Cryptech Alpha FPGA

Pavel Shatov

< meisterpaul1@yandex.ru >

Berlin, 2016-07-15

What is an FPGA?

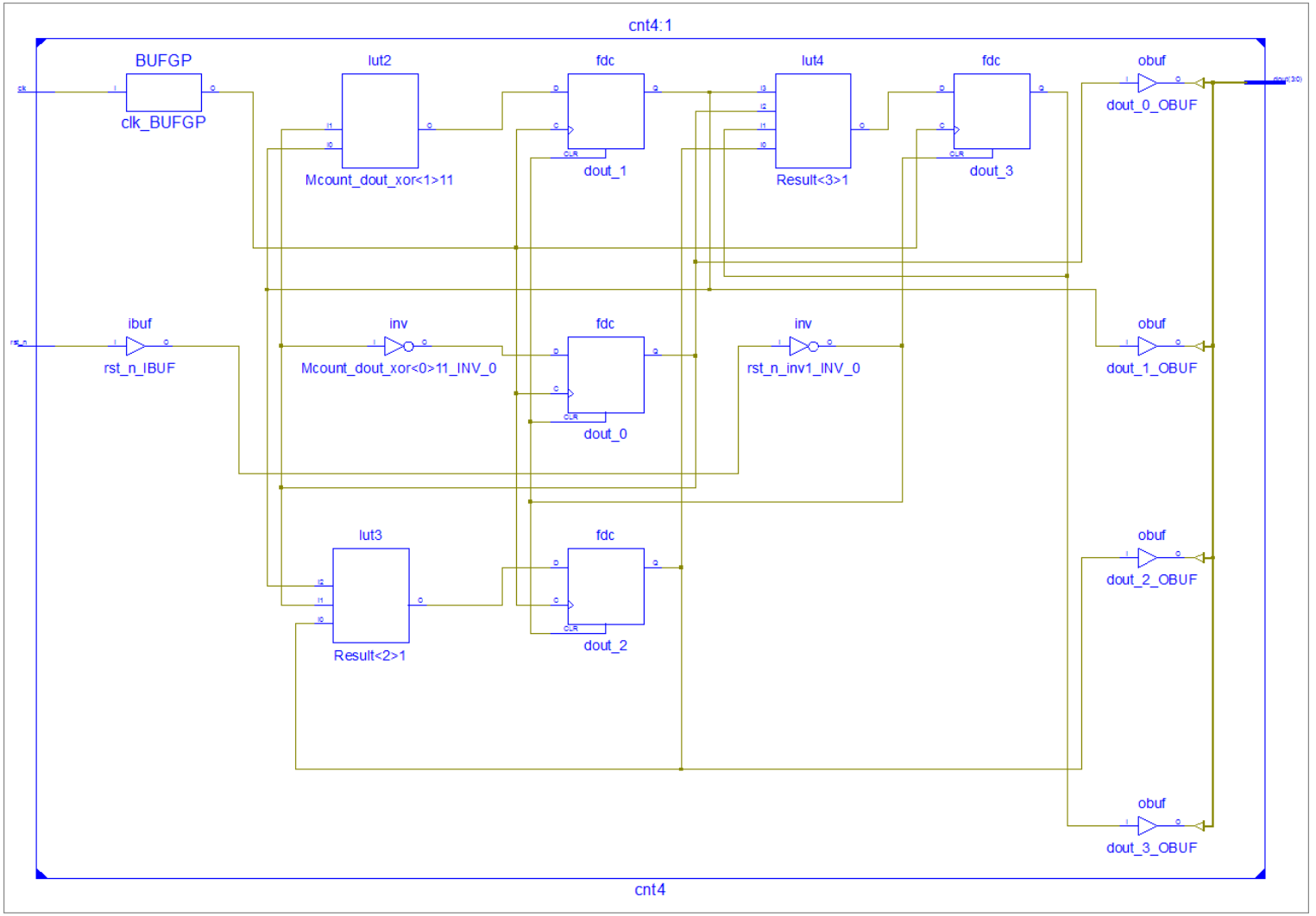
- Large matrix of flip-flops and look-up tables
  - ➔ Flip-flips (aka registers) store bits of data
  - ➔ Look-up tables form Boolean logic functions
- Configurable I/O pins
- Clocking backbone
- Programmable interconnect

FPGA Design Example

```
// Verilog source for 4-bit counter

module cnt4(clk, rst_n, dout);

    input wire clk;
    input wire rst_n;
    output reg [3:0] dout;

    always @(posedge clk or negedge rst_n)
        if (rst_n == 1'b0)      dout <= 4'h0;
        else                    dout <= dout +  1'b1;

endmodule
```

FPGA Design Example

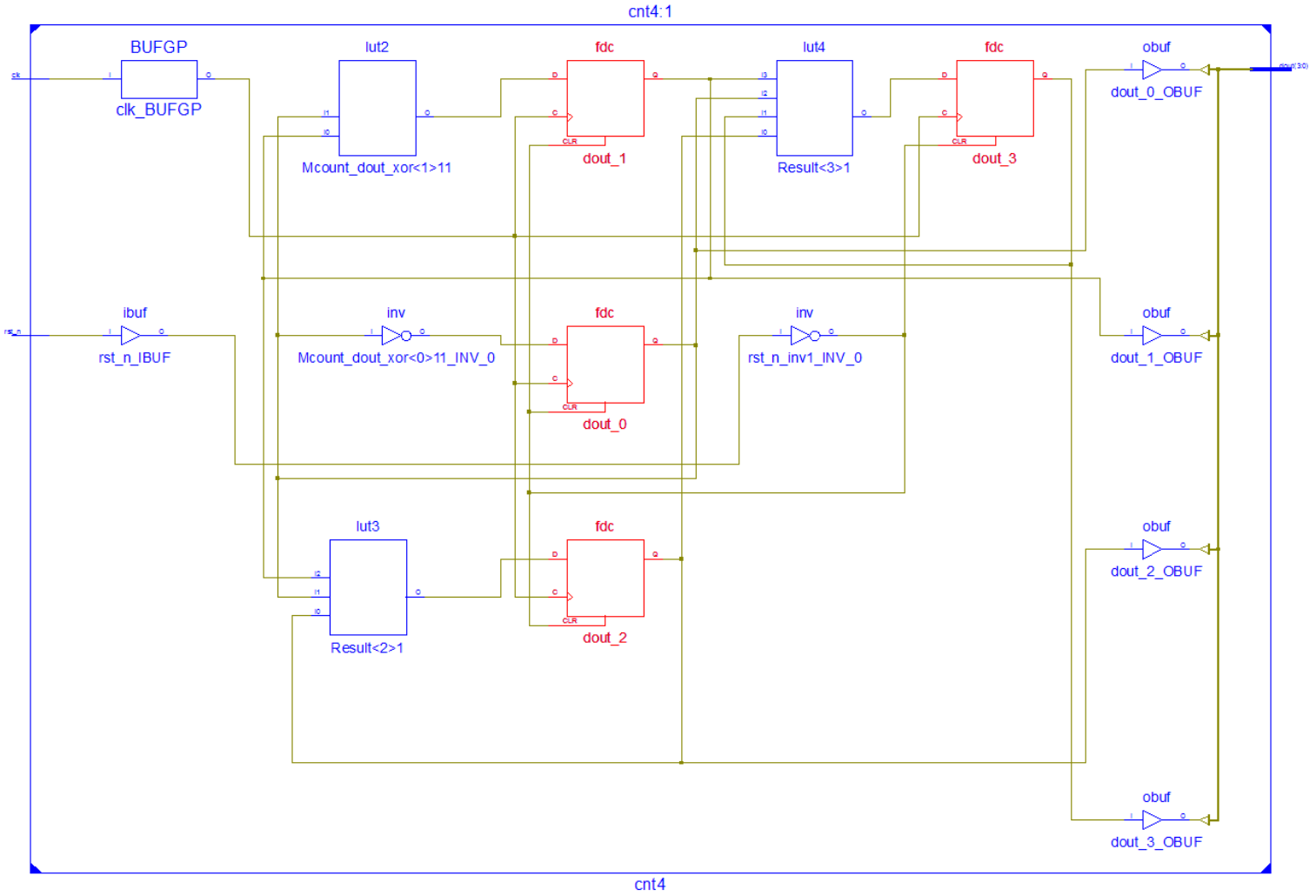
Synthesized
4-bit counter



FPGA Design Example

Synthesized
4-bit counter

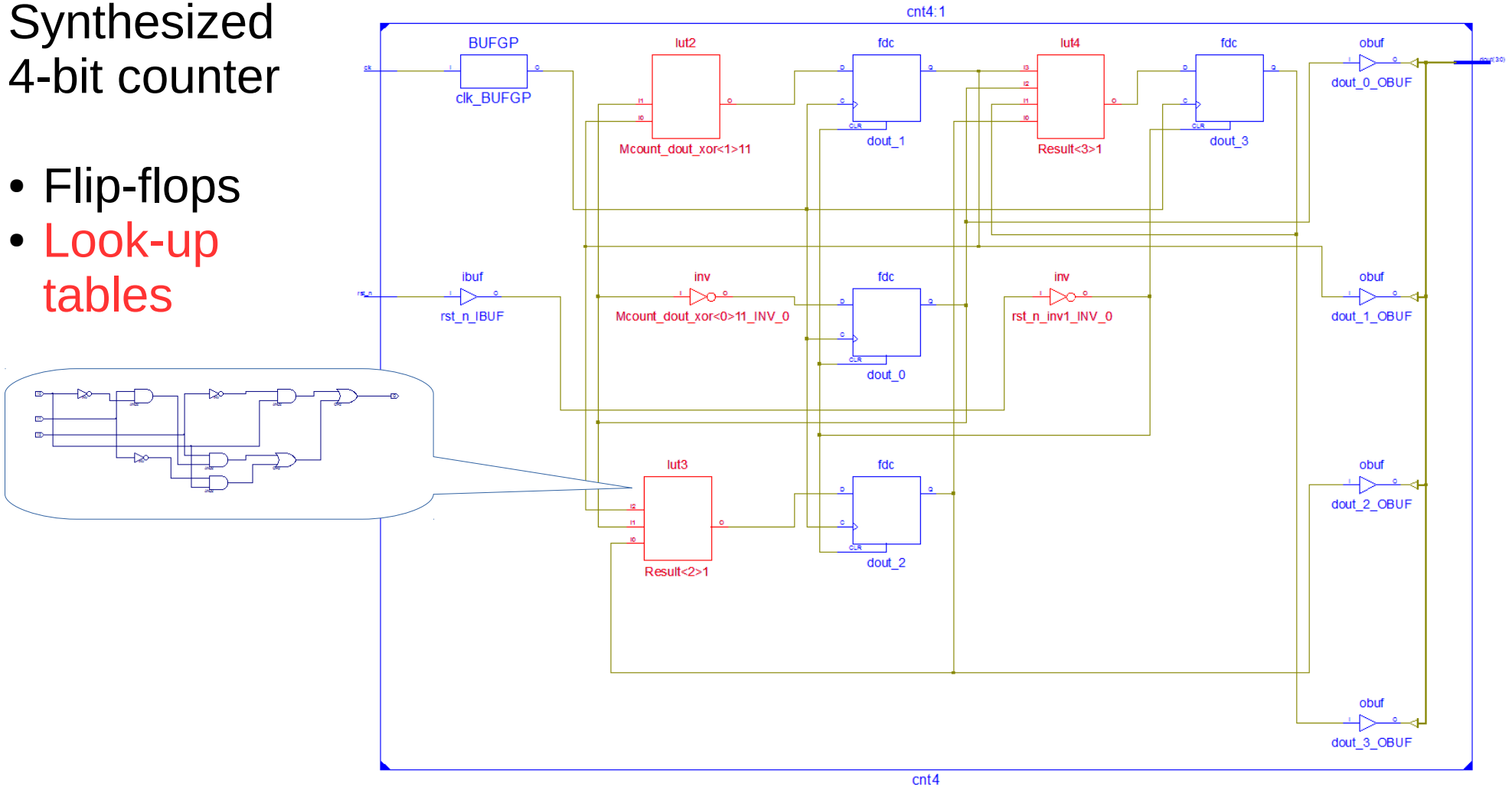
- Flip-flops



FPGA Design Example

Synthesized
4-bit counter

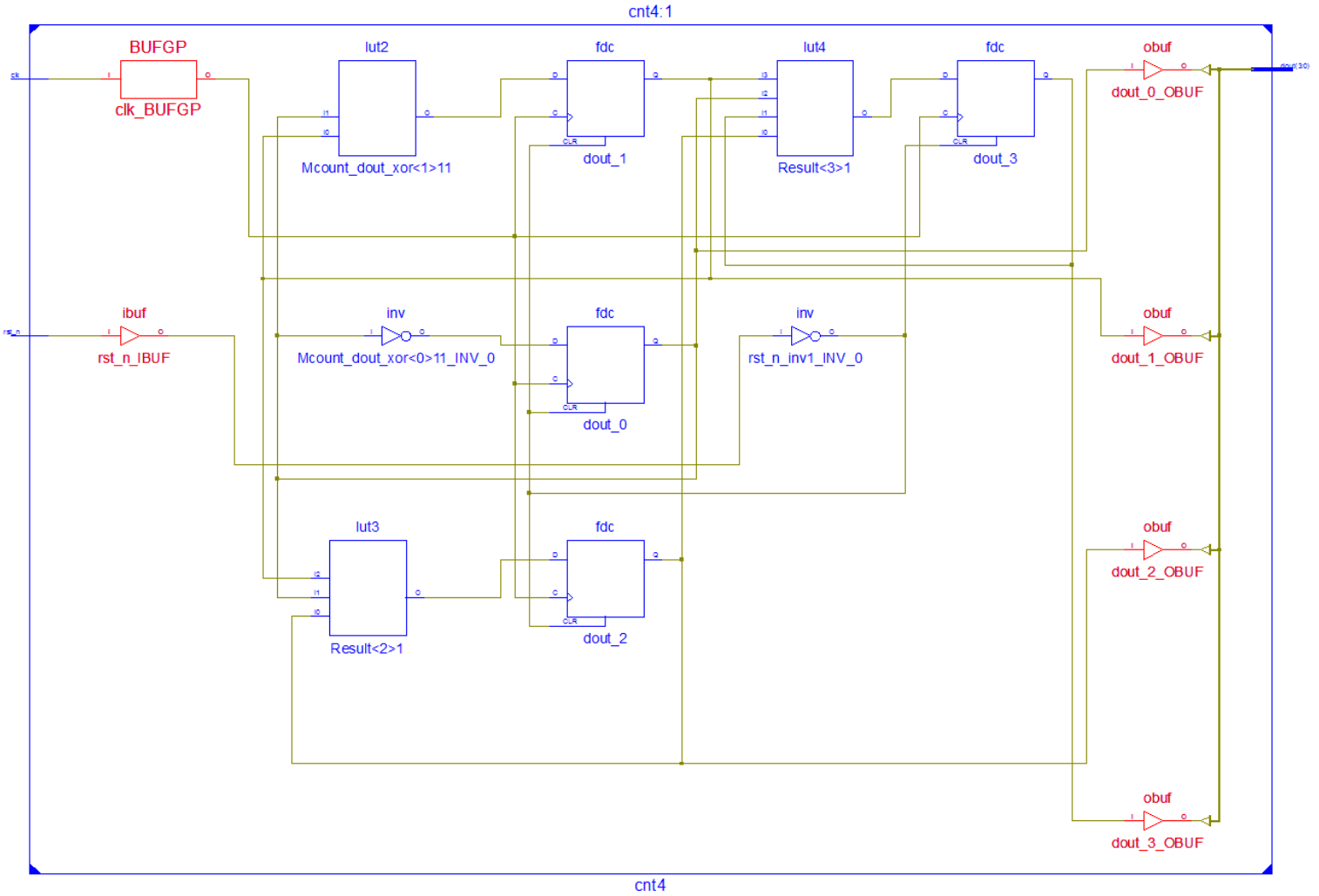
- Flip-flops
- Look-up tables



FPGA Design Example

Synthesized 4-bit counter

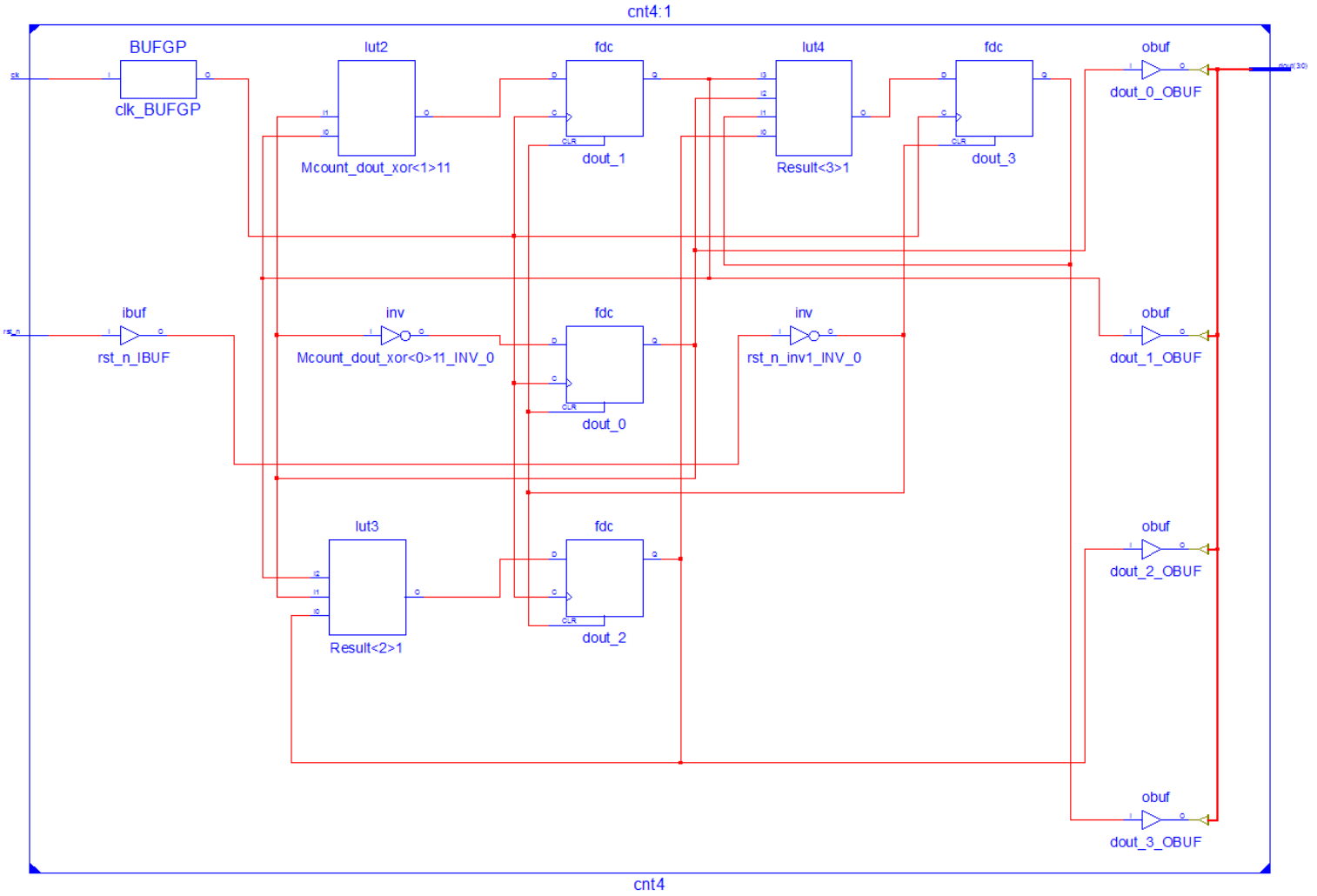
- Flip-flops
- Look-up tables
- I/O pins



FPGA Design Example

Synthesized 4-bit counter

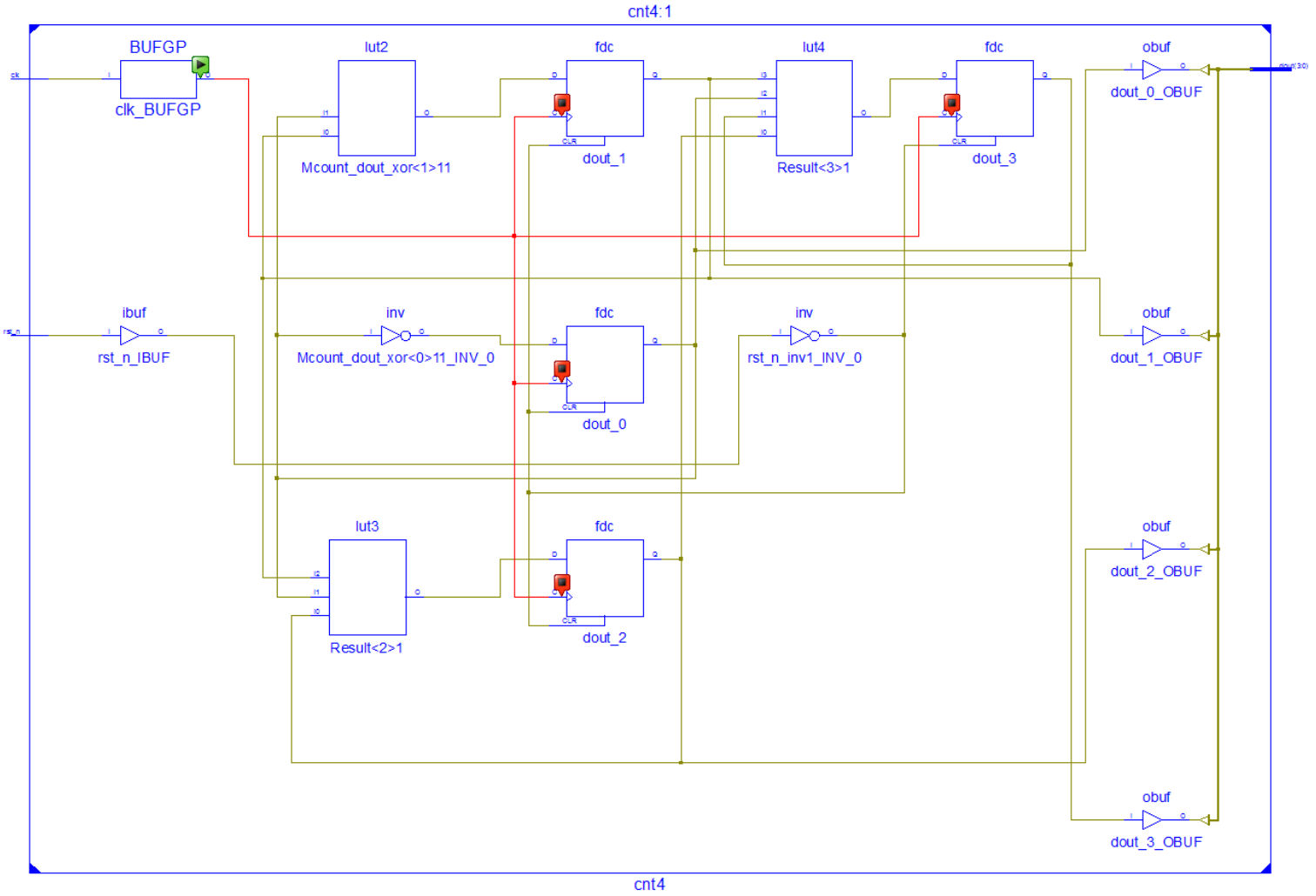
- Flip-flops
- Look-up tables
- I/O pins
- Flexible interconnect



FPGA Design Example

Synthesized 4-bit counter

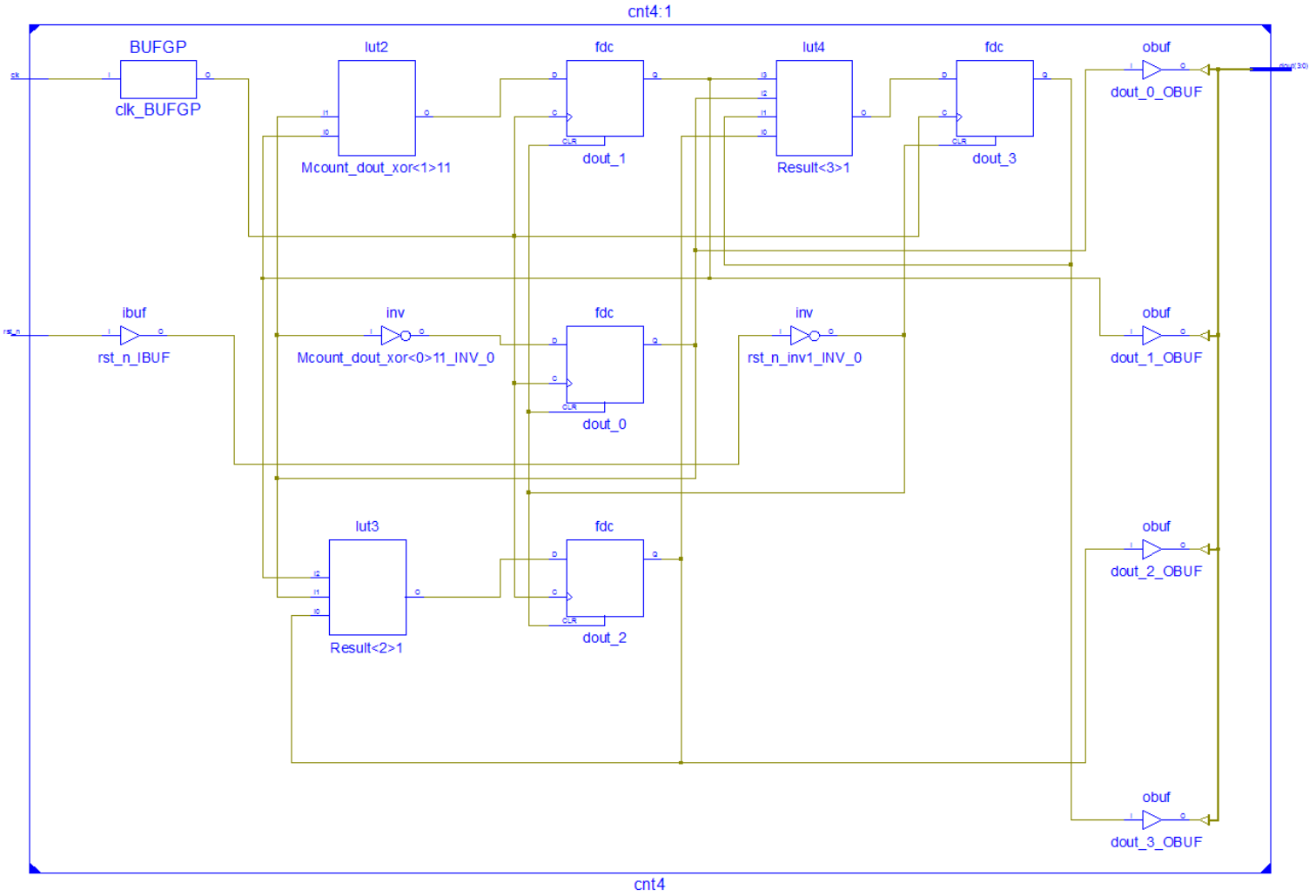
- Flip-flops
- Look-up tables
- I/O pins
- Flexible interconnect
- Clocking backbone



FPGA Design Example

Synthesized 4-bit counter

- Flip-flops
- Look-up tables
- I/O pins
- Flexible interconnect
- Clocking backbone
- PLLs (clock synthesizers)
- Block RAM
- DSP blocks



Why need an FPGA?

- More resistant to common side-channel attacks against crypto hardware
  - ➔ True constant-time-by-design implementation is possible
  - ➔ Absense of data-dependent behaviour

- More robust implementation of crypto algorithms
  - ➔ No stack overflows
  - ➔ No dynamic memory allocations, no pointers
  - ➔ Physical isolation of cores

Why need an FPGA?

- High performance
  - Processors are typically optimized for instruction throughput
  - FPGAs are not optimized per se, users can set their own optimization goals
  - Very linear speed/space tradeoff
- Intermediate step towards an ASIC
  - C implementation of reference model
  - HDL implementation
  - Verification in simulator using testbenches
  - Verification in hardware using FPGA
  - ASIC implementation

Alpha Board FPGA

- XC7A200T from Xilinx (Artix-7 Family)
  - 270k LUTs, 135k FFs
  - 13 Mb of block memory, 740 DSP blocks
  - average price: 190$ (-1 speed grade)

- Pin-compatible alternative: XC7A100T
  - 50% smaller
  - average price: 140$

CrypTech FPGA Cores

- Available cores
  - AES, ChaCha
  - SHA-1, SHA-2, SHA-3
  - RSA (Modular Exponentiation)
  - CSPRNG (Ring oscillator entropy source, entropy mixer)
  - MKM Interface
  - GOST R 34.11-2012 (aka Streebog)

CrypTech FPGA Cores

- Cores being developed
  - ECDSA (curves P-256 & P-384, DNSSEC algorithms 13 & 14)

CrypTech FPGA Cores

- Planned cores
  - GOST R 34.10-2001 (aka ECC-GOST, DNSSEC algorithm 12)
  - Curve25519 / Ed25519
  - ...