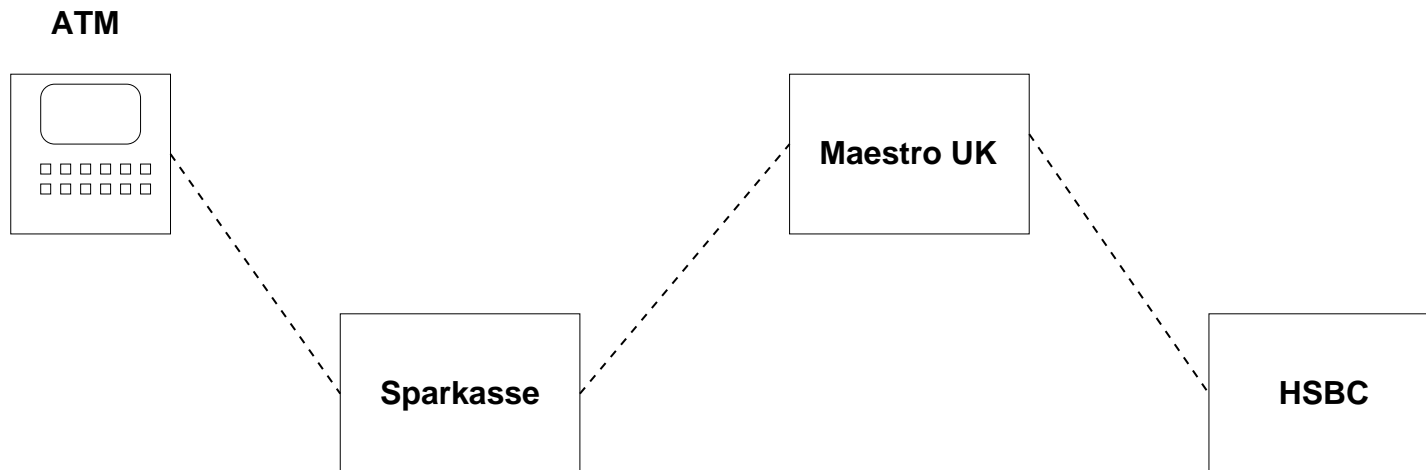

Formal Analysis of PIN Block Attacks

Graham Steel



 School of
informatics

Automated Teller Machine Networks



Hardware Security Modules (HSMs)





PIN Derivation - IBM 3624 Method

Original PIN (IPIN) derived by:

3DES encrypting 0000AAAAAAAAAAAA
under a PDK (PIN Derivation Key)

Where the As are your account number (PAN)

Decimalise result

0123456789ABCDEF

0123456789012345

$\text{PIN} = \text{IPIN} + \text{Offset (modulo 10 each digit)}$

Offset NOT secure!

PIN Blocks

64-bit strings to encode a guessed PIN for encryption

e.g.

VISA format 3

PPPPFFFFFFFFFFFFFFF

ISO 9564 format 0

04PPPPFFFFFFFFFFFFFFF

0000AAAAAAAAAAAAA

PIN Block Attacks

Ingredients:

PAN

Offset

PDK (in 'safe' form)

Encrypted PIN Block (EPB)

Decimalisation Table (Dectab)

Goal:

Use API commands to determine value of PIN

Example - Verify_Offset_PIN

Input:

PIN Block Key

PDK

Encrypted PIN Block

PIN Block format

Offset

PAN

Output: true/false

PIN Block Processing commands

More examples:

Verify_IBM_PIN

Verify_PVV

Translate_Encrypted_PIN

Clear_PIN_Encrypt

Customer enables ones he needs at installation time

ISO-0 Reformatting attack

(Clulow, 2003)

```
04PPPPFFFFFFFFFFFF
```

```
0000AAAAAAAAAAAA
```

Error check ($0 \leq P \leq 9$) leaks information

Extend:

Masquerade ISO-0 as VISA format 3

```
0604PPPPFFFFFFFFFFFF
```

Can now uniquely determine digits

Dectab Attacks

Standard

0123456789ABCDEF

0123456789012345

Attack 1

0123456789ABCDEF

1123456789112345

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

Formal Modelling

Take a customer configuration and an API spec. as input

Using CLP, generate tree of all possible attacks

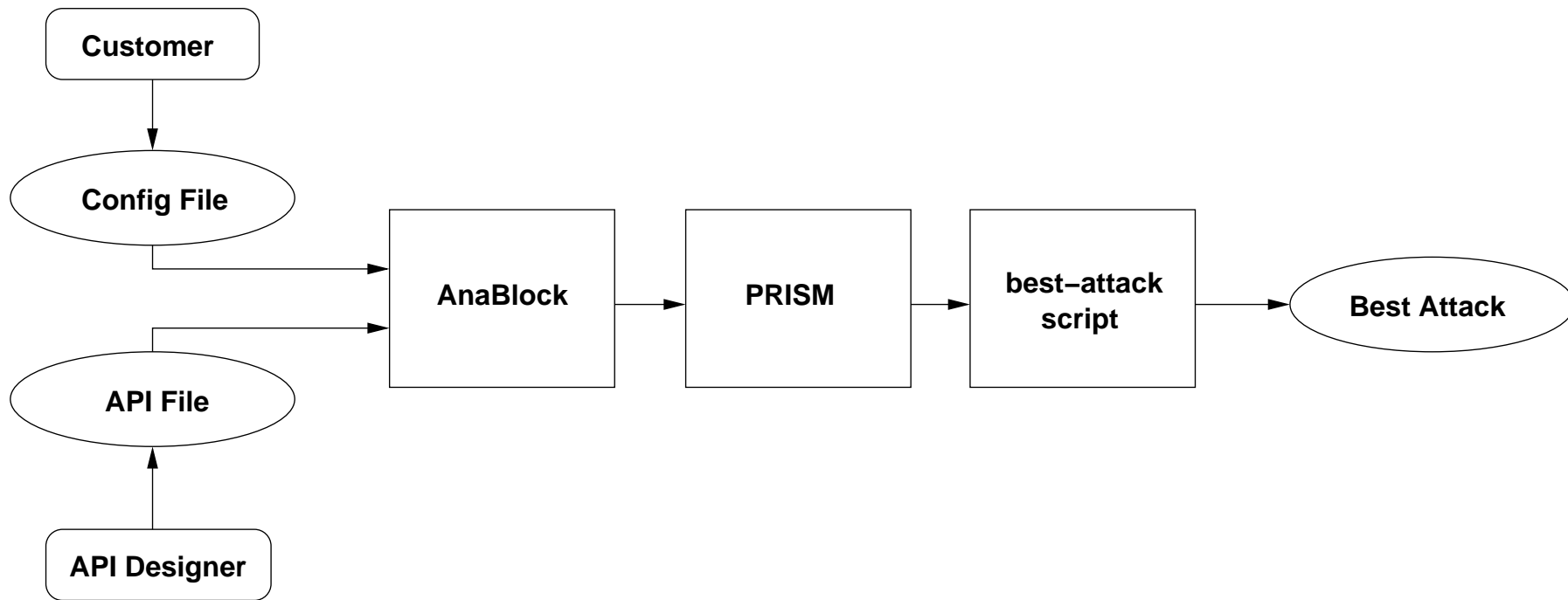
Meta-logical predicates allow us to calculate transition probabilities

Apply PRISM (Kwiatkowska et. al, 2004)

Get minimum expected number of steps to determine PIN

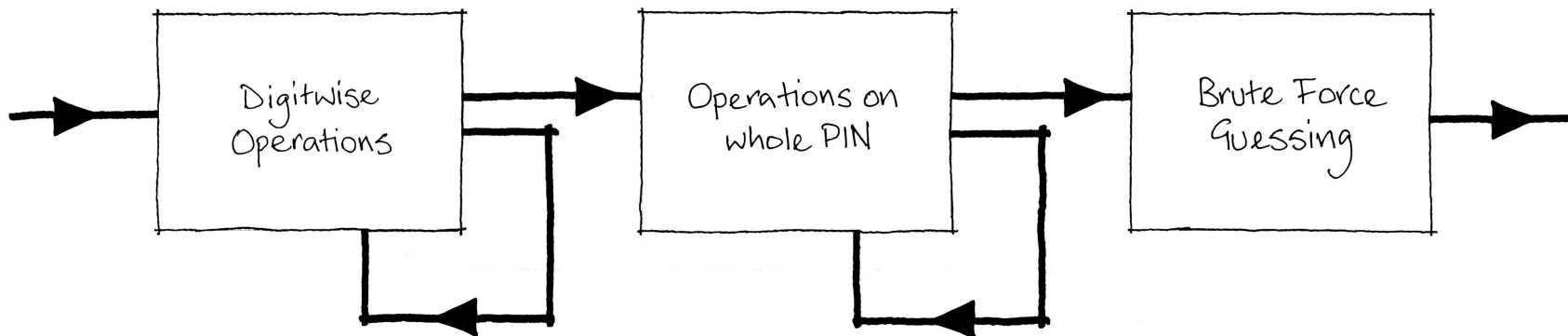
Generate tree for best attack

AnaBlock Diagram

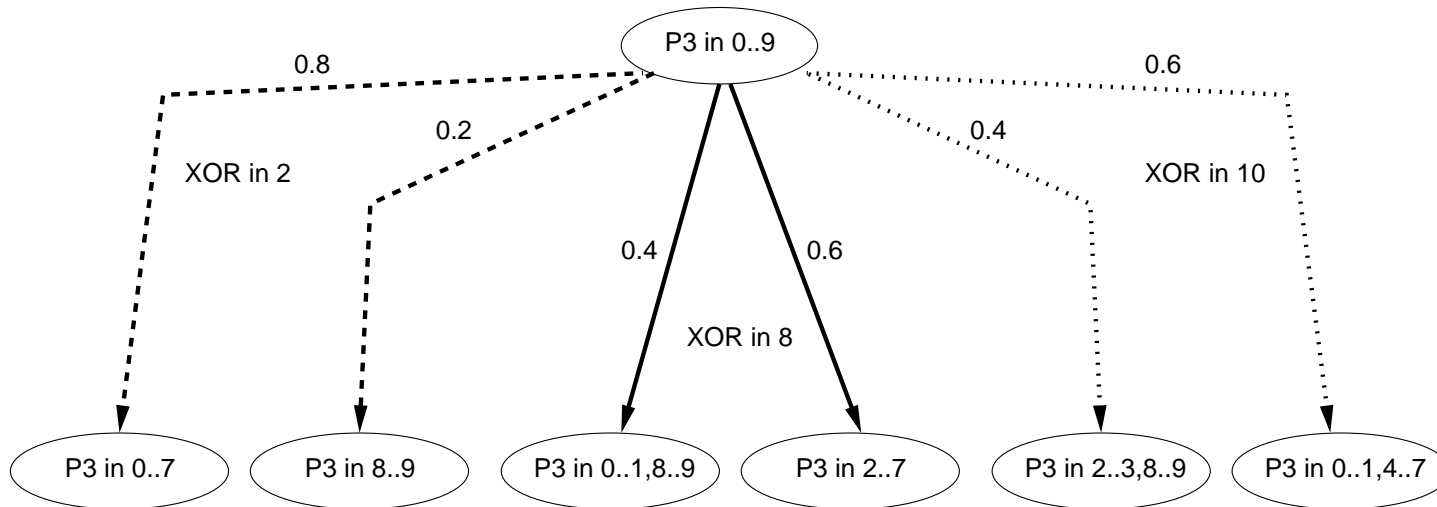


determine Predicate

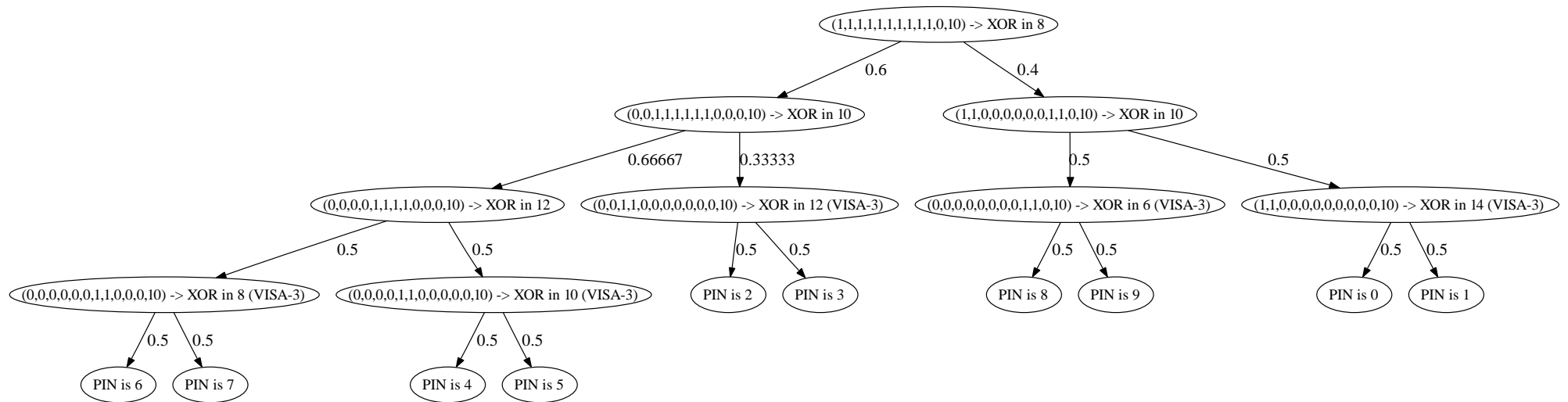
First 4 arguments are constrained PIN digits



Attack Trees



Optimised Attack

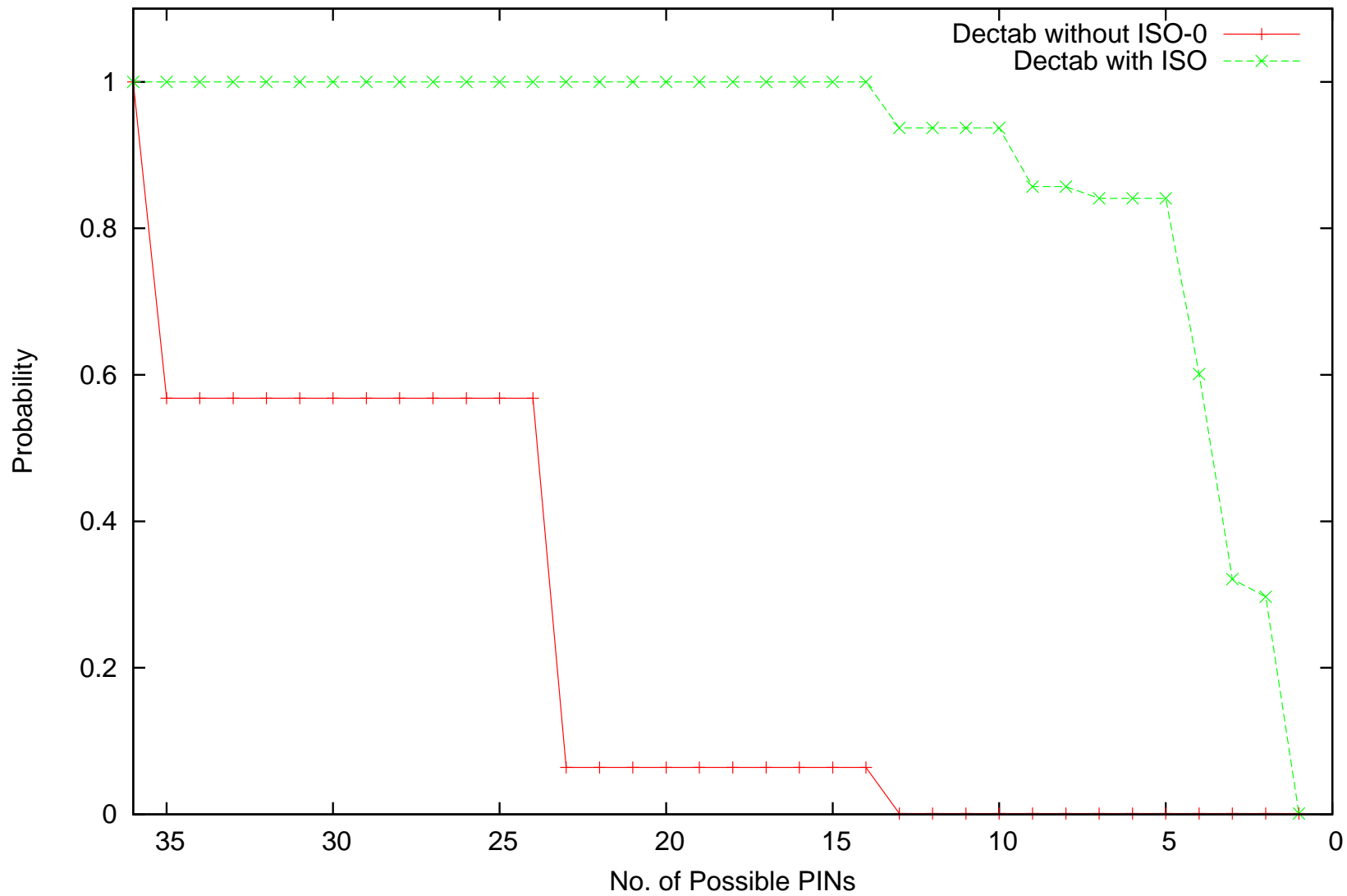


Results from Analysis (Generic API)

No.	Attack	$P(\text{determined})$	$E(\text{Steps})$
(1)	ISO-0 (extended)	1	13.6
(2)	Dectab	1	16.145
(3)	Dectab & ISO (restricted)	1	15.275

No.	Attack	$k = 400$	$k = 36$	$k = 24$	$k = 14$	$k = 1$
(4)	ISO-0 (restricted)	1	0	0	0	0
(5)	Dectab no offset	1	1	0.568	0.064	0.001
(6)	Dectab no offset & ISO-0 (restricted)	1	1	1	1	0.001

Performance of Dectab attack without offset



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.:

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