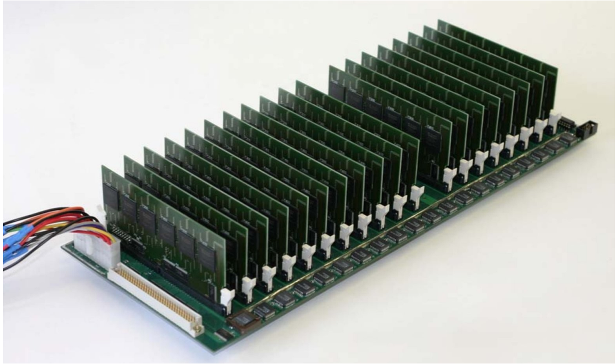
DeepCrack - 1998

- Developed by EFF
- < $250,000
- 80×10^9 keys/sec
- Solved DES challenge in 56 hours

See www.cryptography.com and www.eff.org

COPACABANA - 2006



- SciEngines, German uni's
- 120 FPGAs, 400×10^6 keys/sec/FPGA
- DES in 8.6 days
- $10,000

See www.sciengines.com

(Pentium 4: 2×10^6 keys/sec)

DES in 2013

- Moore's Law: double in speed every 1.5 years
  - Halve in cost every 1.5 years
  - $312 to break DES

RIVYERA S3-5000 - 2013

- SciEngines
- Up to 128 Xilinx Spartan-3 FPGAs
- ~$100 per FPGA (XCS5000)

- AES-128 Brute Force
  - 500x10^6 keys per sec
  - 4x10^6 keys per mW
- Biclique Attack
  - 945x10^6 keys per sec
  - 7.3x10^6 keys per mW

http://www.sciengines.com/products/computers-and-clusters/rivyera-s3-5000.html
http://2012.sharcs.org/slides/bogdanov.pdf
http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf
http://octopart.com/

AES-128 in 2013

Rivyera S3-5000 with 128 FPGAs: ~$15,000

- AES-128, Brute Force
  - 2^{128} keys (measure of time)
  - $64x10^{9}$ keys per sec per $15,000

- $15,000: $1.7x10^{20}$ years
- $15,000,000: 10^{17} years
- $15,000,000,000: 10^{14} years

- AES-128, Biclique
  - 2^{126} time, 2^{88} known, 2^{8} memory
  - $120x10^{9}$ keys per sec per $15,000

- $15,000: $9x10^{19}$ years
- $15,000,000: 10^{17} years
- $15,000,000,000: 10^{14} years

AES-128 in 2028

- Moore's Law: double in speed every 1.5 years
  - Halve in cost every 1.5 years
  - 2^{10} = 1000 times cheaper in 15 years

- $15,000,000,000 in 2028: 100,000,000,000 years

- What about AES-256? 10^{49} years