A Low Cost Hardware Birthday Attack on DES

Mike Bond, Richard Clayton
University of Cambridge
Computer Laboratory
5th June 2001

Predicting Brute Force of DES

- Diffie/Hellman 1977 $20M for 1 key/day
- Jueneman 1980 : by 1985 $10M for 2 secs
- Hoornaert 1984 : $1M for 4 weeks
- Desmedt 1987 : $3M for 4 weeks
  (as Hoornaert but 1M keys in parallel)
- Wiener 1993 : <$1M for 1 key/3 hours

RSA Challenges

- June 97 : 96 days (25% of space)

  DESCHALL – peak day: 2^{32} keys/sec
- February 98 : 41 days (90% of space)

  Distributed Net – peak day: 2^{36} keys/sec
- July 98: 56 hours (27% of space)

  EFF “Deep Crack” – $2^{36.5}$ keys/sec
- January 99 : 22 hours (25% of space)

  Distributed Net + EFF – reached $2^{37.8}$ keys/sec

The EFF Machine

- 1 unit tests 1 key in 16 clocks (40 MHz)
- 24 units/ASIC
- 64 ASICs/board
- 12 boards/chassis, 2 chassis = 1 machine
- Looking for “known plaintext”
- Full 2^{56} search takes 9 days
- $210,000 – of which $80,000 was chips

Later Machines

- Transmogrifier 2a (Univ. Toronto) 1999
  - 32 * Altera 10K100 FPGAs + glue!
  - 25MHz
  - $2^{29.6}$ keys/sec : ie 2.85 years/key
  - $30K cost (estimated – chips were free!)
  - For $210K they estimate 8X EFF speed
- Not many more actually built !

The Magnificent Seven

Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson & Wiener (Jan 1996)

- Surveyed software & FPGA solutions
  - 40 bit keys – one week in software
  - $400 FPGA – 5 hours / 40 bit key = $0.08/key
  - Assumed 60MHz pipeline in the FPGA
- Recommended 90 bits as safe for 20 years even when targeted by major governments

Our Kit-based Machine

- $1000 Excalibur kit (Altera 20K200)
  - But cost ~ $100 for just the chip ?
- 16MHz pipeline (half speed at present)
- 2^{24} keys/second
  - 40 bit problems = 18 hours
  - 56 bit DES = 135 years ($1M = 5..50 days)
- However.. it does 64K keys in parallel

The Meet in the Middle Attack

- Common sense statistics
- Attack multiple keys in parallel
- Need the same plaintext under each key
- Encrypt this plaintext to get a ‘test vector’
- Typical case: A 2^{56} search for one key becomes a 2^{40} search for 2^{16} keys

What to Attack : An Example

- PRISM Security Module used to store keys in electricity meter credit dispenser
- Discovering a vending key allows unlimited token manufacture
- Vending keys stored in a hierarchy, with manually loaded master key at top

The PRISM Module

Master Key Entry

- Master key is a two-key triple DES key
- Each half loaded in three parts, which are XORed together
- Three “trusted” security officers each load one part of each key
- Check digits returned after each load

$$\texttt{Check Digits} = \{\ 0\ \}_K$$

Example Key Entry

Security Officer 1

SM?IK 86 08F8E3983E3BDF26

SM!IK 00 916BA78B3F290101

SM?IK 87 E92F67BFEADF91D9

SM!IK 00 0D7604EBA10AC7F3

Security Officer 2 (... n)

SM?AK 86 FD29DA10029726DC

SM!AK 00 EDB2812D704CDC34

SM?AK 87 48CCA975F4B2C8A5

SM!AK 00 0B52ED2705DDF0E4

Harvesting Test Vectors

- Attacker continues to XOR in chosen bit patterns with each key
- Attacker creates 2^{16} variants of each half

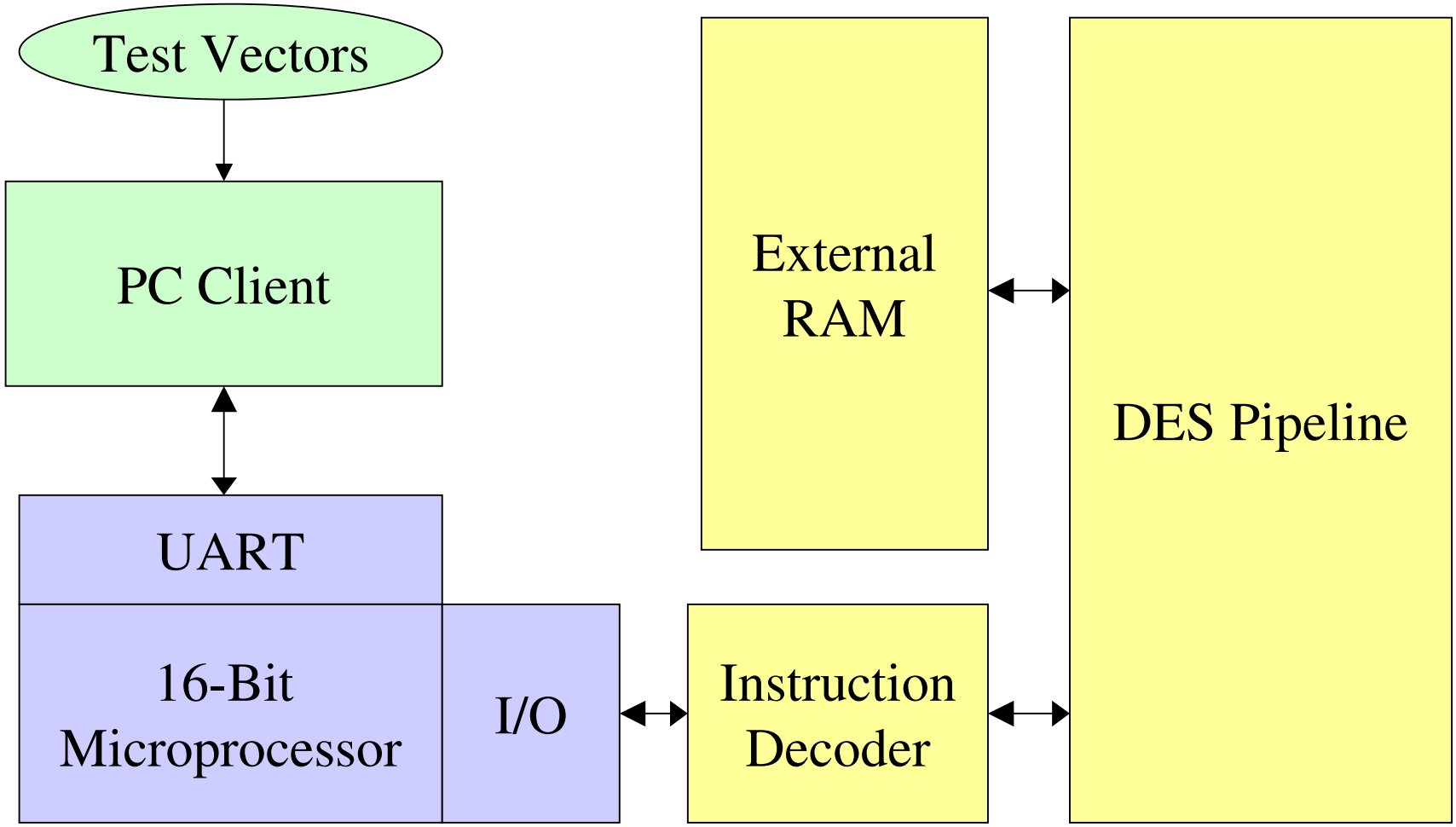
- Result : 2 x ½ MB file of test vectors

Example Algorithm

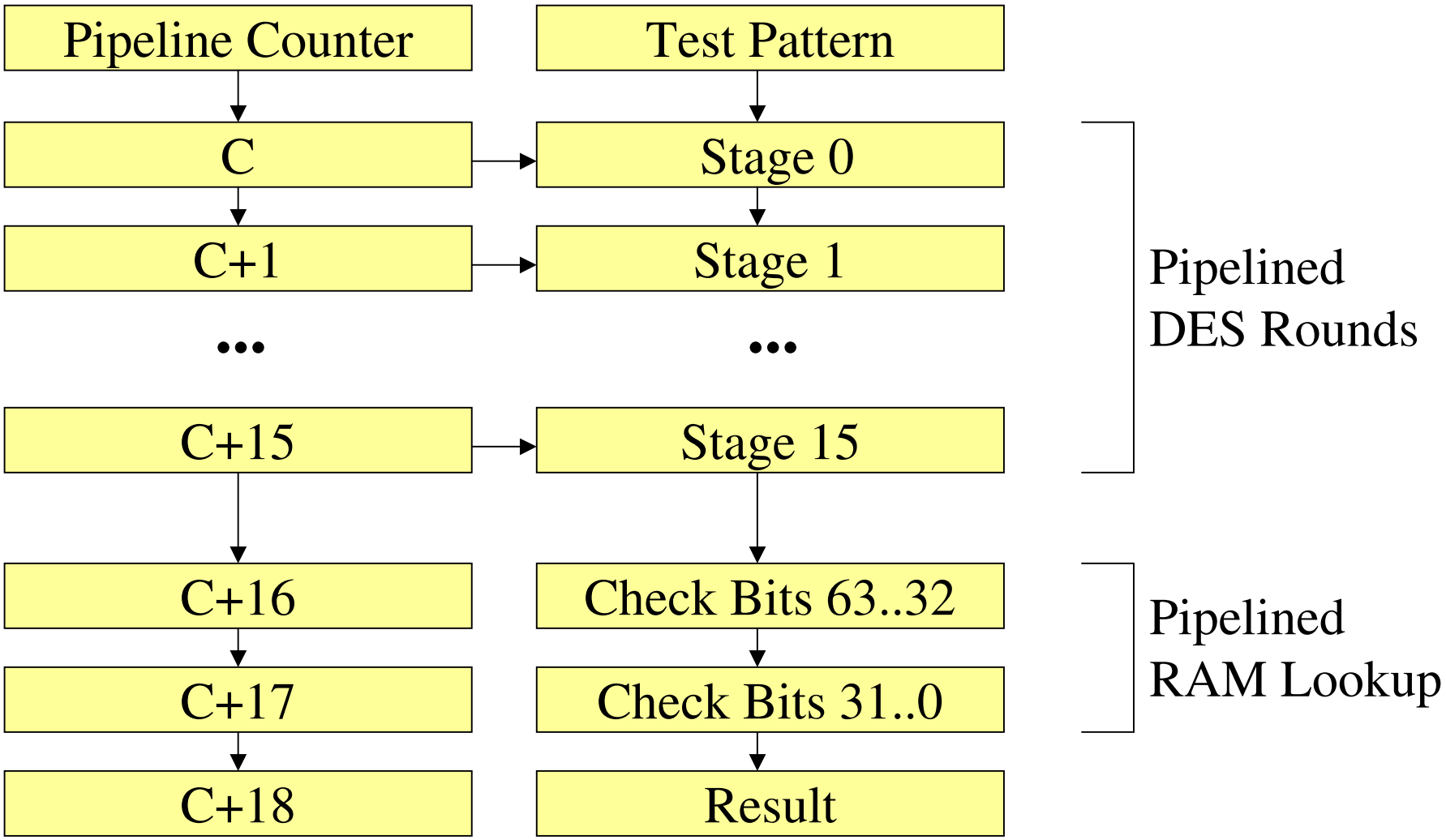
```
For I = 0000000000000001
    to  000000000001FFFF
    {
    SM?AK 87 I xor (I-1)
    SM!AK 00 (result)

    record the pair ( I , result )
    }
```

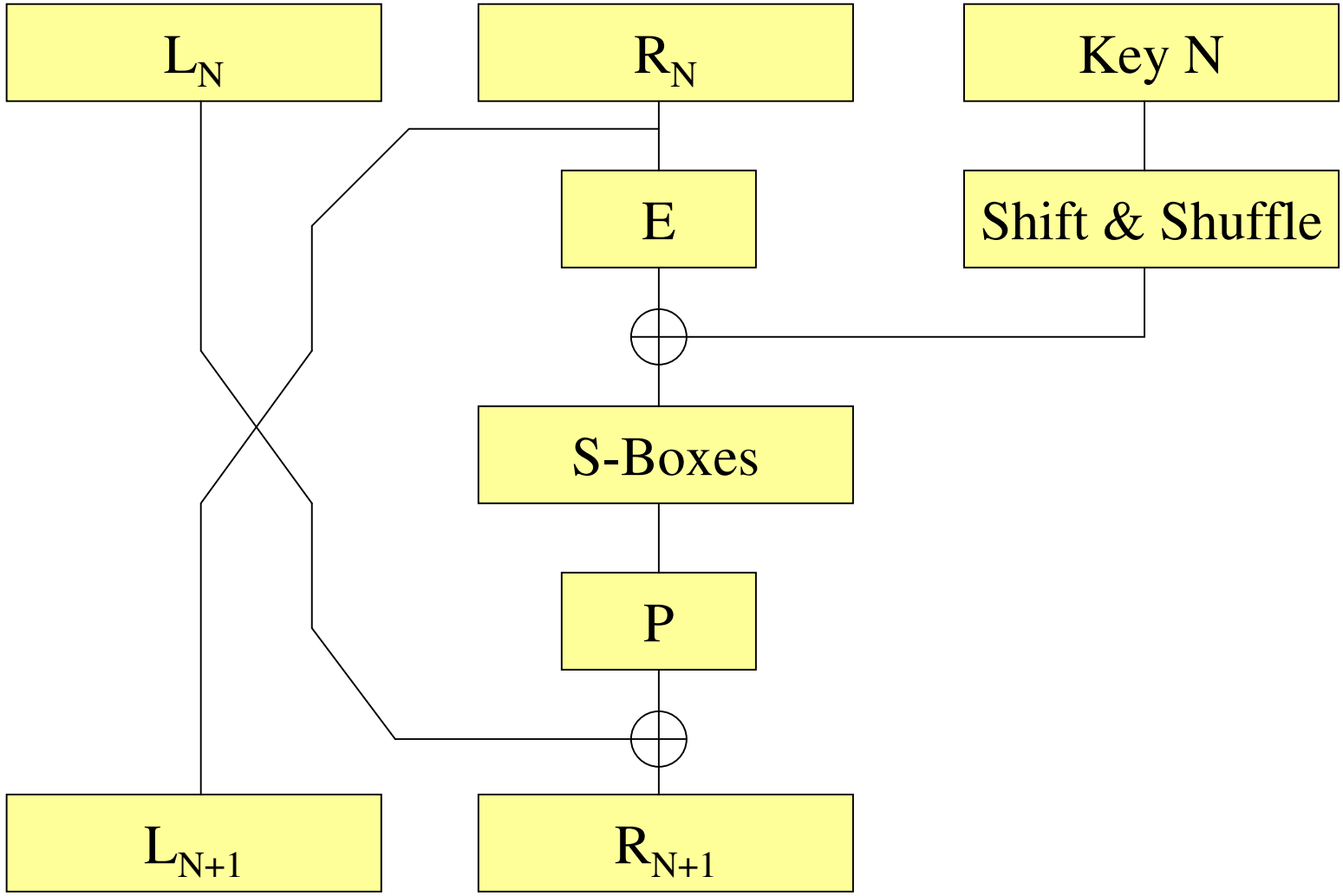
The Big Picture



The DES Engine



A DES Pipeline Stage



Why Hardware?

- Hardware DES implementation is ~25 times faster than the best software implementations
- Software attack on PRISM took 3 ½ days to search 60% of 2^{40} key space
- Used 6 PCs = roughly £4500
- 64 bit key spaces come within range
- Other attacks on cryptoprocessors are active, so would be noticed well within a week

Make Your Own!

http://buy.altera.com/ecommerce/dkc.html

Look out for info at...

http://www.cl.cam.ac.uk/~rnc1/

http://www.cl.cam.ac.uk/~mkb23/research.html