


# Smart Cards and Side-Channel Cryptanalysis

Ryan Junee



## Outline

- About Me
  - About Smart Cards
  - Side Channel Cryptanalysis
  - Part II – Case Study: DPA attack on DES
  - Future Work
- 



## About Me

- Ryan Junee BE (Hons I) BCom
- Research Engineer @ Sensory Networks
- Graduate of Sydney University
- Teach a variety of subjects at Sydney Uni
  - currently head tutor of *ELEC5610 - Computer and Network Security*

[ryan@juneer.org](mailto:ryan@juneer.org)

<http://ryan.juneer.org>



## About Me

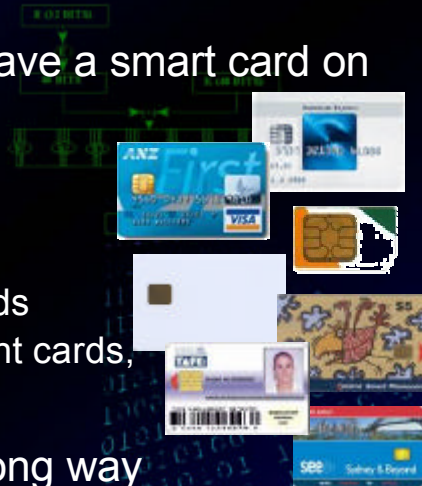
- 2002 Thesis: *"Power Analysis Attacks :: A Weakness in Cryptographic Smart Cards and Microprocessors"*
- Successfully recovered DES secret key using Differential Power Analysis (DPA)
- Featured on the front page of *Australian IT*





## About Smart Cards

- How many of you have a smart card on you?
  - Amex Blue
  - ANZ First VISA
  - Mobile SIM cards
  - Building access cards
  - Phone cards, student cards, travel cards, ...
- And Australia is a long way behind Europe and Asia!



## About Smart Cards

- Technically: cards containing embedded microchips that conform to ISO7816.
  - Memory cards
  - Microprocessor cards
  - Cryptographic cards
  - Java cards
- Often include tamper-resistance and attack countermeasures, but inadequate against a determined attacker.





## About Smart Cards

- Growing use in a wide range of industries worldwide:
  - SMARTICS – identity card for citizens of Hong Kong. Stores ID & 3<sup>rd</sup> party info.
  - Drivers licenses in the Philippines record name, address, fingerprint, photo, offences...
  - Transport ticketing in Washington (1/3 of WMATA Metrorail riders use SmarTrip cards)
  - Pay television, health care, ...



## About Smart Cards

- Recent headlines:
  - “NSW announces smart card fare system”
  - “First Gas Pumps Accept MasterCard® PayPass”
  - “Mexico Moves To Smart Tax Payment System”
  - “Terrorist attacks spark military smart cards”
  - “MasterCard Records 65 Percent Growth in Smart Card Issuance in Asia/Pacific”
- Has anyone considered the risks??



## About Smart Cards

- Smart cards are gaining popularity in applications that require high security and/or store sensitive information.
- Traditionally seen as secure and tamper resistant (especially compared to magnetic stripe cards).
- We are not there yet...



## Side Channel Crypto

- Traditional cryptographic model:

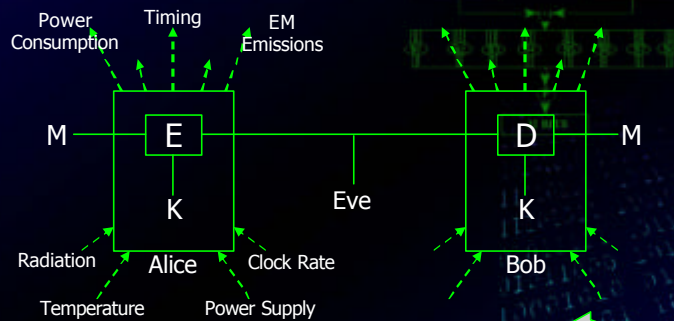






## Side Channel Crypto

- Traditional cryptographic model:



- Improved 'real world' model



## Side Channel Crypto

- Ever cracked a safe/combination lock?

- More Sophisticated Attacks:

- Timing Analysis – Kocher 1995
- Fault Analysis – Boneh, DeMillo, Lipton 1997
- Power Analysis – Kocher, Jaffe, Jun 1998
- EM Emissions – TEMPEST 1950s??
  - Agrawal, Archambeault, Rao, Rohtagi 2002





## Timing Attacks

- Cryptosystems can take different amounts of time to process different inputs.
  - Performance optimisations in software
  - Branching/conditional statements
  - Caching in RAM
  - Variable length instructions (multiply, divide)
- Simply take accurate timing measurements with various input data to deduce internal workings.



## Timing Attacks

- Simple example – Naive password checking function.
- Interesting paradox: As computers become faster and networks have less latency, timing measurements become more accurate!
- Future research: a timing attack on SSH exploiting keystroke timing statistics?



## Timing Attacks

- Countermeasures
  - Make all operations run in same amount of time
    - Can't design platform-independent algorithms
    - All operations take as long as slowest one
  - Add random delays
    - Can take more samples to remove randomness
  - Blind signature techniques
    - Algorithm specific



## Fault Analysis

- Single innocent faults can have large security implications.
- Faults can be induced.
- Simple example: bit controls ciphertext or plaintext output.
  - Flip bit with power surge, radiation, laser etc
- Engineering criteria (e.g. FIPS140-1) generally prevent such simple attacks.







## Fault Analysis

- Differential Fault Analysis
  - Biham, Shamir 1997
- Intrusive Fault Analysis
  - E.g. damaging registers in the last round of a DES operation can reveal S-box input and hence round key.



## Fault Analysis

- Countermeasures
  - Verify correctness of output before transmitting it to outside world
    - Can increase work by a factor of 2
    - Fault could also occur in verification
  - Make devices tamper resistant (strong shielding, detect supply voltages and clock speeds)
    - Costly, increase device footprint





## Power Analysis

- Logic gates made from transistors – draw current when switching states
- Power consumed depends on:
  - opcode, operand data, contents of registers, buses and memory, previous instructions (pipeline)
- Measure current by placing a resistor in series with supply or ground pin



## Power Analysis

- Simple Power Analysis
  - Can observe macro characteristics of underlying algorithm (loops, conditionals etc)
- Differential Power Analysis
  - Use statistical techniques to reveal much smaller power variations
- Inferential Power Analysis
  - Profile hardware. Subsequent attacks require as little as one trace!
- More detail on SPA/DPA in Part II



## Power Analysis

- Countermeasures
  - Don't use secret values in conditionals/loops
    - May mean code has sub-optimal performance
  - Ensure little variation in power consumption between instructions
    - Requires consideration of low level logic design
  - More discussed at the end



## EM Emissions

- Large body of classified literature. Recently being realised in public domain research
- Direct emanations caused by current flows in circuit
- Unintentional emanations caused by electrical/electromagnetic coupling between components in close proximity



## EM Emissions

- 2002 paper from IBM shows different signals present in different parts of spectrum
- Some can be detected with antennas from a distance. Best results if chip is decapsulated from packaging
- Contain more information than power leakage, resistant to countermeasures.
- Watch this space!



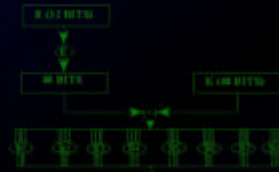
## EM Emissions

- Countermeasures
  - Redesign circuits to prevent unintentional emissions
    - Costly
  - Shielding
    - Costly, increase device footprint
  - Introduce EM noise
    - Can be averaged out





## Part II



### Case Study: DPA attack on DES

1101010101 1101010101  
1101010101 1101010101  
0101010101 0101010101  
0101010101 0101010101  
1001010101 1001010101  
0101010101 1001010101  
1101010101 1101010101  
1001010101 1101010101  
1011110101 1011110101  
001010101 101010101  
1011110101 1101010101

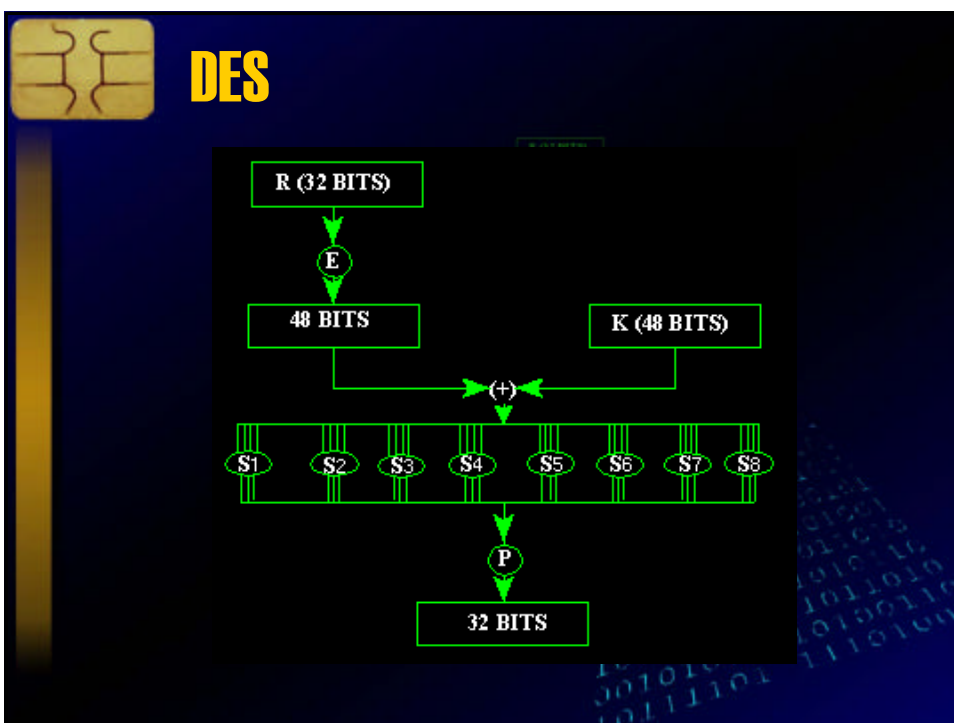
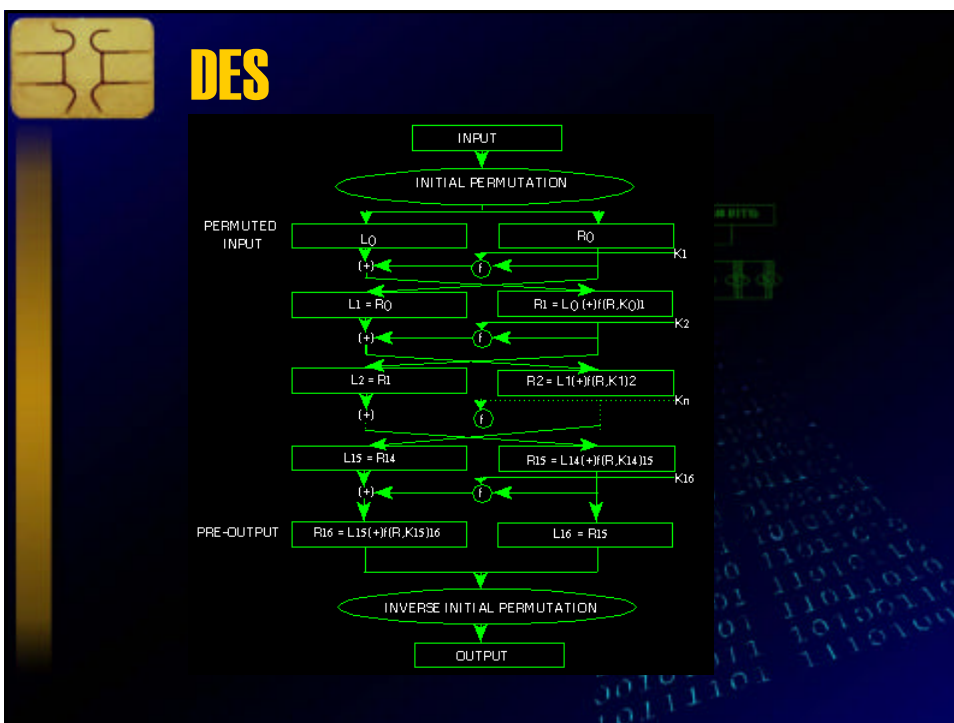


## DES

- Data Encryption Standard (FIPS46-2)
- Variant (3DES) used worldwide in financial networks etc.
- Superseded by AES but still widely used
- 64-bit plaintext input + 56-bit key => 64-bit ciphertext output
- 16-round Feistel network

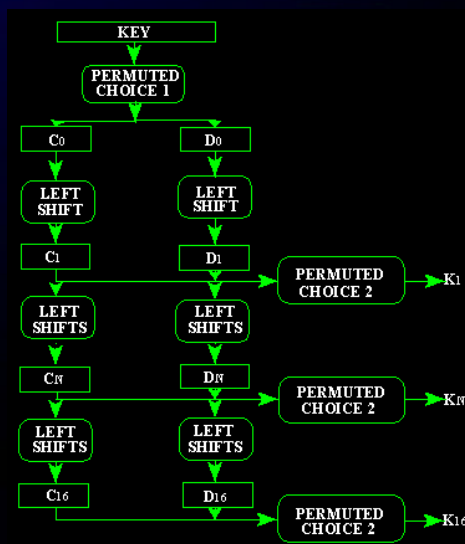
1101010101 1101010101  
0101010101 0101010101  
0101010101 0101010101  
1001010101 1001010101  
0101010101 1001010101  
1101010101 1101010101  
1001010101 1101010101  
1011110101 1011110101  
001010101 101010101  
1011110101 1101010101







# DES



# Attacks on DES

Attack	Computation	Storage
Exhaustive Search	$2^{55}$	Negligible
Exhaustive Precomputation	1	$2^{56}$ texts
Differential Cryptanalysis (KPA)	$2^{55}$	$2^{55}$ texts
Differential Cryptanalysis (CPA)	$2^{47}$	$2^{47}$ texts
Linear Cryptanalysis	$2^{50}$	$2^{38}$ texts
Linear cryptanalysis	$2^{43}$	$2^{43}$ texts
DPA	$2^{19}$	175 traces
DPA	1	325 traces

- I'll show you how...

## Required Equipment

PIC running DES encryptions

High Precision CRO

Computer controls CRO and stores acquired waveforms

- Found in most university engineering labs
- Purchase for under AUD\$10,000

## Simple Power Analysis

- Procedure:
  - Record power traces of DES operation
  - Inspect traces visually

Trigger signal on I/O port

Eight loops in the initial permutation are clearly visible

1 2 3 4 5 6 7 8

Initial Permutation

DES Round 1

DES Round 2

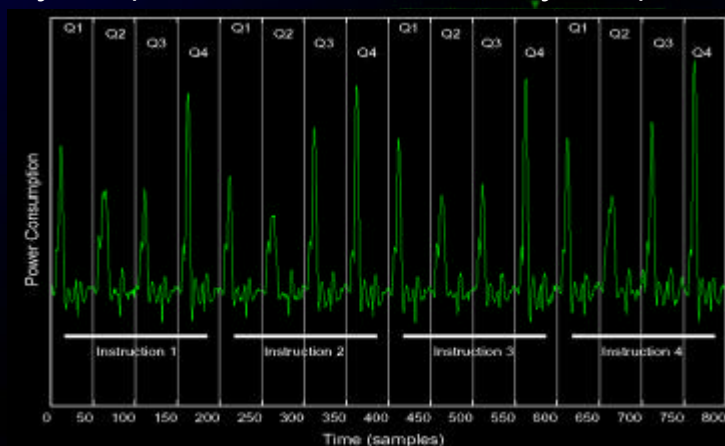
DES Round 3

Instruction	Address	Value
movlw	0x00	0x00
movlw	0x01	0x01
movlw	0x02	0x02
movlw	0x03	0x03
movlw	0x04	0x04
movlw	0x05	0x05
movlw	0x06	0x06
movlw	0x07	0x07
movlw	0x08	0x08
movlw	0x09	0x09
movlw	0x0A	0x0A
movlw	0x0B	0x0B
movlw	0x0C	0x0C
movlw	0x0D	0x0D
movlw	0x0E	0x0E
movlw	0x0F	0x0F



## Simple Power Analysis

- Can see characteristics of each instruction cycle (which takes 4 clock cycles)



## Differential Power Analysis

- Perform approx 400 DES encryptions with arbitrary plaintext. Record the resulting power trace and ciphertext output.
- Brute force a particular 6-bit subkey from DES round 16
  - For each guess, calculate the value of a particular bit in L15 corresponding to the subkey (there are 4 such bits)
  - Partition the traces into two sets, one where the 'select bit' is 0, one where it is 1.



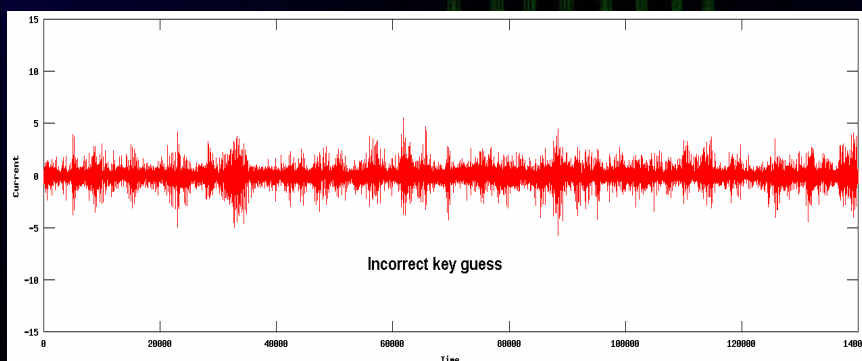
## Differential Power Analysis

- Calculate the average power trace for each set, then subtract to form differential trace.
- Assume correlation between power consumed and value of select bit
  - (it is manipulated somewhere in the power trace)
- If key guess was correct => peaks in the differential trace
- If not we have made a random partition => differential trace should approach zero.



## Differential Power Analysis

- The evidence:

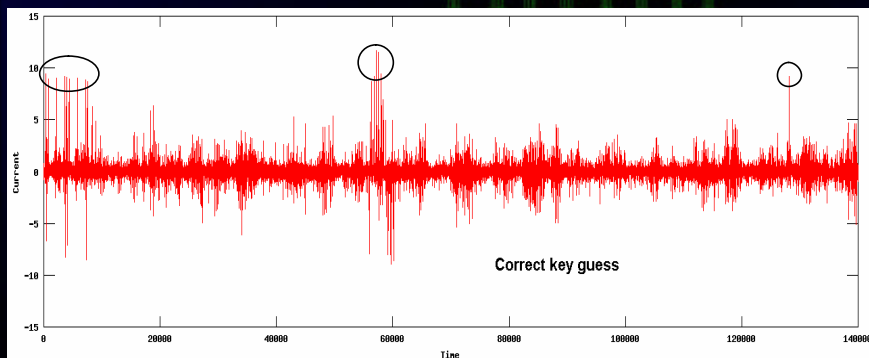






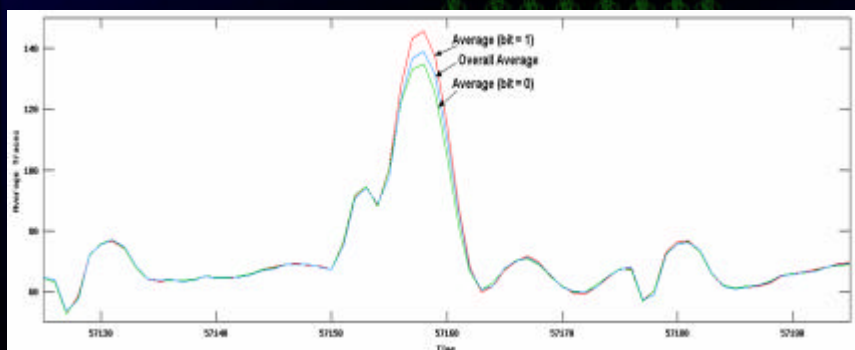
## Differential Power Analysis

- The evidence:



## Differential Power Analysis

- The accuracy is uncanny:





## Differential Power Analysis

- The low down:
  - 400 traces acquired (approx. 22 hours)
  - 1.6 hours computation (Celeron 400MHz)
  - DES key cracked!
  - Brute force key search on same computer would take *57 thousand years*!
- Code is available on my web site (you will need access to a CRO etc)

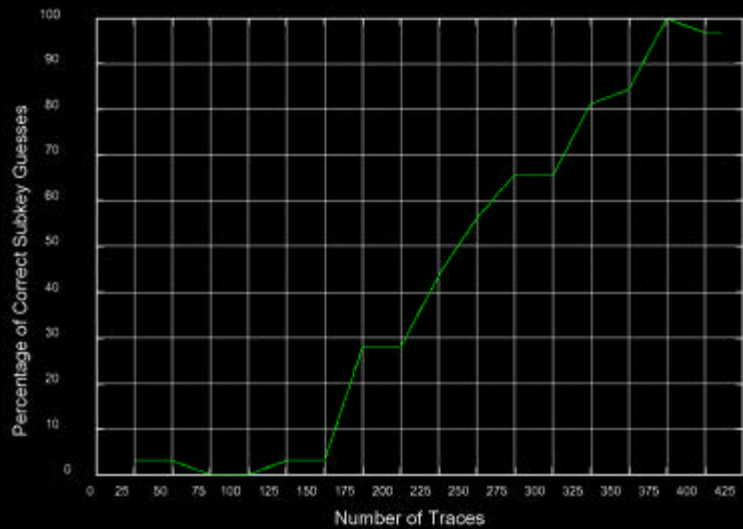


## Improving the Attack

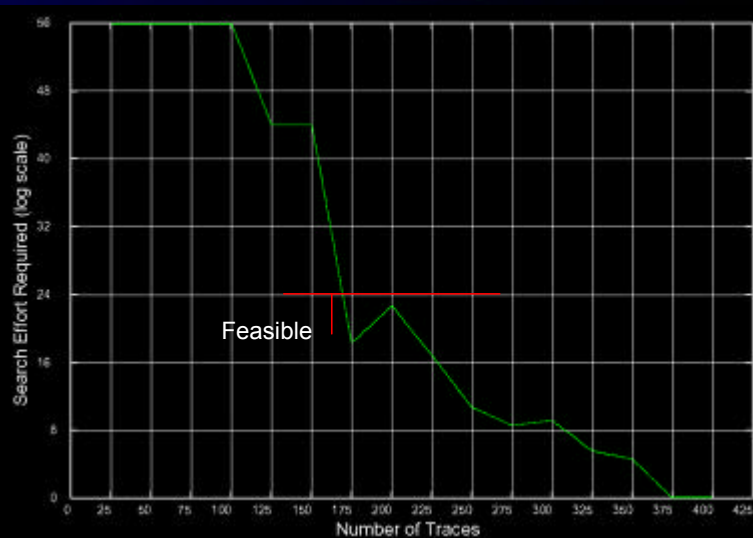
- Improvement 1 – Reduce acquisition time
  - Bottleneck is 38400 baud serial transfer
  - Use ethernet or GPIB
  - Lower sampling rate (currently 50/cycle)
- Improvement 2 – Reduce computation time
  - Use faster CPU
  - Parallel computation
- Improvement 3 – Reduce number of traces required



## Improving the Attack



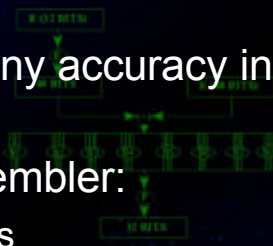
## Improving the Attack





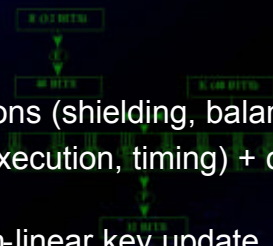
## Future work

- As observed, uncanny accuracy in power traces
- Power trace disassembler:
  - Profile all instructions
  - Use statistical methods or AI to disassemble the execution trace of an algorithm by observing power consumption
  - Reverse engineering tool?



## Power Analysis Countermeasures

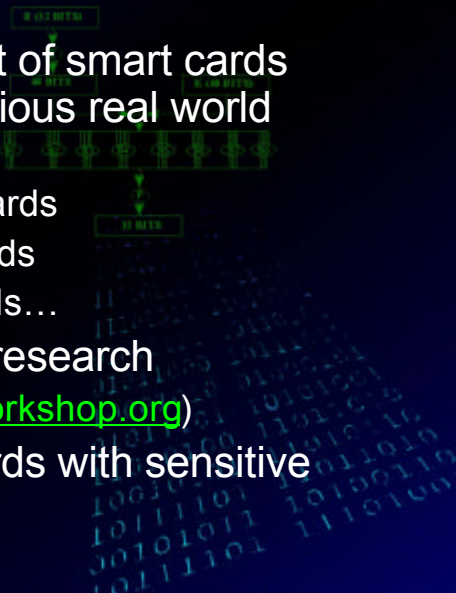
- Countermeasures
  - Reducing power variations (shielding, balancing)
  - Randomness (power, execution, timing) + counters on card
  - Algorithm redesign (non-linear key update, blinding)
  - Hardware redesign (decouple power supply, gate-level design)
- 2002: Kocher released automated DPA cracker. Sell to approved researchers/manufacturers
- Suspect not many cards employ adequate countermeasures





## The Future

- Massive deployment of smart cards means there are serious real world security implications
  - Stored value cash cards
  - Personal identity cards
  - Building access cards...
- Very active area of research
  - CHES ([www.chesworkshop.org](http://www.chesworkshop.org))
- Don't trust smart cards with sensitive information just yet!



## The Future

“The fundamental flaw in the smart card paradigm is that the owner of the card and the owner of the secrets on the card aren't the same” - B. Schneier

