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

- Educational purposes only
- Full disclosure
- I'm not a hardware guy

Goals

- Introduction to FPGAs
  - What is an FPGA?
  - Gate Logic
- Cracking \w Hardware
  - History
- Optimizations
  - Pipelines
  - Parallelism
- Chipper
  - Lanman/NTLM
  - Demo
  - Performance

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

Introduction to FPGAs

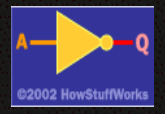
- Field Programmable Gate Array
  - Lets you prototype IC's
  - Code translates directly into circuit logic

What is Gate Logic?

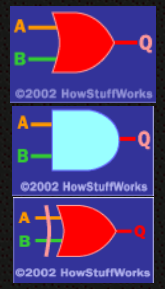
The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- The basic building blocks of any computing system

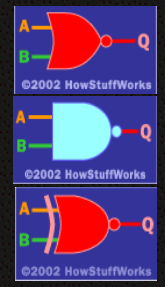
not	~a	not



or	a | b	or
and	a & b	and
xor	a ^ b	xor

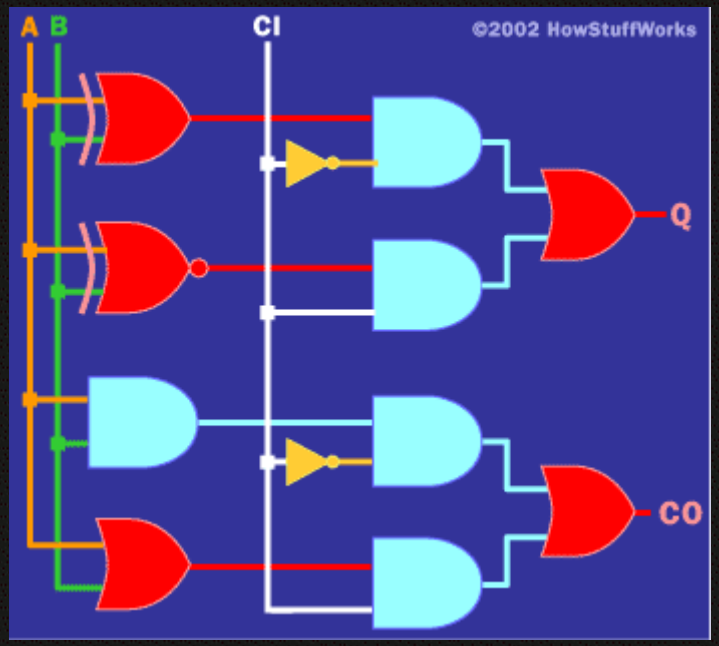


nor	~(a | b)	nor
nand	~(a & b)	nand
xnor	~(a ^ b)	xnor



What is Gate Logic?

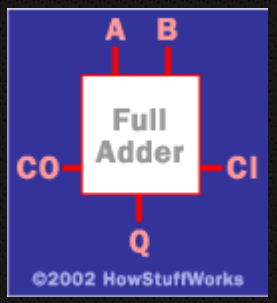
- Build other types of logic, such as adders:

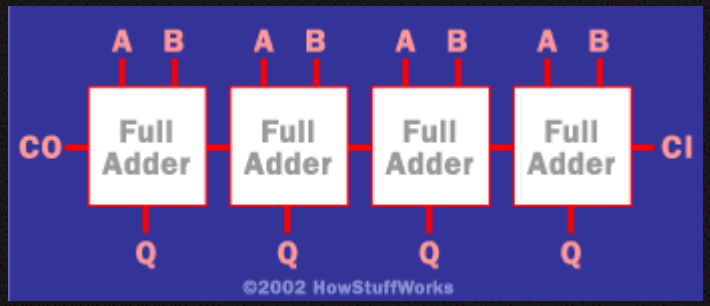


What is Gate Logic?

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- Which can be chained together:



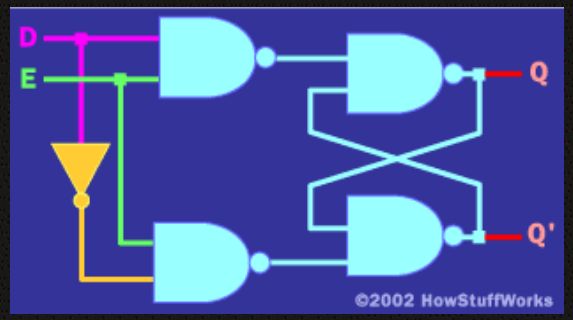


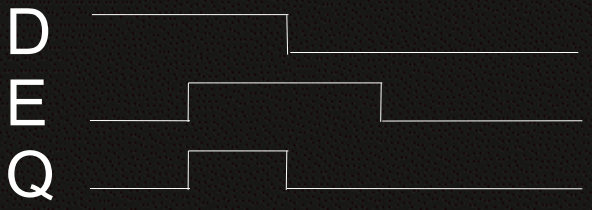
What is Gate Logic?

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

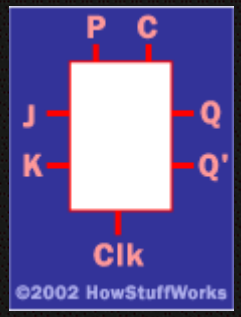
- And can be used for storing values:
  - Feedback

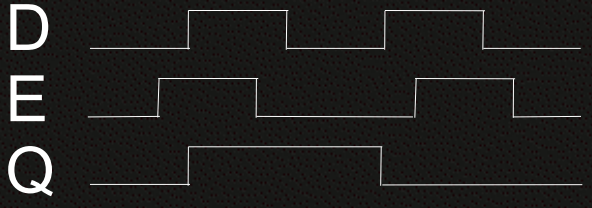
  - Flip-Flop / Latch





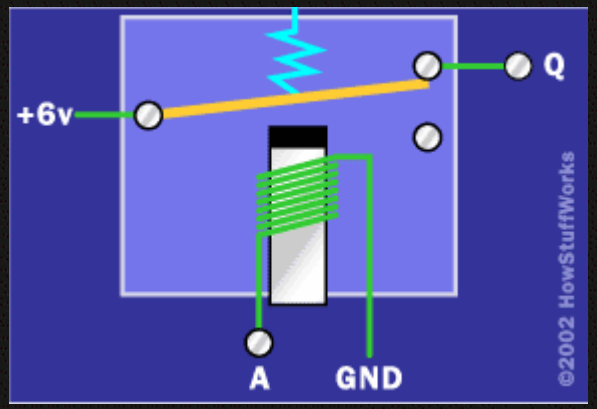
  - JK Flip-Flop



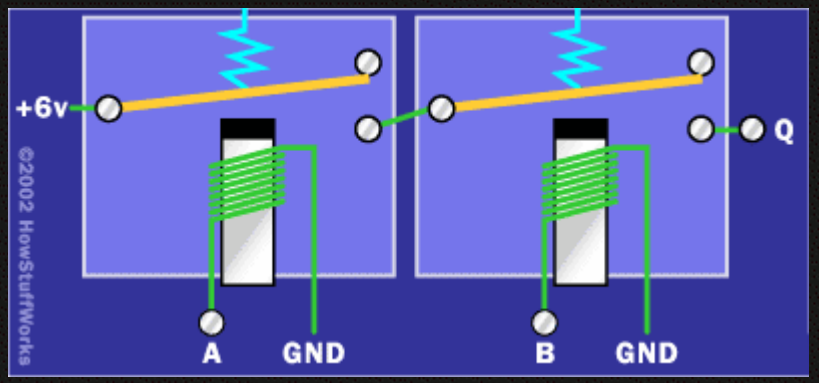


What is Gate Logic?

- This can be implemented with electronics:
  - NOT



  - AND



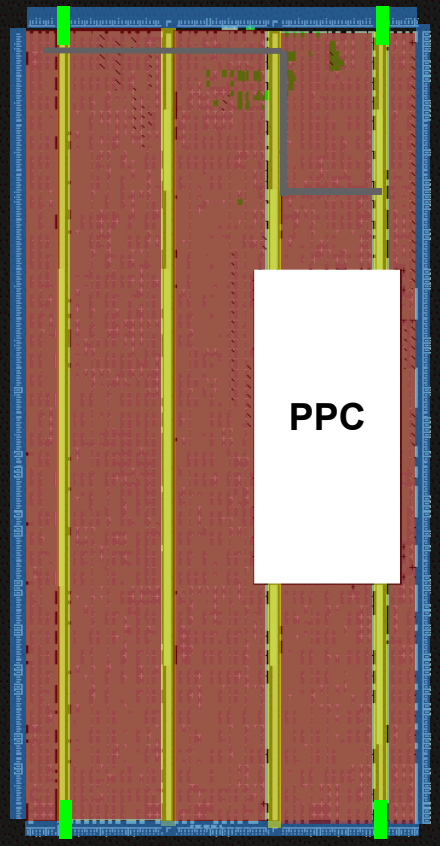
What is an FPGA?

- 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 <0x31337@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



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.

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

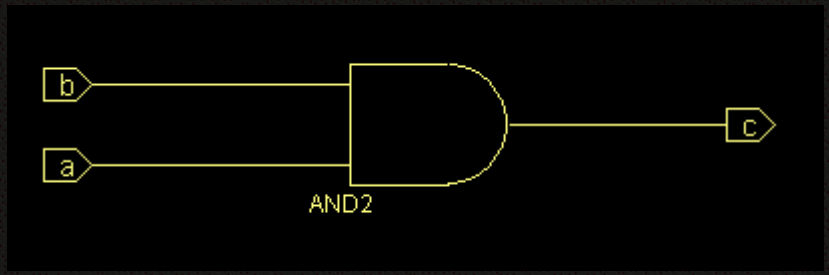
```
u_char and(u_char a, u_char b) {
    return((a & 1) & (b & 1));
}
```

  - Verilog

```
module and(a, b, c);
input a, b;
output c;

assign c = a & b;
endmodule
```

  - Gate



Verilog

- 8 bit AND
  - C

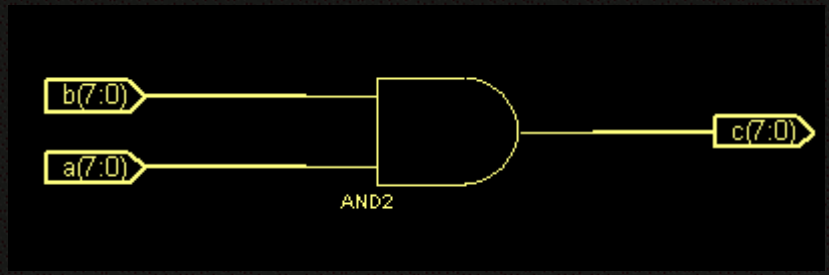
```
u_char or(u_char a, u_char b) {
    return(a & b);
}
```

  - 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

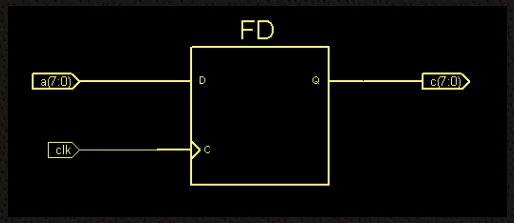
```
u_char or(u_char a) {
    u_char t = a;
    return(t);
}
```

  - 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



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

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

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

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

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

History of FPGAs and Cryptography

- 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

History of FPGAs and Cryptography

- 2002
  - Rouvroy Gael, Standaert Francois-Xavier and others from the UCL Crypto Group
  - Implemented a linear cryptanalysis attack on DES
  - Used FPGAs to generate dictionary tables
  - Chosen-plaintext attack can recover key in 10 seconds with 72% success rate

History of FPGAs and Cryptography

- 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)

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

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

- 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

- 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

- PC

```
data = MultiplyArrays(a, b);
RC4(key, data, len);
m = MD5(data, len);
```

- Hardware

Self-Reconfiguration Example

- PC

```
data = MultiplyArrays(a, b);
RC4(key, data, len);
m = MD5(data, len);
```

- Hardware

Self-Reconfiguration Example

- PC

```
data = MultiplyArrays(a, b);
RC4(key, data, len);
m = MD5(data, len);
```

- Hardware

•Special Components - DSP48s

- DSP48
  - Configurable
  - 18x18-bit Multiplier
  - 48+48-bit Adder
  - Input/Output Registers
  - 18x18 Multiplies @ 500MHz
  - Virtex-4 LX25 comes with 48

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

•Special Components – BlockRAM

- BlockRAM
  - Stores up to 18Kb
  - From 1 to 36 bits
  - Dual-port
  - FIFO Support
  - Virtex-4 LX25 comes with 72

•Special Components – APU

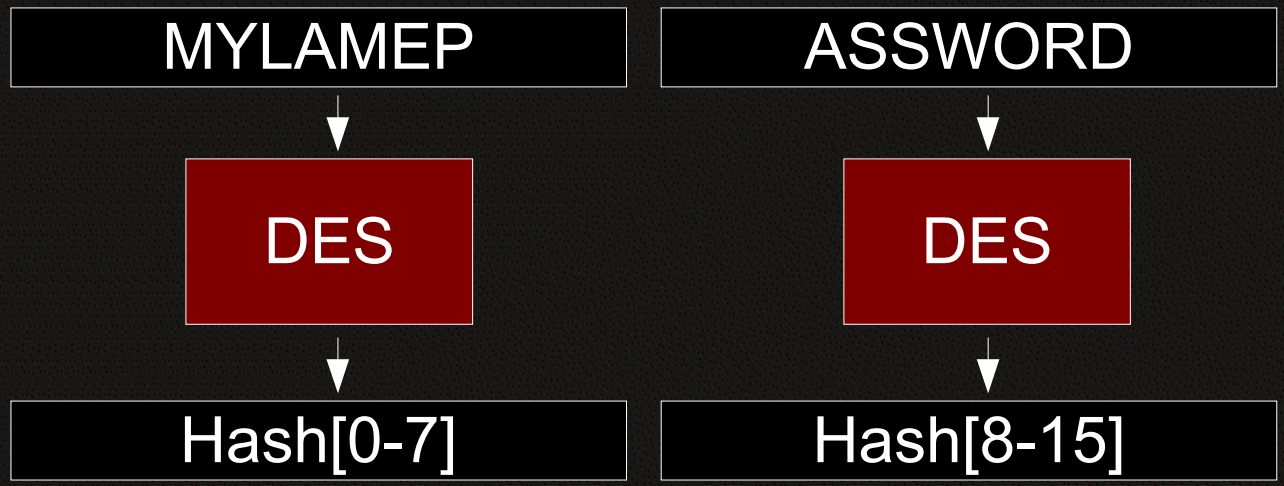
- Auxiliary Processing Unit (APU)
  - PowerPC allows you to implement custom instructions
  - Have access to all of the registers
  - Single instruction from processor triggers your logic
  - e.g. Single instruction DES

Chipper

- Currently Supports
  - Unix DES
  - Windows Lanman
  - Windows NTLM (full-support coming soon)
  - Multiple Cards/FPGAs ;-)

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



Chipper

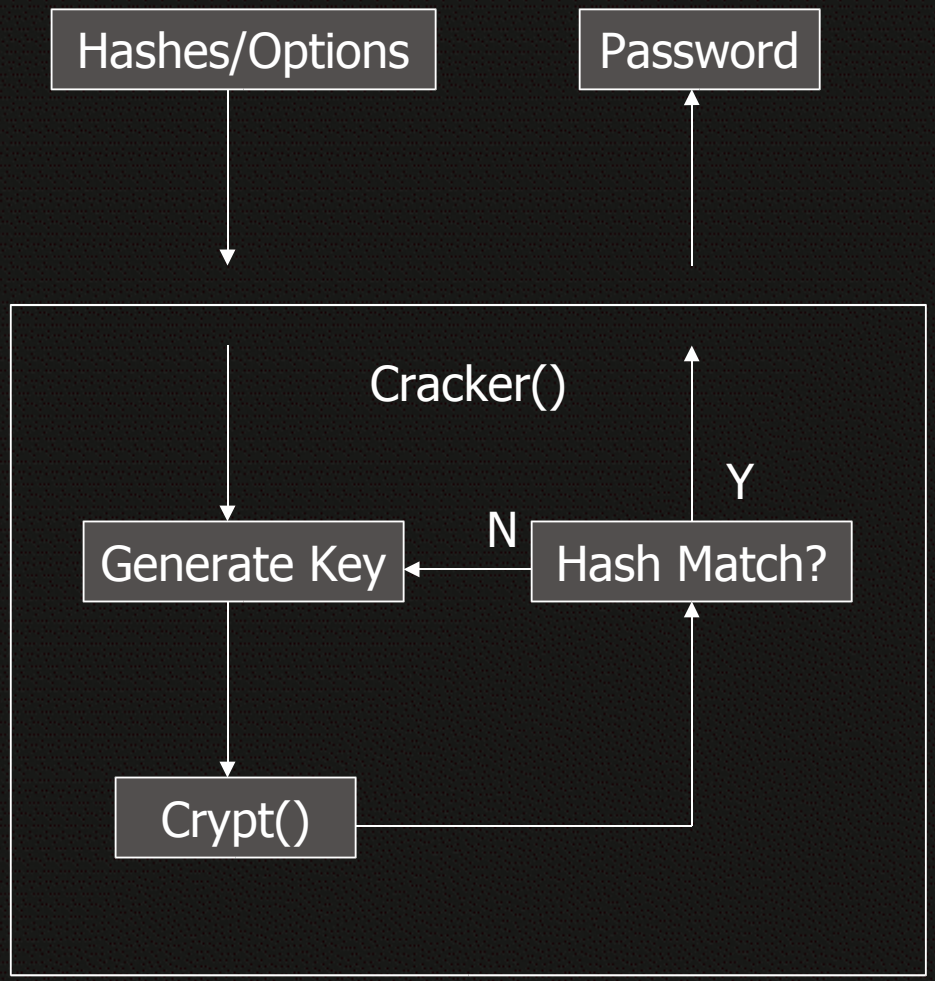
- Hardware Design
  - Pipeline design
  - Internal cracking engine
    - passwords = lmcrack(hashes, options);
  - Interface over PCMCIA
  - Can specify cracking options
    - Bits to search
      - e.g. Search 55-bits (instead of 56)
    - Offset to start search
      - e.g. First card gets offset 0, second card gets offset 2**55
    - Typeable/printable characters
    - Alpha-numeric
    - Allows for basic distributed cracking & resume functionality

Chipper

- Software Design – Thanks Arachne!!
  - GUI and Console Interfaces
  - WxWidgets
    - Windows
    - Linux
    - MacOS X (coming soon)
  - Supports cracking 128 keys in parallel on each card
  - Supports 4x fast mode for just one hash pair
  - Can automatically load required FPGA image
  - Supports multiple card clusters

Password File Cracker

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV



Lanman Cracking

- PC (3.0Ghz P4 \w rainbowcrack)
  - ~ 2,000,000 c/s
- Hardware (Low end FPGA \w Chipper)
  - 125Mhz = 125,000,000 c/s per core
  - 500Mhz = 500,000,000 c/s for fast mode!

Type	P4	E-12	8 E-12
64-characters	25 D	2 H	18 M
48-characters	3.4 D	20 M	1.5 M
32-characters	4.7 H	1 M	9 S

Pico E-12

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

- 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

PicoCrack Demonstration

The Next Generation of Cryptanalytic Hardware
David Hulton <0x31337@gmail.com>
Defcon 13 - July 30th, 2005 - Las Vegas, NV

Demonstration

OpenCiphers.org

- Sourceforge project
  - Chipper
  - Lanman & NTLM cracking cores
  - Modular Exponentiation
  - A5/2 (for some GSM research)

Technology Trends

- Technology Trends
  - Embedded platforms are either cheap and slow or expensive and fast
  - There will always be a cost factor with regards to crypto
  - This has plagued smart cards, speedpasses, mobile devices, etc.
  - The future is definitely implementing more advanced cryptanalysis attacks
  - As cheap chips get faster, the workload for brute-force increases exponentially with the keysize
  - Elegance will be the next generation

Hardware Trends

- FPGAs are increasing according to Moore's Law
  - Different factors though
    - Density - Increasing
    - Clock Speed - Increasing
    - Components – Created and expanded to fit markets
    - Cost - Dropping
  - Slowly starting to compete with ASICs
  - Future Applications:
    - Neural Networks
    - Attacks on WEP/WPA/GSM
    - Analysis and Correlation

Feedback?

- What do you think?
- Possible Applications?
- Questions?

Conclusions / Shameful Plugs

- ToorCon 7
  - End of September, 2005
  - San Diego, CA USA
  - http://www.toorcon.org
- ShmooCon 2
  - February, 2006
  - San Diego, CA USA

Questions ? Suggestions ?

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