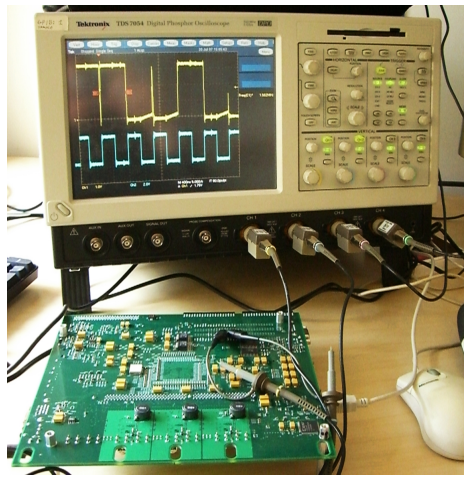
Keep your enemies close

Distance bounding against smartcard relay attacks

Saar Drimer, Steven J. Murdoch

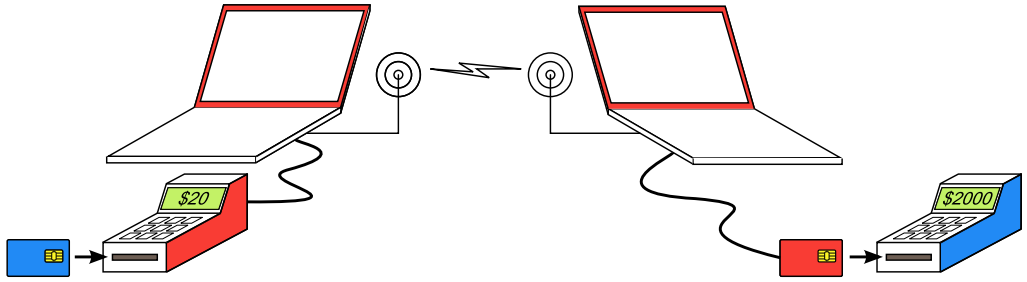
www.cl.cam.ac.uk/~{sd410,sjm217}



UNIVERSITY OF CAMBRIDGE
Computer Laboratory

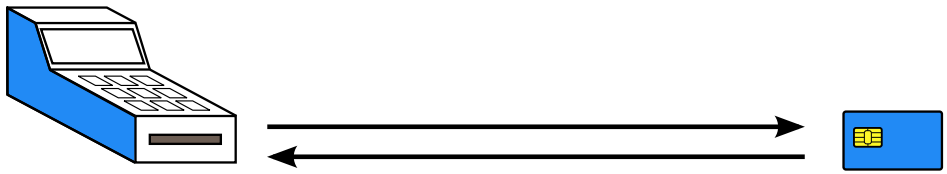
USENIX Security, 8 August 2007, Boston, US

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 defense that limits the distance between participants to a few meters and below, without the need for a high frequency clock on the card.



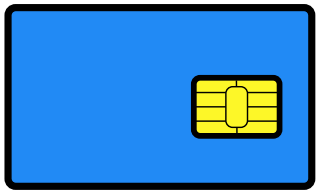
Chip & PIN a is smartcard-based payment system that...

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

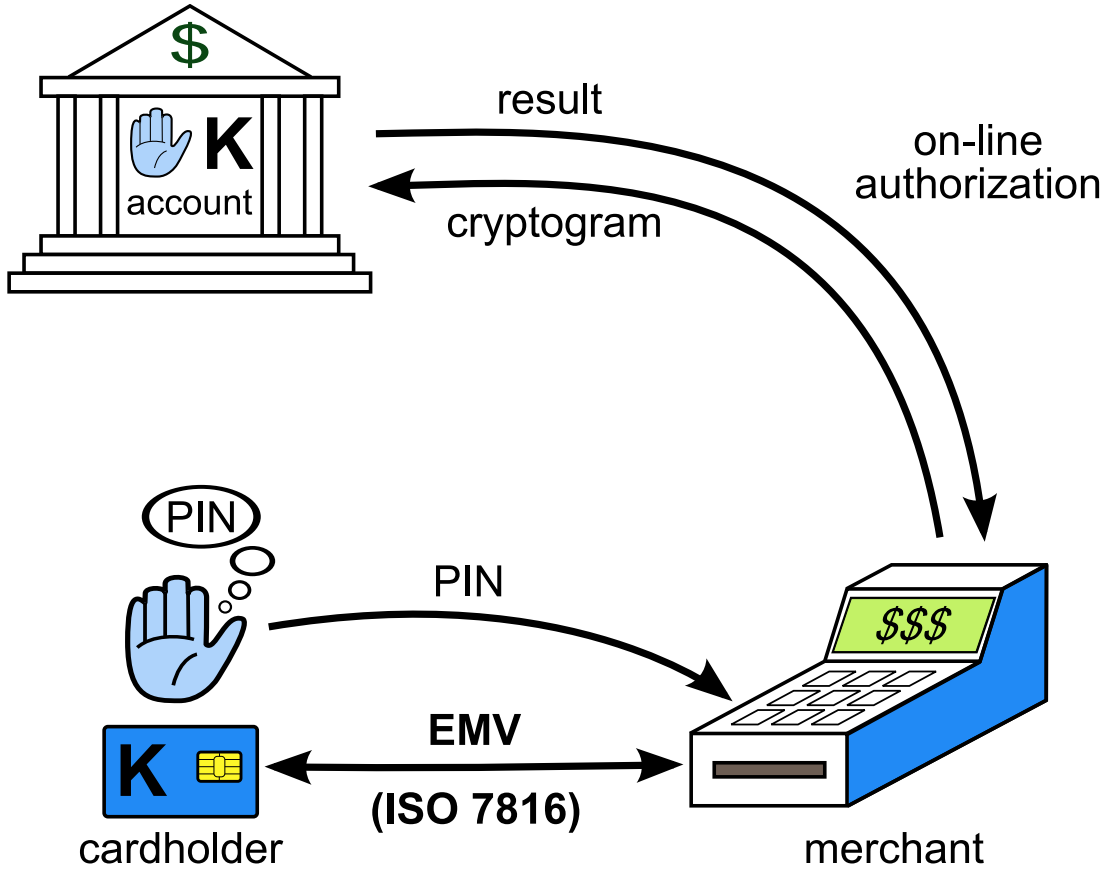
requires a correct 4 digit PIN input for authorizing transactions (both at ATMs and cash registers);



uses RSA 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:



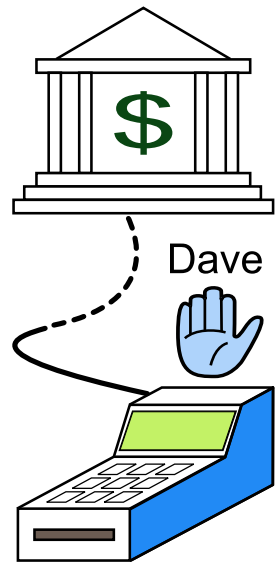
Since data is “static”, authorization must be done on-line to prevent replay attacks; however, off-line authorizations are still possible under some conditions

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"

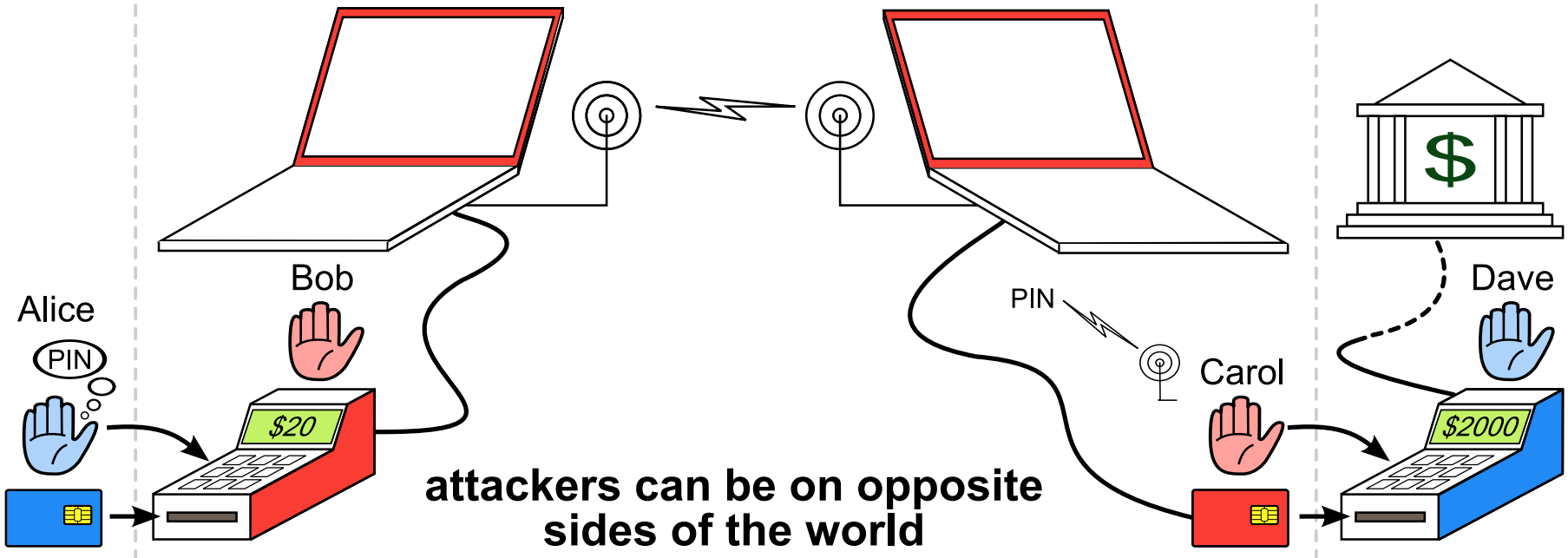
Our demonstration helped many cardholders reach a favorable resolution with banks

The relay attack:



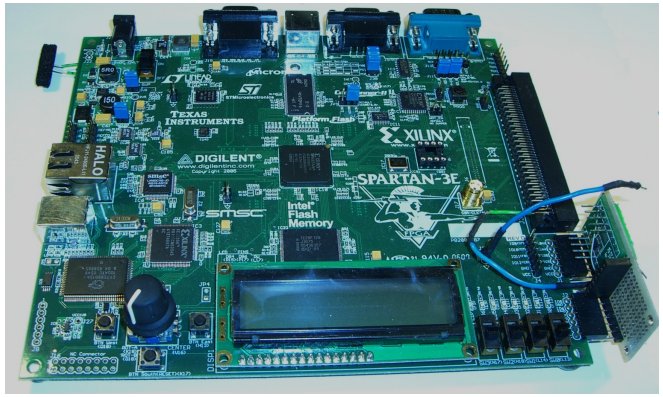
Honest cardholder Alice and merchant Dave are unwitting participants in the relay attack

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”:

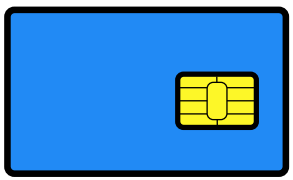


$500 worth of off-the-shelf hardware, two laptops and moderate engineering skill is all it takes.

Despite its low cost, fraudsters are unlikely to be using the relay attack today; other attacks are cheaper and easier:

off-line transactions, and use of "yes-cards"; works because data is static, and fake card can be programmed to accept any PIN;

magnetic-stripe fallback;



mag-stripe data is available on the chip for backwards compatibility; PIN can be observed and fake mag-stripe card used at a foreign ATM.

However, fraudsters will resort to more sophisticated attacks as security holes are gradually "patched"

Previously proposed defenses may not be effective for defending against relay attacks

Tamper evident/resistant terminals?

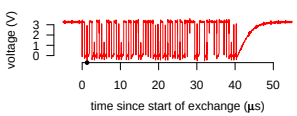
Protects banks by erasing keys upon tampering; cardholders aren't trained to tell the difference.

Physical examination of smartcard?

Fake RFID card is an incremental engineering challenge

Compare card number on receipt?

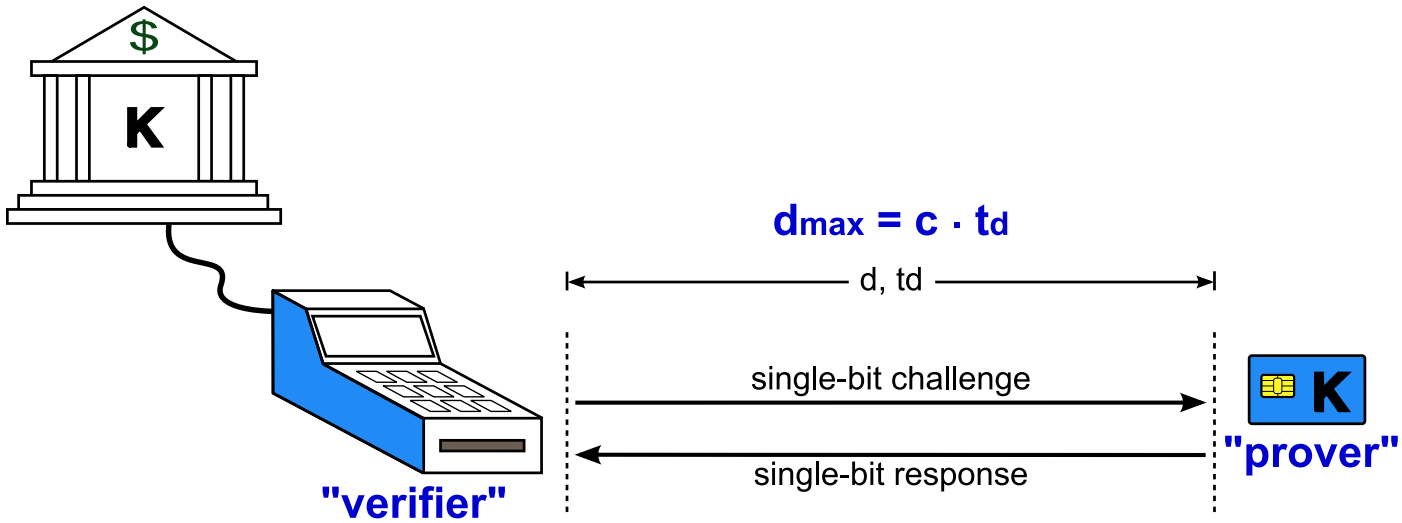
Embossing machines are available; target repeat customers



Impose timing constraints on terminal-card interaction?

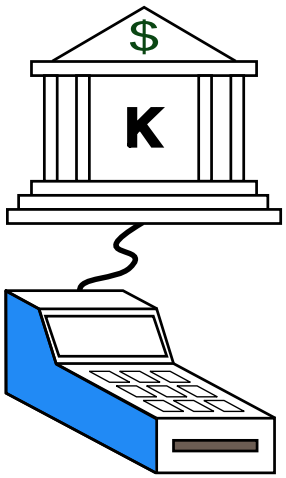
A good start, but short timing advantages translate into long distances; most interactions are predictable

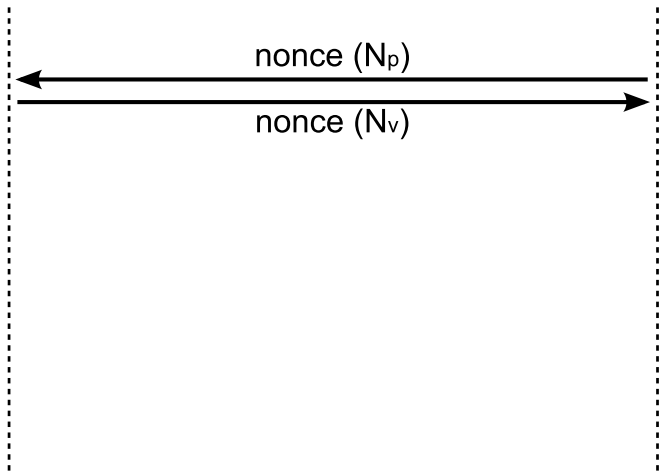
We suggest using “distance bounding”



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.

We suggest using “distance bounding”

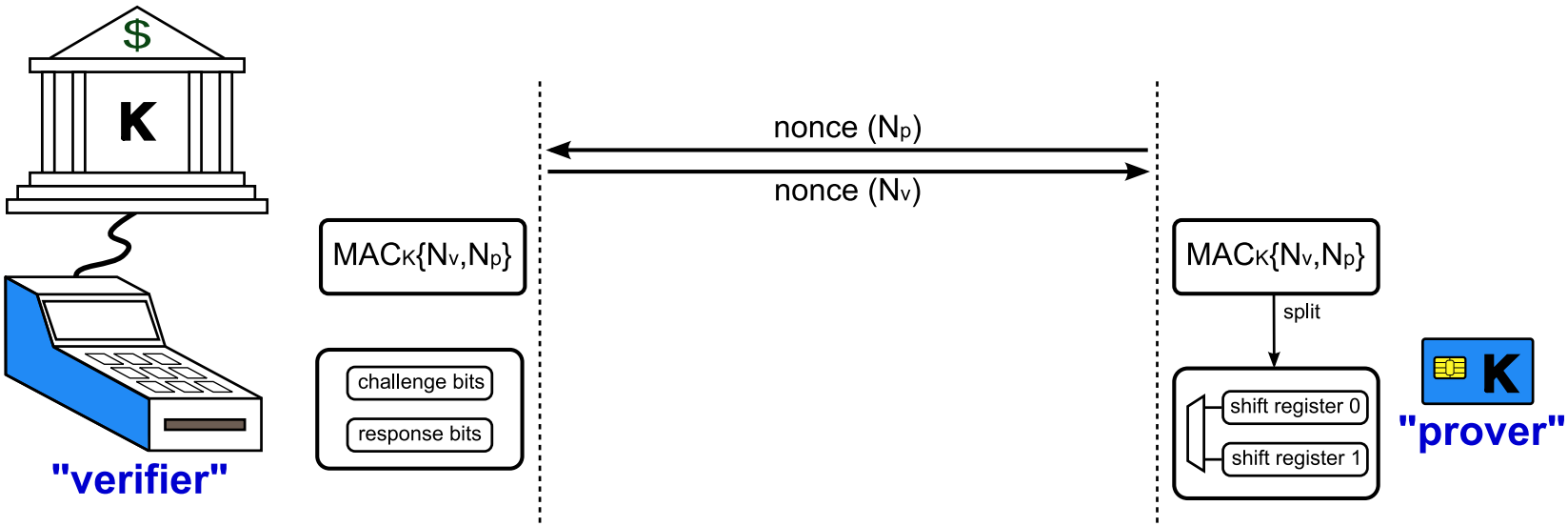




We use the Hancke-Kuhn protocol, which we adapted to a wired, half-duplex implementation considering EMV constraints: a two wire interface and cheap prover

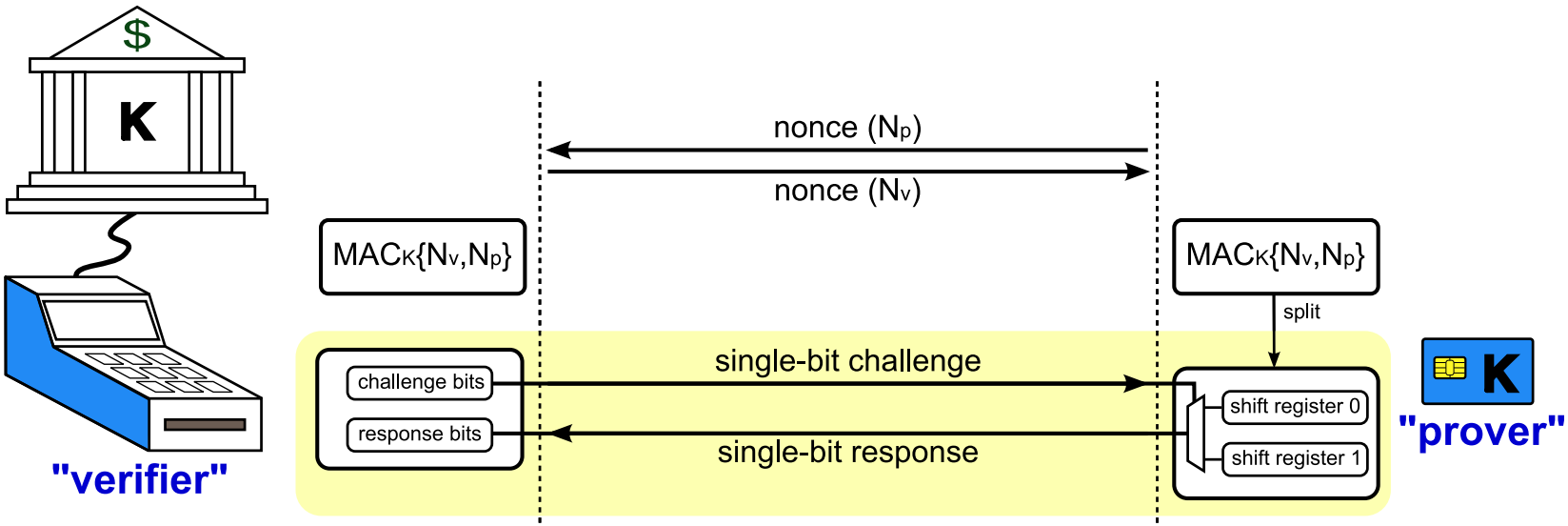
– the protocol starts with a mutual exchange of nonces.

We suggest using "distance bounding"



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

We suggest using "distance bounding"



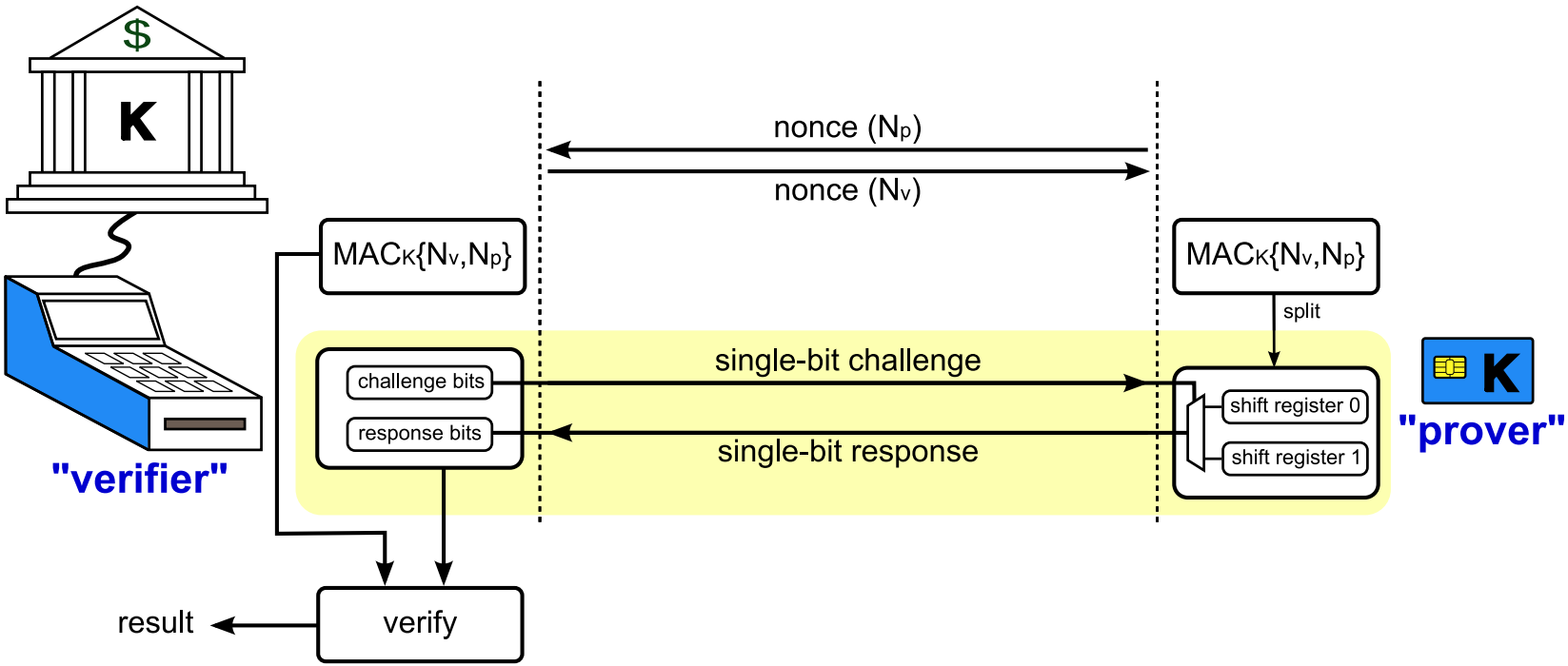
Timing critical phase:

– single bit challenge-response pairs are exchanged;

– response bit is the next bit from the shift register corresponding to the challenge bit's content;

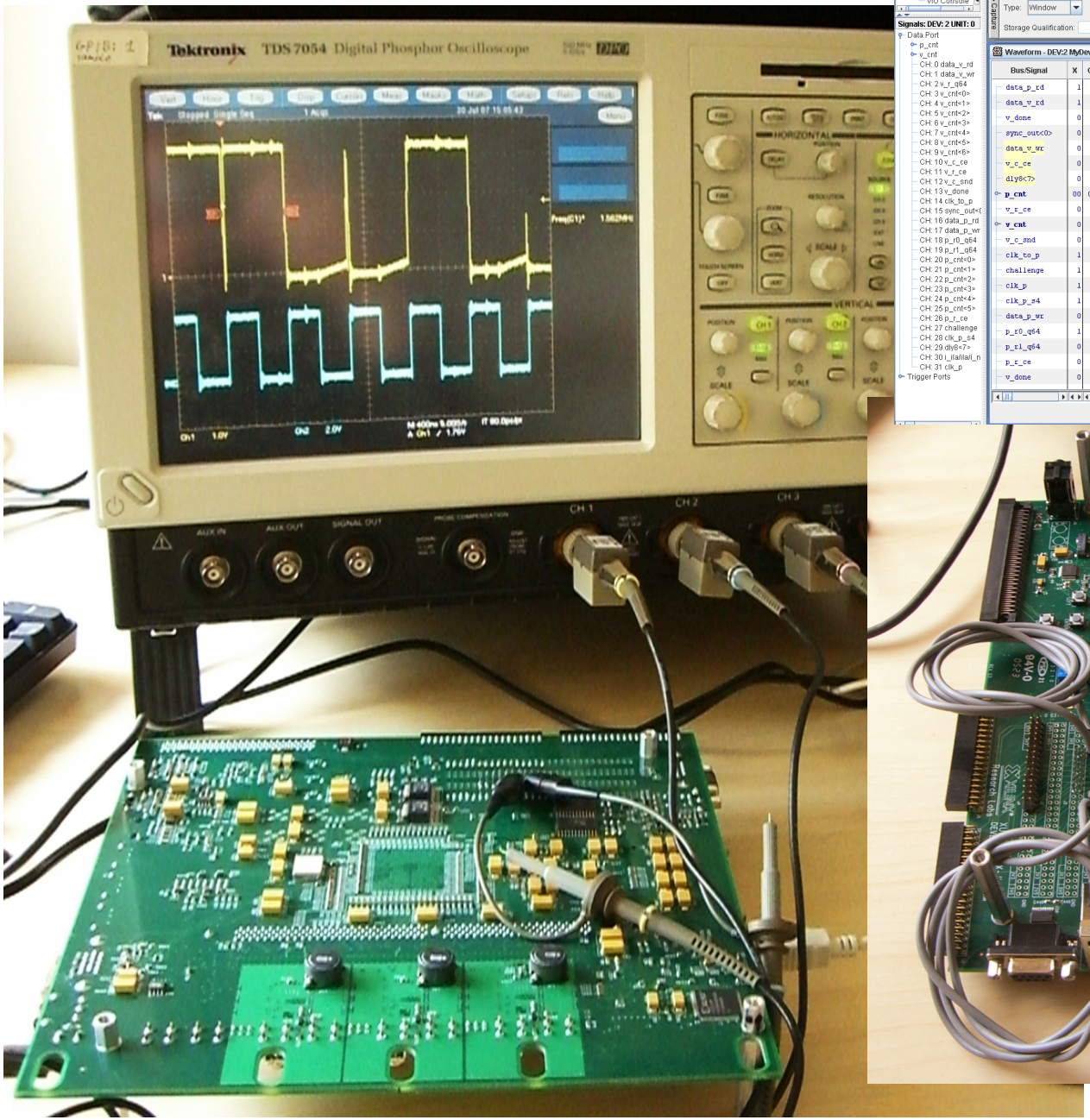
– response bit is deleted at prover and stored at verifier.

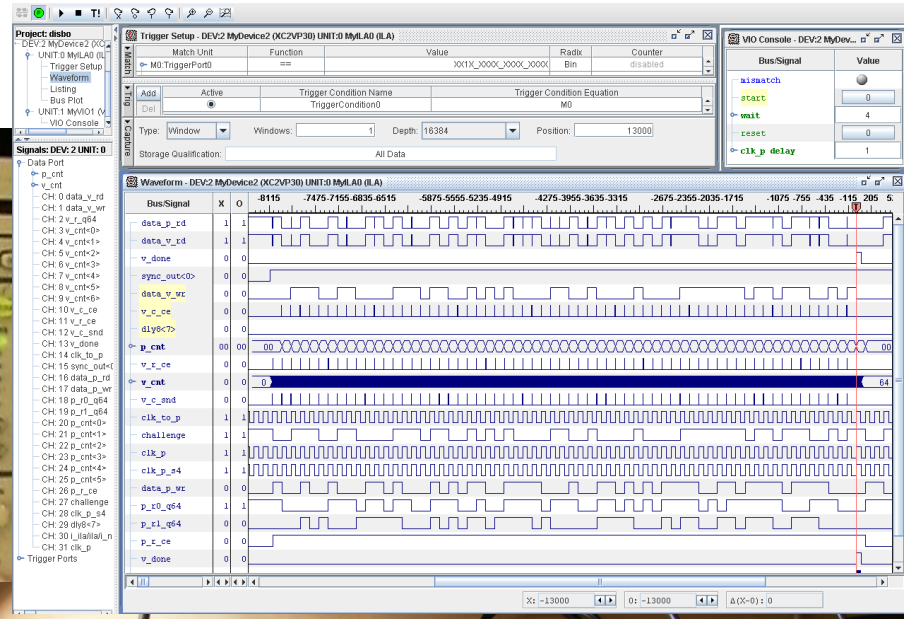
We suggest using "distance bounding"

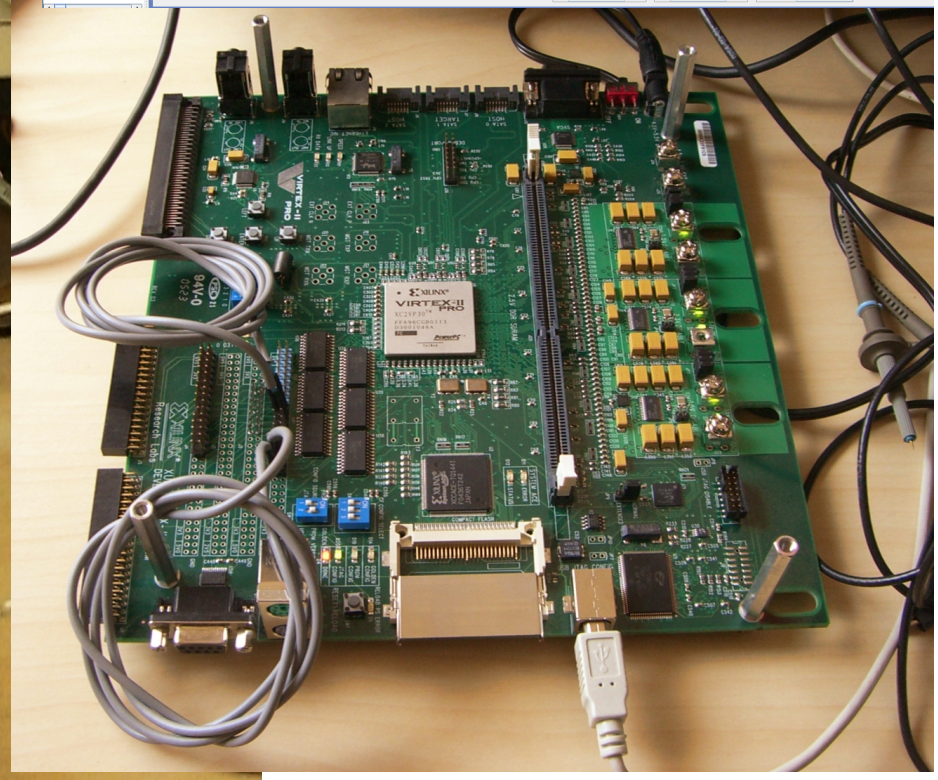


The verifier checks that the responses are correct and concludes, based on its timing settings, the maximum distance the prover is away

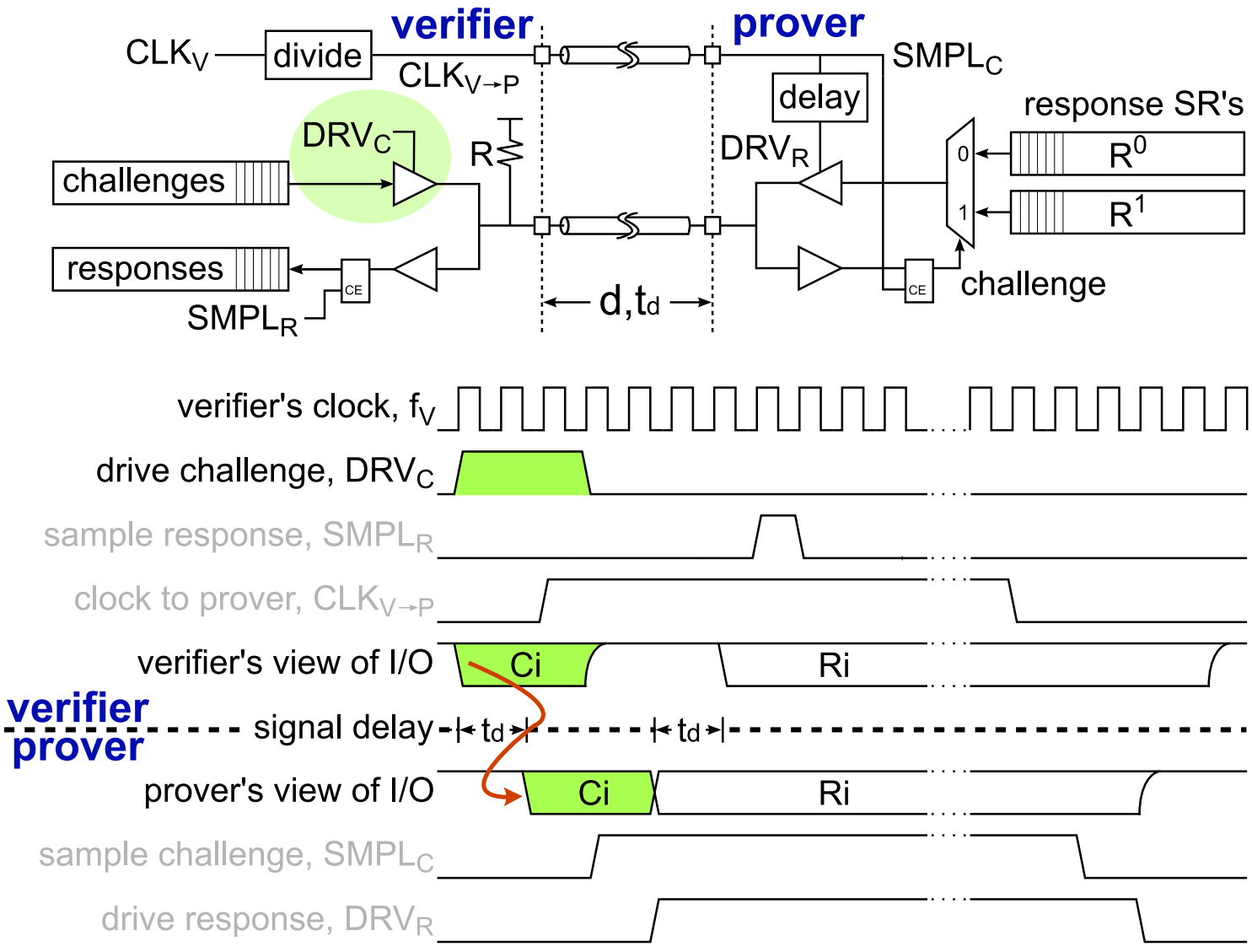
Experimental setup:



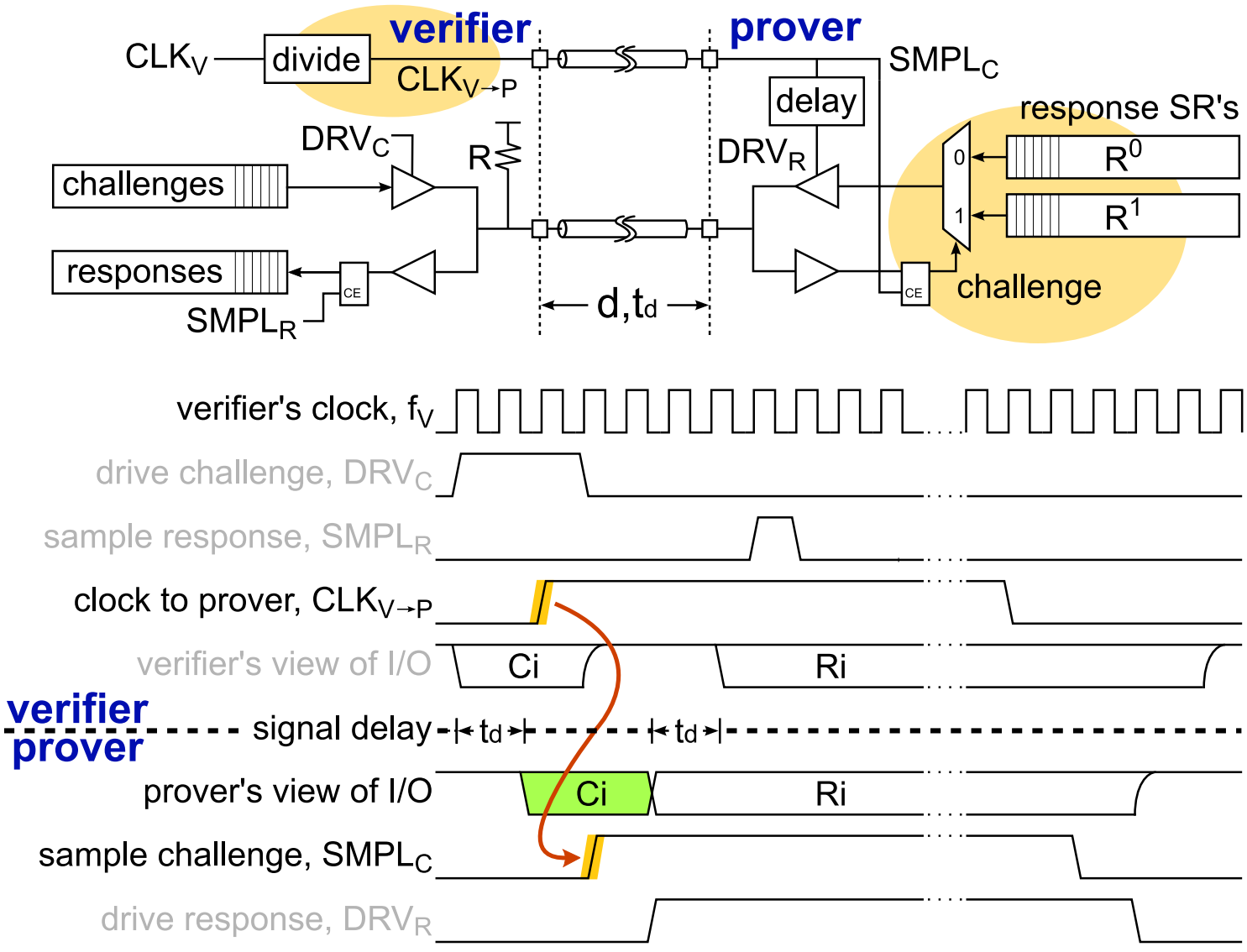




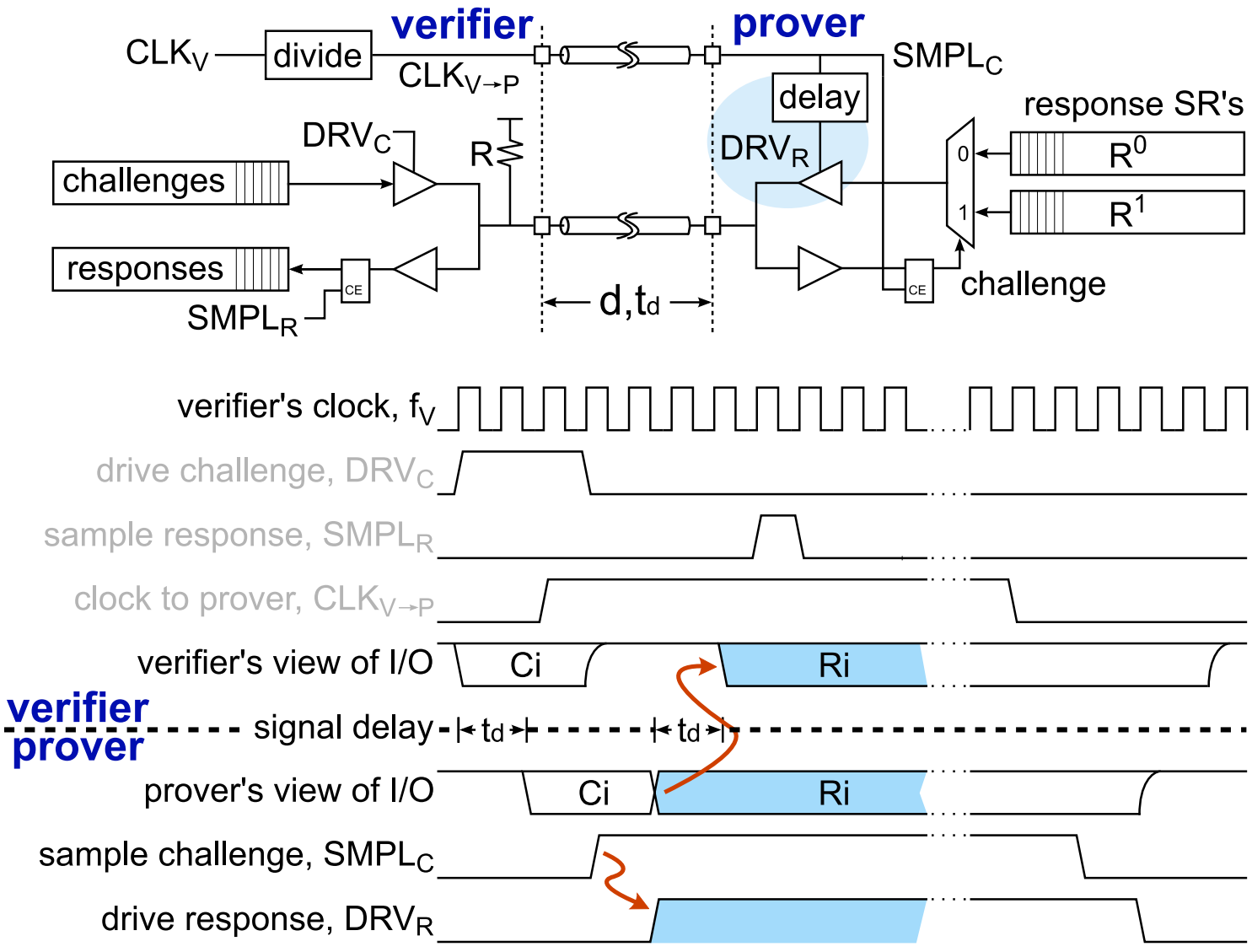
FPGA implementation is robust against capable attackers



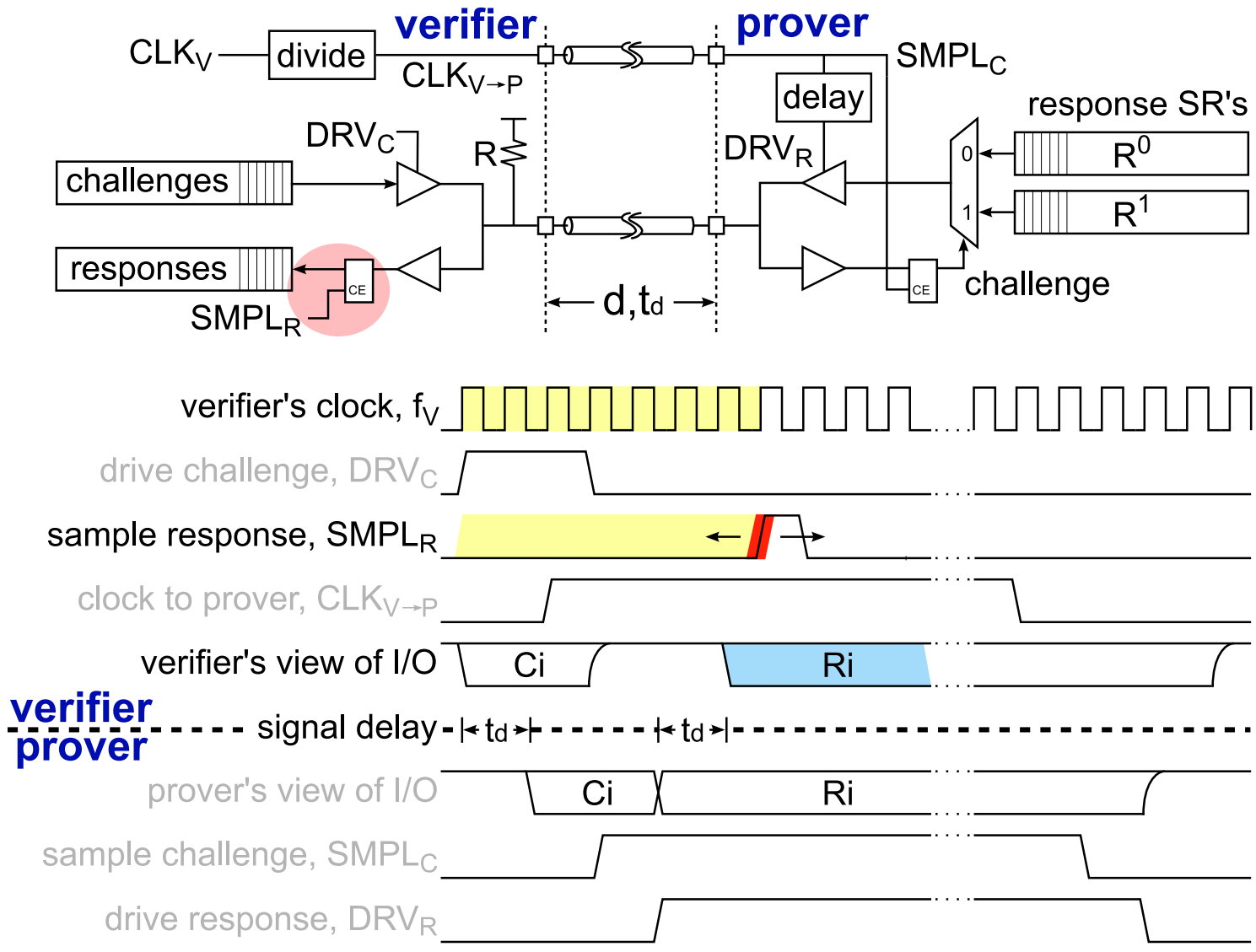
FPGA implementation is robust against capable attackers



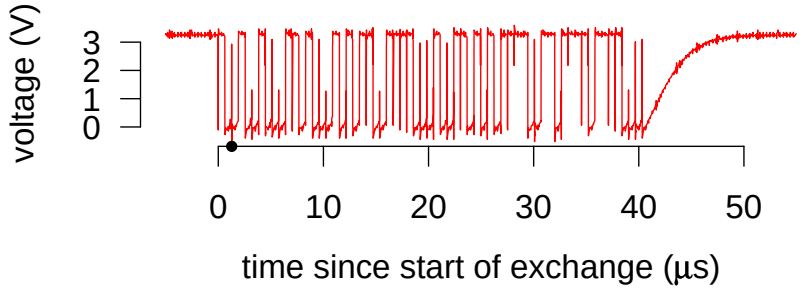
FPGA implementation is robust against capable attackers

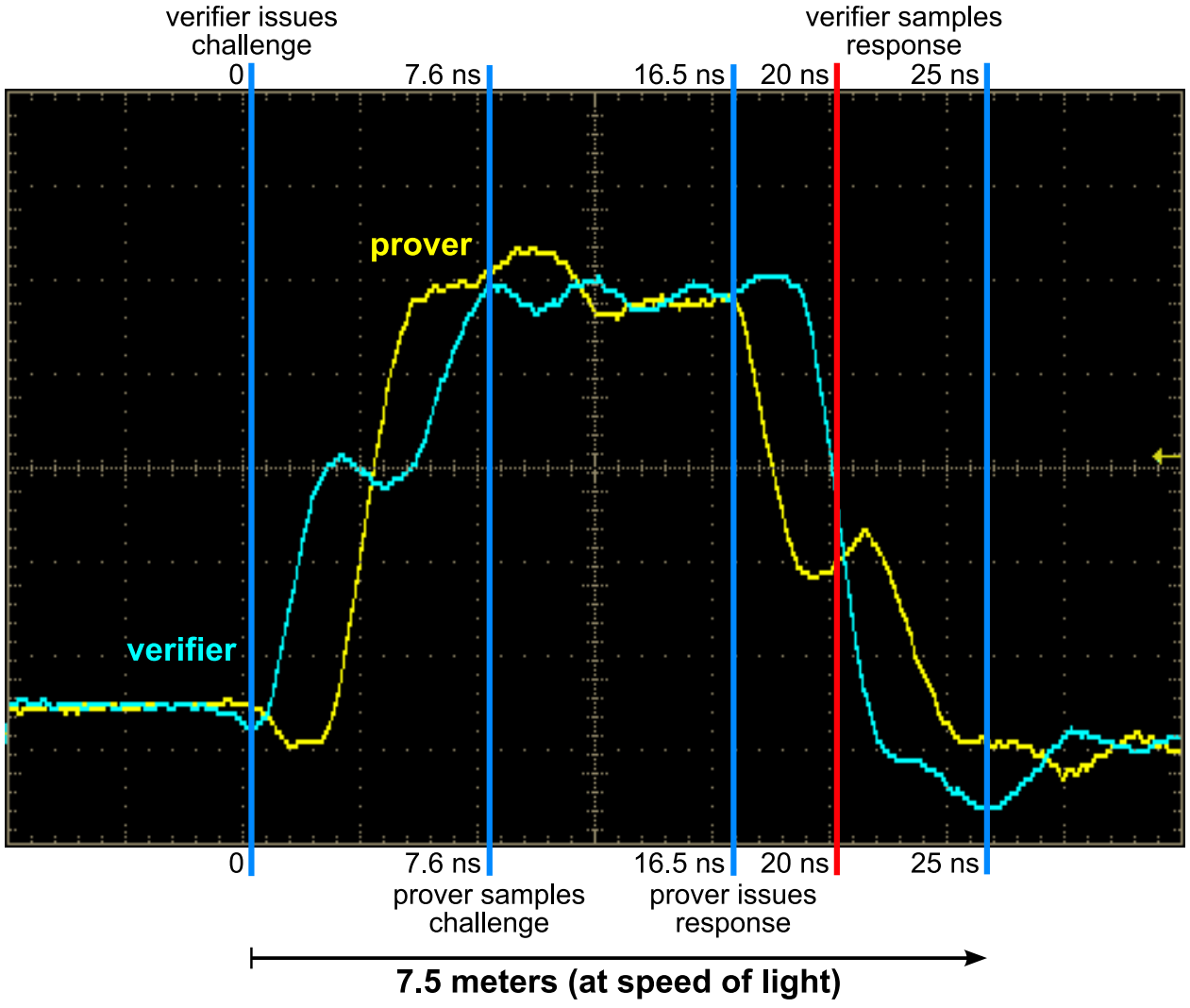


FPGA implementation is robust against capable attackers



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





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 $(\frac{3}{4})^{64} \approx 1 \text{ in } 2^{26}$;
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.

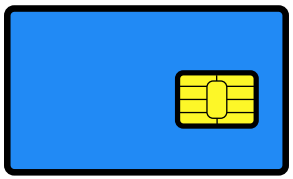
Manipulate delay lines to expose both registers' state:
Temperature compensated circuits or ones designed to prevent this are needed.

System should be designed for a particular distance

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

In summary, we have demonstrated a relay attack on a smartcard payment system, which also helped cardholders to favorably resolve disputes with their banks. Our proposed distance bounding solution provides a robust defense.

Future work:
Identify and apply distance bounding implementation (and attack) to other systems; work towards a secure distance bounding protection for RFID.

Paper, videos, and further discussion at:
`www.cl.cam.ac.uk/research/security/projects/banking/`