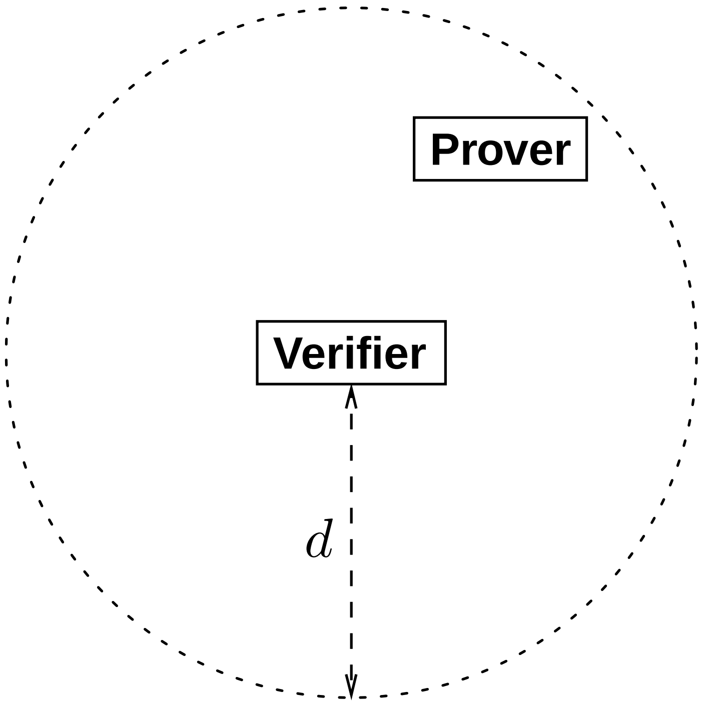
An RFID Distance Bounding Protocol

Gerhard P. Hancke and Markus G. Kuhn

May 22, 2006

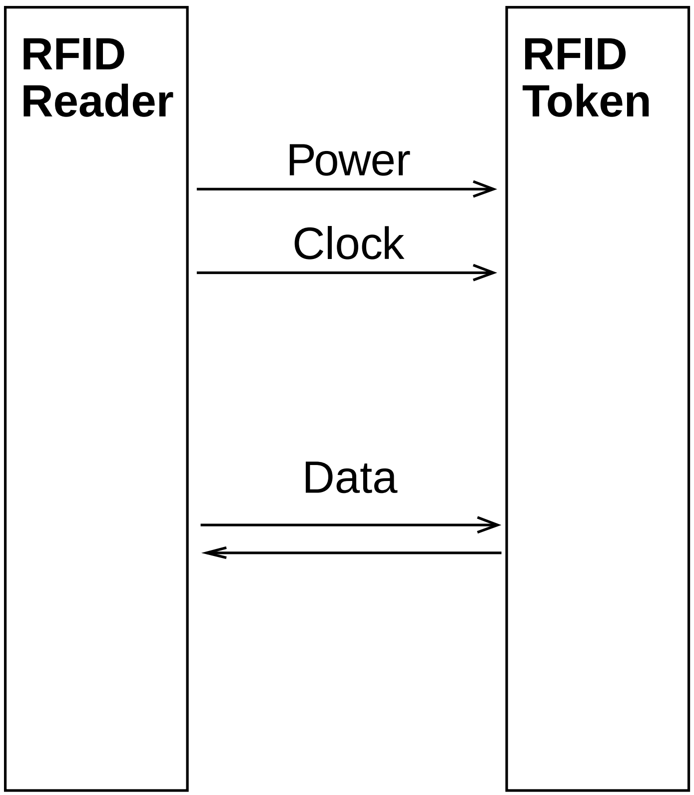
UNIVERSITY OF CAMBRIDGE

Distance bounding



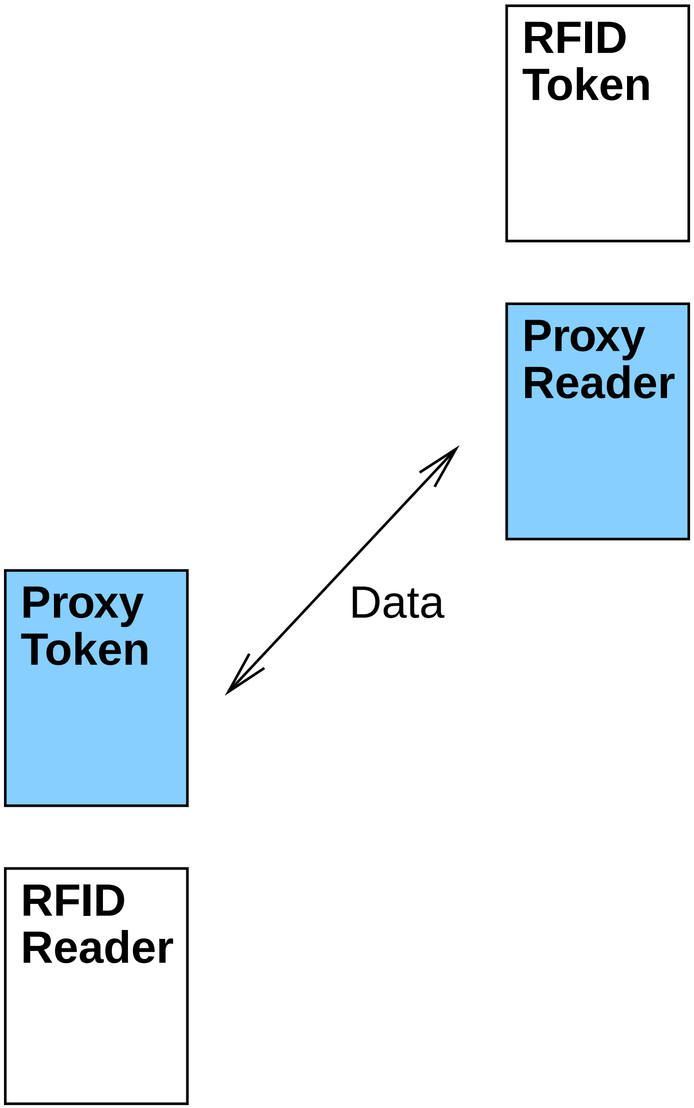
- Places an upper bound on physical distance
- Does not provide absolute location
- Operates on physical characteristics of the communication medium.
- Supplements existing security mechanisms

RFID devices



- Various applications
- Passive devices with low resources
- Limited range
- Used to link an item or person to a location

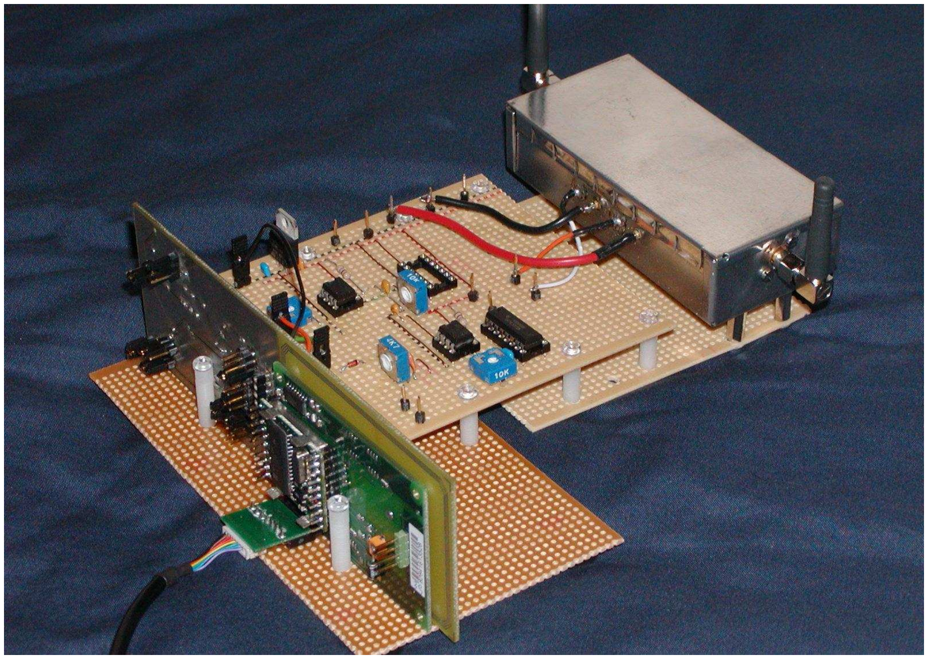
Relay attack



- Simple, well known attack
- Circumvents application layer security protocols

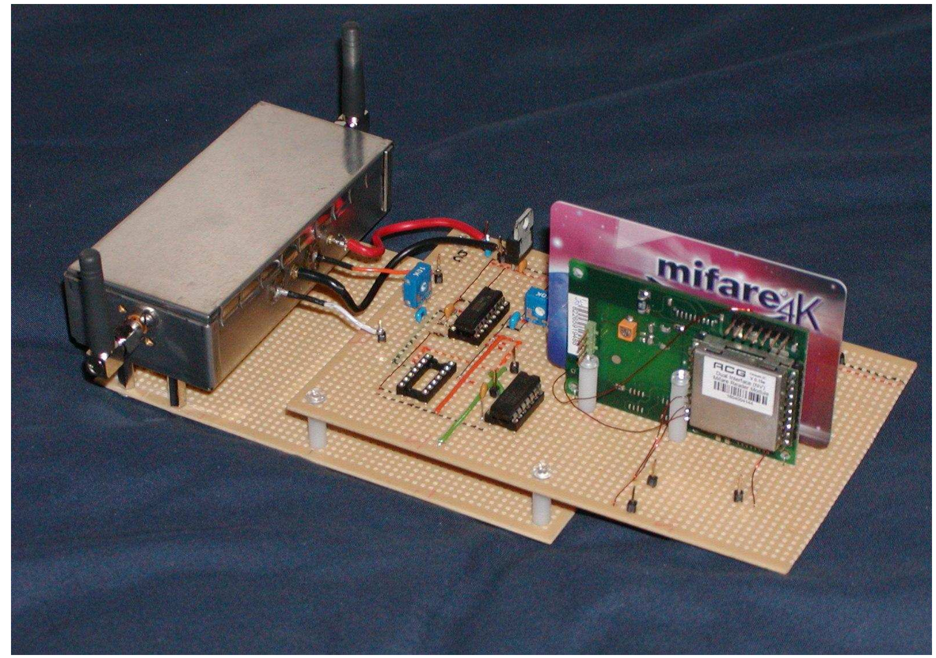
Relay attack demonstration

Proxy Token



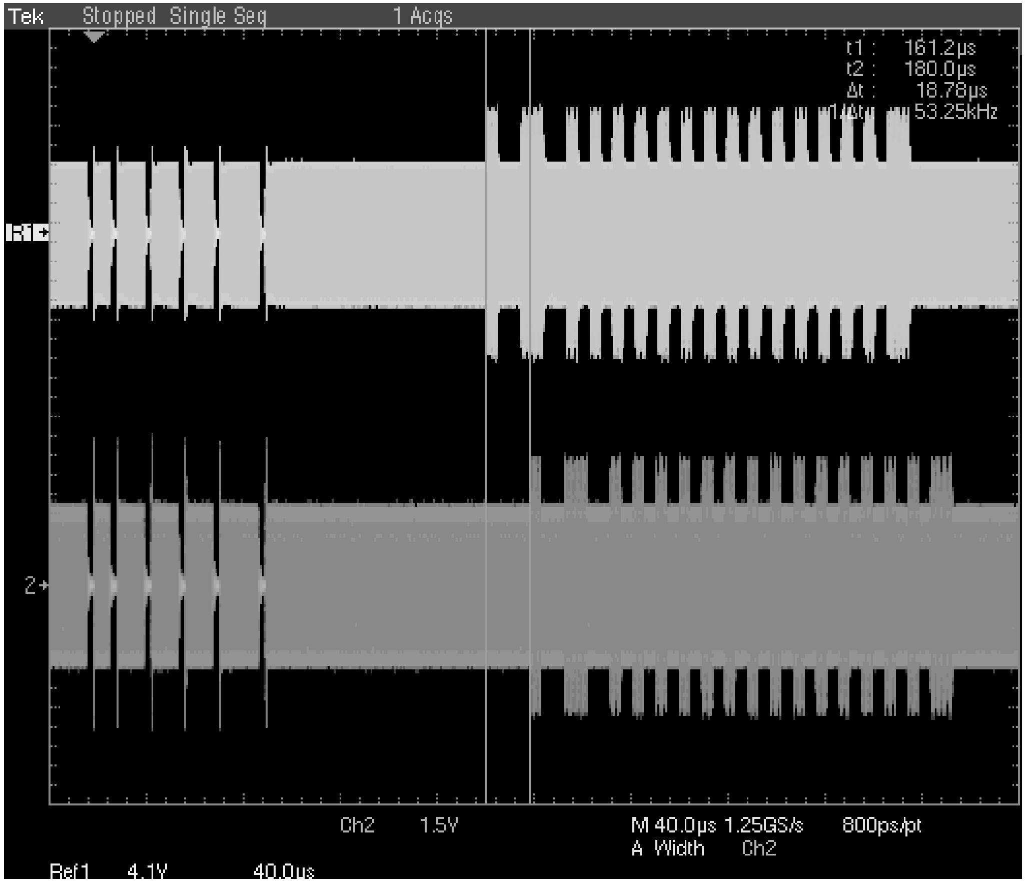
- 14443 A/B test card circuit
- Signal processing with discrete components
- Duplex RF link

Proxy Reader



- Commercial reader module
- Reprogrammed with our firmware
- Price ≈ $ 100

Relay attack detection



Timing difference between an actual token (top) and a Proxy token(bottom) response to a reader's *REQA* command.

- Delay
  - Could be reduced with complex hardware
  - Cannot be less than 3 ns/m
- Physical layer
  - High-resolution timing
- Application layer
  - Timing information lost

Our Protocol

Goals

- Suited to RFID environment
  - Verifier handles demanding processing functions
  - Prover performs simple functions
- Provide same level of security as other distance bounding protocols
  - Should not be worse because it has hardware constraints
- Implementation
  - Suggest practical ideas on how to implement our protocol
  - Protocol should supplement current RFID standards, not suggest wholesale changes

Protocol assumptions

Security target

- Places an upper bound on the distance between Verifier and Prover
- Does not provide non-repudiation of location to a third party
- The Prover does not collude with an attacker

Crypto primitives

- Shared secret key, K
- Shared pseudorandom function, h
- Nonces N_V,N_P are of sufficient length and will not be repeated

Protocol assumptions (2)

Time base

- Verifier is computationally strong
  - Perform accurate timing operations
- Prover is computationally weak
  - Cannot determine accurate timing information
  - Uses external clock signal (received carrier)
  - Prover can detect large deviations in clock frequency

Communication channels

- Low bandwidth error corrected channel
- High bandwidth rapid bit exchange channel

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Secret key K Function h Generate nonce N_V	$\xrightarrow{N_V}$	Secret key K Function h

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Secret key K		Secret key K
Function h		Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$
		Split $R = R_0 \| \| R_1$
		$\boxed{1\ 0\ 0\ 1\ 1\ 0\ 1\ 1} \leftarrow R^0$
		$\boxed{0\ 1\ 1\ 1\ 0\ 1\ 1\ 0} \leftarrow R^1$
$\langle C_i \rangle = 01001100$		

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Verifier (RFID reader) Secret key K Function h		**Prover (RFID token)** Secret key K Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$ Split $R = R_0 \|\| R_1$
		1 0 0 1 1 0 1 1 $\leftarrow R^0$ 0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_1 = 0}$	0 0 1 1 0 1 1
$\langle R_i^{C_i} \rangle = 1$	$\xleftarrow[R_1^{C_1} = 1]{}$	1 1 1 0 1 1 0

Protocol description

Verifier (RFID reader)
Secret key K
Function h

Generate nonce N_V

Generate random bits
$C_1, \ldots, C_n$

$\langle C_i \rangle = 01001100$
$\left\langle R_i^{C_i} \right\rangle = 11$

$\xrightarrow{N_V}$

$\xrightarrow{C_2 = 1}$

$\xleftarrow[R_2^{C_2} = 1]{}$

Prover (RFID token)
Secret key K
Function h

Calculate
$h(K, N_V) = R$
Split $R = R_0 || R_1$

1 0 0 1 1 0 1 1 $\leftarrow R^0$
0 1 1 1 0 1 1 0 $\leftarrow R^1$

0 1 1 0 1 1
1 1 0 1 1 0

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Secret key K Function h		Secret key K Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$ Split $R = R_0 \| \| R_1$ 1 0 0 1 1 0 1 1 $\leftarrow R^0$ 0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_3 = 0}$	1 1 0 1 1
$\left\langle R_i^{C_i} \right\rangle = 110$	$\xleftarrow[R_3^{C_3} = 0]{}$	1 0 1 1 0

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Secret key K Function h		Secret key K Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$ Split $R = R_0 \| R_1$ 1 0 0 1 1 0 1 1 $\leftarrow R^0$ 0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_4 = 0}$	1 0 1 1
$\langle R_i^{C_i} \rangle = 1101$	$\xleftarrow[R_4^{C_4} = 1]{}$	0 1 1 0

Protocol description

Verifier (RFID reader)		Prover (RFID token)
Secret key K Function h		Secret key K Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$ Split $R = R_0 \| \| R_1$
		1 0 0 1 1 0 1 1 $\leftarrow R^0$ 0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_5 = 1}$	0 1 1
$\langle R_i^{C_i} \rangle = 11010$	$\xleftarrow[R_5^{C_5} = 0]{}$	1 1 0

Protocol description

Verifier (RFID reader)		**Prover (RFID token)**
Secret key K		Secret key K
Function h	$\xrightarrow{N_V}$	Function h
Generate nonce N_V		
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V) = R$
		Split $R = R_0 \| \| R_1$
		1 0 0 1 1 0 1 1 $\leftarrow R^0$
		0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_6 = 1}$	1 1
$\left\langle R_i^{C_i} \right\rangle = 110101$	$\xleftarrow[R_6^{C_6} = 1]{}$	1 0

Protocol description

Verifier (RFID reader)

Secret key K

Function h

Generate nonce N_V

Generate random bits

$C_1, \ldots, C_n$

$\langle C_i \rangle = 01001100$

$\langle R_i^{C_i} \rangle = 1101011$

$$\xrightarrow{N_V}$$

$$\xrightarrow{C_7 = 0}$$

$$\xleftarrow[R_7^{C_7} = 1]{}$$

Prover (RFID token)

Secret key K

Function h

Calculate

$h(K, N_V) = R$

Split $R = R_0 || R_1$

1 0 0 1 1 0 1 1 $\leftarrow R^0$

0 1 1 1 0 1 1 0 $\leftarrow R^1$

1

0

Protocol description

Verifier (RFID reader)
Secret key K
Function h
Generate nonce N_V

Generate random bits
$C_1, \ldots, C_n$

$\langle C_i \rangle = 01001100$
$\left\langle R_i^{C_i} \right\rangle = 11010111$

$\xrightarrow{N_V}$

$\xrightarrow{C_8 = 0}$

$\xleftarrow{R_8^{C_8} = 1}$

Prover (RFID token)
Secret key K
Function h

Calculate
$h(K, N_V) = R$
Split $R = R_0 || R_1$

1 0 0 1 1 0 1 1 $\leftarrow R^0$
0 1 1 1 0 1 1 0 $\leftarrow R^1$

Protocol description

Verifier
Secret key K
Function h

$\langle C_i \rangle = 01001100$

Expected $\left\langle R_i^{C_i} \right\rangle$

1 1 0 1 0 1 1 1

Received $\left\langle R_i^{C_i} \right\rangle$

1 0 1 0 0 1 0 1

$\xrightarrow{N_V}$

$\xrightarrow{C_i}$

$\xleftarrow[R_i^{C_i}]{}$

Attacker
Secret key K
Function h

1 0 1 0 1 0 0 1 $\leftarrow R^0$

1 0 1 0 0 1 1 0 $\leftarrow R^1$

- Verifier $\leftrightarrow$ Attacker
  - $\frac{1}{2}$ chance of guessing a response bit correctly

Protocol description

Verifier
Secret key K
Function h

$\langle C_i \rangle = 01001100$

Expected $\langle R_i^{C_i} \rangle$
1 1 0 1 0 1 1 1
Received $\langle R_i^{C_i} \rangle$
1 0 1 0 0 1 0 1

$\xrightarrow{N_V}$
$\xleftarrow{R_i^{C_i}}$
$\xrightarrow[C_i]{}$

Malicious Prover
Secret key K
Function h

1 1 0 1 1 0 1 1 $\leftarrow R^0$
1 1 0 0 0 1 0 0 $\leftarrow R^1$

- Verifier $\leftrightarrow$ Malicious Prover
  - $\frac{1}{2}$ chance of guessing a response bit correctly

Protocol description

Verifier
Secret key K
Function h

$\langle C_i \rangle = 01001100$

Expected $\langle R_i^{C_i} \rangle$
1 1 0 1 0 1 1 1

Received $\langle R_i^{C_i} \rangle$
1 1 0 0 0 1 0 1

$\xrightarrow{N_V}$

$\xrightarrow{C_i}$ $\xleftarrow[R_i^{C_i}]{}$

Attacker
Secret key K
Function h

1 0 0 0 1 0 0 1 R^0
0 1 0 1 0 1 0 0 R^1

$\xrightarrow{N_V}$

$\xrightarrow{A_C}$ $\xleftarrow[R^{A_C}]{}$

Prover
Secret key K
Function h
$h(K, N_V) = R$

1 0 0 1 1 0 1 1 $\leftarrow R^0$
0 1 1 1 0 1 1 0 $\leftarrow R^1$

- Verifier $\leftrightarrow$ Attacker $\leftrightarrow$ Prover
  - $\frac{3}{4}$ chance of guessing a response bit correctly

Protocol description

Verifier
Secret key K
Function h

$\langle C_i \rangle = 01001100$

Expected $\langle R_i^{C_i} \rangle$
1 1 0 1 0 1 1 1

Received $\langle R_i^{C_i} \rangle$
1 1 0 1 0 1 1 1

$\xrightarrow{N_V}$

$\xrightarrow{C_i}$

$\xleftarrow{R_i^{C_i}}$

Attacker
Secret key K
Function h

0 1 0 0 1 0 1 1 R^0
0 1 1 1 1 0 1 0 R^1

1 0 0 1 1 0 1 1 R^0
0 1 1 1 0 1 1 0 R^1

$\xrightarrow{N_V}$

$\xrightarrow{A_C}$

$\xleftarrow{R^{A_C}}$

$\xrightarrow{N_V}$

$\xrightarrow{A_{\bar{C}}}$

$\xleftarrow{R^{A_{\bar{C}}}}$

Prover
Secret key K
Function h

$h(K, N_V) = R$

1 0 0 1 1 0 1 1 $\leftarrow R^0$
0 1 1 1 0 1 1 0 $\leftarrow R^1$

$h(K, N_V) = R$

1 0 0 1 1 0 1 1 $\leftarrow R^0$
0 1 1 1 0 1 1 0 $\leftarrow R^1$

- Overclocking attack
  - Prevented in hardware e.g. Bandpass filter

Protocol description

Verifier (RFID reader)		**Prover (RFID token)**
Secret key K Function h		Secret key K Function h
Generate nonce N_V	$\xrightarrow{N_V}$	
	$\xleftarrow{N_P}$	Generate nonce N_P
Generate random bits $C_1, \ldots, C_n$		Calculate $h(K, N_V, N_P) = R$ Split $R = R_0 \| \| R_1$ 1 0 0 1 1 0 1 1 $\leftarrow R^0$ 0 1 1 1 0 1 1 0 $\leftarrow R^1$
$\langle C_i \rangle = 01001100$	$\xrightarrow{C_1 = 0}$	0 0 1 1 0 1 1
$\langle R_i^{C_i} \rangle = 1$	$\xleftarrow{R_1^{C_1} = 1}$	1 1 1 0 1 1 0

- Overclocking attack
  - Alternative to hardware solutions

Noise

Bit errors will probably occur on the rapid exchange channel

- Accept if at least k bits out of n are correct
  - False accept:

$$p_{\mathrm{FA}} = \sum_{i=k}^{n} \binom{n}{i} \cdot \left(\frac{3}{4}\right)^{i} \cdot \left(\frac{1}{4}\right)^{n-i}$$

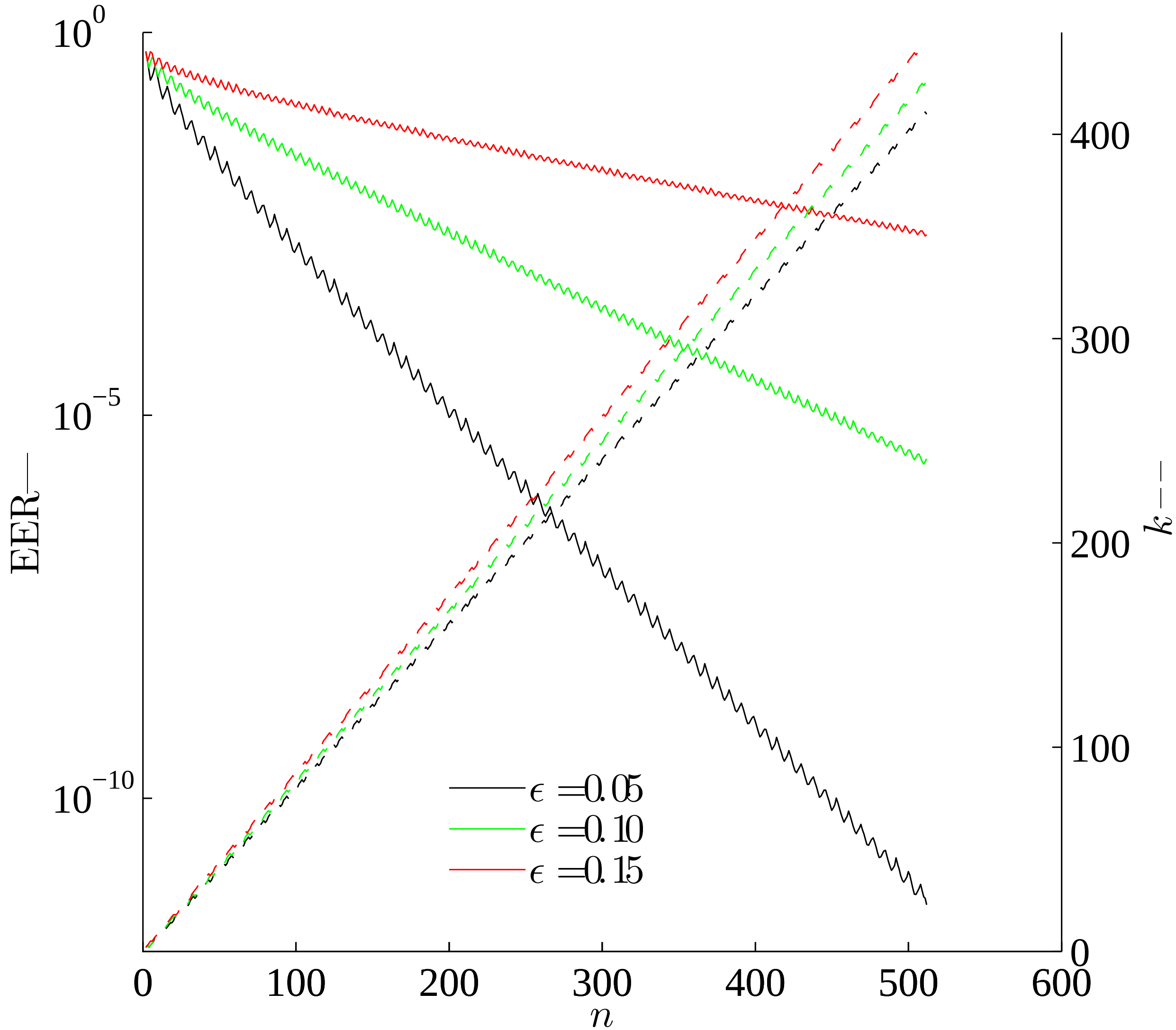
  - False reject:

$$p_{\mathrm{FR}} = \sum_{i=0}^{k-1} \binom{n}{i} \cdot (1-\epsilon)^{i} \cdot \epsilon^{n-i}$$

where ϵ is the bit-error probability.

Noise (2)

Example of parameter tradeoffs in the presence of noise



Related work

$$t_{\mathrm{m}} = 2 \cdot t_{\mathrm{p}} + t_{\mathrm{d}}$$

$$d = v_{\mathrm{p}} \cdot \frac{t_{\mathrm{m}} - t_{\mathrm{d}}}{2}$$

t_{m} = round trip time

t_{p} = one-way propagation time

t_{d} = processing delay

d = distance

v_{p} = signal propagation speed

Distance Bounding Protocols

- Beth and Desmedt (1991)
- Brands and Chaum (1993)

Brands and Chaum

Verifier (RFID reader)		**Prover (RFID token)**
Generate random bits $C_1, \ldots, C_n$		Generate random bits $m_1, \ldots, m_n$
	$\xleftarrow{\text{commit}(m)}$	
	$\xrightarrow{C_i}$	
	$\xleftarrow[R_i]{}$	$R_i = C_i \oplus m_i$
Verify commit	$\xleftarrow{\text{open commit}}$	message $M =$
Verify sign(M)	$\xleftarrow{\text{sign}(M)}$	$C_i \,\lvert R_i\rvert \ldots \lvert C_n\rvert\, R_n$

- Time round trip of single bit exchange
- Processing with variable delay done beforehand
- Minimal processing delay during bit exchange

Brands and Chaum

Verifier (RFID reader)		**Prover (RFID token)**
Generate random bits $C_1, \ldots, C_n$		Generate random bits $m_1, \ldots, m_n$
	$\xleftarrow{\text{commit}(m)}$	
	$\xrightarrow{C_i}$	$R_i = C_i \oplus m_i$
	$\xleftarrow[R_i]{}$	
Verify commit	$\xleftarrow{\text{open commit}}$	message $M =$
Verify sign(M)	$\xleftarrow{\text{sign}(M), C, R}$	$C_i \,\vert R_i\vert \ldots \vert C_n\vert\, R_n$

- Additional commit and sign operations
- Additional bits on slow channel
  - In presence of noise C and R need to be transmitted

Performance vs Brands and Chaum

For $\mathrm{EER} = 10^{-4}$ and $\epsilon = 0.1$

Assume bit exchange rate $= f_{\mathrm{carrier}}/4$

Standard	Time (B and C) $n = 70$	Time (Our protocol) $n = 360$
15693 ‘fast’ 26.4 kbp/s, 13.56 MHz	5.3237 ms	0.1062 ms
15693 ‘long’ 6.62 kbp/s, 13.56 MHz	21.1687 ms	0.1062 ms
14443 A/B 106 kbp/s, 13.56 MHz	1.3414 ms	0.1062 ms

Performance vs Brands and Chaum (2)

For $\mathrm{EER} = 10^{-10}$ and $\epsilon = 0.05$

Assume bit exchange rate $= f_{\mathrm{carrier}}/4$

Standard	Time (B and C) $n = 125$	Time (Our protocol) $n = 440$
15693 ‘fast’ 26.4 kbp/s, 13.56 MHz	9.5066 ms	0.1298 ms
15693 ‘long’ 6.62 kbp/s, 13.56 MHz	37.8012 ms	0.1298 ms
14443 A/B 106 kbp/s, 13.56 MHz	2.3954 ms	0.1298 ms

Positioning technology

Positioning Technology used today

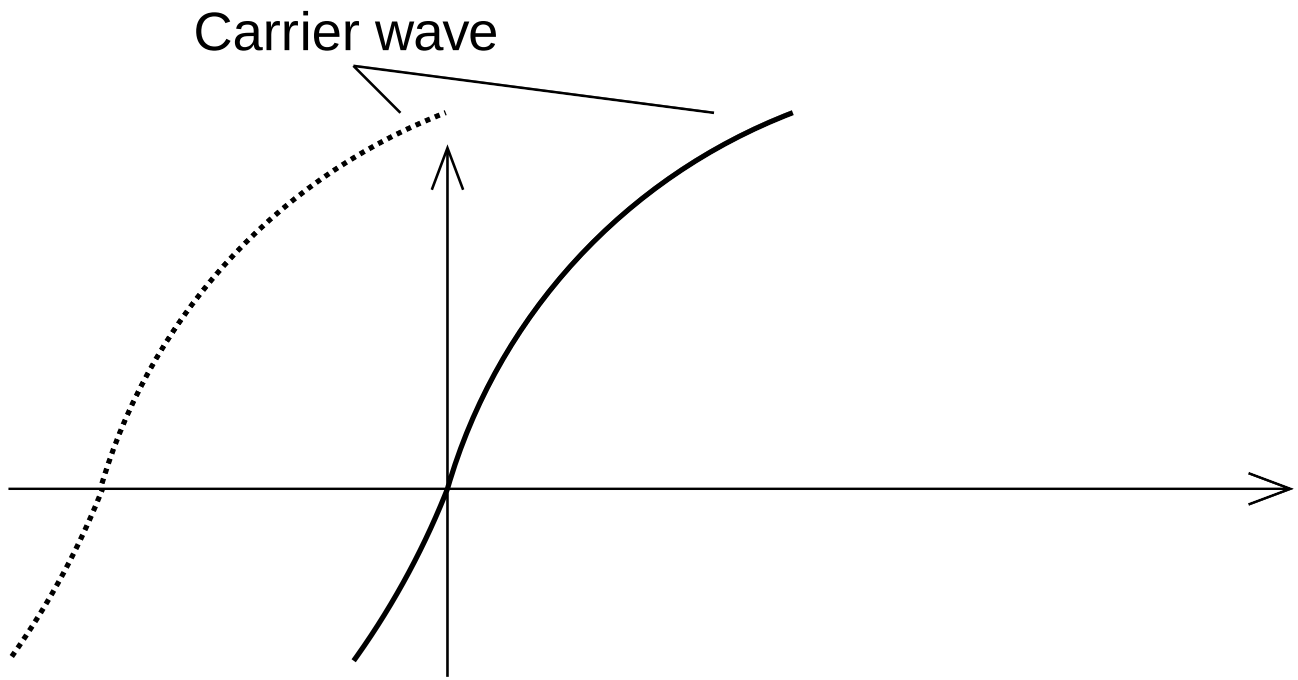
- Radio Frequency
  - Secure but complex
- Ultrasound
  - Appear closer by relaying data with faster RF link
- Received Signal Strength
  - Amplified signal appears closer

Resolution

Estimate $r \approx \frac{c}{B}$, where B is the channel bandwidth

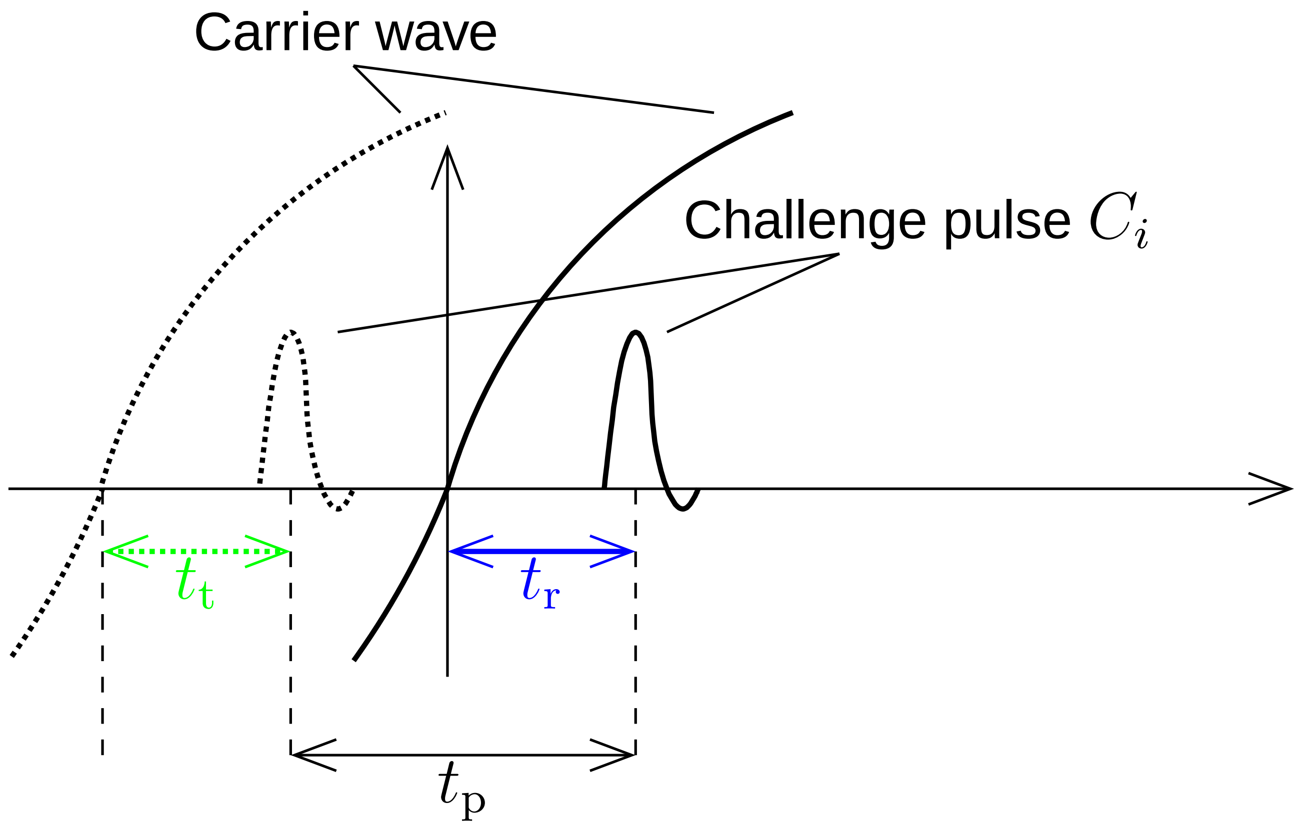
- RFID communication inadequate
  - e.g. for ISO 14443 at 106 kbp/s, $r \approx$ 3 km
- Ultra Wideband Pulses
  - Higher bandwidth equals better resolution
- RFID implementation issues
  - Error free operation requires high resources
    e.g. synchronization, bit placement
  - Crude implementation possible but would allow bit errors
  - Sufficient for bit exchange channel
  - Not to be used for normal communication

Proposed bit exchange channel



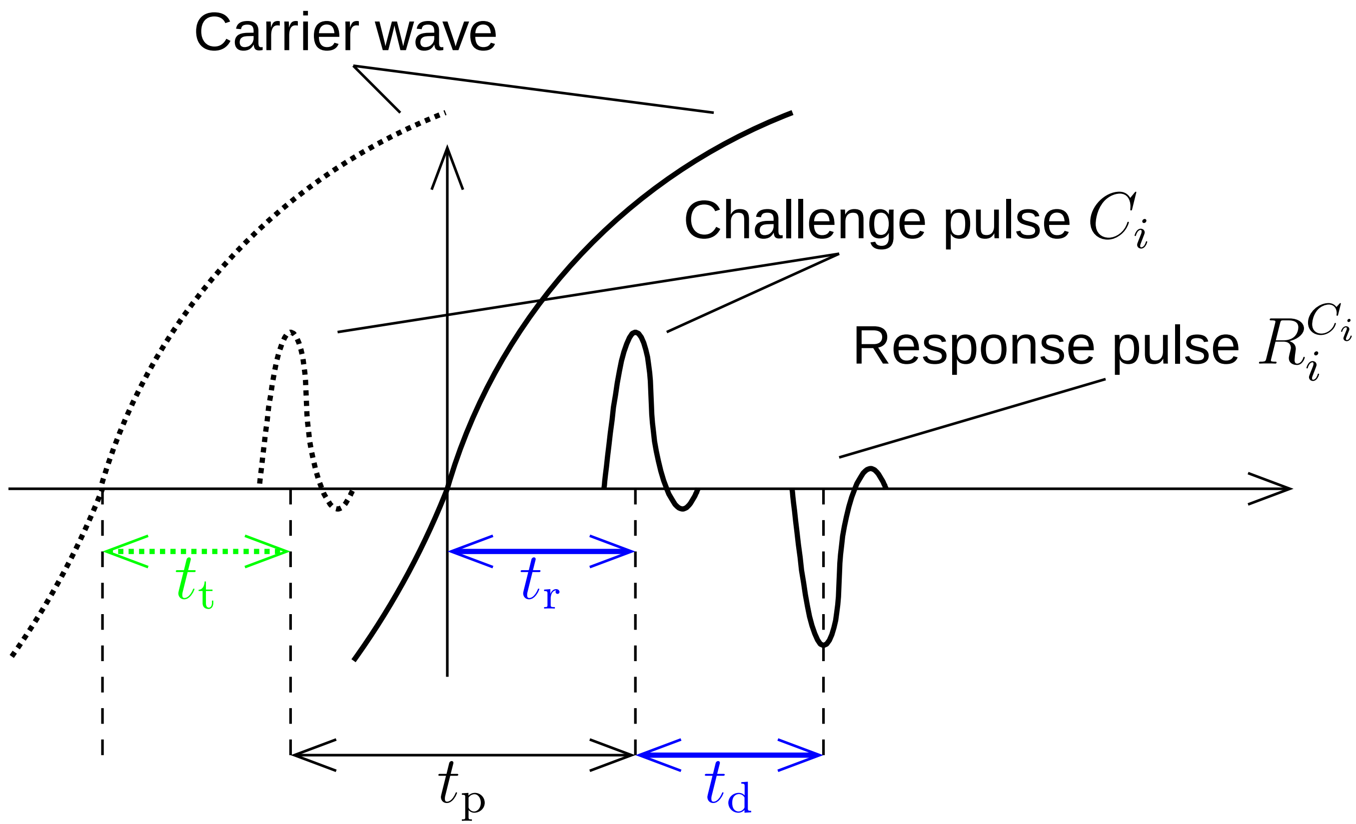
- Use carrier for loose synchronization
  e.g. Zero crossing

Proposed bit exchange channel



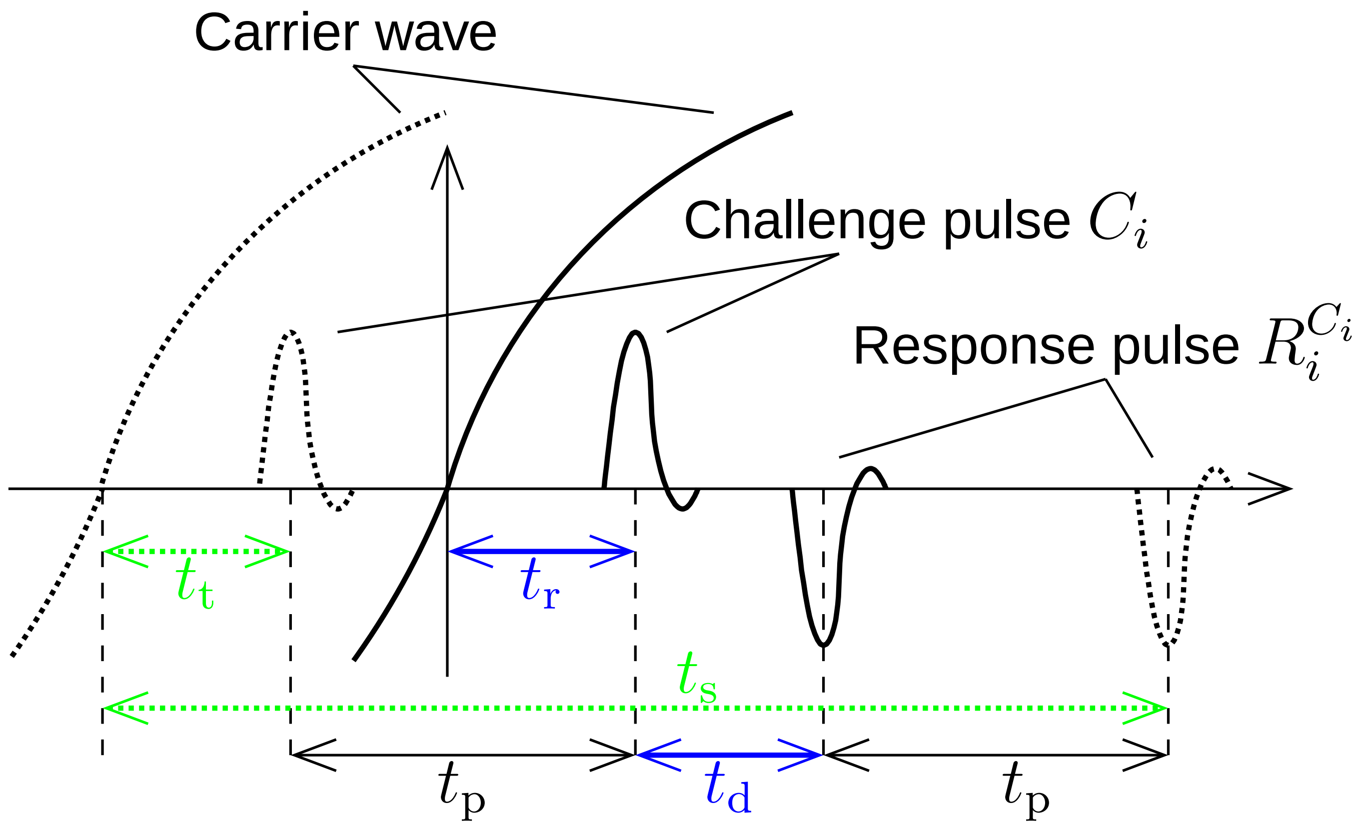
- Reader (Verifier) adjusts t_{t} to match sampling delay t_{r} in the token (Prover)

Proposed bit exchange channel



- t_d is a predictable hardware delay

Proposed bit exchange channel



$$d = c \cdot (t_s - t_t - t_d)/2$$

Conclusion

- Few more bit exchanges to achieve same cryptographic security
  - Chance of attacker guessing correct response $\frac{3}{4}$ vs $\frac{1}{2}$
- Faster operation
  - Extra bits transmitted on faster bit exchange channel
  - Much less data transmitted on slow error corrected channel
- Practical implementation suited for RFID
  - Low power and processing requirements for Prover
  - Timing-sensitive measurements and adjustments done by the Verifier
  - Faster completion of protocol suited for RFID environment

Future work

- Practical implementation
  - Pseudorandom functions suited for RFID device
  - Rapid bit exchange channel
  - UWB antennas for card form factor
- Mutual distance bounding protocol
  - For applications where illegitimate reading attempts are more common e.g e-Passports