CLEMSON UNIVERSITY

Integrated Hardware/Software Security Support

R. R. Brooks
Associate Professor

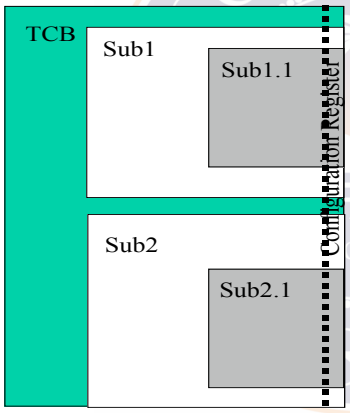
Sam T. Sander
Assistant Professor

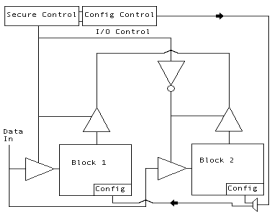
Holcombe Department of Electrical and Computer Engineering
Clemson University
Clemson, SC 29634-0915
Tel. 864-656-0920
Fax. 864-656-5910
email: rrb@acm.org

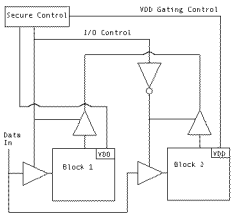
CLEMSON UNIVERSITY

FPGA security enforcement

DAG access with hardware enforcement



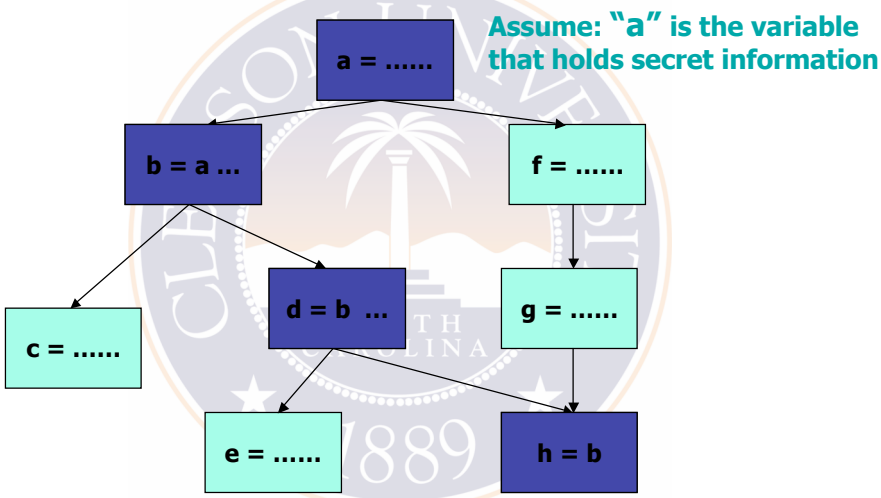




Differential Power Analysis

- Using statistic method in order break the secret key
- Using several runs on several sample inputs, for instance 1000 sample inputs
- An attacker guesses a particular key and based on that key he can determines a theoretical value for one of the intermediate bits generated by the program

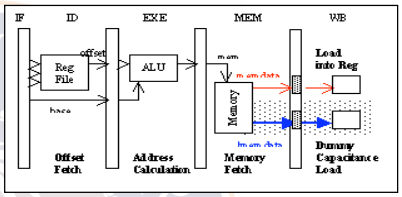
Dataflow Analysis



CLEMSON UNIVERSITY

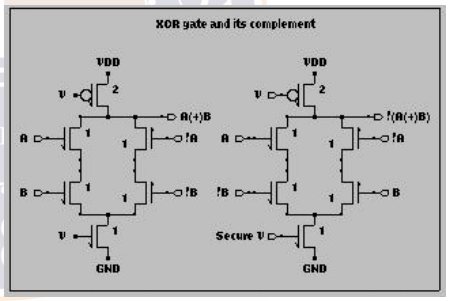
Differential Power Analysis Vulnerability

Data Initial Permutation (L0,R0) = PermuteIP(Data) **Key Permutation** (C0,D0) = PermuteK1(Key) = *denotes insecure assignment*	**Data Initial Permutation** (L0,R0) = PermuteIP(Data) **Key Permutation** (C0,D0) ← PermuteK1(Key) ← *denotes secure assignment*
M^th Rounds **Left Side Operation** Lm = Rm-1 **M^th Key Generation** Cm = Rotate(Cm-1,n) Dm = Rotate(Dm-1,n) Km = PermuteK2(Cm,Dm) **Right Side Operation** E(R) = PermuteE(Rm-1) f(Rm-1,K) = S(E(R)(+)Km) Rm = Lm-1 (+) f(Rm-1,K)	**M^th Rounds** **Left Side Operation** Lm ← Rm-1 **M^th Key Generation** Cm ← Rotate(Cm-1,n) Dm ← Rotate(Dm-1,n) Km ← PermuteK2(Cm,Dm) **Right Side Operation** E(R) ← PermuteE(Rm-1) f(Rm-1,K) ← S(E(R) <+> Km) Rm ← Lm-1 <+> f(Rm-1,K)
Output Inverse Permutation Output=PermuteIP (R16,L16)	**Output Inverse Permutation** Output=PermuteIP (R16,L16)



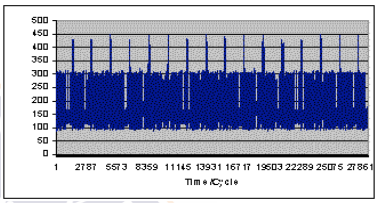

```
        ……..
        // Left Side Operation
        for (i=0; i<32; i++)
                newL[i] = oldR[i]
        ……..

..................          ..................
$L12:                       $L12:
  ..............              ..............
$L15:                       $L15:
  lw      $2,i                lw      $2,i
  ..............              ..............
  la      $4,newL             la      $4,newL
  addu    $3,$2,$4            addu    $3,$2,$4
  move    $2,$3               move    $2,$3
  lw      $3,i                lw      $3,i
  move    $4,$3               move    $4,$3
  sll     $3,$4,2             sll     $3,$4,2
  la      $4,oldR             la      $4,oldR
  addu    $3,$3,$4            addu    $3,$3,$4
  move    $4,$3               move    $4,$3
  lw      $3,0($4)            slw     $3,0($4)
  sw      $3,0($2)            ssw     $3,0($2)
$L14:                       $L14:
  lw      $3,i                lw      $3,i
  addu    $2,$3,1             addu    $2,$3,1
  move    $3,$2               move    $3,$2
  sw      $3,i                sw      $3,i
  j       $L12                j       $L12
$L13:                       $L13:
..................          ..................
```

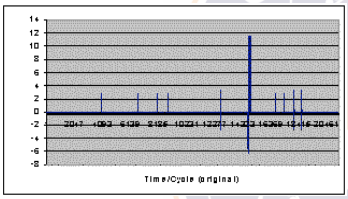
(a) Original Assembly Code **(b) Modified Assembly Code**

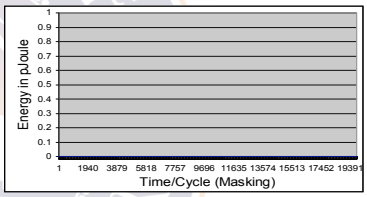


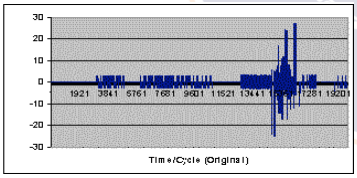
RRB/STS ORNL Workshop

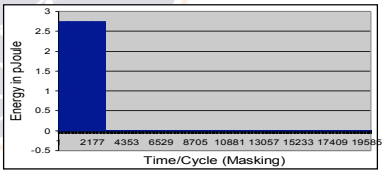
CLEMSON UNIVERSITY











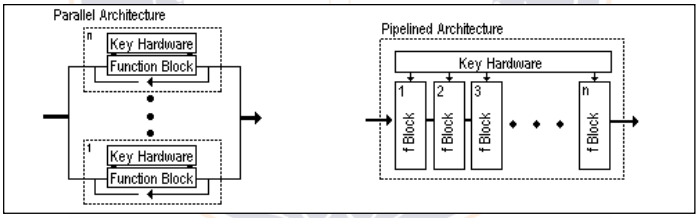
RRB/STS ORNL Workshop

Conclusions

- Since we do not hide the energy behavior of all instructions, our approach consumes less energy overhead than other approaches
- Our approach has 83% less energy overhead than dual-rail logic

Overview of Symmetric Encryption Architectures

- The dotted lines indicate the smallest subset of hardware capable of performing a single encryption.
- Features to note:
  - Parallel architectures have multiple key schedulers. This is both an advantage and a disadvantage.
  - Parallel architectures employ feedback routing.



CLEMSON UNIVERSITY

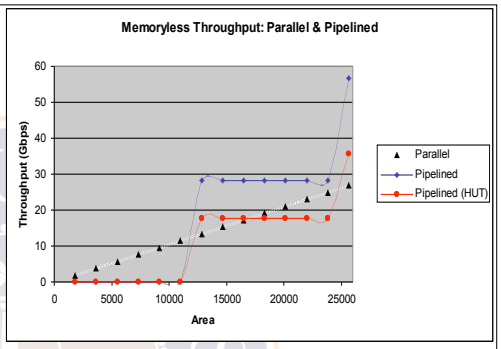
Encryption Implementations – AES

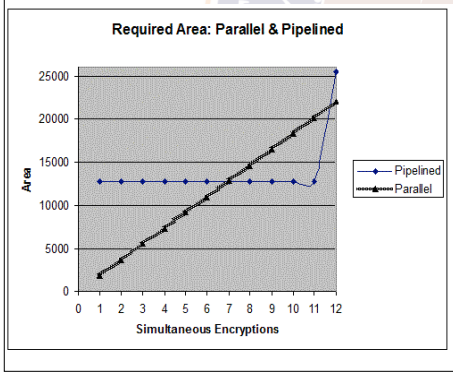
- Industry & Published Results:
  - Helsinki University of Technology:
    - Virtex-II Pipelined: 17.8 Gbps
  - Helion Technology:
    - Spartan-3 Pipelined: 10.0 Gbps
    - Virtex-II Pro Pipelined: 16.0 Gbps
    - ASIC Pipelined: 25.0 Gbps
    - Single Spartan-3: 1.0 Gbps
    - Single Virtex-II Pro: 1.7 Gbps

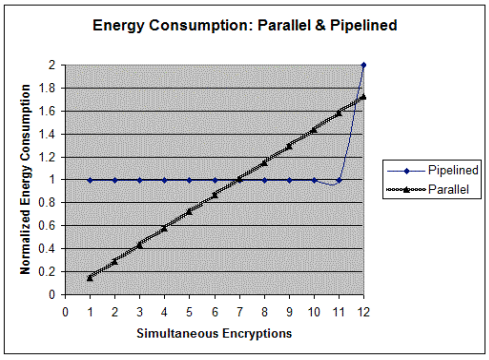
Algorithm	Target Device	System Frequency	Area (Slices)	Throughput
Iterative Encryption	Virtex-II Pro 50	199.960 MHz	1736	2.327 Gbps
Parallel Processor	Virtex-II Pro 50	179.533 MHz	21997	22.98 Gbps
Pipelined Processor	Virtex-II Pro 50	221.141 MHz	12728	28.31 Gbps
Iterative Decryption	Virtex-II Pro 50	199.960 MHz	2795	2.327 Gbps
Iterative Encryption	Spartan-3 5000	157.873 MHz	1826	1.837 Gbps
Parallel Processor	Spartan-3 5000	130.647 MHz	22670	16.722 Gbps

CLEMSON UNIVERSITY

Encryption Implementations – AES







FPGA Security Concerns

- Differential Power Analysis
  - Published Solutions
    - Selective dual-rail logic
      - Use dual-rail logic to create a uniform power profile for sensitive operations. Only minimal additional energy is consumed as dual-rail operations are not always employed.
    - Power supply noise injection
      - Obfuscates the power profile by adding random noise to the supply voltage within a specific range. Maintains functionality while making differential power analysis practically infeasible.
    - Both are good solutions

FPGA Security Concerns

- Parallel Advantages
  - Irregular power profile
    - Variable number of simultaneous encryptions
    - Variable number of different keys
    - Variable number of active modules
    - Variable number of implemented modules
  - Dynamic key values
    - Within each encryption module, both the key data and the encryption data are changed dynamically
  - Differential power analysis becomes practically infeasible

CLEMSON UNIVERSITY

Conclusions

- A number of physical attacks exist:
  - Power analysis
  - Bit flipping
- Pure software solutions can not address them
- Pure hardware solutions can have prohibitive resource requirements (power, heat).
- Integrated compiler / instruction set support needed
- Hardware support essential for necessary throughput (ex. Symmetric encryption)
- Fixed hardware architecture can not adapt to varying system needs (ex. Number of processes requiring encryption.)
- Reconfigurable hardware architectures are attractive.
- Hierarchical verification possible.
- Isolating processes can take many forms (spatial, logical, temporal).