Distance-bounding protocols

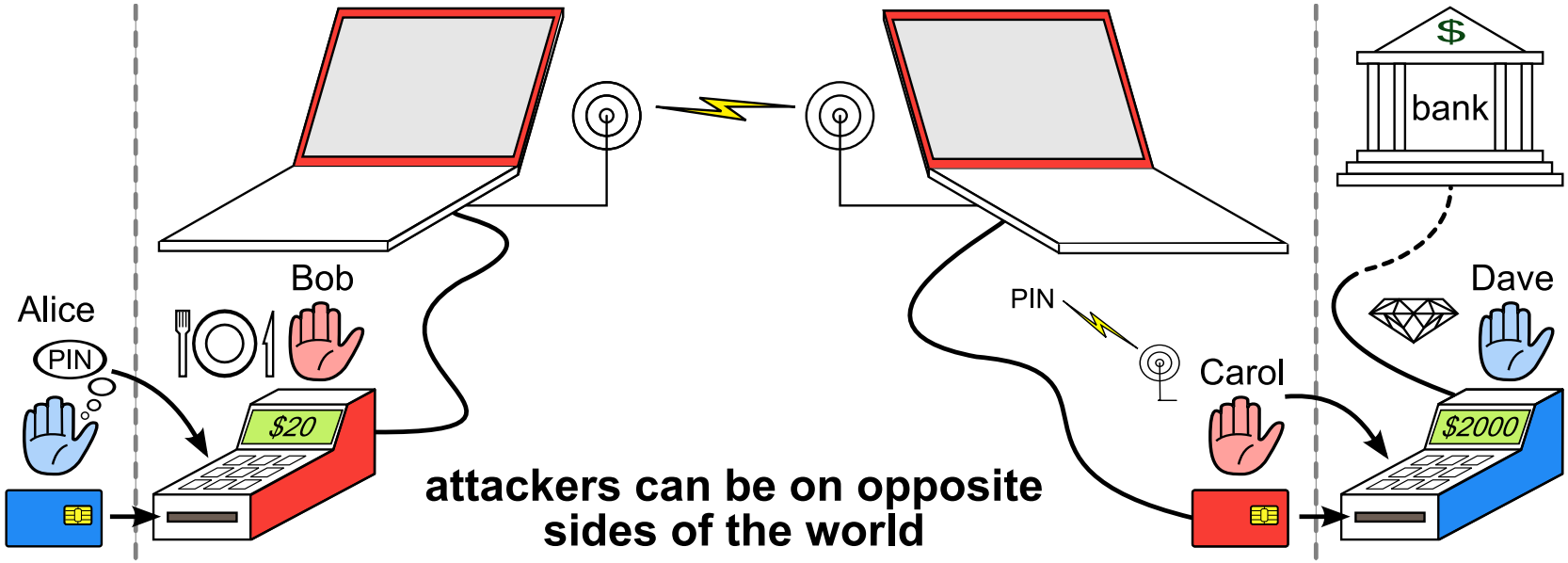
Markus Kuhn

UNIVERSITY OF
CAMBRIDGE

Department of Computer
Science and Technology

`https://www.cl.cam.ac.uk/~mgk25/`

Relay attacks



[Drimer/Murdoch 2007]

- 2008 demonstration of EMV Chip&PIN relay attack on BBC TV
- card terminals tolerated delays of many seconds
- concerns about contact-less EMV transaction (no PIN up to £30)

`https://www.lightbluetouchpaper.org/2007/02/06/chip-pin-relay-attacks/`
`https://www.youtube.com/watch?v=X7pjUIxKoEc`

Distance-bounding protocols

- cryptographic challenge-response authentication protocol
- designed to provide strong upper bound for distance to proofer
- tight bounds (metres) difficult over regular data-communication channels (length of single bit, variability in bitrates, packet latency, headers and checksum trailers)

Applications:

- car keys (passive keyless entry and start)
  `https://www.west-midlands.police.uk/news/watch-police-release-footage-relay-crime`
  `https://www.youtube.com/watch?v=SvriRoD9ZWk`
- card-present payment transactions
- RFID door access control
- desktop authentication
- road-toll OBU
- military friend-foe identification
- prisoner tagging
- wireless sensor network security (wormhole routing attacks)

Location-finding techniques

Received Signal Strength (RSS): Uses the inverse relationship between signal strength and distance to estimate the distance to other nodes.

- But attacker can alter received signal strength: amplifier, higher-gain antenna, relay transponder, etc.

Angle-of-Arrival (AoA): Examines the directions of received signals to determine the locations of transmitters or receivers.

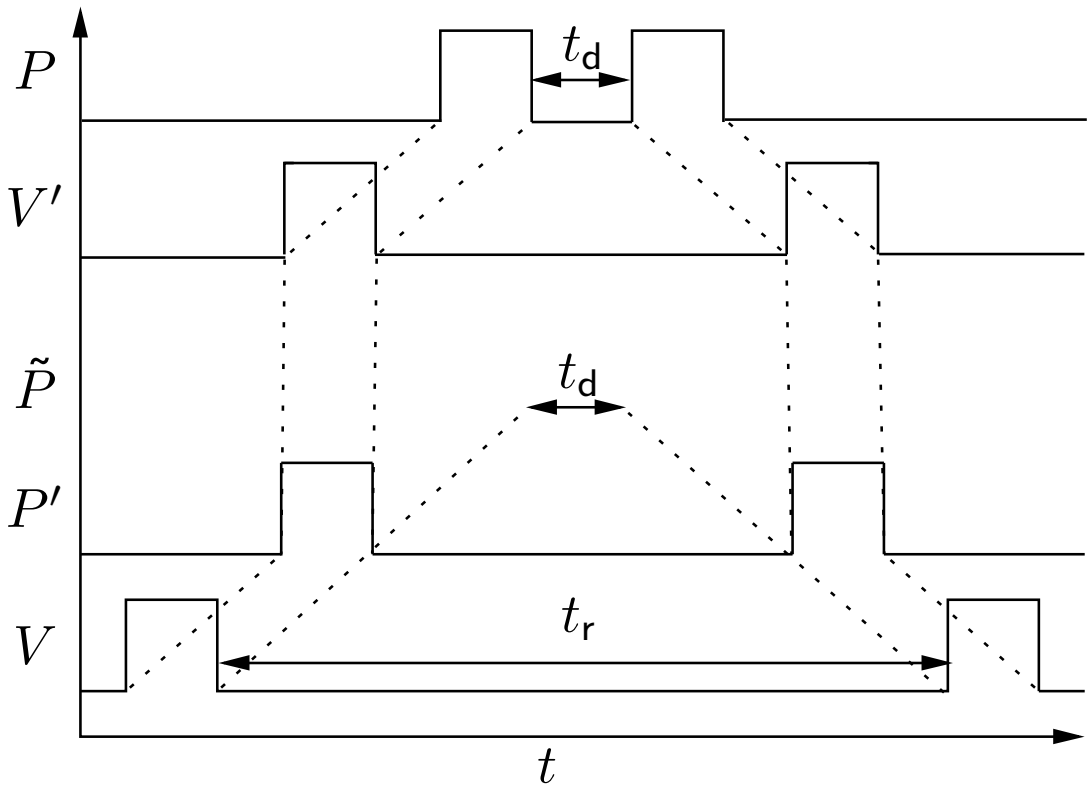
- But attacker can reflect/retransmit from a different direction.

Time-of-Flight (ToF): Measures elapsed time for a message exchange to estimate distance based on the communication medium's propagation speed.

- General Relativity: Universe does not propagate information faster than 30 cm/ns $=$ 300 m/μs $=$ 300 km/ms $= 3 \times 10^8$ m/s.
- Method of choice for high-security distance-bounding approaches.
- Practical near speed-of-light channels: contact, NFC, radio, optical

Acoustic/ultrasonic signals can be relayed via radio

Chose medium with propagation speed c close to speed of light.
Otherwise:



The vertical axis represents position. In this relaying attack, an attacker places a fake prover P' and a fake verifier V' near the actual verifier V and prover P, respectively. The exchanged data is related between P' and V' via a fast radio link. The shortened round-trip time t_r makes V believe that P is at the nearer position $\tilde{P}$.

Naïve approaches

Distance-bounding protocols: adapted authentication protocols to establish an upper bound for the distance of a prover P to a verifier V.

First attempt: a normal authentication protocol with a tight timing constraint:

$$\begin{aligned} V_{t_1} \to P_{t_2} : &\qquad C \in_{\mathsf{r}} \{0,1\}^n \\ P_{t_3} \to V_{t_4} : &\qquad R = \mathsf{Mac}_K(C) \end{aligned}$$

The distance bound is then

$$d(P,V) \leq \frac{t_{\mathsf{r}} - t_{\mathsf{d}}}{2c} = \frac{(t_4 - t_1) - (t_3 - t_2)}{2c}$$

where c is the signal propagation speed, t_{r} is the challenge-response round-trip time, and t_{d} is the processing delay in the prover P.

Problems with regular challenge-response protocols

- cryptographic functions (e.g., MAC) can take thousands of clock cycles to compute
- their inputs and outputs can take hundreds of clock cycles to transmit
- 10 000 clock cycles at 10 MHz = 1 ms
- Basic crystal oscillator – 10^{-4} (100 ppm) relative frequency error
  1 ms $\pm$ 100 ns means $\pm$15 m distance error
- Internal RC oscillator – 10^{-1} relative frequency error
  1 ms $\pm$ 0.1 ms means $\pm$15 km distance error

  Contactless smartcards usually lack crystal oscillators and rely on terminal to provide time reference (RF carrier) to clock communication; may use internal RC circuit and LC tuning of antenna to bound clock frequency.

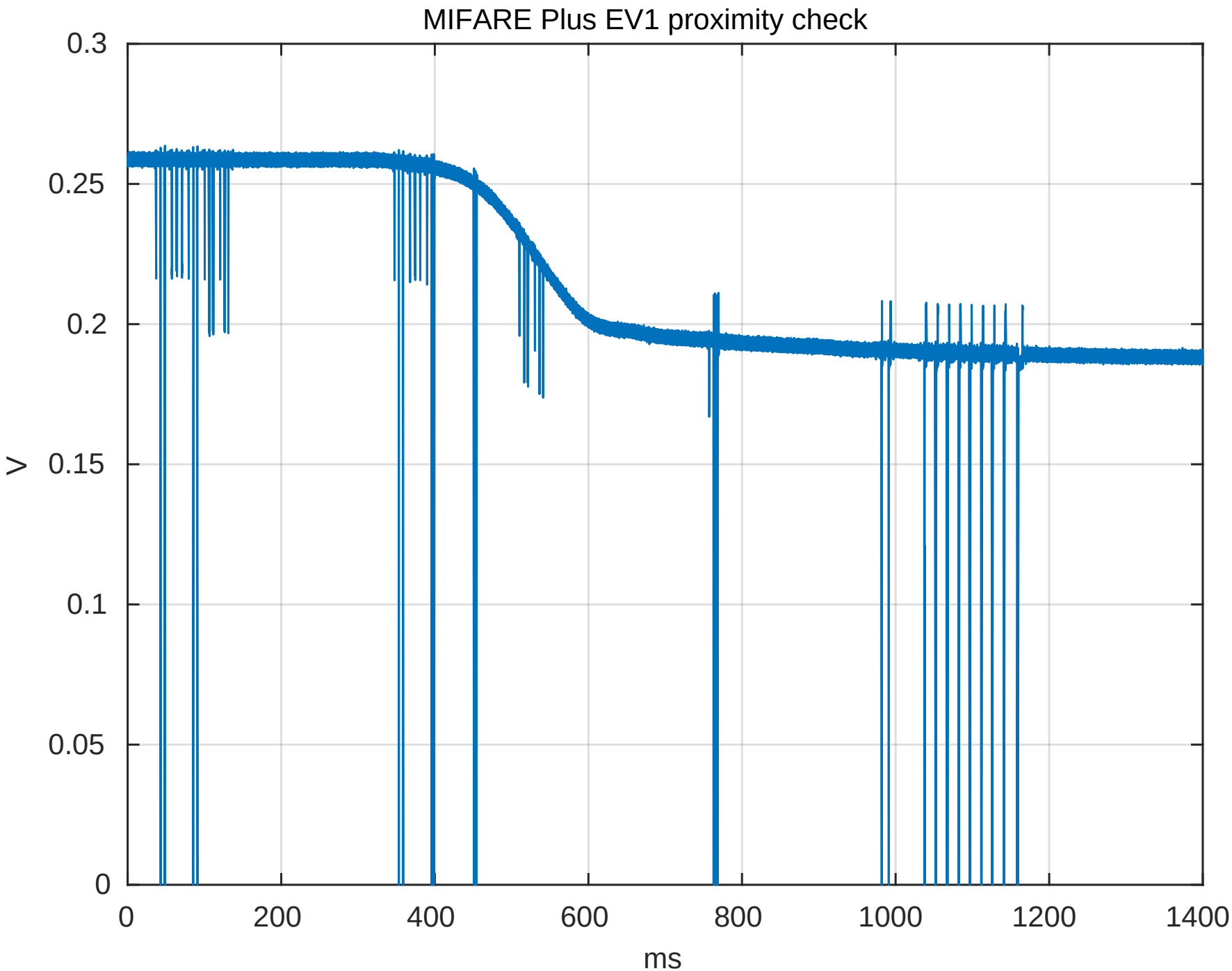
Trusted prover with trusted sampling clock

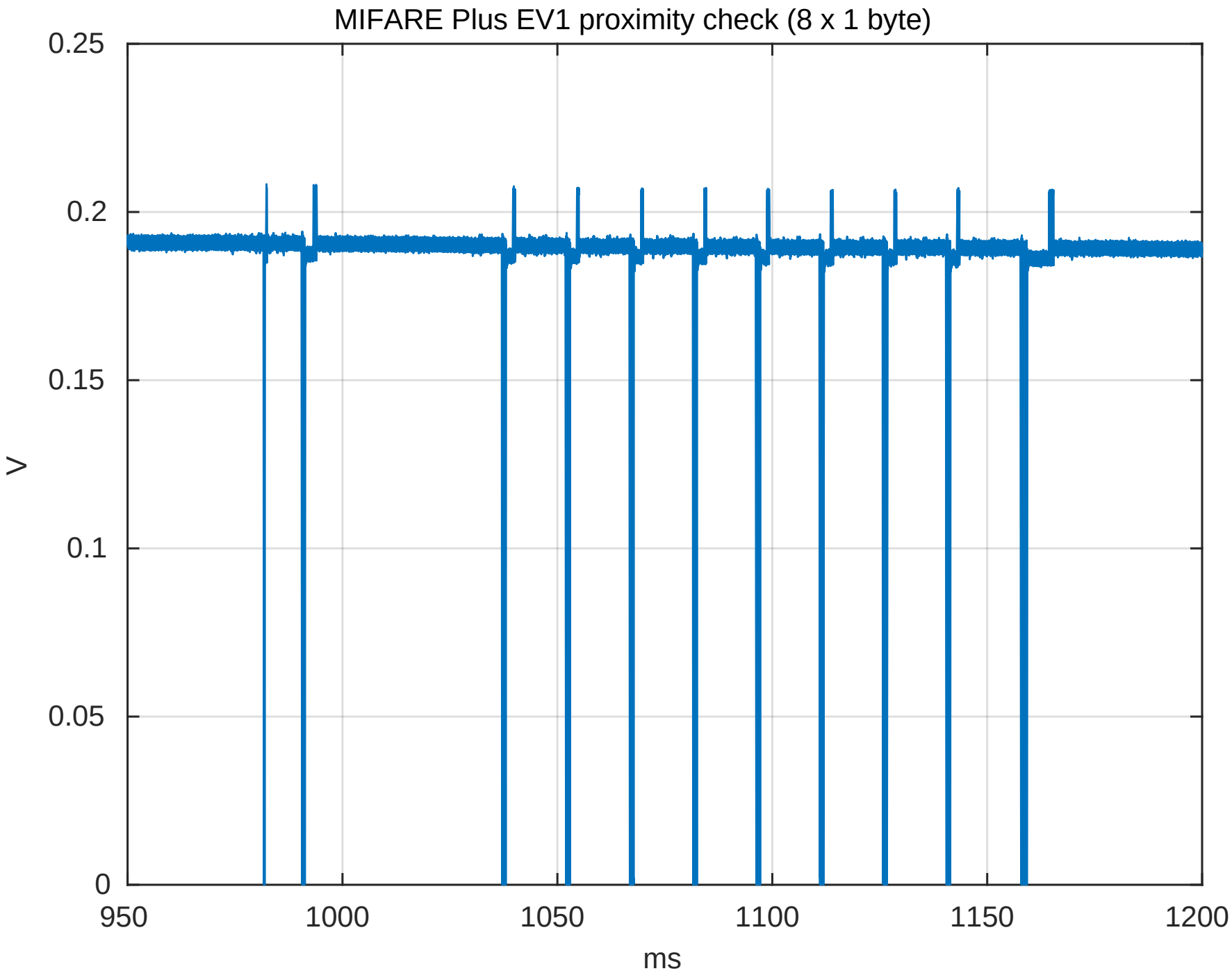
If a prover P is completely trusted (tamper-resistant hardware, tamper-resistant and stable reference clock):

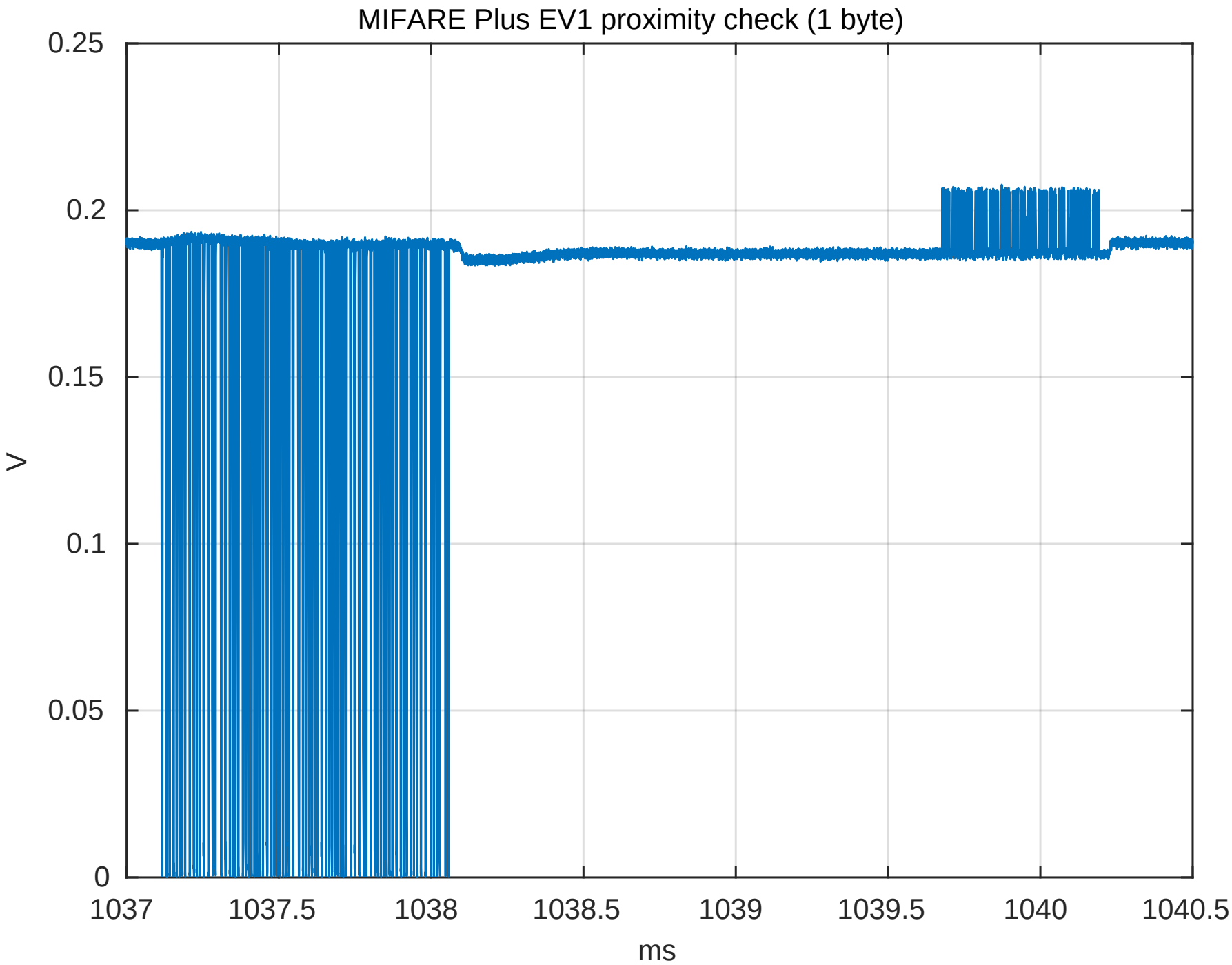
- V generates n random bits $C = C_1 C_2 \ldots C_n$
- P generates n random bits $R = R_1 R_2 \ldots R_n$
- P and V exchange parameters: $(t_R - t_C, n, \Delta t)$
- V sends C
- P samples incoming random bits $C = C_1 C_2 \ldots C_n$ at times $t_{i,C} = t_C + i \cdot \Delta t$ $(i \in \{1, \ldots, n\})$
- P sends its own random bits $R = R_1 R_2 \ldots R_n$ at times $t_{i,R} = t_R + i \cdot \Delta t$ $(i \in \{1, \ldots, n\})$
- P confirms to V the exchanged data afterwards (not time critical): $P \to V : \mathrm{Mac}_K(t_R - t_C, n, \Delta t, C, R)$

With relative frequency error η in P's clock, the resulting distance uncertainty is approximately $\eta c |t_R - t_C|$. Therefore keep $|t_R - t_C|$ as small as possible: $|t_R - t_C| \approx 0$ if duplex transmission is available and $|t_R - t_C| \approx \Delta t(n+1)$ on half-duplex channels.

Commercial implementation: MIFARE Plus/DESFire Proximity Check


MIFARE Plus EV1 proximity check
0.3
0.25
0.2
0.15
0.1
0.05
0
V
0
200
400
600
800
1000
1200
1400
ms


MIFARE Plus EV1 proximity check (8 x 1 byte)
0.25
0.2
0.15
0.1
0.05
0
V
950
1000
1050
1100
1150
1200
ms


MIFARE Plus EV1 proximity check (1 byte)
0.25
0.2
0.15
0.1
0.05
0
V
1037
1037.5
1038
1038.5
1039
1039.5
1040
1040.5
ms

MIFARE Proximity Check

MIFARE Plus EV1 and DESFire EV2 RFID cards support now a basic distance-bounding protocol, running on top of the same standard ISO 14443-4 ("T=CL") protocol and ISO 7816-4 APDU format used for other card transactions.

- RF channel: 13.56 ± 2 MHz (ISO 14443 Type A)
- reader to card: 848 kbit/s, 1 bit $= 4.72$ µs
- card to reader: 212 kbit/s, 1 bit $= 1.18$ µs
- C and R are 8-bytes long each, can be sent all at once or split aross up to eight 1-byte APDUs
- header and CRC overhead due to T=CL and APDU wrapping
- challenge packet: 0.94 ms, response packet: 0.52 ms
- intra-packet gap: 1.7 ms promised, 1.6 ms actual
- 0.1–0.2 ms slack $\rightarrow$ 15 km distance uncertainty
- Linux protocol stack (USB CCID, PCSC-Lite, Perl Chipcard::PCSC::Card) round-trip latency: 14.67 ± 0.1 ms
  $\Rightarrow$ hardware timestamping support in reader desirable

```
reader = ACS ACR122U PICC Interface 00 00
->card 90 f0 00 00 00
<-card 01 06 a0 07 91 90
PubRespTime: 1696 µs
PPS1: 07
DS: 2, card->reader 211.875 kbit/s, etu=4.71976 µs
DR: 8, reader->card 847.5   kbit/s, etu=1.17994 µs
->card 90 f2 00 00 02 01 6c 00
<-card 4b 91 90
elapsed time: 14.632 ms
->card 90 f2 00 00 02 01 c1 00
<-card 78 91 90
elapsed time: 14.772 ms
->card 90 f2 00 00 02 01 8b 00
<-card b8 91 90
elapsed time: 14.652 ms
->card 90 f2 00 00 02 01 d6 00
<-card b9 91 90
elapsed time: 14.607 ms
->card 90 f2 00 00 02 01 0e 00
<-card fa 91 90
elapsed time: 14.7 ms
->card 90 f2 00 00 02 01 6d 00
<-card 11 91 90
elapsed time: 14.596 ms
->card 90 f2 00 00 02 01 f0 00
<-card 28 91 90
elapsed time: 14.593 ms
->card 90 f2 00 00 02 01 56 00
<-card 0d 91 90
elapsed time: 14.597 ms
mac input: fd 01 06 a0 07 4b 6c 78 c1 b8 8b b9 d6 fa 0e 11 6d 28 f0 0d 56
->card 90 fd 00 00 08 51 b2 50 b0 b8 8e c4 95 00
<-card 80 29 e5 4d 52 78 f2 28 91 90
```

EMV®
Contactless Specifications for Payment Systems

Book C-2

Kernel 2 Specification

Version 2.6
February 2016

3.10 Relay Resistance Protocol

3.10.1 Introduction

A relay attack is where a fraudulent terminal is used to mislead an unsuspecting cardholder into transacting, where the actual transaction is relayed via a fraudulent Card (or simulator) to the authentic terminal of an unsuspecting merchant. It may also be that a fraudulent reader is used without the cardholder being aware of the transaction.

3.10.2 Protocol

The relay resistance protocol works as follows:

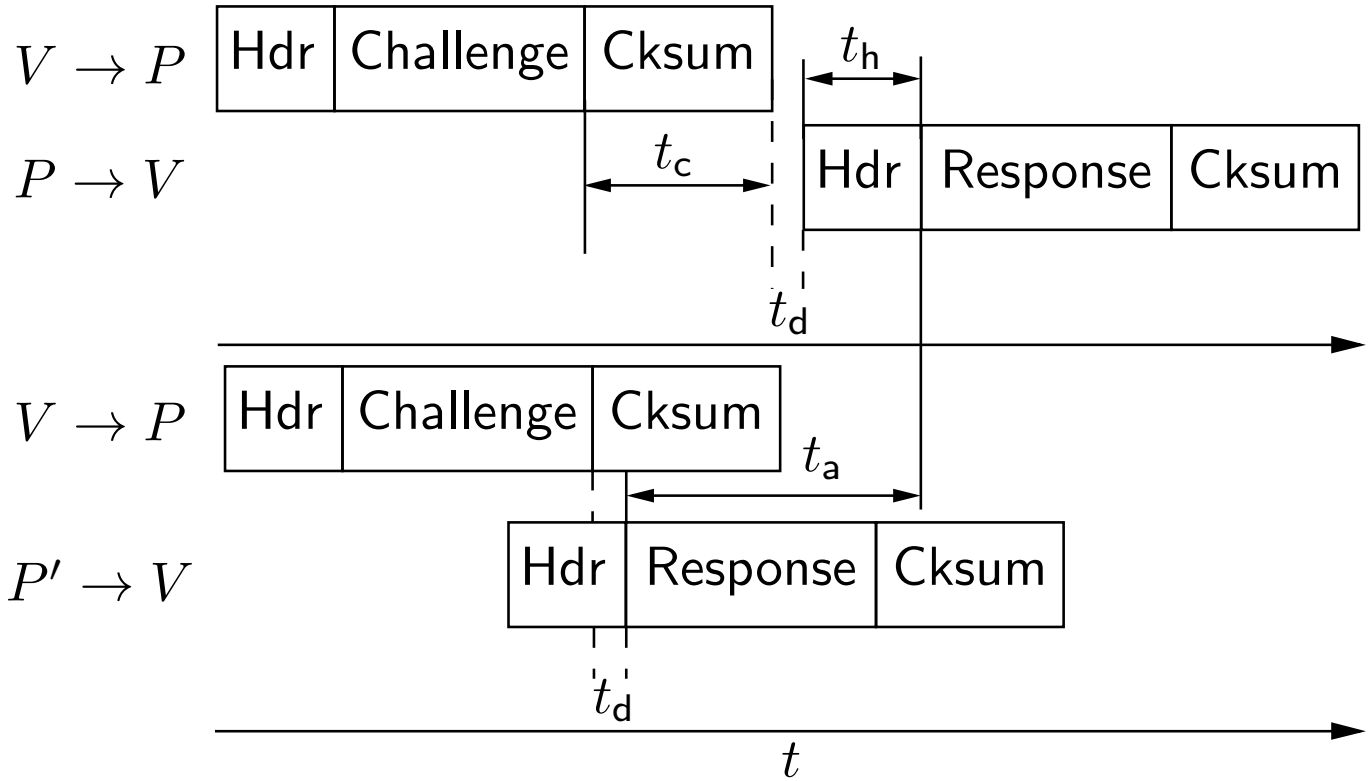
1. A bit in Application Interchange Profile is used to tell the Reader that the Card supports the relay resistance protocol. A bit in *Kernel Configuration* is used to configure the support of the relay resistance protocol by the Reader.
2. The Reader invokes the relay resistance protocol if both the Card and Reader support it. In this case it sends a timed C-APDU (EXCHANGE RELAY RESISTANCE DATA) to the Card with a random number (*Terminal Relay Resistance Entropy*). The Card responds with a random number (*Device Relay Resistance Entropy*) and timing estimates (*Min Time For Processing Relay Resistance APDU*, *Max Time For Processing Relay Resistance APDU* and *Device Estimated Transmission Time For Relay Resistance R-APDU*).
3. If the timings determined by the Reader exceed the maximum limit computed, the Reader will try again in case there was a communication error or in case other processing on the device interrupted the EXCHANGE RELAY RESISTANCE DATA command processing. The Reader will execute up to two retries.
4. *Terminal Verification Results* are used to permit the Reader to be configured

MasterCard Relay Resistance Protocol

- specified in EMV Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.6, February 2016
- timed exchange of two 32-bit random numbers + metadata
- integrated with EMV's existing "Combined Dynamic Data Authentication and Application Cryptogram Generation" (CDA) protocol
- lots of timing parameters provided by both card and terminal, not just maximum but also minimum values (0.1 ms resolution):
  - Min Time For Processing Relay Resistance APDU
  - Max Time For Processing Relay Resistance APDU
  - Device Estimated Transmission Time For Relay Resistance R-APDU
  - Minimum Relay Resistance Grace Period
  - Maximum Relay Resistance Grace Period
  - Relay Resistance Accuracy Threshold
  - Relay Resistance Transmission Time Mismatch Threshold
- specification lacks clear definitions of when to start and stop the timer (in relation to bit edges as seen on a 13.56 MHz AM demodulated ISO 14443-3 A/B channel)

Protocol headers permit low-latency bypass

If packet processing happens outside the trusted hardware module (e.g., TPM does only the MAC) and the trusted hardware interface is much faster than the communications channel used:



Normal communication hardware requires software to commit to the full data packet some time before the first bit is actually sent, and notifies the software some time after the last bit is received.

An attacker can use special hardware without these restrictions.

Low-latency relaying hardware

Fastest relay strategies: analog up-down conversion of carrier or direct modulation of baseband signal (AM, OOK, BSK, FM, FSK):

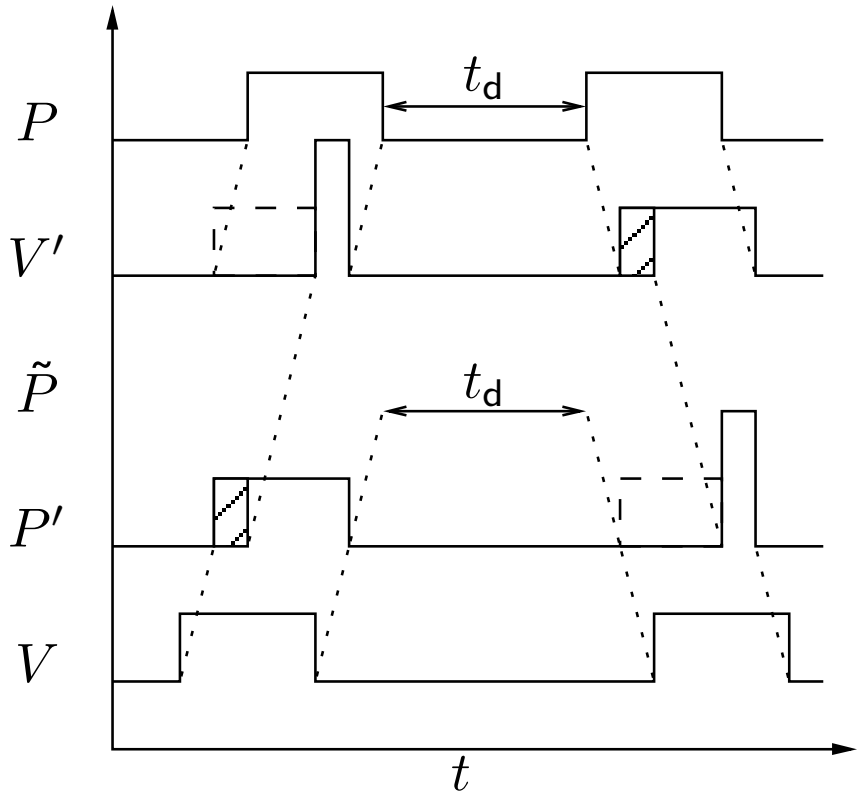
- Processing latency is dominated by the group delay (impulse response duration) of the analog filters involved, approximately 1/bandwidth, or $\approx 1 \ldots 5$ symbols.
- Without repeaters range of mobile UHF transmitters practically limited to a few kilometers (much more if airborn).

Various proprietary IoT UHF transceiver chips (e.g., Murata TRC103) support a low-latency "continuous mode" that bypasses packet buffering, passes each bit directly to the modulator, and thereby limits processing latency to a few tens of microseconds. Typical bitrates: 200–250 kbit/s.

Other transceivers (e.g., TI CC2420) offer pin signal when start-of-frame delimiter is detected. Still data packet latency, but accurate timing of packet arrival time. [Sommer, 2011]

Common standard digital wireless protocol implementations (802.11, Bluetooth, LTE, etc.) all add latencies of at least a few milliseconds, often more than 10 ms.

Special modulator delays commitment on bit value

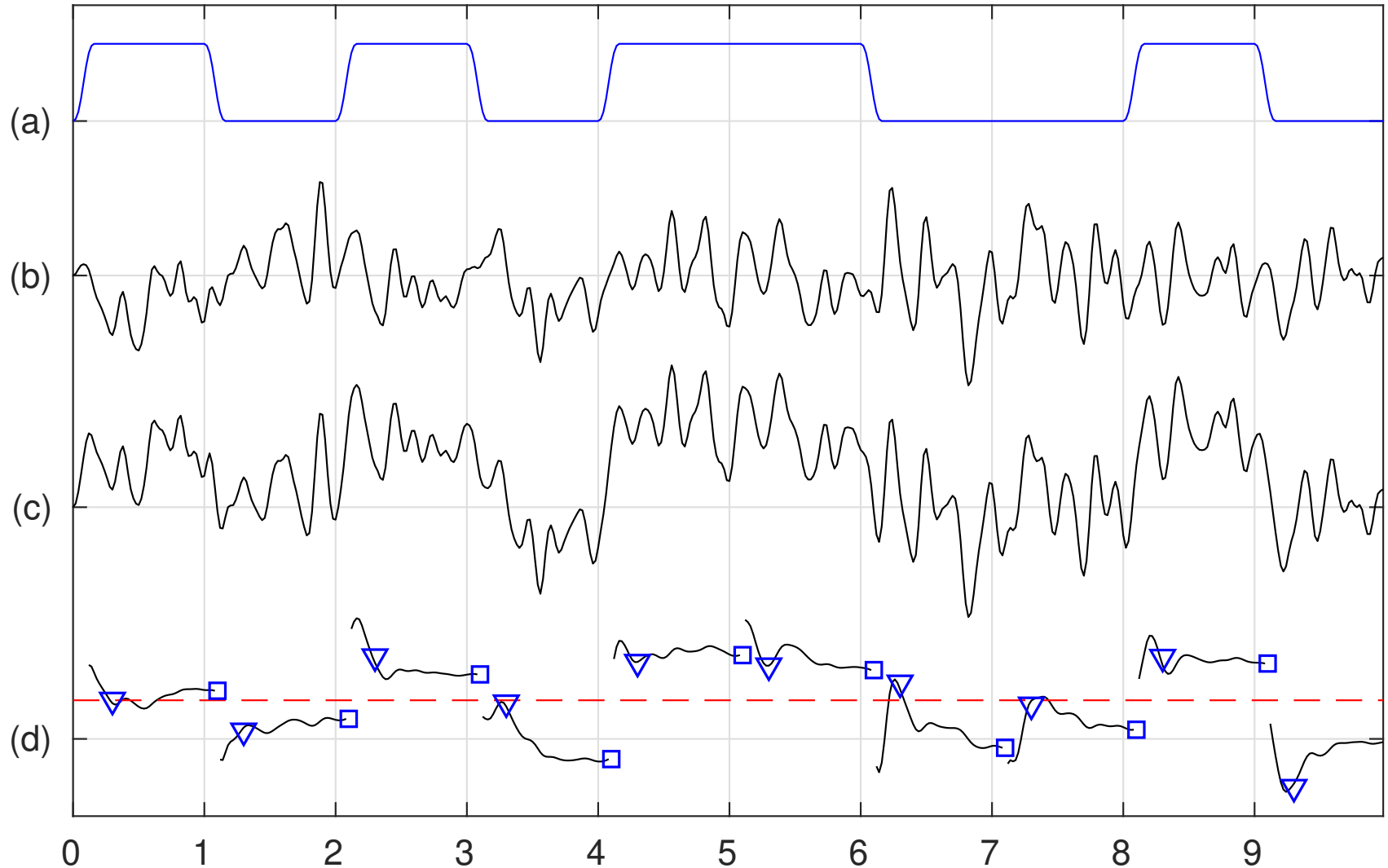


Standard symbol detectors integrate the signal received during the timeslot allocated to a bit, before deciding whether the total energy received was above or below the 0/1 decision threshold (matched filter).

An attacker can place the symbol's energy at the end of the bit slot and can decide on a bit value near the beginning of the slot, thereby bypassing some latency.

At 300 kbit/s (faster than most RFID protocols), a bit is 1 km long.

Special demodulator provides early bit estimate



(a) transmitted signal, (b) channel noise, (c) received signal, (d) integrator output in detector

Secure distance-bounding protocols

Principle 1: Use a communication medium with a propagation speed as close as possible to the physical limit for propagating information: the speed of light in vacuum.

This excludes not only acoustic communication techniques, but also limits applicability of wires and optical fibers.

Principle 2: Use a communication format in which only a single bit is transmitted and the recipient can instantly react on its reception.

This excludes most traditional byte- or block-based communication formats, and in particular any form of error correction.

Principle 3: Minimize symbol length.

In other words, output the energy that distinguishes the two possible transmitted bit values within as short a time as is feasible. This leaves the attacker little room to shorten this time interval further.

Principle 4: The protocol should cope well with substantial bit error rates during the rapid single-bit exchange.

Principle 3 limits the energy that can be spent on transmitting a single bit and conventional error correction is not applicable.

Secure distance-bounding protocols

If timing of communications channel may be manipulated by attacker, ask prover to instantly evaluate a fast function for each challenge bit:

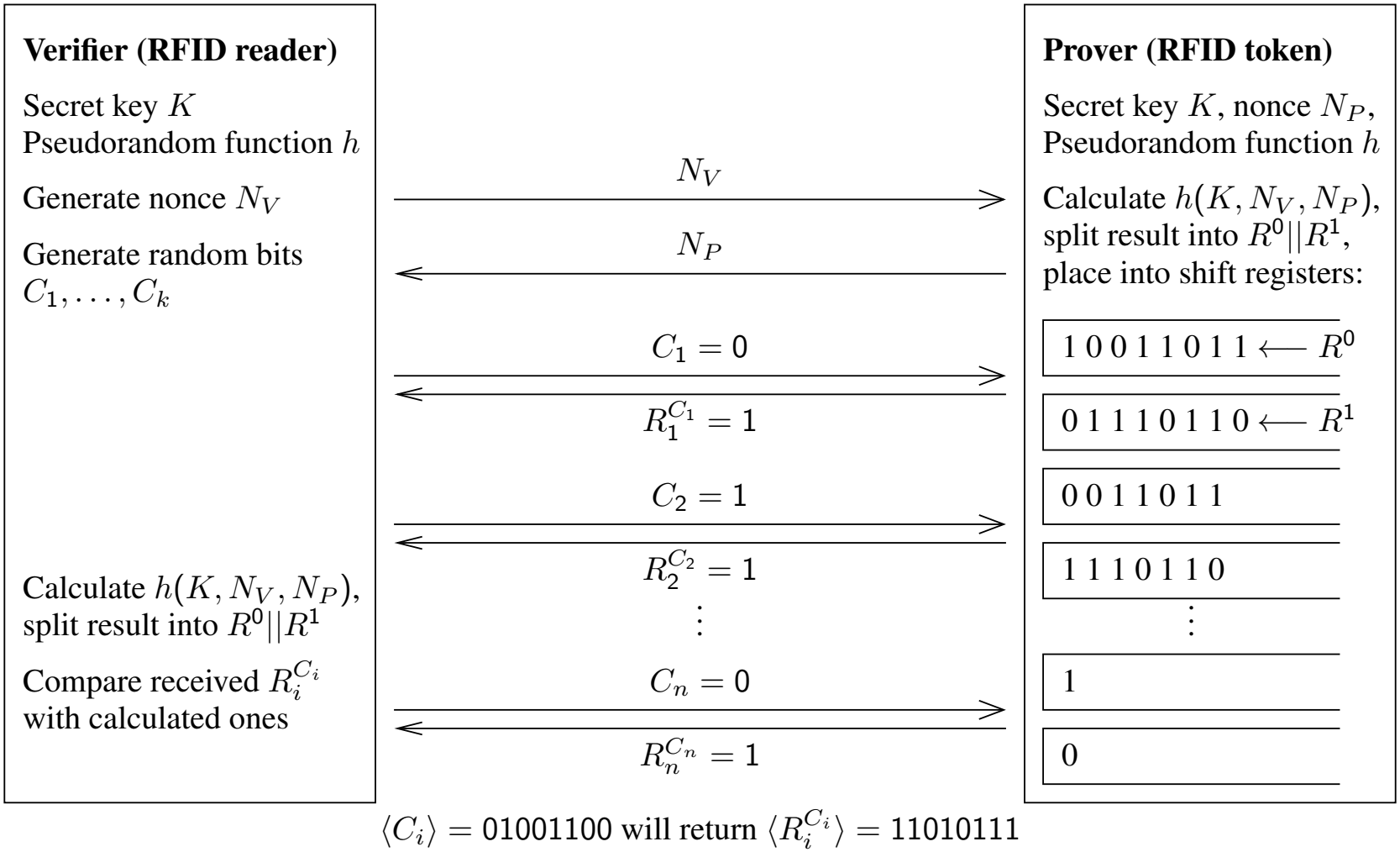
Brands/Chaum (1993): XOR

- V generates bit sequence C, P generates bit sequence M
- P commits to M.
- $\forall i : V$ sends bit C_i, P instantly answers $R_i = C_i \oplus M_i$
- P opens commitment on M and signs C.
- attacker can guess each M_i with 50% probability

Hancke/Kuhn (2005): 1-bit lookup

- avoids need for commitment and final signature, just needs some session-key setup (can be amortized with other transactions!)
- permits rapid/short bit exchange on noisy channel
- attacker can guess each R_i with 75% probability by guessing 50% of challenge bits correctly
- requires more rapid-response bits than Brands/Chaum for equal security, but saves other bits and can use faster bit rate due to error tolerance

Hancke/Kuhn protocol



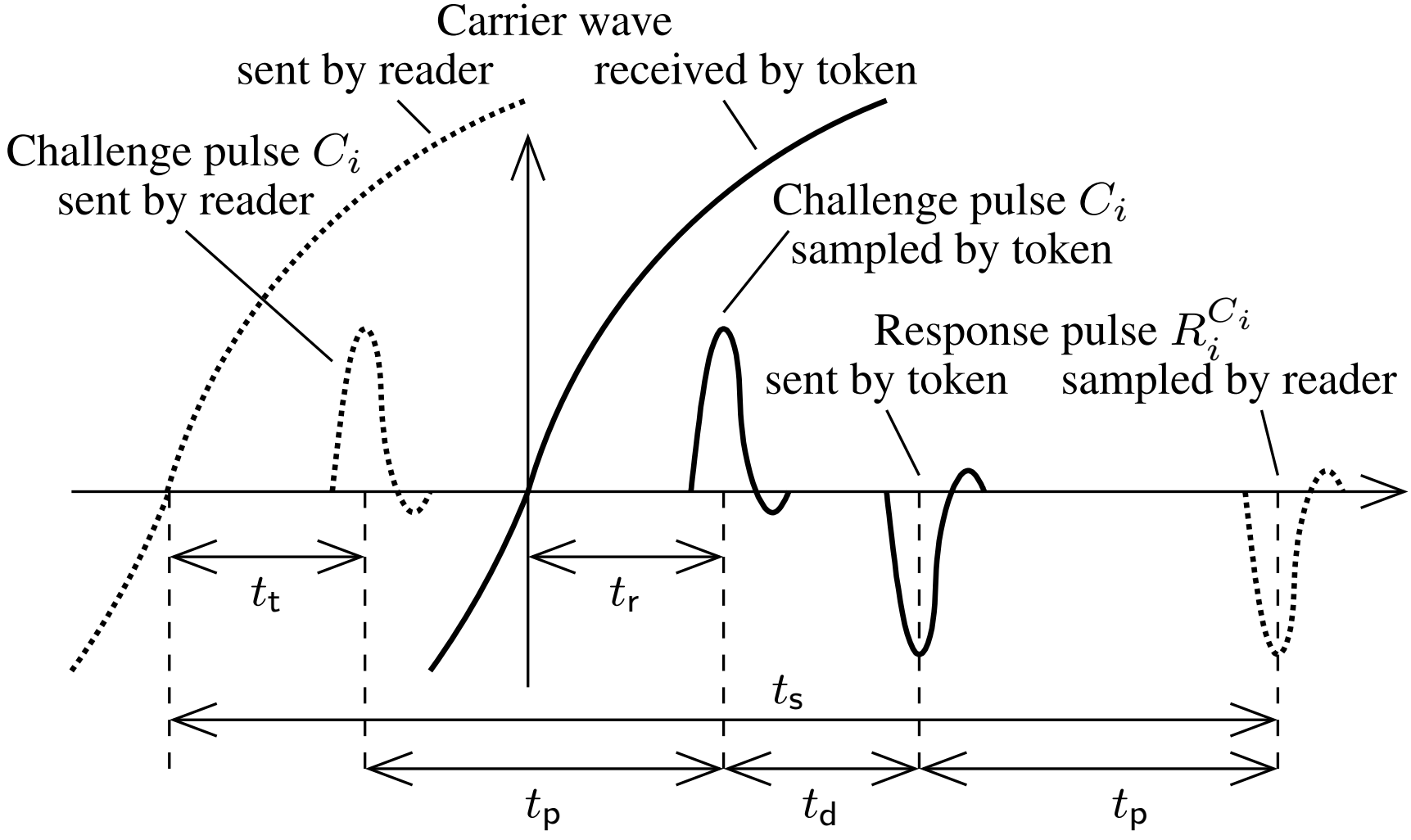
$\langle C_i \rangle = 01001100$ will return $\langle R_i^{C_i} \rangle = 11010111$

Security/robustness: V must get at least k of the n bits $R_i^{C_i}$ correctly.

False accept rate: $p_{\mathsf{FA}} = \sum_{i=k}^{n} \binom{n}{i} \cdot \left(\frac{3}{4}\right)^i \cdot \left(\frac{1}{4}\right)^{n-i}$

False reject rate: $p_{\mathsf{FR}} = \sum_{i=0}^{k-1} \binom{n}{i} \cdot (1-\epsilon)^i \cdot \epsilon^{n-i}$ (bit-error rate ϵ)

Ultra-wideband pulse communication (contactless)

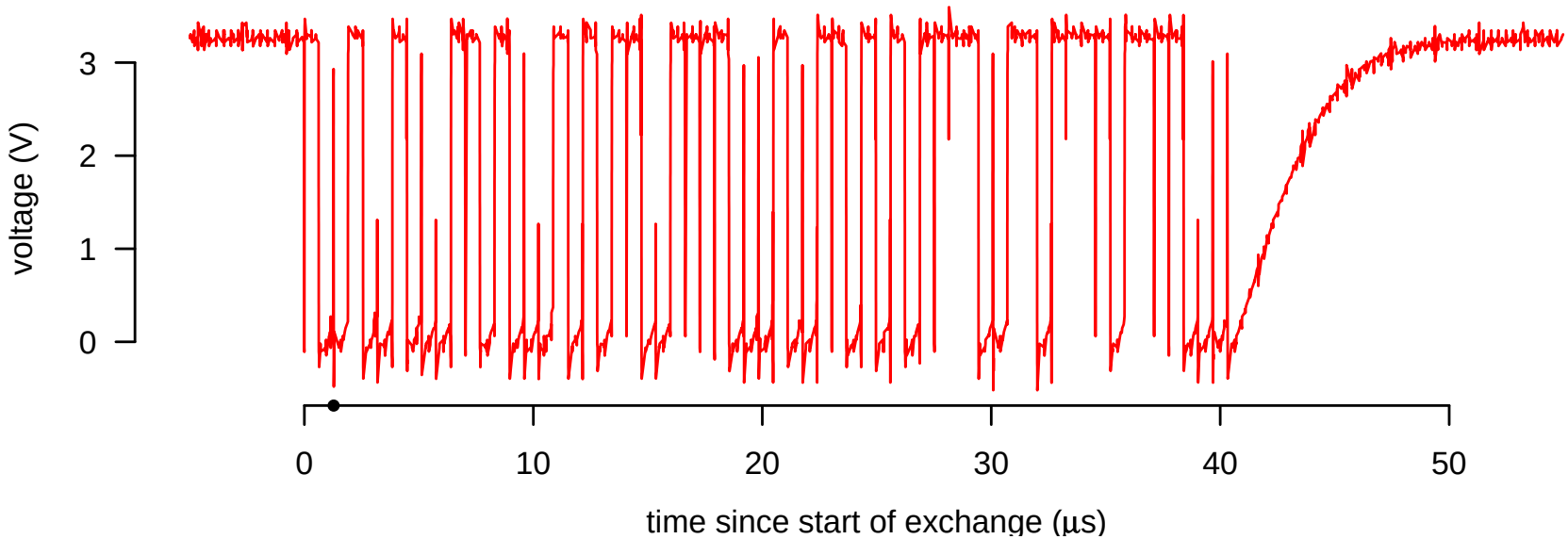


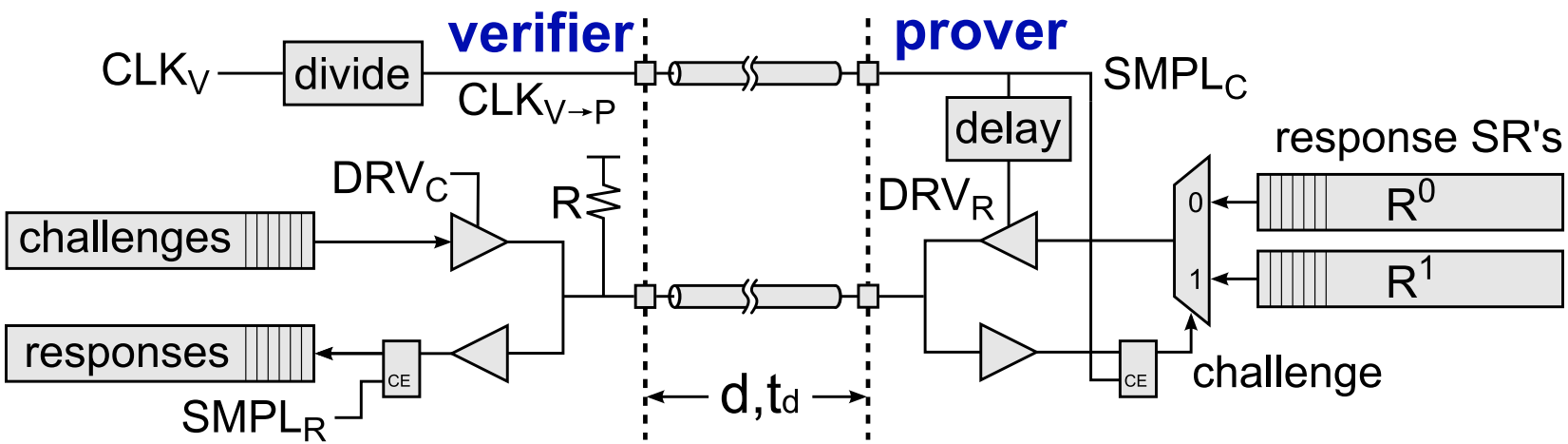
Asymmetric calibration requirement: prover can be low-cost token without trustworthy clock. Verifier (e.g., wall-mounted reader) performs a search to find the best t_t value to match circuit tolerances of t_r in prover.

Verifier may also search for best t_s to match t_d in prover chip and propagation delay t_p.

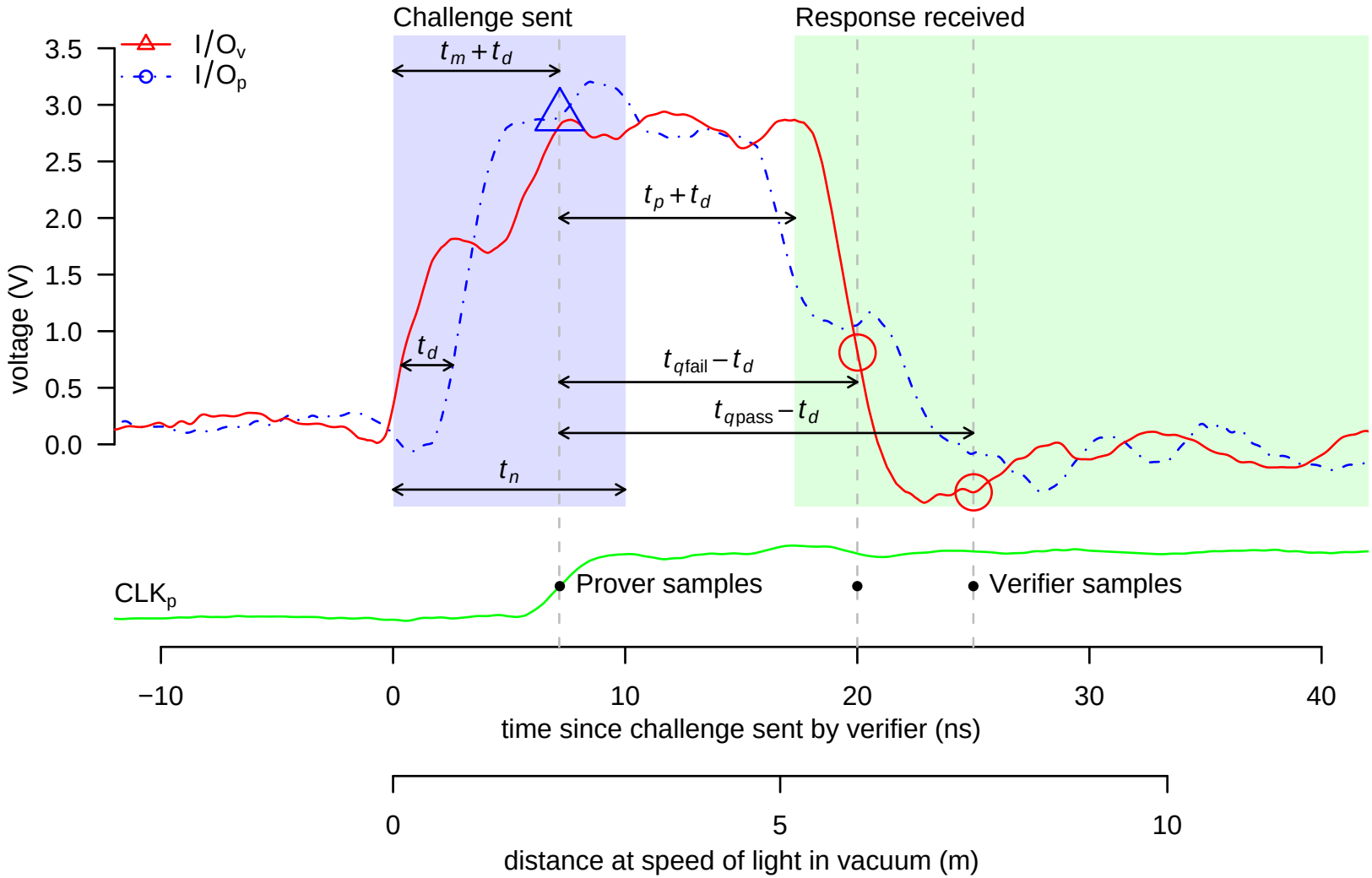
HK demonstration implementation (for ISO 7816 contacts)

Drimer/Murdoch 2007: Hancke/Kuhn over ISO 7816-style half-duplex contact interface with 25 ns roundtrip time (3.75 m abs. distance bound).

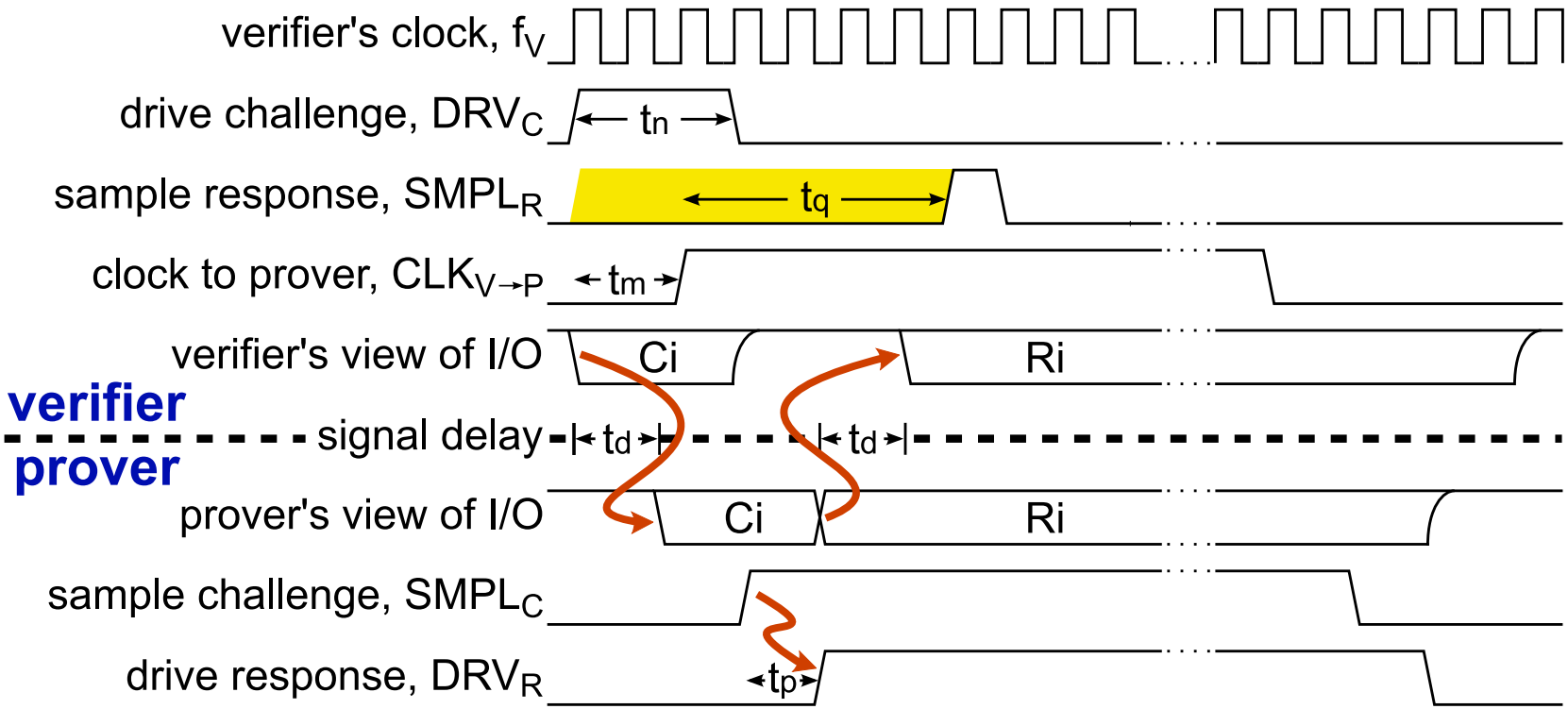




HK demonstration implementation (single-bit exchange)



HK demonstration implementation (control timing)



Commercialization and standardization

- 3db Access AG, ETH Zurich (Danev, Capkun, Basin, et al.)
- IEEE 802.15.4 standard(s) for low-rate wireless networks
  2003: ZigBee PHY (DSSS, 868/915 MHz BPSK or 2.45 GHz O-QPSK)
  2015: a collection of nearly 20 PHYs!
- IEEE 802.15.4z Enhanced Impulse Radio (EiR) task group
- IEEE P802.15 Wireless Speciality Networks
  CSD for 802.15.4z HRP and LRP UWB ranging enhancements
- Existing 802.15.4 (2015) UWB pulse candidate PHYs:
  - High Rate Pulse (HRP) – had already ranging function
  - Low Rate Pulse (LRP) – had already shortest symbols,
    3dB Access AG distance-bounding proposal is a modification of LRP
    (dual-frequency full-duplex mode, etc.)
- "Authenticated ranging of 802.15.4"
  "Secure authenticated ranging"

`https://mentor.ieee.org/802.15/documents`

Conclusions

Tamper-resistant positioning services

- may be required in a wide range of applications
- have to take into account attacks with specialized hardware
- cannot easily be added later at the application protocol layer
- must be designed into the physical protocol layer
- rely on more than just tamper-resistant hardware modules
- require transmission and reception mechanisms that differ substantially from standard ones:
  - rapid single-bit round-trip exchanges for distance bounding
  - delayed correlation of weak signals for satellite positioning
- are another example for application areas where security must be considered in the design from the very beginning

References (distance bounding)

- Stefan Brands, David Chaum: Distance bounding protocols. Eurocrypt 1993, LNCS 765.
- Gerhard P. Hancke, Markus G. Kuhn: An RFID distance bounding protocol. IEEE SecureComm 2005, Athens, 2005, ISBN 0-7695-2369-2.
- Gerhard P. Hancke: Practical attacks on proximity identification systems. IEEE Symposium on Security and Privacy, Oakland, 2005.
- Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, Tyler Moore: So near and yet so far: distance-bounding attacks in wireless networks. European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks, Hamburg, 2006, LNCS.
- Gerhard P. Hancke: A practical relay attack on ISO 14443 proximity cards, February 2005.
- Saar Drimer, Steven J. Murdoch: Keep your enemies close: Distance bounding against smartcard relay attacks. 16th USENIX Security Symposium, Boston, MA, August 2007.

`https://www.cl.cam.ac.uk/~mgk25/publications.html`
`https://www.cl.cam.ac.uk/research/security/`