VoteBox Nano

A Smaller, Stronger FPGA-based Voting Machine

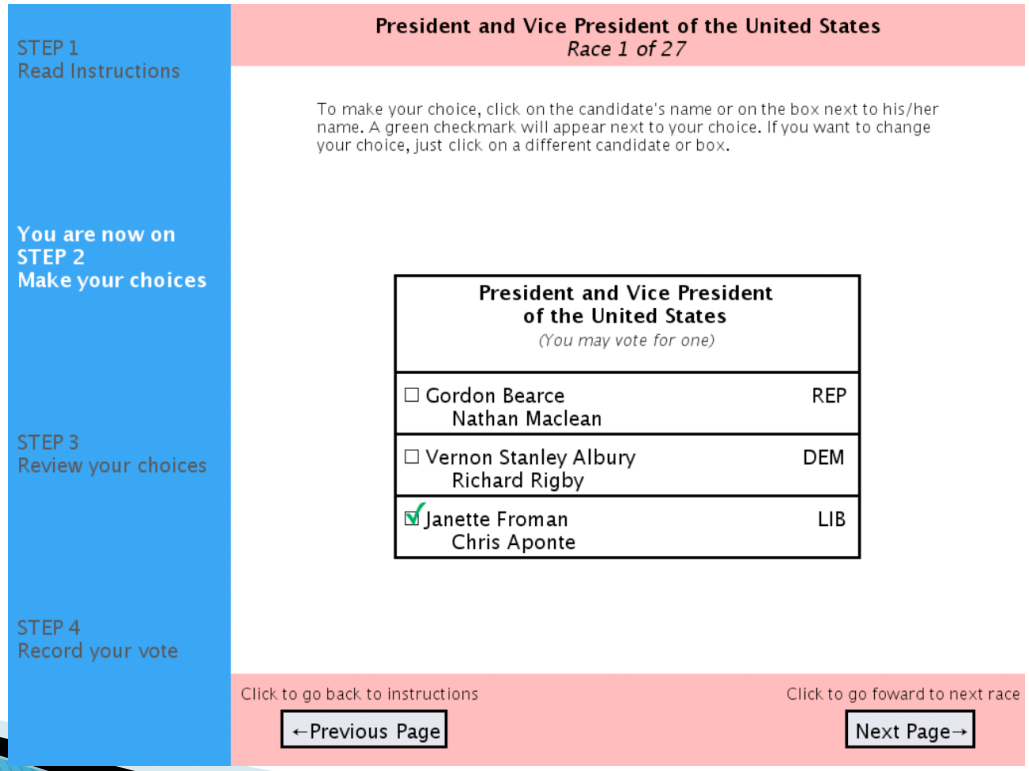
EVT/WOTE '09
AUGUST 10, 2009

Ersin Öksüzoğlu
Dan S. Wallach

RICE

Previously on VoteBox

- VoteBox
  - Full featured DRE voting machine
  - Paper in USENIX Security Symposium 2008



VoteBox (Classic)

Pre-rendered user interface

simplifies the **graphics** subsystem & **code size**

Network ballot replication

increases the **availability** of voting records

Challenge option

casts the votes **as intended**

Elgamal ballot encryption

allows **tallying** the votes independently

Elgamal Homomorphic Encryption

- One way of encryption

$$E(c, r, g^a) = \langle g^r, (g^a)^r f^c \rangle$$

- Two ways of decryption

$$D(\langle g^r, g^{ar} f^c \rangle, a) = \frac{g^{ar} f^c}{(g^r)^a}$$

$$D(\langle g^r, g^{ar} f^c \rangle, r) = \frac{g^{ar} f^c}{(g^a)^r}$$

Problems with VoteBox (Classic)

- In a tampered VoteBox, we cannot detect privacy attacks
  - The random number can be used as a subliminal channel
- VoteBox still needs to be smaller

EVM	Language	LOC
Pvote	Python	460
VoteBox	Java	14500
Diebold AccuVote TSX	C++	64000
Sequoia Edge	C	124000

VoteBox Nano: First FPGA-based EVM

Hardware and software hybrid

Pre-rendered GUI

✓Minimized code size for easier inspection

Challenge option Elgamal Encryption

✓End to end cryptography

True Random Number Generator

✓Better random numbers

Session ID Bitstream Readback

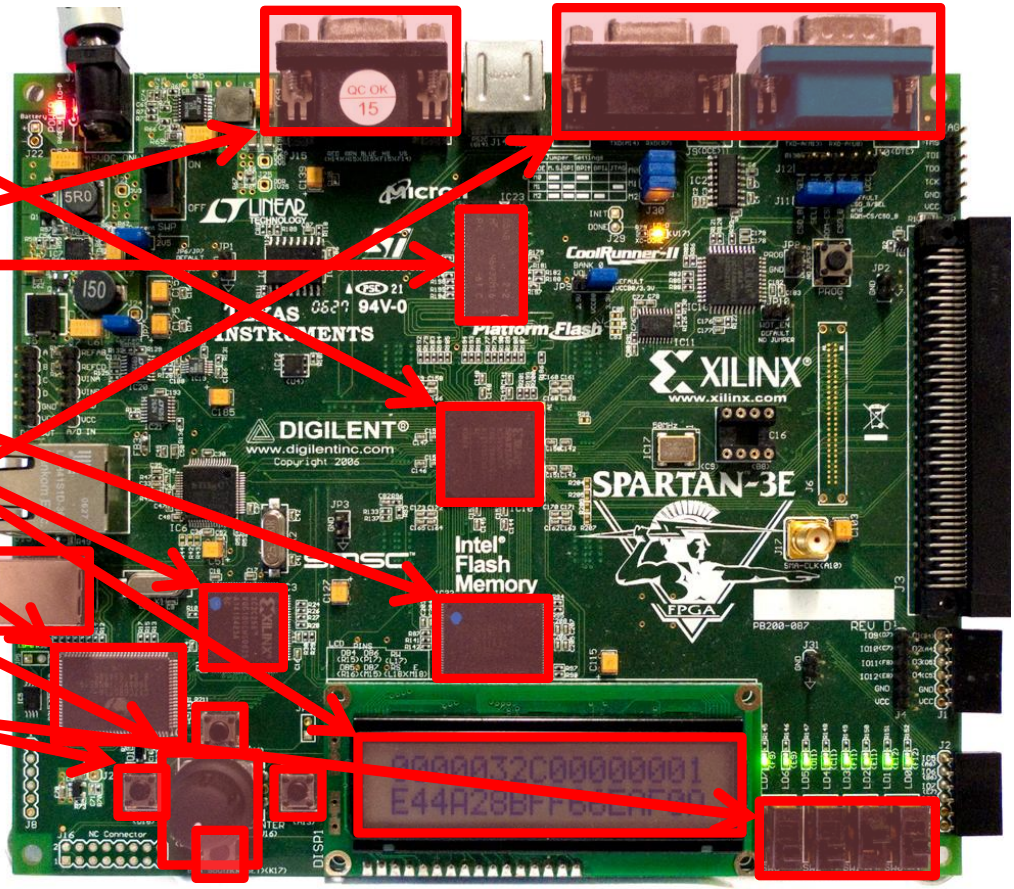
✓Additional tamper-evidence mechanism

FPGA (Field Programmable Gate Array)

- A blank chip that the user can program on the field
  - Emulate any chip
- Used for prototyping custom silicon
  - Accelerate designs taking the advantage of the parallelism
- Widely deployed in the industry ($2.75 billion in 2010)
  - Fast time to market
  - Low initial cost
  - Re-programmable hence easy to update

Xilinx Spartan-3E Starter Kit (~$150)

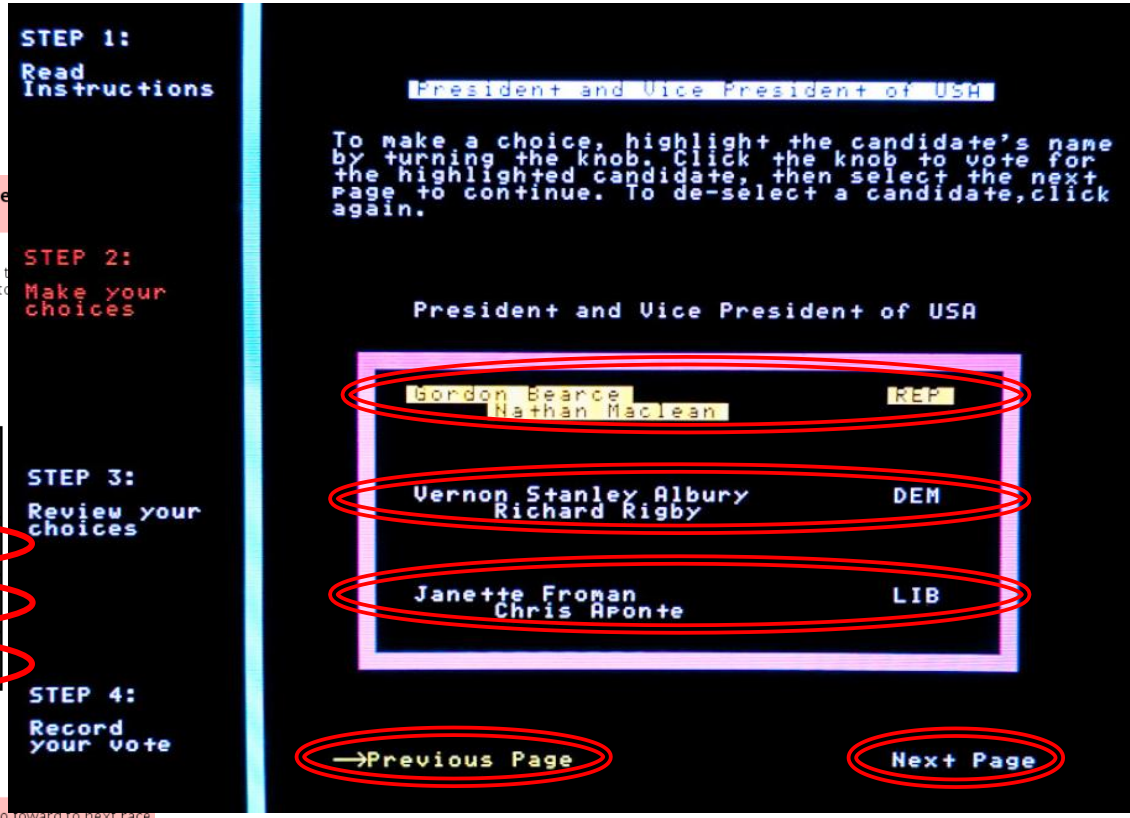
- 500k gate FPGA Chip
- Flash RAM
- DRAM
- VGA port
- Dot Matrix LCD (2x16)
- A rotary encoder
- RS232 serial ports
- Buttons and switches
- USB configuration port
- No CPU, GPU, network chip



VoteBox Nano Lacks

- Network replication and storage facilities
  - We have limited space on board
- Ethernet communication module
  - Instead we have RS232 port
- High resolution bitmap based GUI
  - We have character graphics

VoteBox Classic vs. VoteBox Nano



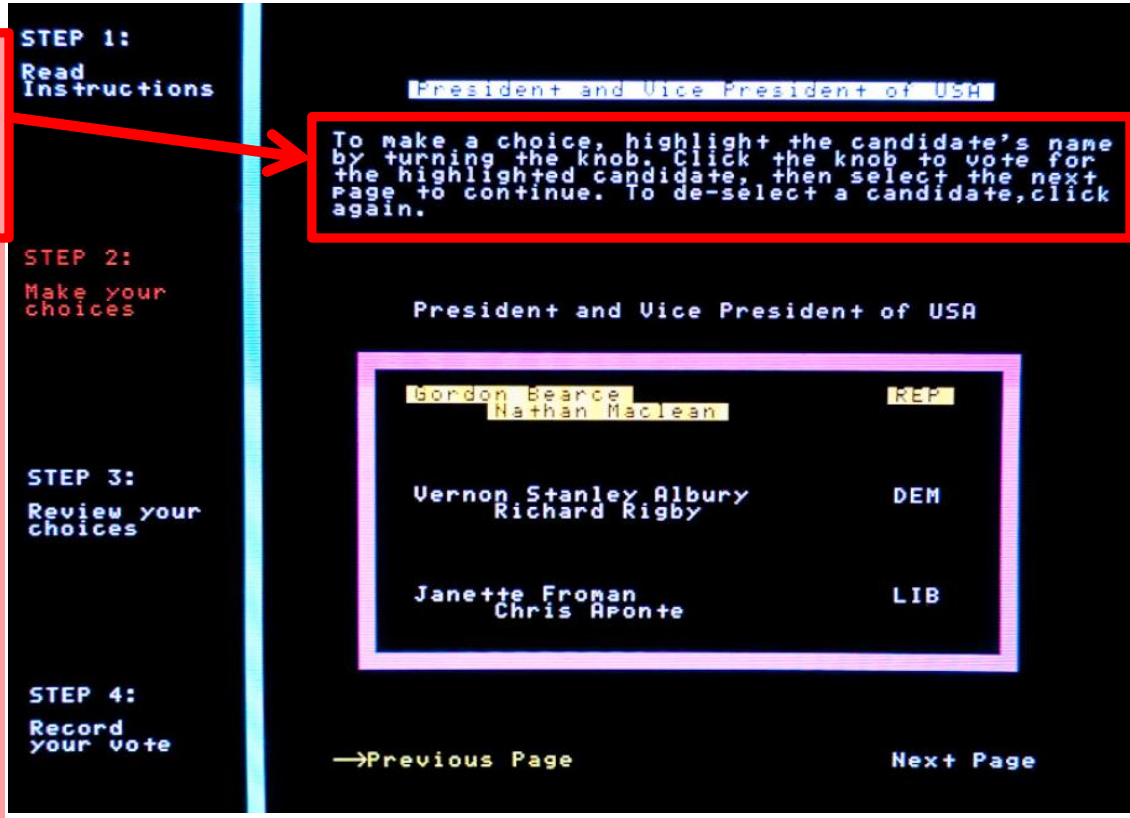
Pre-rendered GUI [Yee]

X Y color text

```
6 25 15 President and the Vice President of USA

9 20 7  To make a choice highlight the candidate's name
10 20 7 by turning the knob. Click the knob to vote for
11 20 7 the highlighted candidate then select the next
12 20 7 page to continue. To de-select a candidate click
13 20 7 again.

19 25 7 President and the Vice President of USA
22 21 1 ========================================
23 21 1 =                                      =
24 21 1 =  Gordon Bearce              REP      =
25 21 1 =        Nathan Maclean                =
26 21 1 =                                      =
27 21 1 =                                      =
28 21 1 =                                      =
29 21 1 =  Vernon Stanley Albury      DEM      =
30 21 1 =        Richard Rigby                 =
31 21 1 =                                      =
32 21 1 =                                      =
33 21 1 =                                      =
34 21 1 =  Janette Froman             LIB      =
35 21 1 =        Chris Aponte                  =
36 21 1 =                                      =
37 21 1 ========================================
```

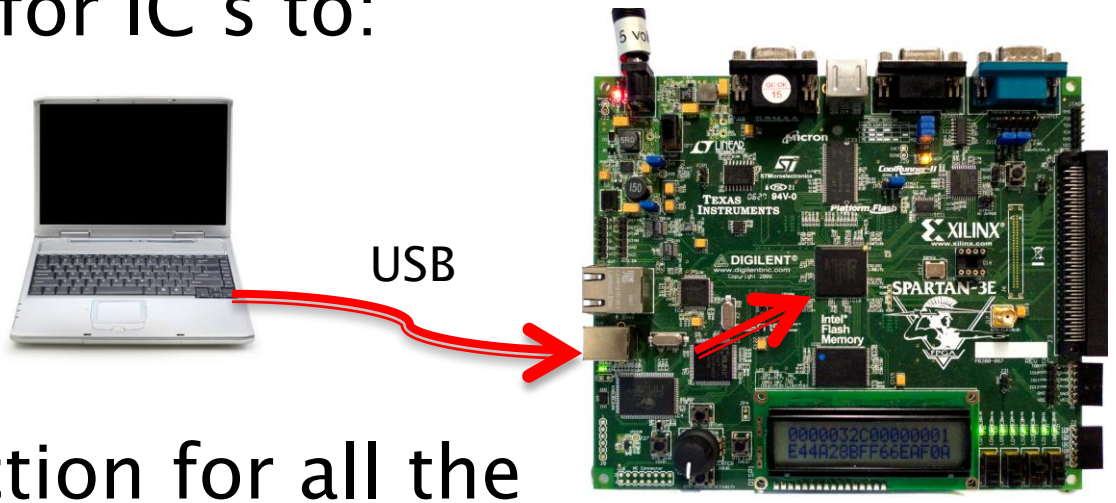


Ballot Definition

VoteBox Nano

JTAG (Joint Test Action Group)

- IEEE port standard for IC's to:
  - Debug
  - Program
  - Monitor

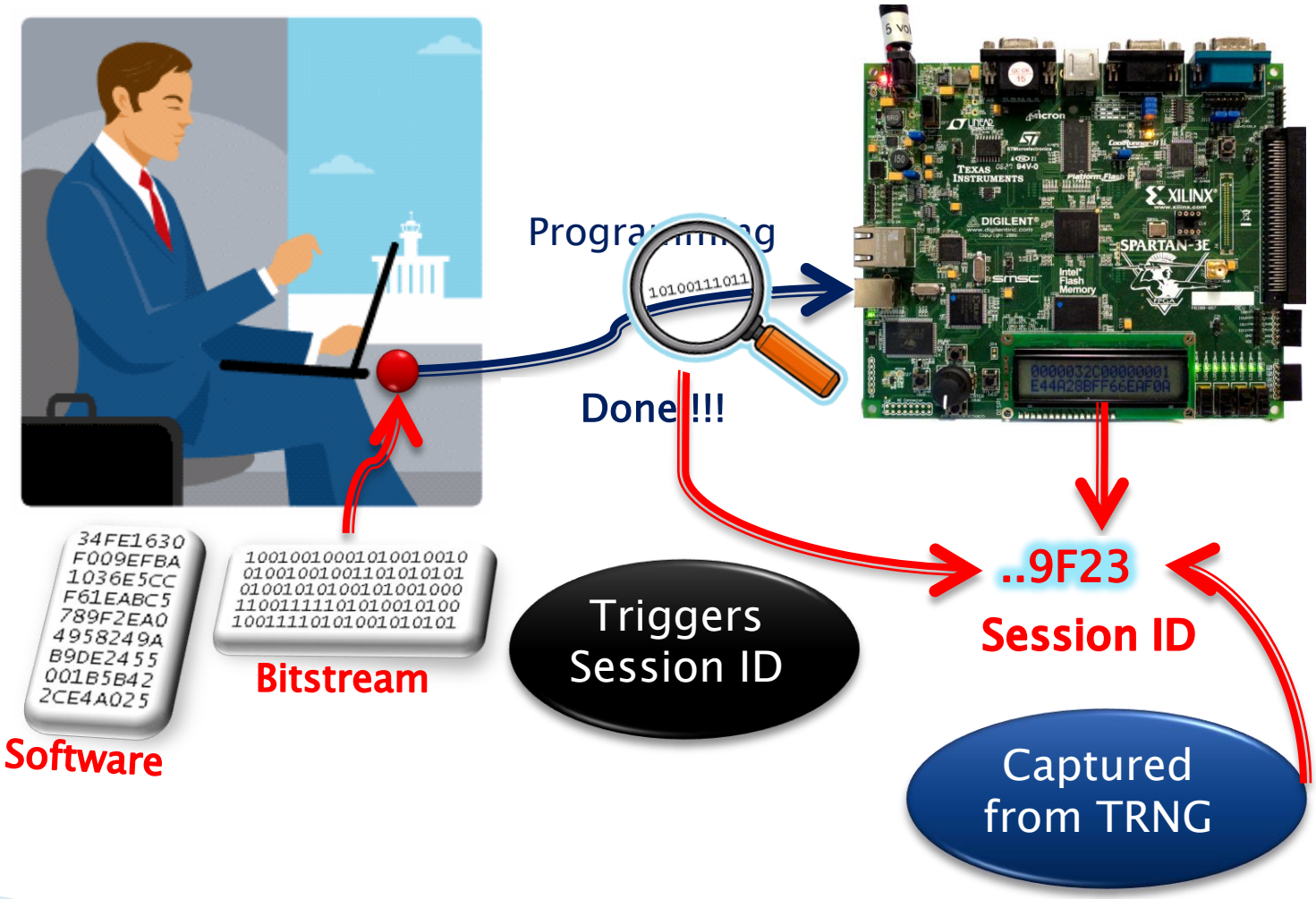


- Daisy chain connection for all the components on board
  - One wire data in
  - One wire data out

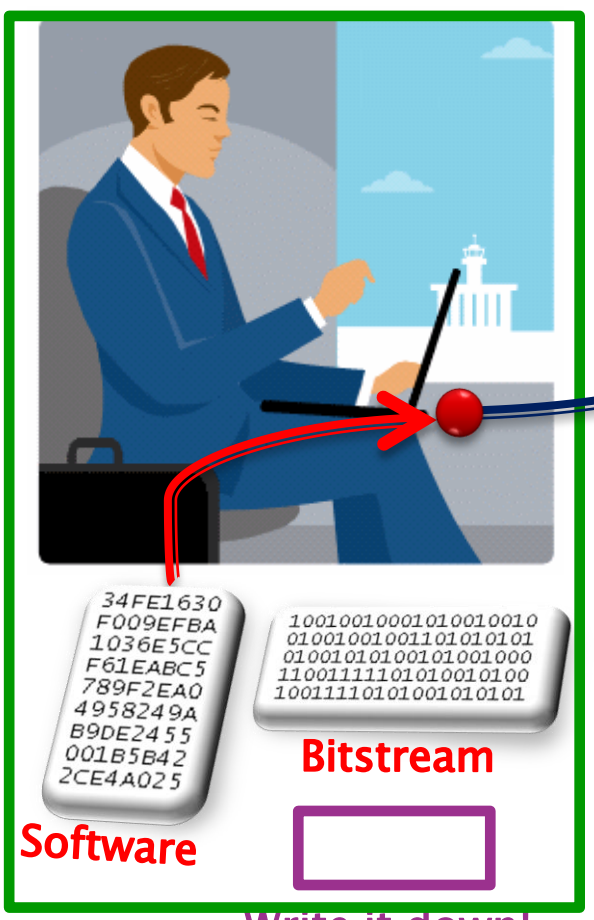
For FPGAs, JTAG is used for

1. Bitstream upload and download
2. Software upload and download
3. Accessing software debugger

Programming FPGA (Hardware)



Programming FPGA (Software)

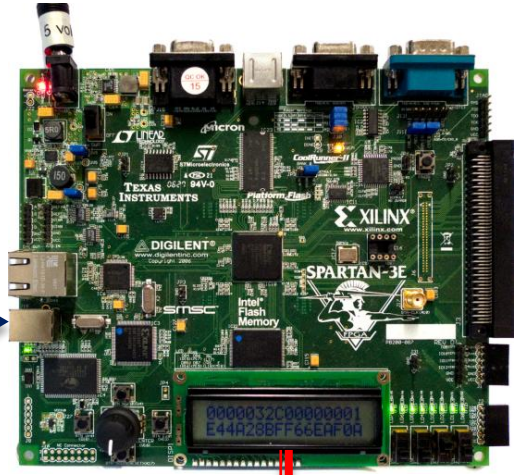


Programming

USB → JTAG

Done !!!

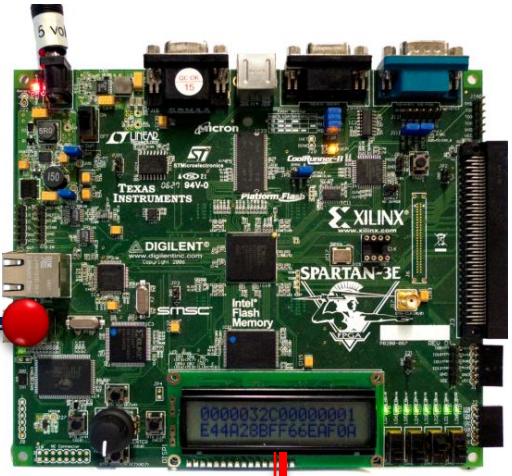
The design is ready!



..0932 FPGA is sealed

Session ID

Attestation



Readback bitstream

Done !!!

..0932

Same ?

..CC21

Seal is broken

Original bitstream

Compare

Bitstream from FPGA

Interesting Attacks

- Upload a new bitstream

- Change software
  - JTAG port is monitored
  - Session ID is read-only

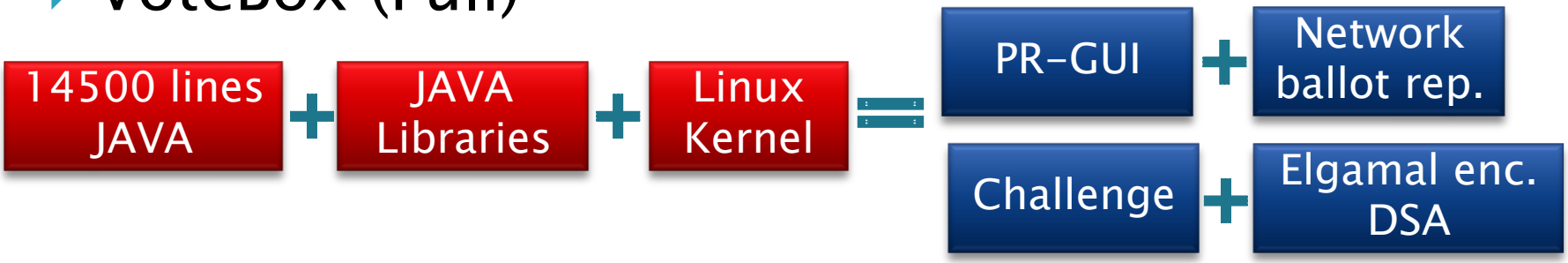
Source Code Length (Software)

EVM	Language	LOC
Pvote	Python	460
VoteBox Nano	**C**	**996**
VoteBox (Stripped)	Java	~7300
VoteBox (Full)	Java	14500
Diebold AccuVote TSX	C++	64000
Sequoia Edge	C	124000

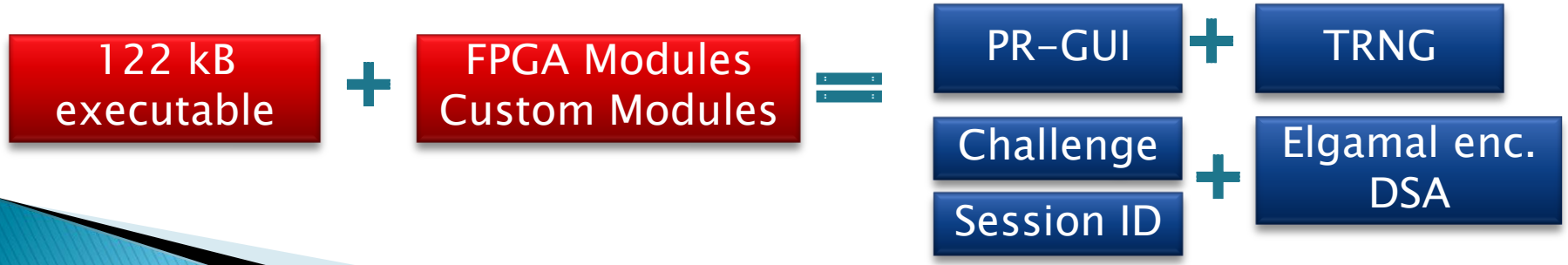
Comparison

- Pvote

- VoteBox (Full)



- VoteBox Nano



Conclusion

- We have shown that a very compact EVM can be built using an FPGA with following features:

Externally verifiable attestation

True Random Number Generator

Elgamal Encryption and DSA

Challenge Option

Pre-rendered GUI
No underlying OS

RICE

VoteBox Nano

Cast or Challenge [Benaloh]

- At the last step, the voter is given two options

The votes are valid
Usual flow

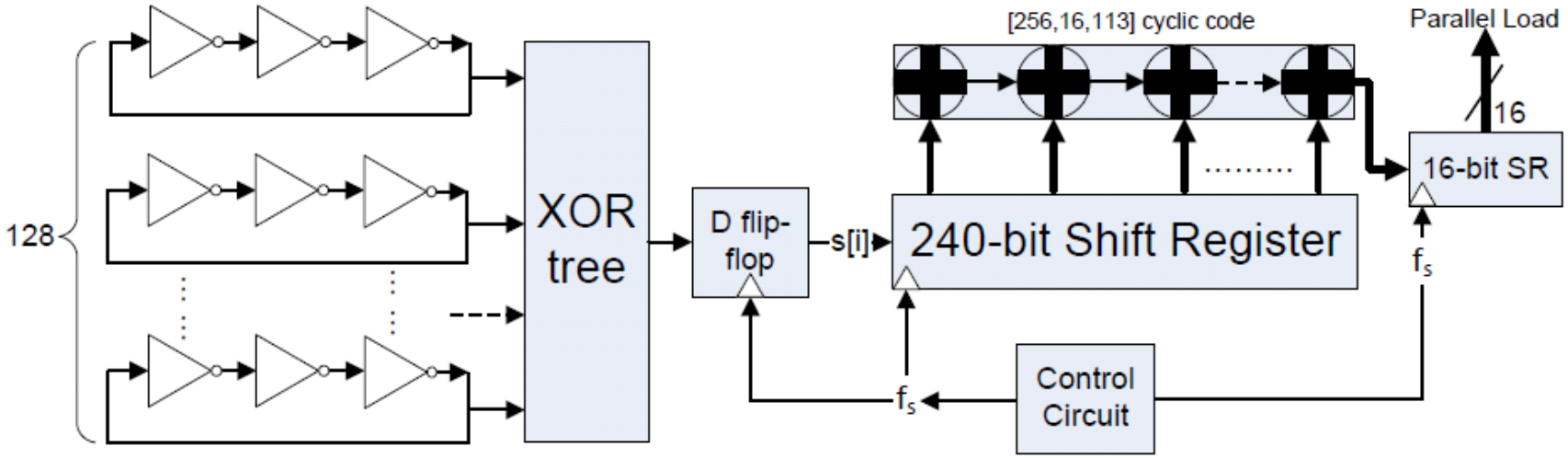
The votes are invalidated
FPGA reveals the random numbers

- FPGA only publishes the random numbers, the secret key is still safe

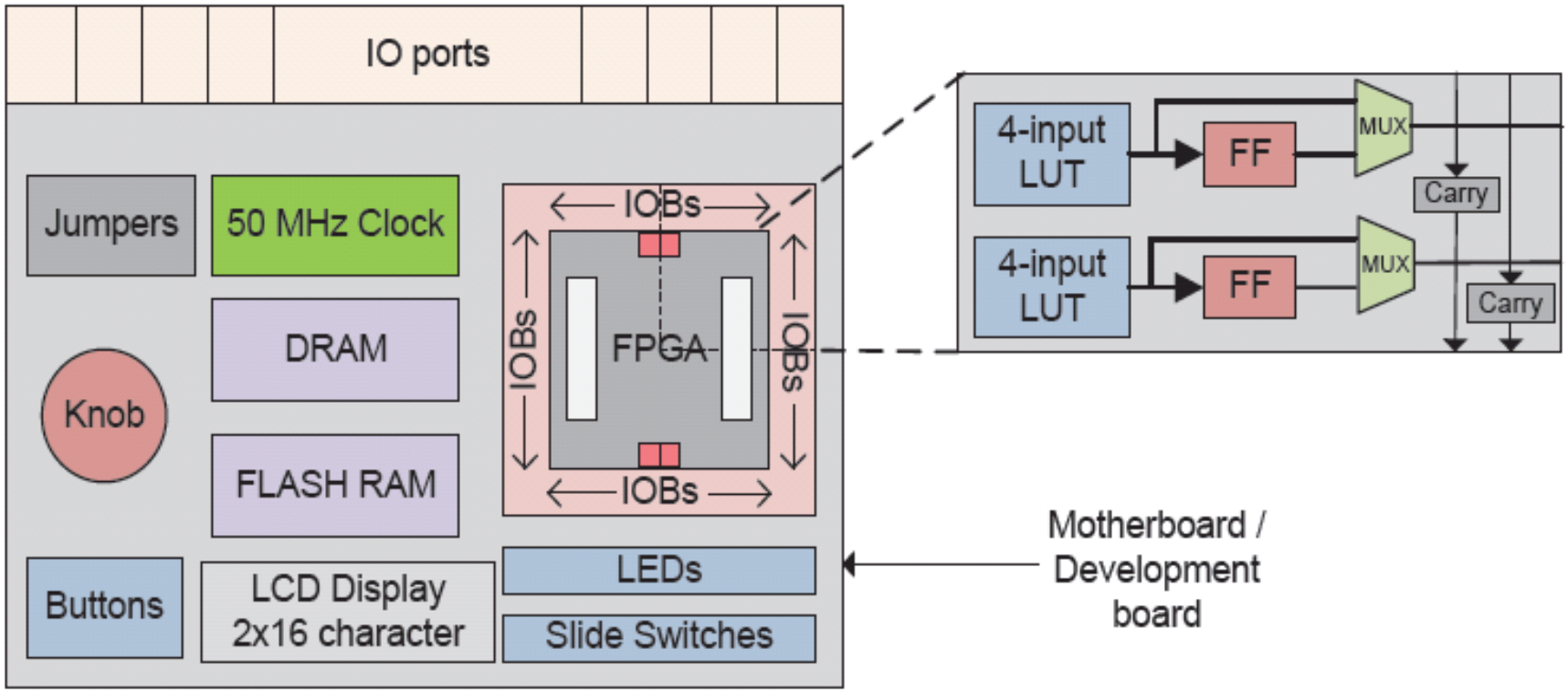
- With a certain amount of challenges, the results are reliable enough

True Random Number Generator

- TRNG has 128 ring oscillators, each consisting of 3 inverters
- f_s is 25 MHz and throughput is 195 kB/s.



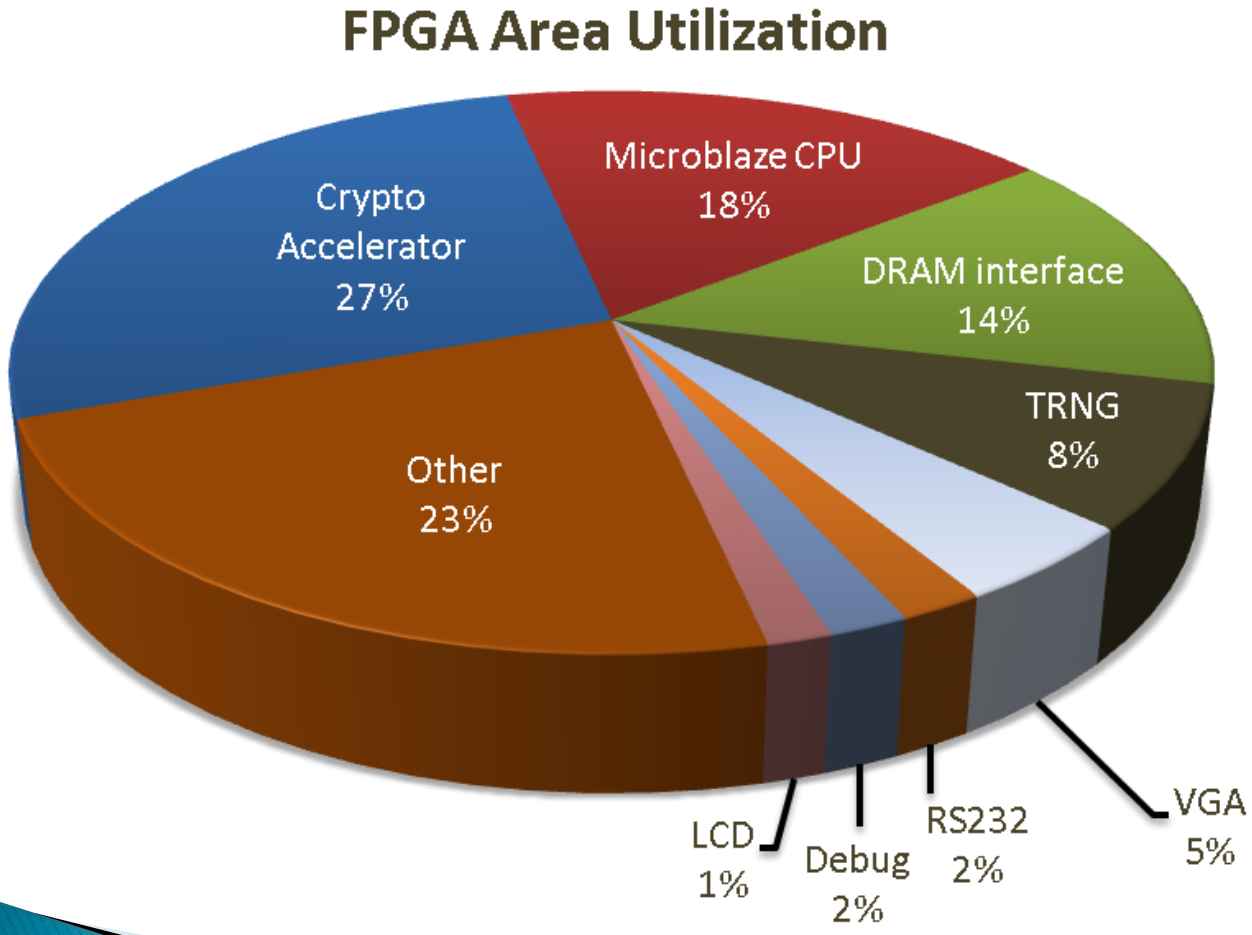
FPGA Structure



Trivial Attacks

- Theft of the device
  - No secret data is stored in long term
- Tapping serial port
  - The votes are encrypted
  - Encryption is probabilistic

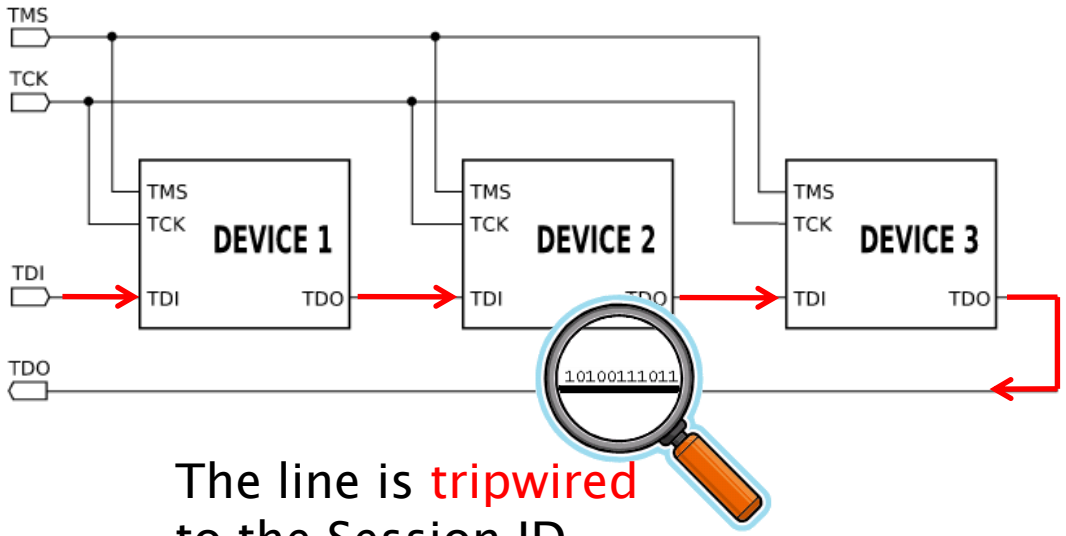
Hardware Modules



Hardware	LOC
Crypto Module	760
TRNG	520
Other	483
Total	**1763**

JTAG port

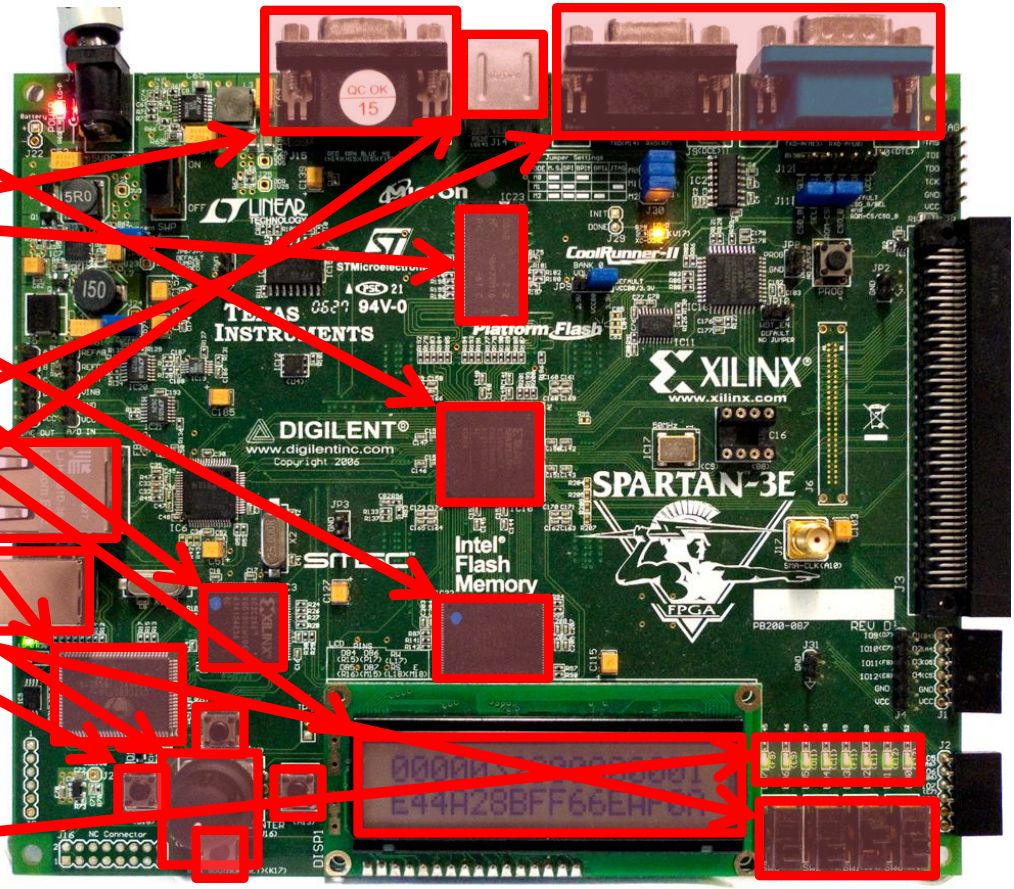
TDI: (Test Data In)
TDO: (Test Data Out)
TCK: (Test Clock)
TMS: (Test Mode Select)



The line is tripwired to the Session ID

FPGA (Field Programmable Gate Array)

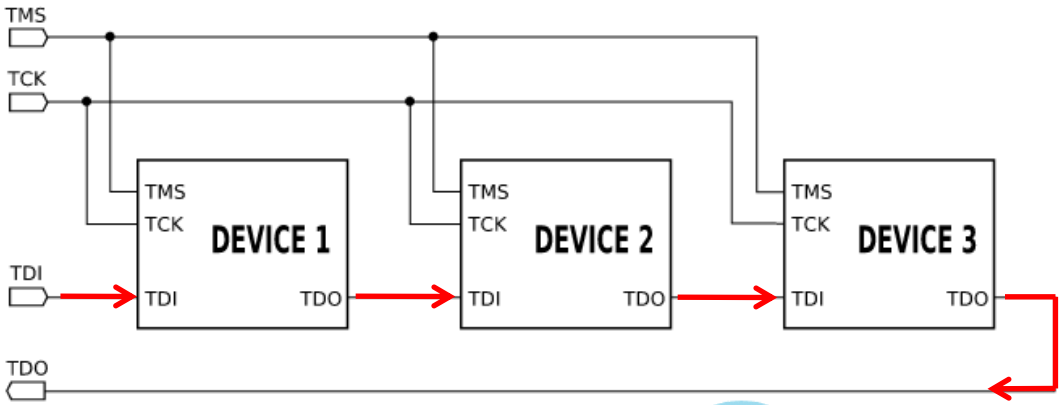
- 500k gate FPGA Chip
- Flash RAM (16 MB)
- DRAM (32 MB)
- VGA port
- Dot Matrix LCD (2x16)
- A rotary encoder
- RS232 serial ports
- Buttons and switches
- USB configuration port
- Ethernet Port
- PS/2 port
- 8 LEDs

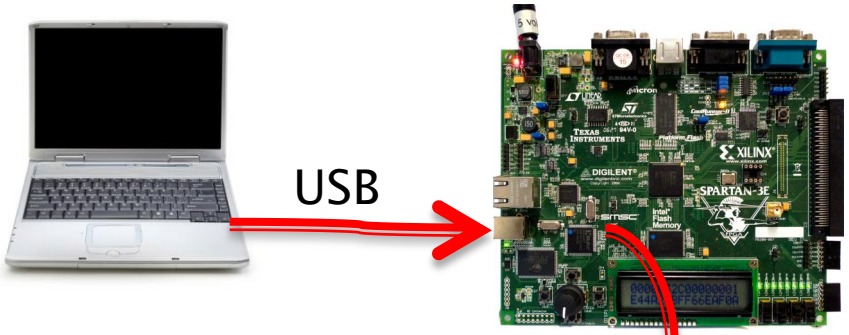


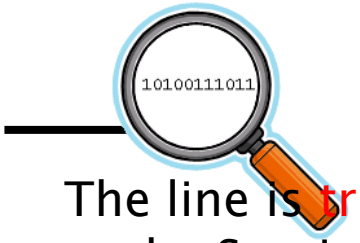
Xilinx Spartan-3E 500 Starter Kit

JTAG port

TDI: (Test Data In)
TDO: (Test Data Out)
TCK: (Test Clock)
TMS: (Test Mode Select)







The line is tripwired to the Session ID

JTAG

For FPGAs JTAG is used for

1. Bitstream upload and download
2. Software upload and download
3. Accessing software debugger