CAD-based Security, Cryptography, and Digital Rights Management

Farinaz Koushanfar
ECE and CS Depts., Rice University
6100 S. Main st. MS-380
Houston, TX 77005
farinaz @rice.edu

Miodrag Potkonjak
CS Dept., University of California, Los Angeles
3532G Boelter Hall
Los Angeles, CA 90095
miodrag @cs.ucla.edu

ABSTRACT

Manufacturing variability is inherent to many silicon and nano-scale technologies and can be manifested in many different ways and modalities (e.g. power and delay). We propose a flow that starts with gate-level integrated circuit (IC) characterization which results in unique identification (ID). The ID's are an integrated part of the design functionality and software and provide a basis for conceptually new CAD-based security protocols. As an examples, we present a new IC metering schemes that ensure very low overhead and digital right management in horizontally integrated IC market. Therefore, after many years of CAD importing and benefiting from many other areas such as numerical analysis, theoretical CS, VLSI design, computer architectures, and compilers, CAD has its historical chance to impact many fields of computer science and engineering through manufacturing variability-based security and right management.

Categories and Subject Descriptors

K.6 [**Management Of Computing and Information Systems**]: Security and Protection—*physical security*; C.4 [**Performance Of Systems**]: [performance attributes]; B [**Hardware**]: Miscellaneous

General Terms

Design, Measurement, Security

Keywords

Computer-Aided Design, Security, Hardware Metering, Digital Rights Management, Intellectual Property Protection

1. THE HIGHWAY FROM CAD TO SECURITY

During the past several decades, the dominant constraint of VLSI designs has gone through a number of major paradigm shifts. While in early days area minimization was the key barrier, in late 80's, dynamic power has been the most important limiting factor. Aggressive scaling in late 90's manifested the increase in leakage power and added another dimension to the power metric. Today, the biggest bottleneck of the designers is the formidable complexity of the design process and the lack of efficient design (intellectual property) reuse methodologies. There is a wide consensus that in the near future, the key design dilemma will be providing security solutions that would cover all aspects of the design, from design-reuse methodology, to architecture and to implementation.

The highway from "CAD" to "security" is enabled via the path of manufacturing variability to security protocols. The path starts with unique and unclonable properties of each IC. In the current silicon technology, the amount of manufacturing process variations across different IC's made from the same mask and the same design is sufficient for unique characterization of each IC with a high signal-to-noise ratio [1, 2].

Until know, these properties are used in very limited way [2, 4], but by making them completely controllable and observable through properly organized measurements and numerical optimization methods for solving systems of equations, linear programs, convex or non-linear programs their qualitative and quantitative application ranges are greatly enlarged. The final steps are *integration of unique ID into functionality* in such a way that only the designer or the owner has the ability to use the IC; and *integration of unique ID with system and utility software* (e.g. compilers) to enable mutual verification.

2. HARDWARE METERING

Metering is the process that ensures the foundry cannot manufacture and sell a larger number of devices than specified in the contract with the design house [3]. A metering is classified as *passive* if it does not affect the program flow on the circuit or its functionality. Otherwise, it is *active*.

Passive metering methods leverage the observability and controllability of the design to find the unique gate-level characterization of an IC. The biggest advantage of this technique is that it does not add any overhead while it is applicable to legacy (traditional) designs. The assumption is that the foundry records a number of common i/o pin test data for each IC. For each certified IC, the foundry sends the test data back to the designer. The test data and the designer's knowledge about the design can be utilized by the designer in an optimization framework that extracts the gate-level characteristics of the IC's. The ID of the design is

DAC 2007, June 4–8, 2007, San Diego, California, USA.

a function of the extracted gate-level characteristics. Let us illustrate an example: extraction of gate-level timing characteristics of a small design (Figure 1).

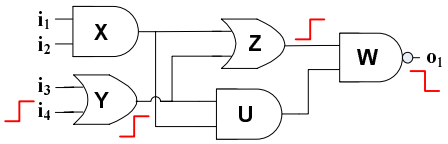

Figure 1: Transition from the input state (0000) to (0001) and the associated path delays.

The example circuit is illustrated in Figure 1. For the sake of simplicity, we ignore the interconnect delays in this example, but we emphasize that they can be added with no additional overhead. For the transition of input states (i_1, i_2, i_3, i_4)=0000 to 0001, the path delay has the following components. (i) $t_{LH}(Y)$, low to high (LH) delay at gate Y; (ii) $t_{LH}(Z)$, LH delay at gate Z; and (iii) $t_{HL}(W)$, high to low (HL) delay at W. Let τ denote the path delay and ϵ denote the error in measuring the delay. The path delay for our transition is expressed in Equation 1.

$$\begin{aligned}\tau_{0000\rightarrow0001} + \epsilon_{0000\rightarrow0001} &= t_{LH}(Y) + t_{LH}(Z) + t_{HL}(W) \quad (1)\\ &= S_{Y(LH)}t_{LH}(OR) + S_{Z(LH)}t_{LH}(OR)\\ &\quad + S_{W(HL)}t_{HL}(NOR)\end{aligned}$$

where $t_{LH}(OR)$ and $t_{HL}(NOR)$ are the delays of standard OR and NOR gates that could be extracted from the standard look-up tables for each technology. The variables S_Y, S_Z and S_W denote the scale factors of the gates Y,Z,W compared to the standard gates of each type.

One can write the linear system of equations consisting of path delays for M different input transitions in a similar way. The unknowns of this system are the scaling factors of the gates and the measurement errors (ϵ's). Now, if one solves the optimization problem of minimizing a metric of errors in the system, say L_1 norm of the errors, i.e., min $\sum_{m=1}^{M} |\epsilon_m|$, subject to the linear system of M equations, they can find the scaling factor of each gate. Because of the manufacturing variabilities, the scaling factors of the individual gates will be different for each IC. Note that, it is possible to use the conventional pass-fail manufacturing tests to measure the path delays, in case the timing measurements to determine the actual delays of paths are not available. Timing measurement can be done by increasing the *output sampling time* T of the pass-fail manufacturing test; T is defined as time period between applying the second input vector and sampling the output response. For each sampling time, one has to only check the timing pass-fail.

Temperature and power supply voltage may have a significant effect on the absolute values of the circuit delays [5]. To overcome these limitations, one could take the ratio of the gate scales, that has been shown to be much more tolerant to environmental variations [2]. One can select many such ratios, making a statistically robust signature. When validating the ownership of one design, it is sufficient to statistically match the characteristics of the signature of the device to the signatures stored in the database.

Even though solving the proposed linear optimization problem might seem to be an easy task, there are multiple challenges to addressing this problem, including:

- Creating a system of equations with full rank.
- Solving the equations in presence of measurement errors.
- Selection of the input transitions such that one could get a good observability and controllability into the design. This ensures that each of the unknown scaling variables appear in multiple equations, for both LH/HL transitions.
- Selecting those ratios that are tolerant to environmental variations, but otherwise sensitive to intra-chip manufacturing fluctuations.
- Choosing input transitions such that the paths are as independent as possible from their neighboring paths. This is because input transitions might affect the delay of neighboring paths.

Integration to functionality, system and software. Perhaps the most interesting application of unique identification comes in active connection to the functionality, system and utility software. Post-silicon passive measurements are not sufficient for this task. Digital IDs that are in form of a unique bit stream [4] have a better potential for integration into the digital designs. For example, addition of IDs to the design functionality could ensure that the device is uniquely locked for the person who does not have the knowledge of the design specifications. As another example, the secure IDs can be used to produce software that can only run on a specific IC, thereby preventing software piracy. The challenge in augmenting the digital IDs to various parts is maintaining the security: if no counter measure is taken, an attacker would able to bypass the IDs, or to emulate them from one IC on the next. Information hiding techniques may be exploited for addressing the bitstream security [6].

3. CONCLUSIONS

Manufacturing variability-based security mechanisms would enable a wide-range of security protocols including watermarking, fingerprinting, HW Trojan horse detection, software or user identification, secret and public key cryptography, and privacy guarantees. For example, we presented a passive metering scheme. Note that, gate-level characterization and controllability and observability techniques have many nice "side" applications such as characterizing foundry processes and enabling custom optimization for energy and speed at each specific IC.

4. REFERENCES

[1] S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi, and V. De. Parameter variations and impact on circuits and microarchitecture. In *DAC*, pages 338–342, 2003.

[2] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas. *Concurrency and Computation: Practice and Experience*, volume 16, chapter Identification and authentication of integrated circuits, pages 1077–1098. John Wiley & Sons, 2004.

[3] F. Koushanfar and G. Qu. Hardware metering. In *DAC*, pages 490–493, 2001.

[4] K. Lofstrom, W. Daasch, and D. Taylor. Ic identification circuits using device mismatch. In *ISSCC*, pages 372–373, 2000.

[5] S. Nassif. Delay variability: sources, impacts and trends. In *ISSCC*, pages 368–369, 2000.

[6] G. Qu and M. Potkonjak. *Intellectual Property Protection in VLSI Design*. Kluwer, 2003.