INTELLECTUAL PROPERTY PROTECTION USING WATERMARKING PARTIAL SCAN CHAINS FOR SEQUENTIAL LOGIC TEST GENERATION

Darko Kirovski and Miodrag Potkonjak
Computer Science Department, University of California, Los Angeles

ABSTRACT

We propose a protocol for intellectual property protection by watermarking the selection of register scan chain during the sequential logic test generation design-for-test step. The watermark, a user-specific digital signature, is embedded into the design by restricting and/or forcing specific registers to appear in the chain of scan registers. Therefore, selection enforcement is enabled by imposing additional signature-specific constraints on the design. This approach to intellectual property protection has a serious advantage with respect to the existing techniques: it does not require reverse engineering of the design. Copyright fraud detection can be performed by inserting a standard set of test vectors and receiving a set of outputs from the scan chain uniquely dependent upon the embedded signature.

1. INTRODUCTION

Recently, design reuse has emerged as a dominant integrated system design and integration paradigm. For example, recently, a number of companies have consolidated their efforts towards developing off-the-shelf application-specific or programmable cores (e.g. ARM, LSI Logic). However, the intellectual property (IP) business model is vulnerable to a number of potentially devastating obstructions, such as misappropriation and IP fraud. To overcome the difficulties in core-based system design, as one of the crucial enabling technology, the Virtual Socket Initiative Alliance has identified the IP protection (IPP) [VSI97].

The problem of effective protection of IP in the EDA environment has been addressed at the level of physical design [Kah98], behavioral specification [Hon98], and combinational logic synthesis [Kir98] level. Although all techniques enable reliable and exceptionally strong proof of authorship with little or no hardware overhead, their accompanying detection mechanisms are:

- **Expensive.** Almost all techniques rely on reverse engineering as a principal method for providing a hardware design used for comparison.
- **Intrusive.** Various levels or portions of the design may be developed by different designers. The reverse engineering process exposes their designs during watermark detection.

To address these issues, we are currently developing a technique (suite of protocols) for watermarking designs at the logic network level during the selection of the chain of scan registers for sequential logic test generation.

Chain of scan registers is augmented into the design specification, replacing ordinary flip-flops and latches, to enable effective sequential logic test. Namely, Cheng and Agrawal have shown that the complexity of testing designs can grow exponentially with respect to the length of cycles in the directed graph of a synchronous sequential network [Che89]. To resolve this problem, they have proposed an approach where a subset of registers is interconnected into a chain that can be controlled and observed from the chip I/O ports (scan registers). The selection has to be such that all circles in the design directed network contain at least one scan register. Therefore, the directed network is made acyclic which results in linear complexity of the testing algorithm for such sequential (acyclic) graph. As an optimization goal the routine for scan chain selection searches for a chain of minimal cardinality. This optimization problem is equivalent to the NP-complete FEEDBACK ARC SET problem (GT8, pp.192, [Gar79]). Efficient algorithms and test vector generation techniques that supplement this design-for-test methodology have been extensively studied [Che89, Chi93, Bha93, Nor96, Mak97a, Mak97b, Cha98].

The watermark, a unique designer- and/or tool-specific information, is integrated into the design in a chain selection preprocessing step by imposing a set of signature-specific constraints on the input logic network. These constraints enforce that the selection is performed according to the user signature. Section 2 describes the details about the proposed watermarking protocols. The application of the chain selection algorithm on the watermarked input results in a solution which satisfies both the original and constrained input. Since the additional constraints do not exist in the original design specification, the proof of authorship is based on the fact that the probability that some other selection algorithm returns a final design which satisfies both the initial and user-specific constraints is infinitesimally small. The proposed watermarking technique is transparent to the synthesis step and can be used in synergy with an arbitrary scan chain selection tool. The proposed IPP approach can be used to:

- *Prove authorship of the design at levels of abstraction lower than logic synthesis.* Existence of a user-specific signature in the final logic network (technology mapping) and its chain of scan registers clearly identifies the author of the input to the design-for-test process.

- *Protect the synthesis tool.* The signature of the chain selection tool developer, embedded in the solution to this design-for-test step, clearly indicates the origin of the chain selection tool.

The IPP protocols proposed in this paper are exactly along the requirements identified in the Strawman [VSI97] proposal of the Development Working Group on IPP. The recognized desiderata reflects: preservation of functionality and timing, transparency to already complex design and verification process, low overhead, provision of a strong and undeniable proof of authorship, flexibility of protection levels with respect to a variety of overhead costs, and persistence. The removal of the embedded watermark should result in a task of the difficulty equal to complete repetition of the specified optimization. In addition to the stated VSI IPP requirements, our approach also provides proportional protection of all parts of the design.

2. THE NEW APPROACH

The pre-processing procedure which watermarks the input to the chain selection algorithm encompasses several phases illustrated in Figure 1. The goal of the watermarking procedure is to add new constraints to the original directed graph G specific to the digital signature of the user.

In the first step the nodes in the input logic network specification are sorted using an industry specified standard. For this step we applied a vertex ordering procedure similar to the one already described in [Kir98]. A node n_i that corresponds to a flip-flop in the circuit has lower identifier than another node n_j if it has lower objective $Obj(n_i, C_a) < Obj(n_j, C_a)$ for the first criteria C_a from the ordered set of criteria $C = \{C_0, ...C_W\}$ where different objective between the two nodes is encountered. The objective is quantified respectively according to the number of gates, their functionality (assuming standardized ordering of typical functionalities), fanin, and fanout, and number of flip-flops at each level of the fanout $FOUT_i$ and fanin FIN_i of node n_i. A gate g_i from the logic network LN that corresponds to G has a level K with respect to the register r_i that corresponds to node n_i, if the longest path in the logic network LN from r_i to g_i is of cardinality K. Since cycles may be encountered while quantifying the objectives, for each node only $Kmax$-deep fanin and fanout are considered. As a result of this procedure, each vertex in the directed graph G of the circuit [Che89] is assigned a unique identifier.

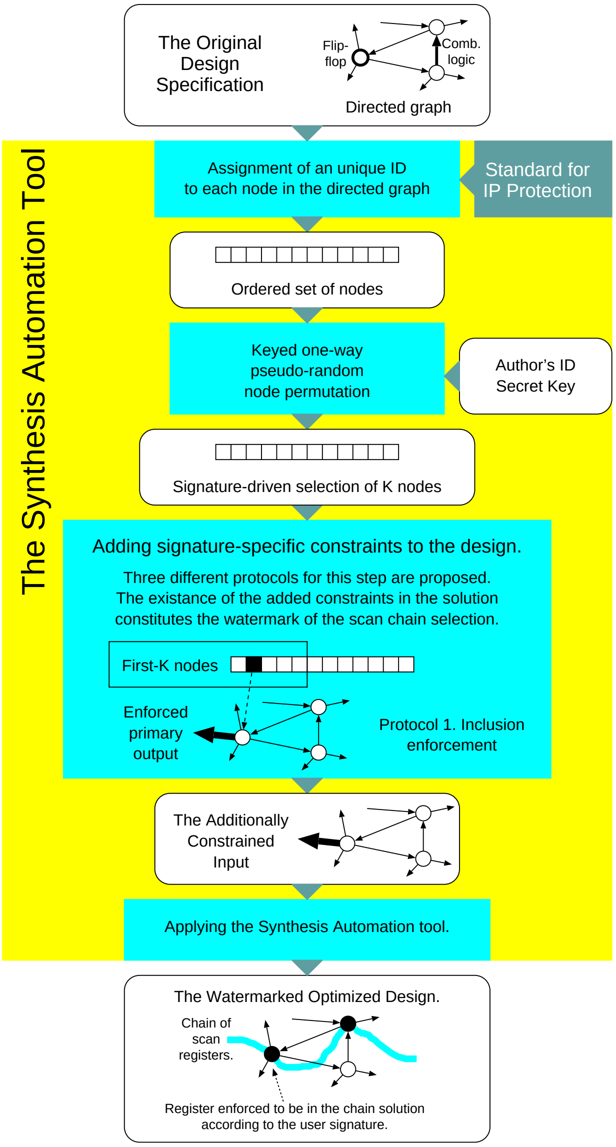
The Original Design Specification
Flip-flop
Comb. logic
Directed graph
The Synthesis Automation Tool
Assignment of an unique ID to each node in the directed graph
Standard for IP Protection
Ordered set of nodes
Keyed one-way pseudo-random node permutation
Author's ID Secret Key
Signature-driven selection of K nodes
Adding signature-specific constraints to the design.
Three different protocols for this step are proposed.
The existance of the added constraints in the solution constitutes the watermark of the scan chain selection.
First-K nodes
Enforced primary output
Protocol 1. Inclusion enforcement
The Additionally Constrained Input
Applying the Synthesis Automation tool.
The Watermarked Optimized Design.
Chain of scan registers.
Register enforced to be in the chain solution according to the user signature.

Figure 1: The protocol for hiding information in the selections of the chain of scan registers for partial sequential scan logic test generation.

Next, the node ordering is permuted in a way specific to the designer's or tool developer's signature. For this purpose, we use a keyed RSA one-way function, initialized with the user's digital signature, to generate a bit stream

[Men97]. This bit stream is used to identify one combination of “first-K choose $|N|$” nodes from the ordered list of all possible combinations. Therefore, two different authors would have additional constraints imposed on two different sets of “first-K” nodes.

In the next phase, using the set N_k of “first-K” selected nodes, the constraints are augmented into the design specification according to one of the following several proposed constraint encoding techniques.

- **Inclusion Enforcement.** The set of “first-K” registers, R_k, that correspond to the set of “first-K” nodes, N_k, is selected for inclusion in the chain of scan registers by enforcement to become primary inputs/outputs. As a primary I/O each of these registers becomes controllable and observable.

- **Exclusion Enforcement.** A new set R^{new} of $M * K$ registers is introduced in the design. This change corresponds to the addition of a set of $M * K$ new nodes N^{new}. Each variable that is originally stored in one of the “first-K” registers, r_i, (registers to be excluded from the final selection) is replicated into distinct M registers R_i^{new} from the set R^{new}. For each edge that has $n_i \rightarrow r_i$ as a destination, a set of M new edges is created with the same source and M different destinations corresponding to each node in N_M^{new}. For each edge that has n_i as a source, a set of M new edges is created with the same destination but M different sources corresponding to each of the nodes in N_i^{new}.

  Any node $n_i \in N_k \cup N^{new}$ becomes unlikely to be selected by any optimization algorithm, since the inclusion of any one of the $M + 1$ nodes in $n_i \cup N_i^{new}$, which correspond to registers that now contain variables originally stored only in r_i, implies inclusion of the remaining M nodes in $n_i \cup N_i^{new}$. To guarantee exclusion and provide a fast watermarking protocol, parameter M is statistically determined and validated and the sequence of watermarking and optimization is repeated with increasing values of M as long as the “first-K” registers are not excluded from the final chain selection. Note that exclusion enforcement and the previous technique may be combined into a synergic watermarking technique.

- **Problem Augmentation.** According to the node ordering, the existing input is augmented with new nodes and edges. Their creation and incorporation into the input is conducted using a RSA-type pseudo-random stream bit generator initialized with the user’s signature [Men97]. The pseudo-code that describes the input augmentation is presented in Figure 2. Initially, a set of N^{new} new nodes is introduced into the directed graph. Next, for each node $n_i \in N^{new}$, using the user-specific bit sequence, we select a combination N_{Ki} of Ki nodes from the ordered set of all possible combinations of Ki nodes from $N \cup N^{new}$ and draw edges from $\forall n_j \in N_{Ki}$ to n_i. Similar procedure is performed to add edges that have the newly set of nodes as sources. Parameters $|N_{Ki}|$ of this constraint encoding technique are also defined using the pseudo-random bit stream. However, their range as well as the cardinality of the set of new nodes $|N^{new}|$ is determined statistically. The main trade-off in the statistical determination is that larger cardinalities result in decreased quality of the solution to the original problem, while smaller cardinalities reduce strength of the proof of authorship.

```
$G(N, E)$ is an directed graph that describes
the sequential circuit.
Add an ordered set $N^{new}$ of new nodes to $G$.
For each node $n_i \in N^{new}$
  $Ki$ = (int) BitStream(USERID)
  Select a combination $N_{Ki}$ of $Ki$ nodes from the
  ordered set of all possible combinations of $Ki$ nodes
  from $N \cup N^{new}$. Note: selection is driven by
  the (stream) BitStream(USERID)
  For each $n_j \in N_{Ki}$
    Draw an edge $n_j \rightarrow n_i$
  End For
  $Ki$ = (int) BitStream(USERID)
  Select a combination $N_{Ki}$ of $Ki$ nodes from the
  ordered set of all possible combinations of $Ki$ nodes
  from $N \cup N^{new}$. Note: selection is driven by the
  (stream) BitStream(USERID).
  For each $n_j \in N_{Ki}$
    Draw an edge $n_i \rightarrow n_j$
  End For
End For
```

Figure 2: Proposed function for watermarking multi-level logic minimization solutions using network augmentation.

After the input is modified, the chain selection algorithm is applied, retrieving a solution which satisfies both the original and user-specific constraints. The proof of authorship is dependent upon the likelihood that some other algorithm, when applied to the initial design specification, retrieves solution which also satisfies the constrained input.

Watermark detection is a process which does not require reverse engineering of the product. To prove authorship, the designer iteratively injects a test vector into

the manufactured design, performs the design functionality (runs the test vector), and retrieves an output vector through the scan chain. By comparing the unique values in the design (can be obtained using simulation) and the retrieved values in the output vector, presence in the scan chain of registers which contain these unique values can be proved. This process is repeated until all registers that are part of the scan chain are not identified.

3. CONCLUSION AND FUTURE WORK

In this proposal, we present a new watermarking technique which leverages the advantages of embedding information into the design at the design-for-test level. The watermark is augmented into the design by modifying the input, according to the digital signature of the author, to the algorithm for selection of the partial chain of scan registers. The modification is accomplished using a set of protocols for standardized ordering of the directed graph of the circuit and addition of user-specific constraints. Due to the specific nature of the design of partial scan chains and their usage, watermark detection becomes, using this approach a trivial procedure.

As a future work, we outline three important tasks: evaluation of the hardware overhead that the watermarking proceeder may induce, quantitative establishment of the provided proof of authorship, and resistance to attacks.

4. REFERENCES

[Bha93] S. Bhatia and N.K. Jha. Synthesis of sequential circuits for easy testability through performance-oriented parallel partial scan. International Conference on Computer Design, pp.151-4, 1993.

[Cha98] D. Chang, M.T.-C. Lee, K.-T. Cheng, and M. Marek-Sadowska. Functional scan chain testing. Design, Automation and Test in Europe, pp.278-83, 1998.

[Che89] K.-T. Cheng, V. Agrawal, D.D. Johnson, and T. Lin. A complete solution to the partial scan problem (IC testing). International Test Conference, pp.44-51, 1989.

[Chi93] V. Chickermane, E.M. Rudnick, P. Banerjee, and J.H. Patel. Non-scan design-for-testability techniques for sequential circuits. Design Automation Conference. Proceedings, 1993. p. 236-41.

[Gar79] M.R. Garey and D.S. Johnson. Computers and intractability: a guide to the theory of NP-completeness. W. H. Freeman, San Francisco, CA, 1979.

[Hig93] H. Higuchi, K. Hamaguchi, and S. Yajima. Compact test sequences for scan-based sequential circuits. Fund. of Electronics, Communications and Computer Sciences, vol.76, (no.10), pp. 1676-83, 1993.

[Hon98] I. Hong and M. Potkonjak. Intellectual Property Protection Techniques for Behavioral Specifications. Unpubl. manuscript, 1998.

[Kah98] A.B. Kahng et al. Robust IP Watermarking Methodologies for Physical Design. To appear, Design Automation Conference, 1998.

[Kir98] D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong. Intellectual Property Protection by Watermarking Combinational Logic Synthesis Solutions. International Conference on Computer-Aided Design, 1998.

[Lac98] J. Lach, W.H. Mangione-Smith, and M. Potkonjak. Fingerprinting Digital Circuits on Programmable Hardware. To appear, Workshop in Information Hiding, 1998.

[Mak97a] S.R. Makar and E.J. McCluskey. Iddq test pattern generation for scan chain latches and flip-flops. IEEE International Workshop on IDDQ Testing, pp.2-6, 1997.

[Mak97b] S.R. Makar and E.J. McCluskey. ATPG for scan chain latches and flip-flops. IEEE VLSI Test Symposium, pp.364-9, 1997.

[Men97] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. Handbook of applied cryptography. Boca Raton, CRC Press, 1997.

[Nor96] R.B. Norwood and E.J. McCluskey. Synthesis-for-scan and scan chain ordering. IEEE VLSI Test Symposium, pp.87-92, 1996.

[VSI97] VSI Alliance. Fall Worldwide Meeting: A Year Of Achievement. Santa Clara, CA, October 1997.