Intellectual property authentication by watermarking scan chain in design-for-testability flow

Cui, Aijiao; Chang, Chip Hong

2008

Cui, A., & Chang, C. H. (2008). Intellectual property authentication by watermarking scan chain in design-for-testability flow. Proceedings of 2008 IEEE International Symposium on Circuits and Systems (pp. 2645-2648), Seattle,WA,USA.

https://hdl.handle.net/10356/90495

https://doi.org/10.1109/ISCAS.2008.4542000

Intellectual Property Authentication by Watermarking Scan Chain in Design-for-Testability Flow

Aijiao Cui and Chip-Hong Chang

Centre for High Performance Embedded Systems, Nanyang Technological University,
50 Nanyang Drive, Research Techno Plaza, 3rd Storey, Border X Block, Singapore 637553

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-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

978-1-4244-1684-4/08/$25.00 ©2008 IEEE

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.

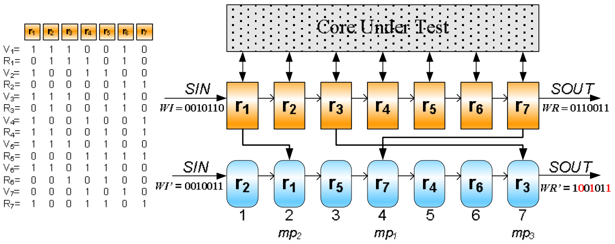
II. Percept of Watermakring by Scan Cell Ordering

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 π is defined as a one-to-one mapping of a set of scan cells, $R = \{r_i\}$ to a set of positions, $P = \{p_j\}$ 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, $S_{out}(mp_j) = w_i$, where $mp_i \in \{p_1, p_2, \ldots, p_N\}$ and $w_i \in \{0, 1\}$. The number of possible solutions that can meet the additional constraints will be reduced to S_{wm}. 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_{wm}/S. The packaged chip that contains the IP can therefore be authenticated on-site by recovering the signature, $W = w_1w_2 \ldots w_m$ from the output response to one or more specific test vectors. This is illustrated by a small example with $N = 7$ and $m = 3$ in Fig. 1.

In Fig. 1, $r_1, r_2, \ldots, r_7$ denote seven scan cells in the scan chain. V_i and R_i on the left hand side denote the i-th test vector and its corresponding output vector, respectively for $\pi(R) = r_1r_2r_3r_4r_5r_6r_7$. Assume that the IP core has been dynamically watermarked [7] with a digital signature, W = '101' of the IP owner. Suppose a new response vector WR = '0110011' that contains W is obtained from a test vector, WI = '0010110' when it is loaded into the scan chain, $\pi(R)$. WI 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, and 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 $\pi_{wm}(R)$ 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, $WI' = \pi_{wm}(WI)$ 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_1 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 $S_{out}(mp_1)$ must produce $w_2 = 0$. Suppose r_1 is selected for p_2 according to the optimization algorithm. The algorithm is free to select an optimal assignment from all unassigned cells for p_3. If r_5 is selected for p_3, only cells from $\{r_3, r_6, r_7\}$ can be selected for p_4 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_3 will be assigned to p_7, which produces $w_3 = 1$. A different WI from the dynamic watermarking of the IP core with WR containing sufficient number of '1's and '0's for W may be used.



	r_1	r_2	r_3	r_4	r_5	r_6	r_7
V_1=	1	1	1	0	0	1	0
R_1=	0	1	1	1	0	1	0
V_2=	1	0	0	1	1	0	0
R_2=	0	0	0	0	0	1	1
V_3=	1	1	1	0	0	1	0
R_3=	0	1	0	0	1	1	0
V_4=	1	0	0	1	0	0	1
R_4=	1	1	0	0	1	0	1
V_5=	1	1	1	0	1	0	0
R_5=	0	0	0	1	1	1	1
V_6=	1	1	0	1	1	0	0
R_6=	0	0	1	0	1	0	0
V_7=	0	0	0	1	0	1	0
R_7=	1	0	0	1	1	0	1

Figure 1: Example of watermarking by scan cell ordering

The watermarked scan chain, $\pi_{wm}(R) = r_2r_1r_5r_7r_4r_6r_3$ is shown in the lower part of Fig. 1. When the permuted vector $WI' = \pi_{wm}(WI)$ = '0010011' is scanned into the watermarked chain, the signature '101' contained in the response WR'='1001011' is shifted out from the 4th, 2nd and 7th 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, $\pi_{wm}(R)$. The probability of coincidence can be made lower if we enumerate the original set of test responses under $\pi_{wm}(R)$ 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, WI' 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 generated by a DfT tool. An m-bit ($m < N$) digital signature $W = w_1w_2 \ldots w_m$ 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 $mp_1, mp_2, \ldots, mp_m$ 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 $mp_1, mp_2, \ldots, mp_m$, R_i will be constrained to $R_i \cap P_0$ or $R_i \cap P_1$ 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.

```
watermark_insert($MSG$, $WI$, $K$, $R$) {
    $W$ = public_key_encrypt($MSG$, $K$);
    Scan $WI$ into $R$ to obtain $WR$;
    $P_0 = \{ r_i \mid wr_i = 0 \ \forall\ r_i \in R$ and $wr_i \in WR \}$;
    $P_1 = \{ r_i \mid wr_i = 1 \ \forall\ r_i \in R$ and $wr_i \in WR \}$;
    $\{mp_1, mp_2, \ldots, mp_m\}$= random($K$, $N$);
    for ($p_i$= 1 to $N$) {
        $R_i$ : the set of unassigned scan cells competing for $p_i$;
        if ($p_i \in \{mp_1, mp_2, \ldots, mp_m\}$) {
            if ($w_i$= 1) $R_i = R_i \cap P_1$
            else $R_i = R_i \cap P_0$
        }
        $OSC$($R_i$, $p_i$);
        remove the assigned cell from $P_0$ or $P_1$;
    }
}
```

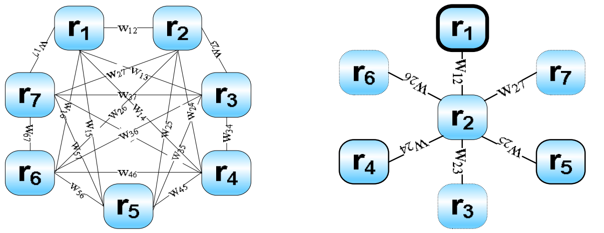
Figure 2: Watermark insertion in scan cell chaining

IV. Watermarking Power-Driven Scan Chain

We use the example of Fig. 1 and the power driven scan cell ordering method in [9] as our *OSC* to demonstrate our watermarking scheme.

The scan-in (scan-out) power for a given test vector has been shown to exhibit a strong correlation with the number of transitions in the test (response) vectors and the relative positions of the scan cells where these vectors are loaded [9]. Given a sequence of test vectors, V_1 to V_7 and *WI* and their responses, R_1 to R_7 and *WR*, the total number of weighted transitions that accounts for the scan chain length and the position of transitions during the test mode can be reduced by reordering the scan cells. Fig. 3(a) shows a connected graph where each vertex represents a scan cell of Fig. 1 and each edge represents a possible connection between two scan cells. Each edge, r_i-r_j is weighted according to the total number of bit differences between two scan cells, r_i and r_j for the complete test sequence.

With a weighted graph, the minimization of the total weighted tranistions becomes that of finding a Hamiltonian cycle of minimum cost in the graph with p_2, p_4 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) [12] greedy algorithm.



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

Figure 3. Watermarking power-driven scan chain ordering

Fig. 3(b) shows a subgraph for assigning a scan cell to watermarked locations, p_2. All cells that have yet been assigned are scattered around the preceding cell, r_2. Any vertex connected directly to r_2 is referred to as the neighbor of r_2 and its distance to r_2 is measured by the weight of the edge connecting them. The search for the nearest neighbor is limited to only those neighbors of r_2 that can output the needed bit '0' when *WI'* is loaded. These scan cells are r_1, r_4 and r_5. The nearest neighor to r_2 is given by r_1 since $w_{12} = min\{w_{12}, w_{24}, w_{25}\} = min\{5, 10, 7\}$.. Thus, r_1 is assigned to p_2. This pruned *NN* search is also applied to the other two watermarked positions. As for the non-watermarked positions, all unassigned cells will be considered. Finally, an oriented cyclic graph with the permutation $\pi_{wm}(R)$ is generated.

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

$$P_c = \frac{1}{P_m^N} (p_0)^{\frac{m}{2}} (p_1)^{\frac{m}{2}} \approx \frac{1}{P_m^N} \left(\frac{1}{2} \right)^m \qquad (1)$$

where p_0 (p_1) is the probabilities 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 I. WATERMARKING SOLUTION EVALUATION

Circuit	N	m	P_c	WT_{org}	WT_{mk}	ΔWT_{total}
B11	31	16	2.43E-27	44647	46924	5.10%
S1269	37	16	5.66E-29	39081	39730	1.66%
S1512	57	32	8.91E-62	97918	100946	3.09%
S1423	74	32	9.89E-67	171695	176691	2.91%
S4863	104	64	4.29E-138	793717	815513	2.75%
S3271	116	64	1.29E-142	883348	905148	2.47%
B12	121	64	2.71E-144	1211980	1244950	2.72%
S5378	179	64	1.42E-158	2623041	2696216	2.79%
S3384	183	64	2.50E-159	878170	893162	1.71%
S9234	211	128	<2.55E-308	7195393	7620915	5.91%
S6669	239	128	<1.04E-308	5298646	5431600	2.51%

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 1.04×10^{-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 WI_b. 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 WI_a, 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

[1] VSI Alliance, Fall Worldwide Member Meeting: A Year of Achievement. Santa Clara, CA, Oct. 1997.

[2] A. B. Kahng et al., "Constraint-Based Watermarking Techniques for Design IP Protection" *IEEE Trans. on CAD*, vol. 20. no. 10, Oct. 2001, pp. 1236-1252.

[3] F. Koushanfar, I. Hong, M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection", *ACM Trans. on Design Automation of Electronic Syst.*, vol. 10, no. 3, July 2005, pp. 523-545.

[4] D. Kirovski, Y.-Y. Wwang, M. Potkonjak, and J. Cong, "Intellectual property protection by watermarking combinational logic synthesis solutions," in *Proc. IEEE/ACM Int. Conf. on CAD*, San Jose, California, USA, Nov 1998, pp.194-198.

[5] A. Cui and C. H. Chang, "Stego-signature at logic synthesis level for digital design IP protection", in *Proc. IEEE Int. Symp. on Circuits and Syst.*, Kos, Greece, May 2006, pp. 4611-4614.

[6] D. Kirovski, and M. Potkonjak, "Intellectual Property Protection using Watermarking Partial Scan Chains for Sequential Logic Test Generation", in *Proc. IEEE High Level Design, Verification, and Test Conf.*, Nov. 1998.

[7] A. T. Abdel-Hamid, S. Tahar and E. M. Aboulhamid, "A Public-Key Watermarking Technique for IP Designs", in *Proc. Design, Automation and Test in Europe*, vol. 1, Mar. 2005, pp. 330-335.

[8] Y. C. Fan, and H. W. Tsao, "Watermarking for Intellectual Property Protection", *IEE Electronics Lett.*, vol. 39, no.18, Sept. 2003, 1316 – 1318.

[9] Y. Bonhomme, P. Girard, C. Landrault and S. Pravossoudovitch, "Power driven chaining of flip-flops in scan architectures", in *Proc. IEEE Int. Test Conf.*, Washington, USA, 2002, pp. 796-803.

[10] S. Narayanan, C. Njinda and M. Breuer, "Optimal Sequencing of Scan Registers", in *Proc. IEEE Int. Test Conf.*, Baltimore, USA, Sept. 1992, pp. 293-302.

[11] V. Dabholkar, S. Chakravarty, I. Pomeranz and S.M. Reddy, "Techniques for Minimizing Power Dissipation in Scan and Combinational Circuits During Test Application," *IEEE Trans. on CAD*, vol. 17, no. 12, Dec. 1998, pp. 1325-1333.

[12] M. Gondran ,M. Minoux and S. Vajda, "Graphs and Algorithms," John Wiley & Sons Inc., New York, 1984.