THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

IEEE SECON™

Revisiting Backscatter Frequency Drifts for Fingerprinting RFIDs: A Perspective of Frequency Resolution

Qingrui Pan, Zhenlin An, Xiaopeng Zhao, Lei Yang

Department of Computing, The Hong Kong Polytechnic University

Department of Computing
電子計算學系

RFID in Daily Life

Retail and Inventory Management

RFID technology assists in accurately tracking goods, enhancing supply chain efficiency and reducing theft.

Transportation and Logistics

RFID is employed for seamless fare transactions in public transportation and real-time package tracking during shipment.

Healthcare and Medical Field

RFID aids in locating equipment, managing supplies, monitoring patients, and ensuring accurate patient-medication matching

Security and Identification

RFID serves a crucial role in providing data storage, passports, and enabling access control, as well as pet identification.

RFID is Everywhere

$12.8B

The Global RFID Market Worth In 2022

$14B

Predicted Global RFID Market Worth In 2023

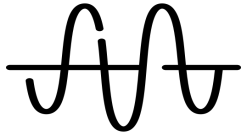
$39.3B

Predicted Number of Sold Passive RFID Tags

Contrasting Its Prevalence,

RFID’s Simplicity Causes Vulnerability

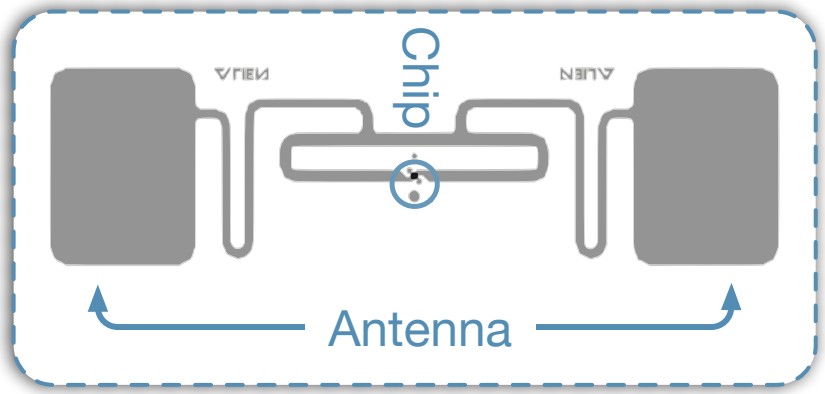
Reader



Tag

Contrasting Its Prevalence,

RFID's Simplicity Causes Vulnerability



- Consist of only Antenna and Chip
- Limited Power and Computation

First Choice,

Protocol-Based Solution

- **Cryptographic protocols** are **not practical** for the limitation of power and computation
- Industry prefers straightforward **Authentication Protocols**, vulnerable to **counterfeiting** attacks

Second Choice,

Hardware Fingerprint

Second Choice,

Hardware Fingerprint

RF Frontend

- Average baseband power *(Danev,2012)*
- Minimum activated power *(Periaswamy, 2010)*
- …

Capacitor

- Persistence Time *(Chen, 2020)*
- …

Clock Drift

- Backscatter Frequency Drift *(Zanetti, 2010)*
- …

Second Choice,

Hardware Fingerprint

RF Frontend

- Average baseband power *(Danev,2012)*
- Minimum activated power *(Periaswamy, 2010)*
- …

Capacitor

- Persistence Time *(Chen, 2020)*
- …

Clock Drift

- **B**ackscatter **F**requency **D**rift *(Zanetti, 2010)*
- …

Advantage

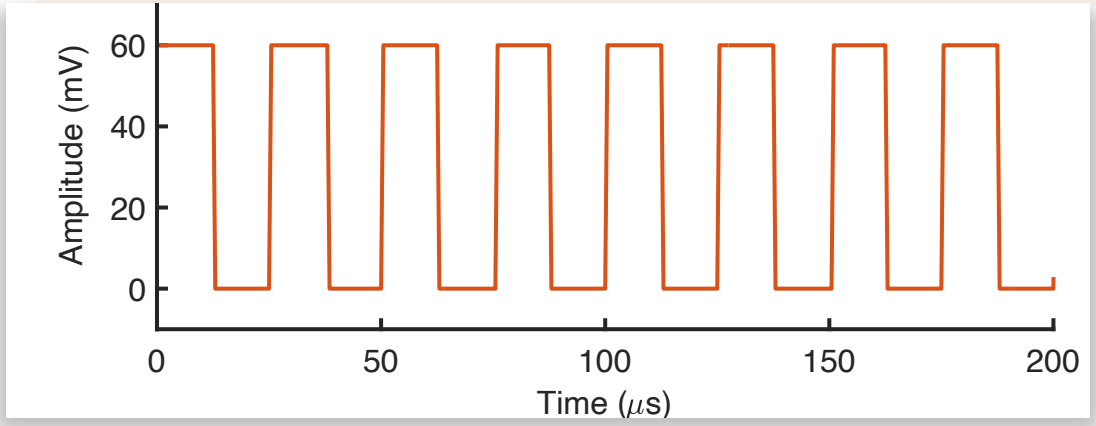
- **Versatility** - Stable across diverse RF systems
- **Robustness** - Resilient to environmental factors; no extra elimination required
- **Tolerance** - Functions even with less intactness than traditional RF-related fingerprints

What is **BFD**?

(Backscatter Frequency Drift)

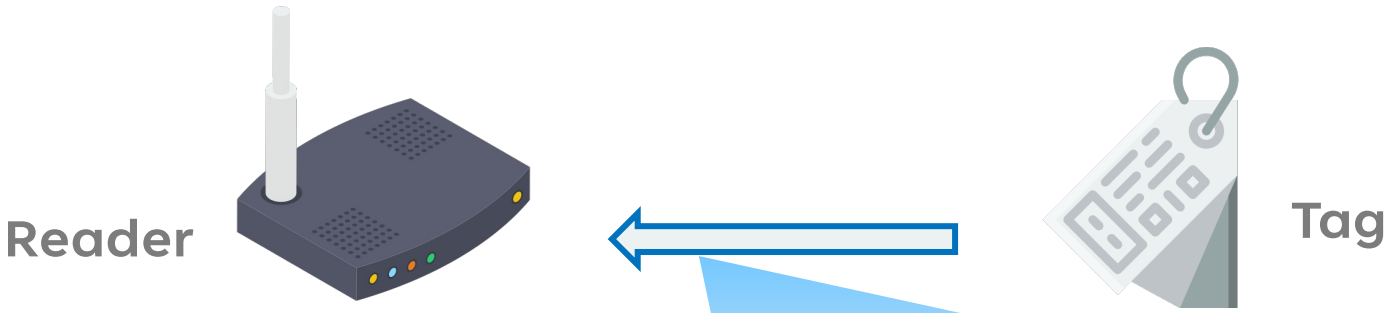
BFD: Backscatter Frequency Drift

Ideal Clock



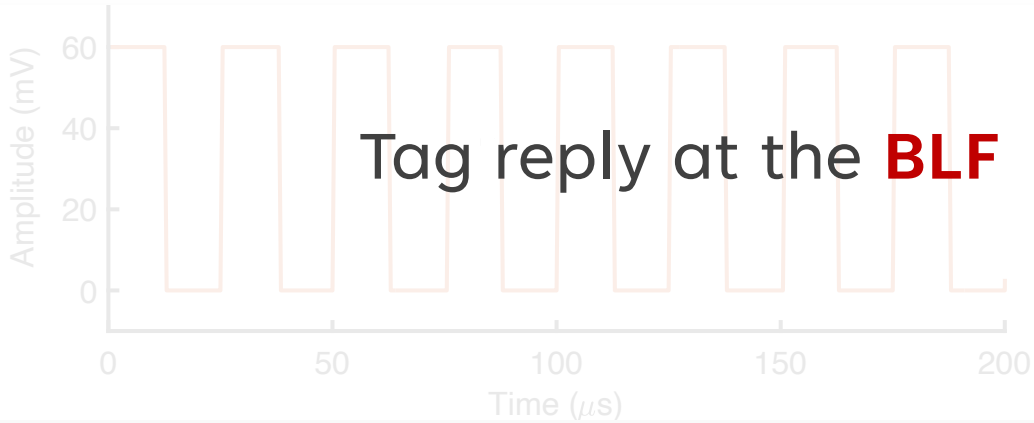
Request tag to reply at a **B**ackscatter **L**ink **F**requency

BFD: Backscatter Frequency Drift

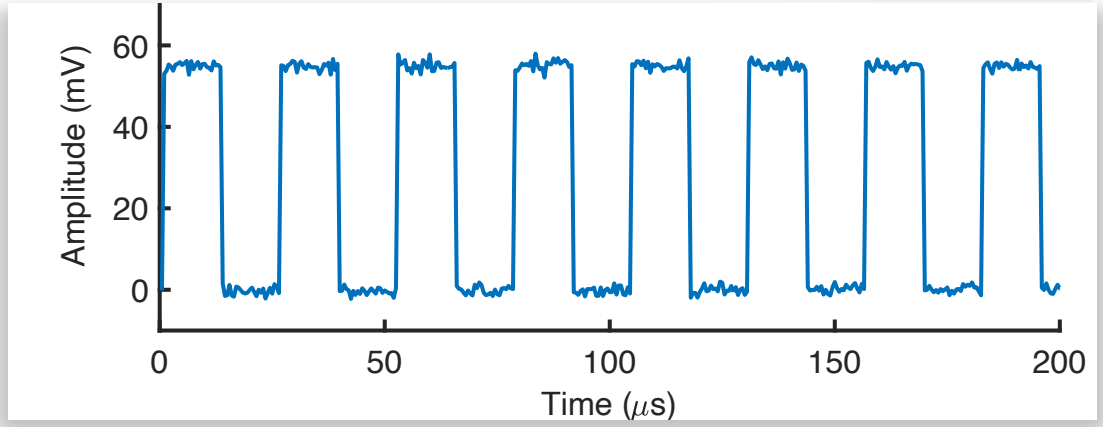


Ideal Clock

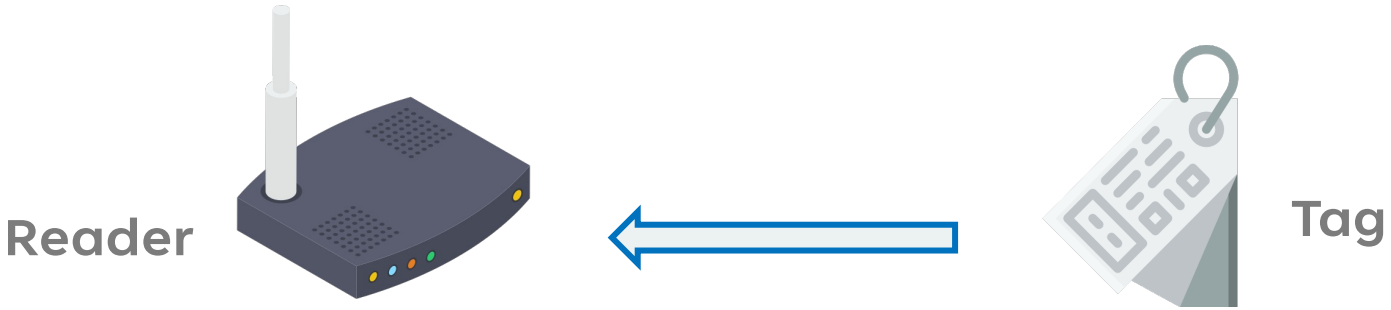
Actual Signal



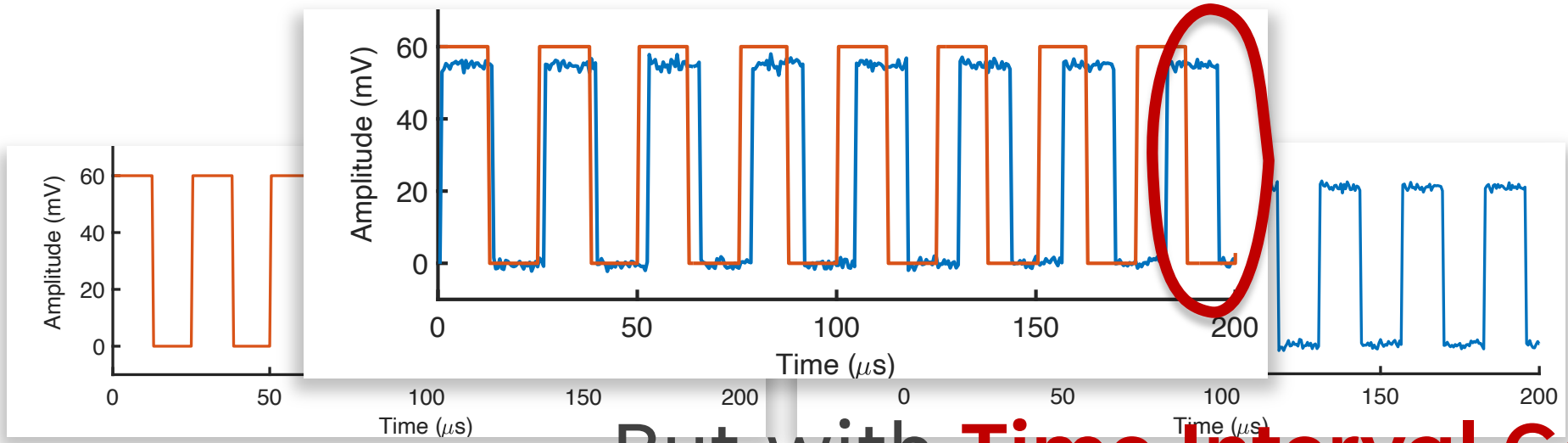
Tag reply at the **BLF**



BFD: Backscatter Frequency Drift

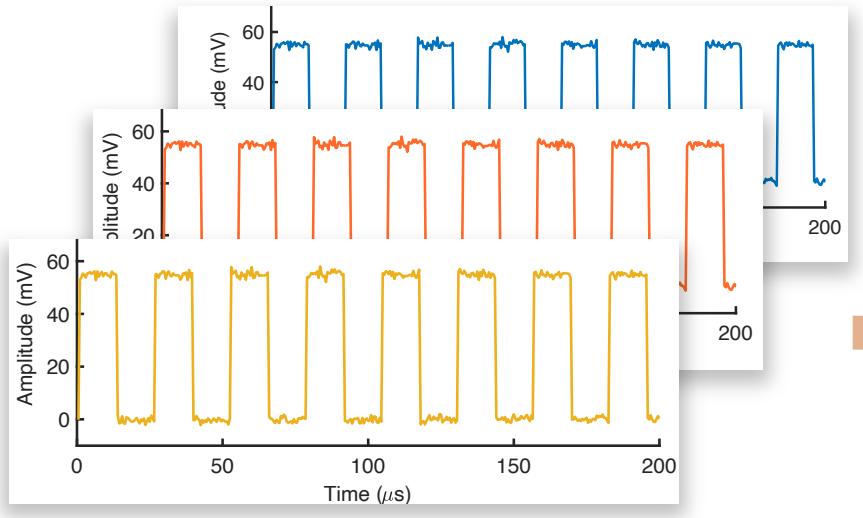


Tag reply at the **BLF ,**

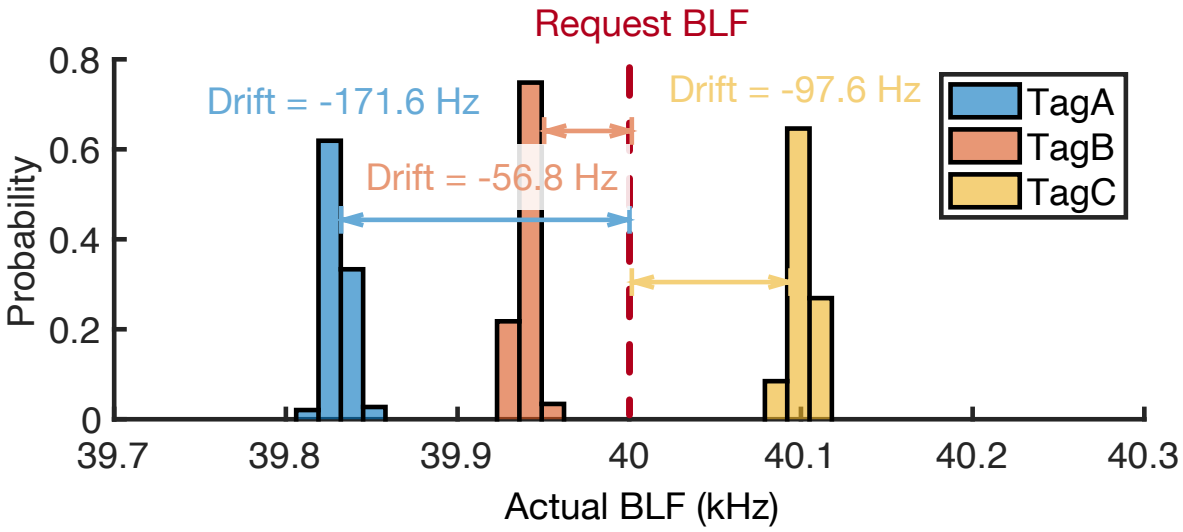


But with **Time Interval Gap !**

Time Domain to Frequency Domain

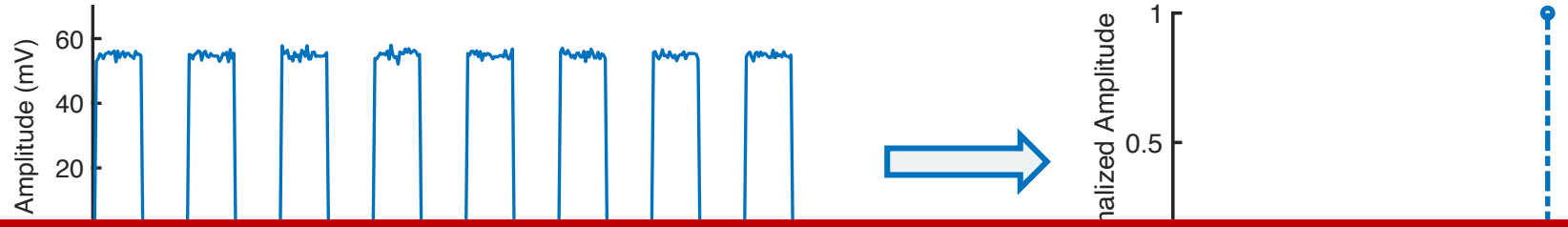


FFT



- BFD can be measured on frequency domain by FFT
- BFD is Unique and suitable for fingerprinting tags

Revisiting BFD from a **Resolution** Perspective



Frequency Resolution = **1.25 kHz**

BFD Bandwidth = **281.6 kHz**

281.6 kHz/1.25kHz ≈ **225 tags at most**

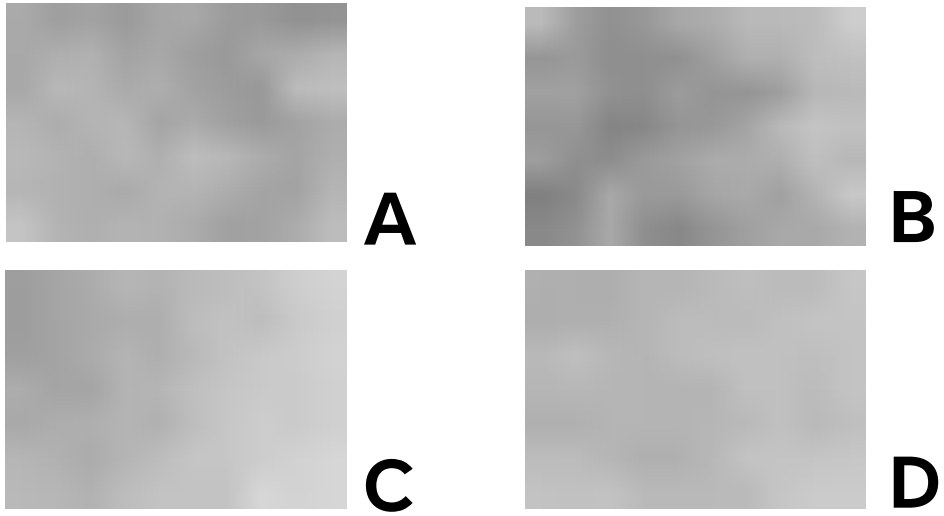
Resolution $\boxed{\mathcal{R}} = \dfrac{\boxed{f_s}}{\boxed{N}}$

f_s: Sampling rate

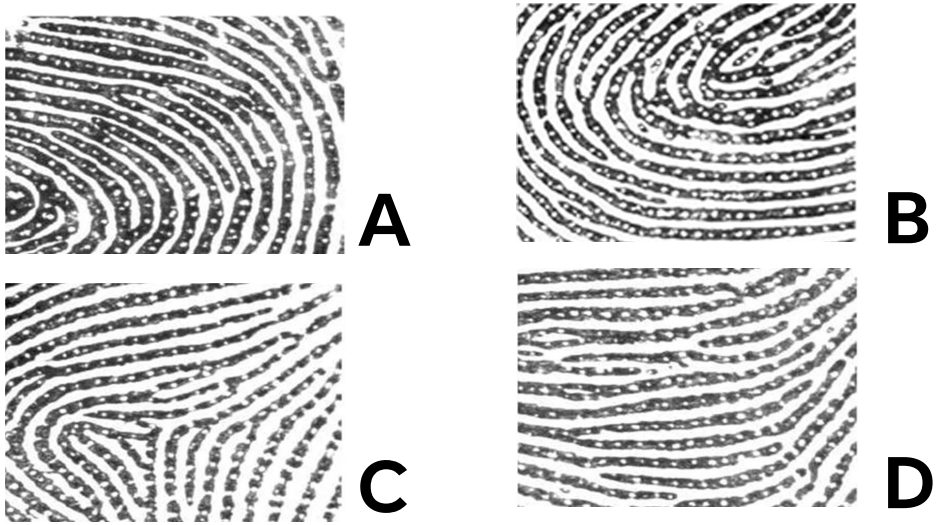
N: Number of Samples

Look into a similar problem

Low-Resolution (10x7 pixels)



High-Resolution (1,000x700 pixels)



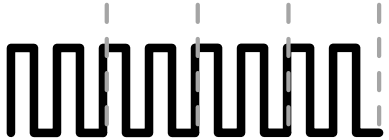
Solution:

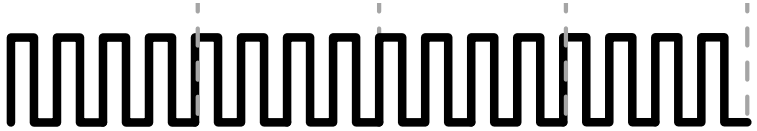
Acquiring Ultra-High-Resolution BFDs

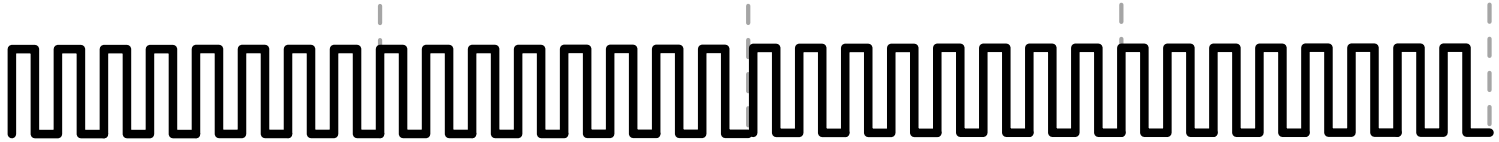
Measure 1: Increase Symbol Number **M**

Using longer Miller Code

$$\mathcal{R} = \frac{f_s}{N\uparrow} = \frac{f_b}{M\uparrow}$$

m=2  **2** symbols each sequence

m=4  **4** symbols each sequence

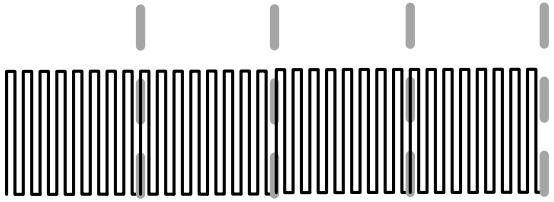
m=8  **8** symbols each sequence

Measure 1: Increase Symbol Number **M**

Using longer Preamble (Pilot Tone)

$$\mathcal{R} = \frac{f_s}{N\uparrow} = \frac{f_b}{M\uparrow}$$

m=8

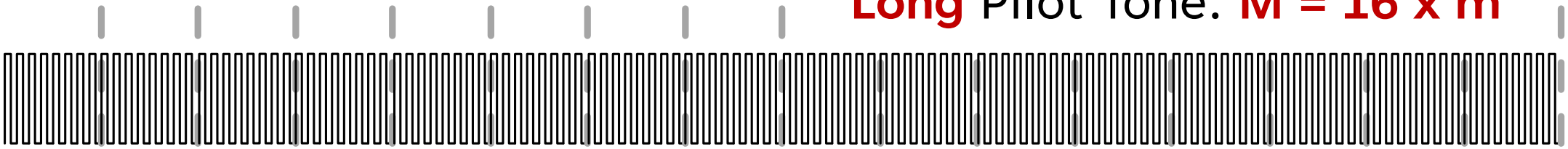


Short Pilot Tone:

M = 4 x m

Long Pilot Tone: **M = 16 x m**

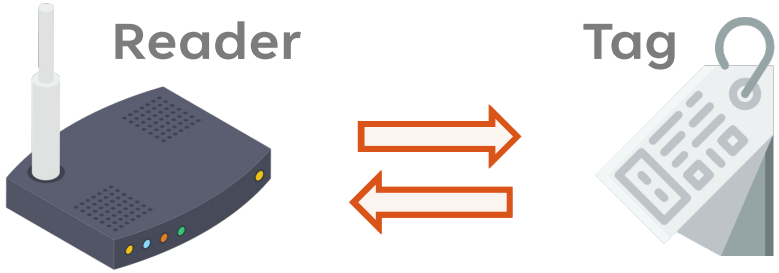
m=8

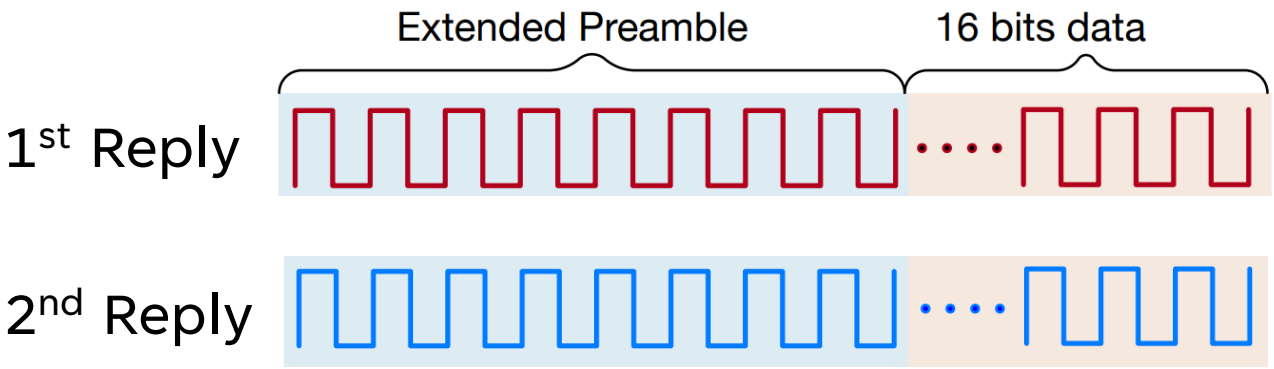


Resolution improved by **16 x** in total.

Measure 2: Increase by Redundancy **R**

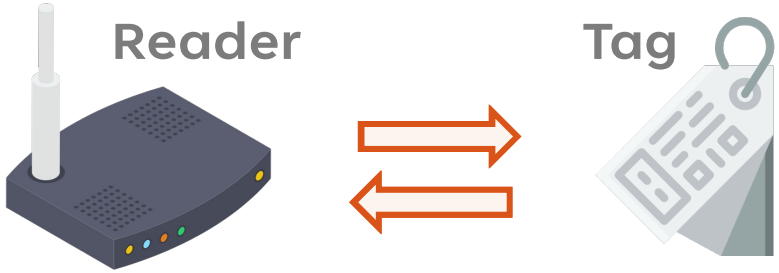
Redundant Replies

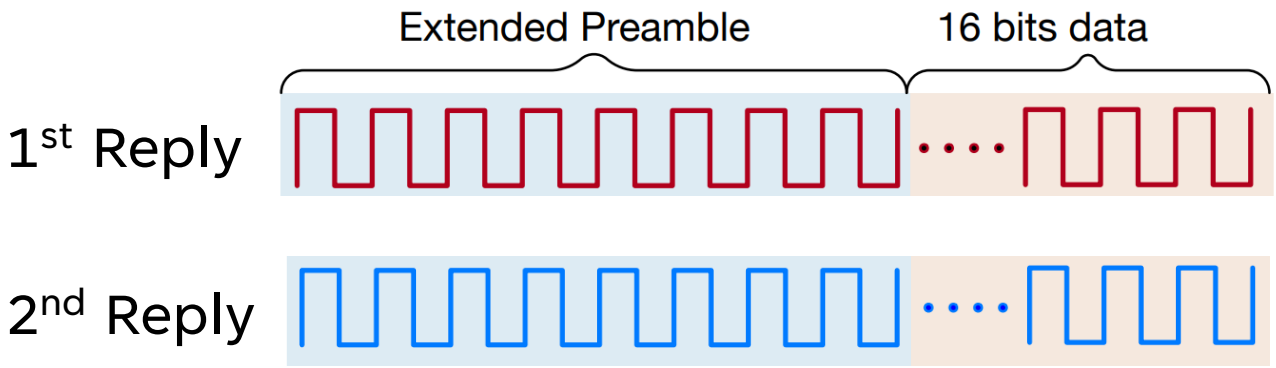


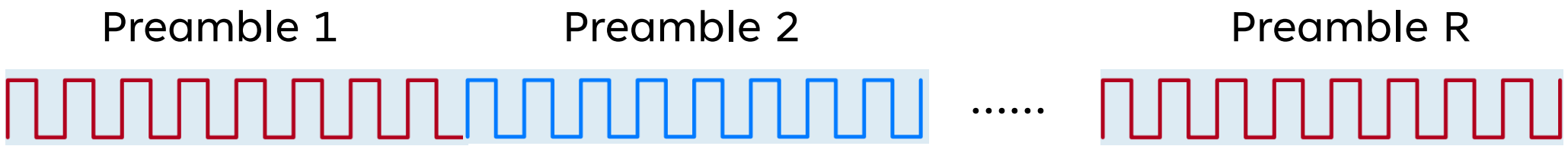


Measure 2: Increase by Redundancy **R**

Redundant Replies



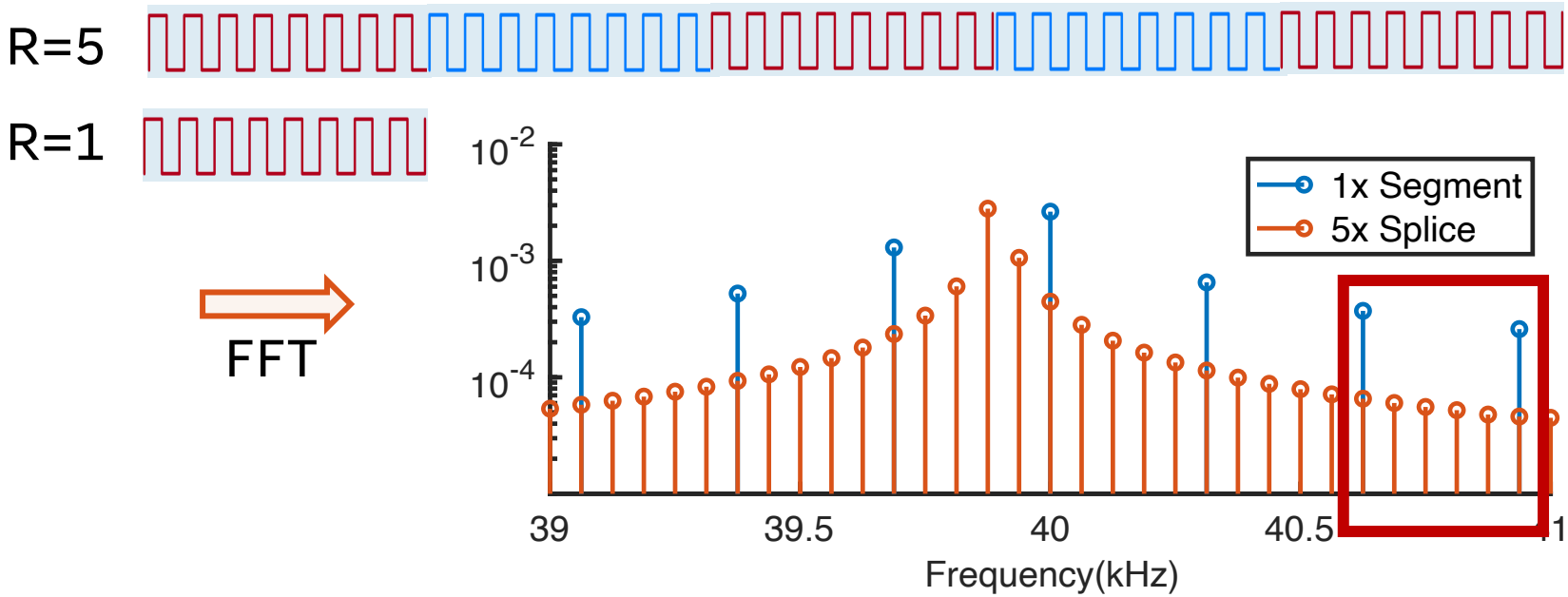




By concatenating **R** segments of the signal, we obtain an FFT input with **R times** the **length**, **Resolution** improved by **R times**.

Measure 2: Increase by Redundancy **R**

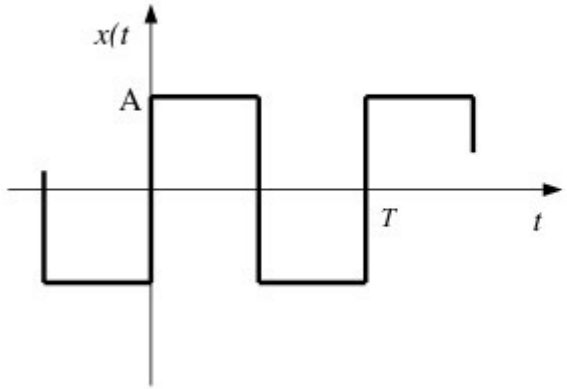
Redundant Replies

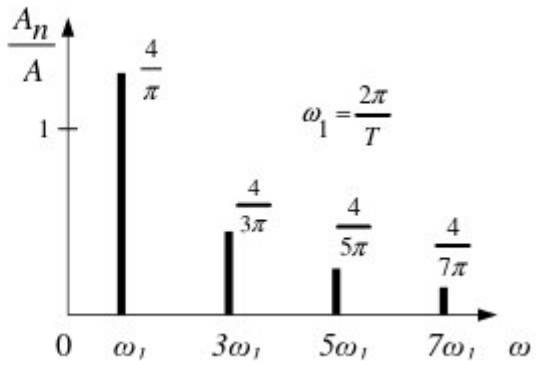


Resolution improved by **R=5** times

By concatenating **R** segments of the signal, we obtain an FFT input with **R times** the **length**, **Resolution** improved by **R times**.

Measure 3: Increase by Harmonics **K**



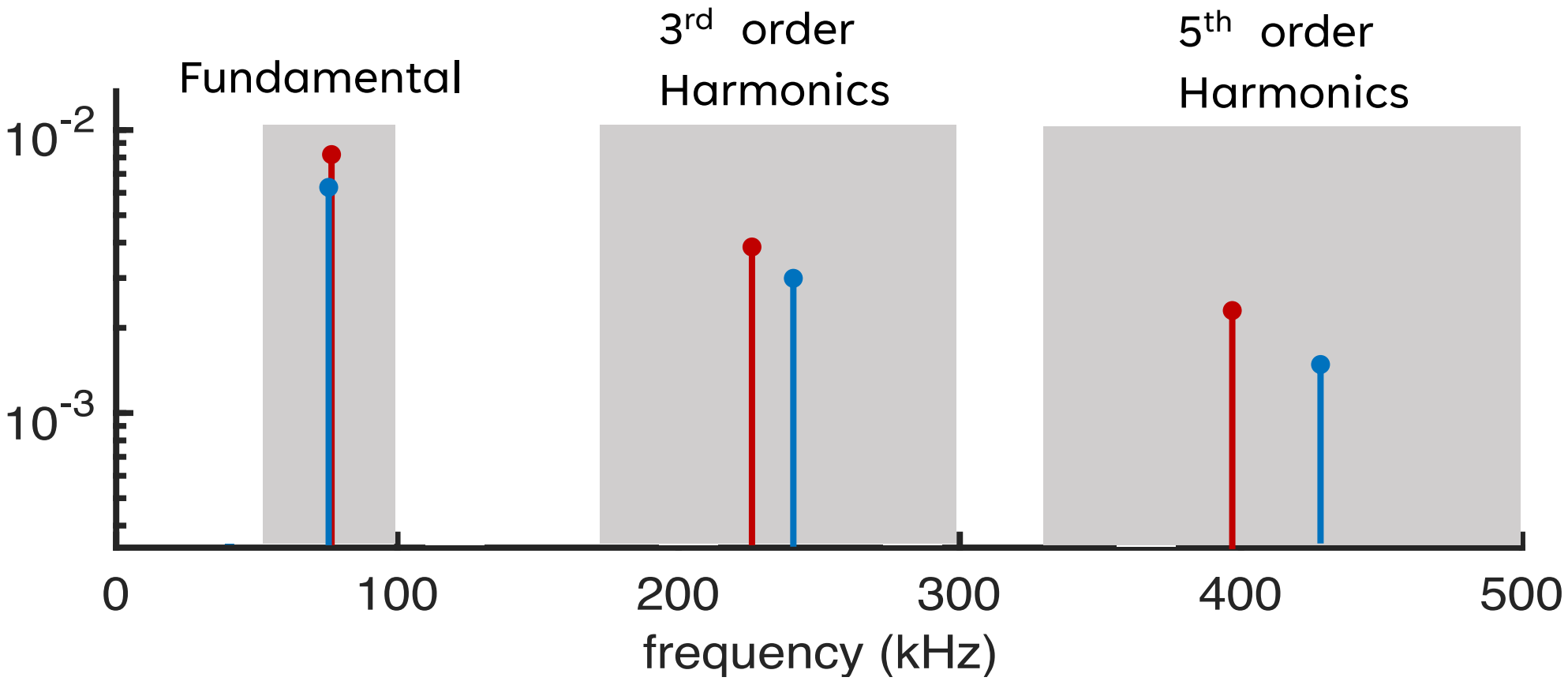


Square wave Taylor expansion:

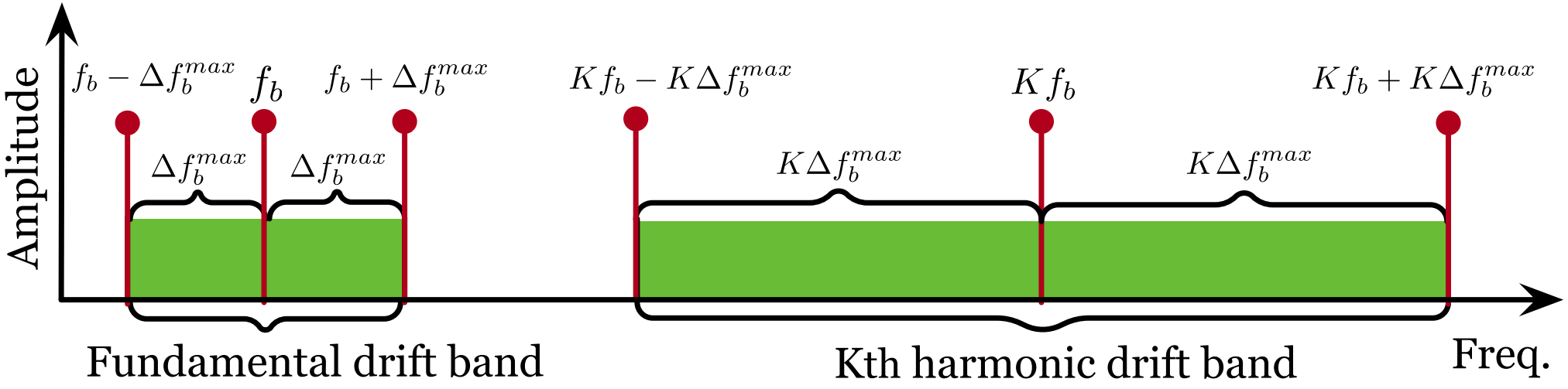
$$x(t) = \frac{4}{\pi} \sum_{k=1}^{\infty} \frac{\sin(2\pi(2k-1)f_b t)}{2k-1}$$

$$= \frac{4}{\pi} \left(\underbrace{\sin(2\pi f_b t)}_{\text{Fundamental}} + \frac{1}{3} \underbrace{\sin(2\pi 3 f_b t)}_{\text{3rd-order}} + \frac{1}{5} \underbrace{\sin(2\pi 5 f_b t)}_{\text{5th-order}} + \cdots + \frac{1}{11} \underbrace{\sin(2\pi 11 f_b t)}_{\text{11th-order}} + \cdots \right)$$

Measure 3: Increase by Harmonics **K**

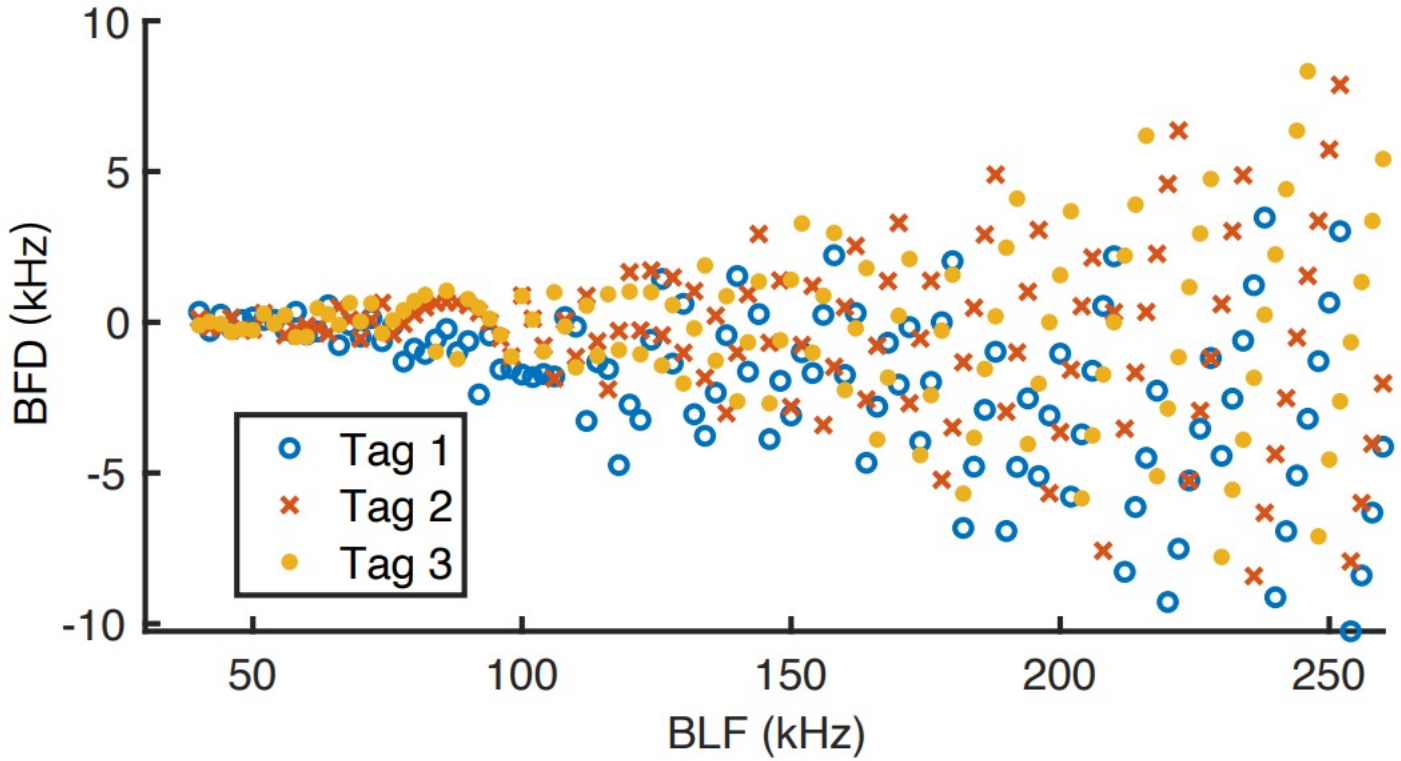


Measure 3: Increase by Harmonics **K**



The **bandwidth** of BFD increases by **K x** wider at the Kth Harmonics

Measure 4: Increase by Multi-frequency **W**



BLF drifts from **40 kHz to 260 kHz** acquired from three commercial RFID tags

Suppose we acquire W BLF drift results at the **W** BLFs as follows:

$$\{\mathcal{D}(f_1), \mathcal{D}(f_2), \cdots, \mathcal{D}(f_W)\}$$

Measure Summary

$$\text{Resolution} = \frac{f_b}{M \cdot R \cdot K \cdot W}$$

M: Number of symbols

R: Multiples of redundancy

Resolution: 1250 Hz → 0.272 Hz (4590×)

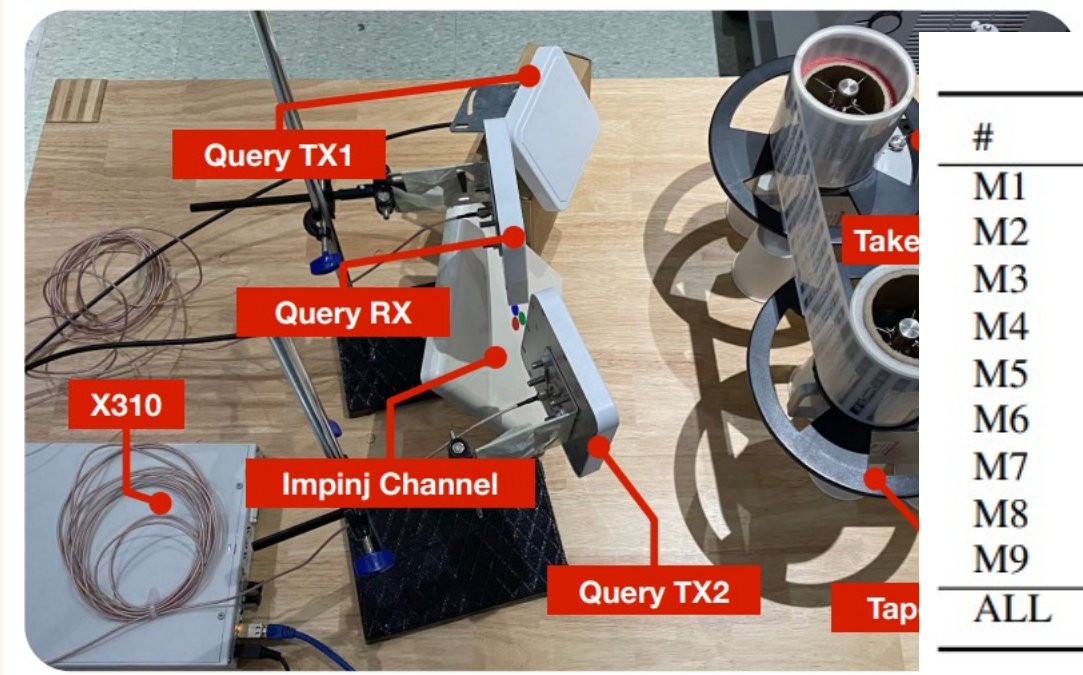
S0	32	1	1	1	$1250 \sim 20,000$	6	0.167	10
S1	32	1	1	10	$125 \sim 2000$	64	1.6e-2	10
S2	128	1	1	10	$31.25 \sim 500$	256	3.9e-3	10
S3	128	5	1	10	$6.25 \sim 100$	1280	7.8e-4	50
S4	128	5	23	10	$0.272 \sim 4.3478$	29440	3.40e-5	50

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Implementation & Evaluation

Implementation

Auto Acquisition System

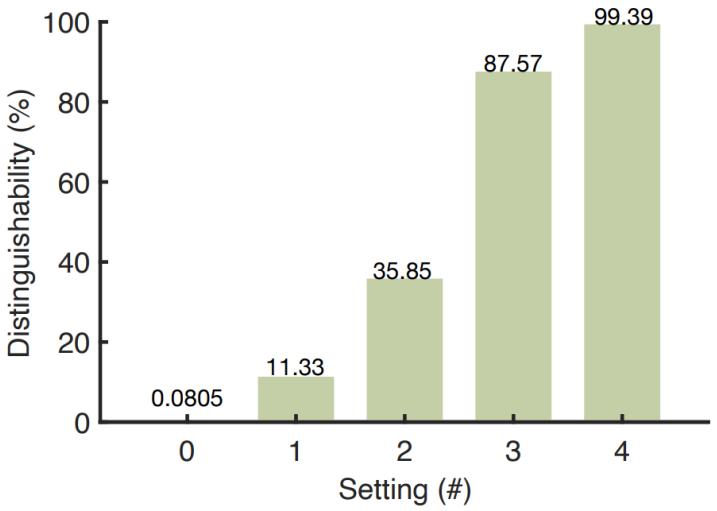


RFID Tags

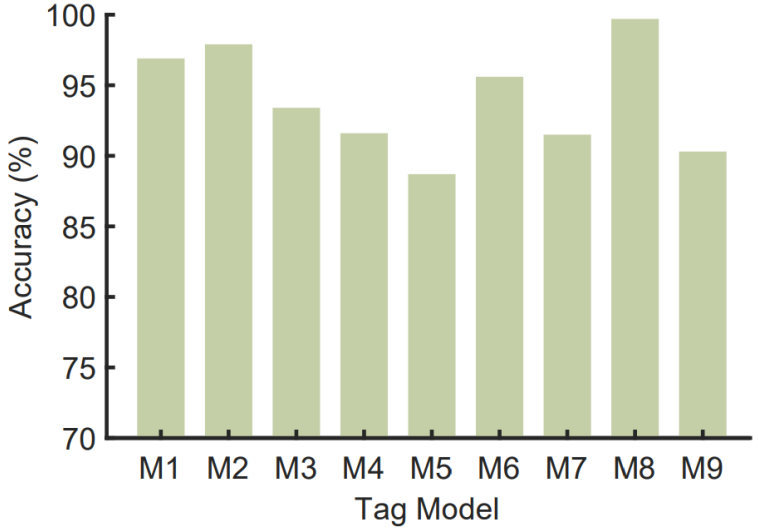
TABLE III: Collected Tags

#	MFR.	IC	Model	Size(mm^2)	AMT.
M1	Alien	H3	9662	73.5×20.2	1161
M2	Alien	H9	9954	96×23	615
M3	Impinj	Monza R6	AZ-H63	49×114	746
M4	Impinj	Monza 4	H47	50×50	880
M5	Impinj	Monza R6	ER62	74×18	1025
M6	Impinj	Monza 4-QT	C90G	97×28	596
M7	NXP	U8	U7015	70×15	881
M8	NXP	U8	C95U	98×12	336
M9	NXP	U8	UR108	70×15	895
ALL					7135

Evaluation: Distinguishability & Accuracy



Distinguishability



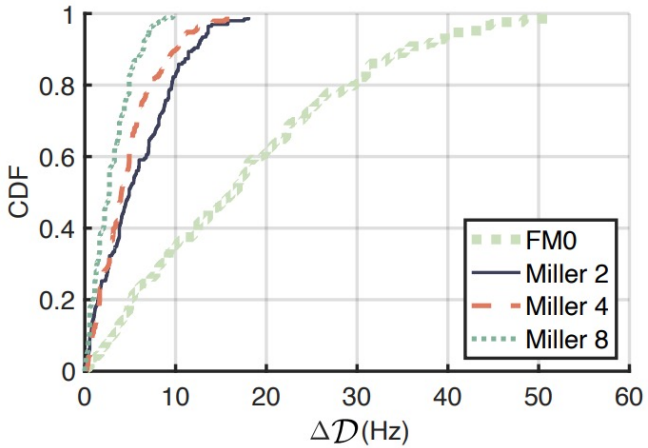
Accuracy

- The percent of unique BFD fingerprints
- the distinguishability is increased to **99.39%** in setting #4

- Mean accuracy of **94%** with std of 3% across all models

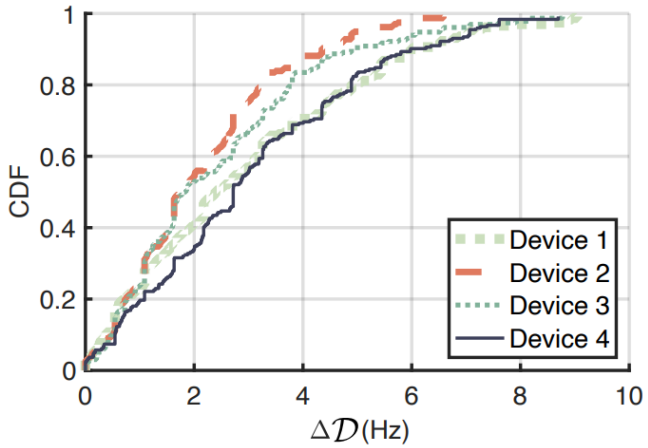
Evaluation: Impact Analysis

Encoding



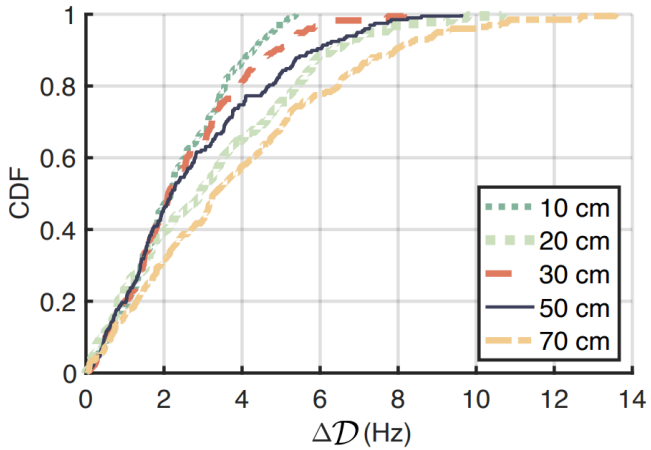
- Miller 4 and Miller 8 perform better than other schemes for more Miller cycles

Device



- Acquisition devices have little impact

Distance



- Distance is increased, the SNR decreases
- More difficult to distinguish harmonics from noise

Conclusion

- Revisiting BFD as a practical fingerprint from the perspective of **resolution**
- Introducing methods to enhance frequency **resolution** from kHz to **sub-Hz** using only time as a trade-off
- Evaluating the fingerprints on **7,000+ tags** under diverse acquisition contexts

Thank You

Q & A