ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.10, No.7, 1–6

Circuit partitioning based fingerprinting method for IP protection

Tingyuan Nie[1a)], **Jie Sun**[1], **Aiguo Ji**[1], **and Zhe-Ming Lu**[2]

[1] *Communication and Electronic Engineering Institute, Qingdao Technological University, No.11, Fushun Road, Qingdao 266033, China*

[2] *School of Aeronautics and Astronautics, Zhejiang University, Zheda Road 38, Hangzhou, 310027, China*

a) *tynie@qtech.edu.cn*

Abstract: The continuously widening design productivity gap in the past few decades gives high incentives to counterfeiting ICs. Existing intellectual property (IP) protection schemes demand high overheads, and some techniques like watermarking do not facilitate tracing of illegal users. In this letter,we propose a novel fingerprinting method based on post-processing on circuit partitions. We evaluate our method on the ISPD98 benchmark suite. The experimental results demonstrate the effectiveness of the proposal. The fingerprinting design is distinct because the Hamming distance between fingerprinted IP designs is large enough to resist a collusion attack.

Keywords: fingerprinting, intellectual property protection (IPP), circuit partitioning

Classification: Integrated circuits

References

[1] C. Marsh and T. Kean, "A security tagging scheme for ASIC designs and intellectual property cores," *Proc. 15th Conf. IP SoC*, France, pp. 6–7, Dec. 2006.

[2] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," *Proc. 26th Conf. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, San Jose, California, USA, pp. 670–673, Nov. 2008.

[3] A. B. Kahng, J. Lach, W. H. M-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

[4] G. Wolfe, J. L. Wong, and M. Potkonjak, "Watermarking Graph Partitioning Solutions," *Proc. 38th Conf. Design Automation (DAC)*, Las Vegas, USA, pp. 486–489, June 2001.

[5] M. Moiz Khan and S. Tragoudas, "Rewiring for Watermarking Digital Circuit Netlists," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 24, no. 7, pp. 1132–1137, July 2005.

[6] T. Nie and M. Toyonaga, "An Efficient and Reliable Watermarking System for IP Protection," *IEICE Trans. Fundamentals*, vol. E90-A, no. 9, pp. 1932–1939, Sept. 2007.

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013

[7] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "FPGA Fingerprinting Techniques for Protecting Intellectual Property," *Proc. Conf. IEEE 1998 Custom Integrated Circuits Conf.*, Santa Clara, USA, pp. 299–302, May 1998.
[8] A. E. Caldwell, H. Choi, A. B. Kahng, S. Mantik, M. Potkonjak, G. Qu, and J. L. Wong, "Effective Iterative Techniques for Fingerprinting Design IP," *Proc. 36th Conf. ACM/IEEE Design Automation Conf.*, New Orleans, LA, USA, pp. 843–848, June 1999.
[9] G. Qu and M. Potkonjak, "Fingerprinting Intellectual Property Using Constraint Addition," *Proc. 37th Conf. ACM/IEEE Design Automation Conf*, New Orleans, LA, USA, pp. 587–592, June 2000.
[10] S. Dutt and W. Deng, "VLSI Circuit Partitioning by Cluster-removal Using Iterative Improvement Techniques," *Proc. 14th Conf. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, San Jose, CA, USA, pp. 194–200, Nov. 1996.
[11] C. J. Alpert, "The ISPD98 circuit benchmark suite," *Proc. Conf. Int. Symp. Physical Design*, CA, USA, pp. 80–85, 1998.

1 Introduction

The gap between potential design complexity and designer productivity has been continuously widening in the past decades. Intellectual property (IP) reuse becomes more popular in IC design. The trends of counterfeiting motivate the needs for development of advanced IP protection techniques. The techniques such as physical tagging, watermarking and fingerprinting are proposed. Security tags including physical unclonable functions (PUFs) have been proposed for implementing unique extrinsic IC identifiers [1, 2]. Watermarking is a comprehensive mechanism implemented to protect IP which is roughly categorized into constraint-based methods [3, 4] or additive methods [5, 6]. However, watermarking techniques do not facilitate the tracing process of illegally resold IPs and therefore cannot provide IP protection for buyers. Fingerprinting techniques are proposed to solve the problem. The main idea is to generate a piece of different fingerprinted IP for different IP buyers.

The early IP fingerprinting technique in the literature is due to Lach et al. [7]. They partitioned an initial solution into a few of parts and provide for each part several different realizations. One can generate a fingerprinting design by the combination of realizations. The technique is sensitive to the geometric structure and has high overhead. Another research is to solve the problem once, generating a relatively small problem based on the solution. The quality of fingerprinted solution is not guaranteed [8]. Qu proposed a technique which superimposed additional constraints on the problem formulation to guarantee a large amount of high quality solutions [9].

In this paper, we propose a fingerprinting method based on the post-processing of circuit partitioning. The method is effective to generate a large number of high quality solutions with zero overhead. The Hamming distance between different fingerprinted IP designs is large enough to keep the design secure.

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013

2 Circuit partitioning problem

Circuit partitioning can be viewed as assigning operations hierarchically from high-level to low-level. Suppose a partition has a total of m levels and in each level the circuit is partitioned into k subcircuits, the partition is called a k-way and m-level partition. The evaluation of the partition result depends on the final integration of all partition levels.

Consider a circuit graph G = (V, E), where V denotes the set of n vertices and E the set of edges. For a k-way balanced partition problem, the objective is to partition G into k components V_1, V_2, ..., V_k, (each component has almost the equal size) so as to minimize the capacity of the edges between separate components. The problem is represented as Formula (1). Particularly, if k=2, the partition is called bipartition or bisection.

$$\Sigma_{\forall e=(u,v)\wedge p(u)\neq p(v)} w(e)$$
$$s.t. \frac{|V|}{2}(1-\varepsilon) \leq |V_i| \leq \frac{|V|}{2}(1+\varepsilon) \quad (1)$$

Where $w(e)$ is the weight of a cut edge, and ε is a relax factor of area constraint.

3 The proposed fingerprinting method

3.1 Fingerprinting model

In this section, we give the basic fingerprinting model. As shown in Figure 1, the proposed fingerprinting scheme consists of two algorithms, *finger* and *identify*; two data spaces, IP_{WM}, the original IP data space with a given probability distribution, and IP_{sale}, the identity data space. *Finger* is a fingerprinting protocol. The inputs are the data to be sold, IP_{WM}, the buyers individual key, $Indiv_b$, and a record string text *Record-list*. The outputs are the data IP_{sale} to the buyer, and *record* to be stored for future disputes. *Identify* is an algorithm that executes to identify the original buyer of a certain copy. The inputs are the original data IP_{WM}, the sold data IP_{sale}, and a record list *Record-list* of all the sales. The output of the identification is the judgement whether the buyer's copy is legal.

The paper mainly discusses the fingerprinting protocol on how to create a large amount of high-quality solutions. We will discuss watermarking detection later.

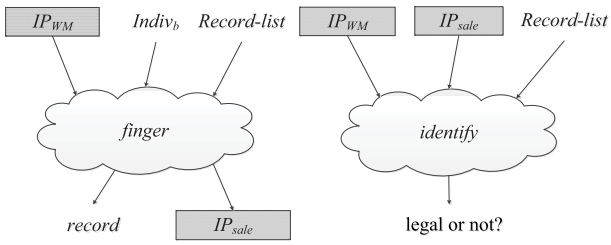

Fig. 1. Basic fingerprinting model

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013

3.2 Fingerprinting method

A fingerprinting method should not only satisfy the requirements of watermark techniques, but also have additional mandatory attributes: collusion-secure and high quality. We propose a fingerprinting method based on post-processing of circuit partitions. The proposal applies such heuristics: (i) in an incremental fashion, and (ii) to produce fingerprinted instances by perturbation according to a buyer's signature.

FM-type partitioning algorithms have been popularly proposed to obtain good results of circuit partitioning. Most of them adopt a bucket data structure to improve the effectiveness of the algorithm. The bucket sorts the cell list by an array BUCKET [-*pmax* ... *pmax*]. In practice, in a bucket there are a lot of cells whose gain is equal to zero. It means that a movement of such a cell from the local subset to its complementary subset will not change the cutsize of the partition. In other words, swapping such cells can generate a number of fingerprinting designs without any quality degradation.

Base on the considerations, we proposed our fingerprinting algorithm. The fingerprinting algorithm consists of seven steps, as shown in Figure 3.

To verify a design, one must show that the fingerprint present in the partitioning design corresponds to the user's signature. The probability P_c that a non-fingerprinted solution coincidentally contains the user's signature must be convincingly low. In our approach, we use RSA with 1024-bit key to encrypt the signature to generate a private fingerprint. The fingerprint is then used as a seed to generate a random number to determine the cells to be swapped. Note that since the attacker does not know which cells correspond to the user's signature, tampering attacks might not be able to succeed. The attacker may try a brute force attack to find ghost signatures. In order for this attack to be computationally difficult, P_c must be sufficiently low.

Fingerprinting Algorithm

Step 1: Generate an initial partition P by finding the best solution out of 10 starts of CLIP for a benchmark.

Step 2: Partition P to get a partition P' by a n-level partitioning with balanced area constraint.

Step 3: Finding out all the cells with gain equal to zero from buckets, put them into a queue.

Step 4: Create a fingerprint Fin_i for a buyer based on its individual signature and secret key.

Step 5: Use the fingerprint Fin_i as a seed of pseudorandom number generator, generate a random number to determine the cells from the queue for fingerprinting.

Step 6: Exchange the selected cells between the bucket pairs with balanced area constraint, Generate fingerprinting solution S_i.

Step 7: Repeat Step 4-6, until the demands of fingerprinting solution is satisfied.

Fig. 2. The proposed fingerprinting algorithm

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013

4 Experimental results

We perform a set of experiments to evaluate the effectiveness of the proposed method. The fingerprinting algorithm is implemented using the C++ language under Linux on a HP B7F41PA workstation with 3.3 GHz CPU and 4 GB of memory.

Table I. ISPD98 circuit benchmark characteristics

Circuit	#Cells	#Pads	#Modules	#Net	#Pins	Max%
ibm01	12506	246	12752	14111	50566	6.37
ibm02	19342	259	19601	19584	81199	11.36
ibm03	22853	283	23136	27401	93573	10.76
ibm04	27220	287	27507	31970	105859	9.16
ibm05	28146	1201	29347	28446	126308	0.00
ibm06	32332	166	32498	34826	128182	13.56
ibm07	45639	287	45926	48117	175639	4.76
ibm08	51023	286	51309	50513	204890	12.10
ibm09	53110	285	53395	60902	222088	5.42
ibm10	68685	744	69429	75196	297567	4.80
ibm11	70152	406	70558	81454	280786	4.48
ibm12	70439	637	71076	77240	317760	6.43
ibm13	83709	490	84199	99666	357075	4.22
ibm14	147088	517	147605	152772	546816	1.99
ibm15	161187	383	161570	186608	715823	11.00
ibm16	182980	504	183484	190048	778823	1.89
ibm17	184752	743	185495	189581	860036	0.94
ibm18	210341	272	210613	201920	819697	0.96

We apply the CLIP FM partitioner [10] on the ISPD98 benchmark suite [11] for the evaluation. Table I shows the characteristics of the benchmark suite. We select six different circuits from the benchmark suite to implement a 2-level bipartition. When the bipartition is completed, one can confirm the cells whose gain is equal to zero. The cells are considered as fingerprint carrier candidates. We hashed and encrypted the buyers signature to generate a 128-bit individual fingerprint. According to the individual fingerprint, we pop-up the corresponding cells and swap them to their complementary subcircuits with a 5% balance constraint. Irrespective of the number of swapped cells, one fingerprinted design can be generated. Table II reports the 2-level partitioning results. Column 2-3 reports the cutsizes of partition level 1 and partition level 2. The CLIP FM partitioner provided a good experimental result. As shown in column 4, the method provided a large number of cells whose gain is equal to zero. This makes it possible to generate a large number of fingerprinted designs by cell swapping. For instance, it can generate $2^{n_1-1} \times 2^{n_2-1} \times 2^{n_3-1} \times 2^{n_4-1} \approx 10^{184}$ different fingerprinting designs on circuit ibm03, where n_i is the number of cells (gain=0) in different subcircuits. As shown in Table II, the larger the circuit, the bigger the number n_i. Therefore in practical uses, the proposed method would provide plenty of fingerprinting designs to satisfy the commercial demand. The last column reports the total runtime of the 2-level bipartition.

In order to identify the distinctness of the fingerprinting designs, we choose 10% cells from the fingerprint carrier candidates according to the buyer's fingerprint. The fingerprinting designs are generated by swapping the selected cells to their complementary subcircuits. Table III reports the fingerprinting results. In the second column, we report the Hamming distance which indicates the transpositions required to transform the original design

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013

Table II. Partitioning results with two levels

Circuit	Cuts(lel1)	Cuts(lel2)		# cells (gain=0)				Time(s)
		Subcir A	Subcir B	Buck1-1	Buck1-2	Buck2-1	Buck2-2	
ibm01	387	415	488	106	46	59	45	0.31
ibm02	427	387	628	0	142	156	47	0.90
ibm03	2827	1451	1158	156	160	93	210	1.05
ibm10	2788	3583	1626	537	363	492	0	5.05
ibm16	7104	7477	5144	706	645	527	506	12.41
ibm18	7971	4073	1115	1012	833	624	414	19.84

to the fingerprinted design. We compared the results with reference [8]. The results indicate that our method provides a more distinct solution than reference [8]. In addition, our method provides fingerprinting solution with no quality degradation due to its zero cost, which is shown in column 3. The time shown in Column 4 implies that the proposed method is effective to generate fingerprinting designs because the consumed time is less than that of the original designs. Column 5 shows the probability P_c that we calculated by using the same way of [4]. The authors presented a watermarking technique on graph partitioning [4]. They did not give numerical experimental results. But from figures they gave, we can see that the values of P_c in both works are sufficiently low to provide strong authorship proof.

The idea may be applied on other problems like logic synthesis, physical design by equivalent unit replacement or rerouting. The methods and estimations need further research.

Table III. Fingerprinting results

Circuit	Distance			Cost		Time(s)	P_c
	Ours	Ref. [8]	Comp. (%)	Ours	Ref. [8]		
ibm01	80.30	71.10	12.94	0.00	252.20	0.12	$\leq 10^{-13}$
ibm02	46.80	41.20	13.59	0.00	272.00	0.35	$\leq 10^{-15}$
ibm03	279.00	263.40	5.92	0.00	881.50	0.56	$\leq 10^{-21}$

5 Conclusion

In this paper, we propose a novel fingerprinting method based on circuit partitioning. We applied the CLIP FM partitioner to bipartition a circuit into 2-level and implemented a post-processing to generate fingerprinting designs. We evaluated the proposed method on the ISPD98 benchmark suite. The experimental results demonstrated the effectiveness of the proposal for generating a large number of solutions without quality degradation. The method provides a distinct solution for fingerprinting and strong authorship proof to the buyers.

Acknowledgments

The Project is sponsored by SRF for ROCS, SEM. The work is also supported by Shandong Province Natural Science Foundation (ZR2009GL007). And it is a Project of Shandong Province Higher Educational Science and Technology Program (J09LG10).

DOI: 10.1587/elex.10.20130138
Received February 22, 2013
Accepted March 19, 2013
Published April 10, 2013