Noisy Carrier Modulation for HF RFID

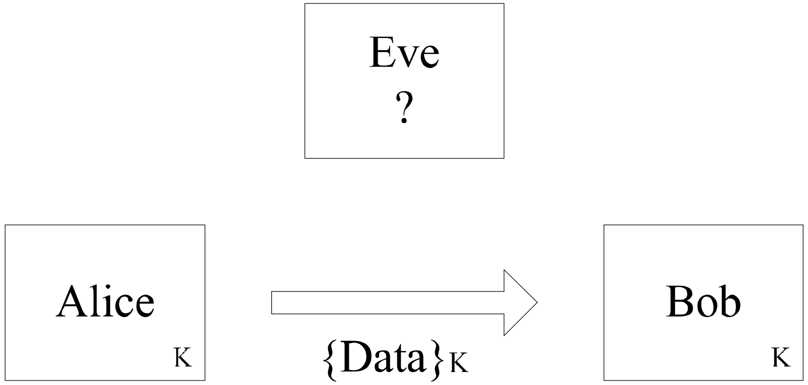
Gerhard P. Hancke

September 25, 2007

Royal Holloway University of London

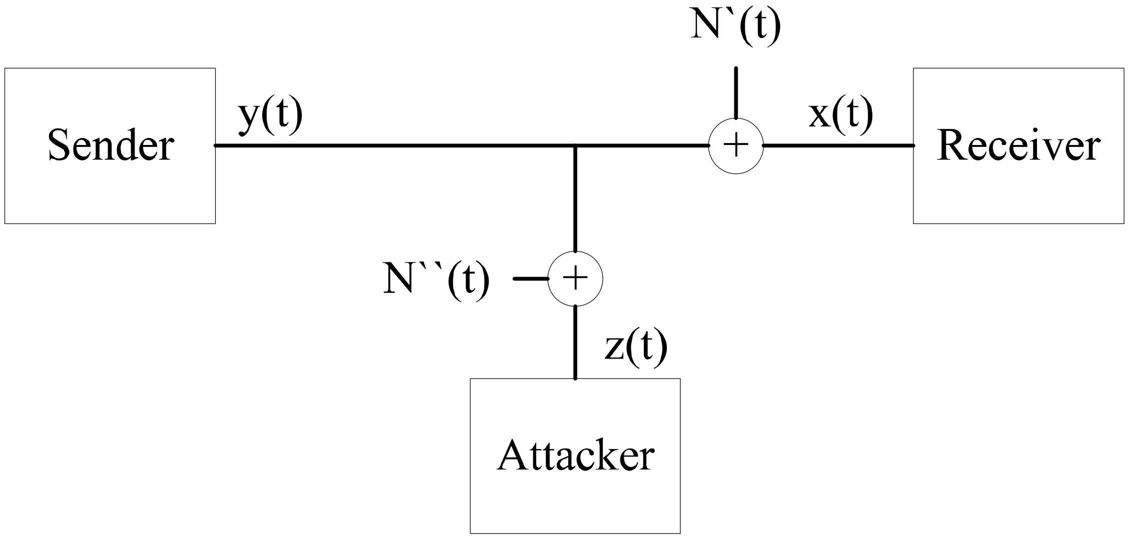
UNIVERSITY OF CAMBRIDGE

Data Confidentiality



- Alice and Bob are exchanging data
- An attacker, Eve, tries to eavesdrop on the communication
- Alice and Bob need to share some key information
- Key management is not always easy

Wire-Tap Model



- Wyner (1975)
  - Receiver: $x(t) = y(t) + N'(t)$
  - Attacker: $z(t) = y(t) + N''(t)$
  - $N'(t) << N''(t)$
- Attacker cannot recover data as result of $N''(t)$
- Problem: No assurance that $N''(t)$ is always sufficient

Cover Noise Proposals

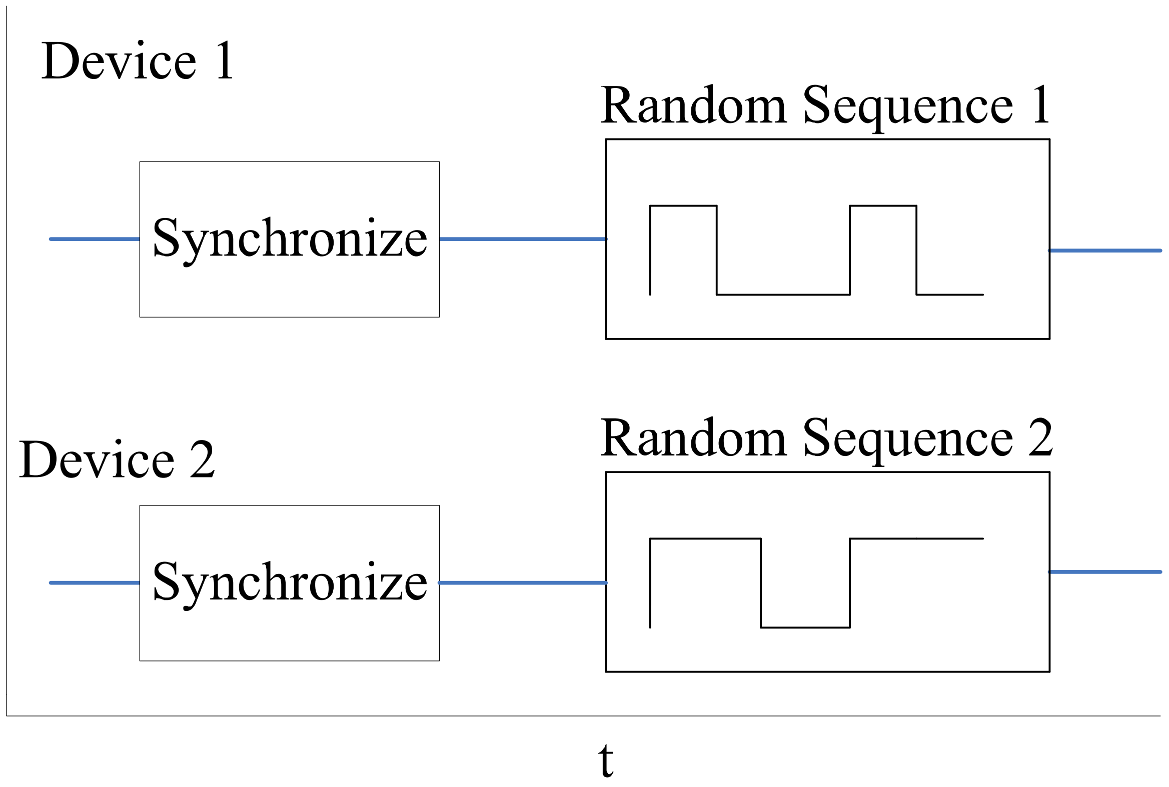
- Intentional introduction of ‘noise’ into the system
- Several RFID proposals use bit-blocking
- Privacy
  - Blocker Tag (Juels, Rivest and Szydlo)
  - RFID Guardian

    (Rieback, Gaydadjiev, Crispo, Hofman and Tanenbaum)
- Key Exchange
  - Noisy Tag Protocol (Castelluccia and Avoine)
  - NFC Key Agreement (Haselsteiner and Breitfuss)

Bit-Blocking Requirements

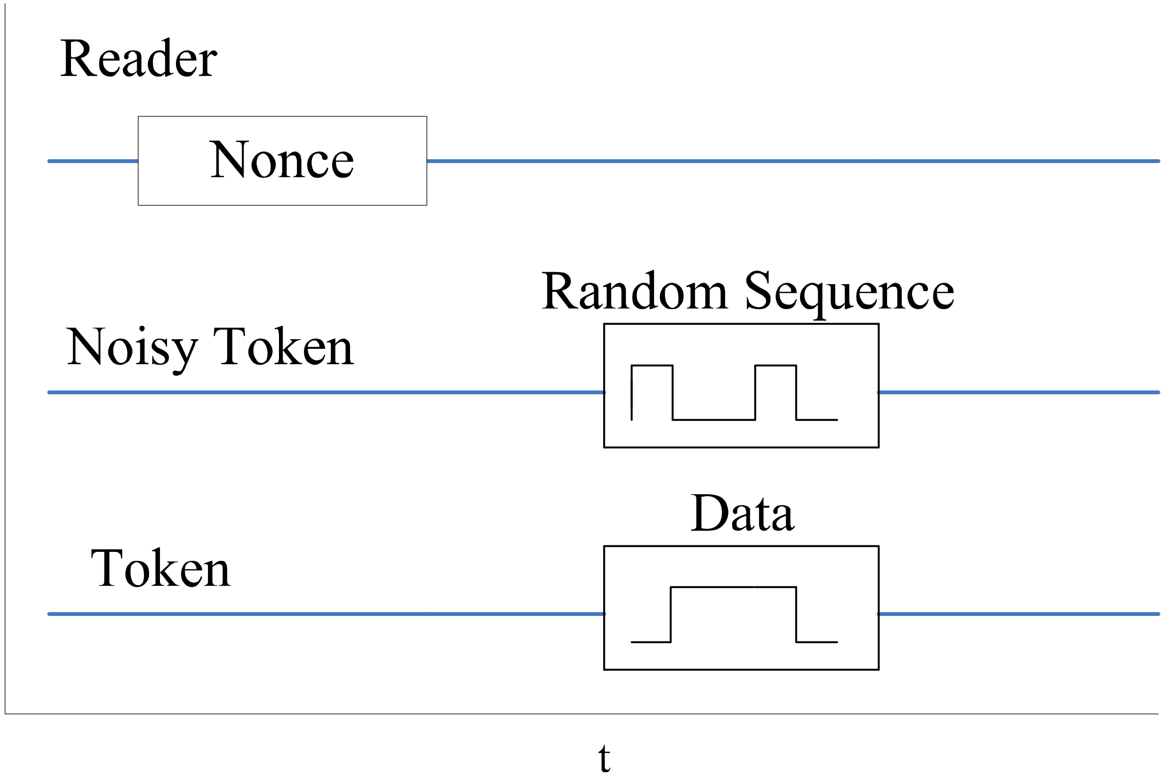
- Two devices transmit at the same time
  - Both transmit a ‘1’ → S_{11}
  - Both transmit a ‘0’ → S_{00}
  - Transmission of ‘0’ and ‘1’ → S_{10} or S_{01}
- It is assumed that $S_{01} = S_{10}$
  - Attacker cannot guess who transmitted the ‘1’ and ‘0’
- Blocking and data sequences must match
  - Amplitude
  - Phase

NFC Key Agreement (NKA)



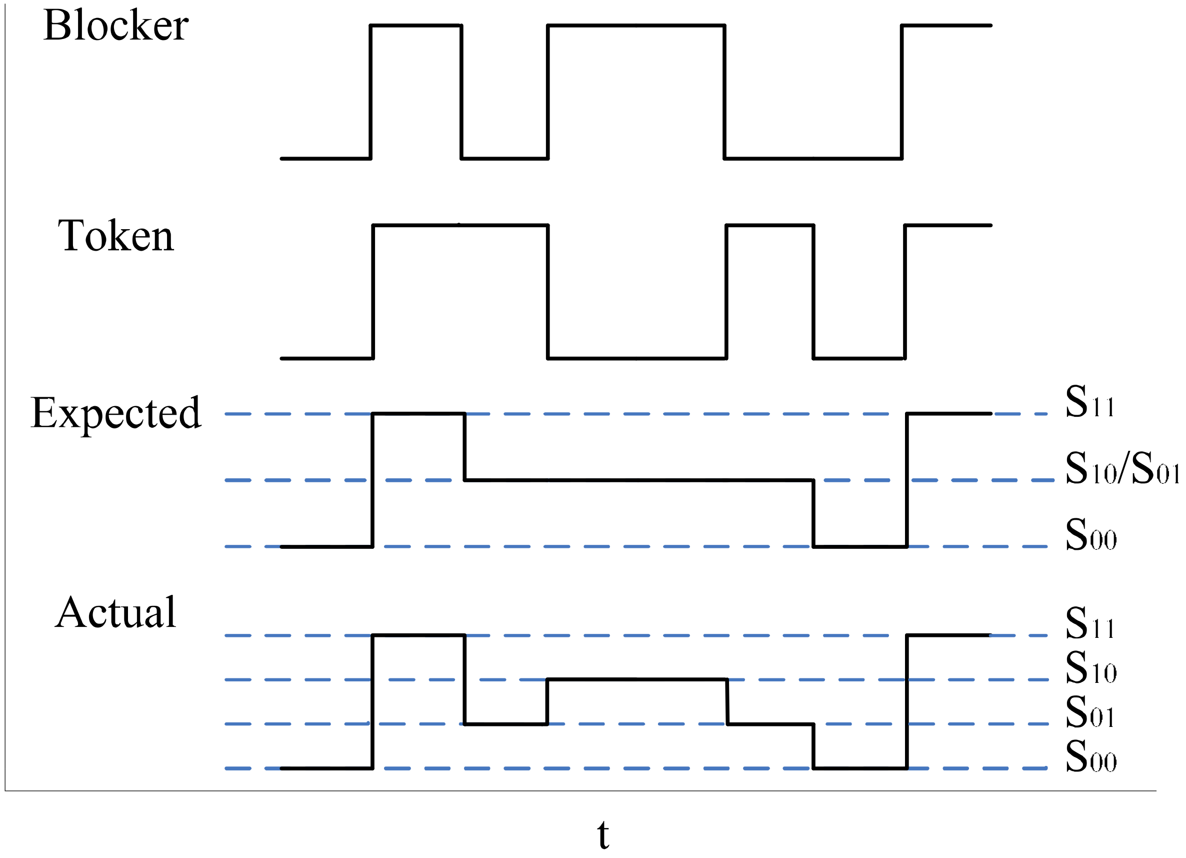
- Devices transmit at same time
- Receiver knows the blocking sequence
- Key refined from S_{01} and S_{10}

Noisy Tag Protocol (NTP)



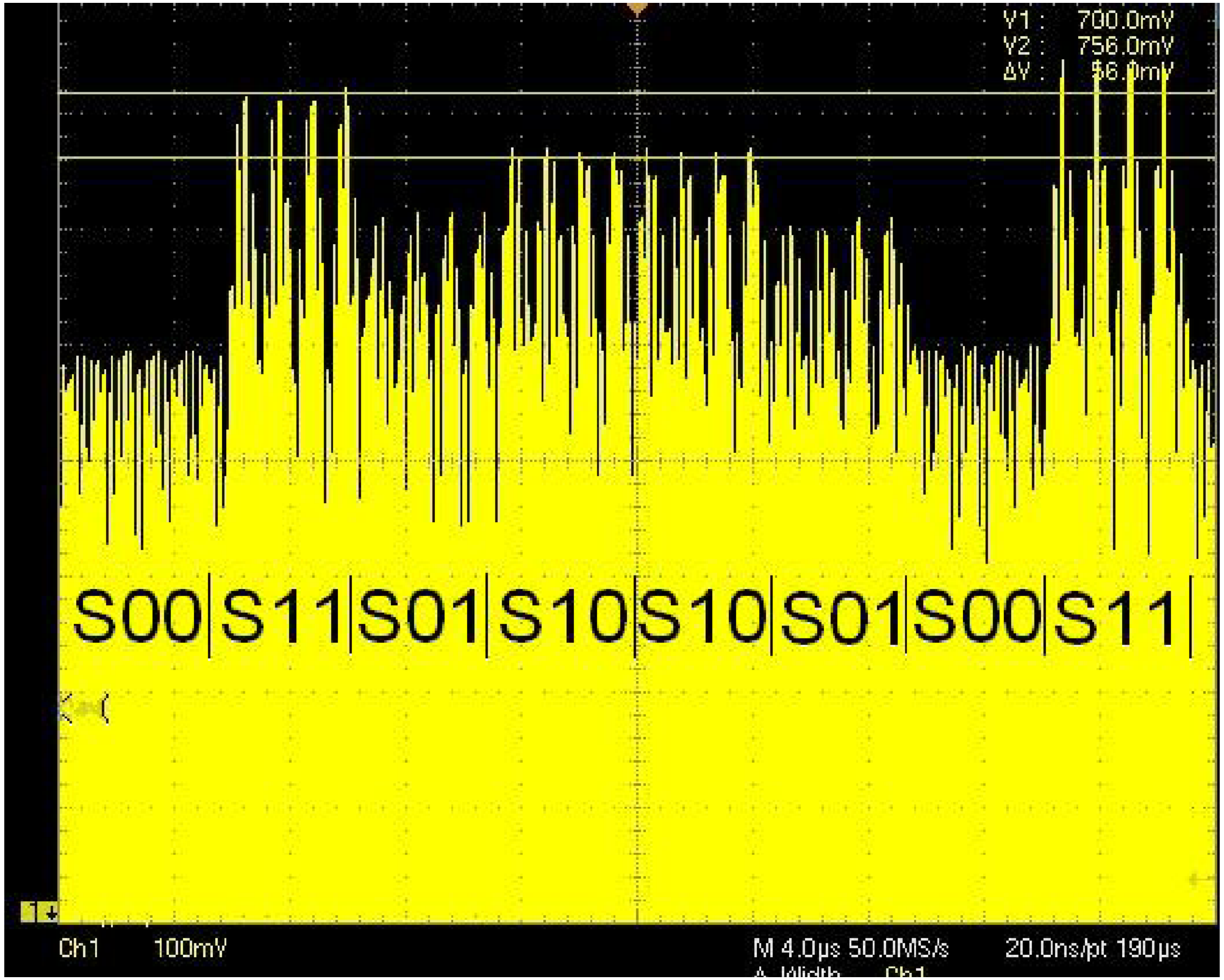
- Additional noisy tag used as blocker
- Noisy tag and reader share a secret
- Key refined from S_{01} and S_{10}

Practical Problems



- $S_{01} \neq S_{10}$
- Attacker can determine who sent which symbol

Practical Problems(2)

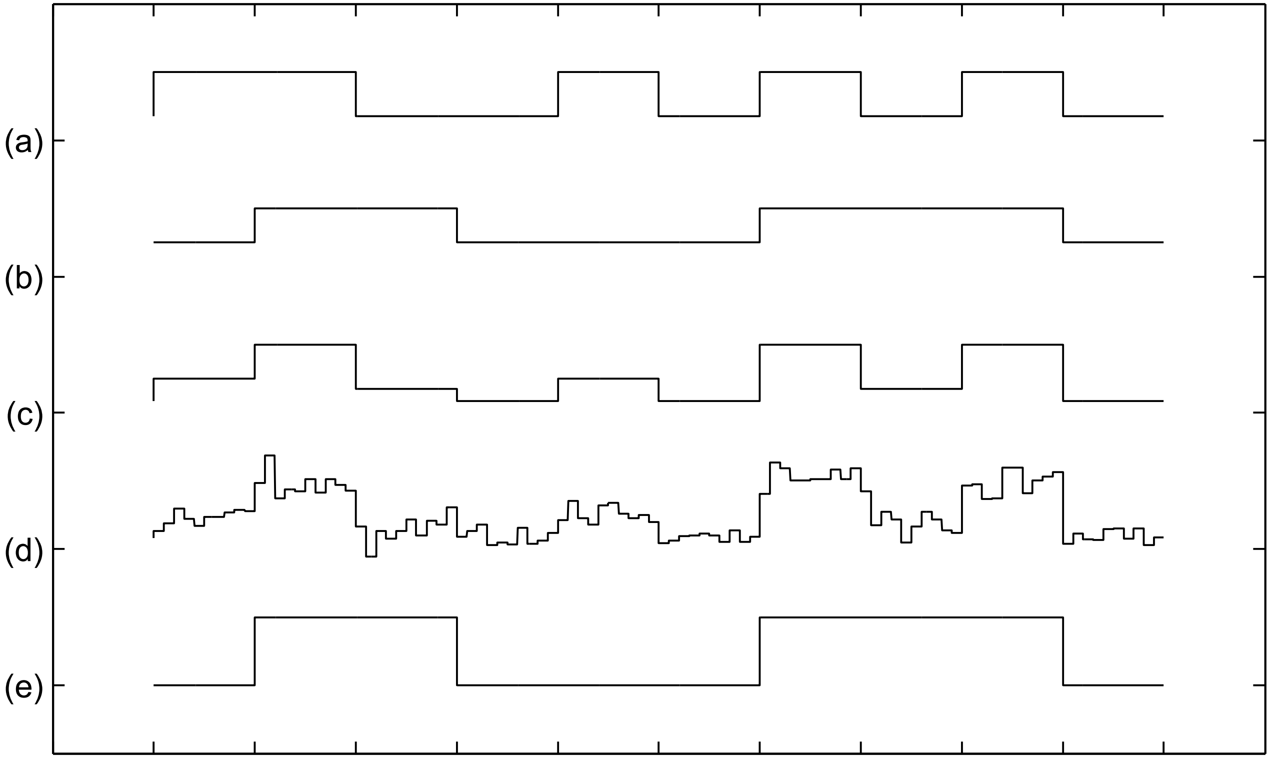


- Bit collision in reply of two ISO 14443A tokens

Solution

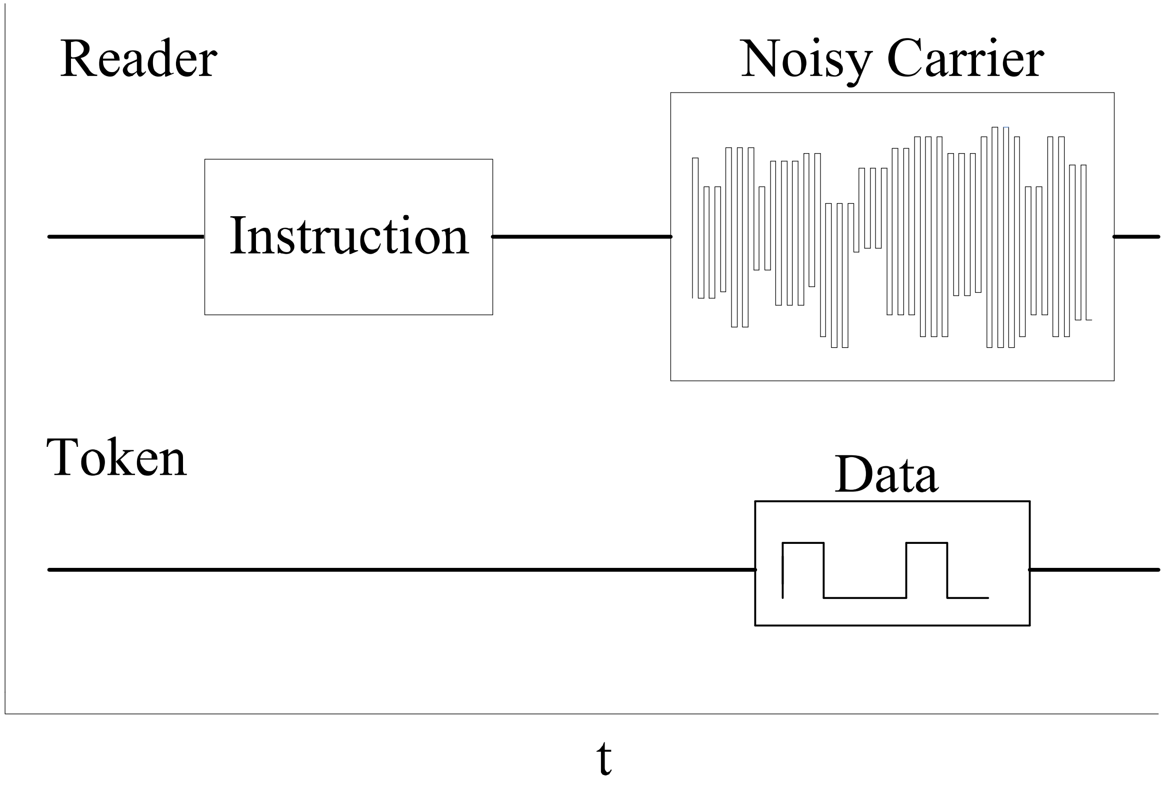
- Prevent attacker from distinguishing S_{01} and S_{10}
- Ensure that $S_{01} \approx S_{10}$
  - Phase: Devices can synchronize, blocker could adjust to different tokens
  - Amplitude: Match blocking sequence to data, difficult for the blocker to adjust
- Randomize the physical characteristics of the communication
  - Amplitude: Change the amplitude of the bit-blocking sequence

Amplitude Randomization



- Add band-limited noise to the blocking sequence
- Obfuscate the difference between S_{01} and S_{10}
- Data recovered if noisy blocking sequence is known

Noisy Carrier Modulation

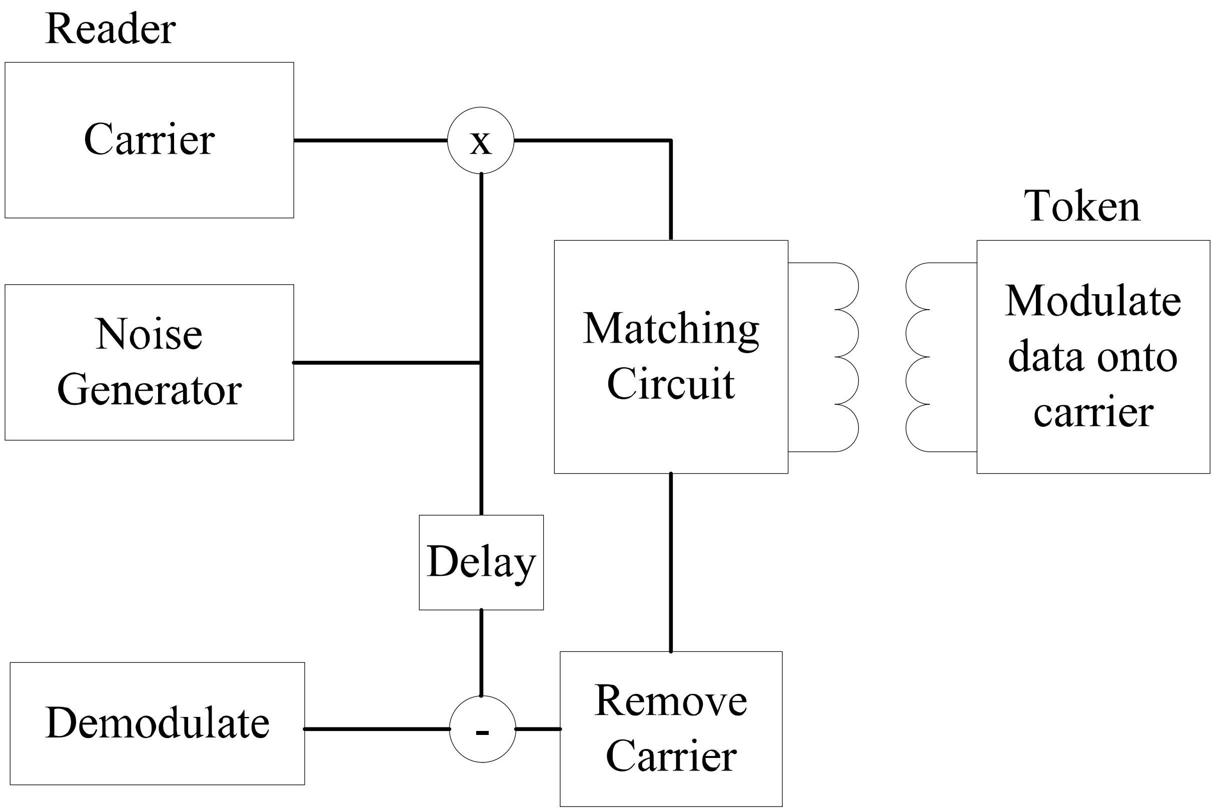


- Transmits the ‘noisy’ carrier during the token’s response
  - Token’s response modulated onto this carrier
- Randomizing the amplitude of the carrier similar effect to bit blocking

Noisy Carrier Modulation(2)

- System assumptions
  - A reader and token exchange a key in the presence of a passive attacker
  - The reader is trusted
  - The cover noise is resistant to analysis
- Enhance current bit-blocking schemes
  - Resolve some practical issues with bit-blocking
  - Not meant to obfuscate data only with noise

Practical Implementation?



- Additional hardware in the reader
  - Blocking-sequence: PRNG and AWGN noise source
  - Recovery: Noise synchronization

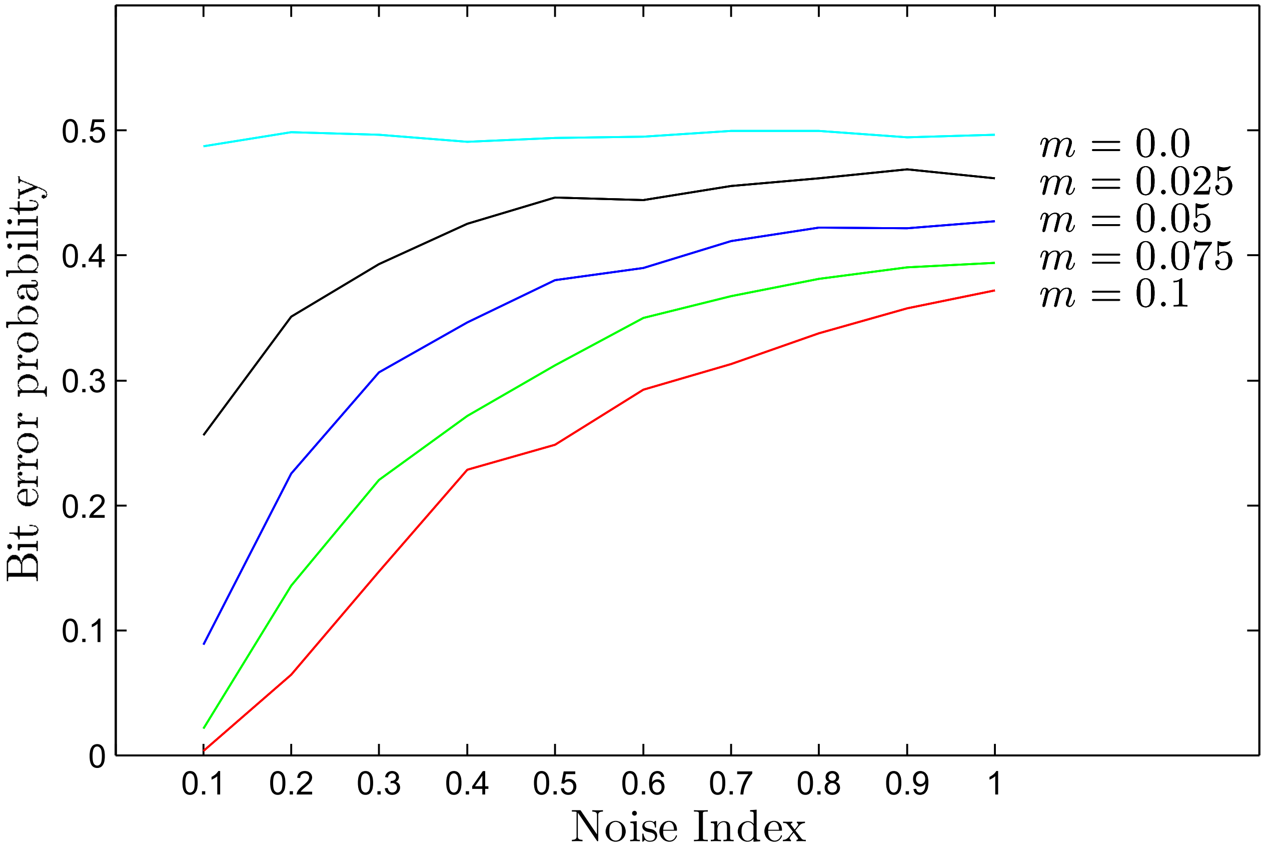
Advantages

- The reader acts as the blocker
  - User does not require additional devices
- No special token required
  - All extra functions build into the reader
  - Scheme can be used without modifications to current standards

Modeling the system

- $S_N\left(t\right) = S\left(t\right) + N\left(t\right) \cdot n_{\text{i}}$
  - $S\left(t\right)$ is the sequence of S_{10} and S_{01} symbols
  - $N\left(t\right)$ in the range $[-1:1]$, scaled by n_{i}
- No additional noise, $N'(t)$
- Attacker uses a correlation receiver
- Attacker knows when the data is sent
- Attacker knows the bit periods of the data

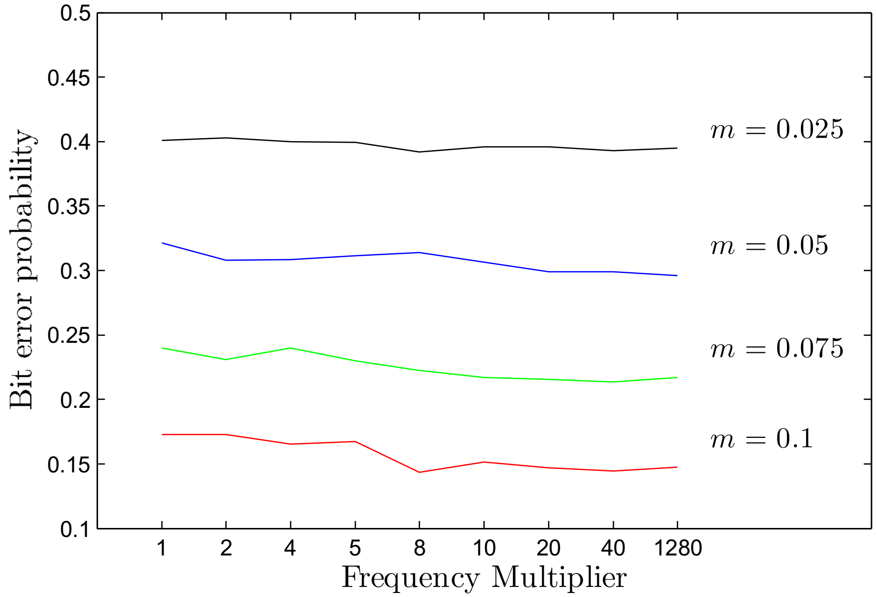
Results



- $m = |S_{10} - S_{01}|$, where max(S_{10},S_{01}) = 1
- BER of 0.5 equivalent to attacker guessing

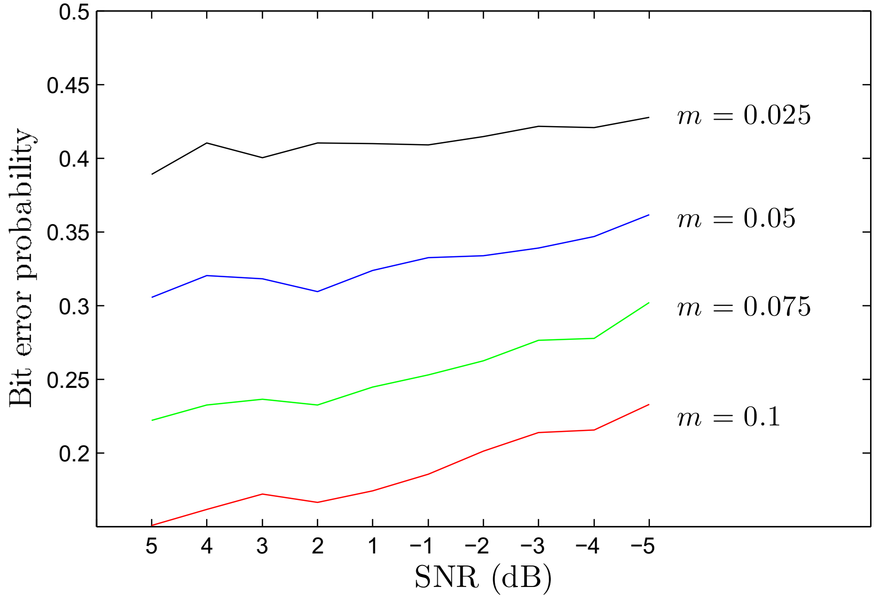
Results(2)

Frequency



- Choose noise to match data

Additional $N'(t)$



- More realistic model

Conclusion

- Show that simple bit-blocking has practical constraints
  - Attacker can distinguish between the blocker and sender because of differences in their communication
- Proposal for making backward channel resistant to eavesdropping
  - Use a modified bit-blocking scheme
  - Additional noise used to randomize amplitude of blocking sequence
  - Simulated results show that this scheme increases the probability that the attacker will make a bit error
  - No really suitable for data encryption

Conclusion(2)

- The reader acts as the blocker
  - Requires that the reader implements additional hardware
  - No need to change token
  - User does not need additional blocking device
- Suitable for implementation with current standards
  - Could be possibly be extended to NFC
- Allows for more secure implementation of current bit-blocking schemes
  - Key exchange
  - RFID proxies and blockers
- At the moment it is only an idea...:-)

Recent Proposal

RFID Noisy Reader How to Prevent from Eavesdropping on the Communication?

O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy
CEA-LETI

Cryptographic Hardware and Embedded Systems – CHES 2007
Vienna, September 2007

- Similar scheme specifically for ISO 14443
- Uses an additional antenna to broadcast cover noise
- More details on noise generation and hardware
- Attack model includes the attacker's distance and coupling efficiency

Done

Thank you, and any questions?

gerhard.hancke@rhul.ac.uk

Smart Card Centre

Royal Holloway, University of London