Durham University

A fundamental evaluation of 80bit keys employed by hardware oriented stream ciphers

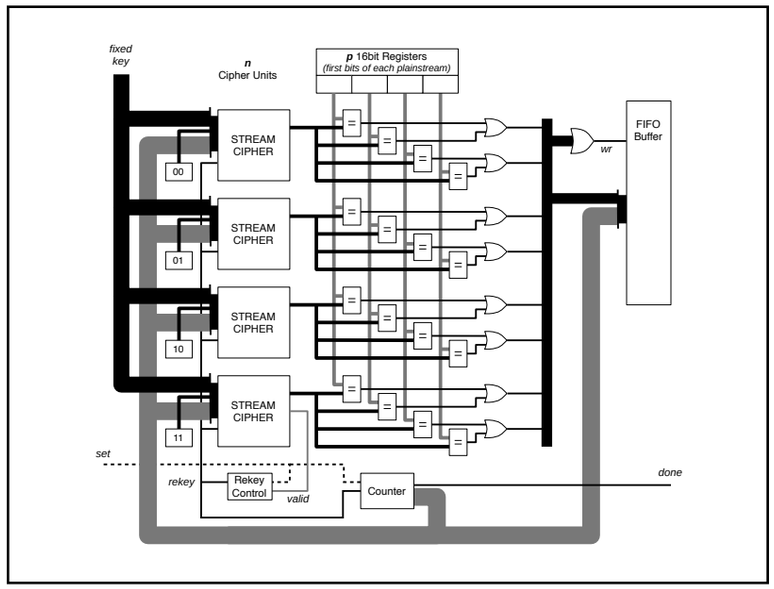
Iain Devlin

Centre for Electronic Systems, Durham University

SHARCS 2006

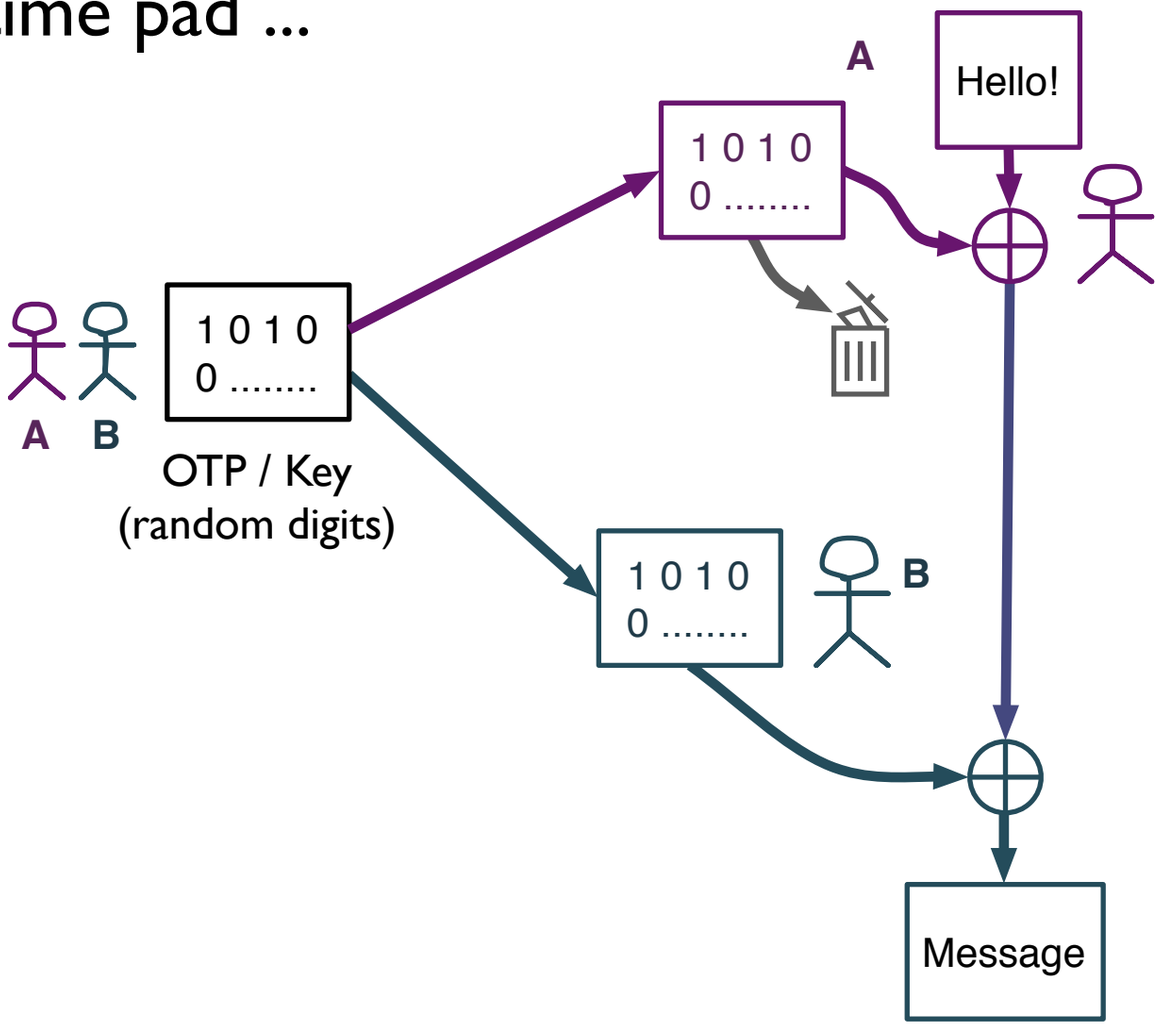
Outline of Presentation

- Background
- Design considerations
- System design
- Economics



What is a Stream Cipher?

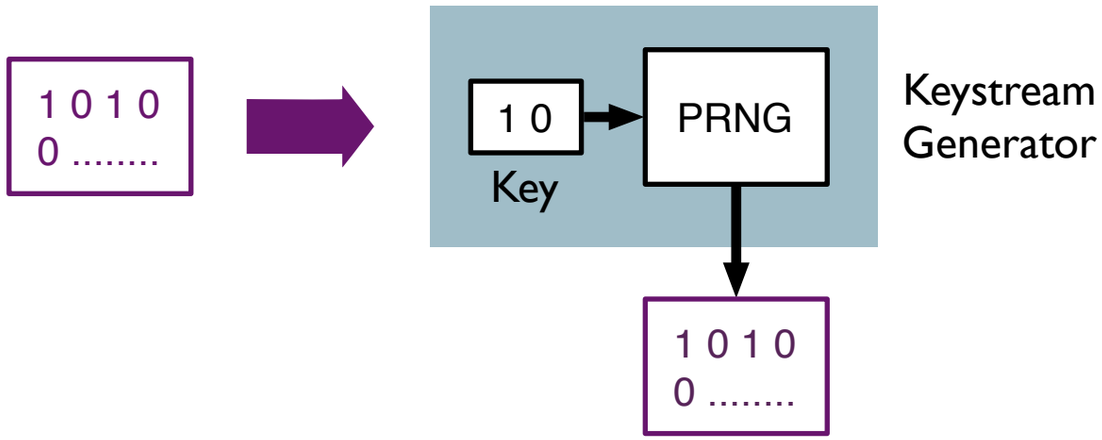
- The one time pad ...



What is a Stream Cipher?

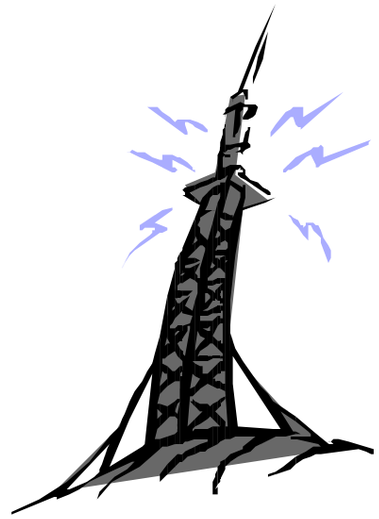
- Awkward to transmit key
  - material must equal message length

- Swap pad for *key* + *pseudo random number generator*
- A Stream Cipher!



Stream Ciphers

- Widely used ...
  - RC4 (WEP)
  - A5 (GSM)
  - E0 (Bluetooth)
- **But** algorithms keep getting broken ...
- ECRYPT eStream - identify some new ones!



eStream

- Call for Primitives in 2004
- Profile I
  - Software applications
  - 128bit keys
- Profile II
  - Hardware applications
  - Resource efficient
  - 80bit keys - trade some security for key length

www.ecrypt.eu.org/stream/

80bit Keys mean what?

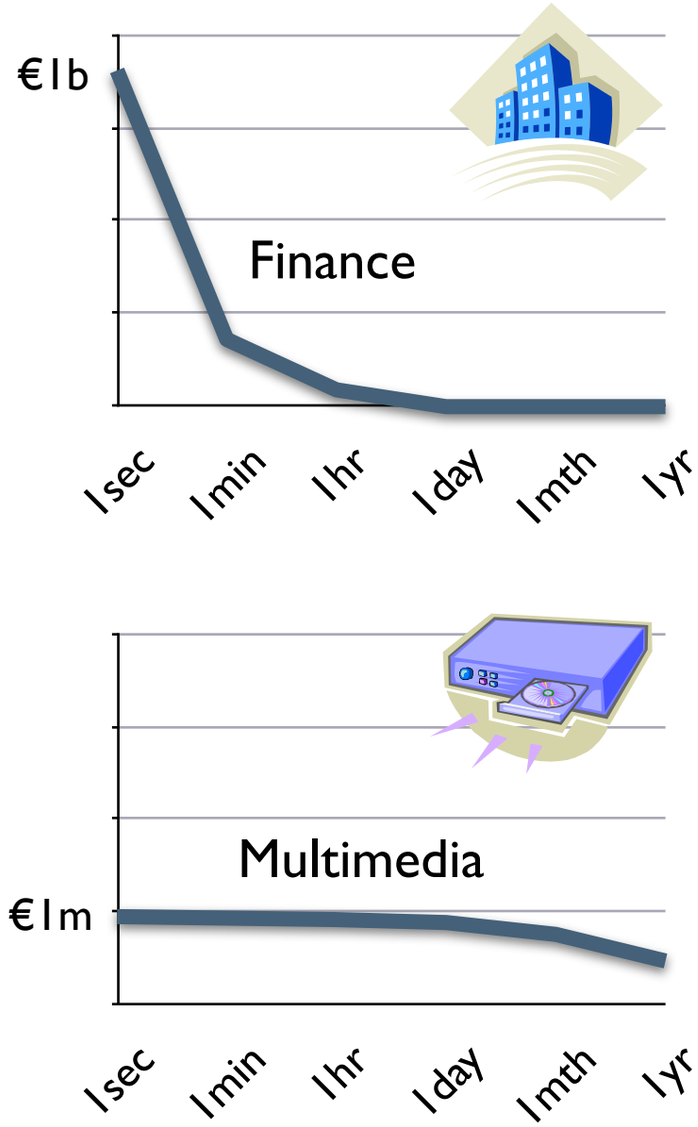
- ECRYPT (Keysizes 2005) deem length suitable for ...

"Very short-term protection against agencies,
long-term protection against small organizations"

- What is the economic value of the protection provided?

Adversary Valuation of Data

- Valuation determines whether data can safely sent by user
- Factors affecting attack value
  - usefulness ...
  - cost of retrieving data
    - Use Plan X
    - Use a key search machine
- Must evaluate all retrieval methods

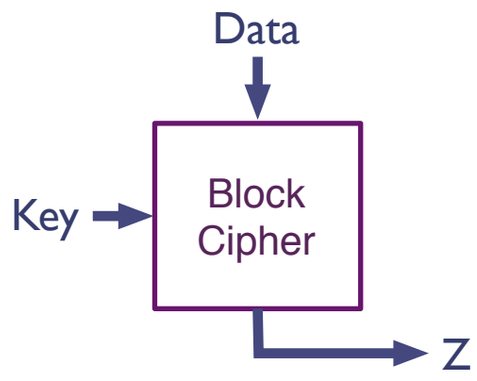


How much would it cost to build a stream cipher key search machine?

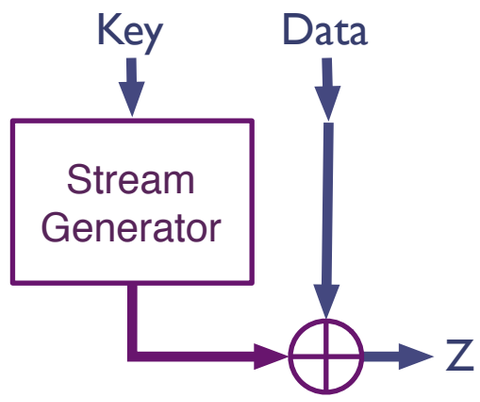
Brute Force Key Search

- Search every key
- Simple
  - Understanding Brute Force (Bernstein 2005)
  - Efficient implementation
    - May be cheaper than many algorithmic attacks!
- Block cipher brute force key search
  - EFF DES cracker (1998)
  - Quisquater (SHARCS 05)
- What about modern stream ciphers?

Difference Between Block and Stream



Small **or** Fast



Small **and** Fast

- No need to process data until output
- Implications from block cipher key search not applicable
  - Is a 128bit block cipher key ≡ 130bit stream key??

Xilinx Spartan III Comparison

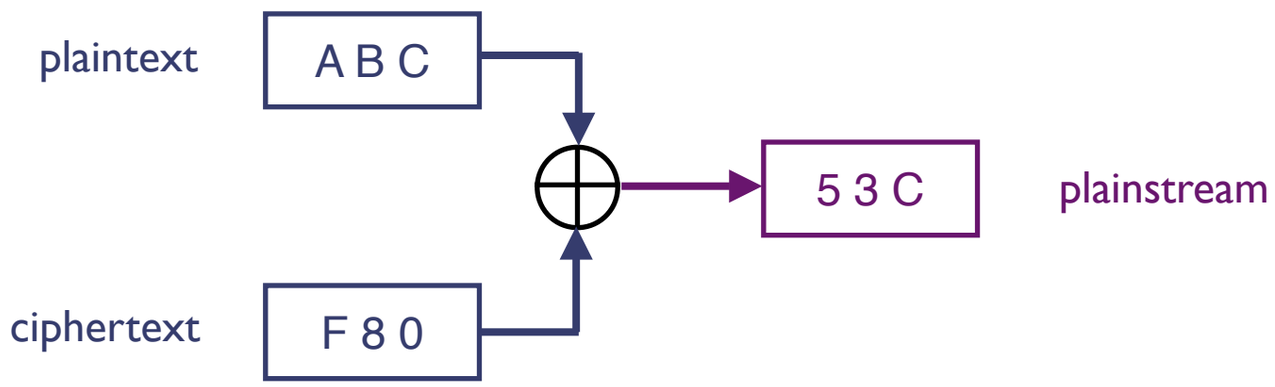
- DES - {*56bit*}
  - 11.5Gbps, 3k slices (UCL Crypto SHARCS 05)
- AES - {*128bit*}
  - Small - 208Mbps, 163 slices (Rouvroy ITCC 04)
  - Big - 25Gbps, 17k slices (Good CHES 05)
- Trivium - {*80bit*}
  - Small - 102Mbps, 40 slices (Good SASC 06)
  - Big - 6.5Gbps, ~

Stream Cipher Brute Force

- Considerations
  - mixing of key and initialisation vector (IV) material
  - throughput: production of keystream
- Initialisation dominates search time
  - produce 1 bit of keystream and 50% of searches can immediately be stopped.
  - i.e. looking for 10010... but keystream is 0.....

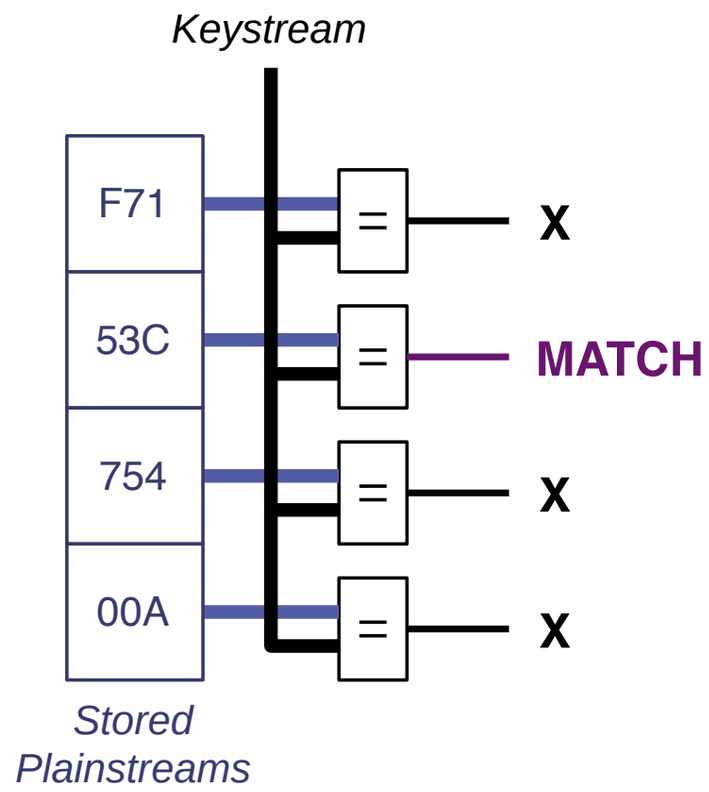
Plainstream

" A keystream derived from knowledge of a plaintext-ciphertext pair. "



Simultaneous Checking of Plainstreams

- Keystream independent of data
- Check multiple plainstreams with each keystream generated

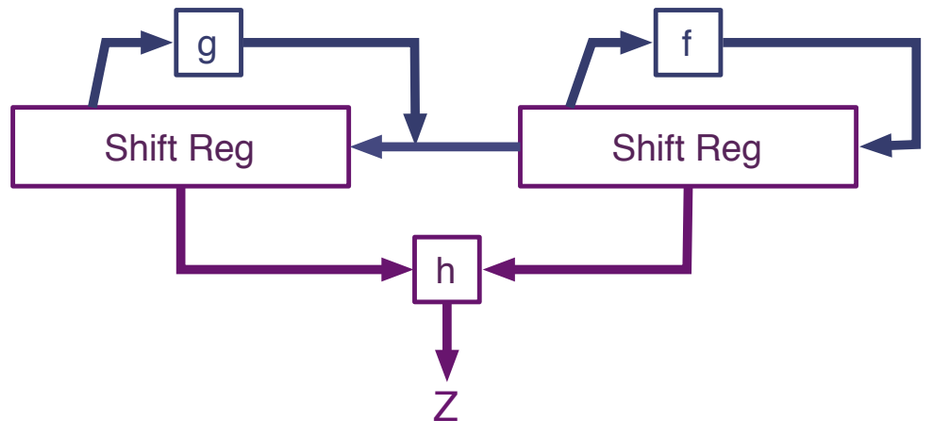


Advantage of Multiple Plainstreams

- 4 plainstreams = 4x chance of match
  - $4 = 2^2$ therefore 2 bits less search space
- Significant improvement in search time for small memory cost
- Time-memory-data trade-off variation
- Assume a small number of plainstreams relating to some known IV available to attacker.
  - file format header
  - counter used for IV

Cipher Choice

- eSTREAM - 34 proposals
  - 8 use 80bit keys
  - Two stand out as fast and efficient in hardware
    - Trivium (De Cannière)
    - Grain (Martin Hell)
- Grain keystream generator
  - Slightly smaller
  - Shorter initialisation
    - 10cycles vs 18cycles



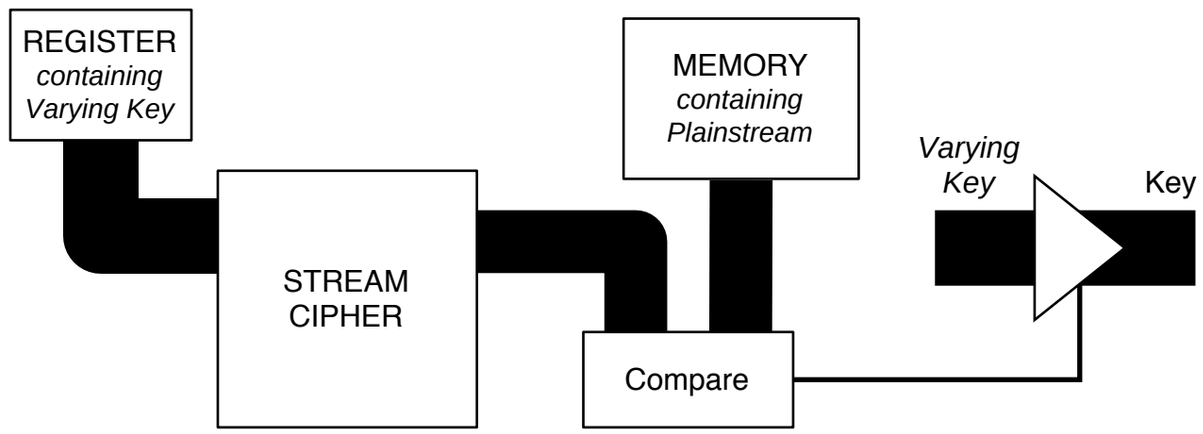
Platform Choice

- ASIC *(application specific integrated circuit)*
  - system design in its rawest form
  - maximum performance
  - high cost unless high volume

- FPGA *(field programmable gate array)*
  - extra layer of design abstraction
  - increasing popularity = falling price
  - no overhead costs
  - covert purchasing

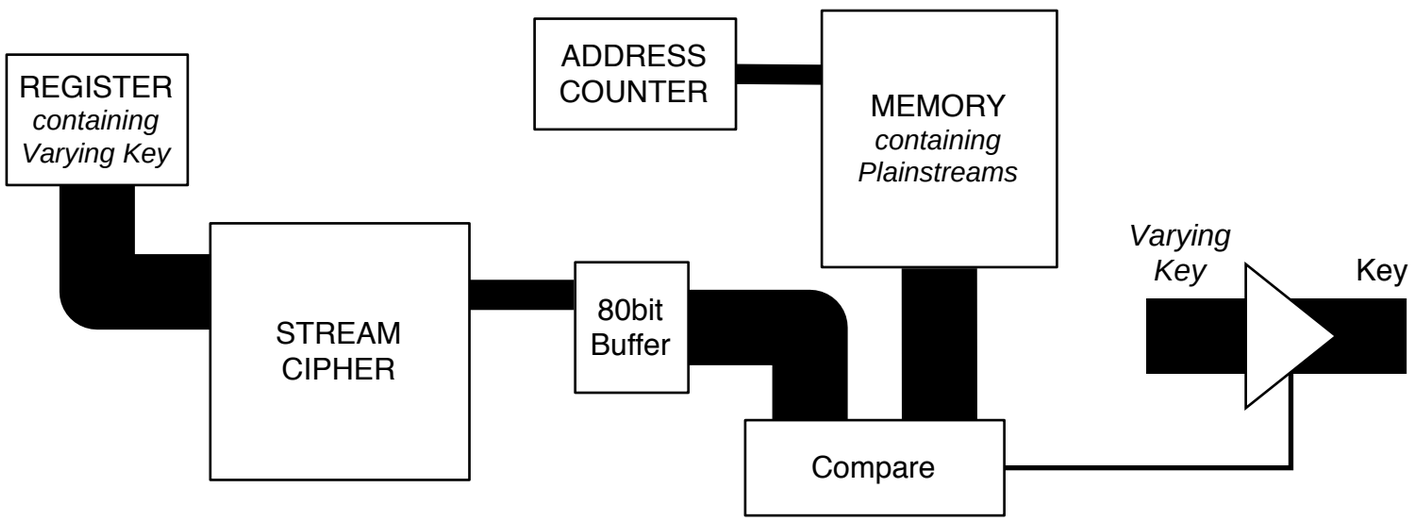
How do you design an efficient stream cipher brute force key search system?

Start Simple



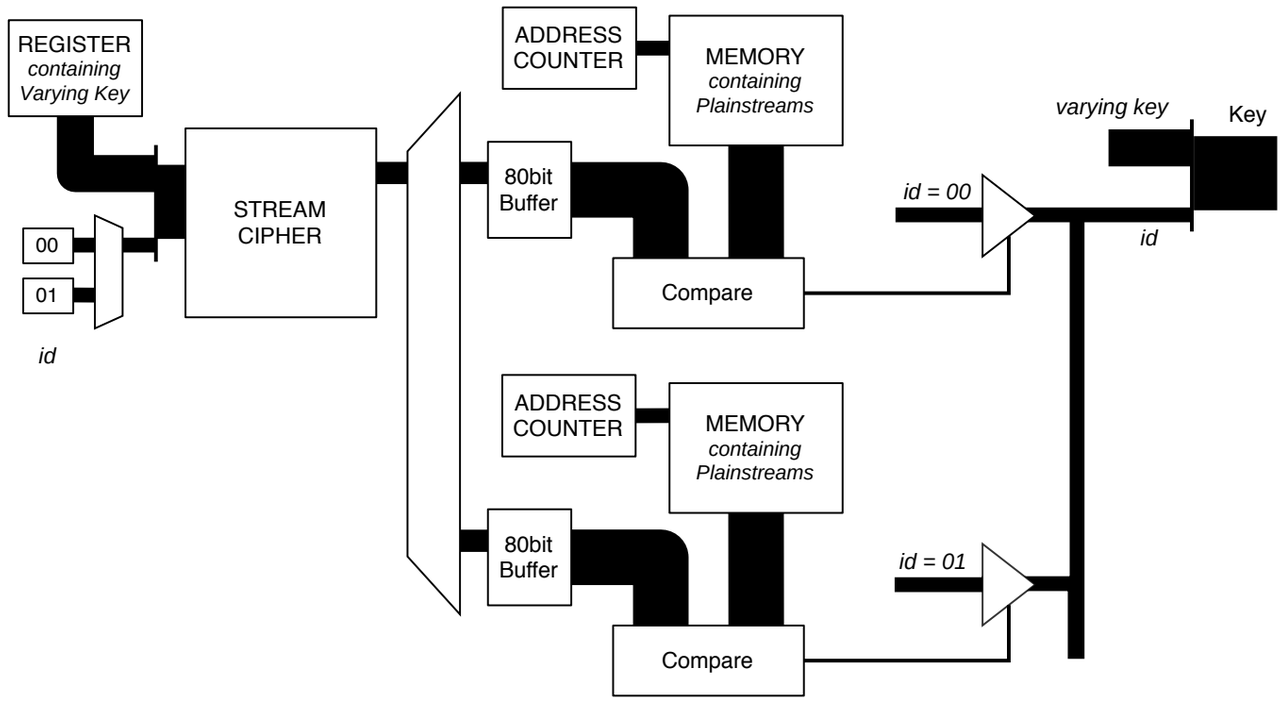
- Simplest brute force search system
  - cipher takes Key & fixed IV
  - compare keystream to stored plainstreams
- 80bit key so check 80bits of keystream
  - want reliable comparison

Increase Plainstreams



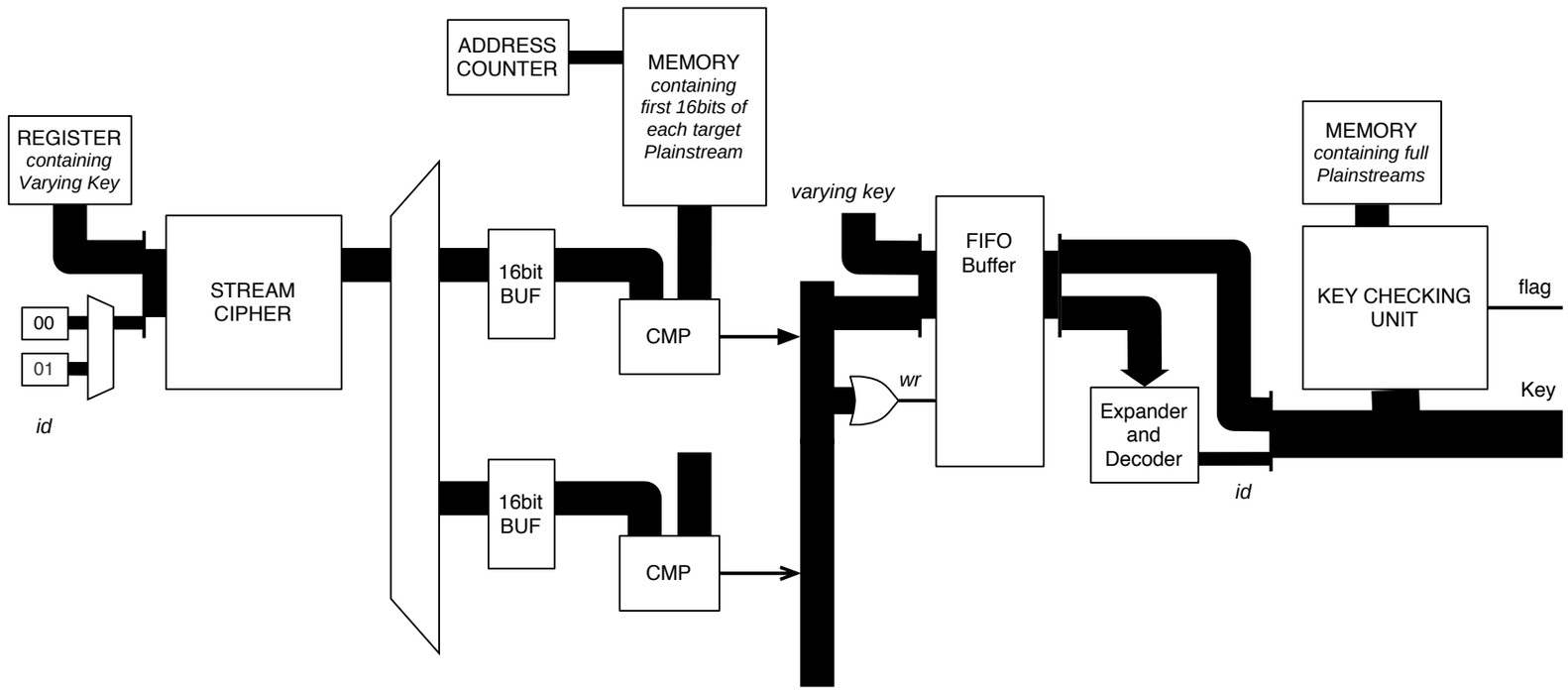
- Store keystream in buffer
- Check plainstreams in-turn while reinitialising

Increase Comparisons



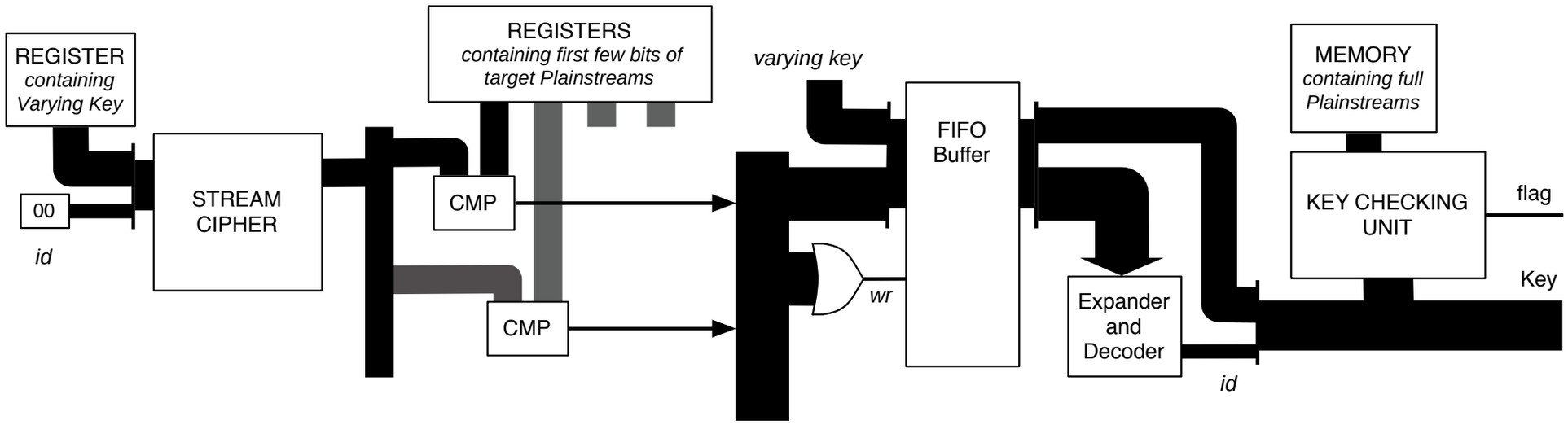
- Number of plainstreams large
  - memory compare >> cipher initialisation
  - add extra comparison units & use identifier

Split Comparison



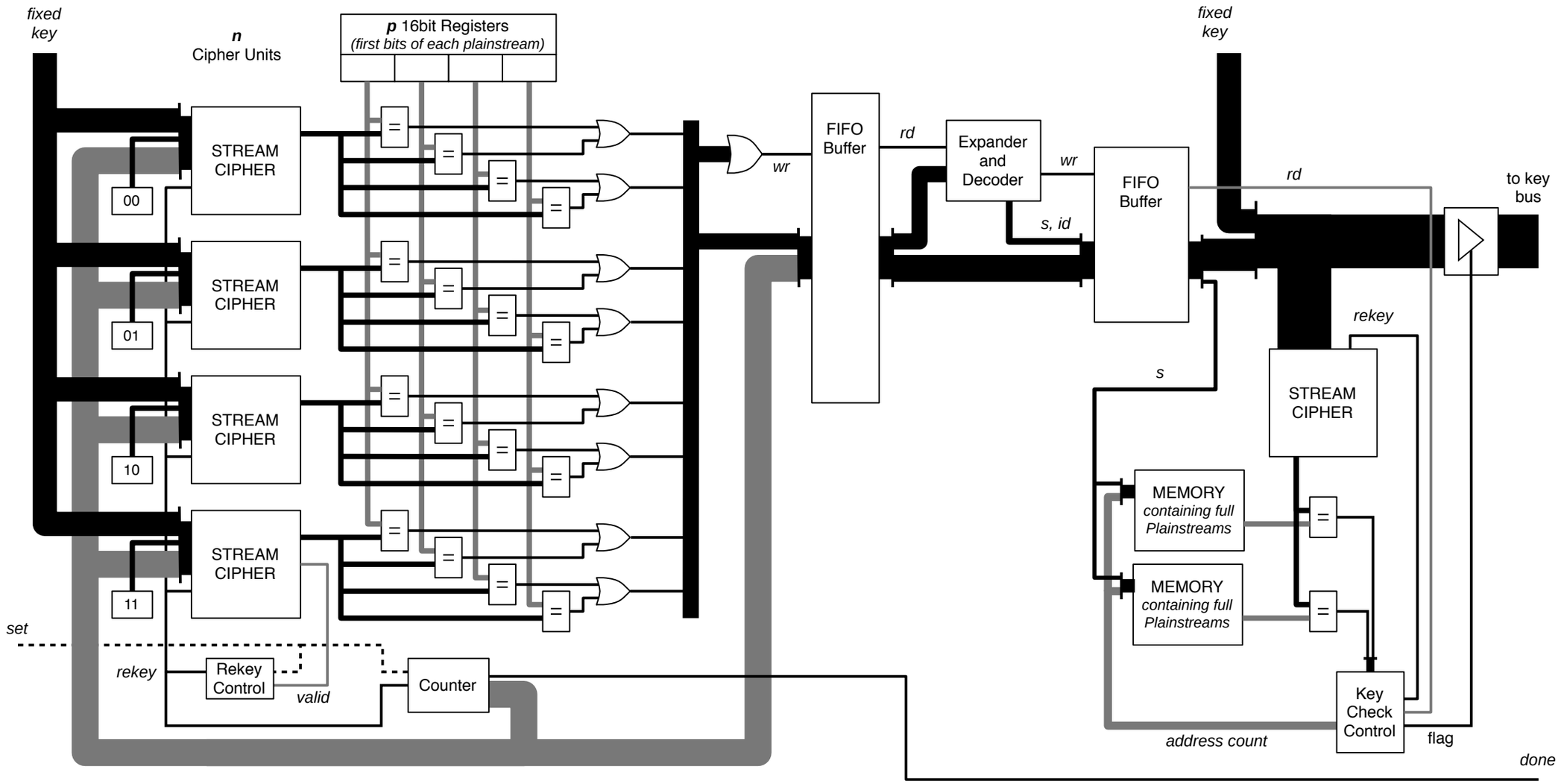
- Only few bits required to discount a key
  - reduce memory to store 16bits
  - add back-end to do reliable comparison on remaining keys

Add Parallelism



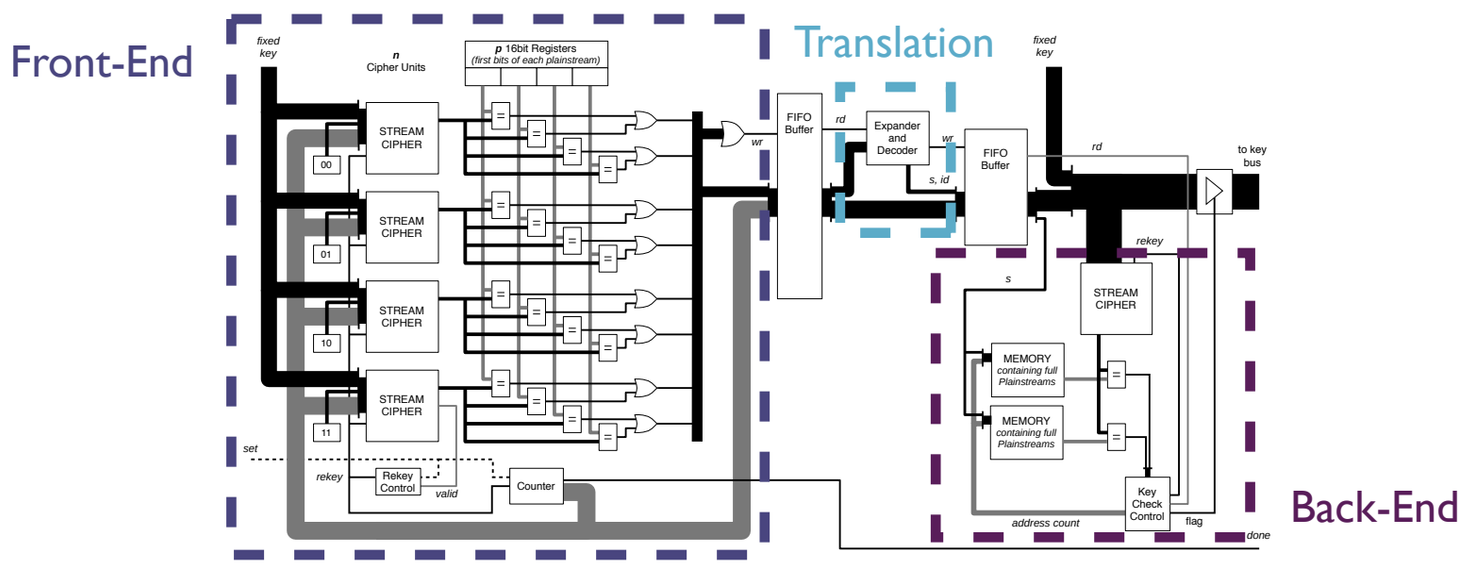
- Check all plainstreams simultaneously
  - efficient when number of available plainstreams small
  - low plainstream count = wide applicability

Final Key Search Module



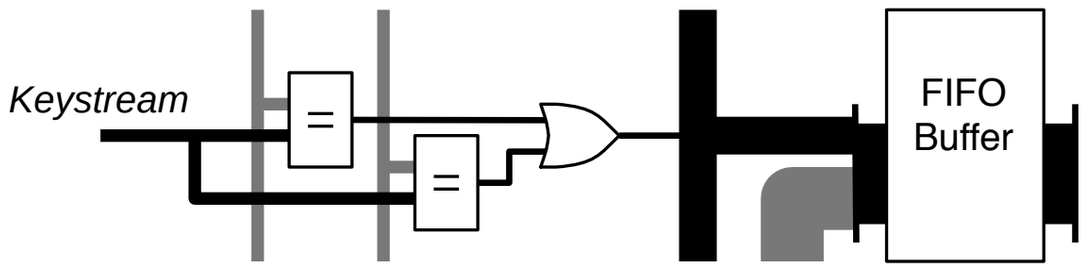
Final Key Search Module

- Three partitions separated by FIFO buffers
  - Front-End Search - eliminate most keys
  - Translation Unit - list keys for further checking
  - Back-End Full Test - reliably obtain actual key



Final Key Search Module

- Parallel search = many simultaneous comparison outputs
- Need compression to reduce memory width
  - use OR gate to half requirement
  - then double up back-end comparison units to compensate
  - net benefit in large systems



System Testing

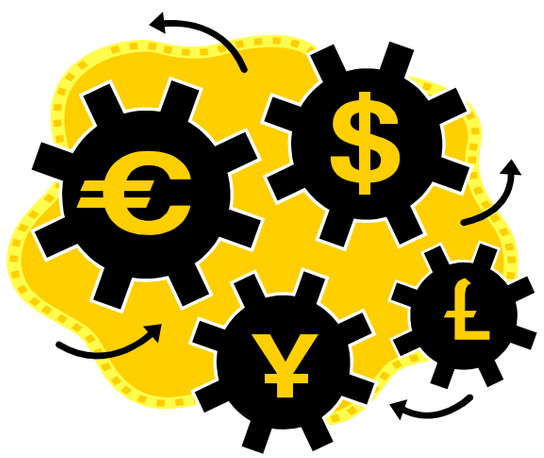
- Altera Cyclone EP1C20F400C6
  - n = p = 16
  - 4 back-end comparison units
  - 12k logic elements, 19kb memory
  - 100MHz
- Quartus 5.0 SP2 used for compilation and simulation

n = number of cipher units

p = number of plainstreams being checked

Economics

- Want to translate system into economic terms
  - allow comparison with data value estimates



What will the future cost of a search system be?

FPGA Progress

- 1984 - Concept invented
- 1985 - Xilinx XC2064

  2µm, 64 logic blocks

- 2006 - Xilinx Virtex 4

  90nm, 200k logic blocks

- Rapid development set to continue
- Price-performance ratio resembles Moore (see Section 3.2)
  - 4x increase every 3 years

Low Cost FPGA System

- Current generation low cost FPGA devices
  - Sparten III *(Xllinx)*
  - Cyclone II *(Altera)*
- Cyclone II EP2C35
  - volume price of $22 per chip
  - 35k logic elements
  - n=32 p=16 system fits the chip
  - 86MHz

Estimated Chip Cost

Recovery Time	2005	2010	2015	2025
1 day	$45b	$11b	$2.8b	$44m
1 month	$1.5b	$380m	$94m	$1.5m
1 year	$120m	$31m	$7.7m	$120k

- Expensive but may be feasible medium-term
- Lots of other associated costs
  - pcb manufacture, wiring, programming chips, power regulators, air conditioning, power consumption, logistics etc.

Hardcopy II

- Altera structured ASIC technology
  - generic chip mass manufactured without top metallisation layers
  - add metallisation to customers spec
- Fast with design advantages of FPGA
  - Lose covert purchasing
  - Gain a Non-Recoverable Engineering Cost of $225k
- HC210W
  - n=64 p=32 system fits $15 chip
  - estimated speed 230MHz

Estimated Chip Cost for HC210W

Recovery Time	2005	2010	2015	2025
1 minute	$3800b	$960b	$240b	$3.8b
1 hour	$64b	$16b	$4.0b	$63m
1 day	$2.7b	$670m	$170m	$2.8m
1 month	$130m	$33m	$8.4m	$350k
1 year	$7.5m	$2.1m	$680k	480 chips

- Results concerning even today

Further Notes

- System uses a small number of plainstreams
  - If 100s available a serial search system should be more efficient

- Original Grain algorithm broken ...

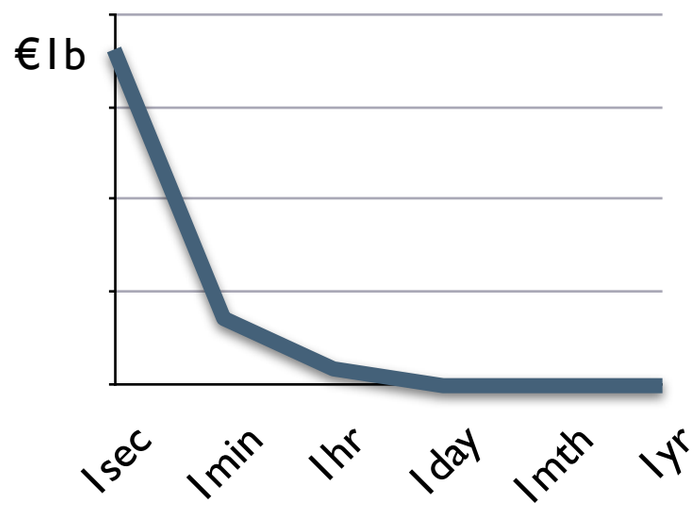
Algorithm	Logic Count	Initialisation	Extra
Grain v0	611 LE	66ns	-
Grain v1	656 LE	75ns	+22%
Trivium	747 LE	140ns	+160%

Cyclone EP1C20T324C8

Use of 80bit Stream Ciphers

- If value profile for adversary looks like this ....

  ... probably ok.



- But if looks like this ...

  ... not such a good idea!