# A Billion-mulmods-per-second PC

Chen-Mou Cheng
National Taiwan University

jointly with: Daniel J. Bernstein, Hsueh-Chung Chen, Ming-Shing Chen,
Chun-Hung Hsiao, Tanja Lange, Zong-Cing Lin, and Bo-Yin Yang

Eurocrypt @ Köln, Apr. 28, 2009

Who wants to be a billionaire?

# Warning: Spoilers Ahead!

- (Some of) you will be hearing a talk on Thursday morning about how important ECM is and how fast we can run ECM on PCs (mainly GPUs)
- Please go get some Kölsch instead if you don't want to spoil the fun!

# Modular Multiplication

- Mulmods are useful
  - Special moduli: ECC, pairing
  - General moduli: ECM, RSA

- How fast can we do mulmods?
  - More interestingly, on PC

# A Brief Time Table

| Date | Raw | Scaled | Comments |
|---|---|---|---|
| Sep., 2008 | 17.91 | 38.09 | GMP-ECM (Q6600) |
| | 22.66 | 48.19 | GPU-ECM (280) |
| Jan., 2009 | 41.88 | 89.07 | No fault of ours (295) |
| Feb., 2009 | 164.31 | 164.31 | Thanks, Thorsten! :) |
| Apr., 2009 | 153.75 | 153.75 | CELL-ECM (QS22) |
| | 200.98 | 200.98 | X86-ECM (K10+) |
| | 400.48 | 481.30 | New GPU-ECM (295) |

- We measure (mul+sq)-mods in scalar multiplication from *actual* ECM
- Earlier numbers are for 280 bits (scaled to 192 bits)

# Squeezing out Extra Bits of Performance

Modern (x86) CPUs tend to be underutilized!

- AMD K10: up to 3 INT and 3 FP/SIMD instructions per cycle dispatched, out of order if necessary
  - INT: $64 \times 64 = 128$-bit mul, per 2 cycles
  - SIMD INT: *two* $32 \times 32 = 64$-*bit* muls per cycle
  - SIMD FP: *two DP (53b mantissa)* muls per cycle

  Can run INT and SIMD (either INT or FP) together

- Intel Core$*$: INT slower, conflict with SIMD execution

# Software Hyper-threading

- Idea: run many "threads" of execution simultaneously to exploit all circuitry available on K10
  - 73 cycles/ mulmod: 64-bit INT muls
  - 426 cycles / 4 mulmods: 128-bit SIMD INT muls
  - Try interlacing two threads at various ratios, say 6:1
- Result: 22.3% speedup from using INT MUL alone
  - Also works on Cell (240%)
  - Doesn't work so well for Intel CPUs (max. $\sim$ 10%)

# The Billion-mulmods-per-second PC

- Buy parts, say, from NewEgg.COM (4/28/2009 3AM)

| ITEM | US$ | Description | Notes |
|---|---|---|---|
| CPU | 190 | AMD Phenom II 940 (3.0 GHz) | retail K10+ |
| MB | 170 | ASUS M4N82 Deluxe | ECC-capable |
| RAM | 107 | 4x DDR2-800 ECC Kingston 2GB | |
| GPUs | 1060 | 2x PNY 896MB NVIDIA GTX 295 | |
| Case | 360 | Supermicro 4U with 865W PS | 5x fans |
| HDD | 110 | 2x Seagate SATA II 320GB | RAID 1 |

- Total: 1997 USD for 1.3 billion 192-bit mulmods/s.