Abstract—This paper proposes an intellectual property (IP) protection scheme at the Design-for-Testability (DfT) stage of VLSI design flow. Additional constraints generated by the owner’s digital signature have been imposed on the NP-hard problem of ordering the scan cells to achieve a watermarked solution which minimizes the penalty on power and cost of testing. As only the order of the scan cells is varied, the number of test vectors for the desired fault coverage is not affected. The advantage of this scheme is the ownership legitimacy can be publicly authenticated on-site by IP buyers after the chip has been packaged by loading a specific verification code into the scan chain. We propose to integrate the scan chain watermarking with dynamic watermarking of the IP core to make the design hard-to-attack while the ownership is easy-to-trace. The proposed scheme is applied to an optimization instance of scan cell ordering targeting at test power reduction. The results on several MCNC benchmarks show that the watermarking scheme has a very low probability of solution coincidence and hence provides strong proof of authorship.

I. INTRODUCTION

Reuse-based design methodology has prevailed in the SoC community. The widespread use and the exchange of IP cores between IP vendors create for them great revenue as well as concern about illegal IP redistribution. To prevent misappropriation and IP fraud in core-based system design, the Virtual Socket Interface (VSI) Alliance [1] has identified ownership detection as a means to IP protection (IPP). Fingerprinting and watermarking realize self-identification ownership detection as a means to IP protection and attract considerable interest among IP owners and researchers.

Unlike the conventional media watermarking, watermarking hardware IP demands the watermarked design to remain functionality correct while keeping the performance and cost overheads as low as possible. The notion of constraint-based watermarking for IPP was first proposed by Kahng et al. [2]. The idea is to transform the user-specific signature into a set of extra constraints for producing unique solutions to Boolean satisfiability (SAT) problems in electronic design automation. This concept has been used to develop many watermarking schemes for IPP at different abstraction levels of VLSI design flow [2]-[7]. The undeniable authorship proof is substantiated by the low probability of solution coincidence. However, the watermark detection process generally requires reverse engineering [6] the watermarked design to the original SAT instance to verify that the additional constraints generated by the signature are satisfied. This process is expensive and intrusive as it exposes the grammar used to generate the extra constraints and some design information.

Static watermarking has limitation on detection mechanism as the watermark is considered as a property of the design. Dynamic watermarking enables the watermark to be detected by running the watermarked IP with some user specified input combinations. One example is the Finite State Machine (FSM) watermarking [7]. Although ownership can be authenticated directly, the state-transition graph needs to be retrieved from the watermarked IP to inject the verification code. It does not permit the ownership to be detected directly after the IP core has been integrated into SoC and packaged.

Since only the test signals can be traced after the chip is packaged, watermarking the build-in self-test circuits has also been proposed [6], [8]. In [8], the watermark generation is integrated in the on-chip test module. Since only the test circuit instead of the IP core is marked independently, it is vulnerable to removal attack. The scheme proposed by Kirovski [6] marked the design by restricting some specific registers to appear in the scan chain at the DfT stage. The watermark is verified by comparing some simulation values of the design and the retrieved values in the output vector during test. It is only applicable to partial scan architectures but not full-scan designs. No specific attention has been paid on potential aggravation of the cost and power consumption at test mode due to watermarking.

The problem of ordering scan cells or scan registers in multiple cores, multiple clock domains SoC has been studied in order to minimize the test power [9], [11] and the test time [10]. We propose an IPP method based on the heuristic solution to the NP-hard problem of scan cell chaining for test power minimization. It is applicable to both full-scan and partial scan designs. The fault coverage will not be affected [9]. The scan routing area overhead can be kept acceptably low by clustering the design with regards to the routing constraint given to an efficient physical synthesis tool. A captivating merit of this scheme is that it can allow the authorship to be field authenticable publicly without the fear of authorship forgery by injecting a specific
key into the scan-in pin. It blends well with existing
dynamic watermarking technique for the core protection
to augment the ownership detectability and traceability.

II. PERCEPT OF WATERMARKING BY SCAN CELL
ORDERING

In this section, we illustrate the basic percept of a non-
intrusive watermarking scheme that can be seamlessly blent
into any existing Design for Testability (DfT) flow.

In a full-scan design, the scan path provides controlled
access to the combinational circuit of the IP core to carry
out the stimulus-response tests. The stimuli (test vectors) are
serially applied through a scan-in, $S_{in}$ pin and the responses
(output vectors) are collected serially from a scan-out, $S_{out}$
pin. Therefore, although the test vectors are independently
generated and compact to provide the desired fault coverage
of the core under test, their bit streams are ordered according
to the scan cells positions in the scan chain.
Consider a full-scan architecture with $N$ scan cells, \( r_1, r_2, \ldots, r_N \) in the scan chain. We assume a single IP core and a scan
chain of length $N$ in this simple illustration. The idea can be
extended to designs that contain multiple cores and multiple
clusters of scan cells.

A permutation \( \pi \) is defined as a one-to-one mapping of a
set of scan cells, $R = \{r_i\}$ to a set of positions, $P = \{p_i\}$ such
that the $j$-th bit of the test vector is loaded into the $i$-th scan
cell once a complete test vector has been shifted into the
scan chain, where $i, j = 1, 2, \ldots, N$. The aim of the scan cell
ordering is to find an optimal \( \pi: R \rightarrow P \) to minimize the test
time or the power consumption during scan test. This
optimization problem is known to be NP-hard [11]. Suppose
there are $S$ possible solutions to order the scan cells under a
given test time or power consumption constraint. The
assignment of scan cells to $m$ ($m < N$) randomly selected
positions, $mp_1, mp_2, \ldots, mp_m$ can be further constrained such that
the scan output, $S_{out}(mp)$, $w_i$ where $mp_i \in \{p_1, p_2, \ldots, p_m\}$ and $w_i \in \{0, 1\}$. The number of possible
solutions that can meet the additional constraints will be
reduced to $S_{m}/S$. From the perspective of IP watermarking,
the probability that an unwatermarked scan chain carries the
same watermark as the watermarked solution by coincidence is
given by $S_{m}/S$. The packaged chip that
contains the input vector used to detect $W$ in the dynamic
watermarking scheme of the IP core. Assume that the
watermark bits, $w_1, w_2, \ldots, w_3$ are to be extracted from $mp_1 = p_4, mp_2 = p_2$ and $mp_3 = p_7$. The optimization algorithm is
now constrained to find a permutation $\pi_{m}(R)$ that produces
an output vector, $WR'$ with $S_{out}(mp_1) = 1, S_{out}(mp_2) = 0$ and
$S_{out}(mp_3) = 1$ while minimizing the test power consumption
when a test vector, $WT' = \pi_{m}(WT)$ is applied onto $S_{in}$. Any
scan cell chaining optimization algorithm can be used to
assign the scan cells except that some restriction is imposed
on the assignment of scan cells to $p_2, p_4$ and $p_7$. If $r_2$ has
been assigned to $p_2$ by the algorithm, then only a reduced
subset of \( \{r_1, r_4, r_5\} \) can be assigned to $p_2$ even though the
scan cells \( \{r_3, r_6, r_7\} \) have not been assigned yet. This is
because $S_{out}(mp_i)$ must produce $w_2 = 0$. Suppose $r_1$ is
selected for $p_2$ according to the optimization algorithm. The
algorithm is to select an optimal assignment from all
unassigned cells for $p_2$. If $r_5$ is selected for $p_2$, only cells
from \( \{r_3, r_6, r_7\} \) can be selected for $p_2$ since $S_{out}(mp_2)$
must produce $w_1 = 1$. If $r_7$ is picked for $p_4$ followed by $r_4$ and $r_6$
into the next two positions, then the remaining cell, $r_5$ will
be assigned to $p_7$, which produces $w_1 = 1$. A different $WT$
from the dynamic watermarking of the IP core with $WR$
containing sufficient number of ‘1’s and ‘0’s for $W$ may be
used.

The watermarked scan chain, $\pi_{m}(R) = r_2 r_3 r_4 r_5 r_6 r_7$ is
shown in the lower part of Fig. 1. When the permuted vector $WI' = \pi_{m}(WT) = \{001001\}$ is scanned into the watermarked
chain, the signature ‘101’ contained in the response
$WR'='1001011'$ is shifted out from the $4^{th}, 2^{nd}$ and $7^{th}$
positions of the receiving scan cells for the authorship proof.

On the left hand side of Fig. 1, it is observed that none of
the original test vectors, $V_1, V_2, \ldots, V_7$ produces an output
response that contains the signature ‘101’ in $p_4, p_2$ and $p_7$
under the scan chain order, $\pi_{m}(R)$. The probability of
coincidence can be made lower if we enumerate the original
set of test responses under $\pi_{m}(R)$ to find the set of test
vectors that could be used to generate the signature, and
make them a part of the set of inputs, $WT$ to be run for
ownership authentication.

III. WATERMARK INSERTION

The proposed watermark insertion process is shown in
Fig. 2. The initial scan chain, $R = \{r_i\}$ of the IP core is

![Figure 1: Example of watermarking by scan cell ordering](image-url)
generated by a DfT tool. An $m$-bit ($m < N$) digital signature $W = w_1w_2...w_m$ is generated by signing an ownership message $MSG$ with the IP owner’s secret key $K$. The output response, $WR$ is obtained by shifting a user-specific $WI$ into the scan chain. The scan cells corresponding to the positions of the ‘0’ and ‘1’ in $WR$ are stored in the sets $P_0$ and $P_1$, respectively. A keyed one-way function, random is used to generate $m$ unique indices $mp_1$, $mp_2$, ..., $mp_m$ between 1 and $N$. The scan cells assigned to these positions will be constrained to output the signature $W$. The ownership information, $MSG$ can be verified by any legal IP recipient by decrypting $W$ using the IP owner’s public key.

The scan chain is watermarked based on a scan cell ordering algorithm, OSC. The OSC that assigns scan cells with reduced switching activity is detailed in Section IV. Let $R_i$ be the set of unassigned scan cells competing for the position, $p_i$. If $p_i$ is equal to one of $mp_1$, $mp_2$, ..., $mp_m$, $R_i$ will be constrained to $R_{i−1} \cap P_0$ or $R_{i−1} \cap P_1$ depending on the value $w_i$. Once assigned, the cell will be removed from the set $P_0$ or $P_1$, accordingly. This process is repeated until every scan cell has been assigned a unique position in the scan chain.

With a weighted graph, the minimization of the total weighted transitions becomes that of finding a Hamiltonian cycle of minimum cost in the graph with $p_2$, $p_3$ and $p_7$ constrained to some deterministic binary values for the watermarked response $WR$. The cost of a cycle is obtained by summing the total edge weights of the cycle. This problem has a complexity equivalent to the Traveling Salesman problem. Therefore, a heuristic watermarked solution is obtained by a Nearest Neighbour (NN) greedy algorithm.

![Image](340x543 to 348x589)

(a) Weighted connected graph (b) Weighted neighborhood of $r_2$

Figure 3. Watermarking power-driven scan chain ordering

**V. EXPERIMENTAL RESULTS AND DISCUSSIONS**

Our proposed scheme supplements existing dynamic watermarking of IP core to enable a direct detection of IP ownership after packaging. We present the probability of coincidence, $P_c$ as an undeniable proof of authorship. $P_c$ is the probability that a non-watermarked design carries the watermark by coincidence. Assume that $WR$ has an equal number of ‘1’ and ‘0’ bits and that it is equally probable for a scan cell at the watermarked position to output a ‘1’ or a ‘0’. Since the probability of selecting an ordered sequence of $m$ unique integers from $N$ integers is $1/P_m^n$, we have

$$P_c = \frac{1}{P_m^n} (p_1^n) \frac{1}{2} = \frac{1}{P_m^n} (\frac{1}{2})^n$$  \hspace{1cm} (1)$$

where $p_0$ ($p_1$) is the probability that a scan cell at the watermarked position outputs a ‘0’ (‘1’) bit under a specific input vector.

In the experiments, we use Mentor Graphics DfT tool to generate the scan chains and test vectors for several circuits in the MCNC benchmark suite. According to the length of
the scan chain, 16, 32, 64 or 128-bit long watermark is embedded into each design. The results are shown in Table I.

<table>
<thead>
<tr>
<th>Circuit</th>
<th>N</th>
<th>m</th>
<th>(P_c)</th>
<th>(WT_{org})</th>
<th>(WT_{mk})</th>
<th>(\Delta WT_{total})</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>31</td>
<td>16</td>
<td>2.43E-27</td>
<td>44647</td>
<td>46924</td>
<td>5.10%</td>
</tr>
<tr>
<td>S1269</td>
<td>37</td>
<td>16</td>
<td>5.66E-29</td>
<td>39081</td>
<td>39730</td>
<td>1.66%</td>
</tr>
<tr>
<td>S1512</td>
<td>57</td>
<td>32</td>
<td>8.91E-62</td>
<td>97918</td>
<td>100946</td>
<td>3.09%</td>
</tr>
<tr>
<td>S1423</td>
<td>74</td>
<td>32</td>
<td>9.89E-67</td>
<td>171695</td>
<td>176691</td>
<td>2.91%</td>
</tr>
<tr>
<td>S4863</td>
<td>104</td>
<td>64</td>
<td>4.29E-138</td>
<td>793717</td>
<td>815515</td>
<td>2.75%</td>
</tr>
<tr>
<td>S3271</td>
<td>116</td>
<td>64</td>
<td>1.29E-142</td>
<td>883348</td>
<td>905148</td>
<td>2.47%</td>
</tr>
<tr>
<td>B12</td>
<td>121</td>
<td>64</td>
<td>2.71E-144</td>
<td>1211980</td>
<td>1244950</td>
<td>2.72%</td>
</tr>
<tr>
<td>S5378</td>
<td>179</td>
<td>64</td>
<td>1.42E-158</td>
<td>2623041</td>
<td>2696216</td>
<td>2.79%</td>
</tr>
<tr>
<td>S3384</td>
<td>183</td>
<td>64</td>
<td>2.50E-159</td>
<td>878170</td>
<td>893162</td>
<td>1.71%</td>
</tr>
<tr>
<td>S9234</td>
<td>211</td>
<td>128</td>
<td>2.55E-308</td>
<td>7195393</td>
<td>7620915</td>
<td>5.91%</td>
</tr>
<tr>
<td>S6669</td>
<td>239</td>
<td>128</td>
<td>1.04E-308</td>
<td>5298646</td>
<td>5431600</td>
<td>2.51%</td>
</tr>
</tbody>
</table>

In Table I, the columns ‘N’ and ‘m’ indicate the lengths of the scan chain and the watermark, respectively. The values of \(P_c\) are shown in the next column. The data provided in the columns ‘\(WT_{org}\)’ and ‘\(WT_{mk}\)’ are the total weighted transitions of the unmarked and watermarked scan designs optimized by \(OSC\). The percentage difference between them is given in the last column. It represents the overhead on test power due to watermarking.

Design ‘S6669’ with 128-bit signature and 239 scan cells exhibits the lowest \(P_c\) of less than 1.04\(\times10^{-308}\). For a fixed watermark length, the ownership proof is enhanced with longer scan chain. Also, the test power overhead based on the total weighted transition metric is very low in general. The maximum overhead among all designs is less than 6%.

The following attack scenarios are discussed with Alice being the IP owner and Bob the attacker.

**Ghost Searching:** Bob digitally signs his own message \(MSG_b\) with his private key, \(K_b\) to generate his signature \(W_b\). He also generates \(WR_b\) with an arbitrary \(W_{mk}\). He selects from \(WR_b\) some bits to make up \(W_b\) in order to claim his ownership rights. Alice can repudiate Bob’s ownership claim by showing that her \(m\) watermarked positions are uniquely generated by a keyed one-way function. Meanwhile, Bob cannot do this unless he can reverse Alice’s one-way hash function.

**Removal Attacks:** Bob may delete the test circuit and then add his own. This will result in a task of the difficulty equal to complete repetition of the specified test generation and optimization. Alternatively, he may randomly change the order of some scan cells to alter some watermark bits. The test power overhead and scan cell re-routing effort limit the extent of such modification. If the scan chain is much longer than Alice’s signature, the probability that Bob will successfully detect many watermarked positions is low. Moreover, the output of the reordered cells may not necessarily change under \(W_{mk}\) making the probability of altering Alice’s digital signature, \(W_a\) even lower.

**Unauthorized Addition:** Bob randomly finds \(m\) scan cell positions to embed his own signature, \(W_b\) according to the proposed method. However, this will not stop Alice from detecting her watermark from Bob’s watermarked design but the reverse is not possible for Bob. Since public key cryptography is used to generate Alice’s digital signature, \(W_a\), the unauthorized addition can be thwarted by time-stamping \(W_a\) by a trusted agency.

VI. CONCLUSION

The lack of an efficient and direct detection scheme for IP buyers to validate the authenticity of an IP has been a major obstruction for IP business to thrive. In this paper, we propose a watermarking scheme at the DFT process to enable the ownership rights to be publicly validated after the core protected by some dynamic watermarking scheme has been packaged. Our method hosts the watermark information in some scan cell positions determined by a keyed one-way function. The watermarked scan chain is generated by some scan chain optimization algorithm that minimizes the test time and/or test power. During the test mode, an authentication code can be scanned out under a user-specific input sequence. This user-specific input sequence can be made design and signature dependent. The watermarking scheme is implemented with a power-driven scan chain ordering algorithm to show that the authorship can be verified with very low \(P_c\) and power consumption overhead during the test mode.

REFERENCES


