Are Your Passwords Safe: Energy-Efficient Bcrypt Cracking with Low-Cost Parallel Hardware

Katja Malvoni

(kmalvoni at openwall.com)

Solar Designer

(solar at openwall.com)

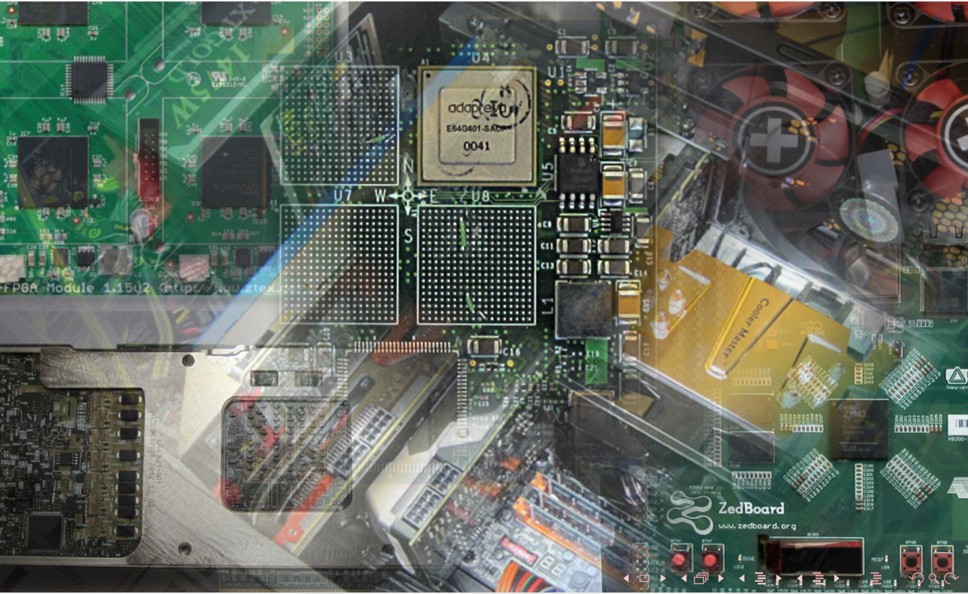
Josip Knezovic

(josip.knezovic at fer.hr)

Motivation

- Bcrypt is:
  - Slow
  - Sequential
  - Designed to be resistant to brute force attacks and to remain secure despite hardware improvements
- You could almost think why even bother optimizing

But

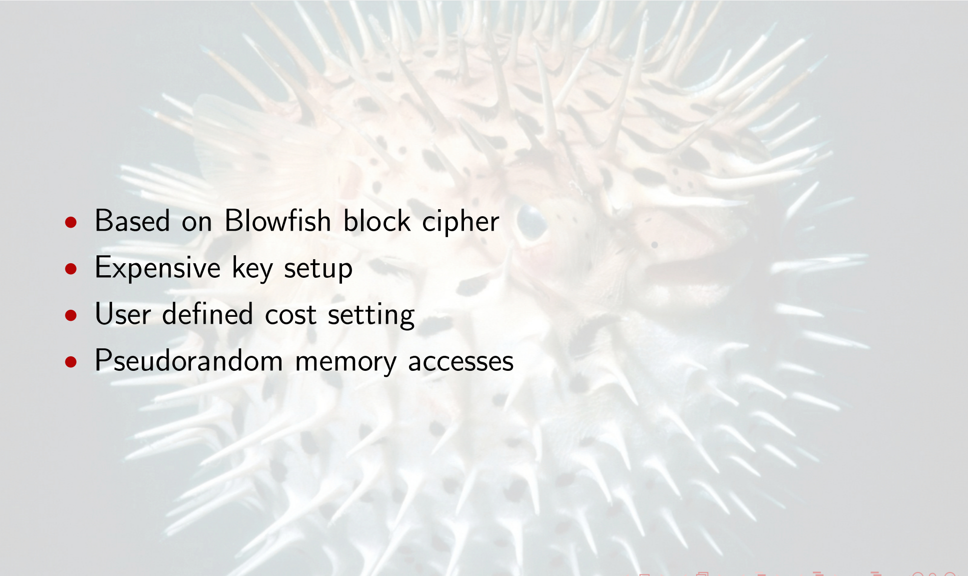

FPGA Module 1.15y2
adapteva
E64G401-SACP
0041
U3
U4
U1
U5
U7
U8
N
S
W
E
L1
Cooler Master
ZedBoard
www.zedboard.org

Outline

1. Bcrypt
2. Implementations
   - Parallella/Epiphany
   - ZedBoard and ZC706
3. Experimental Results
4. Future work
5. Takeaways

Bcrypt

- Based on Blowfish block cipher
- Expensive key setup
- User defined cost setting
- Pseudorandom memory accesses



Blowfish. Photo source: http://wallpapers.free-review.net

Architecture

Epiphany

- 16/64 32-bit RISC cores operating at up to 1 GHz/800 MHz
- **Energy-efficient** - 2 W maximum chip power consumption
- 32 KB of local memory per core
- FPU can be switched to integer mode

Implementation

Epiphany

- John the Ripper prepares data on ARM cores
- Bcrypt hashes computed on Epiphany
- Optimized in assembly
- Each Epiphany core computes two bcrypt hashes
- Computation overlapped to exploit dual-issue architecture
  - Integer ALU
  - FPU in integer mode

Architecture

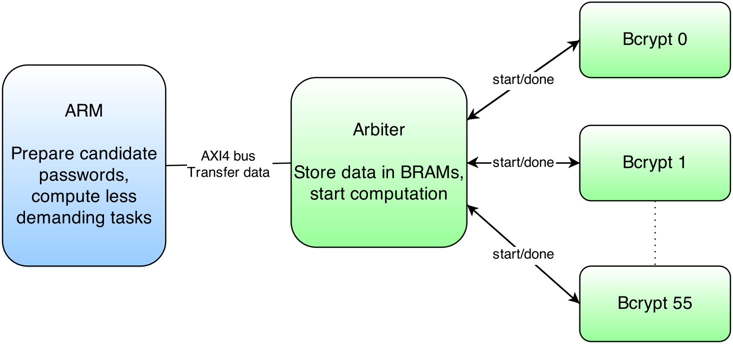
Zynq 7020 and Zynq 7045

- Heterogeneous device
- Dual ARM Cortex-A9 MPCore
- Advanced low power 28nm programmable logic
- Zynq 7045 $\sim$4 times bigger than Zynq 7020
- AXI buses used for CPU-FPGA communication

Implementation

Zynq 7020 and Zynq 7045

- John the Ripper prepares data on ARM cores
- Bcrypt instances compute hash(es)

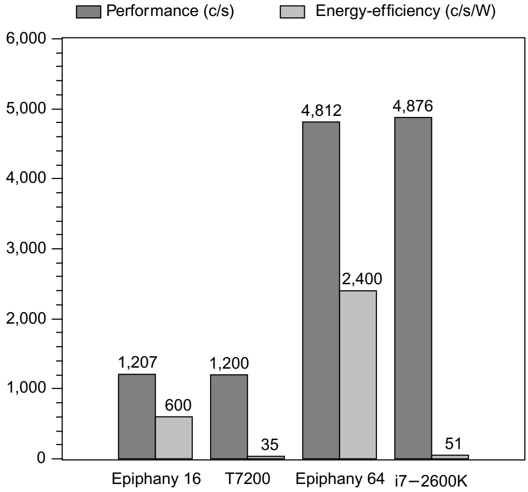


Implementation

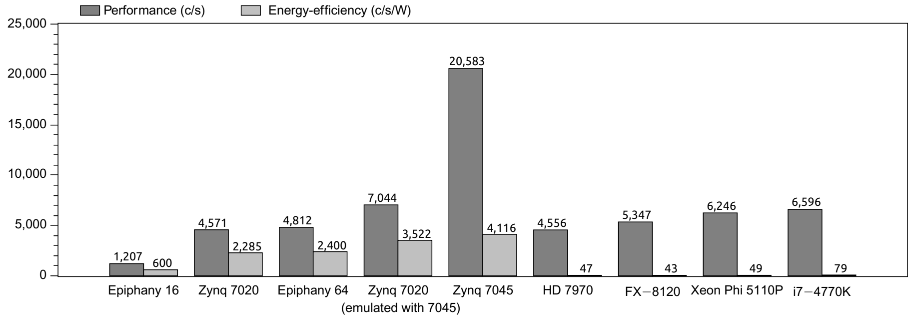
Number of concurrent instances

- Number of concurrent instances limited by available BRAM
- Overlapping multiple bcrypt instances in one module
  - 56, 70 or 112 instances on Zynq 7020 with 140 BRAMs
    - or many more on Zynq 7045 with 545 BRAMs
- Large communication overhead for low bcrypt cost setting
- Hardware defects of boards limit optimizations

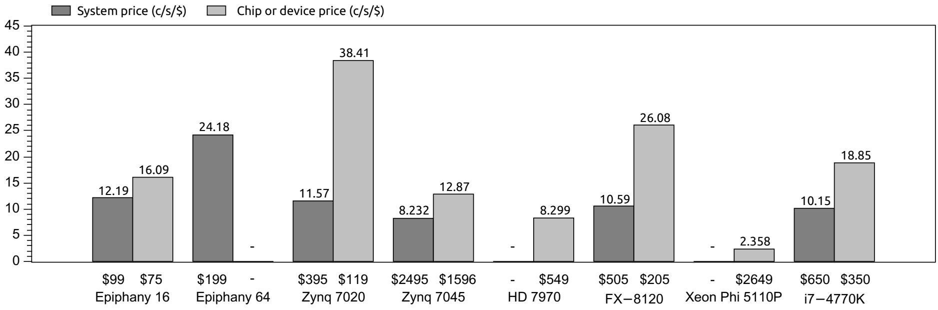
Epiphany vs x86



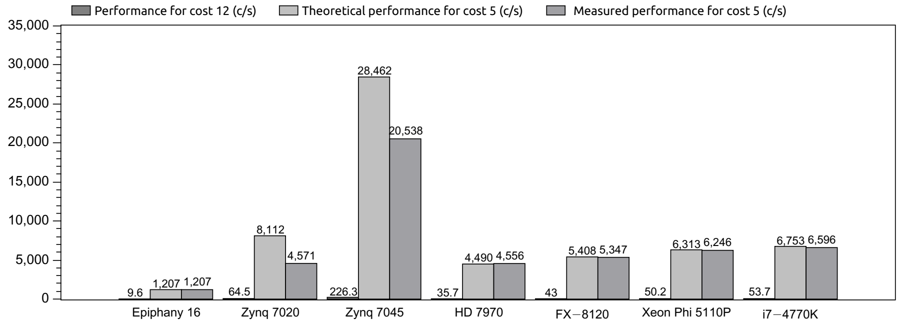
Performance and efficiency comparison



Cost comparison



Derived performance from cost 12



Theoretical Peak Performance Analysis

Theory

$$c/s = \frac{N_{ports} * f}{(2^{cost} * 1024 + 585) * N_{reads} * 16} \quad (1)$$

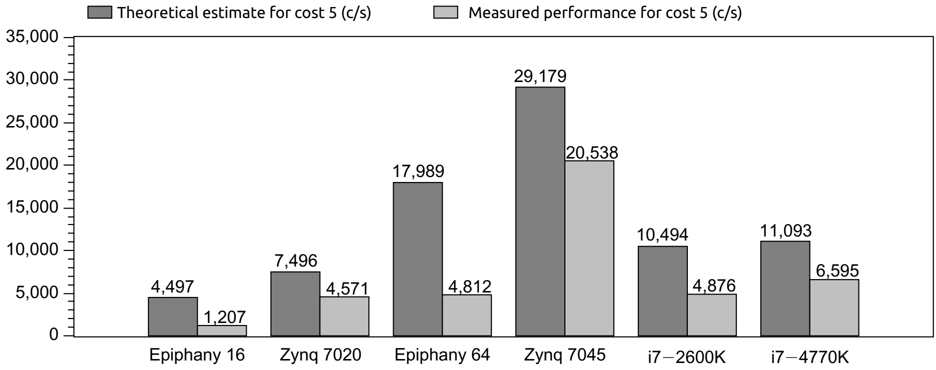
- N_{ports} - number of available read ports to local memory or L1 cache
- N_{reads} - number of reads per Blowfish round
- $2^{cost} * 1024 + 585$ - number of Blowfish block encryptions in bcrypt hash computation
- f (in Hz) - clock rate

bcrypt(cost, salt, pwd)

```
state ← InitState()
state ← ExpandKey(state, salt, key)
repeat(2^cost)
    state ← ExpandKey(state, 0, salt)
    state ← ExpandKey(state, 0, key)
ctext ← "OrpheanBeholderScryDoubt"
repeat(64)
    ctext ← EncryptECB(state, ctext)
return Concatenate(cost, salt, ctext)
```

Theoretical Peak Performance Analysis

Comparison



Related work

- F.Wiemer, R. Zimmermann. Speed and Area-Optimized Password Search of bcrypt on FPGAs
    - bcrypt running on ZedBoard at 80 MHz
    - 40 parallel instances
    - 5208 c/s at cost 5, 41.6 c/s at cost 12
- Yuri Gonzaga, Google Summer of Code 2011

Future work

- Parallella/Epiphany
  - Using both Epiphany and Zynq 7020 at once
  - Possible to integrate up to 64 chips on a single board
  - Scalability of current implementation is promising
  - 64 * 64 = 4096 cores with theoretical performance of 300000 c/s
- FPGA
  - Zynq 7020 and 7045 optimizations
    - Improve clock rate
    - Reduce communication overhead
  - Targeting bigger FPGAs
  - Targeting multi-FPGA boards

Takeaways

- Many-core low power RISC platforms and FPGAs are capable of exploiting bcrypt peculiarities to achieve comparable performance and higher energy-efficiency
- Higher energy-efficiency enables higher density
  - More chips per board, more boards per system
- It doesn't take ASICs to improve bcrypt cracking energy-efficiency by a factor of 45+
  - Although ASICs would do better yet

Thanks

- Sayantan Datta
- Steve Thomas
- Parallella project
- Google Summer of Code
- Xilinx
- Faculty of Electrical Engineering and Computing, University of Zagreb

Questions

?