# Eavesdropping Near Field Contactless Payments: A Quantitative Analysis

Thomas P. Diakos[1] Johann A. Briffa[1] Tim W. C. Brown[2]
Stephan Wesemeyer[1]

[1]Department of Computing, University of Surrey, Guildford

[2]Centre for Communication Systems Research, University of Surrey, Guildford

Computer Laboratory, University of Cambridge, January 21, 2014

UNIVERSITY OF SURREY

# Outline



UNIVERSITY OF SURREY

# Near Field Communications

## Near Field

- Distance $\ll$ Wavelength ($\approx$ 22m)
- HF 13.56 MHz radio inductive coupling
- H-fields
- Reader and tag (passive)
- Short ('from a touch to a few cm') range of operation

## NFC devices

- Reader and tag on the same device
- Power on-board

# Near Field Communications

## Near Field Contactless Payments

- Marketed as ideal for quick, convenient transactions
- Contactless Cards and NFC devices
- 23 million cards in the UK alone
- 13.32% of smartphones equipped with NFC

# Near Field Communications

## Near Field Contactless Payments

- Marketed as ideal for quick, convenient transactions
- Contactless Cards and NFC devices
- 23 million cards in the UK alone
- 13.32% of smartphones equipped with NFC

## What's the catch?

'Because the transmission range is so short, NFC-enabled transactions are inherently secure.'

`http://nfc-forum.org/what-is-nfc/nfc-in-action/`

UNIVERSITY OF SURREY

# Motivation

## Eavesdropping - Chosen attack

- Why eavesdropping?

# Motivation

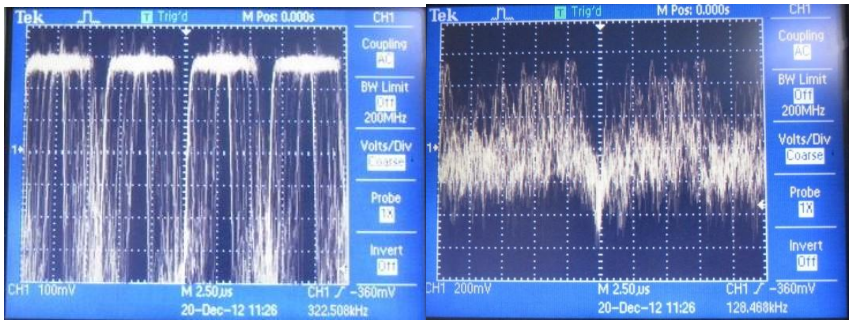
## Eavesdropping - Chosen attack

- Why eavesdropping?
- 'Inherently' secure?
- Difficult to defend against
- 'Contact world' heritage

# Motivation

## Eavesdropping - Past work

- Expensive, cumbersome equipment
- No control over transmit power
- Traces on a scope?




## Our contribution

UNIVERSITY OF SURREY

# Motivation

## Eavesdropping - Past work

- Expensive, cumbersome equipment
- No control over transmit power
- Traces on a scope?

## Our contribution

- Relatively inexpensive, inconspicuous equipment
- Varying Magnetic field strength
- Quantitative analysis

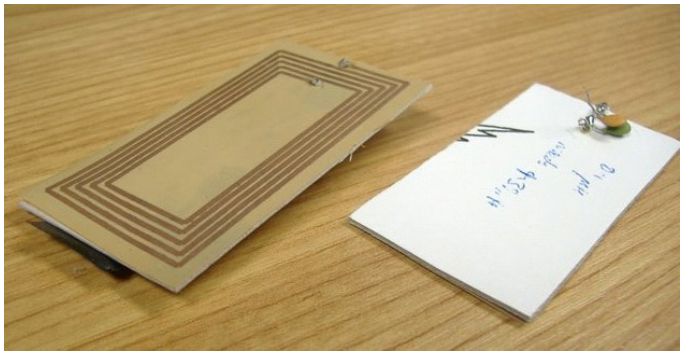
## Design Factors

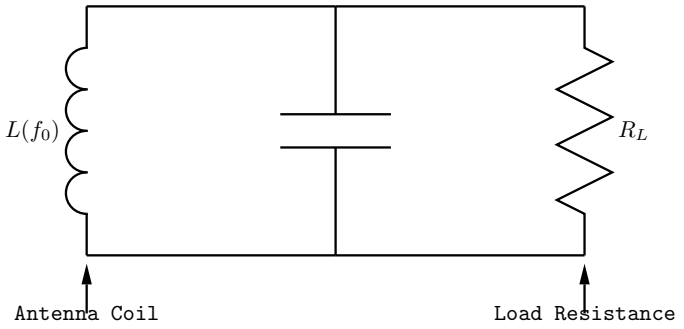
### The ideal eavesdropping antenna

- Maximise SNR
- Resonance
- Suitable Q factor
- Impedance matched

# NFC antenna design principles

## Ideal H-antenna






- H-field antenna
- $L$ constant
- $R$ (DC) negligible

# NFC Antenna Design Principles

## H-Antenna Receiver Mode

- In RX mode:

$$\frac{V_L}{V_{in}} = \frac{1}{1 + \frac{j\omega L(\omega)}{R_L} - \omega^2 LC} \tag{1}$$

- At resonance:

$$\frac{V_L}{V_{in}} = \frac{R_L\sqrt{C}}{j\sqrt{L(\omega_o)}} \tag{2}$$

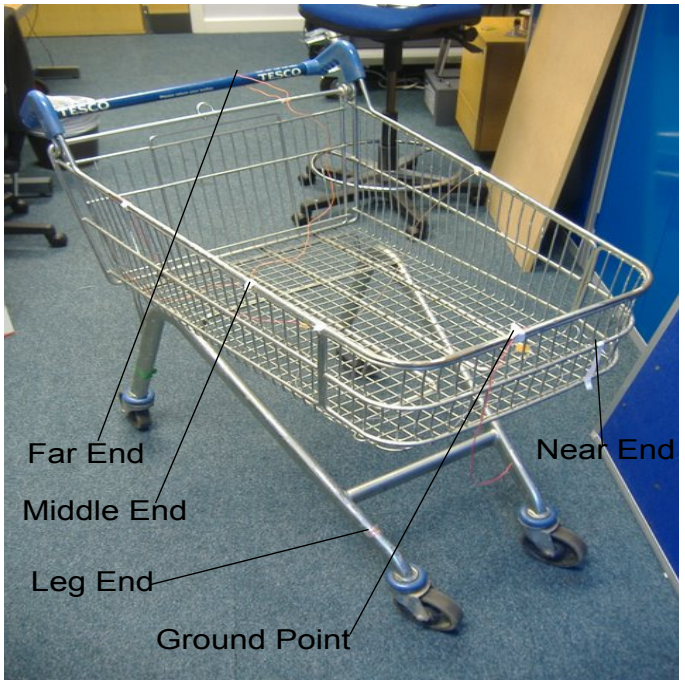
## H-Antenna Conclusions

- Low Inductance, high load Resistance
- Magnitude of 2 is equal to the Q-factor

UNIVERSITY OF SURREY

# Large Metallic structures

## The shopping trolley




- Various distances
- Fixed Ground
- Network Analyser

# The shopping trolley

## Findings at 13.5 MHz

| Scenario | Inductance at 13.5 MHz / $\mu$H | Resistance at 13.5 MHz / $\Omega$ |
|---|---|---|
| Near End | 0.42 | 1.31 |
| Middle End | 1.42 | 18.48 |
| Leg End | 3.73 | 70.66 |
| Far End | 2.59 | 7.67 |

- Connection point dependence

## Shopping Trolley antenna

### Pros

- Ease of execution (variable C)
- High load resistance desirable
- Short connection points

### cons

- Trolley resistance
- Loop size

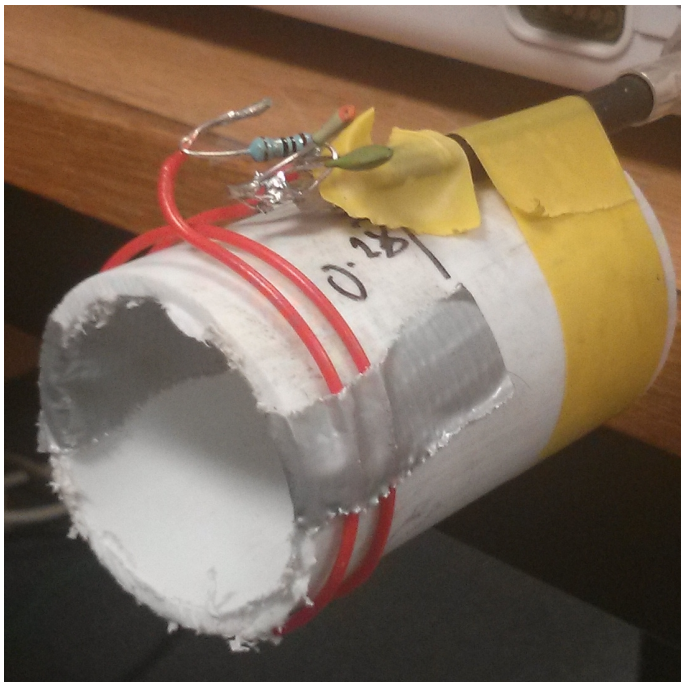
# Eavesdropping Antenna Benchmarks

## Eavesdropping H-fields

- H-loop antenna used as a transmitter
- Controlled H-field through current
- Signal generator and power amplifier
- Three types of eavesdropping antennas
- Path Loss measurements

# NFC Antenna Design Principles

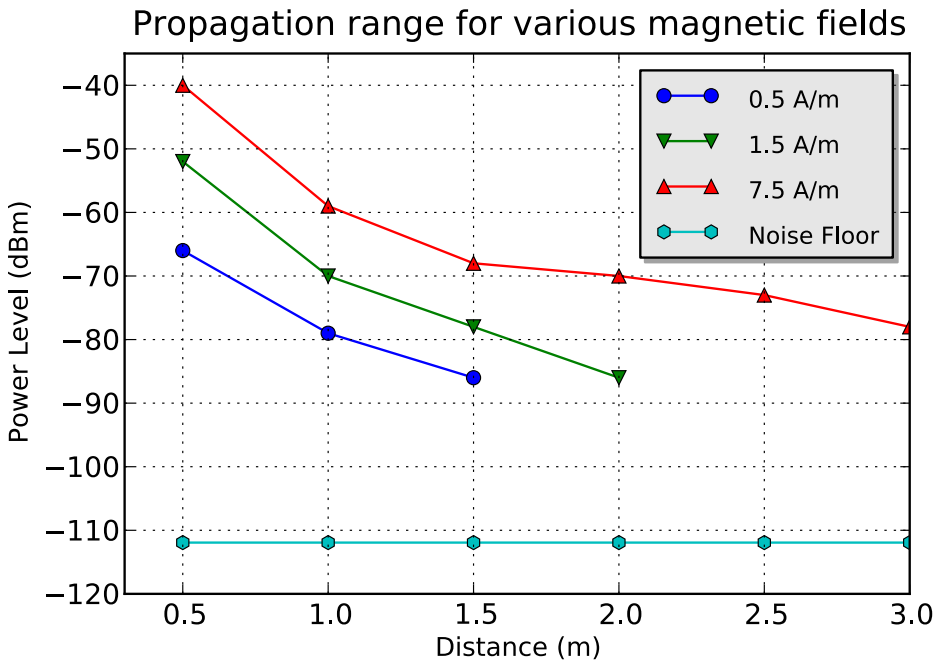
## H-Loop Antenna



- Matched to 50 Ω with a resistor (10 Ω) in series

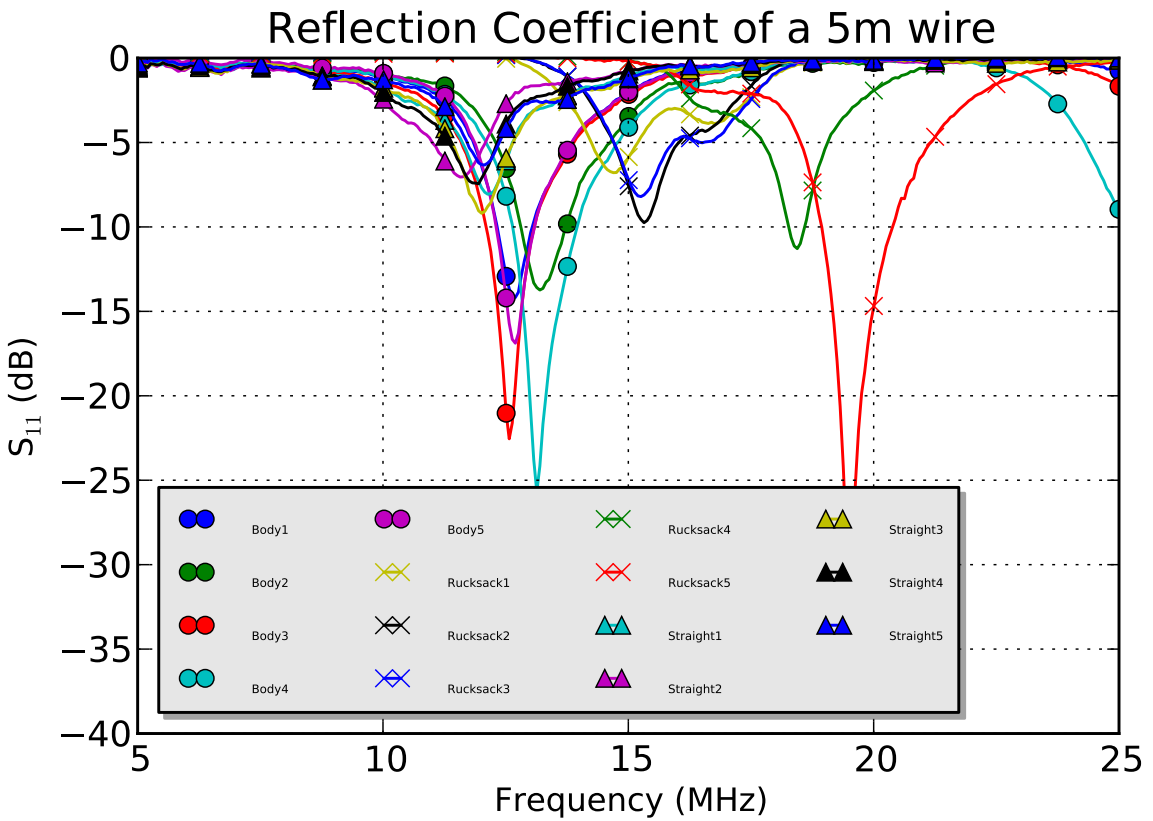
# Path Loss Measurements

## Various H-fields for H-loop and trolley only



# Quarter Wavelength Antenna

## $S_{11}$ Reflection Coefficients



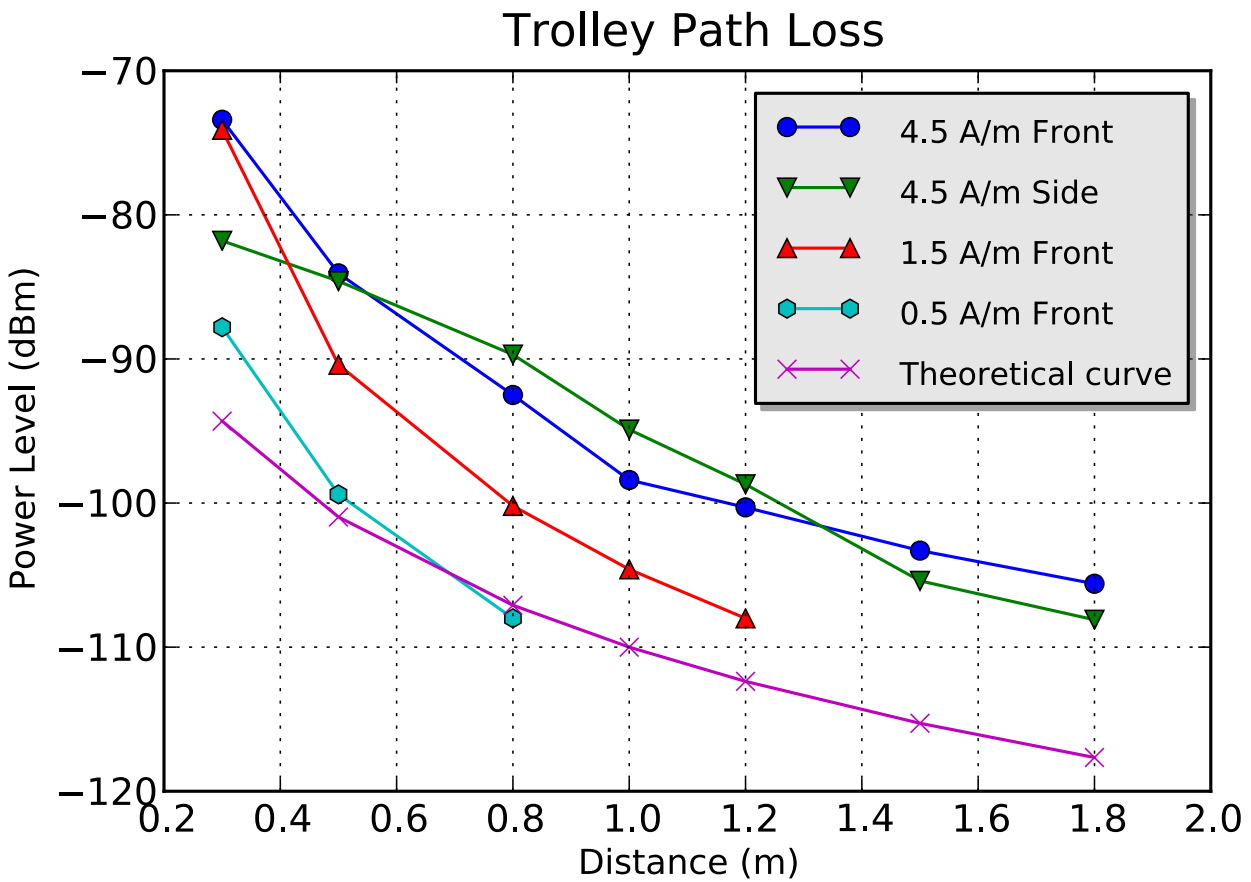
# Quarter Wavelength Antenna

## Worn over body

- Water content of body reduces efficiency

# Path Loss Measurements

## Trolley



# Path Loss Measurements

## Summary

- H-loop and trolley are most efficient
- Antenna orientation
- H-field strength
- Proceed with FER measurements

# Eavesdropping Near Field Contactless Payments

## Near Field Contactless Payments

- PHY layer based on ISO 14443 standard
- Half-duplex communication
- Type A and Type B

# Near Field Contactless Payments

## ISO 14443 type A communication

- 106kbps or 9.4 µs bit duration
- Manchester encoded baseband
- 847 kHz Subcarrier modulation (OOK)
- Standard / short frames
- SOF and EOF markers

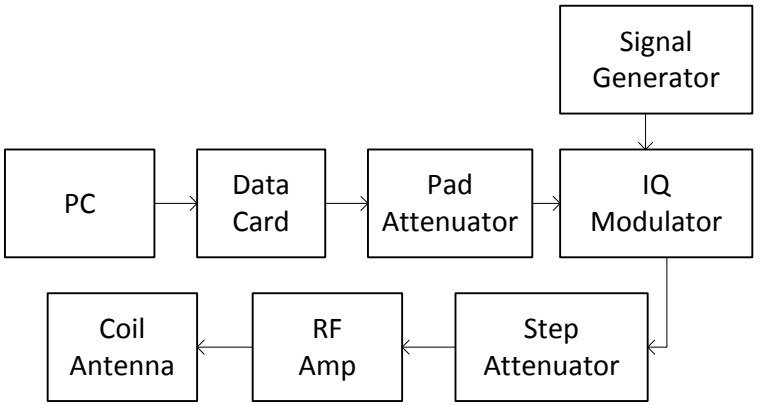
# Eavesdropping Near Field Contactless Payments

## Computing Frame Error Rates

- A known (random), long sequence
- Transmitter / Receiver
- Processing and computation

# Eavesdropping Near Field Contactless Payments

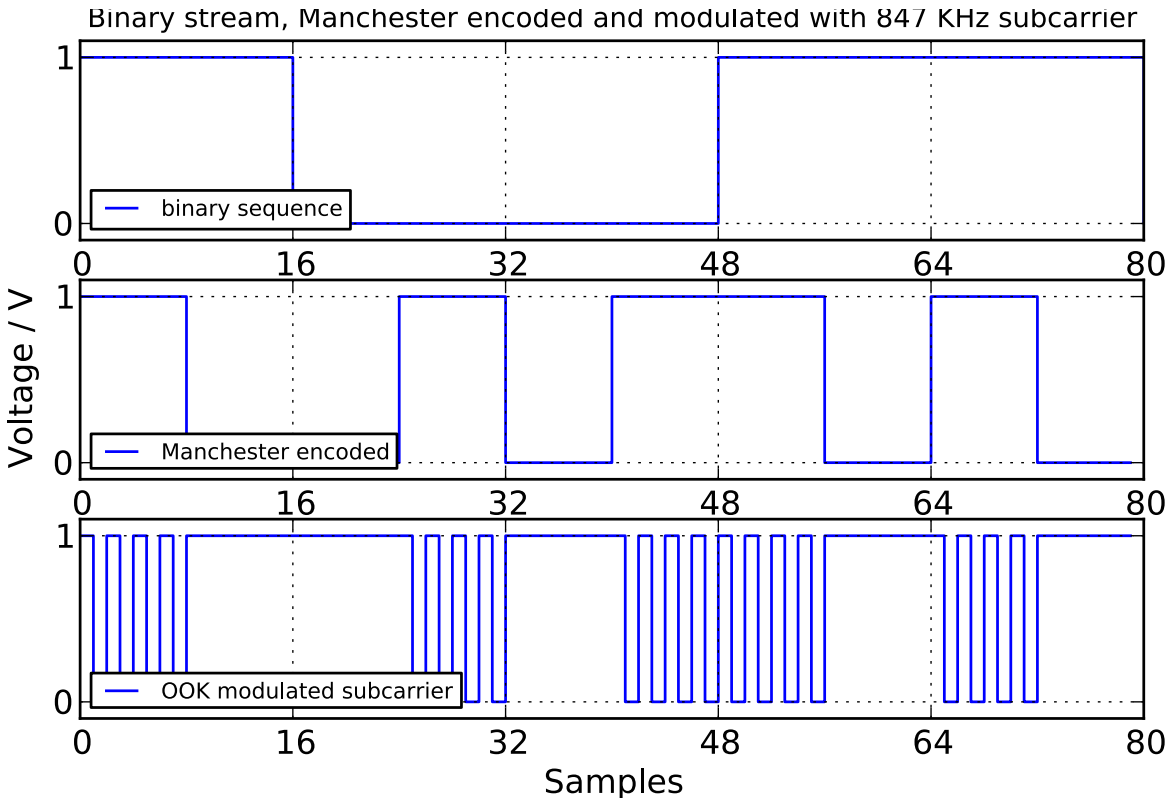
## Transmitter arrangement




- Synthetic data, 60 bytes per frame
- Subcarrier generated in software
- External trigger signal at 1.7 MHz

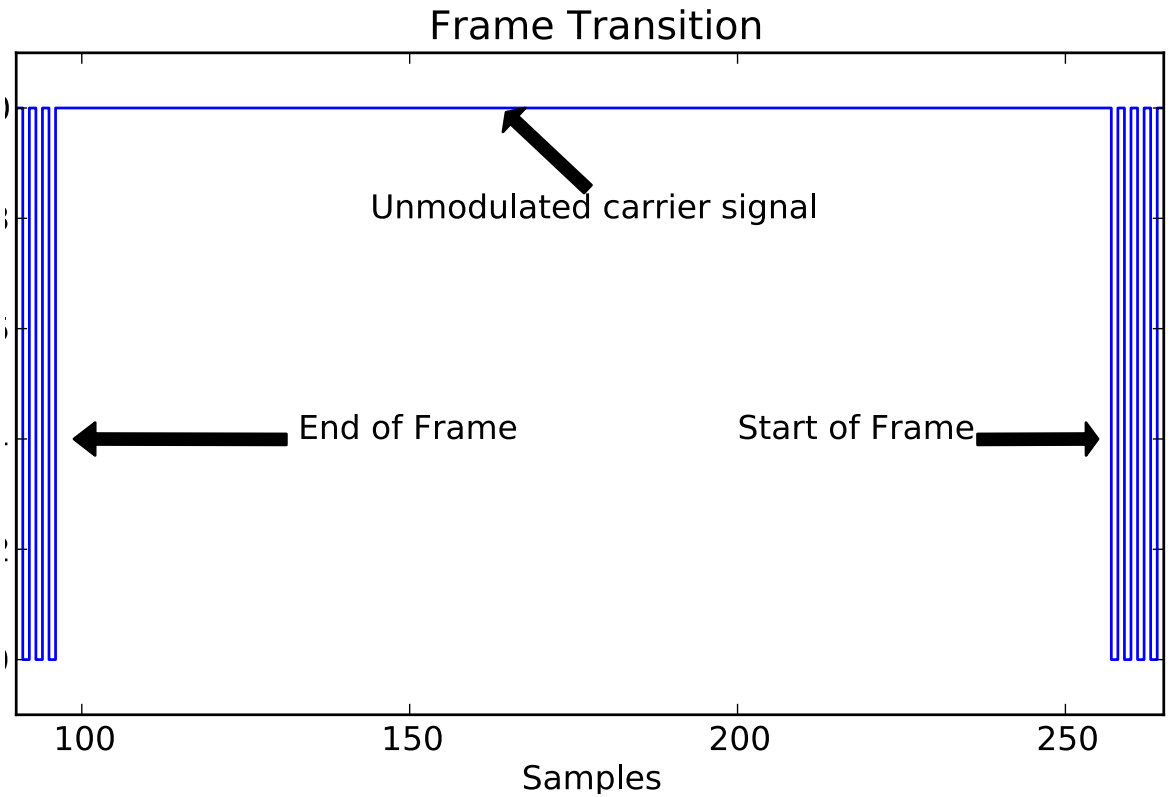
# Eavesdropping Near Field Contactless Payments

## Sequence of 5 bits



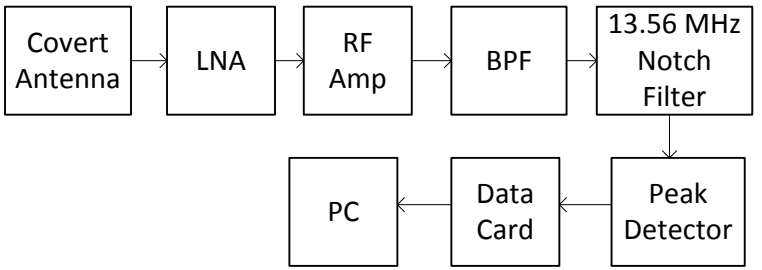
# Eavesdropping Near Field Contactless Payments

## Transition between two PICC frames



# Eavesdropping Near Field Contactless Payments

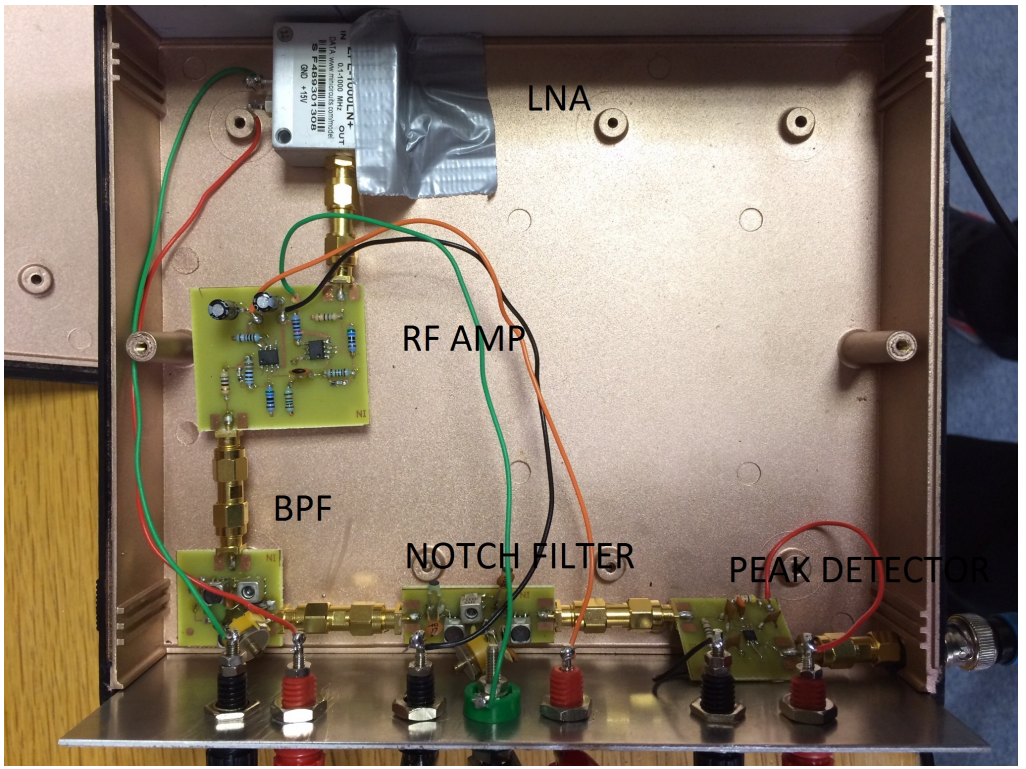
## Receiver arrangement




- LNA maximises SNR
- Band Pass Filter 12.7-14.4MHz
- Logarithmic detector

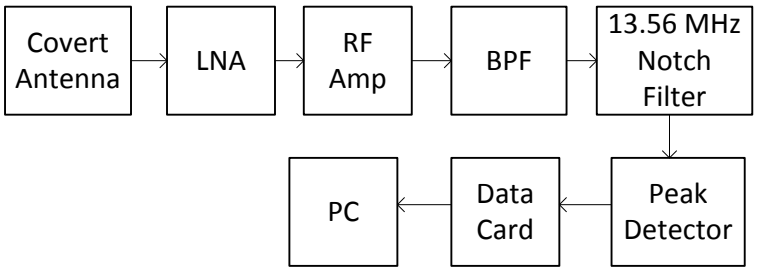
# Eavesdropping Near Field Contactless Payments

## Receiver arrangement



# Eavesdropping Near Field Contactless Payments

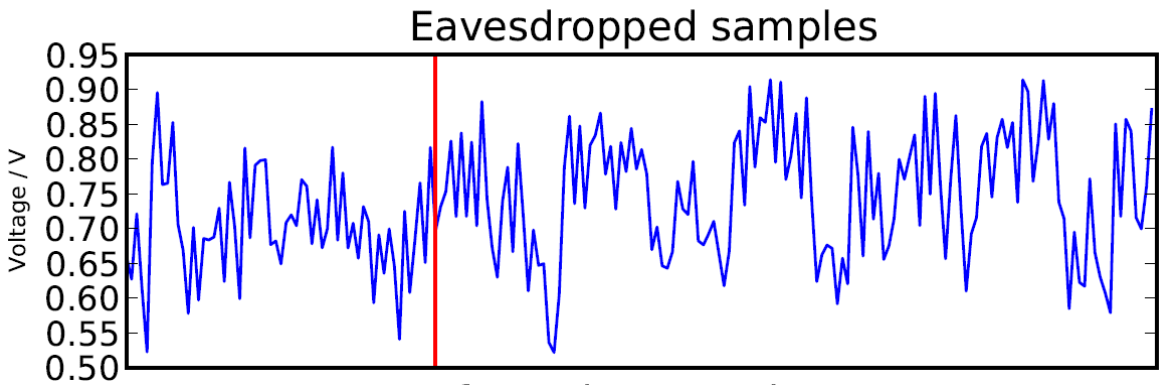
## Receiver arrangement




- LNA maximises SNR
- Band Pass Filter 12.7-14.4MHz
- Logarithmic detector
- Capture card sampling at 1.7MS/s

# Eavesdropping Near Field Contactless Payments

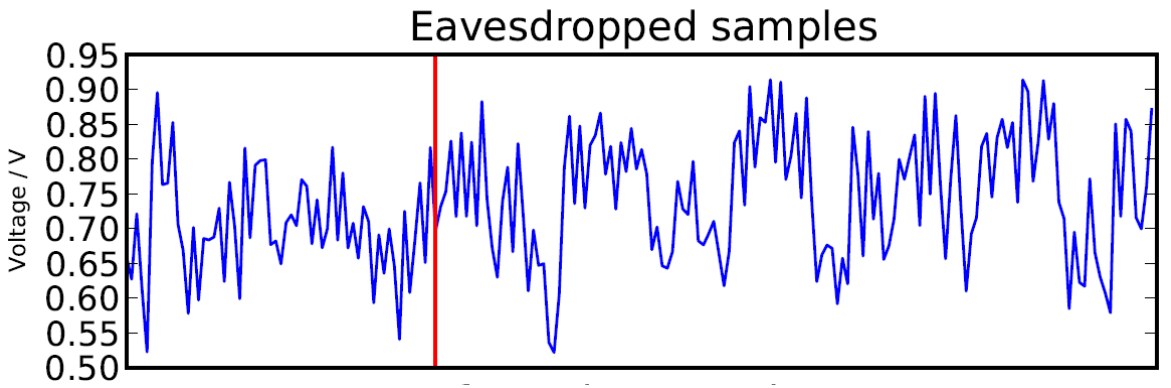
## Noise corruption




- Frame synchronisation becomes challenging

# Eavesdropping Near Field Contactless Payments

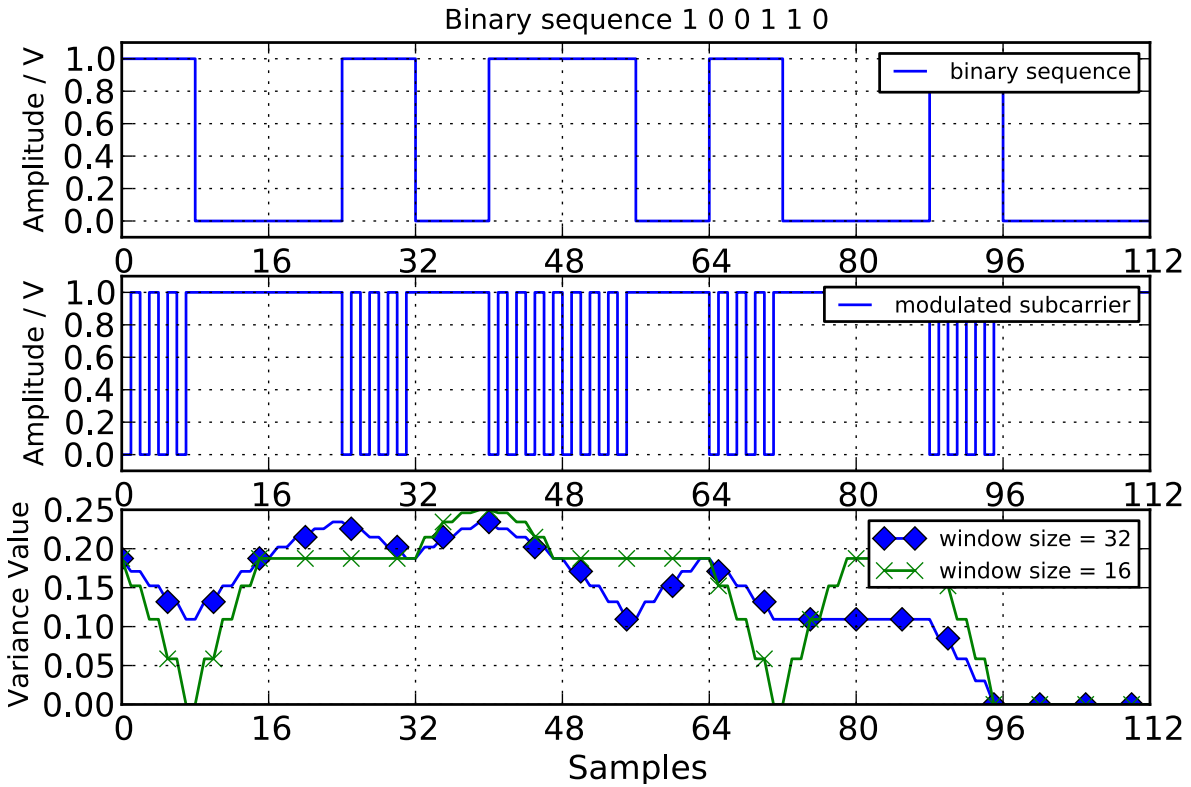
## Noise corruption




- Frame synchronisation becomes challenging
- Variance computing sliding window
- Threshold crossing

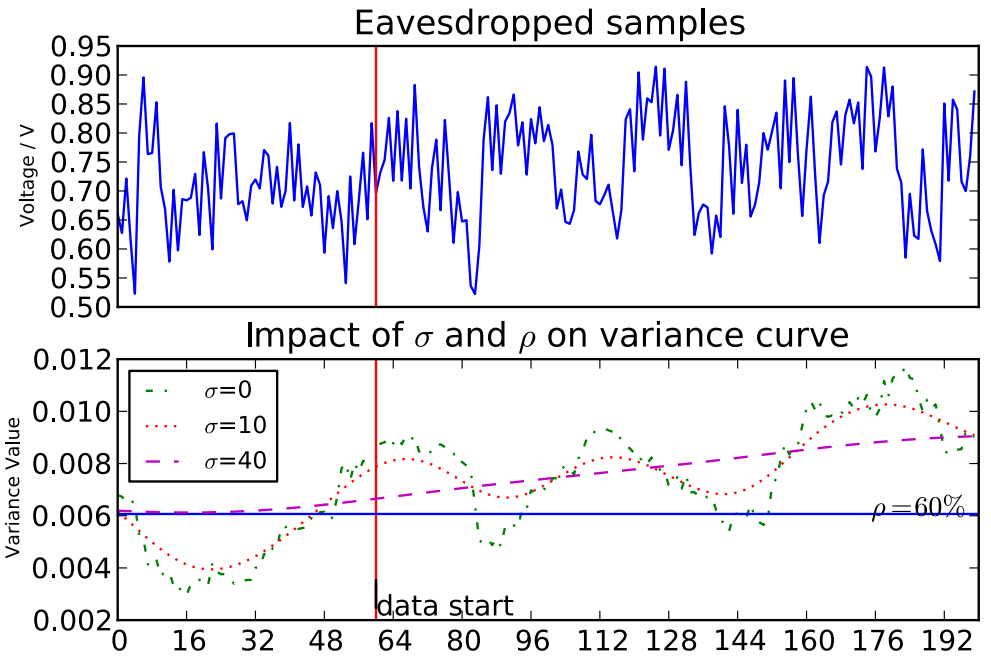
# Eavesdropping Near Field Contactless Payments

## Variance sliding window



# Eavesdropping Near Field Contactless Payments

## Variance smoothing and threshold




- Gaussian smoothing

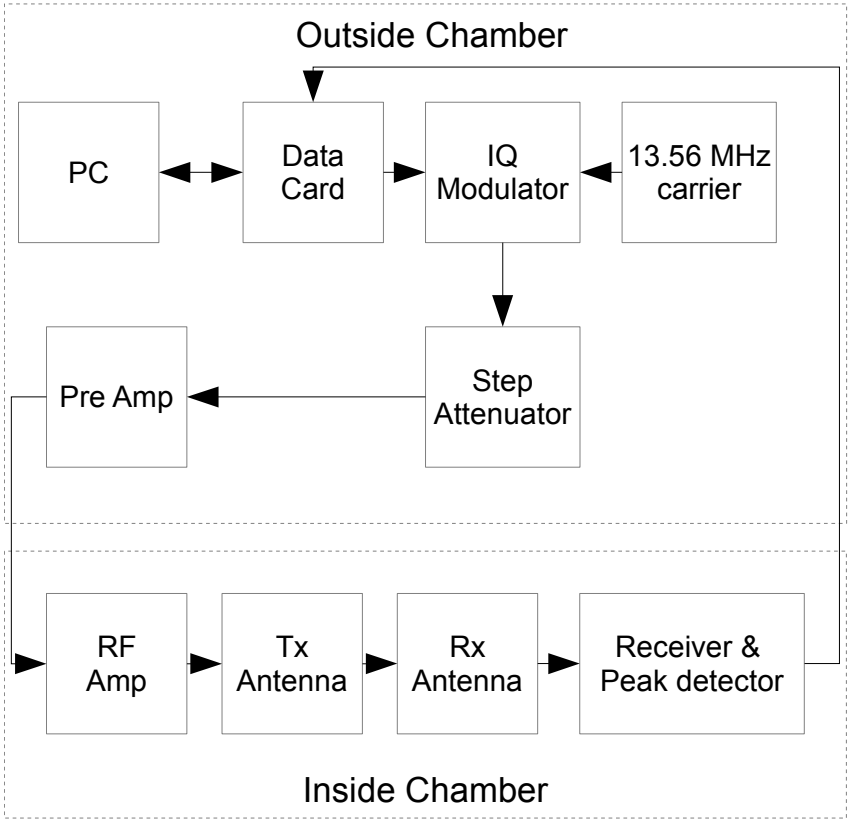
# Eavesdropping Near Field Contactless Payments

## Robust Frame Synchronisation

- Frame length
- Rough estimate based on $\rho$ crossing
- $(EOF - SOF - 32) \pm Y \Rightarrow$ multiple of 144
- Cross correlation for bit decoding

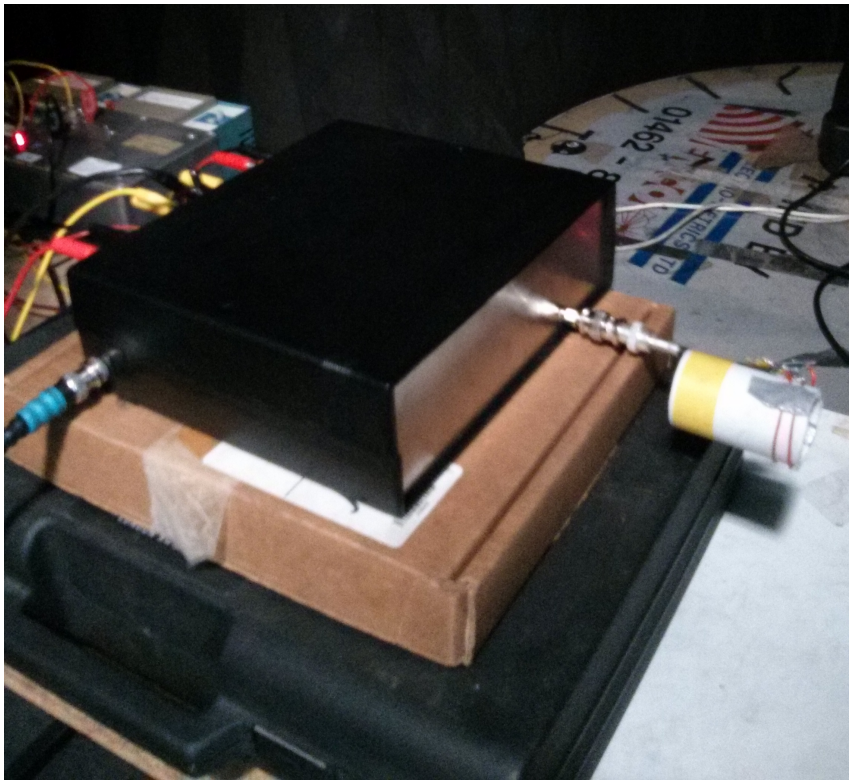
# Eavesdropping Near Field Contactless Payments

## Experimental Set-up



# Eavesdropping Near Field Contactless Payments

## Receiver circuit and antenna



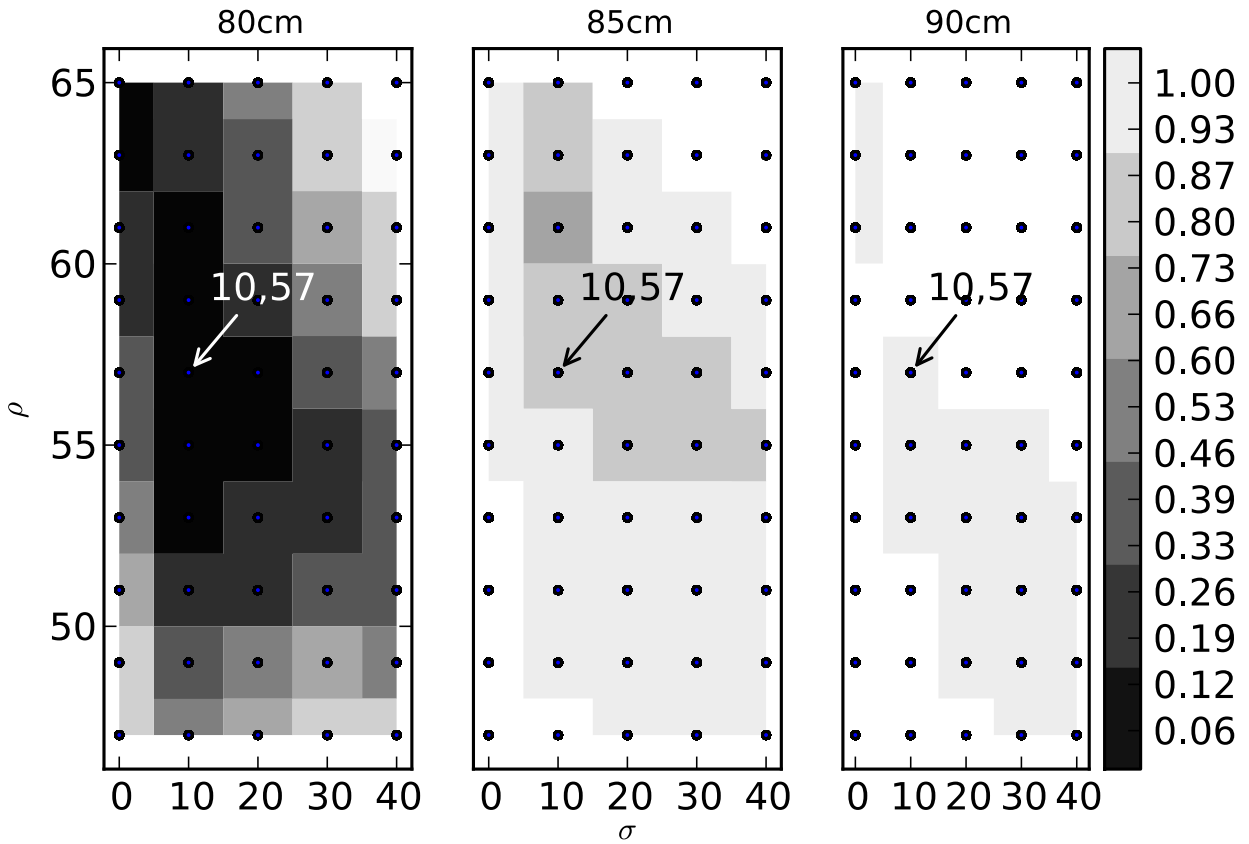
# Eavesdropping Near Field Contactless Payments

## Preliminary testing

- Anechoic chamber
- Controlled environment
- 500 frame tests
- Establish $\sigma$ and $\rho$ values

# Eavesdropping Near Field Contactless Payments

## $\sigma$ and $\rho$ selection at 7.45 A/m



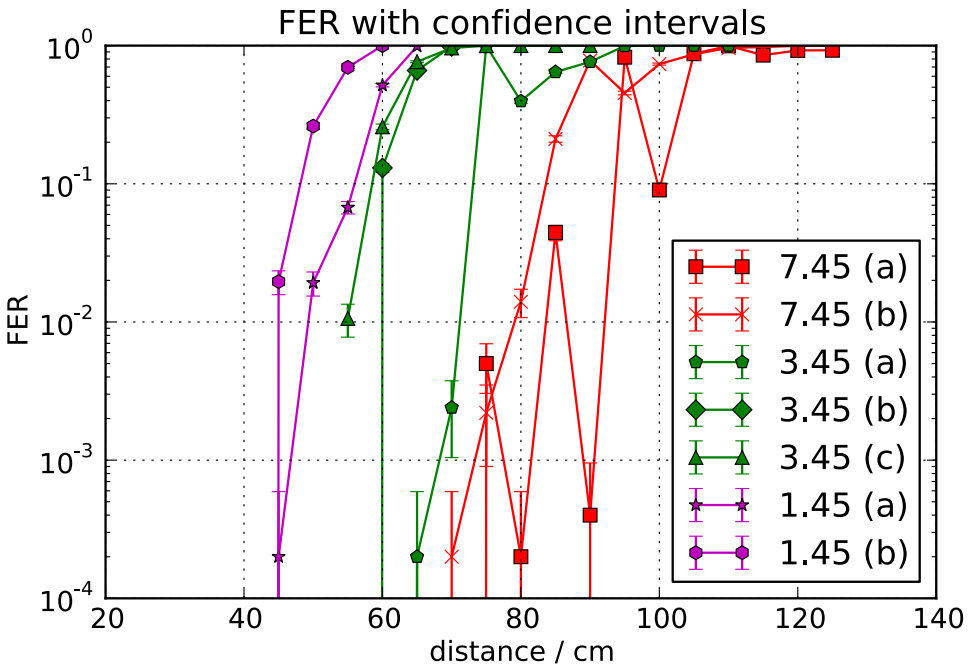
# Eavesdropping Near Field Contactless Payments

## Experimental procedure

- 5000 frames (20 minutes per run)
- 20–170 cm, increments of 5 cm (2–30 cm for trolley)
- 1.5, 3.45, 7.45 A/m
- Experiments ran over 2 days

# Results

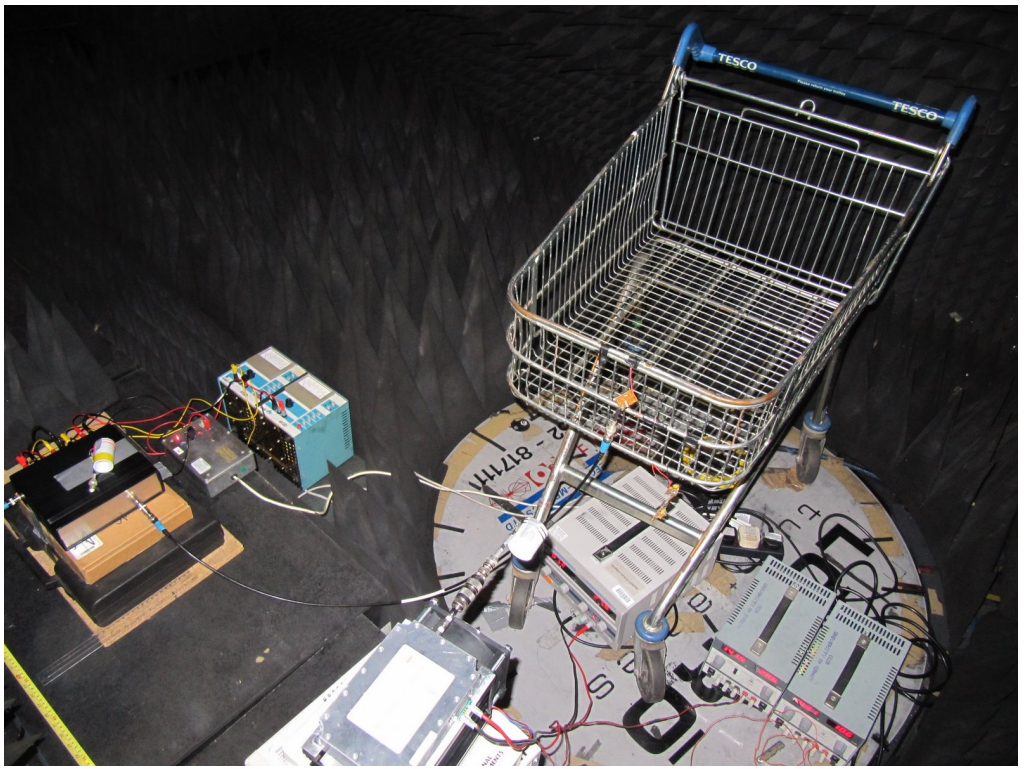
## H-Loop Antenna FER




- Normal approximation, 95% confidence interval levels

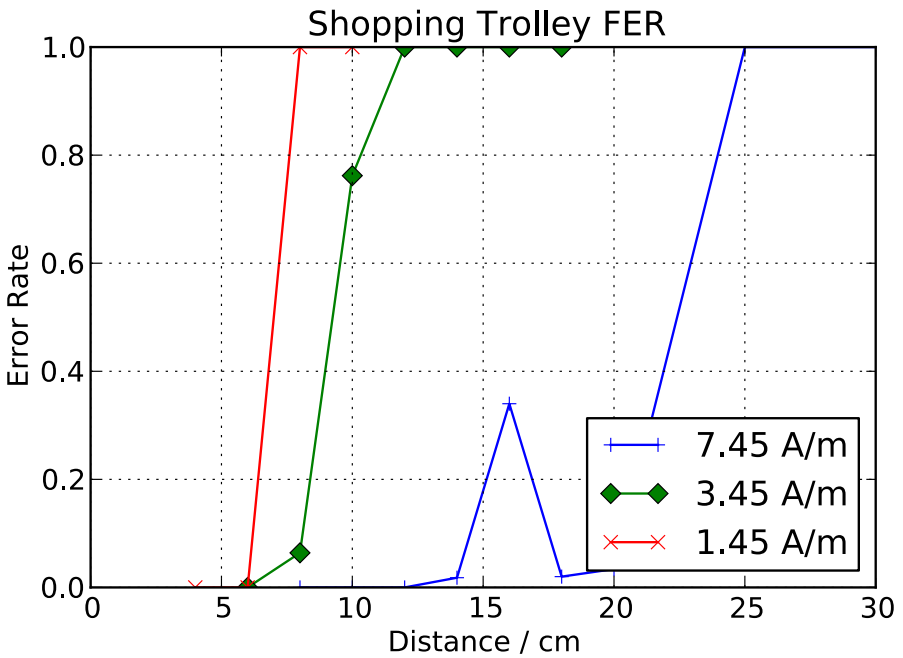
# Eavesdropping Near Field Contactless Payments

## Shopping trolley eavesdropping arrangement



# Eavesdropping Near Field Contactless Payments

## Shopping trolley FER ($\sigma = 10$, $\rho = 50$)




- Trolley generates its own noise, lossy antenna

# Conclusions and Future work

## Conclusions

- Eavesdropping distance 45-90 cm in shielded environment
- Similar conditions to those found in underground stations
- Relatively inexpensive equipment, inconspicuous antennas
- Gaussian filtering and variance computation are reliable

## Future work

- Real data with real devices
- Improve portability (FPGA), integrate a skimmer
- What does this mean for the user?

UNIVERSITY OF SURREY

# Eavesdropping Near Field Contactless Payments

Thank you for listening

Please forward any questions