The Next Generation of Cryptanalytic Hardware

FPGAs (Field Programmable Gate Arrays) allow custom silicon to be implemented easily. The result is a chip that can be built specifically for cracking passwords. This presentation focuses on uncovering some of the underlying basics behind gate logic and shows how it can be used for performing extremely efficient cracking on FPGAs that runs hundreds of times faster than a PC.

David Hulton <dhulton@picocomputing.com>

Founder, Dachb0den Labs
Chairman, ToorCon Information Security Conference
Embedded Systems Engineer, Pico Computing, Inc.

Disclaimer

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- Educational purposes only

- Full disclosure

- I'm not a hardware guy

Goals

- This talk will cover:
  - Introduction to FPGAs
    - What is an FPGA?
    - Gate Logic
  - Optimizations
    - Pipelines
    - Parallelism
  - Cryptography
    - History
    - PicoCrack
  - Conclusion

Introduction to FPGAs

- Field Programmable Gate Array

  - Lets you prototype IC's
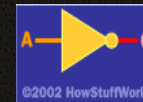
  - Code translates directly into circuit logic

What is Gate Logic?

- The basic building blocks of any computing system

not	~a	not
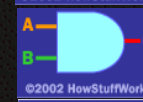
or	a | b	or
and	a & b	and
xor	a ^ b	xor

nor	~(a | b)	nor
nand	~(a & b)	nand
xnor	~(a ^ b)	xnor
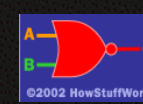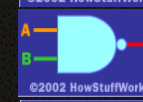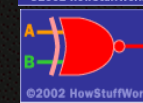
What is Gate Logic?

- Build other types of logic, such as adders:

What is Gate Logic?

- Which can be chained together:
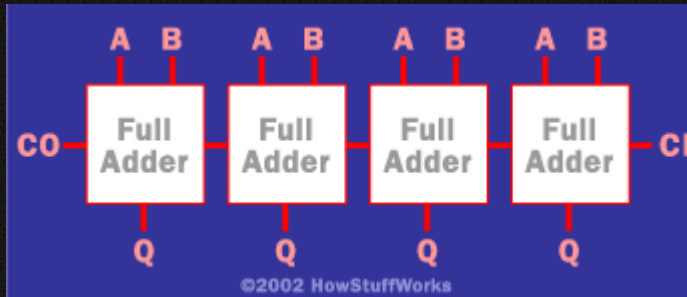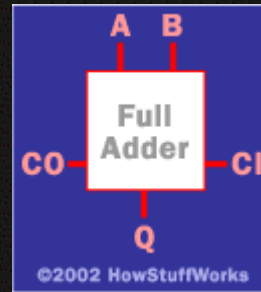
What is Gate Logic?

- And can be used for storing values:

  - Feedback

  - Flip-Flop / Latch
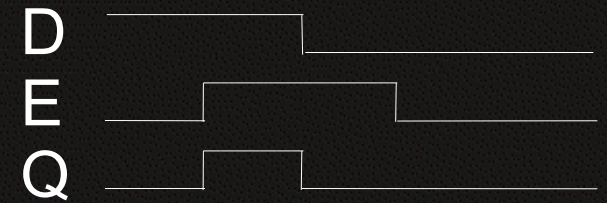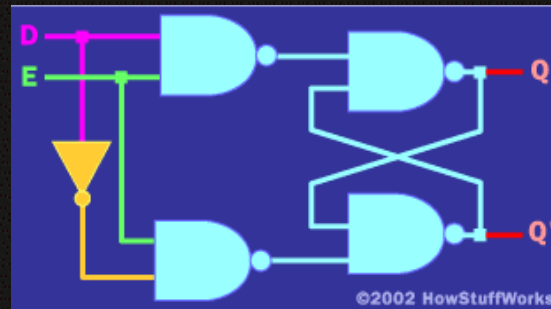
  - JK Flip-Flop
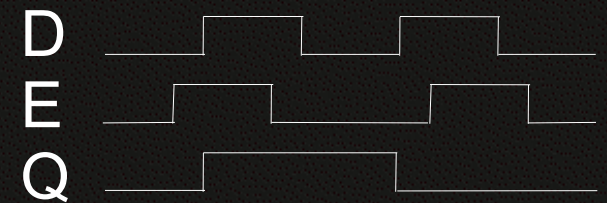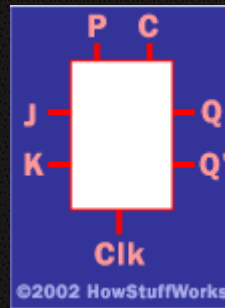
What is Gate Logic?

- This can be implemented with electronics:
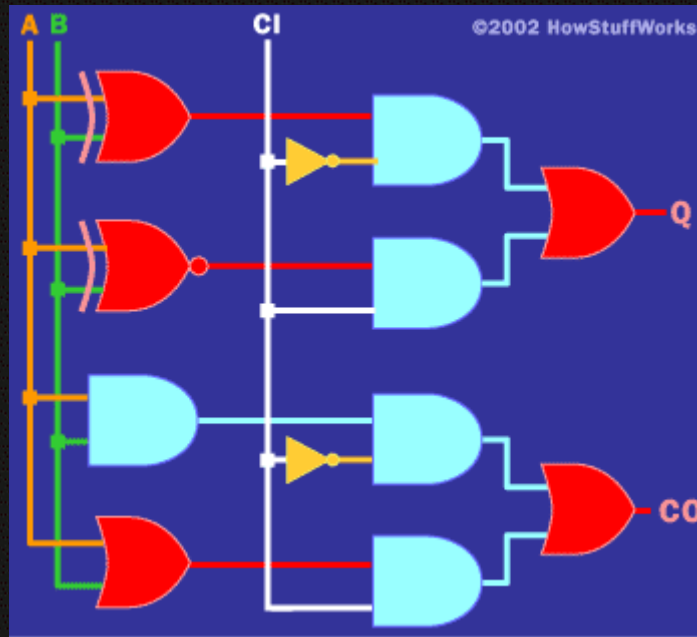
  - NOT

  - AND

What is an FPGA?

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV
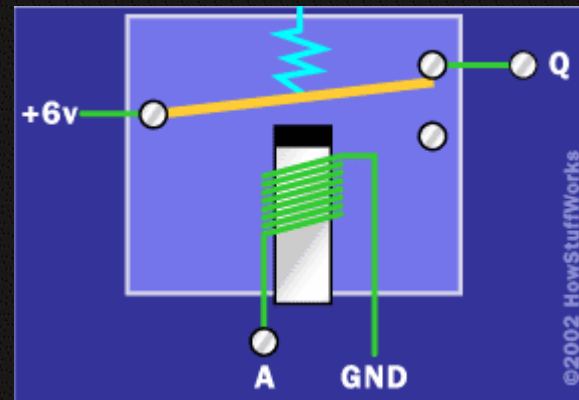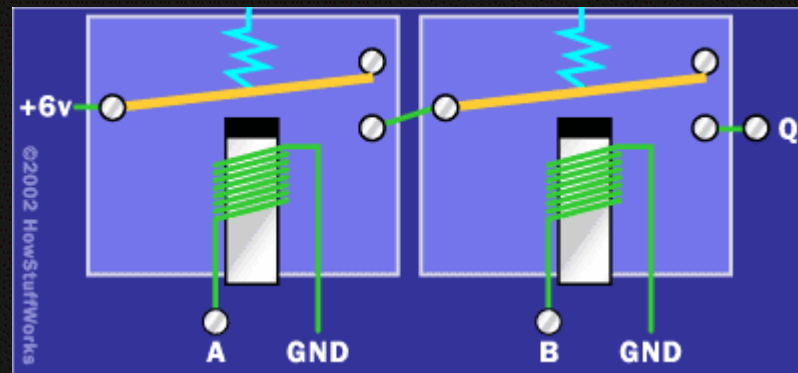
- An FPGA is an array of configurable gates

  - Gates can be connected together arbitrarily

  - States can be configured

  - Common components are provided

  - Any type of logic can be created

What is an FPGA?

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- **Configurable Logic Blocks (CLBs)**
  - Registers (flip flops) for fast data storage
  - Logic Routing
- **Input/Output Blocks (IOBs)**
  - Basic pin logic (flip flops, muxs, etc)
- **Block Ram**
  - Internal memory for data storage
- **Digial Clock Managers (DCMs)**
  - Clock distribution
- **Programmable Routing Matrix**
  - Intelligently connects all components together
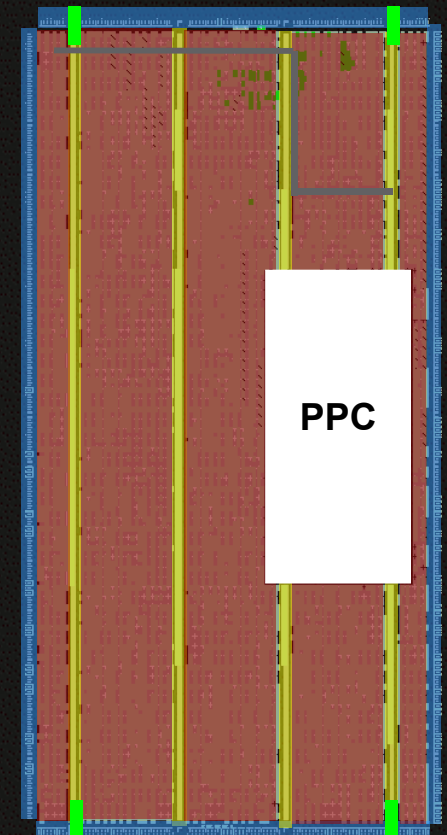
PPC

FPGA Pros / Cons

- Pros
  - Common Hardware Benefits
    - Massively parallel
    - Pipelineable
  - Reprogrammable
    - Self-reconfiguration
- Cons
  - Size constraints / limitations
  - More difficult to code & debug

Introduction to FPGAs

- Common Applications
  - Encryption / decryption
  - AI / Neural networks
  - Digital signal processing (DSP)
  - Software radio
  - Image processing
  - Communications protocol decoding
  - Matlab / Simulink code acceleration
  - Etc.

Introduction to FPGAs

- Common Applications
  - Encryption / decryption
  - AI / Neural networks
  - Digital signal processing (DSP)
  - Software radio
  - Image processing
  - Communications protocol decoding
  - Matlab / Simulink code acceleration
  - Etc.

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

Types of FPGAs

- Antifuse

  - Programmable only once

- Flash

  - Programmable many times

- SRAM

  - Programmable dynamically

  - Most common technology

  - Requires a loader (doesn't keep state after power-off)

Types of FPGAs

- Xilinx
  - Virtex-4
  - Optional PowerPC Processor
- Altera
  - Stratix-II

Verilog

- Hardware Description Language

- Simple C-like Syntax

- Like Go - Easy to learn, difficult to master

Verilog

- ## One bit AND

  - ### C

```c
u_char or(u_char a, u_char b) {
    return((a & 1) & (b & 1));
}
```

  - ### Verilog

```verilog
module or(a, b, c);
input a, b;
output c;

assign c = a & b;
endmodule
```
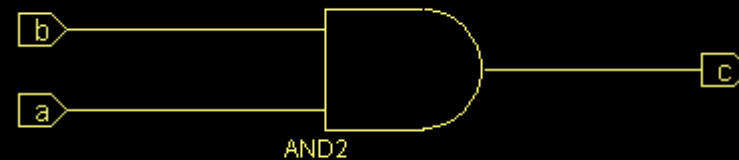
  - ### Gate

Verilog

- 8 bit AND

  - C

```
u_char or(u_char a, u_char b) {
    return(a & b);
}
```

  - Verilog

```
module or(a, b, c);
input [7:0] a, b;
output [7:0] c;

assign c = a & b;
endmodule
```
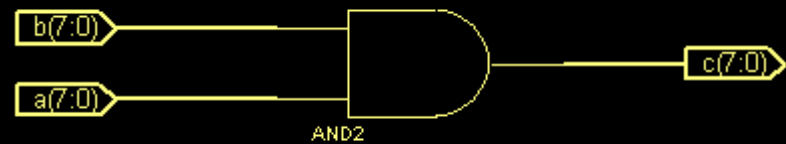
  - Gate

Verilog

- 8 bit Flip-Flop

  - C

```
u_char or(u_char a) {
    u_char t = a;
    return(t);
}
```

  - Verilog

```
module or(clk, a, c);
input clk;
input [7:0] a;
output [7:0] c;
reg [7:0] c;

always @(posedge clk) c <= a;
endmodule
```

  - Gate
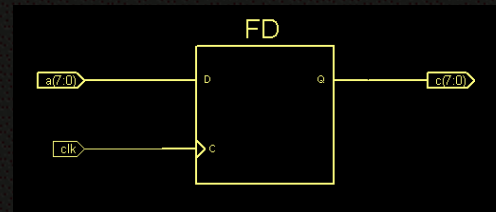
Massively Parallel Example

- PC (32 * ~ 7 clock cycles ?) @ 3.0Ghz

```
for(i = 0; i < 32; i++)
    c[i] = a[i] * b[i];
```

- Hardware (1 clock cycle) @ 300Mhz
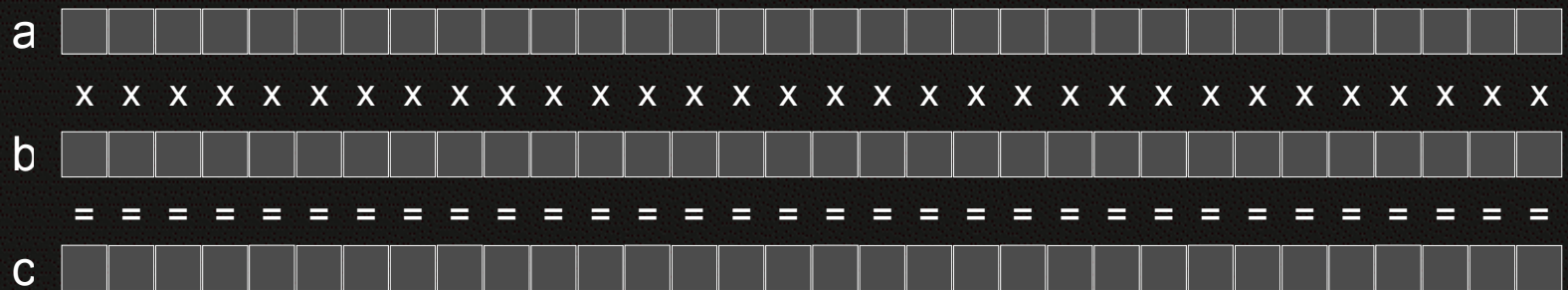
Massively Parallel Example

- PC
  - Speed scales with # of instructions & clock speed
- Hardware
  - Speed scales with FPGA's:
    - Size
    - Clock Speed

Pipeline Example

- PC   (x * ~ 10 clock cycles ?) @ 3.0Ghz

  for(i = 0; i < x; i++)

      f[i] = a[i] + b[i] * c[i] – d[i] ^ e[i]

- Hardware   (x + 3 clock cycles) @ 300Mhz

+	x	-	^
Stage 1	Stage 2	Stage 3	Stage 4

In ————→   → Out

1ns   2ns   3ns   4ns

Pipeline Example

- PC   (x * ~ 10 clock cycles ?) @ 3.0Ghz

  for(i = 0; i < x; i++)

  f[i] = a[i] + b[i] * c[i] – d[i] ^ e[i]

- Hardware   (x + 3 clock cycles) @ 300Mhz

+	x	-	^
Stage 1	Stage 2	Stage 3	Stage 4

In ——— Out

1ns   2ns   3ns   4ns

Pipeline Example

- PC   (x * ~ 10 clock cycles ?) @ 3.0Ghz

  for(i = 0; i < x; i++)

    f[i] = a[i] + b[i] * c[i] – d[i] ^ e[i]

- Hardware   (x + 3 clock cycles) @ 300Mhz

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

Pipeline Example

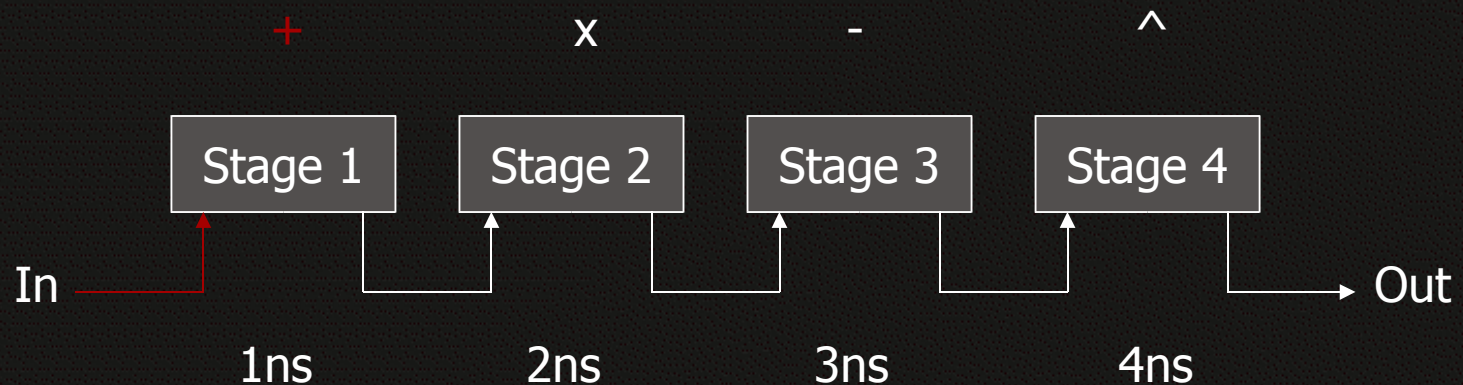- PC   (x * ~ 10 clock cycles ?) @ 3.0Ghz

  for(i = 0; i < x; i++)

        f[i] = a[i] + b[i] * c[i] – d[i] ^ e[i]

- Hardware   (x + 3 clock cycles) @ 300Mhz
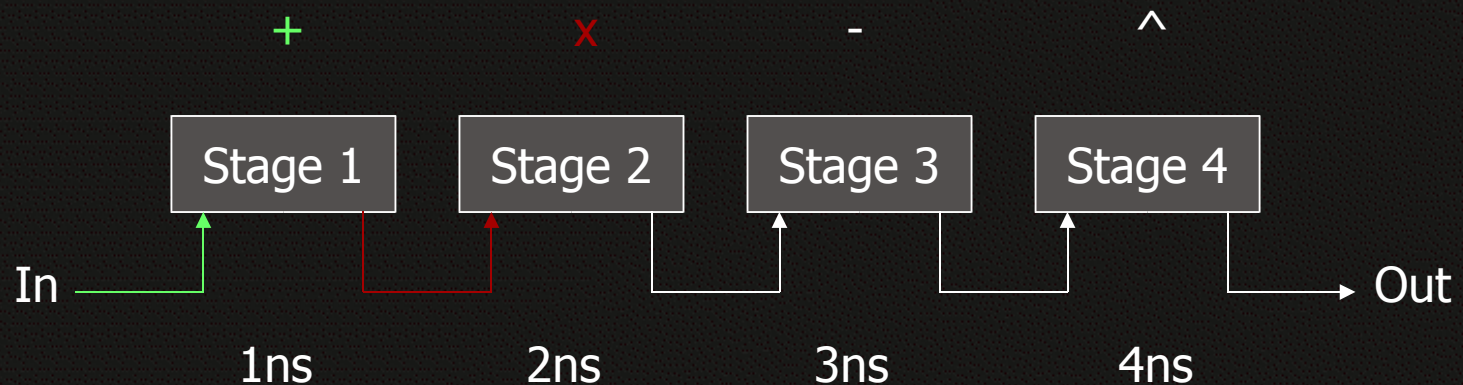
Pipeline Example

- PC   (x * ~ 10 clock cycles ?) @ 3.0Ghz

  for(i = 0; i < x; i++)

    f[i] = a[i] + b[i] * c[i] – d[i] ^ e[i]

- Hardware   (x + 3 clock cycles) @ 300Mhz

Pipeline Example

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- PC

  - Speed scales with # of instructions & clock speed

- Hardware

  - Speed scales with FPGA's:

    - Size

    - Clock speed

    - Slowest operation in the pipeline

Self-Reconfiguration Example

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- PC

  data = MultiplyArrays(a, b);

  RC4(key, data, len);

  m = MD5(data, len);

- Hardware

Control Logic

MultiplyArrays.bit

RC4.bit

MD5.bit

Self-Reconfiguration Example

- PC

  data = MultiplyArrays(a, b);

  RC4(key, data, len);

  m = MD5(data, len);

- Hardware

Control Logic

| MultiplyArrays.bit |
| RC4.bit |
| MD5.bit |

Self-Reconfiguration Example

- PC

  data = MultiplyArrays(a, b);

  RC4(key, data, len);

  m = MD5(data, len);

- Hardware

Control Logic

| MultiplyArrays.bit |
| RC4.bit |
| MD5.bit |

History of FPGAs and Cryptography

- Minimal Key Lengths for Symmetric Ciphers
    - Ronald L. Rivest (R in RSA)
    - Bruce Schneier (Blowfish, Twofish, etc)
    - Tsutomu Shimomura (Mitnick)
    - A bunch of other ad hoc cypherpunks

History of FPGAs and Cryptography

Budget	Tool	40-bits	56-bits	Recom
Pedestrian Hacker				
Tiny	Computers	1 week	infeasible	45
$400	FPGA	5 hours	38 years	50
Small Company				
$10K	FPGA	12 min	556 days	55
Corporate Department				
$300K	FPGA	24 sec	19 days	60
	ASIC	0.18 sec	3 hrs	
Big Company				
$10M	FPGA	0.7 sec	13 hrs	70
	ASIC	0.005 sec	6 min	
Intelligence Agency				
$300M	ASIC	0.0002 sec	12 sec	75

History of FPGAs and Cryptography

- 40-bit SSL is crackable by almost anyone

- 56-bit DES is crackable by companies

- Scared yet?

This paper was published in 1996

History of FPGAs and Cryptography

- 1998
  - The Electronic Frontier Foundation (EFF)
  - Cracked DES in < 3 days
  - Searched ~9,000,000,000 keys/second
  - Cost < $250,000
- 2001
  - Richard Clayton & Mike Bond (University of Cambridge)
  - Cracked DES on IBM ATMs
  - Able to export all the DES and 3DES keys in ~ 20 minutes
  - Cost < $1,000 using an FPGA evaluation board

- 2004

  - Philip Leong, Chinese University of Hong Kong

  - IDEA
    - 50Mb/sec on a P4 vs. 5,247Mb/sec on Pilchard

  - RC4
    - Cracked RC4 keys 58x faster than a P4
    - Parallelized 96 times on a FPGA
    - Cracks 40-bit keys in 50 hours
    - Cost < $1,000 using a RAM FPGA (Pilchard)

PicoCrack

- Currently Supports
  - Unix DES
  - Windows Lanman
  - Windows NTLM (full-support coming soon)

Lanman Hashes

- Lanman

  - 14-Character Passwords

  - Case insensitive (converted to upper case)

  - Split into 2 7-byte keys

  - Used as key to encrypt static values with DES

MYLAMEP	ASSWORD
↓	↓
DES	**DES**
↓	↓
Hash[0-7]	Hash[8-15]

PicoCrack

- Hardware Design

  - Pipeline design

  - Internal cracking engine

    - passwords = lmcrack(hashes, options);

  - Interface over PCMCIA

  - Can specify cracking options

    - Bits to search

      - e.g. Search 55-bits (instead of 56)

    - Offset to start search

      - e.g. First card gets offset 0, second card gets offset 2**55

    - Typeable/printable characters

    - Alpha-numeric

    - Allows for basic distributed cracking & resume functionality

PicoCrack

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- Software Design
    - GUI and Console Interfaces
    - WxWidgets
        - Windows
        - Linux (coming soon)
        - MacOS X (coming soon)
    - Supports cracking multiple keys at a time
    - Can automatically load required FPGA image
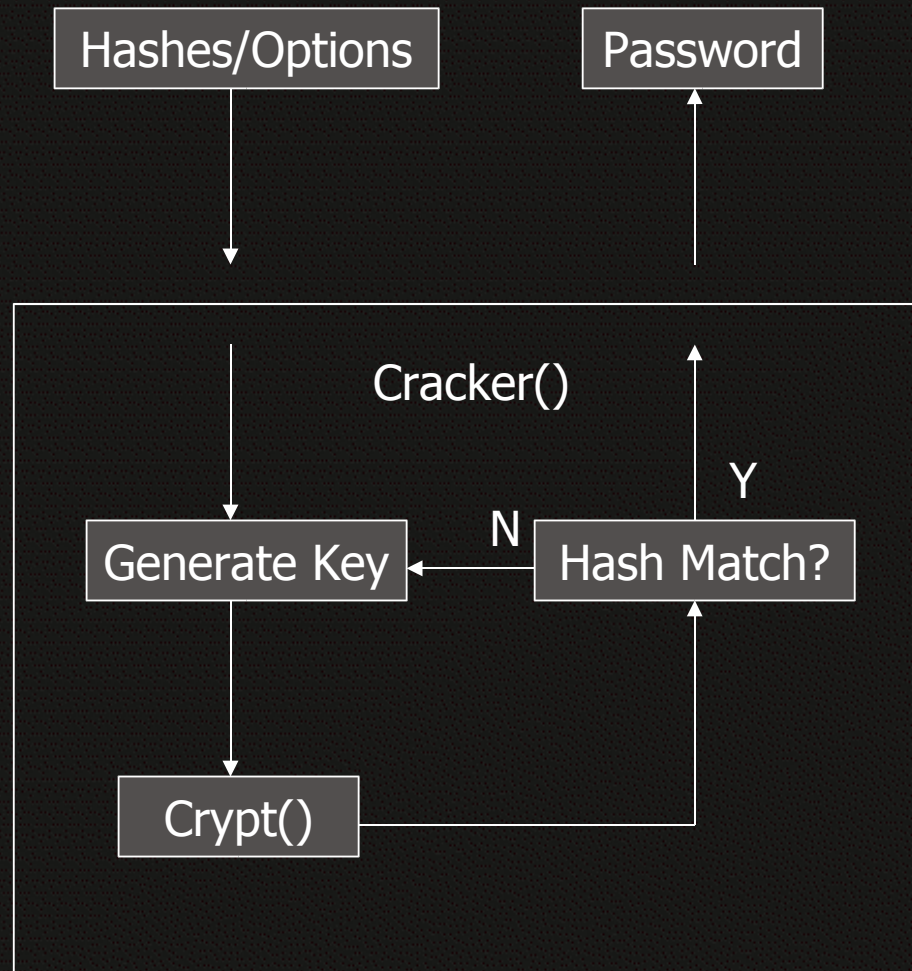   - Supports multiple card clusters

Password File Cracker

Hashes/Options   Password

Cracker()

Generate Key ←N— Hash Match? —Y→

Crypt()

Lanman Cracking

- PC (3.0Ghz P4 \w rainbowcrack)

  - ~ 2,000,000 c/s

- Hardware (Low end FPGA \w PicoCrack)

  - 100Mhz = 100,000,000 c/s

  - When timing is optimized it should run at 200Mhz

Type	P4	E-12	8 E-12
64-characters	25 D	12 H	90 M
48-characters	3.4 D	100 M	12 M
32-characters	4.7 H	5.7 M	43 S

Pico E-12

- Pico E-12

  - Compact Flash Type-II Form Factor

  - Virtex-4 (LX25 or FX12)

    - 1 Million Gates (~25,000 CLBs)

    - Optional 450 MHz PowerPC Processor

  - 128 MB PC-133 RAM

  - 64 MB Flash ROM

  - Gigabit Ethernet

  - JTAG Debugging Port

E-12 Card

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3133337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

Demonstration

Feedback?

- What do you think?

- Possible Applications?

- Questions?

Conclusions / Shameful Plugs

The Next Generation of Cryptanalytic Hardware
David Hulton <0x3137@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- ToorCon 7

  - End of September, 2005

  - San Diego, CA USA

  - http://www.toorcon.org

Questions ? Suggestions ?

- David Hulton
  - 0x31337@gmail.com
  - h1kari@dachb0den.com
- OpenCores
  - http://www.opencores.org
- Xilinx
  - ISE Foundation (Free 60-day trial)
- Pico Computing, Inc.
  - http://www.picocomputing.com