Cryptanalytic Applications of the PlayStation 3: the Case of DES

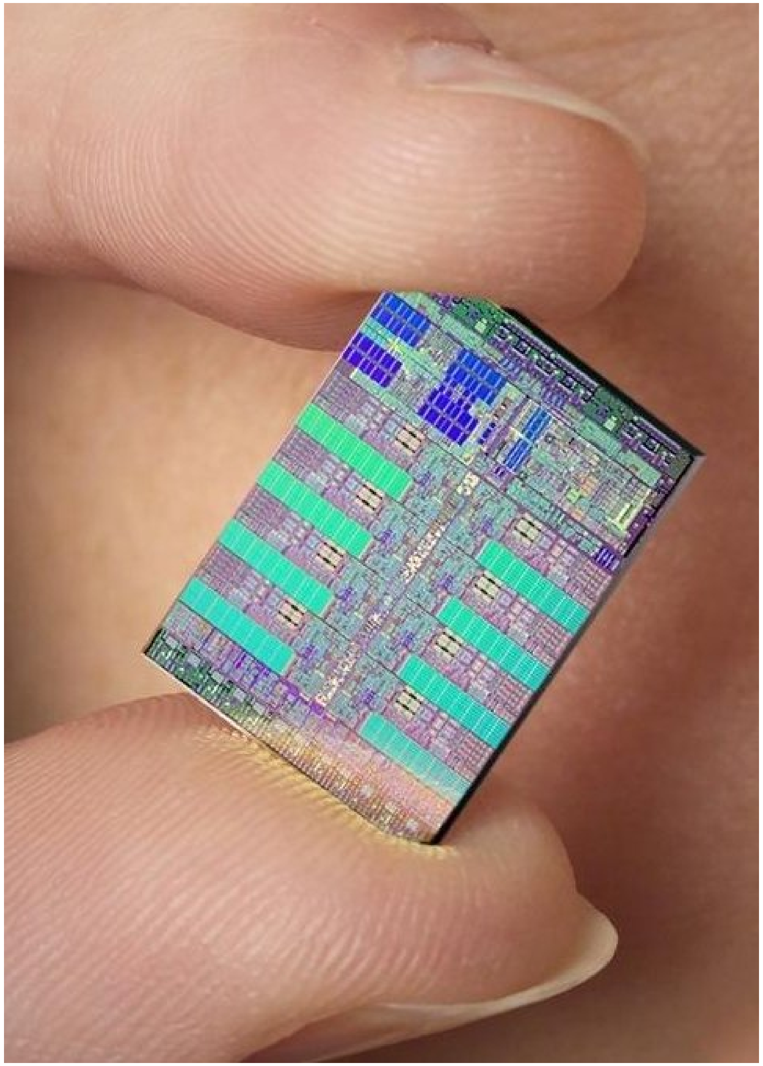
Dag Arne Osvik

Eran Tromer

Weizmann Institute of Science

Cell Broadband Engine

- 1 PowerPC core
  - Based on the PowerPC 970
  - 128-bit AltiVec/VMX SIMD unit
- 8 or 7 "synergistic processors"
  - 256KB of fast local memory
  - 128-bit, 128-register SIMD
- Runs at ~3.2GHz



- An x86-64 core has a single 128-bit SIMD unit with just 16 registers.

Running DES on the Cell

- Bitsliced implementation of DES
  - 128-way parallelism
  - S-boxes optimized for CPU instruction set using the S-box optimizer of Dag Arne Osvik
- 4Gbit/sec = 2^{26} blocks/sec per SPU
- 32Gbit/sec per Cell chip
- Verified using IBM's Cell simulator
- Can be used as a cryptographic accelerator (ECB, CTR, many CBC streams)

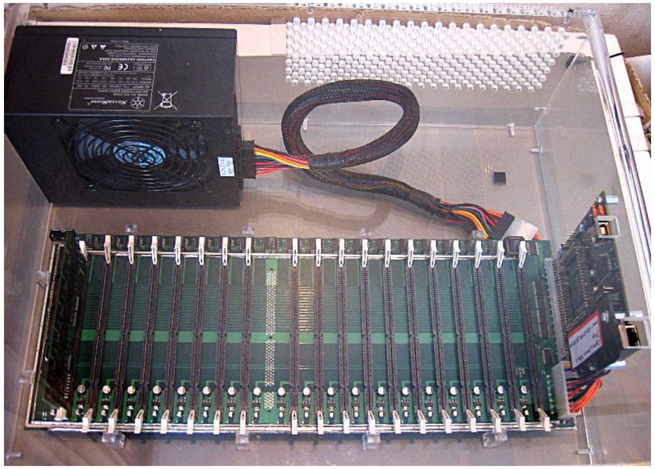
Breaking DES on the Cell

- Reduce the DES encryption from 16 rounds to the equivalent of ~9.5 rounds, by shortcircuit evaluation and early aborts.
- Performance:
  - $108M=2^{26.69}$ keys/sec per SPU
  - $864M=2^{29.69}$ keys/sec per Cell chip

Comparison to FPGA

Expected time to break:

- COPACOBANA
  - ~9 days
  - €8,980
  - A year to build



- 52 PlayStation 3 consoles
  - ~9 days
  - €30,056 (at US$700 each)
  - Off-the-shelf

- Divide by two if you get $E_K(X)$ and $E_K(\overline{X})$.

DreamHack 2004 LAN Party

5852 connected computers

Under 1 hour for a real-time DES break.

Other cryptographic applications for the Cell Broadband Engine

- Limited by SPU microarchitecture and memory
- Good match for low-memory, straight-path computation over small operands.
- Other promising applications:
  - AES acceleration
    (tentative results: x86-scale performance per SPU)
  - Stream cipher cryptanalysis
  - Sieving for the Number Field Sieve
  - Hash collisions