

---

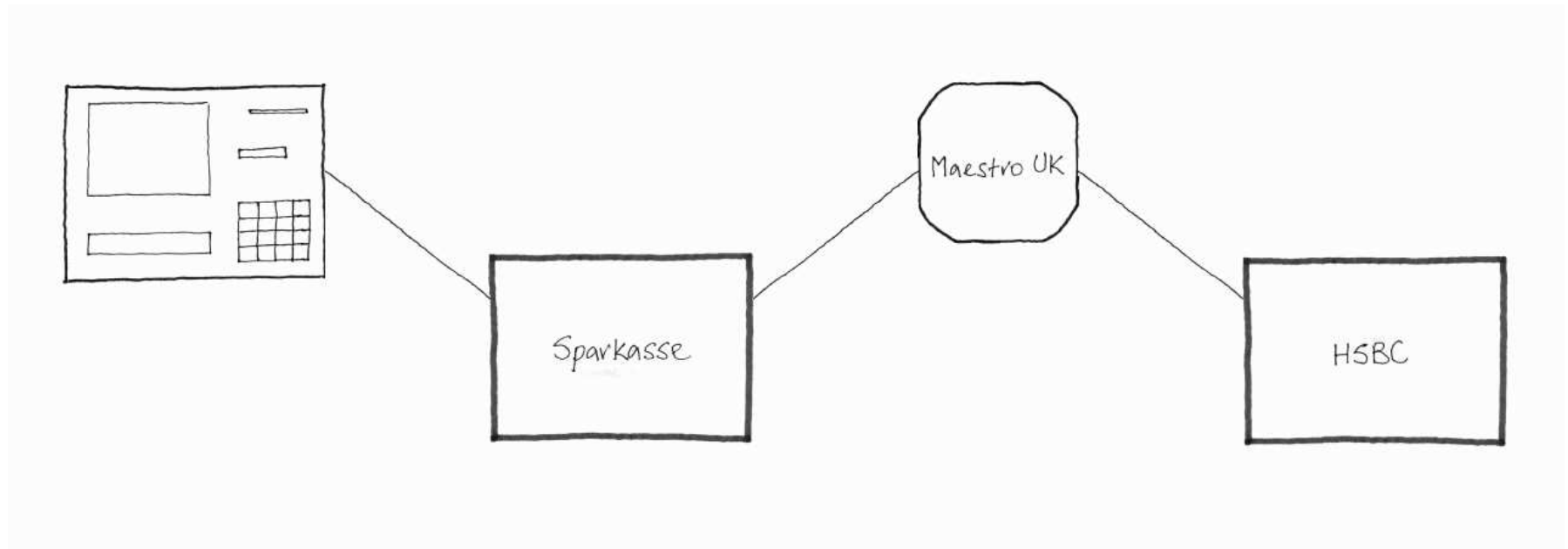
# Formal Analysis of PIN Block Attacks

Graham Steel



 School of  
**informatics**

# Automated Teller Machine Networks



## Hardware Security Modules (HSMs)



## PIN Blocks

64-bit strings to encode a guessed PIN for encryption

e.g.

VISA format 3

PPPPFFFFFFFFFFFFFFF

ISO 9564 format 0

04PPPPFFFFFFFFFFFFFFF

0000AAAAAAAAAAAAAA

Error check on translation ( $0 \leq P \leq 9$ ) leaks information (Clulow, 2003)

## Dectab Attacks

$$\text{PIN} = \text{dectab}(\{ \text{PAN} \}_{\text{PDK}}) + \text{OFFSET}$$

Standard

0123456789ABCDEF

0123456789012345

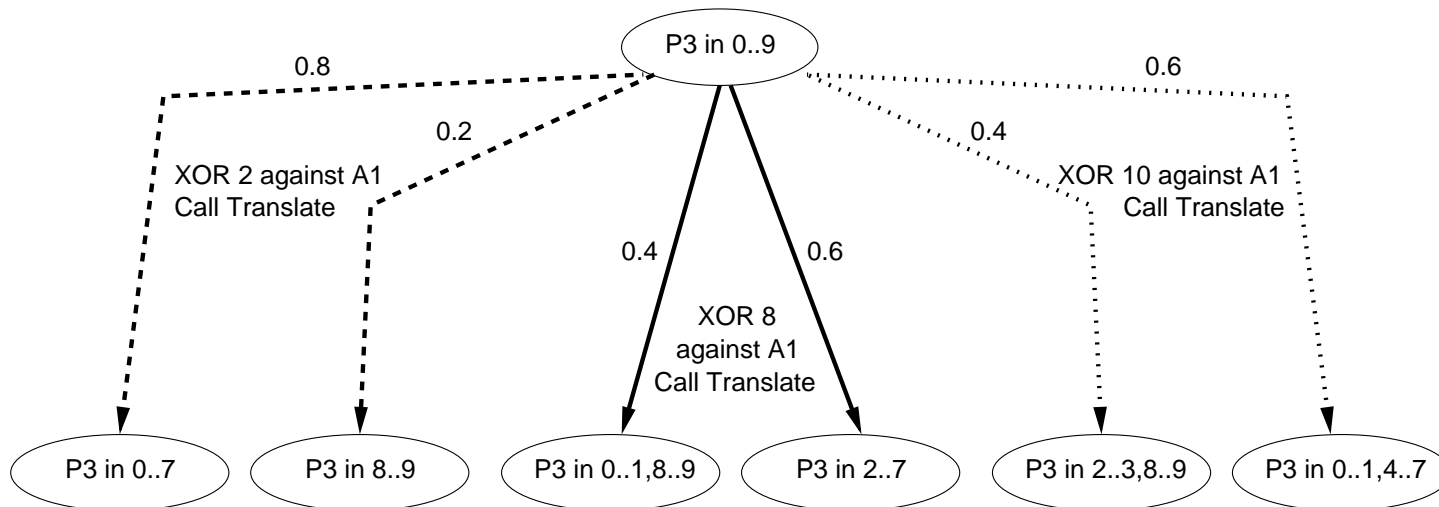
Attack 1

0123456789ABCDEF

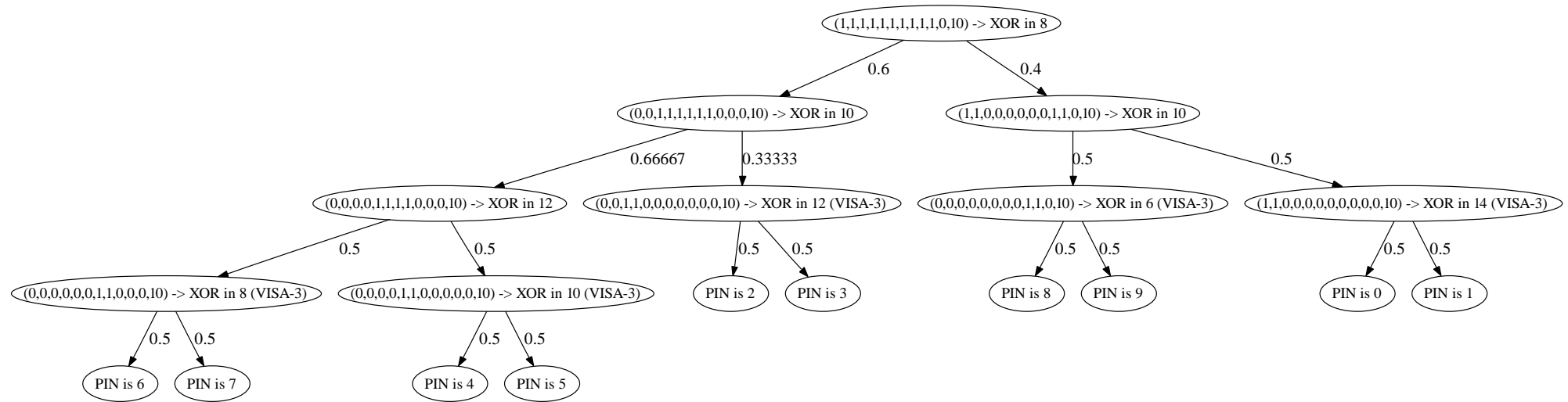
1123456789112345

Alter offset to establish position of digits (Bond + Zieliński, 2003)

# Attack Trees



# Optimised Attack



## Summary

- Have probabilistic framework for PIN block attack analysis
- Can analyse varying configurations
- API definition file requires some care  
aim to automate this in future

---

More details, downloads, etc.:

*Formal Analysis of PIN Block Attacks*. To appear in a special issue of  
**Theoretical Computer Science** on Security Protocol Analysis, 2006.

<http://dream.inf.ed.ac.uk/projects/aascs/>