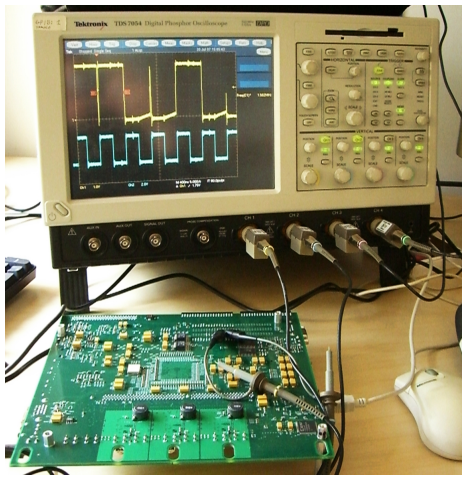
# Relay attacks on card payment: vulnerabilities and defences

Saar Drimer, Steven J. Murdoch
http://www.cl.cam.ac.uk/users/{sd410, sjm217}

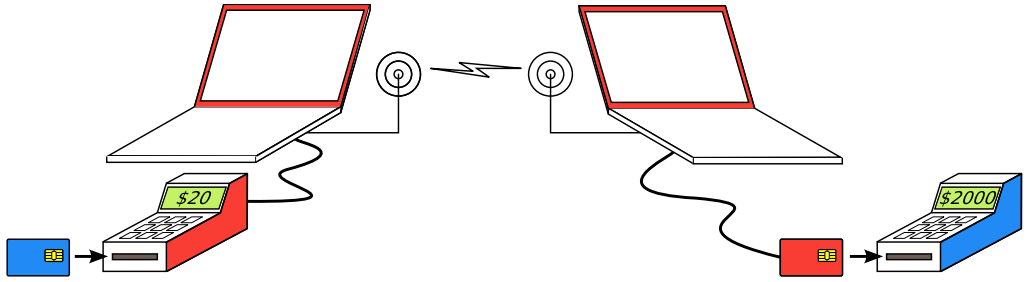



UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

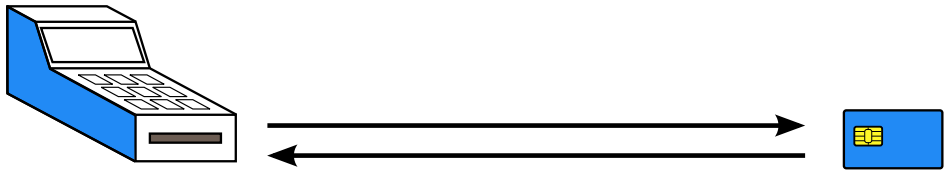
24C3, 29 December 2007, Berlin, Germany

# This talk describes our implementation of...




a relay attack on a live smartcard-based payment system in the UK; and

a low-cost distance bounding defence that limits the distance between participants to a few meters and below, without the need for a high frequency clock on the card.



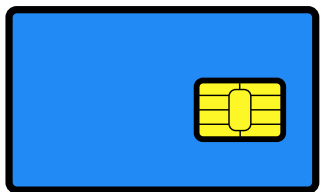
# *Chip & PIN* a is smartcard-based payment system that...


is fully deployed in the UK since 2006, with banks making grand claims of security;


uses the EMV (Europay MasterCard Visa) protocol with ISO 7816 mechanical/electrical/basic interface;

1066

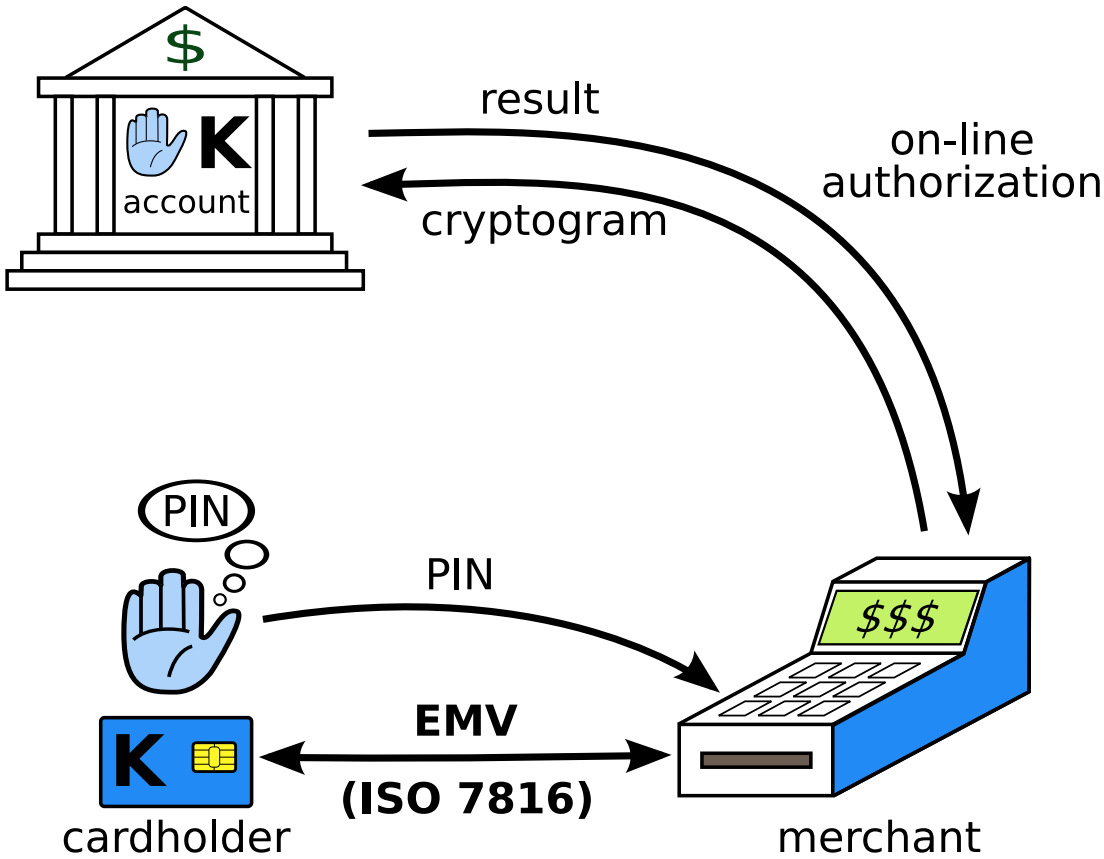
requires a correct 4 digit PIN input for authorizing transactions (both at ATMs and cash registers);



uses 3DES for Static Data Authentication (SDA); requires a symmetric key shared by bank and card;


has several security flaws identified by researchers early in deployment, one being the relay attack.

# A simplified smartcard transaction:



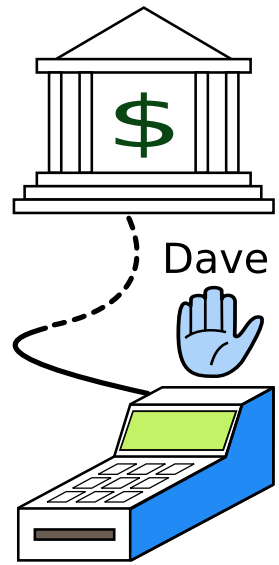

Since data is “static”, authorization must be done on-line to prevent replay attacks; however, off-line authorizations are still possible under some conditions

# Our attack was shown on BBC1's consumer-watch program, which aired February 2007

*"We got our highest ratings of the run for the story (6.2 million, making it the most watched factual programme of last week)... it's provoked quite a response from viewers."* – Rob Unsworth, Editor, "Watchdog"

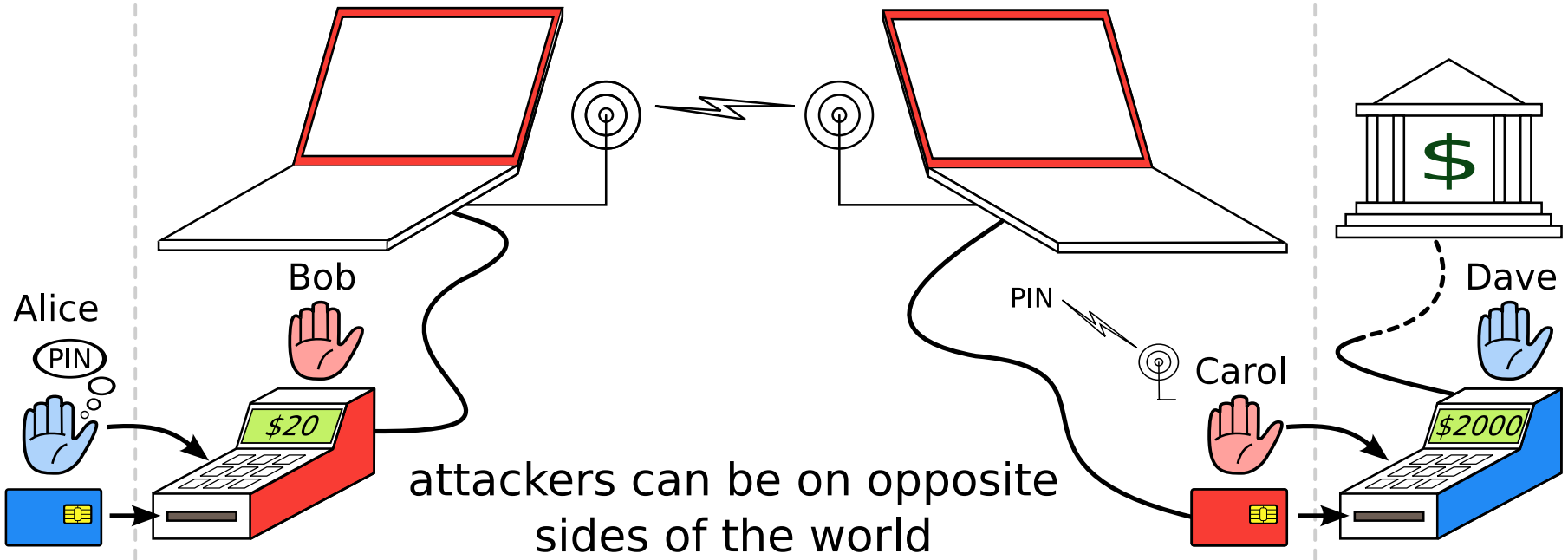
**Our demonstration helped many cardholders reach a favourable resolution with banks**

# The relay attack: Alice thinks she is paying $20, but is actually charged $2 000 for a purchase elsewhere

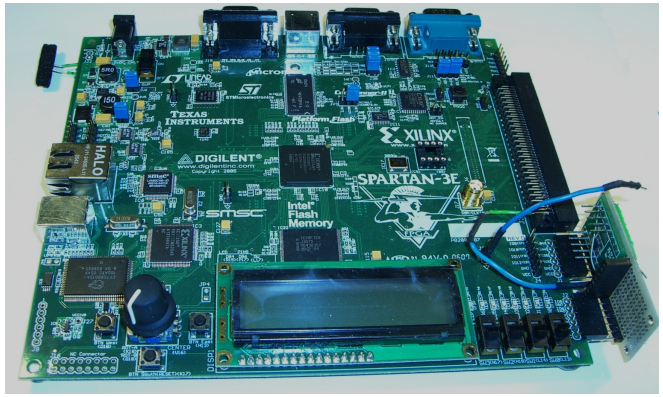

Honest cardholder Alice and merchant Dave are unwitting participants in the relay attack

# The relay attack: Alice thinks she is paying $20, but is actually charged $2 000 for a purchase elsewhere




Alice inserts her card into Bob's *fake* terminal, while Carol inserts a fake card into Dave's *real* terminal. Using wireless communication the $2 000 purchase is debited from Alice's account

# The relay “kit”:





$500 worth of off-the-shelf hardware, two laptops and moderate engineering skill is all it takes.

# Previously proposed defences may not be effective for defending against relay attacks

## Tamper evident/resistant terminals?

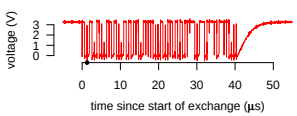
Protects banks by erasing keys upon tampering; cardholders aren't trained to tell the difference.

## Physical examination of smartcard?

Fake RFID card is an incremental engineering challenge


## Compare card number on receipt?

Embossing machines are available; target repeat customers




## Impose timing constraints on terminal-card interaction?

A good start, but short timing advantages translate into long distances; most interactions are predictable

# Existing timing tolerances are too wide to be effective

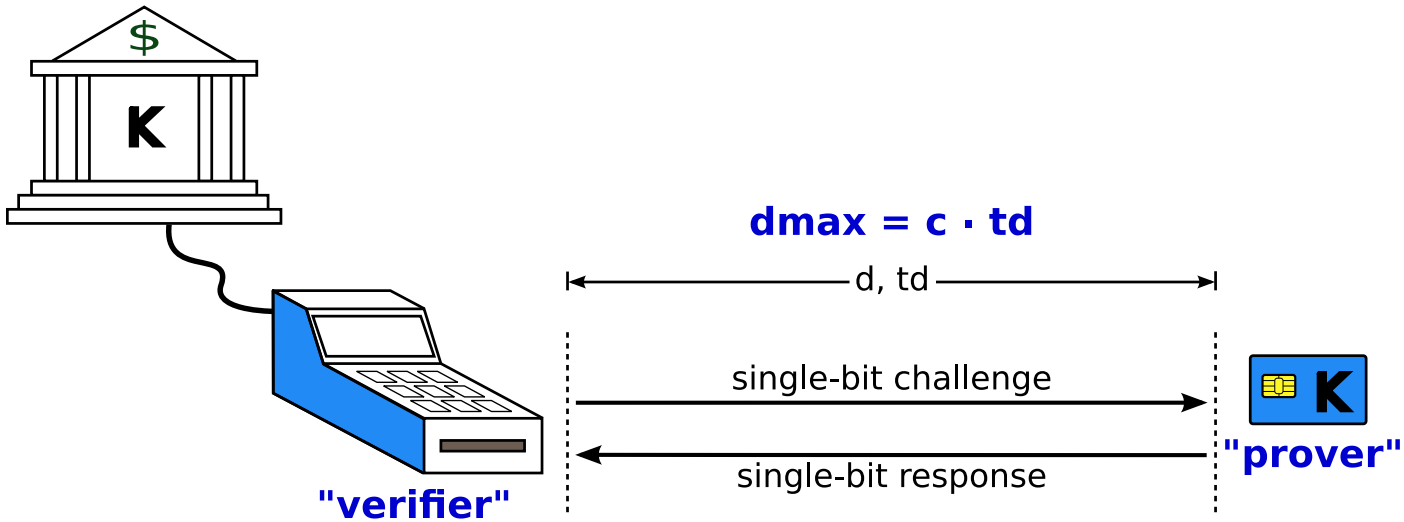
One device we tested allowed a 3 second round trip delay, which at the speed of light allows the real card to be 899 377 km away, i.e.:

- 11 times around the earth
- To the moon and back
- Not quite as far as Mars (their credit cards are safe)

Even reducing the constraints to the minimum is not sufficient, since by only speeding up the card slightly, a large time advantage can eventually be built up

The key to accurate distance bounding is to send short, 1-bit, messages

# The basic distance bounding protocol is a rapid bit-exchange



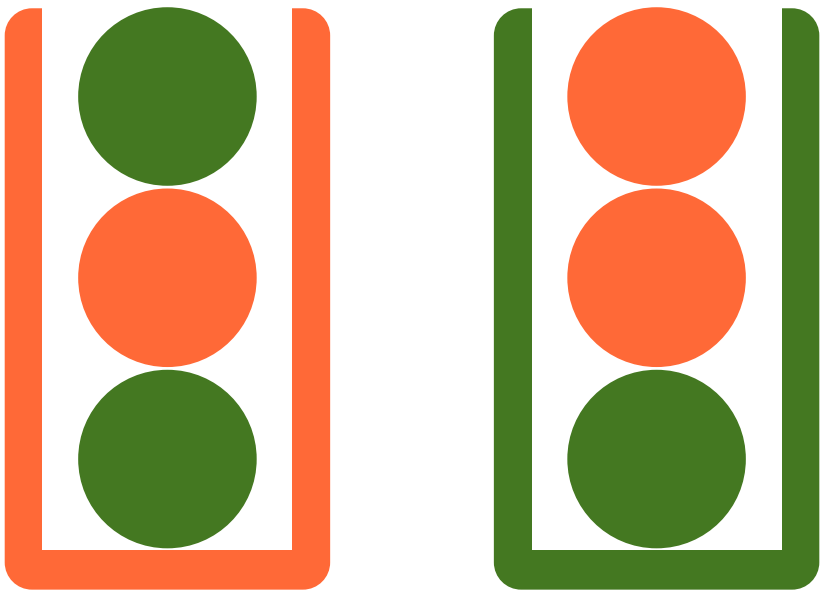

Distance bounding gives the terminal (verifier) assurance that the card (prover) is within a maximal distance by repeating multiple single-bit challenge-response exchanges and assuming signals travel at the speed of light.

# Demonstration of the basic protocol...

Both legitimate participants know the bit-sequences

The goal is to prove that the distance between them is within a maximum bound

An attacker should not be able to make it seem as if the two legitimate participants are closer

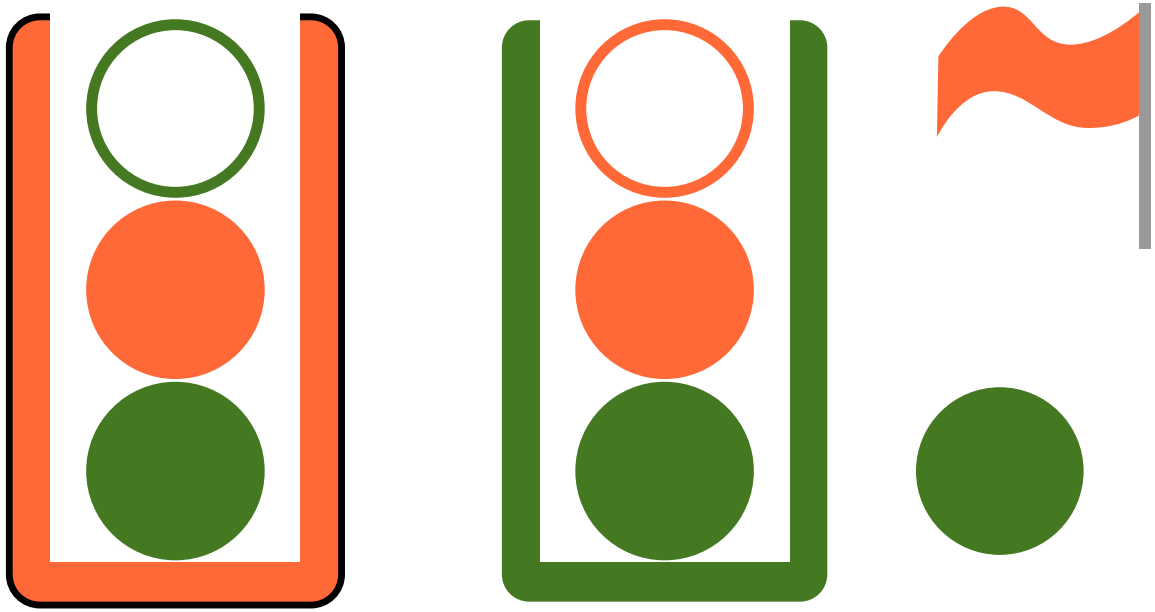


# Demonstration of the basic protocol...

Both legitimate participants know the bit-sequences

The goal is to prove that the distance between them is within a maximum bound

An attacker should not be able to make it seem as if the two legitimate participants are closer

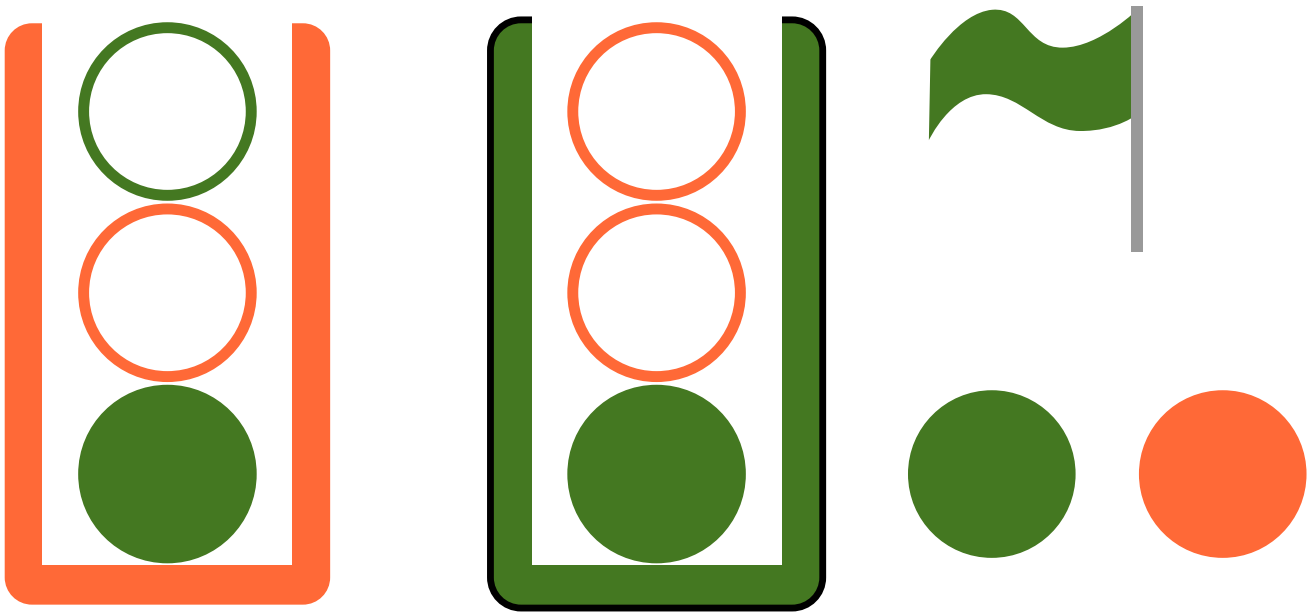


# Demonstration of the basic protocol...

Both legitimate participants know the bit-sequences

The goal is to prove that the distance between them is within a maximum bound

An attacker should not be able to make it seem as if the two legitimate participants are closer

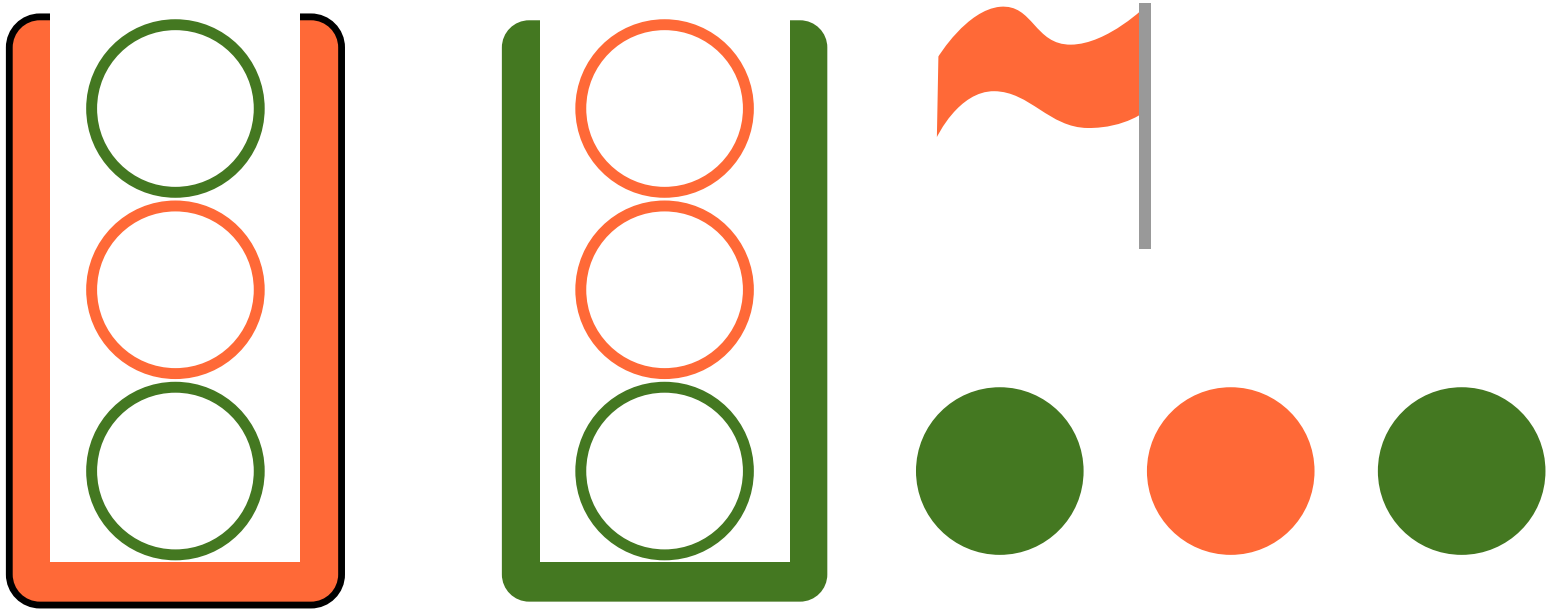


# Demonstration of the basic protocol...

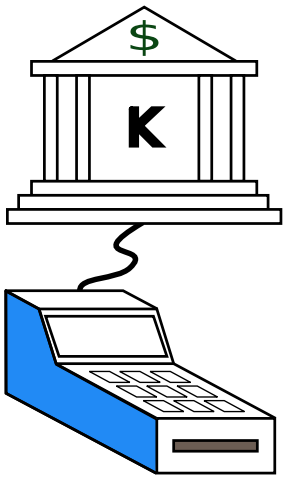
Both legitimate participants know the bit-sequences

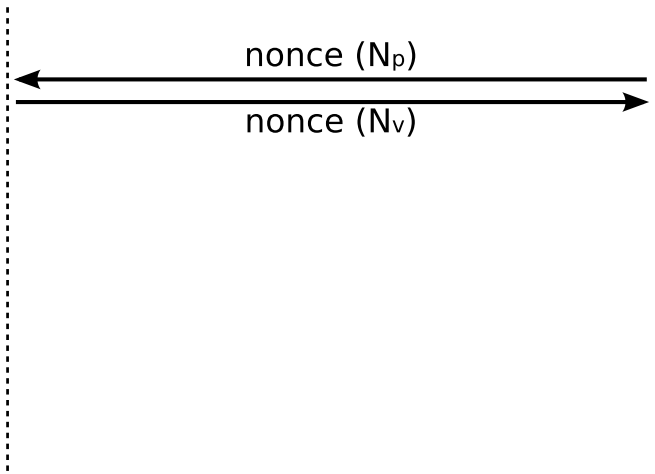
The goal is to prove that the distance between them is within a maximum bound

An attacker should not be able to make it seem as if the two legitimate participants are closer



# The distance bounding protocol in detail...



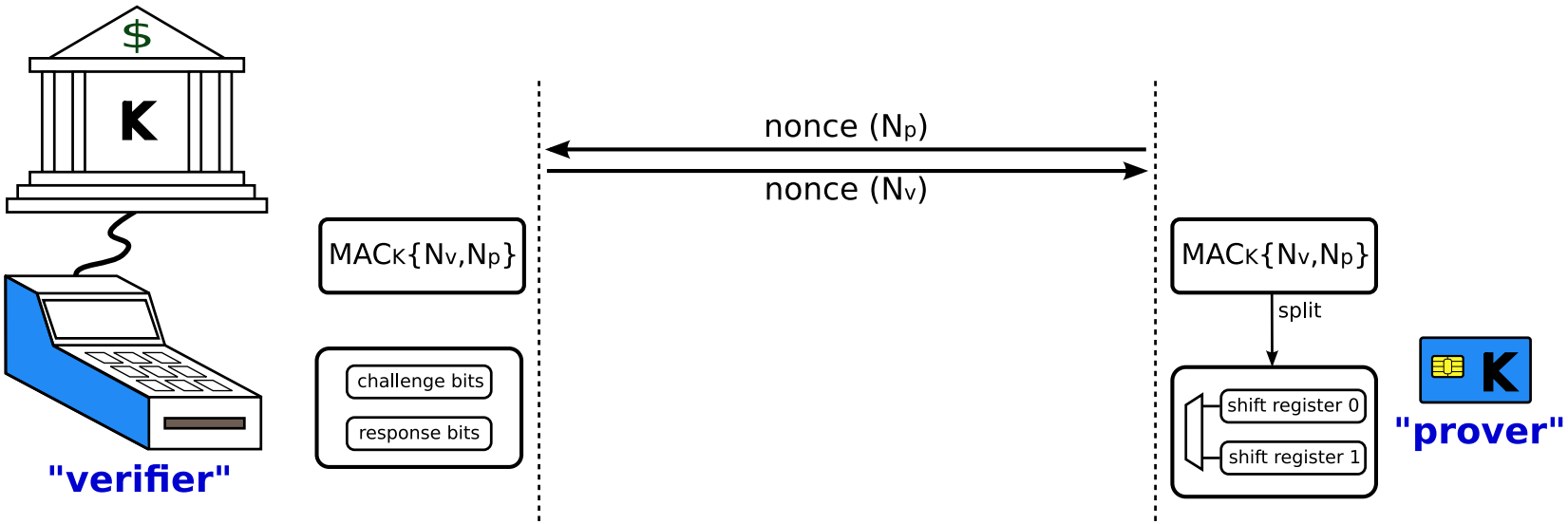





We use the Hancke-Kuhn protocol, which we adapted to a wired, half-duplex implementation considering EMV constraints: a two wire interface and cheap prover

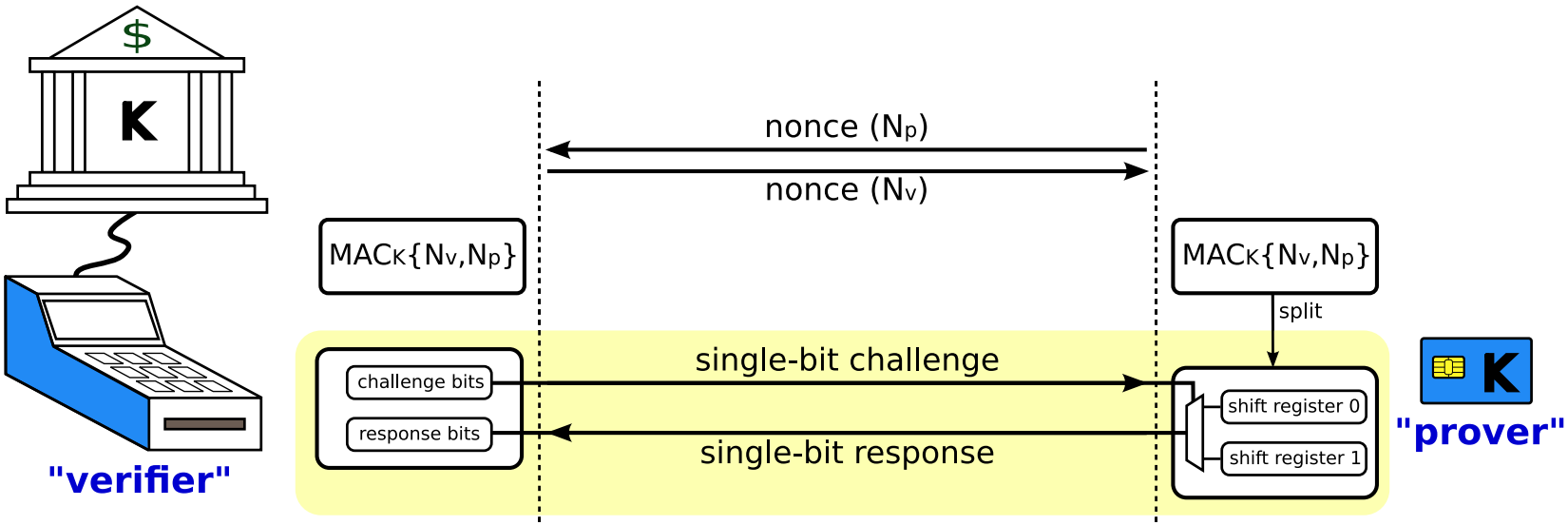
– the protocol starts with a mutual exchange of nonces.

# The distance bounding protocol in detail...



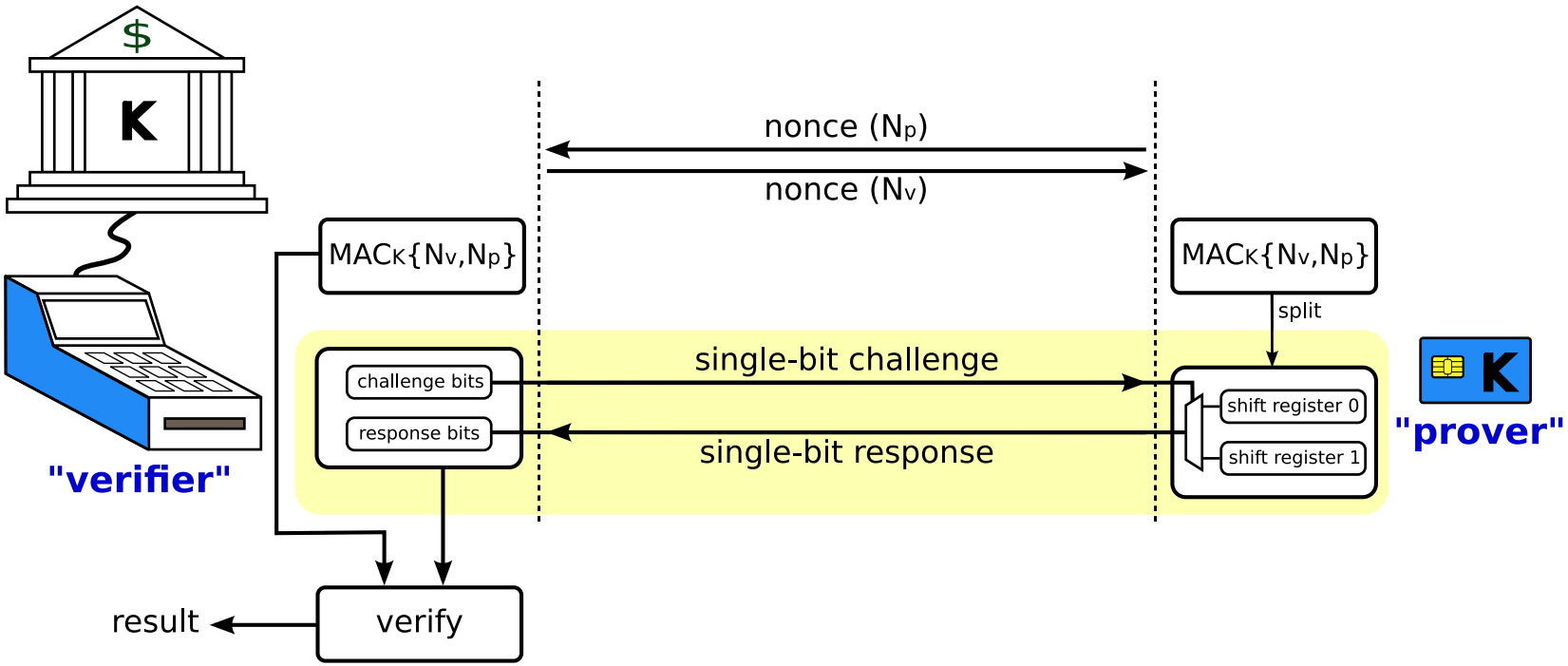

– MACs are computed under shared key;
– verifier loads a shift register with random bits;
– prover splits MAC into two shift registers.

# The distance bounding protocol in detail...




Timing critical phase:
– single bit challenge-response pairs are exchanged;
– response bit is the next bit from the shift register corresponding to the challenge bit's content;
– response bit is deleted at prover and stored at verifier.

# The distance bounding protocol in detail...




The verifier checks that the responses are correct and concludes, based on its timing settings, the maximum distance the prover is away

# An attacker can try to get an advantage by...

Guessing $\frac{1}{2}$ of challenges and $\frac{1}{2}$ of responses;
With 64-bit, success probability $(\frac{3}{4})^{64} \approx 1$ in $2^{26}$;
however, only a single attempt is possible per nonce pair;

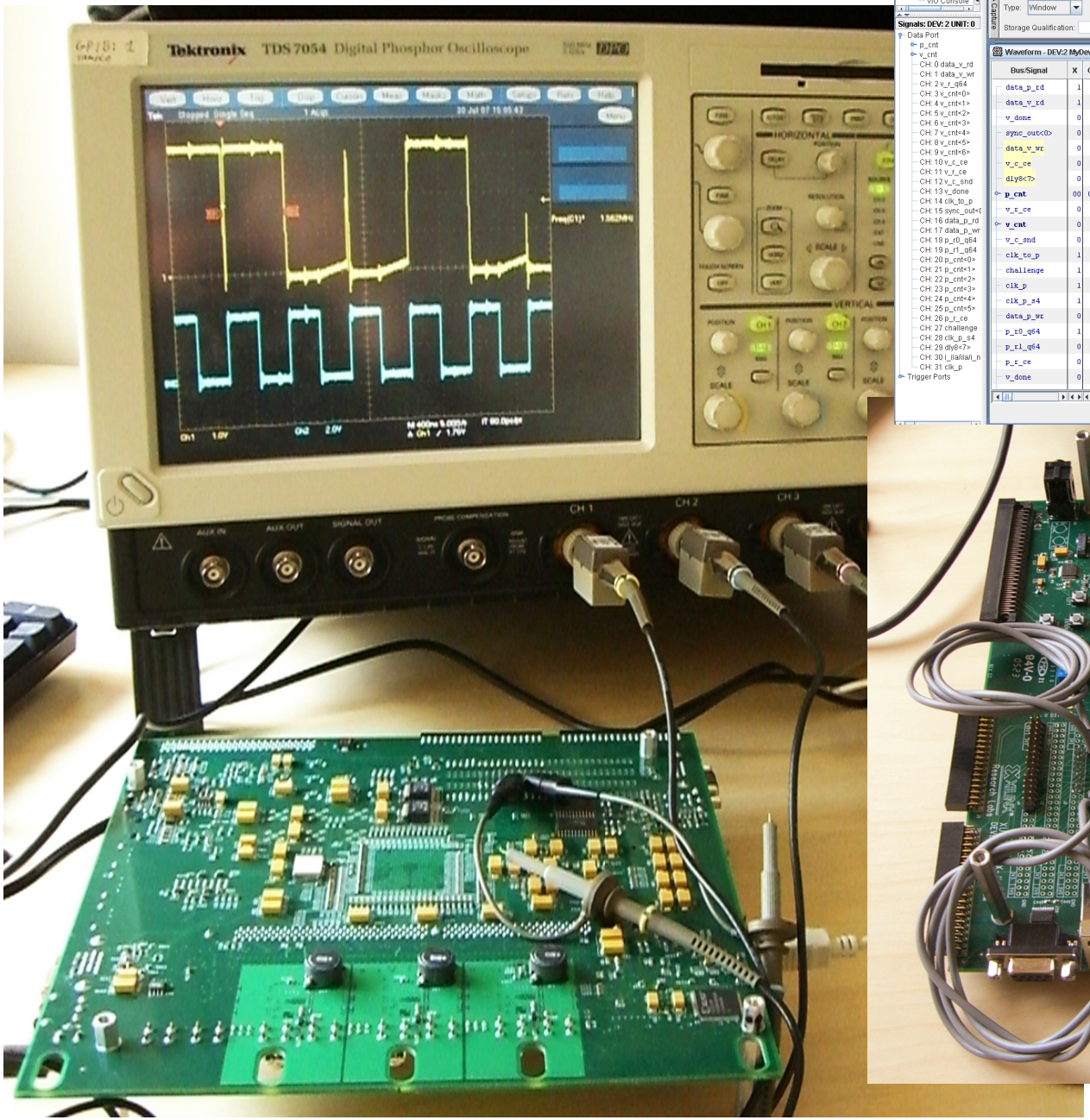
Revealing both response registers by running the protocol twice:
Prevented by the prover providing a nonce of its own.

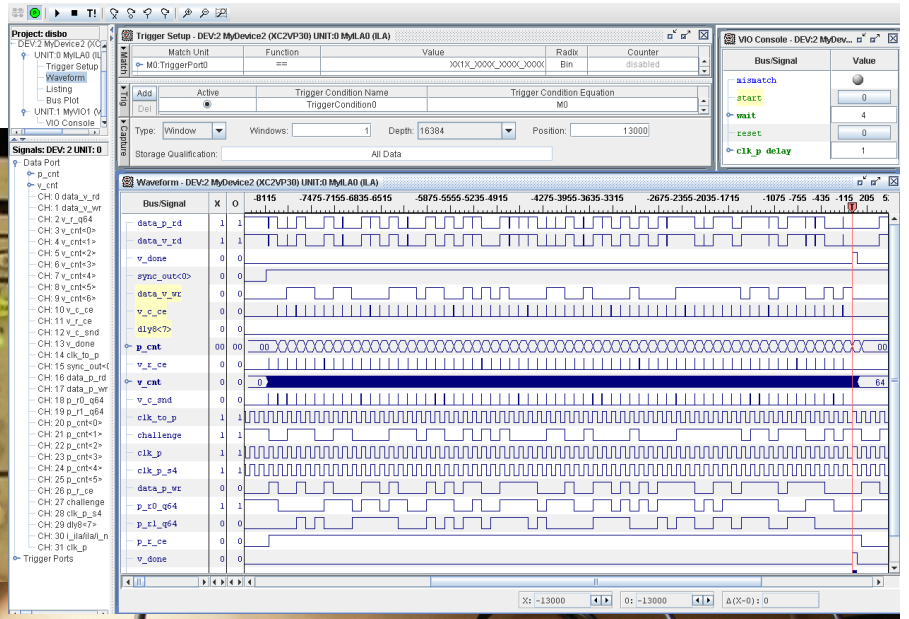
Sampling signals immediately, manipulate clock, transmit "fast":
Critical time is still very short, requiring a very capable attacker.

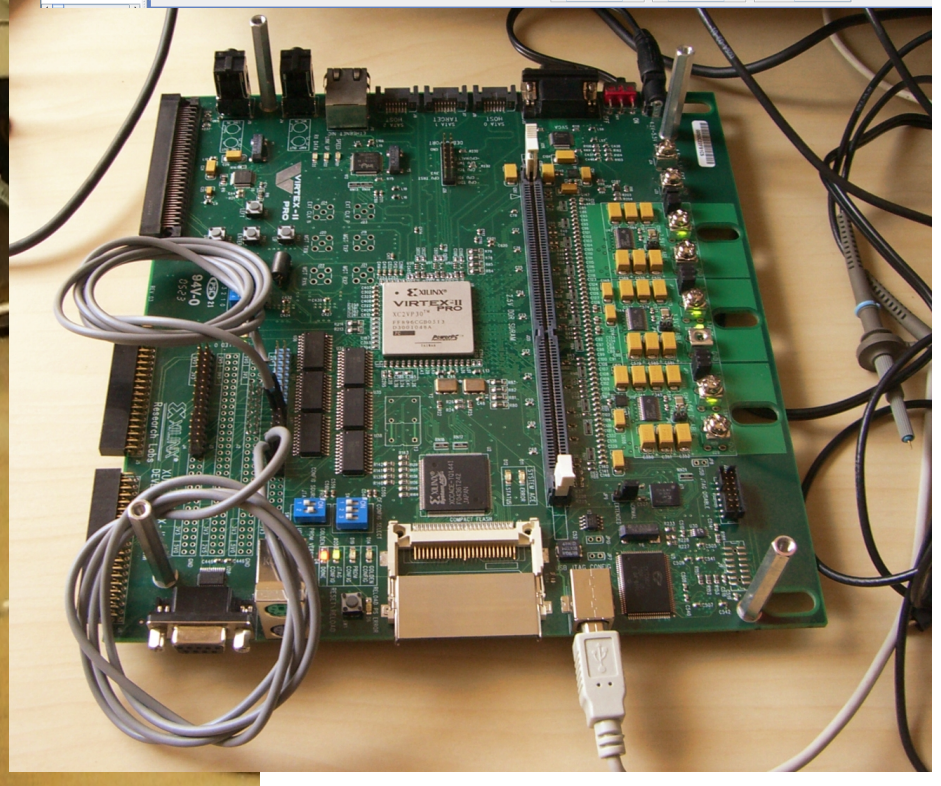
Fool prover into exposing both registers' state:
Careful hardware design can prevent this.

**System should be designed for a particular distance**

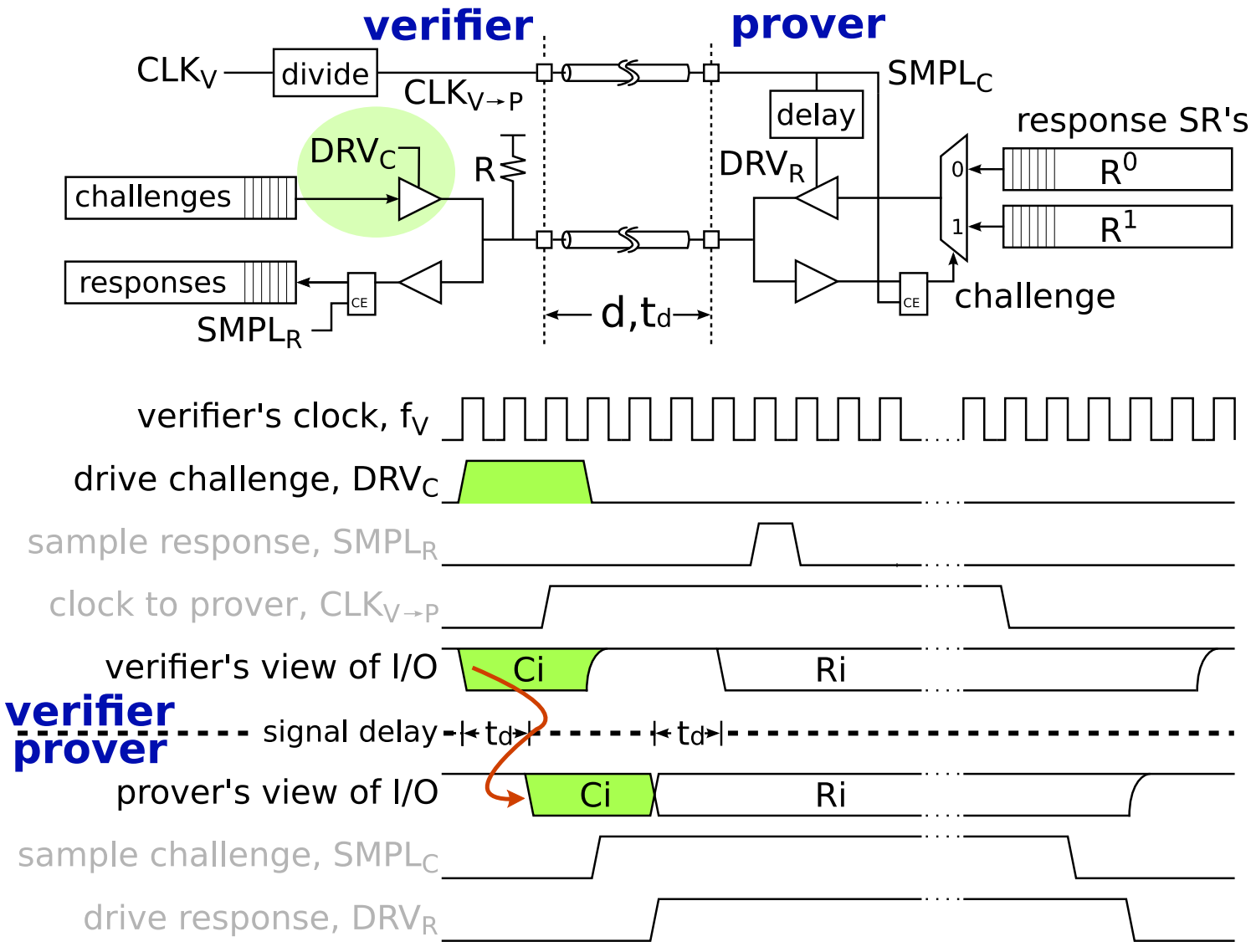
# Experimental setup:



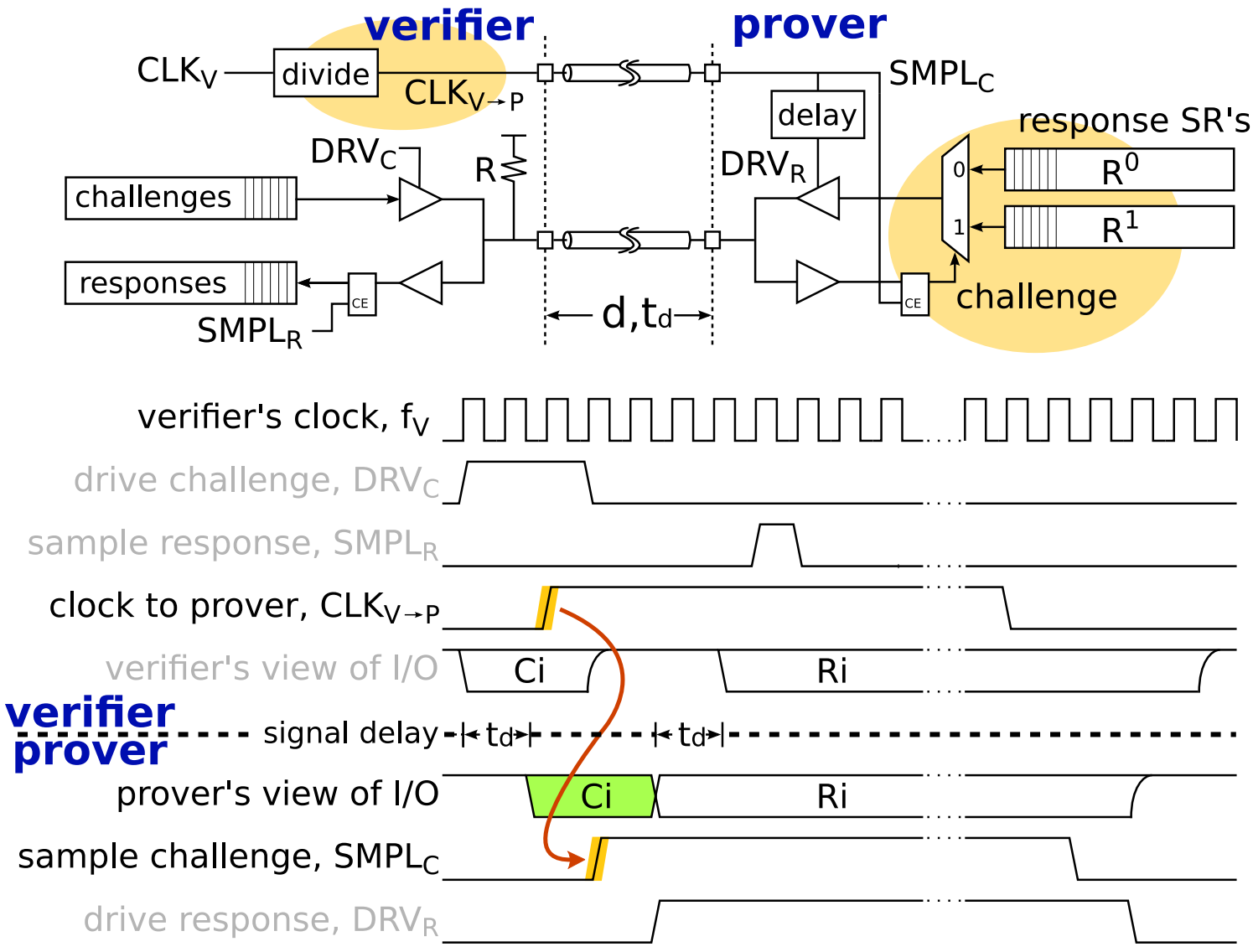



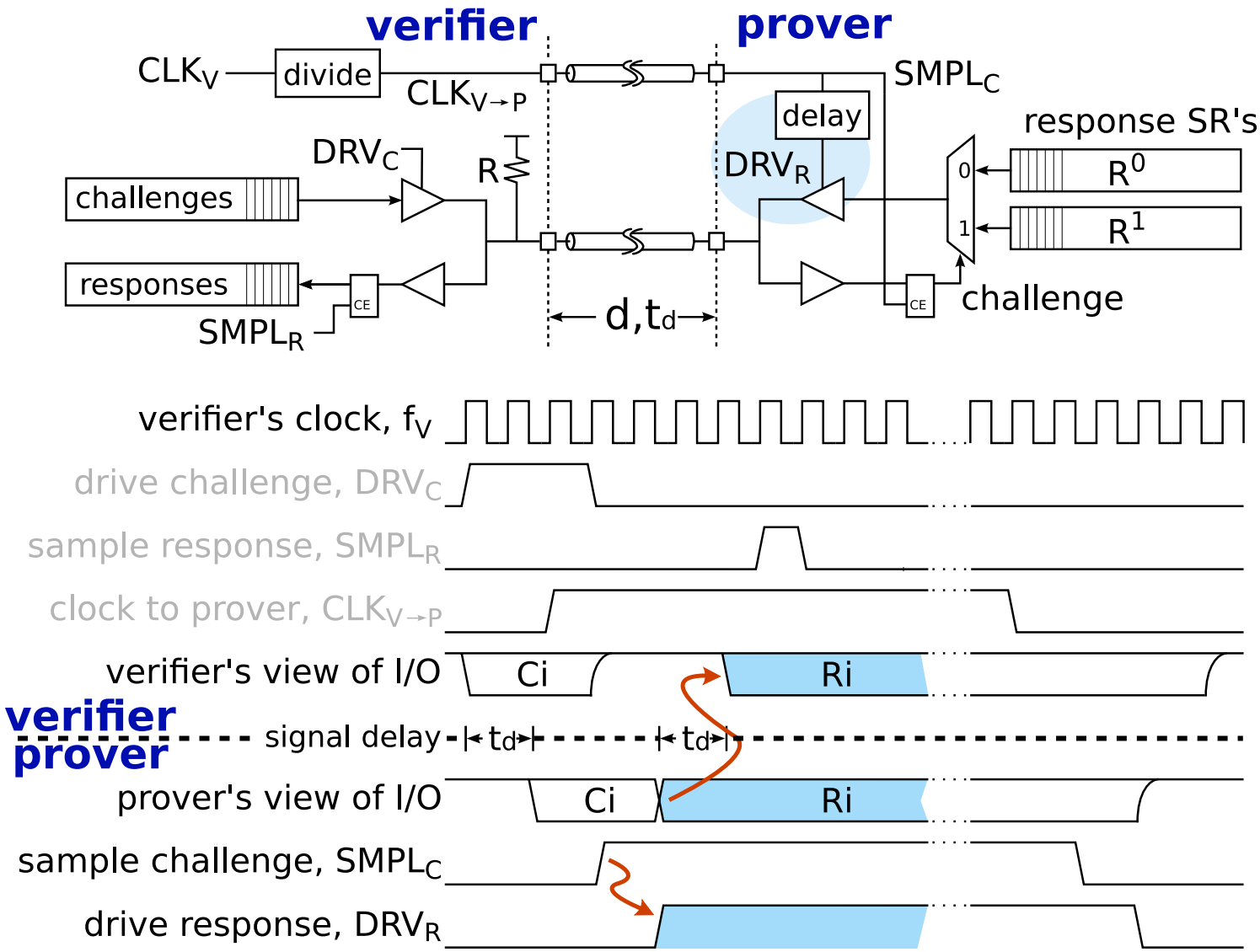
# FPGA implementation is robust against capable attackers



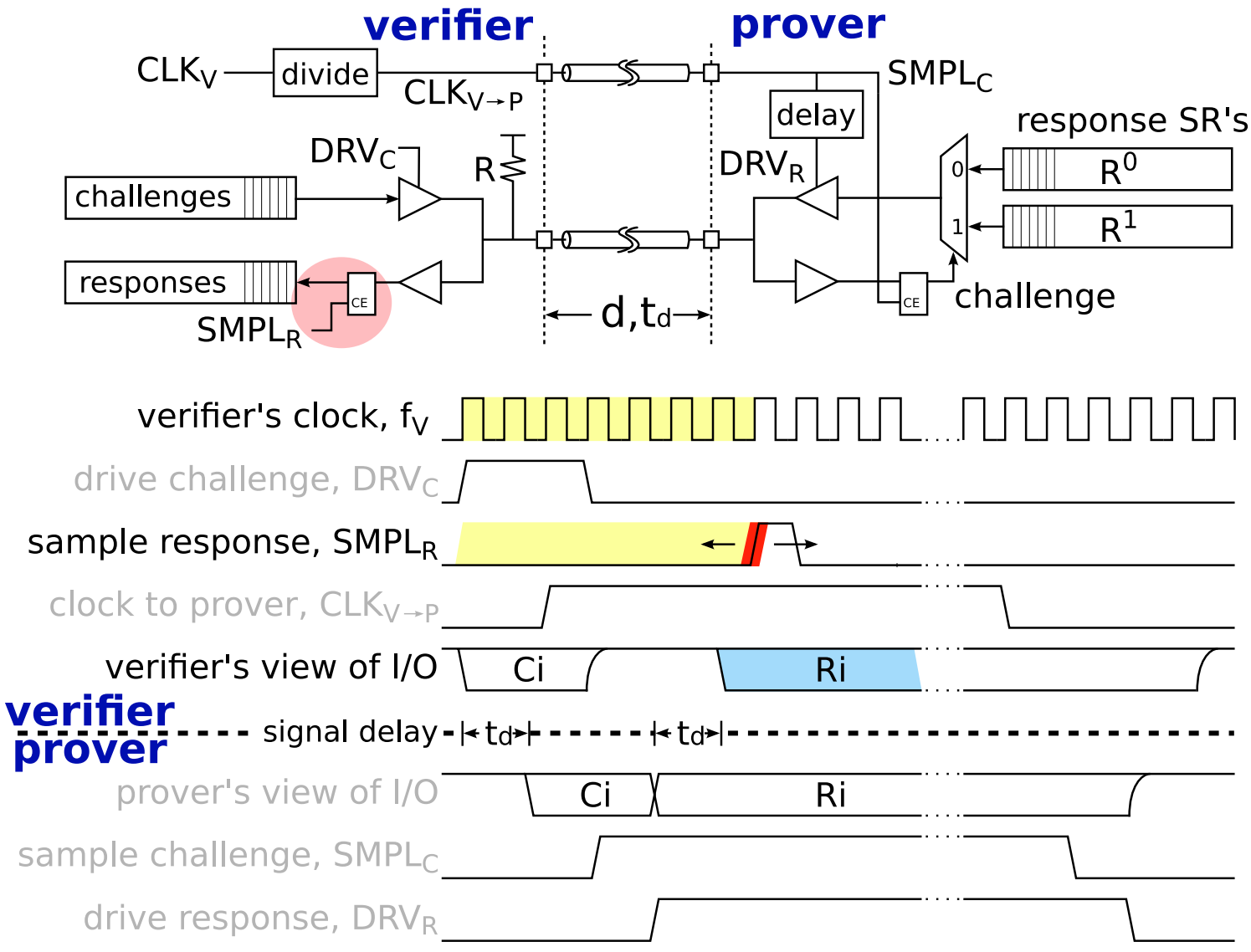
# FPGA implementation is robust against capable attackers



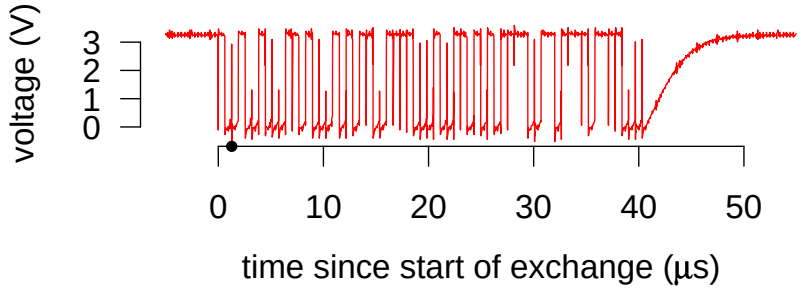
# FPGA implementation is robust against capable attackers

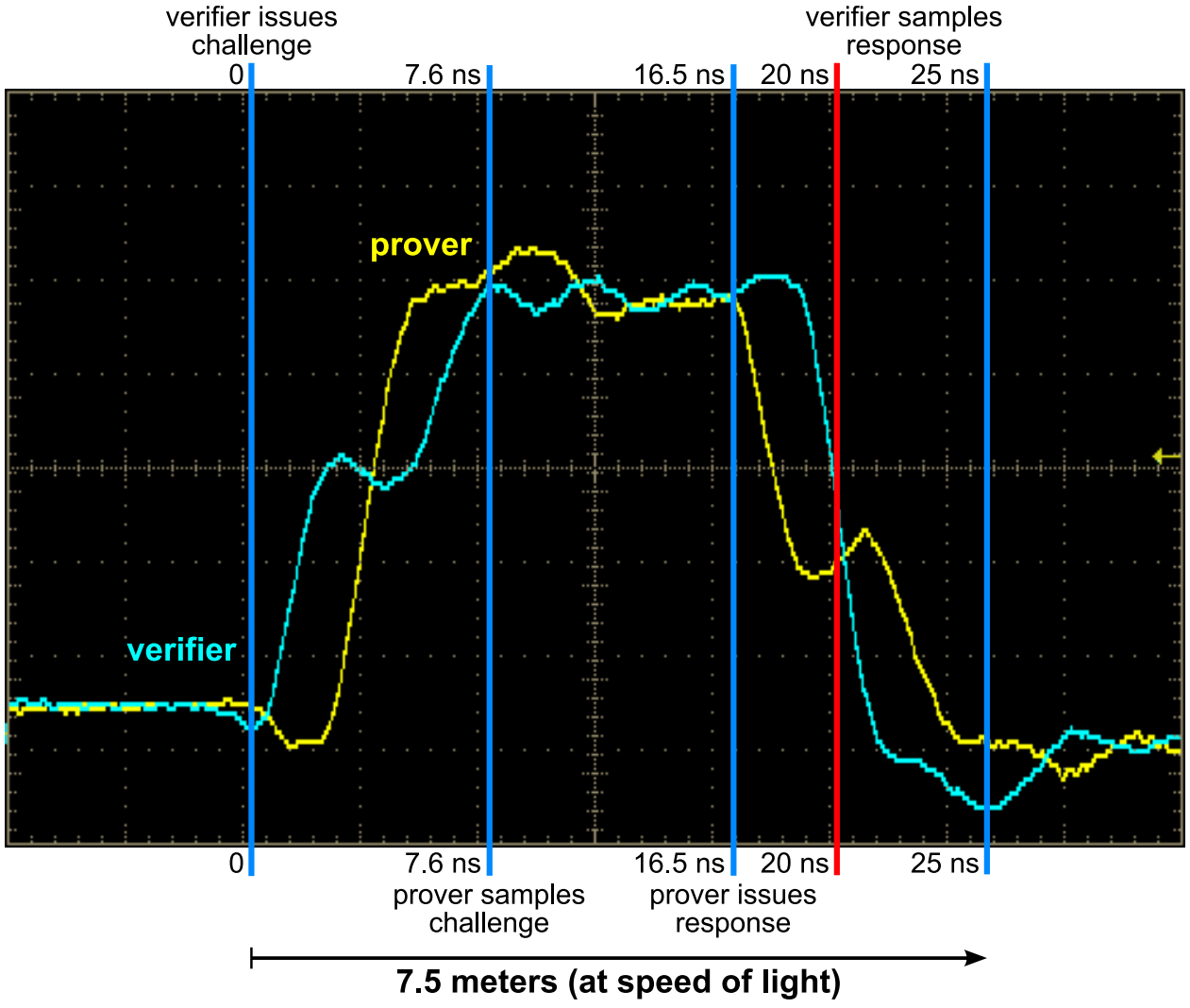


# FPGA implementation is robust against capable attackers



# A single bit-pair exchange: challenge=1, response=0

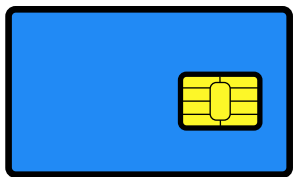


# Our solution is low-cost and robust


Distance bounding support needs to be added to EMV specs;

Terminals need to operate at higher frequencies, plus shift registers and control circuitry;



cards added with shift registers and control; re-issued with public-key (CDA/DDA);

card-terminal interface is unchanged; customer-merchant experience unchanged.

As banks adopt more secure methods of authentication, distance bounding should be added to thwart relay attacks

# Current attacks on Chip and PIN are much less sophisticated

Your name, account number and all information needed to make a fake card are stored on the card's magnetic stripe

This includes the "CVV", which banks use to confirm that the card is legitimate (not to be confused with the CVV2 printed on the back)

A fraudster can use a magnetic stripe reader to perform a "double-swipe"

The fraudster can watch/film the customer entering their PIN


Tonight (ITV, 2007-05-04)

# Card details and PIN can be intercepted “on the wire”

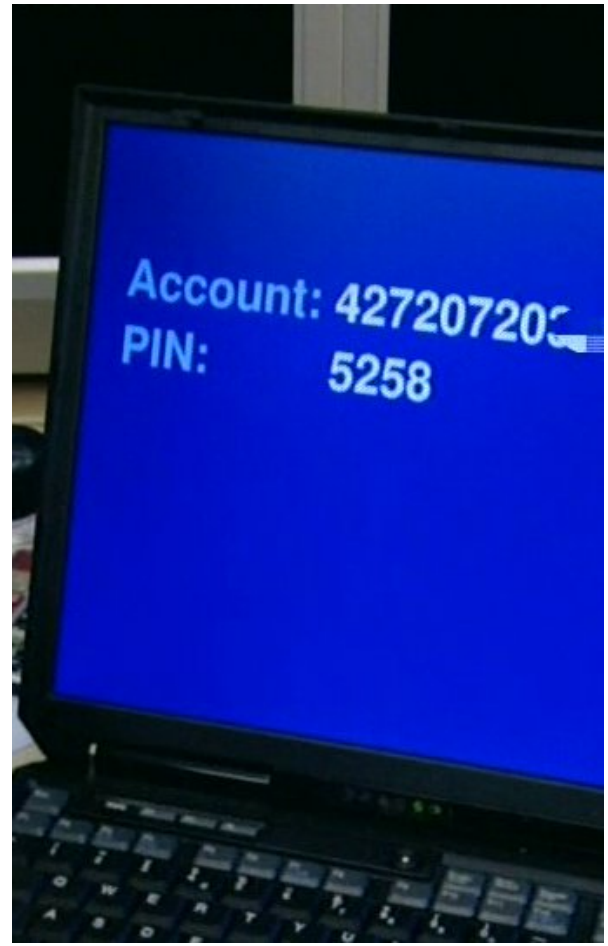
In some cases, the magnetic stripe details are also sent along wires and can be intercepted there

Another place to intercept communications is between the chip and the terminal

The account number is sent from the chip to the terminal

The PIN entered is sent from the terminal to the chip for verification

So all the information needed by fraudsters can be collected from a single point




Plusminus (ARD, 2006-03-07)

# Once the details have been collected, a fake card can be created

Even though UK cards have chips, ATMs will accept clones which appear to have a broken chip

Alternatively, fraudsters can use the card abroad where ATMs do not have chip readers

There, the cloned cards can be sold, protecting the people who collected the details originally

Any magnetic stripe card will suffice, even a mobile phone top-up card


ITV News (2006-06-12)

# If the bank doesn't believe you're a victim, it can be very difficult to get your money back

> The Firm has provided an 'audit trail' of the transactions disputed by you. This shows the location and times of the transactions and evidences that the card used was 'CHIP' read.

Financial Ombudsman Service

# If the bank doesn't believe you're a victim, it can be very difficult to get your money back

> Although you question the Firm's security systems, I consider that the audit trail provided is in a format utilised by several major banks and therefore can be relied upon.

Financial Ombudsman Service

# If the bank doesn't believe you're a victim, it can be very difficult to get your money back

> Although you have requested this information from the Firm yourself (and I consider that it is not obliged to provide it to you) I conclude that this will not make any difference, because this Service has already reviewed this information.

Financial Ombudsman Service

# If the bank doesn't believe you're a victim, it can be very difficult to get your money back

> As we have already advised you, since the advent of CHIP and PIN, this Service is not aware of any incidents where a card with a 'CHIP' has been successfully cloned by fraudsters so that it could be used by them successfully in a cash machine.

Financial Ombudsman Service

# If the bank doesn't believe you're a victim, it can be very difficult to get your money back

> My conclusion therefore is that it is likely that the original card was used to carry out the transactions disputed by you.

Financial Ombudsman Service

# In summary, the banking card payment system suffers from a number of significant vulnerabilities

The more simple problems, currently being exploited, can be fixed by disabling backwards compatibility features

Other problems will require banks to adopt more secure, but slightly more expensive, types of cards

Even if these steps are taken, relay attacks are still a risk; defending against these requires new hardware

The root cause of these difficulties is that banks are able to pass the costs of fraud onto the victims

A change in culture is needed to ensure liability for losses lies with the banks, who are in a position to improve security

Paper, videos, and further discussion:
`http://www.cl.cam.ac.uk/research/security/banking/`
`http://www.lightbluetouchpaper.org/`

end.