A Sequential Circuit-Based IP Watermarking Algorithm for Multiple Scan Chains in Design-for-Test

*Wei LIANG[1,2,3], *Xingming SUN[1,3], Zhiqiang RUAN[1,3], Jing LONG[2], Chengtao WU[3]

[1]Jiangsu Engg. Center of Network Monitoring, Nanjing Univ. of Information Sci. & Technology, Nanjing, 210044, China
[2]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
[3]School of Computer and Communication, Hunan University, Changsha, 410082, China

idlink@163.com, sunnudt@163.com, rzq_911@163.com, longjing0404@163.com, chengtao_wu@163.com

Abstract. *In Very Large Scale Integrated Circuits (VLSI) design, the existing Design-for-Test(DFT) based watermarking techniques usually insert watermark through reordering scan cells, which causes large resource overhead, low security and coverage rate of watermark detection. A novel scheme was proposed to watermark multiple scan chains in DFT for solving the problems. The proposed scheme adopts DFT scan test model of VLSI design, and uses a Linear Feedback Shift Register (LFSR) for pseudo random test vector generation. All of the test vectors are shifted in scan input for the construction of multiple scan chains with minimum correlation. Specific registers in multiple scan chains will be changed by the watermark circuit for watermarking the design. The watermark can be effectively detected without interference with normal function of the circuit, even after the chip is packaged. The experimental results on several ISCAS benchmarks show that the proposed scheme has lower resource overhead, probability of coincidence P_c and higher coverage rate of watermark detection ΔS by comparing with the existing methods.*

Keywords

IP reuse, VLSI, DFT, LFSR, multiple scan chains.

1. Introduction

With the rapid development of deep sub-micron integrated circuit systems, SOC (System on Chip) has become the mainstream in IC (Integrated Circuit) design. IP (Intellectual Property) reuse used by more semiconductor companies is essential to shorten design time and reduce product risk [1-3]. The problem of effective IP protection has been widely concerned.

Digital watermarking applied in DFT design has been extensively concerned [4], [5]. For most of the DFT watermarking techniques, the authors can insert their copyright into IP core, thus enabling identification of these cores. DFT watermarking, typically "protection and detection", is an IP protection technique for embedding watermark at various design stage of SOC design by using testability.

Recently, a number of DFT watermarking techniques have been proposed [6-22]. In the methods proposed by Fan et al. [7-8], the watermark generation is integrated in the test module. Five possible methods for watermark hiding are presented. Since only the test circuit instead of the IP core is marked independently, it is vulnerable to removal attacks. Cui et al. [9-11] proposed to insert watermark through reordering the scan cells in a single scan chain minimizing power overhead. Saha et al. [12-13] proposed to watermark both the scan tree and single scan chain, separately embedding the signatures of the owner of physical design tool and that of the logic design tool. The scheme proposed by Kirovski [14-15] 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 vectors in the test mode. It is only applicable to the partial scan architectures but not full scan designs. These techniques solve the problems of watermark embedding time, additional overhead and traceability existed in the previous methods. However, with the increasing complexity of circuit, the correlation of test vector for multiple scan chains may affect the circuit performance. Moreover, these methods are vulnerable to reverse engineering attack. The attackers can damage the overall project only by resynthesis and remapping.

An IP protection method is proposed by watermarking multiple scan chains in sequential circuit. The proposed scheme adopts DFT test model in SOC design, and uses an LFSR for pseudo random test vector generation [16]. All of the test vectors are shifted in scan input for the construction of multiple scan chains with minimum correlation. A watermark logic circuit is designed to change specific registers in multiple scan chains for watermarking the design.

2. Related Work

Usually, digital watermarking [17-20] methods are used along with DFT design in practical application. In this section, some basic definitions lay out the theoretical foundation for the construction of multiple scan chains with the minimum correlativity.

Definition 1: If there is at least one path from input vector S_I to output vector S_O in sequential circuit, S_I is connected with S_O. If there is at least one output vector S_O connected with input vectors S_{I1} and S_{I2} respectively, then S_{I1} and S_{I2} are correlated; otherwise, uncorrelated.

Definition 2: In sequential circuit, N output vectors connected with input vectors S_{I1} and S_{I2} respectively, if it exists, the correlation is N, denoted by $(S_{I1}, S_{I2}) = N$ or $(S_{I2}, S_{I1}) = N$; otherwise, S_{I1} and S_{I2} are uncorrelated, $(S_{I1}, S_{I2}) = 0$ or $(S_{I2}, S_{I1}) = 0$.

Definition 3: In multiple scan chains M, supposing each chain has equal length, denoted by d (except as hereinafter provided). The ordering of scan cells in c_1 and c_2 is represented by $\{s_{1,1}, s_{1,2},\ldots,s_{1,n}\}$ and $\{s_{2,1}, s_{2,2},\ldots,s_{2,m}\}$ respectively. The correlation of scan chains c_1 and c_2 is denoted by $\Upsilon(c_1, c_2)$:

$$\Upsilon(c_1, c_2) = \sum_{i=1}^{d} (s_{1,i}, s_{2,i}). \tag{1}$$

Similarly, in multiple scan chains M with λ scan chains $c_1, c_2,\ldots,c_\lambda$, correlation of M is the sum of correlation of every two different scan chains, denoted by $\Phi(M)$:

$$\Phi(M) = \sum_{i=1}^{\lambda-1}\sum_{j=i+1}^{\lambda} \Upsilon(c_i, c_j) = \sum_{i=1}^{\lambda-1}\sum_{j=i+1}^{\lambda}\sum_{k=1}^{d} (s_{i,k}, s_{j,k}) = \sum_{k=1}^{d} \Pi(k). \tag{2}$$

Here, $\Pi(k) = \sum_{i=1}^{\lambda-1}\sum_{j=i+1}^{\lambda} (s_{i,k}, s_{j,k})$ denotes the sum of correlation of every two different input signals in column k of the multiple scan chains.

Definition 4: In multiple scan chains M, considering two input signals s_{θ,k_1}, s_{φ,k_2} respectively in columns k_1, k_2, if the inequation

$$\sum_{i=1,i\neq\theta}^{|k_1|} (s_{i,k_1}, s_{\varphi,k_2}) + \sum_{i=1,i\neq\varphi}^{|k_2|} (s_{i,k_2}, s_{\theta,k_1}) < \sum_{i=1,i\neq\theta}^{|k_1|} (s_{i,k_1}, s_{\theta,k_1}) + \sum_{i=1,i\neq\varphi}^{|k_2|} (s_{i,k_2}, s_{\varphi,k_2}) \tag{3}$$

is satisfied, that is $\sum_{\theta,\varphi}^{k_1} + \sum_{\varphi,\theta}^{k_2} < \sum_{\theta}^{k_1} + \sum_{\varphi}^{k_2}$, where $k_1 \neq k_2 \in [1, d]$, $\theta \in [1, |k_1|]$ and $\varphi \in [1, |k_2|]$, then s_{θ,k_1} and s_{φ,k_2} is exchangeable, the exchange operation is called vector exchange.

Theorem: Multiple scan chains M_0 is transformed into M_p after series of vector exchanges. In multiple scan chains M_p, two input signals s_{θ,k_1}, s_{φ,k_2} in any two columns k_1 and k_2, the inequation $\sum_{\theta,\varphi}^{k_1} + \sum_{\varphi,\theta}^{k_2} \geq \sum_{\theta}^{k_1} + \sum_{\varphi}^{k_2}$ is satisfied, where $\forall k_1 \neq \forall k_2 \in [1, d]$, $\forall\theta \in [1, |k_1|]$, $\forall\varphi \in [1, |k_2|]$. Therefore, correlation of the multiple scan chains $\Phi(M_p)$ is the minimum.

Proof: Consider M_0, if any two input signals in any two columns satisfy the inequation in theorem, M_0 is equal to M_p; otherwise, there must be at least two input signals in different columns not satisfying the inequation. Randomly selecting two input signals P and Q, P in column k_i and Q in column k_j, $k_i \neq k_j \in [1, d]$, $\sum_{P,Q}^{k_i} + \sum_{P,Q}^{k_j} < \sum_{P}^{k_i} + \sum_{Q}^{k_j}$, the vector correlation of M_0 is defined as:

$$\begin{aligned}\Phi(M_0) &= \Pi(k_i) + \Pi(k_j) + \sum_{k=1,k\neq k_i,k\neq k_j}^{d} \Pi(k) \\ &= \sum_{P}^{k_i} + \sum_{Q}^{k_j} + u + m\end{aligned} \tag{4}$$

u is constant uncorrelated with P and Q, m represents vector correlation sum of other columns except k_i and k_j. By exchanging the positions of P and Q in M_0, we get multiple scan chains M_1. In $\Phi(M_1)$, the correlation of the vectors has no change except that of columns k_i and k_j, thus we have

$$\begin{aligned}\Phi(M_1) &= \Pi(k_i^1) + \Pi(k_j^1) + \sum_{k=1,k\neq k_i,k\neq k_j}^{d} \Pi(k) \\ &= \sum_{P,Q}^{k_i} + \sum_{Q,P}^{k_j} + u + m\end{aligned} \tag{5}$$

Comparing (4) and (5), since $\sum_{P}^{k_i} + \sum_{Q}^{k_j} > \sum_{P,Q}^{k_i} + \sum_{Q,P}^{k_j}$, we have $\Phi(M_1) < \Phi(M_0)$.

We perform the same operations on M_1. Considering M_1, if any two input signals in any two columns satisfy the inequation, M_1 is equal to M_p; otherwise, perform another exchange for new multiple scan chains M_2, having $\Phi(M_2) < \Phi(M_1)$, repeat by the same logic. Considering multiple scan chains M_p, any two input signals s_{θ,k_1}, s_{φ,k_2} in any two columns k_1 and k_2, $\sum_{\theta,\varphi}^{k_1} + \sum_{\varphi,\theta}^{k_2} \geq \sum_{\theta}^{k_1} + \sum_{\varphi}^{k_2}$ is satisfied. If k_1 is equal to k_2, the correlation $\Phi(M_p)$ will not be affected after exchanging positions; otherwise, the correlation of the new multiple scan chains after exchanging positions must be equal or greater than $\Phi(M_p)$. Thus the vector correlation of multiple scan chains M_p denoted by $\Phi(M_p)$ is the minimum. Simultaneously, correlation of vectors in new multiple scan chains decreases a positive integer after an exchange operation. Therefore, for any design with multiple scan chains architecture, the minimum correlation must be equal or greater than 0, i.e. multiple scan chains M_0 will be transformed into M_p after finite times of exchange operations and M_p has the minimum correlation.

3. Multiple Scan Chains-Based Watermarking

3.1 Watermarking Principle

The test architecture of multiple scan chains has emerged for solving the test time problem in single scan chain [21]. Here, architecture of multiple scan chains with the minimum correlation is presented for better performance. The multiple scan chains M_d could be transformed into M_p with the minimum correlation $\Phi(M_p)$ after exchange operations. Fig. 1 shows the test architecture of multiple scan chains. LFSR shifts test vectors in multiple scan chains for testing. By comparing with single scan chain, multiple scan chains architecture has the advantage of less test time and good resistance.

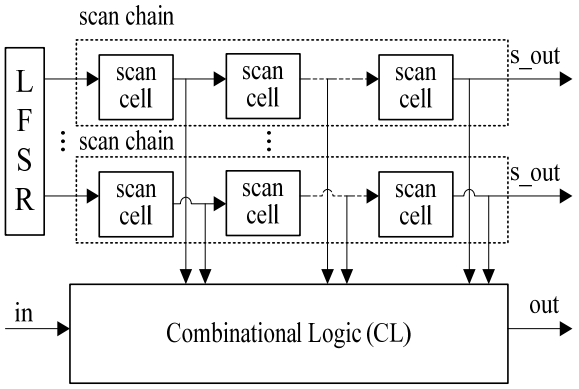


Fig. 1. The test architecture of multiple scan chains.

Fig. 2 shows the watermarking architecture of multiple scan chains in DFT. LFSR provides test vectors for *n* chains and input of watermark circuit (WMC). After watermarking, the watermarked response vectors will be shifted out.

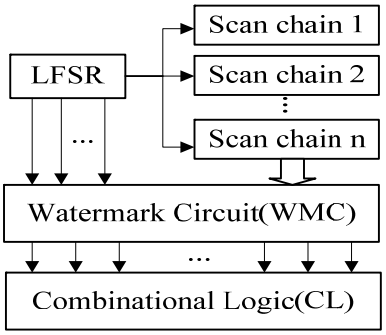


Fig. 2. The watermarking architecture of multiple scan chains.

Fig. 3 shows an example for watermarking multiple scan chains. Assume that, the circuit under test consists of 6 scan cells s_i , $i = 1, 2,\ldots,6$, these cells are organized into two scan chains $c_1 = \{s_1, s_2, s_3\}$ and $c_2 = \{s_4, s_5, s_6\}$. In the watermark circuit, one input of XOR gate is connected to one cell in multiple scan chains, and another controlled by watermark enable signal *w_en* and output of arbitration logic circuit (ALC). However, the output of ALC is under the control of states in LFSR.

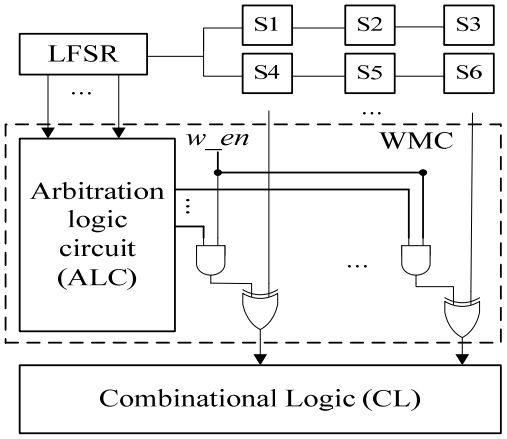


Fig. 3. An example of multiple scan chains based watermarking.

In the normal mode (*w_en*=0), the circuit under test executes normal scan test and in the watermark mode (*w_en*=1), a specific state shifted in ALC may cause 1, thus values of some cells in multiple scan chains will be reversed and then be output. The IP identification could be verified by comparing the output in normal mode and watermark mode for the same input vector.

3.2 Watermark Embedding

First of all, the signature, which can intuitively represent one's identity, is encrypted and then hashed [22]. The generated digital digest is inserted into IP core as watermark. Hash function *H* is actually a transformation, using *x* as input, the returned value is called hash value, denoted by *h*, i.e. $h = H(x)$. Since hash is an oneway function, given a value *h*, it is impossible to calculate *x* by using $H(x) = h$.

Assume that, the signature is "hnulw…", firstly, we transform it into ASCII code "110100011…". The RSA algorithm is used for encryption, with the encrypted text denoted by *W*. By using hash function *H*, the digital digest $Msg = H(W)$ is generated, i.e. the watermark W_m. After that, we generate a random sequence without repetition, represented by $Rn = \{r_1, r_2,\ldots,r_n\}$. With the sequence, the watermark W_m will be grouped into a number of fragments, denoted by $w_{m_1}, w_{m_2},\ldots, w_{m_\lambda}$. These fragments are mapped into a set of position constraints for watermark embedding.

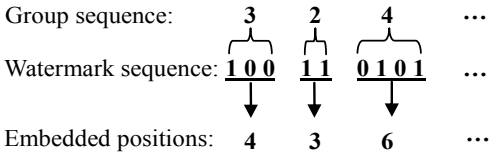


Fig. 4. The generation of watermark fragments.

Suppose that the generated digital digest *Msg* =100110101…, i.e. the watermark W_m. The random sequence *Rn* = {3, 2, 4…} is used to group watermark into fragments, the numbers in *Rn* represent the length of each watermark fragment w_{m_i} ($i = 1,2,\ldots,\lambda$). As shown in Fig. 4, after grouping, the first three watermark fragments are $w_{m1} = 100$, $w_{m2} = 11$, $w_{m3} = 0101$, and the corresponding decimal numbers are respectively 4, 3, 6. This sequence represents the positions of the watermarked registers. The specific registers at these positions will be changed through watermark circuit for watermarking.

The following pseudo-code summarized the approach:

1 Read in netlist and desired signature S;
2 $W_A = CHAR\_TO\_ASCII(S)$;
3 $W_{AR} = \Psi(W_A)$;
4 $W_m = H(W_{AR})$, store W_m;
5 Generating random sequence $Rn(k) = Random()$, store $Rn(k)$;
6 $Rn(k)$: *Group* (W_m);
7 for(i=1; group number i<number of watermark fragments λ; i++){

8 $Position(i{+}{+}) = BIT\_TO\_DEC(W_m)$;
9 store $Position(i)$;
10 }
11 w_en=1, watermark circuit is active;
12 $Position(i)$:change specific registers;
13 Embedding watermark.

Lines 1 to 4 preprocess the signature and generate the watermark. The watermark is stored and should be compared with the extracted watermark for copyright identification. Lines 5 and 6 generate a random sequence without repetition and use for grouping watermark into fragments. Lines 7 to 10 transform the watermark fragments into position information. This information is stored for watermark extraction. In line 11, the watermark circuit is active. Finally, line 12 and 13 are executed for watermark embedding.

3.3 Watermark Extraction

When the IP core is suspicious to be misappropriation, the author could apply to the third party for the verification of watermark by the following steps.

First of all, we read in the watermarked design and insert architecture of multiple scan chains. LFSR is used for the generation of test vectors. At present, w_en=1, the watermark circuit is active. The test vectors are shifted in multiple scan chains. The response vectors will be output through the combinational logic in the test circuit. Therefore, the watermarked responses R_m could be detected at the scan output. Then we set w_en signal as '0', now the scan results become the original response R since the watermark circuit is not active. Accordingly, given a specific input vector, by comparing the response vector R and R_m, respectively before and after watermark, the watermark positions will be found. After a series of transformations, the watermark fragments distributed in the whole design are found. Using the stored sequence $Rn(k)$, the watermark fragments can be recombined as an extracted watermark W_m'. The IP identity could be verified by comparing W_m and W_m'. This process is summarized as follows:

1 Read in the watermarked design D_w;
2 LFSR: generate test vector V ;
3 V: $R_m = SCAN\_TEST(V)$;
4 w_en=0;
5 V: $R = SCAN\_TEST(V)$;
6 *Compare* (R, R_m), find the changed positions $Position'(i)$;
7 for(i=1; group number i<number of watermark fragments λ; i++){
8 extract watermark fragments;
9 $W_{m_i}' = DEC\_TO\_BIT(Position(i++))$;
10 }
11 $Rn(k) : W_m' = Combinate(W_{m_i}')$;
12 If ($W_m' = W_m$) then successfully extract watermark;
13 Verify IP copyright.

4. Experimental Results and Performance Analysis

The proposed scheme by watermarking multiple scan chains with the minimum correlation is implemented in VC on a 1.2 GHz Sun UltraSPARC-T1 machine. The watermarking scheme is applied on sequential circuits from ISCAS'85, ISCAS'89 and ISCAS'99 [9] benchmark suites. The performance analysis of the proposed scheme will focus on resource overhead, resistance to attacks and comparison of experimental results.

4.1 Resource Overhead

It is critical to evaluate the resource overhead after watermarking. We select five circuits with the gate number over thousand for experiments. The zero delay models in [23] are used for resource evaluation, through which the transition times will be computed for reflecting the actual resource overhead. The experiment is conducted by the following steps:

(1) Generate the pseudo random vectors by using LFSR and construct the optimal scan architecture with the minimum correlation, and then output the test vectors;

(2) load the test vectors in the circuit under test and record the transitions of internal nodes, and then calculate peak power and average power;

(3) partition the test point in sequential circuit according to the architecture of multiple scan chains;

(4) use LFSR for the generation of test vectors once again, and obtain the watermarked response vectors; calculate the peak power and average power after watermark by recording the transitions of internal nodes during test.

As shown in Tab. 1, the cells number of combinational circuit and sequential circuit are shown in column 2 and 3 respectively. The columns, "P_w", "P_f" and "ΔK" are respectively the average power, peak power and the coverage rate of the test nodes. The experimental results in Tab. 1 show: the average power and peak power both reduce accordingly, while the coverage rate increases slightly. It proves that the proposed scheme has the advantages of lower resource overhead and higher coverage rate without affecting the normal circuit function.

4.2 Resistance to Attacks

In actual application, power attacks will be much more complicated than the attacks applied in benchmark circuits. Therefore, we evaluate the resistance of the proposed scheme to power attacks by resistance of the benchmark to transient power attacks. The evaluation model of resistance to transient power attacks proposed in [8], is used for computing the time for attackers to successfully attack and resource overhead. In this way, the resistance of the watermark to power attacks can be effectively evaluated.

The robustness of the proposed IP watermarking scheme is generally evaluated by the probability of coincidence P_c. Basically, P_c represents the probability of a non-watermarked design carrying the legitimate watermark. Let λ be the watermark fragments for embedding. The probability of λ cells being randomly selected from n scan cells is $1/C_n^{\lambda}$. Suppose that the selected cells have equal number of "0" and "1". p_{01} and p_{10} respectively represent the probability of "0" to "1" and that of "1" to "0", we have $p_{01} = p_{10} \approx 0.5$. Thus the probability of coincidence P_c is shown as

$$P_c = \frac{1}{C_n^{\lambda}} (p_{01})^{\frac{\lambda}{2}} (p_{10})^{\frac{\lambda}{2}} \approx \frac{1}{2^{\lambda} C_n^{\lambda}}. \quad (6)$$

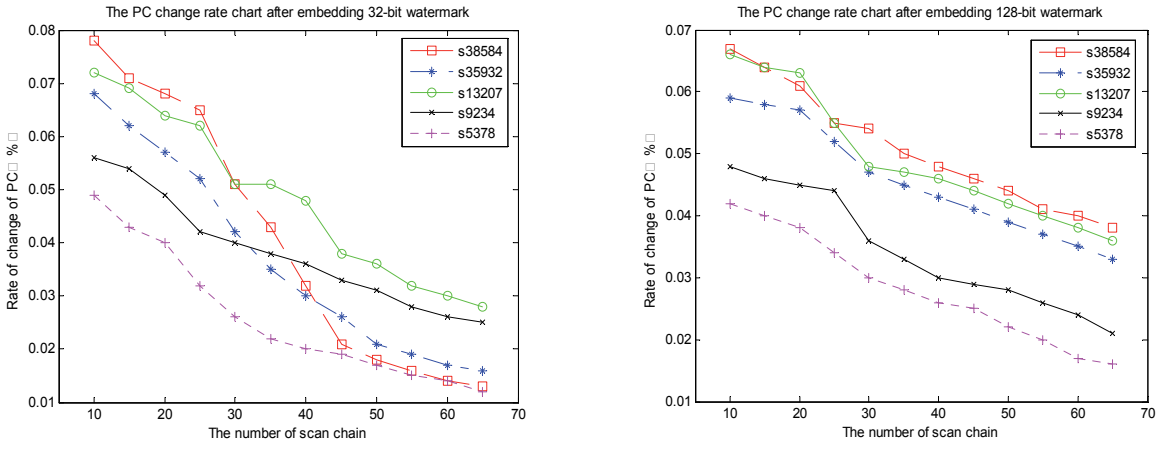
To have a strong proof of IP identity, the probability must be convincingly low.

The architecture of multiple scan chains M_p with the minimum correlation is constructed on the basis of M_0. The proposed scheme embeds 32 bits and 128 bits watermark into the optimal architecture. Then, we conduct 1000 random attacks on the watermarked benchmark circuits.

If the attackers attempt to remove the watermark and add their own test circuits, they need to modify the logic circuit and replace part of functional logic. The difficulty may be basically equal to redesign. Five larger circuits in the benchmark suites are selected for experiment. The P_c change rate after embedding watermark, 32bits and 128bits respectively, are shown in Fig. 5. The experimental results show that the number of chains is increasing with the complexity of the test circuits, while P_c presents a downtrend. The decline of P_c change rate in (b) is slower than that in (a), which precisely proves that embedding watermark with larger size in complicated circuit has strong resistance to attacks.

Circuit	Combinational Logic N	Sequential Logic C	Original Circuit			Watermarked Circuit		
			P_w	P_f	ΔK(%)	P_w	P_f	ΔK(%)
S5378	2779	179	3797	1968	84.56	3461	1876	90.11
S9234	5597	211	6785	3622	90.12	6123	3601	98.54
S13207	7952	669	10908	6471	82.16	9875	5947	88.34
S35932	16066	1728	41235	19677	89.64	32471	17983	91.44
S38584	19354	1546	20657	14906	92.82	18195	12876	96.01

Tab. 1. The performance comparison of the original and watermarked circuit



(a) The P_c change rate after embedding 32bits watermark

(b) The P_c change rate after embedding 128bits watermark

Fig. 5. The P_c change rate after embedding watermark.

4.3 Comparison of Experimental Results

The experiments are conducted on the multiple scan chains with the minimum correlation. The comparison of the proposed scheme with methods in [9] and [15] are shown in Tab. 2.

Assume that, $\Phi(M_p)$ is the minimum correlation, P_c denotes the probability of coincidence and ΔS represents the coverage rate of watermark detection. Tab. 2 shows that the proposed scheme has lower P_c than other methods, which verify the stronger resistance of our scheme to attacks. The coverage rate of watermark detection ΔS is larger. Since the architecture of multiple scan chains we use in the scheme, the watermark has become more observable and testable. Therefore, the proposed scheme has lower probability of coincidence P_c and better coverage rate of watermark detection.

Circuit	$\Phi(M_p)$	Proposed		[15]		[9]	
		P_c	ΔS (%)	P_c	ΔS (%)	P_c	ΔS (%)
i7	18	2.17E-21	91.02	2.91E-21	86.49	7.52E-20	90.23
i9	19	1.02E-14	90.62	3.49E-14	85.07	1.05E-13	88.48
i2	22	1.91E-23	97.83	6.38E-23	83.24	2.64E-19	79.41
i8	15	5.77e-32	94.27	1.67E-32	88.36	2.60E-31	91.86
frg2	14	1.23E-19	92.06	6.02E-18	91.68	1.91E-19	70.77
alu4	25	1.93E-41	94.82	7.14E-34	79.91	1.70E-39	86.09
apex6	20	5.77E-33	99.15	3.06E-24	95.28	8.16E-31	93.62
rot	20	4.98E-26	100.00	8.75E-25	94.76	1.41E-21	87.71
x3	18	4.66E-36	95.37	8.08E-25	89.41	6.28E-35	71.44
k2	33	2.42E-32	96.53	3.24E-32	92.09	8.64E-32	83.57

Tab. 2. Comparison of watermarking methods.

5. Conclusions

A novel DFT watermarking scheme is proposed based on sequential circuit for IP protection. The scheme has solved the problems of large overhead, low resistance to attacks and coverage rate of watermark detection in previous DFT watermarking methods. The test vectors generated by LFSR are shifted in scan input for the construction of multiple scan chains with minimum correlation. A watermark logic circuit is designed to change specific registers in multiple scan chains for watermarking the design. The watermark can be effectively detected without interference with normal function of the circuit, even after the chip is packaged. The experimental results show that the proposed scheme has lower resource overhead, probability of coincidence P_c and higher coverage rate of watermark detection by comparing with the existing methods. We will study on DFT watermarking techniques on the basis of scan tree and scan forest in the future.

Acknowledgments

This work is supported by National Basic Research Program of China (973 Program, Grant Nos. 2009CB326202, 2010CB334706), Key Program of National Natural Science Foundation of China (Grant No. 60736016), National Natural Science Foundation of China (Grant Nos.60973128, 61073191, 61070196 and 60973113) and PAPD, Scientific Research Fund of Hunan Provincial Education Department (Grant No.09C403), Natural Science Foundation of Xiangtan United Fund of Hunan Province (Grant No. 09JJ9006).

References

[1] CHANG, H., COOK, L., et al. *Surviving the SOC Revolution: A Guide to Platform-Based Design.* Norwel, MA: Kluwer Academic Publishers, 1999.

[2] KIROVSKI, D., HWANG, Y., et al. Protecting combinational logic synthesis solutions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2006, vol. 25, no. 12, p. 2687-2696.

[3] ABDEL-HAMID, A. T., TAHAR, S., et al. IP watermarking techniques: Survey and comparison. In *The 3rd IEEE International Workshop on System-on-Chip for Real-Time Applications,* 2003, p. 60-65.

[4] GHOUTI, L., YUAN, L., et al. VLSI design IP protection: solutions, new challenges, and opportunities. In *Proc. of NASA/ESA Conf. on AHS,* 2006, p. 469 - 476.

[5] ABDEL-HAMID, A. T., TAHAR, S., et al. A survey on IP watermarking techniques. *International Journal on Design Automation for Embedded Systems,* 2005, vol. 9, no. 3, p. 211-227.

[6] WONG, J. L., KIROVSKI, D., et al. Computational forensic techniques for intellectual property protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2004, vol. 23, no. 6, p.987-994.

[7] FAN, Y., TSAO, H. W. Watermarking for intellectual property protection. *Electronics Letters,* 2003, vol. 39, no. 18, p. 1316-1318.

[8] FAN, Y. Testing-based watermarking techniques for intellectual property identification in SOC design. *IEEE Transactions on Instrumentation and Measurement,* 2008, vol. 57, no. 3, p. 467-479.

[9] CUI, A., CHANG, C. H., et al. IP watermarking using incremental technology mapping at logic synthesis level. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2008, vol. 27, no. 9, p. 1565 - 1570.

[10] CUI, A., CHANG, C. H. Intellectual property authentication by watermarking scan chain in design-for-testability flow. In *Proc. of Intl. Symposium on CAS*, 2008, p. 2645-2648.

[11] CUI, A., CHANG, C. H. Stego-signature at logic synthesis level for digital design IP protection. In *Proc. IEEE International Symposium Circuits Syst.* Kos (Greece), 2006, p. 4611-4614.

[12] SAHA, D., DASGUPTA, P., et al. A novel scheme for encoding and watermark embedding in VLSI physical design for IP protection. In *Proc. of the International Computing Conference: Theory and Algorithms.* 2007, p. 111-116.

[13] SAHA, D., SUR-KOLAY, S. A unified approach for IP protection across design phases in a packaged chip. In *23rd International Conference on VLSI Design.* Bangalore(India), 2010, p.105-110.

[14] KIROVSKI, D., POTKONJAK, M. Local watermarks: methodology and application to behavioral synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2003, vol. 22, no. 9.

[15] KIROVSKI, D., HWANG, Y. Y., et al. Protecting combinational logic synthesis solutions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2006, vol. 25, no. 12, p. 2687-2696.

[16] HALDER, R., DASGUPTA, P., et al. An internet-based IP protection scheme for circuit designs using Linear Feedback Shift Register (LFSR)-based locking. In *Proceedings of the 22nd Annual Symposium on Integrated Circuits and System Design: Chip on the Dunes,* Natal, RN, Brazil, 2009.

[17] CASTILLO, E., MEYER-BAESE, U., et al. Digital signature embedding technique for IP core protection. In *3rd Southern Conference on Programmable Logic (SPL 2007).* 2007, p.143-148.

[18] CASTILLO, E., PARRILLA, L., et al. Intellectual property protection of IP cores at HDL design level with automatic signature spreading. In *International Conference on Advances in Electronics and Micro-electronics*, 2008.

[19] CASTILLO, E., PARRILLA, L., et al. Automated signature insertion in combinational logic patterns for HDL IP core protection. In *4th Southern Conference on Programmable Logic.* San Carlos de Bariloche, 2008, pp. 183-186.

[20] LIANG, W., SUN, X., et al. The design and FPGA implementation of FSM-based IP watermark algorithm at behavioral level. *Information Technology Journal,* 2011, vol. 10, no. 4, p.870-876.

[21] CHARBON, E., TORUNOGLU, I. Watermarking techniques for electronic circuit design. In *Proceedings of the 1st International Conference on Digital Watermarking,* 2003, p. 147-169.

[22] QU, G. Publicly detectable watermarking for intellectual property authentication in VLSI design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2002, vol. 21, no. 11, p.1363 -1368.

[23] KHAN, M., TRAGOUDAS, S. Rewiring for watermarking digital circuit netlists. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2005, vol. 24, no. 7, p.1132-1137.

About Authors…

Wei LIANG was born in 1978. He received his BS in Automation from the Central South University, China, in 2003, MS in Computer Science and Technology from Hunan University of Science and Technology, China, in 2008, and he is currently pursuing his PhD in Computer Science and Technology from Hunan University, China. His current research interests include steganography, steganalysis, real-time embedded systems, intellectual property protection, and field programmable gate arrays.

Xingming SUN (Corresponding author) received his BS in Mathematics from Hunan Normal University, China, in 1984, MS in Computing Science from Dalian University of Science and Technology, China, in 1988, and PhD in Computing Science from Fudan University, China, in 2001. He is currently a professor in the School of Computer and Communication, Hunan University, China. His research interests include network and information security, digital watermarking, digital forensic, database security, and intellectual property protection.

Zhiqiang RUAN was born in 1982. Since 2009, he has been a Ph. D. candidate in Computer Science from Hunan University. His current main research interests include security in wireless sensor networks, intellectual property protection and field programmable gate arrays.

Jing LONG received her BE in Hunan University of Science and Technology, China, in 2009, and is currently pursuing her M.S. in Computer Application at the School of Computer Science and Engineering of Hunan University of Science and Technology, China. Her research interests include real-time embedded systems, intellectual property protection, field programmable gate arrays, wireless sensor networks.

Chengtao WU received his BE in Hunan University of Science and Technology, China, in 2010, and is currently pursuing his M.S. in Computer Science and Technology at the School of Computer and Communication of Hunan University, China. His research interests include information security, intellectual property protection, field programmable gate arrays.