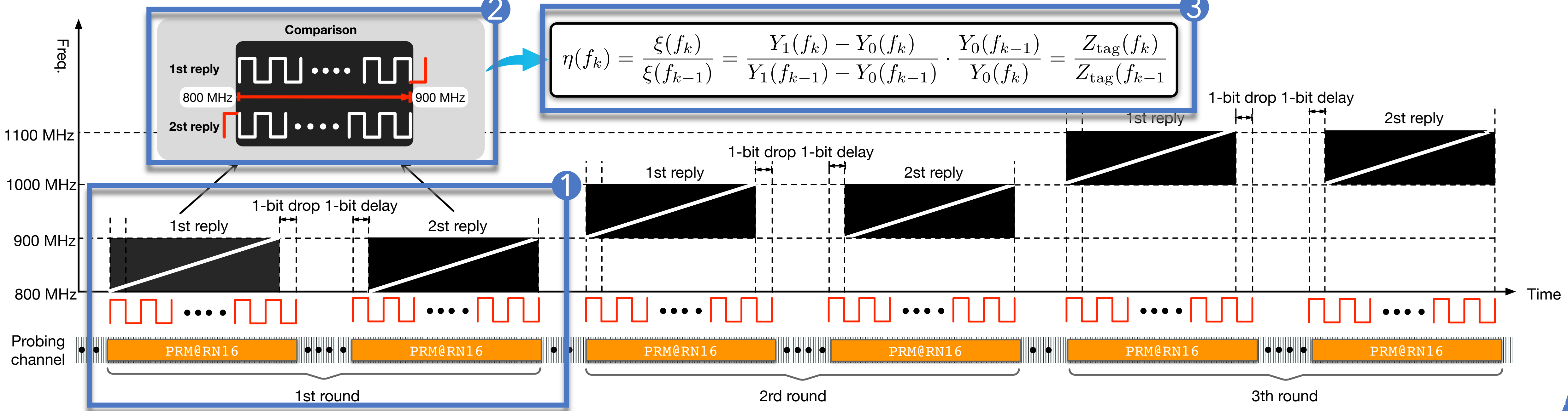


Two channels are utilized:

- The **query** channel: at in-band frequency f_q is to power up the tag
- The **probing** channel: at targeting frequency f_k to acquire the corresponding intrinsic response

It takes 6.7 hours to acquire 300MHZ response for each single tag!

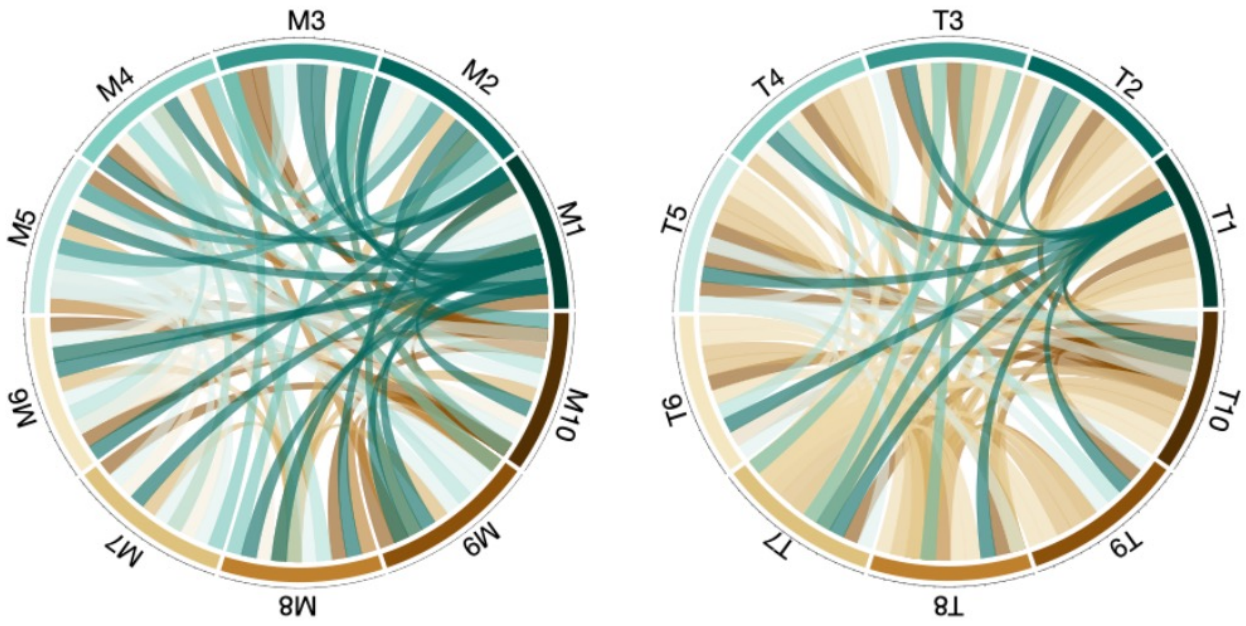
Solution: Chirp-based Profiling



- Profiling RF-DNA across 300MHz in six times by sending **chirp** in probing channel
- Time cost turns **from 6.7 hours to 120.4 ms**

Challenge 3: how to **match** RF-DNAs with RFIDs?

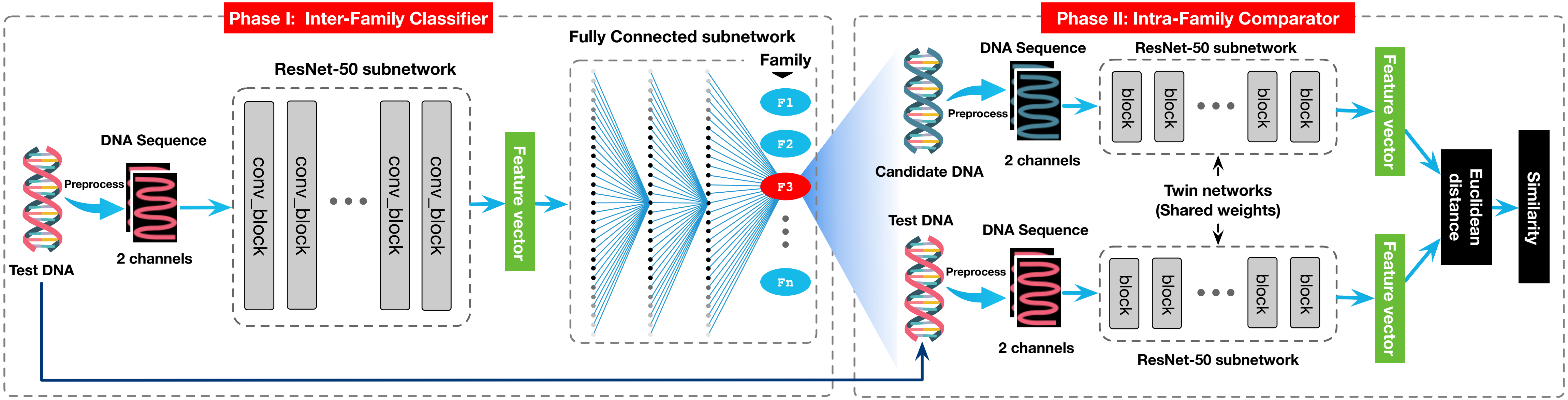
Problem: Similarity is Hierarchical!



(a) Inter-family (b) Intra-family

RF-DNAs from **different families** are much more **distinguishable** than those from the same family

Solution: Two Phase Neural Networks



- **(Phase I) Inter-Family Classifier:** To classify a DNA sequence into a model-based group called family by **RestNet-50** network followed by a three-layer **fully connected network**
- **(Phase II) Intra-Family Classifier:** To discriminate a tag from others in the same family by the popular neural network called **siamese network** which aims to compute the similarity of two inputs

Implementation & Evaluation

Implementation

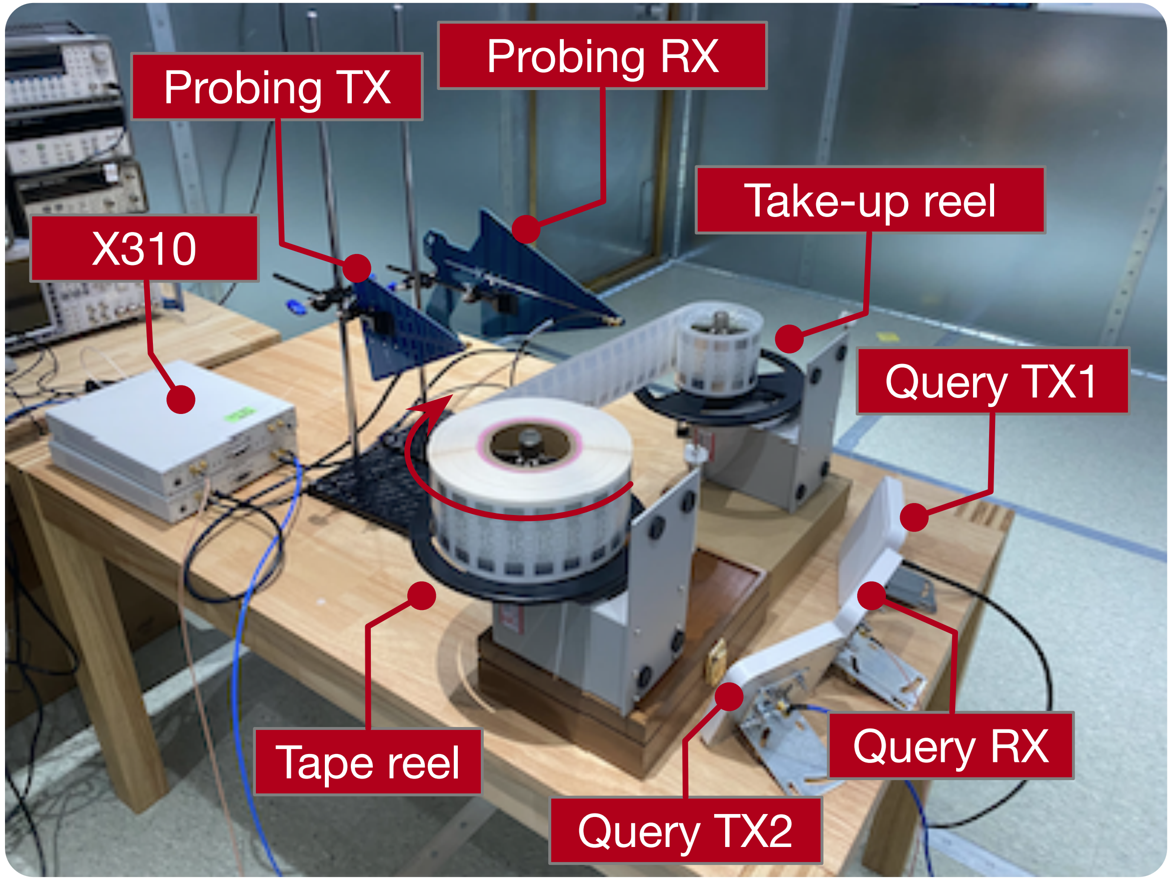
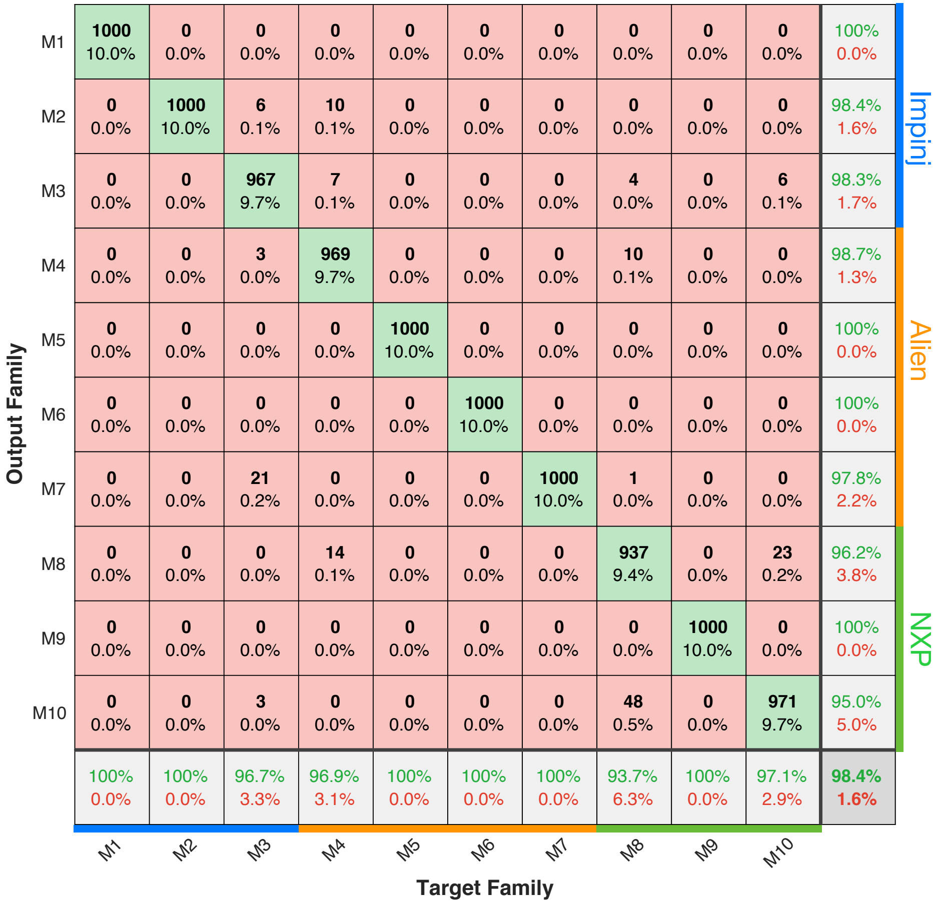


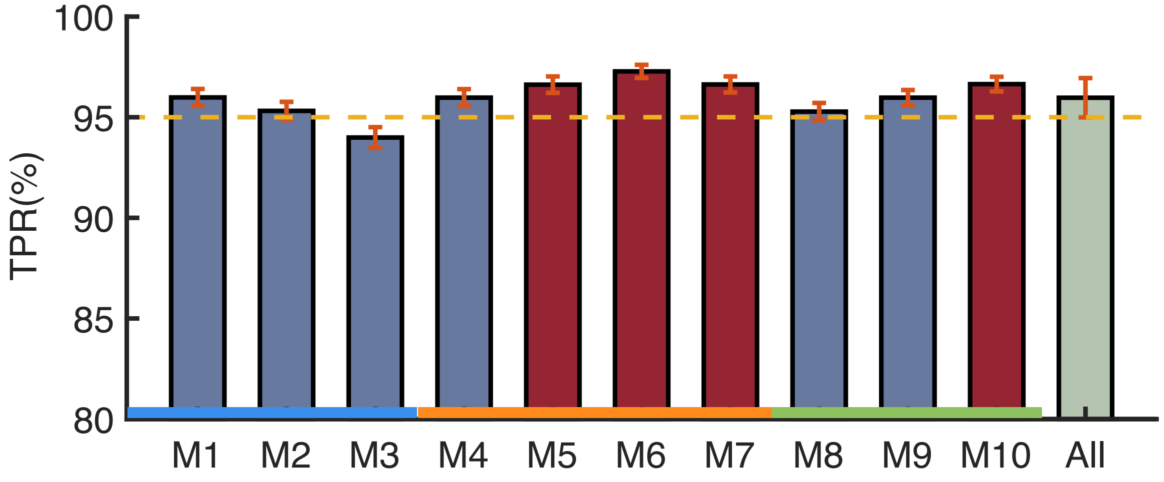
Table 2: Collected Tags

#	MFR.	IC	Model	Size(mm^2) .	AMT.
M1		Monza 4QT	H47	50×50	2000
M2	Impinj	Monza R6	ER62	74×18	2000
M3		Monza R6	AZ-H63	49×114	2000
M4		Higgs 3	9662	70×17	1000
M5	Alien	Higgs 3	9640	94.8×8.25	2000
M6		Higgs 3	9654	93×19	1000
M7		Higgs 9	9962	73.5×20.2	1000
M8		Ucode8	U9627	96×27	2000
M9	NXP	UR108	U7015	70×15	2000
M10		Ucode7	U5030	50×30	1000

Evaluation: Inter/Intra-family classification



Confusion Matrix of Inter-Family Classification
(98.4% Precision)



Intra-Family Recognition
(96.0% overall TPR)

Conclusion

- First introducing the **out-of-band backscatter response** as a powerful hardware **fingerprint** for the physical-layer identification of RFID tags
- Developing a novel **context-free extraction algorithm** to acquire RF-DNA from tags in real-world environments
- Taking advantage of two-phase **deep neural networks** and fully exploit the hidden information of RF-DNA
- Successfully extending the capability of physical layer identification to **ten thousands of tags** for the first time

Q & A

Thank you!