Conceptual Framework of Side Channel Attack Resistant Secure CAD Flow

Biswadeep Chatterjee
IT Engineering
Intel Technology India Pvt Ltd

Intel Information Technology
innovative. strategic. solutions.

Agenda

- Security Concerns with Integrated Circuits
- Potential sources of Side Channel Attacks
- Considerations for a ‘secure’ VLSI Design Flow
- Changes to the traditional design flow
- Conclusion

“All observations/comments expressed in this presentation represent the views of the speaker only in personal capacity and does not represent Intel in any manner whatsoever”

Security Concerns in VLSI Circuits

- Potential threat to microchips for security applications
  - Algorithmic layer
    - Attack on system during computational cryptanalysis
    - Exploit vulnerability in AES (Advanced Encryption Standard)
  - Physical layer
    - Gather “physical parameters” leaked by the system during cryptanalysis
    - Collectively known as ‘side channel information’

- Types of Physical Attacks on security systems
  - Non-invasive attack on the system under its normal mode of operation
    - Timing Characteristics
    - Power Dissipation
    - Electromagnetic Radiation
  - Data collection over time and subsequent statistical analysis can reveal the ‘secret key’

Considerations for a ‘secure’ CAD flow

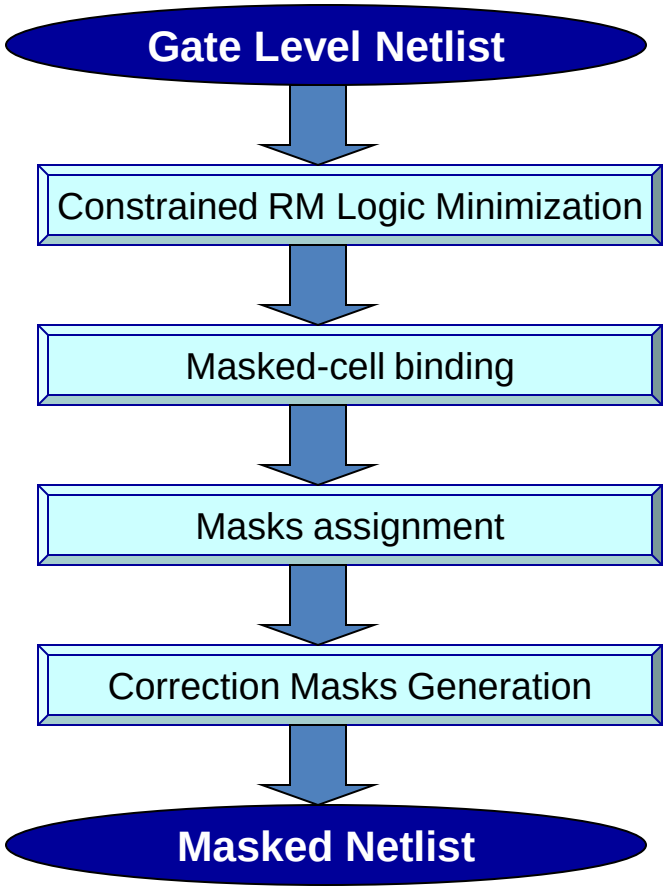
- Source of side channel leak from cryptographic system
  - Power consumption in traditional logic design is dependent on the signal activity
    - Dependence on both signal values and the signal transitions, i.e. the Hamming distance between consecutive data values.

- Goal of a secure digital design flow is to architect a logic style with constant power consumption
  - Instead of concealing or de-correlating the side-channel information, these techniques try not to create any side channel information
  - A major advantage of these techniques is that it is independent of the cryptographic algorithm

- Key design strategies
  - Ensure that there is exactly 1 switching event per clock cycle during which a constant amount of charge is used
    - Can be implemented through innovations in logic design
  - Load capacitance at the 2 outputs must be matched to assure that the load capacitance is independent of the switching event.
    - Can be achieved through a special place & route approach

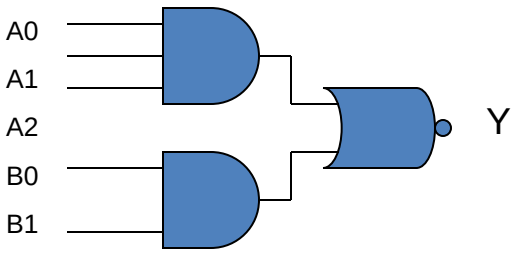
Logic Optimization in secure CAD flow

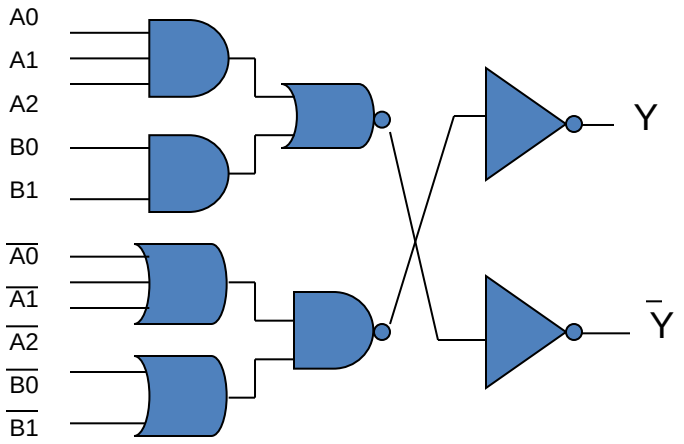
- Logic Optimization Approach
  - Mask each computed data to make probably attacked signals unpredictable
    - Achieved by exclusive-oring (XOR) a signal *b* with an uniformly distributed random variable m_b (i.e. p(m_b =0)=p(m_b =1)=1/2)
  - Represent circuit structure by AND-XOR style, i.e. Reed Muller (RM) form, rather than AND-OR style.
    - RM logic style usually can save much area from AND-OR style for cryptographic applications
- Optimization Constraints
  - ***Optimization issue 1****: The logic minimization of RM expression should put emphasis on the number of literals rather than the number of product.*
  - ***Optimization issue 2****: Multi-input AND gates must be decomposed to a network of 2-input AND gates. The total number of 2-input AND gates should be minimized without violating timing constraint.*
  - ***Optimization issue 3****: The mask bits should be minimized without violating independency constraint.*



Choice of logic cells for optimization

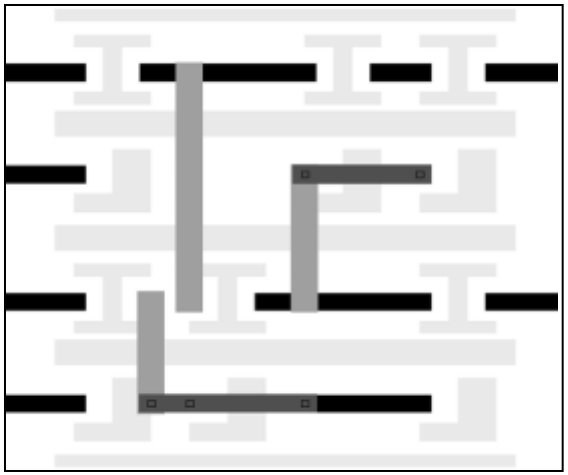
- Sense Amplifier Based Logic (SABL)
  - ✓ Advanced circuit techniques guarantee that load capacitance has a constant value
  - ✓ Completely controls the portion of the load capacitance that is due to the logic gate
  - ✓ Intrinsic capacitances at the differential input and output signals are symmetric
  - × High non-recurrent engineering costs of custom designed cell library
  - × Suffers from a large clock load common to all clocked dynamic logic styles
- Wave Dynamic Differential Logic (WDDL)
  - ✓ Implemented with static complementary CMOS logic
  - ✓ Static CMOS standard cells are combined to form secure compound standard cells with reduced power signature
  - ✓ Results in a small load capacitance on the pre-charge control signal
  - ✓ Benefits from low supply current derivative di/dt as gates do not pre-charge in parallel thereby lowering supply bounce

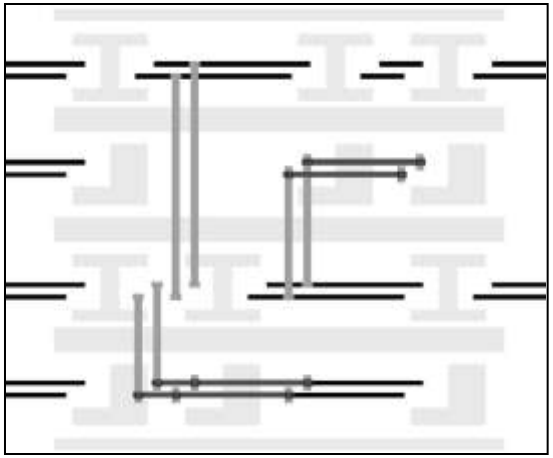




Modification of Place & Route Flow

- Changes in routing strategy to ensure matched interconnect impedances
  - Achieved by routing the differential pairs in parallel on the same layer with exactly same wirelength
  - Eliminate any potential crosstalk effects by either shielding these routes or ensuring that the separation distance is greater than critical distance
- Customizing P&R Tool to handle differential routing
  - ***Option 1**: Post process netlist to define a 'custom wire' that consists of both the differential pairs with requisite spacing and preferentially route the custom wire. Once routing is complete, replace the 'custom wire' with individual wires.*
  - ***Option 2**: Define 'net weights' and assign very high affinity between the differential pairs so that they are routed as closely as possible.*





Conclusion

- Threat of side channel attacks on secure microelectronics system is real
  - Increasing number of secure transactions justify the business need to invest effort and build hardware protection in these secure systems
- Goal is to build a generic design methodology that can use off-the-shelf EDA tools and cell libraries
  - Ensure that the standard design methodology can be extended to secure subsystem with minimal changes to ensure consistency in design process
- Discussed methodology ensures minimum deviation from standard flow
  - Use of a logic synthesis and optimization technique that can work off available standard cell libraries
  - Use of custom routing strategy ensures consistency with rest of P&R flow
  - Methodology allows easy incorporation with remaining parts of the design flow (in case only a part of the system is designed using secure design flow)
- Careful trade-off between perceived threat and increased cost
  - Implementation of ‘secure’ design leads to silicon area increase, increased validation complexity and higher time to production
  - Use of this flow should be limited to subsystems which necessitate such protections

Acknowledgement

I am deeply indebted to the works of Kris Tiri who pioneered the concept of “secure design implementation” and to Dr. Debdeep Mukhopadhyaya of Indian Institute of Technology-Kharagpur, India for drawing my attention to the need of defining a standard design framework to provide hardware protection for side-channel attacks

Thank You