A Flexible Pay-per Device Licensing Scheme for FPGA IP Cores

Sudeendra kumar K, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, K.K.Mahapatra
ECE Dept., NIT Rourkela, India
kkm@nitrkl.ac.in

***Abstract*- FPGA based product development companies need third party IP cores to complete the product design time effectively and cost effectively. The one-time payment upfront licensing of IP cores is impractical for FPGA based products, which does not benefit either IP core vendors or product engineering companies. There is a need for good competitive pricing scheme which benefit product development companies and also secure the revenue to IP core vendors. The Pay-per-Device (PPD) pricing model scheme is a suitable pricing scheme. The PPD pricing schemes proposed in the past are complex in terms of communication between different stake holders and inflexible for product development companies to change the FPGA vendor. In this paper, we propose a PPD pricing scheme which overcomes the disadvantages of earlier techniques with better key management and without compromising the security of IP cores. The product development company can change the FPGA vendor at any time in the product life cycle by incorporating the proposed PPD pricing model. The proposed scheme is verified on Xilinx Artix-7 series FPGA.**

***Keywords:* FPGA IP core, Hardware Security, IP Rights.**

I. INTRODUCTION

In last two decades, FPGA device market has evolved into multi-billion dollar market. Starting from the days of glue logic now, FPGA's now host a microcontroller and necessary peripherals along with traditional reconfigurable logic. The cost of FPGA devices reduced drastically in last few years and at present FPGA's are available at competitive prices with commercial microcontrollers. This has led to widespread use of FPGA's in many electronic applications [1]. There is a research interest in FPGA devices in the name of reconfigurable computing which includes self-adaptive hardware systems. The self-adaptive hardware systems are capable of changing hardware functionality during runtime [2]. With the advent of partial reconfiguration, it is possible to update the submodules of design in FPGA hardware whenever required without disturbing the complete design, based on the customer requirement [2]. The companies using FPGA's in their product design will source the IP (Intellectual Property) cores from the IP vendors. Due to time to market pressures, it is inevitable for product engineering/system developers (SD) to depend upon the third party IP cores for different functionalities. IP based design supports design-reuse which also shorten the design time in future projects. The modern FPGA devices and development tools support the IP based methodology by the adoption of standard IP interface buses (ex: AXI etc). It is easy to integrate 3rd party IP cores into FPGA design [3]. However, there is a need to address pricing model and security related issues in FPGA IP core business; otherwise it could hinder the growth of business [4]. IP vendor would have invested money and time in IP development. The IP vendor will generate his revenue by granting IP usage license to other firms involved in FPGA based product development or system integrator. The concerns of IP core vendor are: -

- System Integrators/product companies may extort bitstreams provided by IP vendor as their own. Unprotected IP cores are vulnerable to adversaries who can perform reverse engineering, malicious licensing etc.
- The pricing model is another important concern of IP core developers. One-time payment will give an unlimited access to system developer/product design house. An adversary who has an access to bitstream can easily share with others and misuse. This will lead to revenue loss to IP core vendor [4].

The one-time costly license fee for IP cores is suited for ASIC products. The large volumes of chips are manufactured and Chip Company can generate money for next few years. The one-time costly licensing model will work for ASIC designs. FPGA based products are targeted for small and medium scale production volumes. This will force the FPGA IP core vendors to maintain cheaper licensing models. System developers expect attractive licensing model, safe (No malicious inclusions like hardware Trojans) and authentic IP core with proper legal framework like copyright act for smooth business with IP core vendor [5] [6]. FPGA vendors (FV) (Xilinx, Altera etc) are well aware of security issues connected with design security. Most of the FPGA vendors equip the FPGA devices with secured on-chip non-volatile memory for key storage and hardwired decryption engine to support bitstream decryption. These on-chip cryptographic facilities on FPGA are used to protect the bitstreams getting stolen during porting designs to FPGA [7].

The "Pay Per Device" (PPD) pricing model is presented in [4], will benefit both IP core vendors and system developers. System developer will pay IP core vendors for the number of products getting produced and at the same time, IP core vendor will get recurring revenue till product is under production. The execution of PPD pricing model should be flexible, support multiple cores from the same IP core vendor and should be robust against attacks. The different approaches are presented by various researchers on the execution of PPD pricing model for FPGA IP. R. Maes et al, in [4], propose pay-per use licensing scheme which is designed using available on-chip cryptographic modules in FPGA. The PUF-based FSM binding scheme for PPD pricing is proposed in [8]. This scheme [8] uses PUF CRP to lock and unlock the design functionality. L.Zhang and others propose [9] PPD scheme

978-1-5090-6762-6/17/$31.00 ©2017 IEEE

which is an improvement to [4], which also uses on-chip cryptographic modules in the FPGA. In this paper, we propose an improvement to previous PPD techniques by reducing transactions between different stake holders and better security against attacks. Our contributions are: -

- Designing a PPD pricing scheme to secure the IP cores, which can benefit both SD and IP core vendor.
- The proposed scheme is less complex in terms of design and communication between the different stake holders.
- In the proposed scheme, the SD can change the FV at any time during product life cycle. With earlier techniques, it is difficult for SD to change FV.

In next section we discuss the previously proposed PPD pricing implementation schemes. In section III, we present our PPD pricing model. The section IV discusses the security analysis and implementation of proposed model and finally section V concludes the paper.

II. PRIOR WORK

A. FPGA security issues: - FPGA designs are more vulnerable to attacks than ASIC designs. Duplicating the FPGA design bit streams is much easier than copying or stealing ASIC designs. The well-known FPGA design security issues are: cloning, overbuilding, reverse engineering and tampering. Cloning is an illegitimate copy of original product which is produced without proper licensing and by violating the copyright act etc. Overbuilding is one of the primary hardware security issues in ASICs. And most of the FPGA vendors are fabless and overbuilding of FPGA chips by contract manufacturers located offshore is threat to FPGA vendors. In reverse engineering, adversary will try to analyse the algorithm, implementation technique, design related issues of IP cores. The intention of an adversary may be using IP core illegally or cloning the part or complete IP itself. Finally, tampering can be invasive or non-invasive. Extracting a secret keys or data and physically damaging the product are the general intentions of tampering [10].

B. FPGA design/bitstream security: - Recent FPGA devices with cryptographic modules will support bitstream security/design security. The complete design on FPGA is protected as monolithic IP. This type of security provided by FPGA vendor will support IP core security for upfront licensing (one-time payment). A good IP/design security model supporting PPD pricing will benefit both system developers and IP core vendors [8] [9].

C. Prior Work: - The brief description of three significant PPD pricing models proposed in the recent past is presented in Table I. All three proposals, consider FPGA vendor, System developer and IP core vendor as stake holders. The PPD pricing model proposed by R.Maes, et al [4] need an extra entity called metering authority (MA), a trusted third party to coordinate and to assist IP core installation. MA plays a crucial role when the litigation arises between stake holders. In the first two proposals [4] [9], IP core vendor (ICV) has to register his IP core with FPGA vendor (FV). When the number of ICV's was small in the market, FV's used to enrol IP cores of ICV's based on their target markets. In the current market scenario, many ICV firms (start-up's etc) try to enrol IP core with FV. Due to other major security issues like hardware Trojans (HT's), FV's are reluctant to entertain ICV's. The number of system developers/integrators (SD) or product development companies using an IP core can recommend ICV to FV. In the case of more number of recommendations, FV may enrol ICV's IP core in its IP catalogue. It is very difficult to enrol the IP core with FV for a small and medium scale firms. In the technique proposed by L.Zhang et al in [9], the ICV will share core installation module (CIM) which carries a secret key with FV. FV will install CIM in all the devices supplied to SD and further ICV will work with SD for IP core installation. In this scheme [9], ICV and FV should work closely for the success of PPD pricing model. FV has to take the responsibility of installation of CIM. Every ICV can design a module similar to CIM and ask FV for installation and coordination. It will be difficult for FV to entertain all ICV's. And an adversary at FV, leaks the base secret key from which other keys are derived, then the security of IP core will be fragile.

In the technique proposed by J.Zhang [8], Physical Unclonable Function (PUF) is used as security primitive to implement PPD pricing model. In techniques proposed in [4] and [9], encrypted bitstreams are decrypted on-chip. Keys to decrypt the bitstream for specific device are generated by ICV. In the case of [8], PUF is used to lock the Finite State Machine (FSM), such that functionality will get unlocked only for a set of CRP or keys. In [8], authors did not explain who will collect PUF CRP's prior to installation of IP core. FV should collect CRP's and share with all stake holders in value chain when a PUF is implemented as hard macro. ICV should collect CRP's for all devices on which IP core will get installed. It will be time consuming for ICV to collect PUF CRP's of all devices and maintaining the CRP's safely is a costly affair. Due to commercial issues, if SD wants to change the FV, the ICV has to work with new FV again which is again a time consuming process. Working with all FPGA vendors is not easy for ICV firms. All these issues discussed are not addressed in earlier techniques. With the above literature survey, we can conclude the following: -

- Including all the stakeholders FV, SD and ICV will complicate the PPD model communications and security.
- ICV will be comfortable working with SD, not every time with FV. SD should be free to choose any FV at any time during product design and manufacturing, which is difficult in the above discussed techniques.
- PUF CRP's are vulnerable to environmental conditions. The reliability of CRP's will be affected, which is crucial in licensing/security applications. No FV has announced an inclusion of PUF hard macro in FPGA devices. Implementing PUF on reconfigurable logic will consume more space, for which SD may not agree. Recently Xilinx announced the inclusion of PUF in their future high end Zynq devices [11].
- The best protection to IP cores targeted to FPGA can be designed at bitstream level, which is generated at final stage of design flow. And it is easy to encrypt the bitstream using a cryptographic algorithm and can be sent to customer through public channels. So it always better to design IP core security at bitstream level, to secure the interests of ICV.

- There is a need to design a security scheme to support PPD pricing model in which ICV can independently work with SD. FV can be involved during very high volume production requirements. For small or medium scale production targets, ICV and SD can work together to protect the mutual interests.

D. General FPGA business model: - The SD or product development companies will develop designs on evaluation boards initially supplied by FV [12]. Gradually with the help of FV, custom boards/proof of concept boards are developed and design is validated. When the production volume is small, the SD will source the required FPGA from the open market and develop production boards. Design is deployed on the production boards and sold to customer. When there is requirement for very large volumes, SD will share bitstream/design to FV. FV will have different set of devices meant for high volume production, which works only for specific customer/bitstream. Xilinx EasyPath FPGA devices/Altera HardCopy are good examples [13]. Translating the design from common FPGA to EasyPath (or any other FV equivalent) will reduce the cost of the device and it will be competitive to ASIC equivalent. So when there is need for large scale production of FPGA products, SD will translate their design into Xilinx Easypath or its other FV equivalent.

Initially, ICV will work with SD to sell their IP core. ICV will optimize or remodel the IP core for SD requirement and allow SD to evaluate the IP core. After evaluation, SD will decide on the inclusion of IP core from ICV or look for any other alternative. Evaluation period is normally for few weeks. The ICV should provide license to SD for a limited period to access IP core for evaluation. After evaluation, once production prototype is complete, the SD will decide on production volume. The production volume is small, SD will source FPGA from open market and ask for ICV to provide IP core license for each FPGA device. In this type of cases, the coordination between FV, SD and ICV is not required. Directly ICV should be able to provide license for given number of FPGA's to SD. In the case of mass production, SD and ICV should work with FV to license IP cores in design specific/customer specific FPGA parts.

Design specific FPGA solutions (ex: Xilinx easypath) offer cost reduction for complex platform FPGA designs. Design specific FPGA's provide fast, seamless, low NRE, easy migration of generic FPGA designs to high volume production without any re-qualification or engineering effort. Only NRE expense for design specific FPGA's is to create the design specific test program using FPGA vendor specific test pattern generation tools for post-production testing. This type of devices will free the companies from burden of ASIC conversion of designs. FPGA prototype can migrate to high volume production without much cost and engineering effort [13]. The design specific FPGA's can be configured on-field for pre-defined bitstreams for which they are custom manufactured. Few devices (ex: Xilinx Virtex-4) support two pre-defined bitstreams in their easy-path equivalents.

In this FPGA business model, ICV has to protect the IP cores during: -

- When SD is evaluating the IP core prior to purchase.
- When SD transfer design to production prototype, ICV will collect details of FPGA devices which SD has procured from open market to enable the IP installation on the FPGA devices. (in the case of small and medium scale production)
- When SD plans for mass production, ICV has to share the IP core bitstreams with FV. ICV has to protect IP core during this phase also.

There is a need design the security infrastructure supporting PPD pricing model which address all the above discussed concerns of ICV. In this paper, we propose a PPD pricing model to serve interests of both ICV and SD. In the proposed PPD pricing model, ICV can work with SD independently without involvement of FV and any other trusted third party. Only when there is a requirement for mass production of design, ICV and SD has to work with FV for IP security issues.

III. Proposed PPD Pricing Model

A. Prerequisites: - Most of the modern day FPGA devices are equipped with on-chip cryptographic modules to support bitstream security. Another mandatory inclusion found is Device Identifier (DI) in all FPGA devices irrespective of FV. Generally, the on-chip cryptographic modules are symmetric decryption engine (commonly AES, ex: Xilinx Virtex series FPGA's and Arria and Stratix series FPGA's) and cryptographic hash algorithm (HMAC) for bitstream authentication. The earlier PPD pricing techniques [4] and [9] will make use the DI, HMAC and decryption engine. It is difficult and uneconomical to design a PPD pricing model without on-chip cryptographic hard macros. In this paper, we design a PPD pricing model using DI and on-chip cryptographic macros.

The ability of dynamically changing the functionality in order to suit the situation will make FPGA's best fit into the Internet of Things (IoT). Partial reconfiguration technology has made reconfigurable systems more versatile in IoT. External reconfiguration ports like JTAG interface are driven by external devices such as PC etc, are used to port bitstreams into FPGA devices. Modern FPGA devices from few years support Internal Configuration Access Port (ICAP) which can be directly accessed by other modules inside FPGA, which helps in reconfiguration of its own structure during run time. In Xilinx devices, access to ICAP is generally through OPBHWICAP peripheral attached to OPB bus. This method will occupy large amount of logic space, as it needs software driver running on the processor in FPGA and system buses connected to it. There are several other methods of connecting ICAP are described in [14].

B. Evaluation of IP core from SD: - ICV will provide evaluation license to few IPs to potential customers. It is routine part of the business and will give wide publicity to the IP core. ICV will get feedback about their product from the potential customers. IP evaluation is also an important step for SD, since it helps SD to understand the IP core parameters like correctness of design, power, performance, number of logic blocks consumed, configurability, portability across different FPGA's, testability and compatibility with other modules in the design. SD can also look for alternative IP cores in the market and take comparison between IP cores on

different parameters before taking a decision. Allowing IP cores for evaluation may lead to IP piracy, which will lead to loss of revenue to ICV. It is not a good business model to lock the evaluation IP for single device by applying PPD model. There are several techniques available to protect IP cores during evaluation [12]. An extra timing/counter circuitry is added to design; such that once counter overflows, design functionality is locked. The overflow time may be two to four weeks. When this type of techniques are used for IP core protection during evaluation, SD is allowed only to access the bitstream not soft IP as in the case of up-front one time licensing.

C. Description of proposed model: - The figure 1 shows the block diagram of proposed PPD pricing implementation (PPDI) module (PPDI). PPDI comprises of DI, Hash function, Symmetric Decryption unit and RSA Decryption unit and ICAP. The DI, Hash function, Symmetric Decryption and ICAP are on-chip infrastructure which is available in most of the FPGA's as hard macro's. And this on-chip security infrastructure can be accessed by an application program. PPDI is designed using on-chip security infrastructure and an extra RSA decryption block. The arrangement and connections between the different blocks is shown in figure. 1.

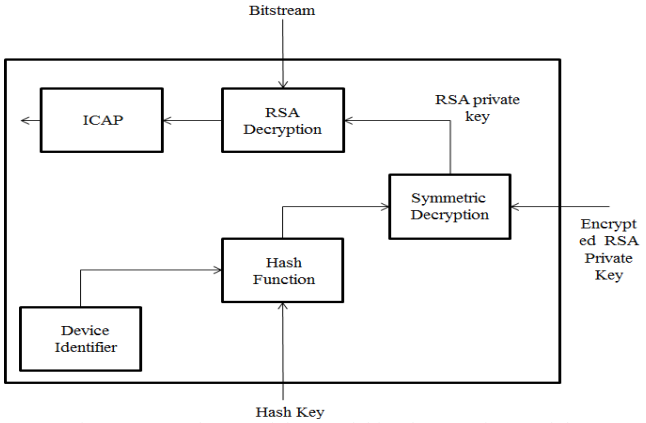

Fig. 1.Proposed PPD pricing model implementation module

The functional description of the PPDI is as follows: -

1. Once evaluation of IP core is completed, SD will start making production prototype boards. Even at this stage, ICV can support SD with limited period evaluation bitstreams of IP core to validate the production prototypes.
2. When SD freezes the design for production and procures the required number of FPGA's for small and medium scale manufacturing of product. ICV will collect the device identifier (DI) of every FPGA device procured by SD for production operations.

The following are performed by ICV: -

1. ICV will encrypt the bitstream with RSA algorithm and encrypted bitstream is sent to SD.
2. Device Identifier is hashed with key and digest is created. The hash digest is used as key to encrypt the RSA private key using symmetric cryptography (like AES in Xilinx FPGA's) which is also used to decrypt the bitstream.
3. The key used for hashing DI, encrypted RSA key, encrypted bitstream is sent to SD.
4. ICV will also send the PPDI program/bitstream to SD and SD will install it on all FPGA devices used in manufacturing the product.

The SD will perform the following: -

1. Install the PPDI in all the FPGA devices procured for manufacturing.
2. Decrypt the bitstream by pumping in the hash key and encrypted RSA key into the PPDI.

In each device, PPDI installed and SD can keep PPDI installation permanently or can erase after successful installation of IP core. After successful installation of IP core, SD can erase the RSA decryption block. SD needs to install the PPDI again during upgradation or to update the IP core, when ICV release the new versions. In the proposed method there is no need to store the key either permanently on non-volatile memory or in a temporary register. In the case of high volume production, the SD will use design-specific devices (ex: - EasyPath in Xilinx). In high volume production cases, ICV will share its IP core bitstreams with FV. To implement PPDI, ICV will request FV with the approval of SD to add RSA decryption block into the device. ICV will share RSA decryption bitstream along with IP core bitstreams.

IV. Implementation and Security Analysis

Security Analysis: - SD or an adversary in SD can try to tap out the bitstream of IP core or RSA private key used for encryption. The PPDI is sent to SD as a bitstream. Bitstreams can be debugged using high end tools. SD can understand the architecture of PPDI. And an adversary at SD can assume, RSA private key can be tapped easily after decryption. RSA private key is dynamic and different for different devices. Even though there is no direct link between RSA private key used to decrypt the bitstream of IP core and device identifier, ICV will maintain a different private RSA key for each device of SD. So it is nearly impossible for SD to install IP core on any other device out of license. The proposed technique is safe, as there is no storage of secret key in non-volatile memory or in any temporary registers. Installation of IP core using PPDI and following all steps by SD and ICV, the IP core is protected by cloning and reverse engineering by low and middle class adversaries. FPGA internals can't be accessed by low and middle class adversaries and bitstream remains secret once it installed in product.

In the large scale production, design-specific FPGA's are used by SD. Even in such cases, PPDI will work similar as in the case of general FPGA devices. Sharing bitstreams of IP core with FV can be seen as security threat. Generally, FV are trusted in the cases of high volume businesses.

TABLE I
DESCRIPTION OF PPD PRICING IMPLEMENTATION TECHNIQUES FROM LITERATURE

Sl.No	Technique	Description	Disadvantages

1	R. Maes [4] et al. (2012)	• Device identifier (similar to Xilinx Device DNA is used as base number and a Metering Authority (MA) will help in secure key communication between core vendor and system developer. The encrypted bitstream is decrypted on-chip using keys loaded by MA.	• ICV has to pay MA for co-ordination, which makes IP core costly. • FPGA vendors may not agree to work with extra entity like MA. • Major disadvantage is more number of communications between different stake holders. • SD can't change FV once production is started.
2	L. Zhang [9] et al (2014)	• In the place of MA, this proposal will place a faith FPGA vendor (FV). FPGA vendor will load the secure infrastructure (Core Installation module (CIM)) which carries secret key for further secure installation of IP cores. Device ID plays a crucial role.	• Enrolling an IP with FPGA vendor for IP core firm is not an easy task. • Secret key is not very secure and adversary at FV can leak the key easily. • SD can't change FV once production is started.
3	J. Zhang [8] et al (2015)	• Physical unclonable function (PUF) based IP licensing and protection scheme. • Based on PUF-CRP's on each device are collected prior to installing IP core.	• PUF consumes enormous amount of logic space on FPGA. There is no FPGA device in market with PUF as a hard macro, which will be highly helpful in the implementation of this technique. May be future releases of FPGA devices carry PUF hard macros, limited to high-end devices. • Collecting and managing the large number of CRP's is difficult task for ICV.

TABLE II
COMPARISON BETWEEN PROPOSED PPDI AND EARLIER TECHNIQUES

Parameter	Roel Maes [4]	L.Zhang [9]	J.Zhang [8]	Proposed PPD
Trust	An extra trusted entity called Metering Authority (MA) is involved. All stake holders will have trust in MA.	Core Installation Module (CIM) is installed by FV. This technique trusts the FV completely.	PUF CRP collection of each FPGA device, its secure transmission and storage is very important for the success of this technique.	In the proposed PPD, encryption of bitstreams and RSA key management (encryption of private RSA key and distribution) must be in the trusted hands. And for large volume manufacturing FV is trusted
Communication between stake holders	Communication is complex. Data is exchanged between FV, ICV, SD and MA. ICV has to pay fee to MA, which makes IP core costly.	Complex communications involved between ICV and FV, ICV and SD.	Relatively Simple. The FV is not involved. Data is exchanged between ICV and SD.	Relatively Simple. The FV is not involved. Data is exchanged between ICV and SD. SD can change FV any time during product life cycle.
Complexity	Technique is relatively simple. It does not need an extra block designed and added to implement PPD pricing model.	Complex. Make use all on-chip crypto modules and extra NVM's required for implementation.	Complexity is high due to inclusion of PUF. Handling large number of PUF CRP's increase complexity.	Relatively simple in comparison with other techniques. An extra RSA decryption block required for implementation.
Security	Secure. Bitstream read back facility must be disabled.	Secure. An adversary in FV should not leak the secret key.	Secure. PUF CRP's must be handled securely.	Secure. Only trusted people should be allowed handle RSA keys at ICV.

Implementation: - Any application program can access DI and other on-chip cryptographic modules. To install the IP core the procedure is as follows: -

- ICV will send PPDI to SD. SD will install it in all devices.
- SD will pump in hash key first and once hash digest is created, signal is generated which is connected to LED,

which confirms hash digest is created successfully for the user.

In the next stage, the encrypted RSA private key and bitstream is fed at appropriate inputs, to get IP core installed.

The proposed PPDI is verified on Artix-7 devices. Nexsys 4 board is used for implementation. PPD pricing model implementation has become much simpler with the advent of partial reconfiguration technology. Most of the modern day FPGA's support partial reconfiguration.

Comparison between proposed PPDI and earlier techniques: -
Comparison between the proposed technique and other earlier techniques is presented in Table II. The comparison is performed based on the trust, complexity, security and number of data transfers required between different stake holders. When PUF is available as hard macro in commercial FPGA's, the technique proposed by J.Zhang [8] will become more attractive. The advantage of proposed technique is it does not require a non-volatile memory to store secret key in comparison with earlier techniques. RSA cryptosystem generate more dynamic keys which make the proposed PPDI more secure.

V. Conclusions

In this paper, we have proposed a pay-per device licensing scheme, which simplifies the communication between different stake holders and improve security of IP core. In the proposed scheme: - IP core vendor will have more flexibility in working with system developers and product engineering companies. There is no requirement for IP core vendor to work with FPGA vendors and no need to store the key in non-volatile memory or temporarily which makes IP core more secure. SD will have a flexibility to change the FV at any stage during product life cycle. RSA cryptosystem is used along with available on-chip cryptographic circuits which makes the key management easy for IP core vendor. The proposed scheme for the implementation of PPD pricing model is beneficial for securing the IP cores and also flexible for system developers to adopt. This will reduce the costs for system developer and secure recurring revenue flow to IP core vendor.

References

[1] C.Maxfield, "The Design Warrior's guide to FPGAs: Devices, Tools and Flows" 1st edition, Amsterdam, The Netherlands, Elsevier-2004.

[2] Dirk Koch, "Partial Reconfiguration of FPGAs: Architectures, Tools and Applications", Lecture notes in Computer Science, Vol-153, Springer-2013.

[3] AXI4 Interconnect Paves the Way to Plug-and-Play IP (V1.0), Xilinx, San Jose CA, USA, Oct, 2010.

[4] R.Maes, D.Schellekens and I.Verbauwhde, "A pay per-use licensing scheme for hardware IP cores in recent SRAM-based FPGAs", *IEEE Trans. Inf.Forensics Security*, Vol.7, no.1, pp. 98-108, Feb-2012.

[5] Xilinx, "*Common License Consortium for Intellectual Property*", http://www.xilinx.com/products/allaince/signonce.htm.

[6] S. Drimer, T. Guneysu, M.G. Kuhn and C.Paar (2008), "*Protecting Multiple FPGA cores in single FPGA design*" http://www.cl.cam.ac.uk/~sd410/papers/protect_many_cores.pdf.

[7] S.McNeil, Solving Today's Design Security Concerns(V.1.2), San Jose, CA, USA: Xilinx, Jul-2012.

[8] J.Zhang, et al, "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-PerDevice Licensing" *IEEE Trans. on Information Forensics and Security*, Vol.10, Issue 6, June-2015.

[9] L.Zhang et al, "A Pragmatic Per-Device Licensing Scheme for Hardware IP Cores on SRAM-Based FPGAs" *IEEE Trans. on Information Forensics and Security*, Vol.9, Issue 11, Nov-2014.

[10] "Protecting the FPGA design from common threats (v1.0)", Altera San Jose, CA, USA, Whitepaper 01111, Jun-2009.

[11] Graham prophet, "Xilinx to add PUF security to Zynq devices" EE Times, Europe, http:// www.electronics-eetimes.com/news/xilinx-add-puf-security-zynq-devices-0.

[12] S.Narasimhan et al, "Hardware IP Protection during evaluation using embedded sequential Trojan", IEEE Design and Test, Issue 99, Aug-2012.

[13] Xilinx, "EasyPath FPGA Explained", https://www.xilinx.com/products/easypath/files/EasyPath_FAQ.pdf.

[14] Victor Lai and Oliver Diessel "ICAP-I: A reusable interface for the internal reconfiguration of Xilinx FPGAs", International Conference on Field-Programmable Technology, (FPT-2009) 9-11Dec-2009.