Talk presented at IEEE Security and Privacy 2014

Chip and Skim: Cloning EMV cards with the pre-play attack

Mike Bond, **Omar Choudary**, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson

Computer Laboratory

UNIVERSITY OF CAMBRIDGE

EMV – leading system for payments across the world

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

EMV – introduced to remove magstripe counterfeiting

- EMV uses CHIP & PIN
- Should protect against card cloning and abuse
- Should decrease fraud

Chip and PIN

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

EMV is not totally secure in practice

- We discovered 2 important flaws in EMV
  - engineering flaw
  - protocol flaw
- In practice these allow same effect as card cloning
  - we can perform a “CHIP & PIN” transaction without the original EMV card

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

EMV protocol for POS/ATM

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

EMV protocol – online authorisation

K

K

D={Amount, Country, Date, **UN**, …}

REQ={UN,ATC,IAD,…}, AUTH REQ=MAC_K(D, **ATC**, IAD)

RESP={OK/BAD}, AUTH RESP=MAC_K(RESP, AUTH REQ,…)

UN = Unpredictable Number

ATC = Application Transaction Counter

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Evidence from real data: UN is a counter!

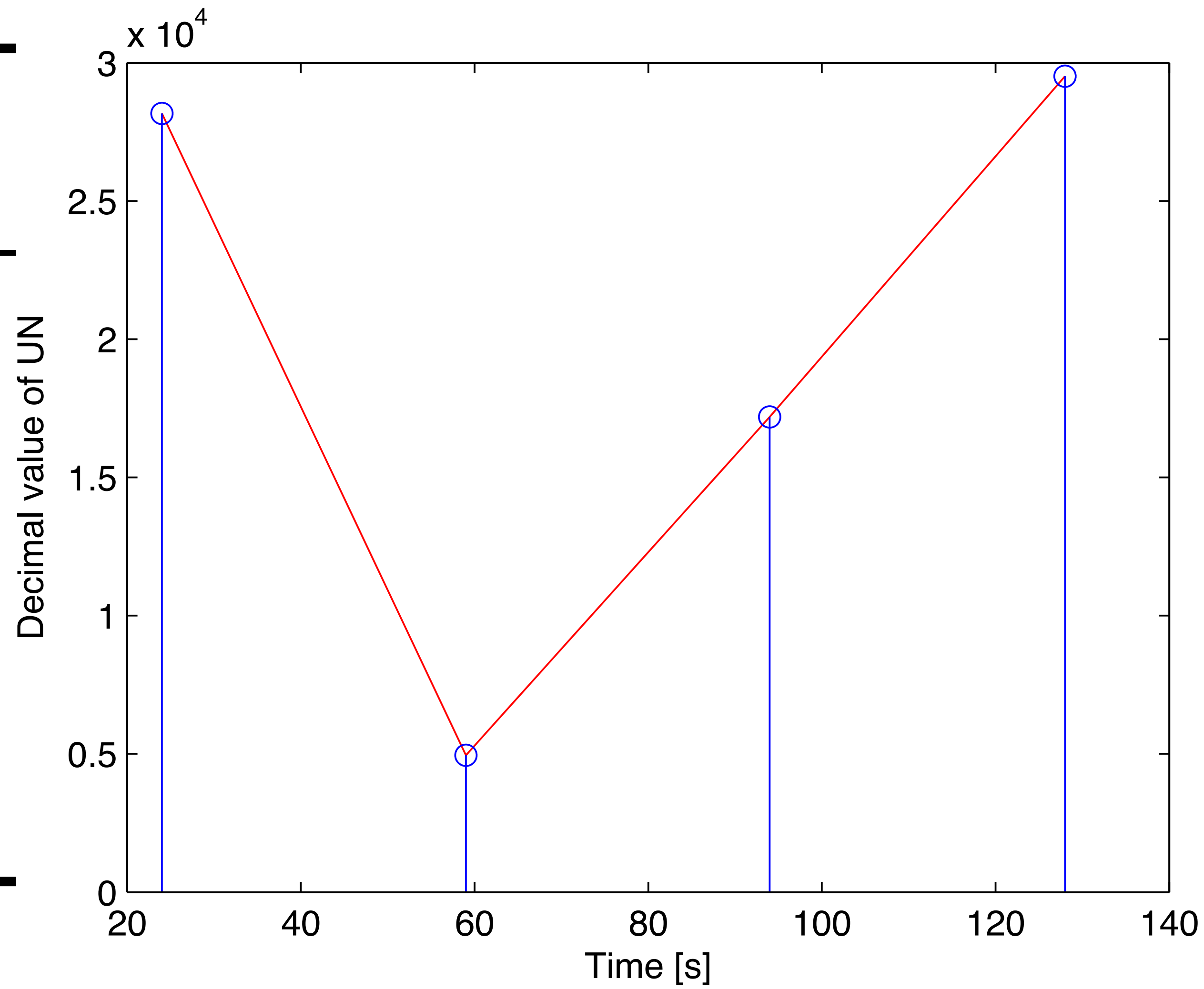
Time	UN
10:37:24	F1246E04
10:37:59	F1241354
10:38:34	F1244328
10:39:08	F1247348

- 17 bits fixed
- 15 bits seem to follow a linear counter

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Evidence from real data: UN is a counter!

Time	UN
10:37:24	F1246E04
10:37:59	F1241354
10:38:34	F1244328
10:39:08	F1247348



- 17 bits fixed
- 15 bits seem to follow a linear counter

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

No terminal ID

K

K

D={Amount, Country, Date, **UN**, …}

REQ={UN,ATC,IAD,…}, AUTH REQ=MAC$_K$(D, **ATC**, IAD)

RESP={OK/BAD}, AUTH RESP=MAC$_K$(RESP, AUTH REQ,…)

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Pre-play attack: exploit predictable UN

Step 1: Skim PIN & data for set of UNs

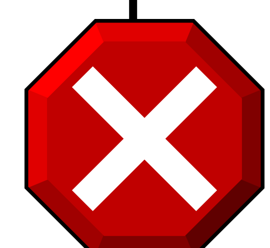
$D_1=\{\text{Amount, Country, Date, } \mathbf{UN_1}, \ldots\}$ →

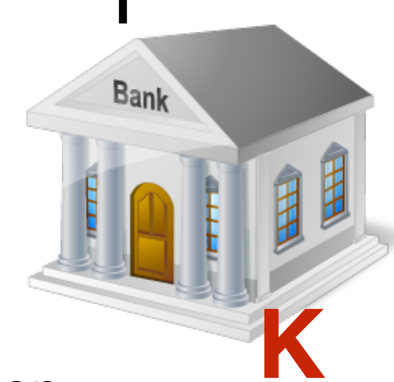
← AUTH REQ_1

$D_2=\{\text{Amount, Country, Date, } \mathbf{UN_2}, \ldots\}$ →

← AUTH REQ_2

⋮





ID	UN	AUTH REQ
1	xx	aa
2	yy	bb
…		

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Pre-play attack: exploit predictable UN

Step 2: replay data to get diamond

D={Amount, Country, Date, **UN**, …}

Replay from table of skimmed data

ID	UN	AUTH REQ
1	xx	aa
2	yy	bb
…		

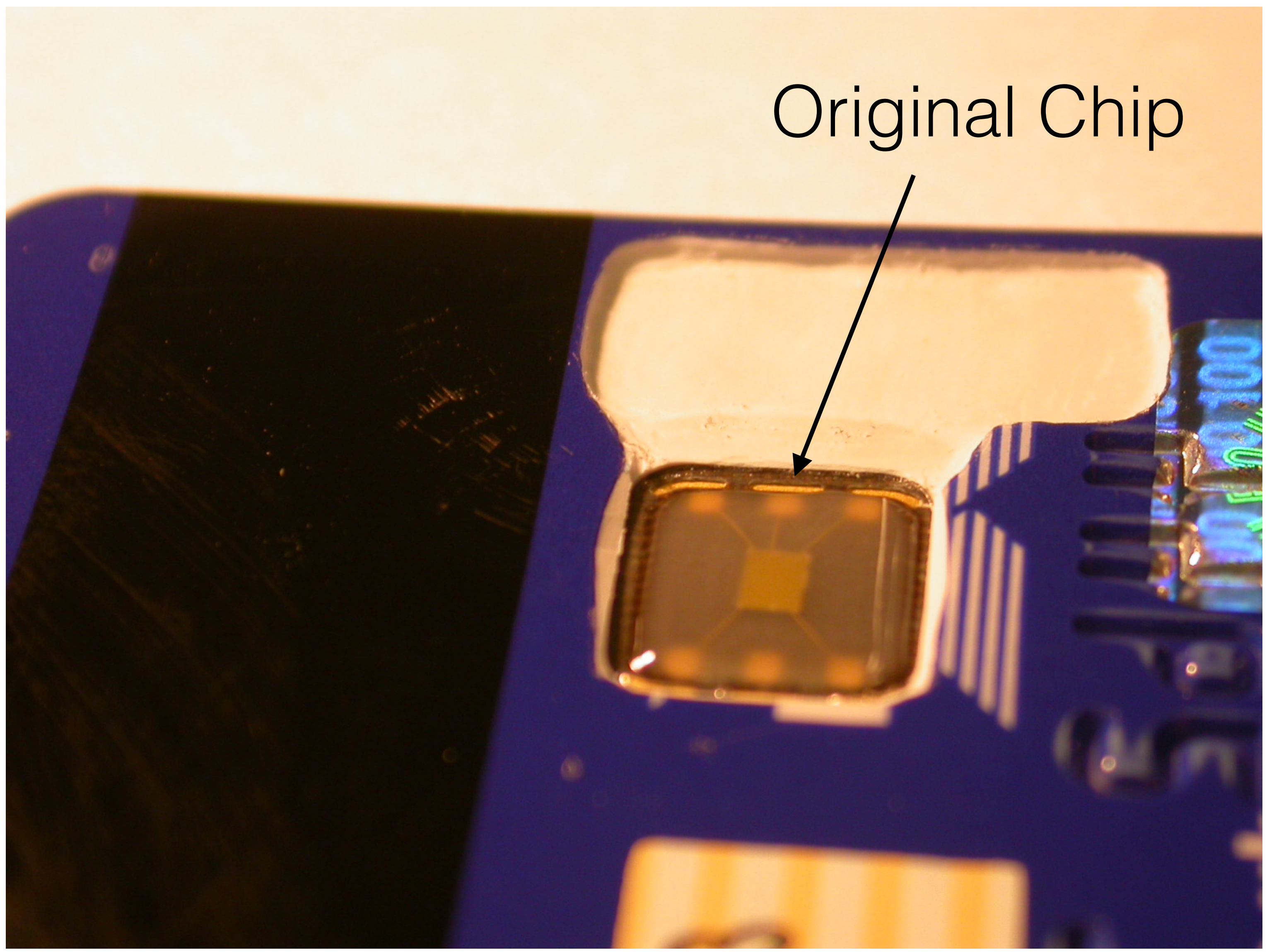
Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we find weak RNGs?

- Previous EMV specs only required 4 consecutive UNs to be different
    - a counter would work better than a secure TRNG
- We decided to find out …

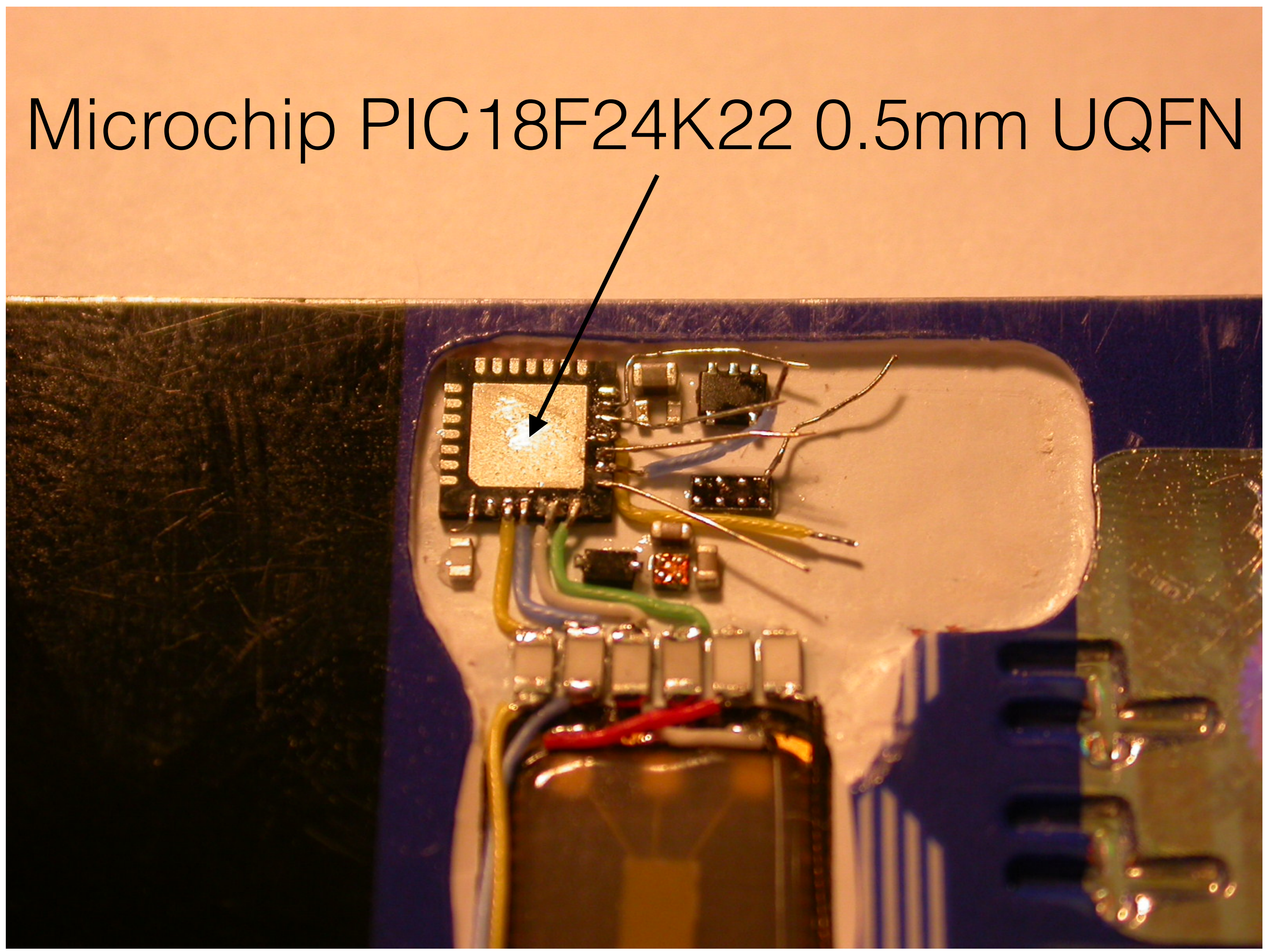
Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using ATM logger



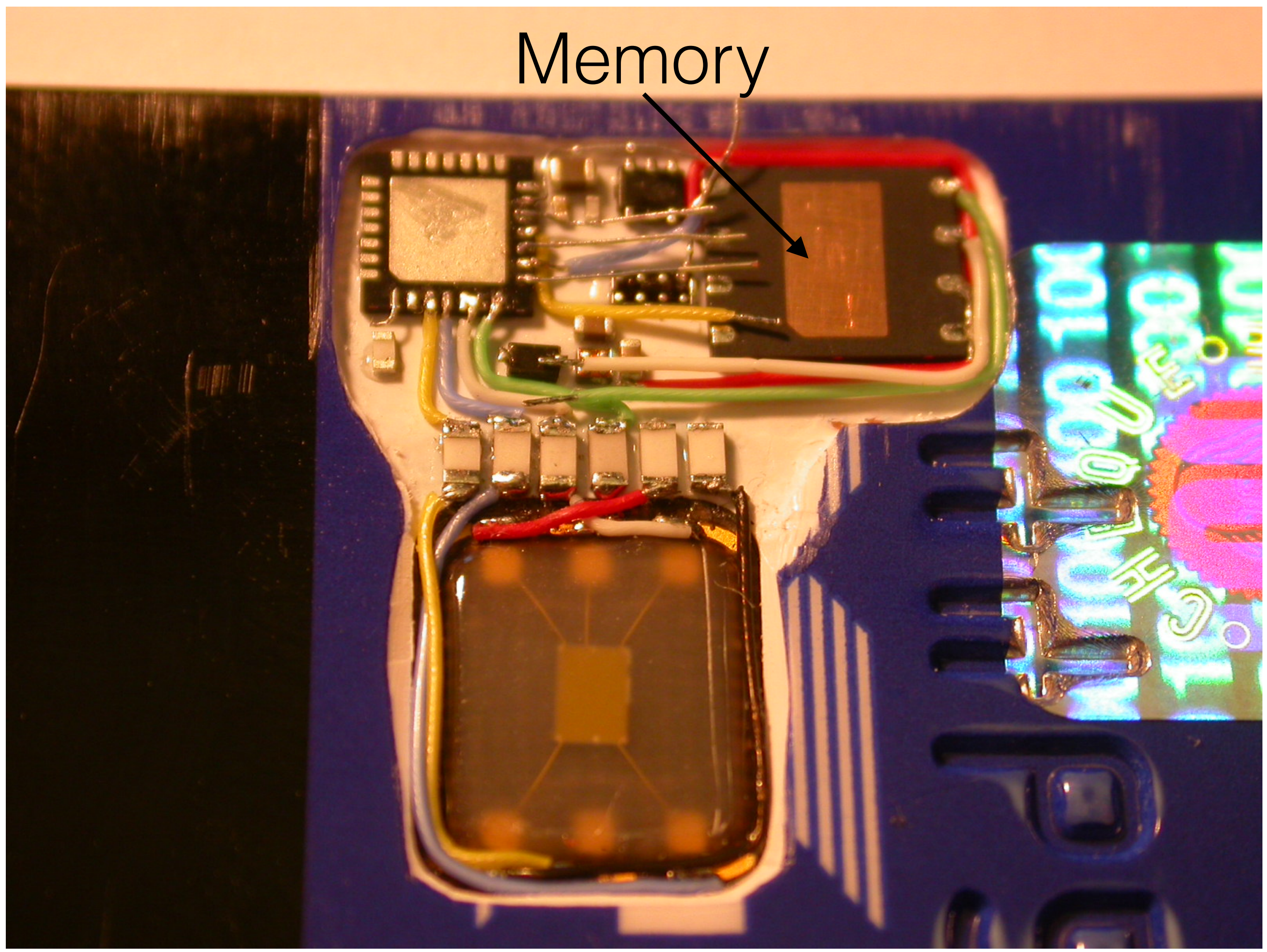
Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using ATM logger



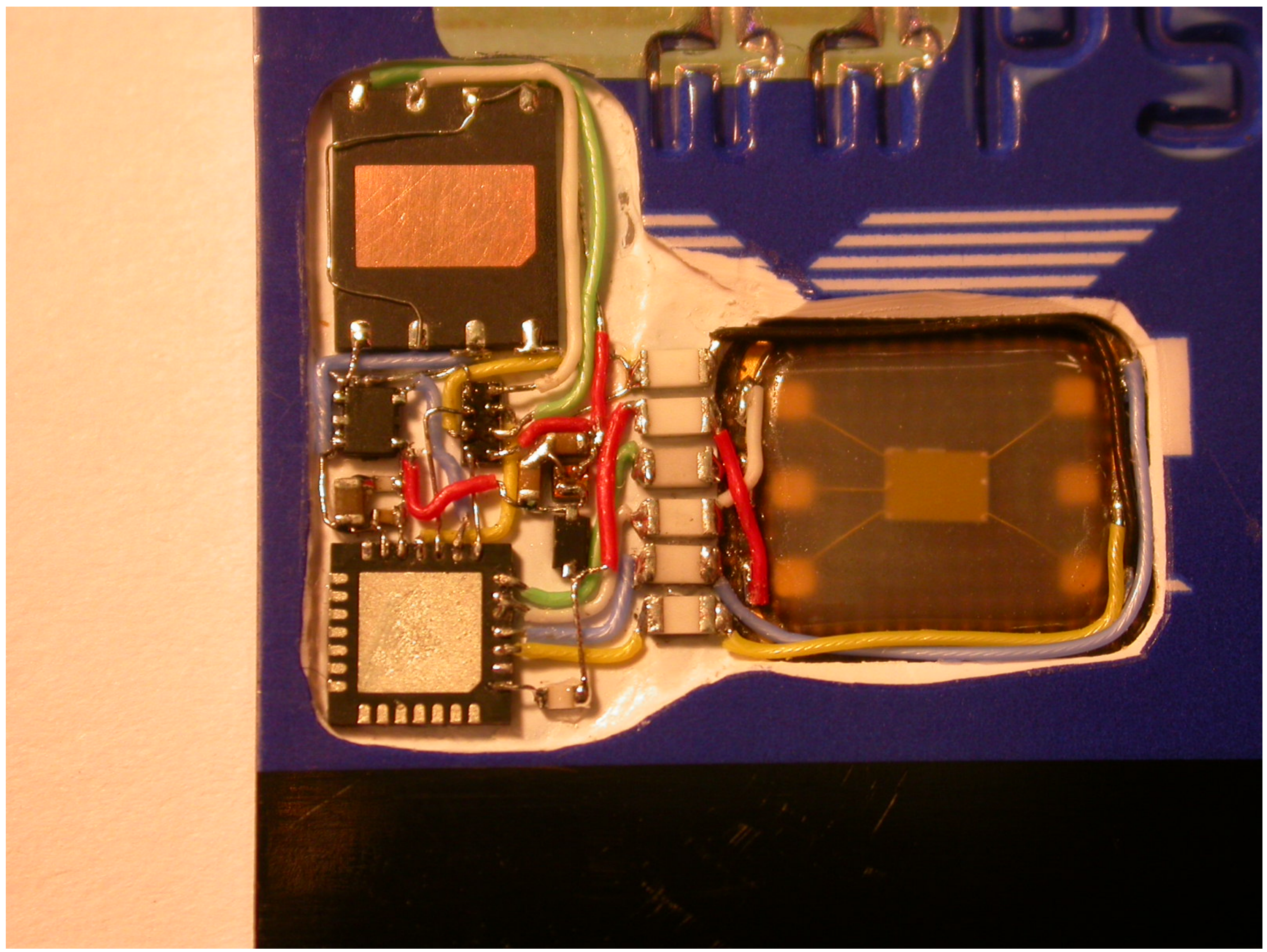
Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using ATM logger



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using ATM logger



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using ATM logger

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

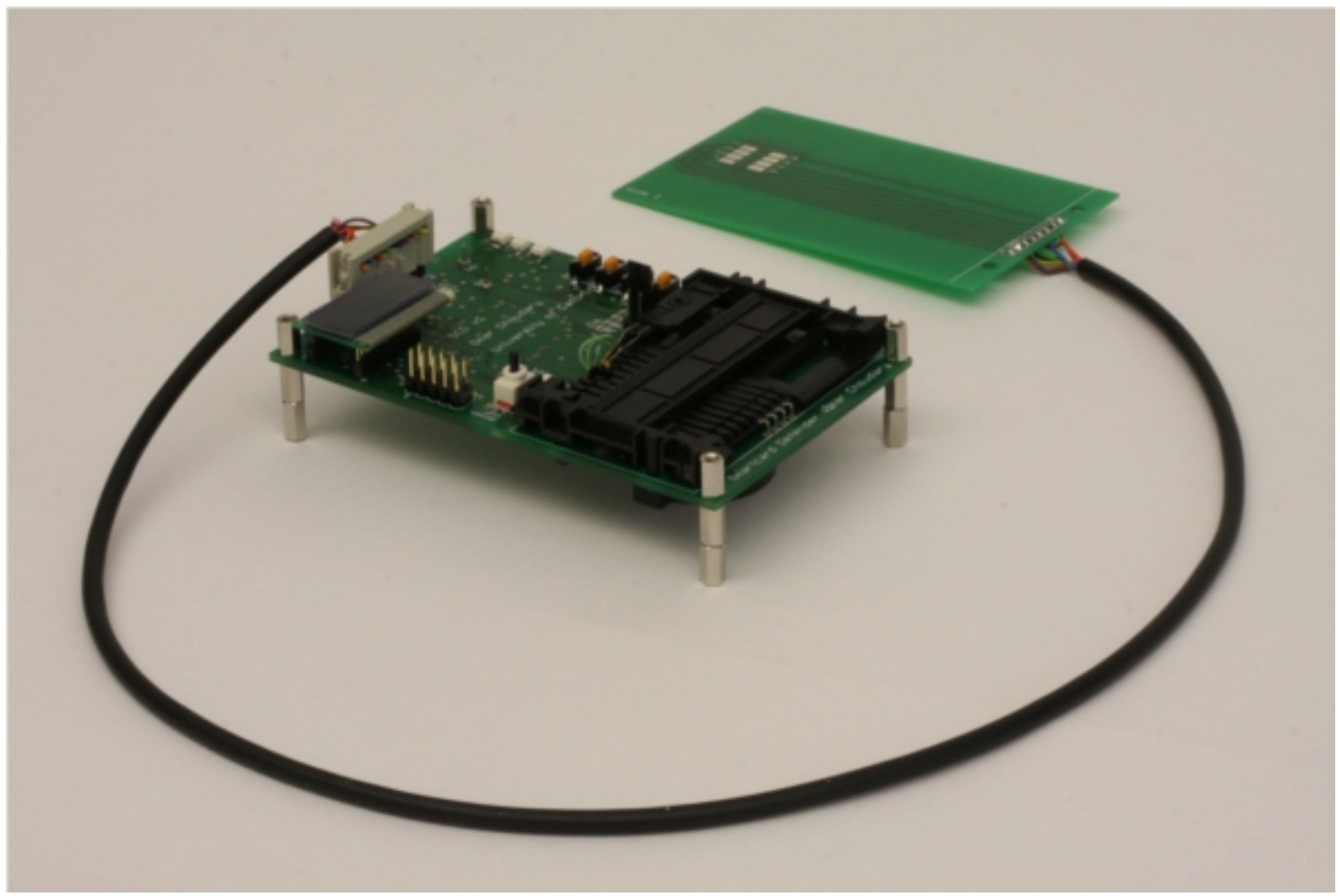
Searching for weak RNG: using ATM logger

- Characteristic C (5 bits fixed):
  - Third nibble is 0
  - First bit is 0
- 11 ATMs had same output
- Possibly due to common lib

Weak RNGs	
ATM1	690d4df2
ATM1	69053549
ATM1	660341c7
ATM1	5e0fc8f2
ATM2	6f0c2d04
ATM2	580fc7d6
ATM2	4906e840
ATM2	46099187

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using SmartCard Detective



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Searching for weak RNG: using SmartCard Detective

- Results from local POS
- First bit still 0, but otherwise could not find clear pattern

Stronger RNGs	
POS1	013A8CE2
POS1	01FB2C16
POS1	2A26982F
POS1	39EB1E19
POS1	293FBA89
POS1	49868033

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

The deeper problem:
We can use our own UN!

K

K

D={Amount, Country, Date, **UN**, …} →

← REQ={UN,ATC,IAD,…}, AUTH REQ=$\text{MAC}_{\mathbf{K}}$(D, ATC, IAD)

RESP={OK/BAD}, AUTH RESP=$\text{MAC}_{\mathbf{K}}$(RESP, AUTH REQ,…) →

UN generated by Terminal (POS, ATM), not issuer!

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

The pre-play attack by tampering UN

Step 1: get PIN & data for a **chosen** UN

D={Amount, Country, Date, **UN**, …}

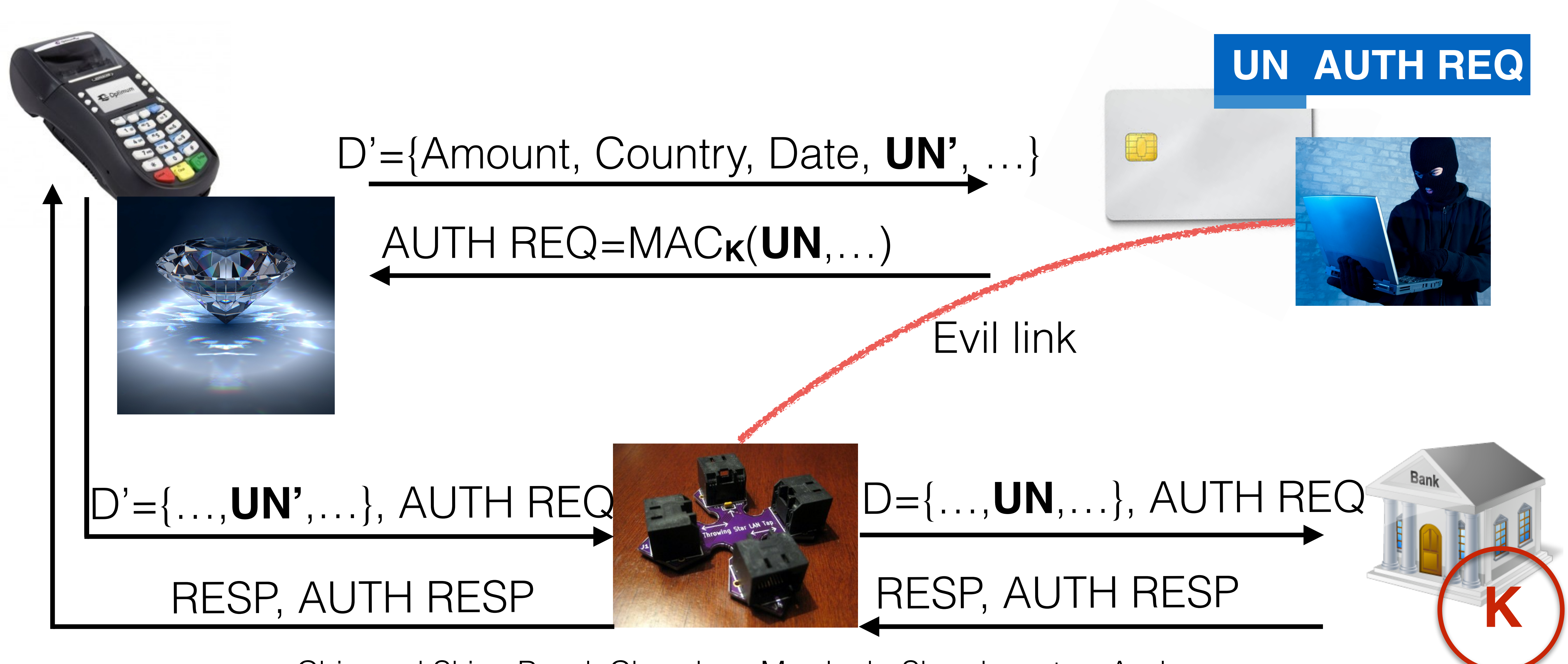
AUTH REQ=MAC$_K$(D, ATC, IAD)

K

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

The pre-play attack by tampering UN

Step 2: replay data & tamper UN to get diamond



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we actually modify the UN sent by the terminal ?

Likely. It depends on bank, country, regulator, etc.

Issuer

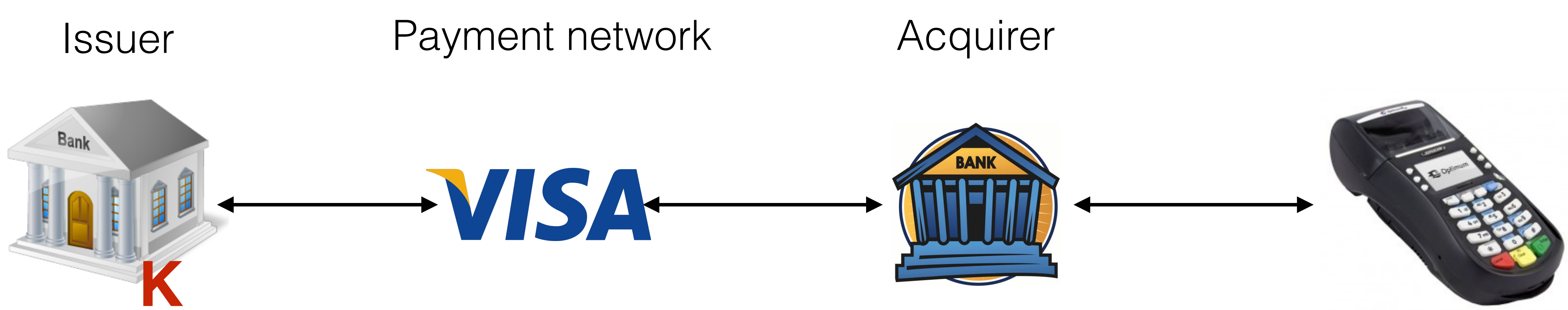
syntax, semantic: ISO 8583, ISO 20022, …

transport: AS2, AS3, SWIFT, FTP, IFX, …

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we actually modify the UN sent by the terminal ?

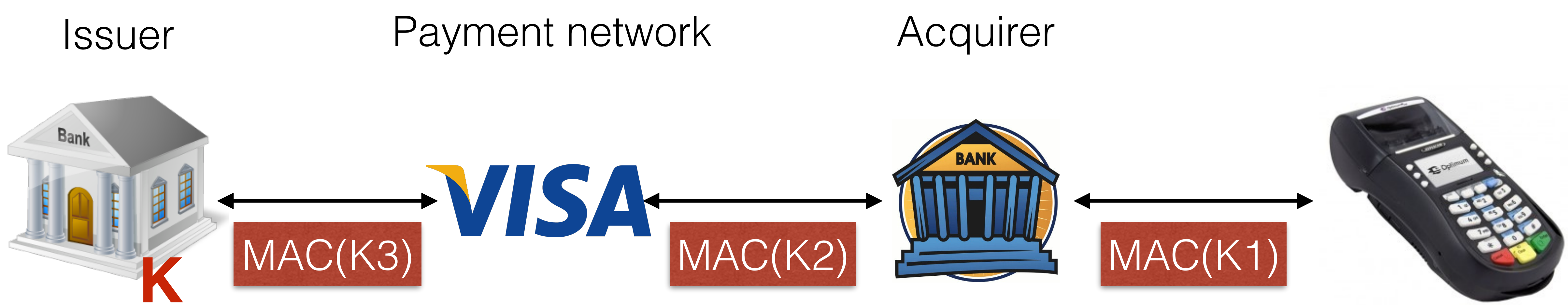
Likely. It depends on bank, country, regulator, etc.



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we actually modify the UN sent by the terminal ?

Likely. It depends on bank, country, regulator, etc.



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we actually modify the UN sent by the terminal ?

… ***emergence of new functionality such as authentication methods*** …
[VISA "Transactions Acceptance Device Guide" 2013]

Practical example: Maxwell Parsons in UK

- injected data into the bank system (reverse transactions), steeling £2,560,000 in 7 months

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Can we actually modify the UN sent by the terminal ?

- Even if authentication is enabled, there are options:
  - Malware infection of POS/ATM
  - Supply chain attacks (react on covert signal)
  - Collusive or dishonest merchant

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

It is a protocol problem

- Issuer relies on fresh UN for transaction
- But UN generated by terminal
- Terminal might not have incentive to cooperate

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Card authentication via DDA does not help

Start transaction

Card data records

Signature over data records

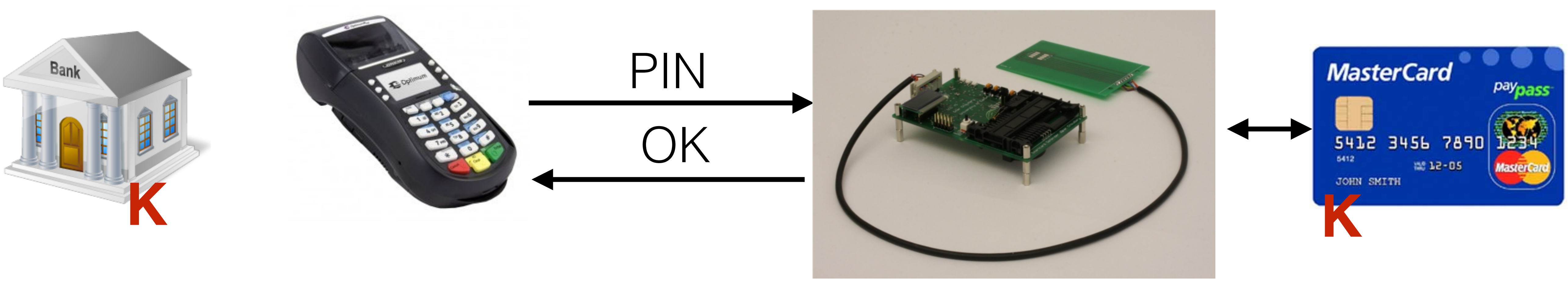
PKI

Same UN for both DDA and ARQC => skim signature as well

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

PIN verification does not help either

Simply skim PIN during step (1) of attack, or lie [Oakland '10]



Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Blocking a pre-play attack using the Transaction Certificate (TC)

K

K

D={Amount, Country, Date, **UN**, …}

REQ={UN,ATC,IAD,…}, AUTH REQ=MAC_K(D, ATC, IAD)

RESP={OK/BAD}, AUTH RESP=MAC_K(RESP, AUTH REQ,…)

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Blocking a pre-play attack using the Transaction Certificate (TC)

K

K

D={Amount, Country, Date, **UN**, …} →

← REQ={UN,ATC,IAD,…}, AUTH REQ=$\text{MAC}_{\mathbf{K}}$(D, ATC, IAD)

RESP={OK/BAD}, AUTH RESP=$\text{MAC}_{\mathbf{K}}$(RESP, AUTH REQ,…) →

External Authenticate

RESP, AUTH RESP →

D’ →

Final exchange

← TC=$\text{MAC}_{\mathbf{K}}$(D’, ATC, **IAD**)

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Importance of TC not taken into consideration

- Problem 1: TC not routinely kept
  - not needed for clearance, may be discarded
  - only needed to ensure that card does not need to go online (issuer) at next transaction and to provide liability protection to acquirer
- Problem 2: TC may be sent within 24 hours
  - good: send daily TC batches to reduce #messages
  - bad: this leaves system open to pre-play attack

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

What could EMV do

- Fix RNG everywhere
- Mandatory authentication between all parties
- Request terminal to keep log of UNs for disputes
- Mandatory check or at least storage of TC for every transaction
  - **TC should be the only probative evidence** in case of disputes
- For high-value transactions, check TC before customer leaves the shop!

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Conclusions

- We discovered a deep and important flaw in the EMV implementation, indistinguishable from card cloning
- Issuer relies on freshness, but this is generated by another party
  - Changing the protocol is unlikely to happen
  - Practical solution is mandatory use or retention of TC
- Lack of understanding and deliberate overstatement of security may lead to customers being defrauded
- Bank regulators should prohibit EMV liability shift

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Questions?

Speaker: Omar Choudary

Co-authors: Mike Bond, Steven Murdoch, Sergei Skorobogatov, Ross Anderson

E-mail: firstname.lastname@cl.cam.ac.uk

Security Group, Computer Laboratory

UNIVERSITY OF CAMBRIDGE

Industry response

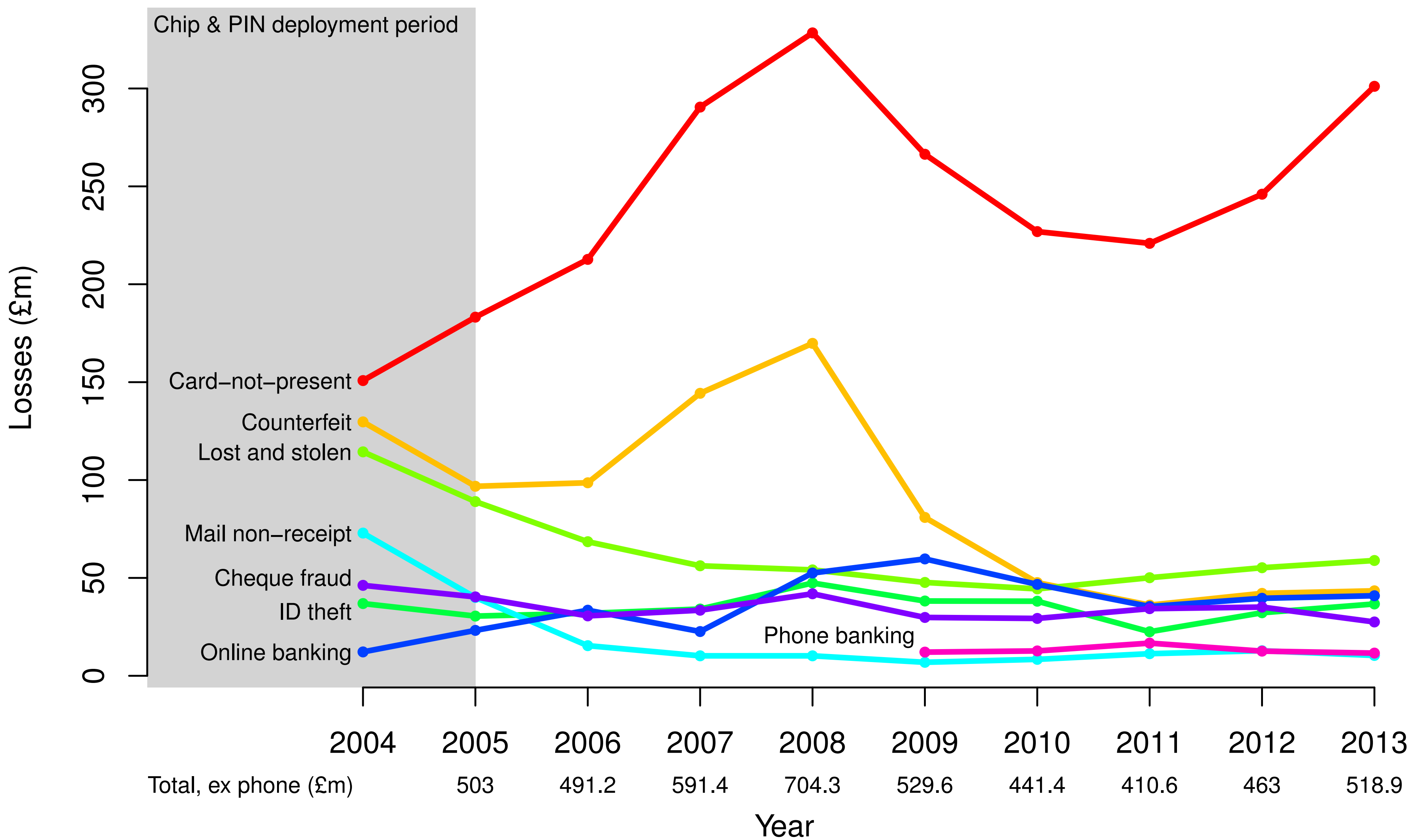
- RNG attack disclosed in early 2012
- Banks and payment switches acknowledge receipt
- April 2012 EMVCo publishes update on RNG
- However, ATMs and terminals still vulnerable to malware
  - industry insider mentioned Malta's case may involve ATM malware

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

ATM reverse engineering

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.

Bank losses by kind



Fraud levels on UK-issued payments cards

Chip and Skim. Bond, Choudary, Murdoch, Skorobogatov, Anderson.