Future Generation Computer Systems 71 (2017) 89–101

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Low overhead symmetrical protection of reusable IP core using robust fingerprinting and watermarking during high level synthesis

Dipanjan Roy, Anirban Sengupta *

Discipline of Computer Science and Engineering, Indian Institute of Technology Indore, India

HIGHLIGHTS

- Proposed approach offers symmetrical protection at less than 1% area overhead.
- Proposed approach offers symmetrical protection at less than 1.1% latency overhead.
- Our work leverages HLS steps to embed vendor watermark and buyer fingerprint in IP design.

ARTICLE INFO

Article history:
Received 9 November 2016
Received in revised form
1 January 2017
Accepted 21 January 2017
Available online 27 January 2017

Keywords:
Reusable IP core
Symmetrical protection
Buyer
Fingerprint
Seller
Watermark
High level synthesis
Low overhead

ABSTRACT

Intellectual Property (IP) core used in computing system-on-chip provides a unique blend of yielding enhanced design productivity with reduced design cycle time. However, leveraging benefits of IP core require protection against threats from both seller's and buyer's perspective. This paper proposes a novel symmetrical IP core protection methodology that embeds a buyer fingerprint and seller watermark simultaneously during high level synthesis (HLS). The proposed work leverages major HLS steps to concurrently embed buyer fingerprint signature and seller watermark signature into a reusable IP core design. The proposed signature encoding for fingerprint and watermark is multi-variable in nature offering strong robustness, low embedding cost and low design overhead. Results on standard benchmarks indicated that the proposed symmetrical approach satisfies all the major protection features of a watermark and fingerprint such as strong robustness to both seller & buyer, low overhead, low runtime and low embedding cost. Further on comparison with baseline design (no protection), the proposed approach offers symmetrical protection (both buyer and seller) at less than 1% area overhead and less than 1.1% latency overhead. Additionally on comparison with a recent unsymmetrical approach, the proposed approach offers symmetrical protection (both buyer and seller) at 0% area overhead and less than 1.1% latency overhead.

1. Introduction

With the sky-rocketing progress of application and implementation technology in the domain of system-on-chip (SoC) based products, designs have become more sophisticated and innovatory. In order to address these complex design challenges, a balance between design productivity and time-to-market is required, which is where the use of reusable intellectual property (IP) cores [1] designed through high level synthesis is essential. High Level Synthesis [2] is a process of converting a behavioral/algorithmic description of an IP into its equivalent register transfer level counterpart consisting of several sub-steps like compilation, transformation, scheduling, allocation and binding. Reusable IP cores not only expedite the productivity of complex design process but also assist in cost reduction. However for sustainable employment of reusable IP cores in complex designs, its protection against threats is highly critical. In case of a reusable IP core there are two entities involved viz. buyer and seller. Let us look at the protection aspects from both buyer's and seller's perspective: In a reusable IP core, an IP buyer may demand *exclusive user right* as a buyer i.e. would not want the same IP copy to be resold/redistributed in the market. This happens when an IP buyer procures an IP based on his custom specifications from an IP seller, thus creating an unique mapping between an IP seller and an IP buyer. Buyer fingerprint facilitates *tracing of illegally resold/redistributed copies* of an IP core by a *dishonest IP seller* [3]. Similarly an IP core seller, when selling his design to a buyer, must protect his work from *piracy/forgery and false claim of ownership* [4–11].

* Corresponding author.
E-mail address: asengupt@iiti.ac.in (A. Sengupta).

http://dx.doi.org/10.1016/j.future.2017.01.021
0167-739X/

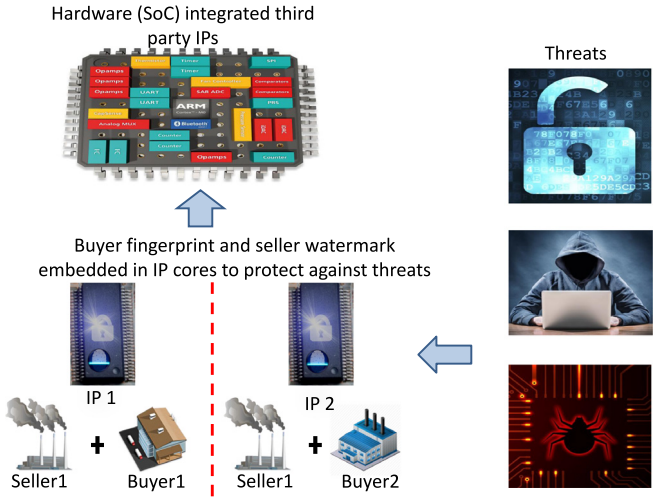

Fig. 1. Motivation for symmetrical IP core protection.

This necessitates robust symmetrical protection of reusable IP cores from both buyer's and seller's perspective. A diagrammatic overview of proposed symmetrical IP core protection is shown in Fig. 1. It is well acknowledged that most of these IPs need substantial time and effort to be designed and verified, yet they can be easily resold, copied, or modified. Buyer and seller of IP designs thus demand assurances that their content will not be illegally redistributed and falsely claimed. Protection against such complex challenges is implemented by embedding dual entity robust signature scheme during high level synthesis in the form of hidden buyer signature and hidden seller signature in a reusable IP core unit.

Existing intellectual property protection schemes [12] like copyrights, patents, trademarks, trade-secret, industrial design rights etc. are quite scattered, limited in possibilities and inadequate in protecting reusable IP cores from buyer and seller perspective. The ultimate two objectives of reusable IP core protection is: (a) from buyer's perspective: trace illegally resold/redistributed copies by a dishonest seller (b) from seller's perspective: protect against piracy/forgery and false claim of ownership [13]. In past few decades various signature hiding schemes have been proposed in different contexts of multimedia, like text, audio, image, video etc. But, all these techniques are inapplicable to reusable IP core protection as it may change functionality and accuracy during signature insertion. Thus buyer fingerprint and seller watermark signature insertions in the context of IP core protection must not only provide necessary protection to both entities but also preserve the correct functionality of the design. Although it is a well acknowledged that it may not be easy to embed protection mechanisms at zero design overhead (area and latency), however the goal is to minimize it as much as possible without compromising the protection capability of an IP. This paper proposes a novel low overhead symmetrical protection methodology for reusable IP cores based on robust multi-variable buyer fingerprint and seller watermark that incorporates hidden constraints during scheduling and register allocation steps of high level synthesis process. *(Note: Latency/Area overhead is the extra delay/area incurred in a design due to insertion of watermarking or fingerprinting constraints).*

The rest of the paper is as arranged as follows: Section 2 discusses novel contributions of this paper. Section 3 discusses about the background on fingerprint and watermark, related major approaches on IP core protection, while Section 4 presents our proposed low cost symmetrical IP protection HLS methodology. Further, experimental results have been presented in Section 5, followed by conclusion in Section 6.

2. Proposed approach: threat models, target platform and motivation

The novel contributions of the current paper are as follows:

- Proposes *multi-variable fingerprinting methodology that embeds buyer's signature during scheduling and register allocation phases of HLS* to protect the reusable IP core from buyer's perspective.
- Proposes *a symmetrical IP core protection during high level synthesis* that incorporates *seller watermark* and *buyer fingerprint* encoding simultaneously.
- Proposes symmetrical protection methodology obtains *extremely low overhead design* in terms of hardware area and latency.
- Proposes a symmetrical IP core protection methodology offers *higher robustness, lower design overhead/embedding cost, fault tolerance, and faster signature encoding/decoding.*

The above differences also highlight the novelties over our previous work [14]. In this paper, we propose a novel low overhead symmetrical protection methodology for reusable IP core during high level synthesis from both buyer's and seller's standpoint by employing robust fingerprint and watermarking respectively.

Threat model: The proposed work protects a reusable IP core from threats for two different parties: buyer and seller.

- **Threat model for buyer:** Tracing illegally resold/redistributed copies of a reusable IP core by a dishonest IP seller, thus providing exclusive user right to the buyer. Accomplished through buyer fingerprint in proposed work.
- **Threat model for seller:** Protection of ownership of the seller against false claim of ownership. Also protection against IP piracy and IP counterfeiting. Accomplished through seller watermark in proposed work.

Target technology/platform: Our proposed symmetrical IP protection methodology can be easily integrated with any EDA tools of current generation. Hardware description language (HDL) or any high level language used for IP generation can easily merge with proposed technique in the design tools.

Why symmetrical IP core protection at architecture level (during HLS)? HLS for digital ICs is way matured starting from performance optimization, power optimization, to process variation optimization, conducted at the architecture level [15,16]. In the current era of smart devices, reusable IP core based designs are essential to meet the time to market demand where HLS techniques can play more crucial role for the design engineers [17]. So, a natural progression of HLS research is to equip protection feature for reusable IP cores along the other challenges at the architecture level. Symmetrical IP core protection through embedding buyer fingerprint and seller watermark during HLS (during pre-synthesis phase) not only protects the lower level designs but also offers low overhead and lesser complexity/effort in implementation. Therefore, symmetrical IP protection during HLS in the form of concurrently embedded buyer fingerprint and seller watermark not only offers robust protection, low design overhead and low implementation runtime, but simultaneously provides necessary protection to both concerned entities involved.

3. Related prior works

3.1. Background on fingerprint and watermark

Both watermark and fingerprint are the signature provided by two different parties to preserve their right in protection of a reusable IP core. While watermark carries the signature of the IP seller, fingerprint is meant for the IP buyer. In the domain of IP protection a watermark and/or fingerprint should satisfy the following major properties as hidden signature: