http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (6): 1107-1115, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1107.1115

A Robust Hierarchical FSM Structure for Active IC Metering

Wenjie Che, Yaping Lin, Aobo Pan and Jiliang Zhang
College of Information Science and Engineering, Hunan University,
No. 252, Lushan South Road, Changsha, 410082, China

Abstract: Security is the key issue for active IC metering schemes. A hierarchical FSM (HFSM) structure combined with Physically Unclonable Functions (PUFs) is proposed to improve the robustness against brute-force attacks for a classic active IC metering scheme. The proposed HFSM structure uses the PUF outputs to determine the transitional path and then the rest input bits are utilized to improve the security of the structure. The security level of the proposed scheme is analyzed and is compared with the related scheme with the growth of added structure layers. Experiments are conducted to study and compare the area, power and delay overhead of the two schemes. Experimental results on the MCNC'91 benchmarks show that the scheme has exponentially improved the security level with an acceptably low overhead cost.

Key words: Active IC metering, IC overbuilding, physically unclonable function, finite state machine

INTRODUCTION

In the prevailing semiconductor horizontal business model, the asymmetric relationship between the manufacturer and designers introduces threats for protecting the designers' rights: the manufacturer has full access of the masks and design files and the detailed process of manufacturing chips is nontransparent to the designer, resulting in the lack of control of the post-fabricating process for the ICs. Illegal IC replicas bring a huge revenue loss to the designers and reduce their ability to invest in research and development (R and D) (AGMA, 2005). Therefore, preventing IC piracy, theft and overbuilding has become more intense recently for the government, industry, businesses and even defenses.

Various Digital Right Management (DRM) techniques, such as hardware watermarking, hardware metering and fingerprinting, have been proposed by researchers to prevent IC piracy, theft and overbuilding. Hardware metering is proposed and generally defined as a set of security protocols that enable the design house to gain post-fabrication control by passive or active control of the number of produced ICs, their properties and use, or by runtime disabling of ICs in case of tamper detection (Koushanfar and Qu, 2001; Koushanfar *et al*., 2001). Note that hardware metering is different from hardware watermarking, which aims to uniquely identify each IP, not each chip, by embedding a tag into a certain IP (Zhang *et al*., 2012a, b). Hence, watermarking is not effective in countering overbuilding problem because it fails to distinguish different chips produced by the same mask. The basic idea of the first hardware metering scheme (Koushanfar *et al*., 2001) is that the scheme uses a small part of the design to embed a unique signature for each IC by utilizing configurable technology; however, the scheme is passive. Alkabani and Koushanfar (2007) introduced the first active metering scheme in 2007 . The method adds an exponential number of states to the original FSM and each chip randomly powers up to one of the added states according to the unique response of Physically Unclonable Functions (PUFs). PUFs are objects that exploit process variations to generate unique IDs for each chip (Busch *et al*., 2010). Another active metering scheme (S and R scheme) is proposed through selecting several original FSM states and then replicates each of them and edges multiple times to form a locking structure (Alkabani *et al*., 2007). The transitional inputs are function of two-bit RUB outputs, unless a two-bit key is provided, the design can never jump to the next state. However, the security level mainly depends on the length of the provided keys and increasing the key length results in a linear increase of the locking structure, which generates a comparatively large overhead.

This study proposes a hierarchical FSM (HFSM) structure merged into the functionality of the design combined with PUF to prevent the overbuilding problem.

Corresponding Author: Yaping Lin, College of Information Science and Engineering, Hunan University, No. 252, Lushan South Road, Changsha, 410082, China Tel: 86-731-88821932 Fax: 86-731-88821977

Contributions are as follows:

- A robust HFSM structure for active IC metering is introduced. The introduced FSM structure uses the PUF outputs to determine the transitional path and then utilizes the rest input bits to improve the robustness against brute force attack. Security analysis shows the proposed scheme has improved the security level exponentially compared to the S and R scheme
- Sufficient experiments are conducted to demonstrate that the proposed scheme has an acceptably low area, power and delay overhead. Attacks and countermeasures for the proposed scheme are discussed

PRELIMINARIES

Physically unclonable functions (PUF): These are objects that provide a mapping from their inputs (challenges) to outputs (responses) which is based on the manufacturing variations. As the manufacturing variations are randomly determined by the chip's inherent physical properties, the uniqueness of every Challenge-Response Pair (CRP) is therefore ensured. Therefore, PUFs can be used to produce unique and uncloneable chip IDs that can be integrated embedded within the functionality of design for the active metering scheme.

Finite state machine (FSM): In digital design, sequential functionalities of the circuits are modeled by FSMs. FSMs are a set of finite states, transitions between states, inputs and outputs during the transitions. It is formally defined as a 6-element tuple:

$$M = (\Sigma, \Delta, Q, q_0, \delta, \lambda)$$

where, Σ and Δ are non-empty sets of inputs and outputs, respectively; Q is a finite set of states, among which q_0 is the reset state; $\delta(q, a)$ is the state transition function on q and a $(Q\times\Sigma\rightarrow Q)$, while $\lambda(q, a)$ denotes the output function on q and a $(Q\times\Sigma\rightarrow\Delta)$, where, q and a denote the current state and input, respectively in δ and λ definitions. The transition of the states, the inputs and outputs in FSMs are represented by a State Transition Graph (STG).

Design description: As mentioned in the horizontal model of the IC industry, the design files are sent to foundries in the form of layout and net-lists files which are called the manufacturing files. While high-level behavioral descriptions are not accessed by the manufacturers. This is not only because the low-level design description files are already sufficient to fabricating the products, but the behavioral-level descriptions is the target form of design that need to be protected by designers. During the IC design flow, the behavioral description will first be mapped by the designer to a specific technology.

PROPOSED SCHEME

Overflow of the proposed scheme: A closer look at the proposed scheme flow is illustrated in Fig. 1. There are also two entities in the proposed scheme: (1) a design house who is the IP owner of the IC and (2) a foundry house that is responsible for manufacturing IC chips. The overall flow is described as follows. First, the designer extracts the original FSM and then adds the hierarchical FSM (HFSM) structure to it for forming a locking structure. Then the designer sends the manufactured specification files to the foundry to produce a required number of IC products. Each manufactured IC will be

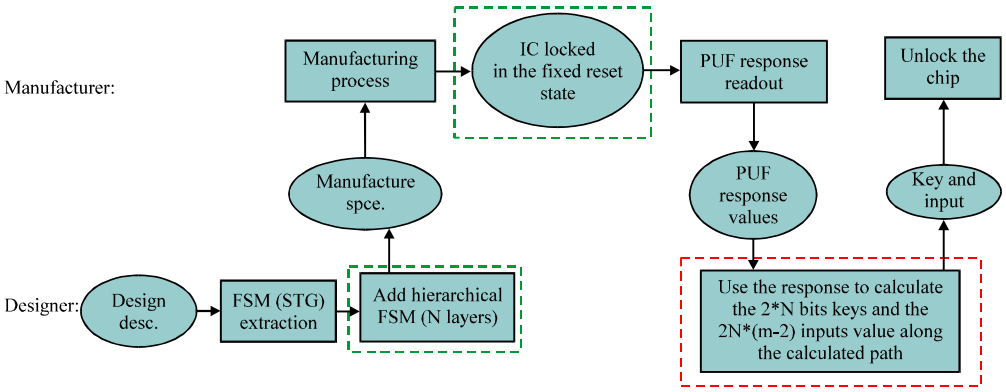

Fig. 1: Overall flow of the proposed HFSM scheme, N represents the number of added HFSM layers, m is the length of the input

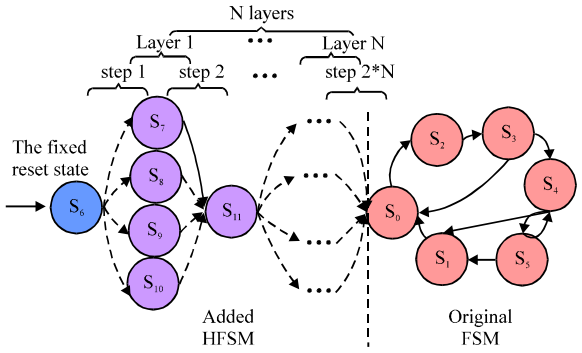

Fig. 2: Proposed HFSM structure merged with the original FSM, N represents the number of added HFSM layers

uniquely locked by the HFSM structure due to the uniqueness of its PUF output sequence. As the designer is the only entity who designs the HFSM, the manufacturer has to turn to him to unlock the chip. To achieve this, the manufacturer first needs to read out the unique PUF response and send it to the designer. Next, the designer uses the received PUF response and the N-layer HFSM structure to figure out the unlocking paths, and then send the 2*N bits keys and the input value along this unlock path back to the foundry. The manufacturer then uses the received N*2 bits key and the N*2(m-2) bits input values to unlock and activate each locked IC.

Hierarchical FSM (HFSM) structure: Figure 2 depicts the overall HFSM structure merged with the original FSM. In the merged design, the first state of the added HFSM S_R is assigned as the new fixed power-up state. The added FSM is a hierarchical-like structure: each layer consists of five states forming two transition steps. The first transition step begins from a top state with four transitional edges connected to the other four states. Then the second transition step goes from each of these four states to the top state of the next layer. After N layers transitions (2*N transition steps), the design will transition to the original reset state S_0, which is the unlocking state, as shown in Fig. 2.

Assume the transitional input of the original FSM is m-bit long, then the m bits input is defined as a sequence:

$$\{b_1b_2\ldots b_k\ldots b_m\}_i^j,\ 1\le k\le m,\ 1\le j\le 4,\ 1\le i\le 2N$$

where, b_k stands for the k-th bit, j denotes the j-th path in a transitional step and i represents the i-th transition step in an N-layer (2N transitional-steps) HFSM. In each

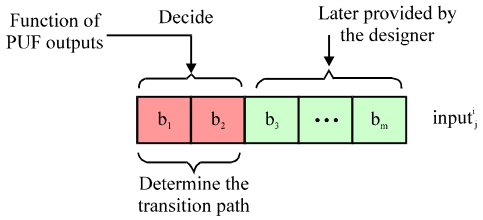

Fig. 3: Structure of the m-bit transition input for the HFSM, m represents the length of input bits, j denotes the jth path in a transitional step, and i represents the ith transition step in an N-layer (2N transitional-steps) HFSM structure

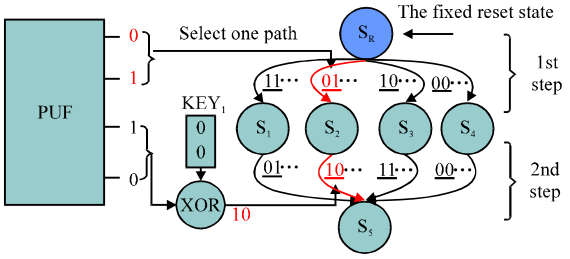

Fig. 4: One-layer HFSM structure

transitional step, the m-bit inputs are divided into two parts: the first two bits $\{b_1b_2\}_i^j$ and the rest (m-2) bits: $\{b_3\ldots b_m\}_i^j$, shown in Fig. 3. The first two bits $\{b_1b_2\}_i^j$ are the function of a two-bit PUF outputs and it is used to determine the transition path in the transitional step. The rest (m-2) bits of the determined path will be later provided by the designer to enable the transition step and hence this part is used to enhance the security of the structure.

A one-lay HFSM structure is composed by two transitional steps, as shown in Fig. 4; each step consists of 4 edges, the first two bits of them are pre-designed to be 4 different values in the 4 edges. The value of the first two bits inputs of the 1st transitional step will be decided by a two-bit PUF output to select a path, while the first two bits inputs of the 2nd transitional step depends on the "XOR" result of another two-bit PUF with a two-bit key. For example in Fig. 4, as the first two PUF outputs value is "01", which equals to the pre-designed $\{b_1b_2\}_1^2$, thus the first transition step will transition from S_R to S_2. Then in the second transition step, the design can only possibly transition from S_2 to S_5 when the first two input bits are equal to $\{b_1b_2\}_2^2$ "10". Thus, the second two PUF outputs "10" should be XOR'd with a two-bit key that is able to generate the result "10" (in this case the key is "00").

The 4-bit PUF outputs determine the transition path in a layer as is illustrated above. However, to enable the

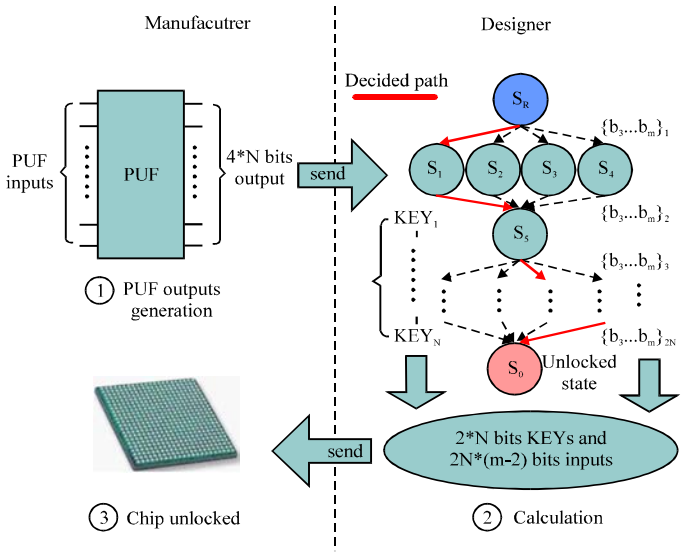

Fig. 5: Unlocking process of an N-layer structure

determined transition, the value of the rest (m-2) bits inputs of each transitional step should be further provided. Therefore, the manufacturer needs to send the PUF outputs to the designer to get the two-bit key value and the rest 2*(m-2) bits input of the decided path in one layer. Then the manufacturer is able to enable the transition in a layer.

Unlocking process: As each layer needs 4 PUF bits and a two-bit key value, for an N-layer HFSM structure, 4*N bits PUF outputs are needed and 2*N bits keys should be provided.

The unlocking process is presented in Fig. 5. After being manufactured, each chip will be provided a specific set of PUF inputs. Upon powering up, each chip is locked into the fixed top state S_R. To unlock a chip, the following steps need to be implemented.

- Generation of the unique PUF outputs. The manufacture uses the provided PUF inputs to generate the unique PUF outputs for the chip and the unique 4*N bits PUF outputs are then sent to the designer
- Unlocking path calculation. The designer uses the received 4*N PUF outputs to calculate the decided path in the N layers and then provide the corresponding 2*N bits key and the 2(m-2)*N bits inputs along the decided path to the manufacturer
- Unlock the chip. With the received 2*N bits key and the 2(m-2)*N bits input sequence, the manufacturer is able to correctly activate the chip. Through 2*N transitions from the reset state S_R to the unlocking state S_0, the chip then can be finally unlocked by the provided unlocking keys

The unlocking process provides a more secure way to uniquely unlock each chip due to the expanded 2(m-2)*N bits inputs sequence. The designer is able to take an efficient remotely control over the legal manufactured chips from the foundry and thus achieve an active IC metering.

SECURITY ANALYSIS

We consider the following scenarios to analyze the security resilience of the proposed HFSM structure.

Brute-force attack: This kind of attack aims to guess the N*2 correct key values and rest N*2(m-2) bits inputs along the determined path to unlock an N-layer structure, thus the security level is $2^{N*(2m-2)}$. As is analyzed above, the robustness is exponential to the original input bits m and the number of added HFSM layers N. Thus, this attack can be prevented by increasing number of layers in the designed HFSM.

Reverse engineering of HFSM: This attack aims to infer the added HFSM structure from the manufacturing files received from the designer. However, this process is regarded computationally intractable; because a successful reverse-engineering would require the re-fabrication of new ICs, something extremely costly and time consuming (Huang and Lach, 2008).

Combinational redundancy removal: The attackers try to remove the combinational logic part which is not essential for the proper functionality of the design. Merging of the HFSM structure within the original sequential functions

makes this attack ineffective. Besides, attackers have to compute a set of reachable states, which can only be done and applicable for relatively small circuits (Alkabani and Koushanfar, 2007).

PUF emulation and removal/tampering attack: The emulation attack tries to construct a model that is able to simulate or emulate the PUF behaviors on the hardware. If it succeeds, the characteristic of the hardware PUF is cloned and thus the PUF CPRs behavior can be predicted. The state of art of the PUF technology makes this attack impractical (Majzoobi *et al*., 2008a, b). As to the removal/tampering attack, attackers try to find the structure and then remove or temper PUF's structure. This attack can be prevented by the integration of the PUF signal to the timing part of the functional description. In this way, once the PUF structure is changed or removed, the timing behavior will be destroyed or affected. Note that the another potential risk may lie on the instability of the PUF's uniqueness, a lot of work of how to adjust the error and unstable bits of PUFs has been proposed to ensure a reasonable stability of the responses (Yu and Devadas, 2010) and one assumption made in this study is that the PUF used is able to generate stable responses.

EXPERIMENTAL EVALUATIONS

Experimental setup: The sequential benchmarks from the MCNC'91 set are used for experiments and the Berkeley SIS tool is used for synthesis. The area, delay and power overheads using our scheme and the S and R scheme are studied and compared. The sequential benchmark files are modified in KISS format which can be read and processed by SIS. Note that a series of pure SIS mapping commands are used without optimization because different combinations of optimization commands result in different overhead results, it is difficult to adjust a combination of optimized commands that performs the same experimental parameters with the S and R scheme. Each original FSM benchmark is modified by adding 1-10 layers using our scheme and correspondingly, by selecting 1-10 original states for replication (each state is replicated 3 times) using the S and R scheme.

Improved robustness against brute force attack: In the structure proposed in the S and R scheme, the input value of each transition is only 2 bits and it is the function of a two-bit PUF outputs. The security level of a one-layer structure only depends on the length of the provided two-bit keys, thus the security level is 2^2. While in the proposed HFSM scheme, an attacker not only needs to guess out the 2 bits key in a layer but also to figure out the other 2*(m-2) bits input value in a layer. Hence the security level of one layer is 2^{2m-2}. Therefore, compared with the S and R scheme, the security level of the proposed HFSM is improved by $2^{[2*(m-2)]}$ for one layer and thus is improved by $2^{[N*2*(m-2)]}$ for an N-layer structure. The security level against brute force attack of the two schemes is compared when N layers are added, respectively. The security level using the proposed scheme is improved exponentially to the input length m and the number of added layers N.

Table 1 records the security level of the two schemes increased with the layers N on the 8 tested benchmark circuits. The second column shows the input length m of the tested benchmarks. It can be seen from Table 1 that the security level of our scheme increases exponentially not only with the number of added layers N but with the input length m, while that of the S and R scheme only increases exponentially with N. The table lists the security level of the two schemes when 1, 5 and 10 layers are added to the eight benchmarks, respectively. We can see that using our scheme, the average security level of the eight benchmarks has been improved by $2^{N*16.6}$ when N layers are added compared to the S and R scheme. For adding 10 layers, our scheme is more secure against brute force

Table 1: Security level by adding N layers using the two schemes on the 8 benchmarks

		Security level of the proposed HFSM scheme				Security level of the S and R scheme				
Benchmark	Input length m	N layers	N = 1	N = 5	N = 10	N layers	N = 1	N = 5	N = 10	Improved security N layers
styr	9	2^{N*16}	2^{16}	2^{80}	2^{160}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*14}
s1494	8	2^{N*14}	2^{14}	2^{70}	2^{140}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*12}
sand	11	2^{N*20}	2^{20}	2^{100}	2^{200}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*18}
planet	7	2^{N*12}	2^{12}	2^{60}	2^{120}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*10}
s510	19	2^{N*36}	2^{36}	2^{180}	2^{360}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*34}
s298	3	2^{N*4}	2^4	2^{20}	2^{40}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*2}
s1488	8	2^{N*14}	2^{14}	2^{70}	2^{140}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*12}
s832	18	2^{N*34}	2^{34}	2^{170}	2^{340}	2^{N*2}	2^2	2^{10}	2^{20}	2^{N*32}
Average	10.3	$2^{N*18.6}$	$2^{18.6}$	2^{93}	2^{186}	2^{N*2}	2^2	2^{10}	2^{20}	$2^{N*16.6}$

N represents the number of added HFSM layers; m is the lenght of the input

attack by 2^{166} on average of the eight benchmarks. Figure 6 depicts the exponential growth of security level of the two schemes by adding 1-10 layers on the eight benchmarks. The figure represents the data in semi-log coordinates where the horizontal coordinate stands for the number of linear added layers and the vertical

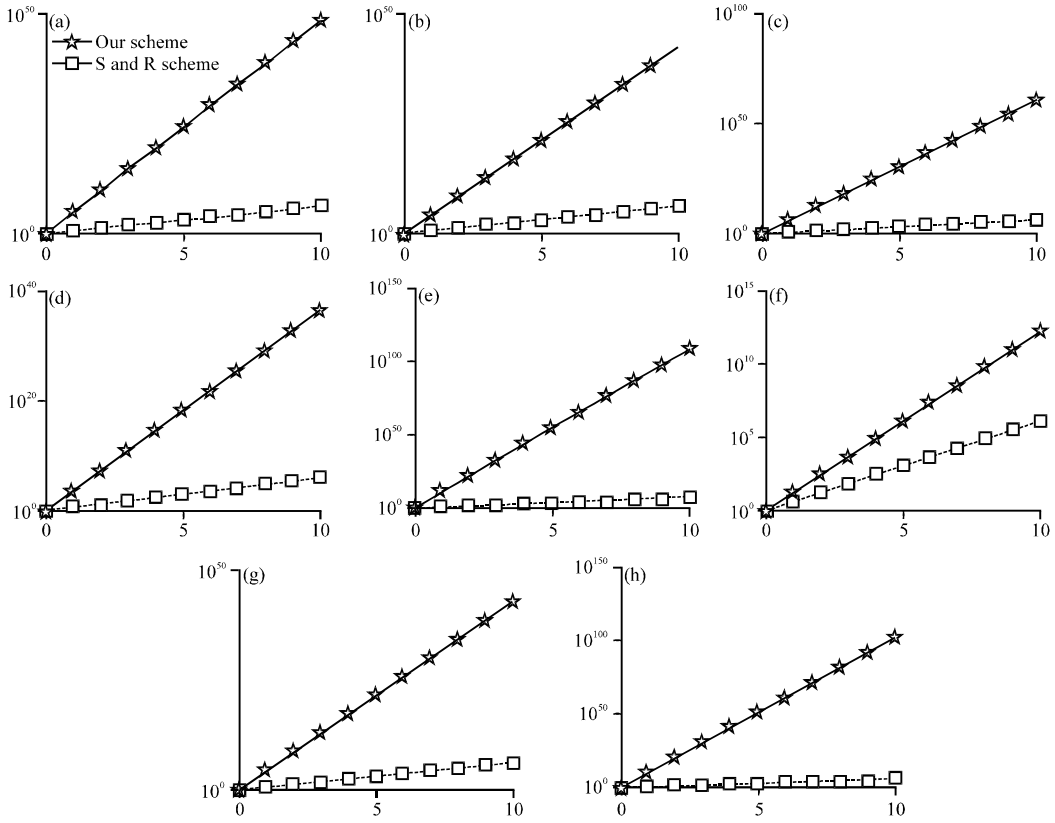

Fig. 6(a-h): Security level by adding 1-10 layers of the two schemes on the 8 benchmarks, (a) Styr, (b) s1494, (c) Sand, (d) Planet, (e) s510, (f) s298, (g) s1488 and (h) s832

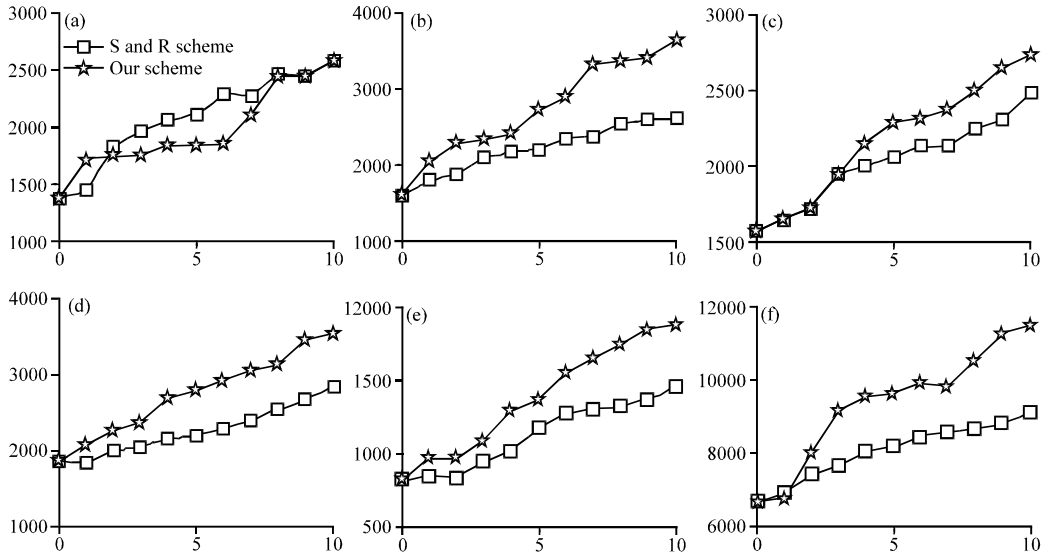

Fig. 7(a-h): Continue

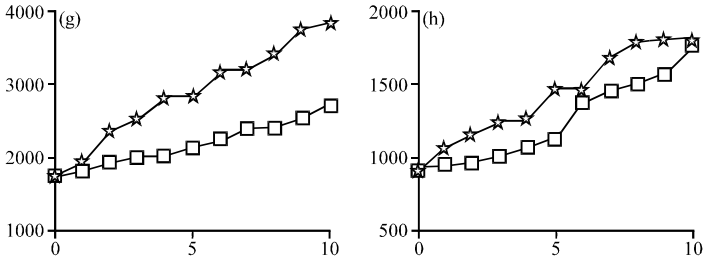

Fig. 7(a-h): Area overhead by adding 1-10 layers using the two schemes on the 8 benchmarks, (a) Styr, (b) s1494, (c) Sand, (d) Planet, (e) s510, (f) s298, (g) s1488 and (h) s832

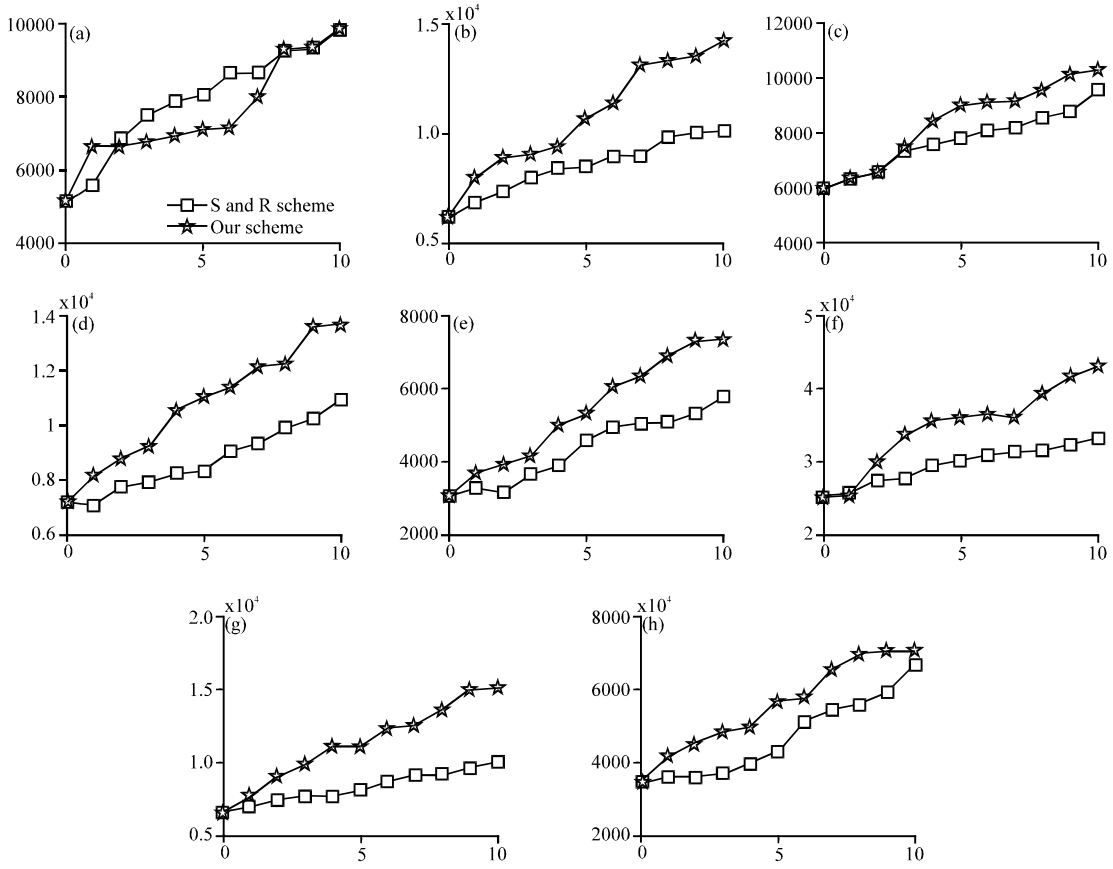

Fig. 8(a-h): Power overhead by adding 1-10 layers using the two schemes on the 8 benchmarks, (a) Styr, (b) s1494, (c) Sand, (d) Planet, (e) s510, (f) s298, (g) s1488 and (h) s832

coordinate denotes the exponential security increasing with the constant base 10. It can be seen obviously that with the growth of added layers N, the improved security level of our scheme compared to the S and R scheme increases exponentially.

Overhead of the proposed scheme: Figure 7-9 show the area, power and delay overhead of the 8 modified benchmark files, respectively of our scheme and the S and R scheme. The horizontal coordinate stands for the number of added layers and the vertical coordinates represents the overhead results.

Figure 7 shows that the area overhead on the eight benchmarks increases with the added layers for both schemes and our scheme generally generates a little more. While the largest exceeding overhead of our scheme to the S and R scheme is no more than 42.8% and our scheme even generate a smaller overhead for the

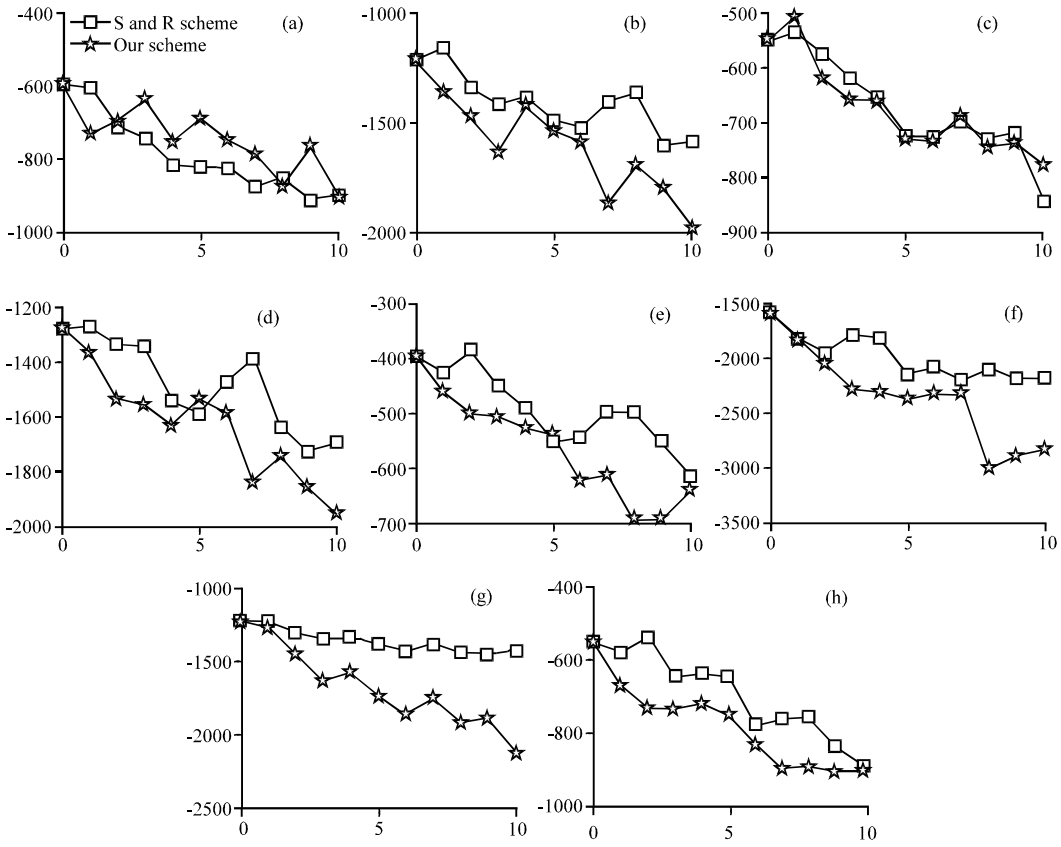

Fig. 9(a-h): Delay overhead by adding 1-10 layers using the two schemes on the 8 benchmarks, (a) Styr, (b) s1494, (c) Sand, (d) Planet, (e) s510, (f) s298, (g) s1488 and (h) s832

benchmark styr, the overhead of our proposed scheme is still acceptable.

Figure 8 shows the power overhead of the two schemes. As can be seen from the figure, the proposed HFSM scheme also generally generates little more power cost than that of the S and R scheme, but the maximum exceeding power of our scheme toward the S and R scheme is less than 49.2%, which is still an acceptable cost in power.

As illustrated in Fig. 9, the general trend of the delay overhead is fluctuating with the increase added layers for both schemes, but the overall tends to increase. For all the benchmarks, the proposed scheme also generally generates more timing but no more than 48.4% compared with the S and R scheme.

As can be seen from Fig. 7-9, the proposed HFSM scheme generates a little more area, power and delay overhead compared to the S and R scheme with the growth of added layers. But the maximum exceeding ratio is no more than 50% compared to the S and R scheme. Therefore, the overhead of the proposed scheme are still acceptable.

CONCLUSION

This study proposed an HFSM structure combined with PUFs for active metering scheme. The proposed structure utilizes the unique PUF outputs of each chip to decide the transitional paths and then uses the rest inputs bits along the paths to enhance the security against brute force attack. Experimental analysis and results demonstrate that the proposed structure achieves an exponentially better robustness than the existing scheme with an acceptably low cost in overhead of less than 50%.

ACKNOWLEDGMENTS

We would like to thank Prof. Yousra Alkabani for the help on the experiments. This study was supported by National Natural Science Foundation of China under Grant No. 61173038 and the Postgraduate Research and Innovation Project of Hunan Province of China under grant No.CX2012B142.

REFERENCES

AGMA, 2005. Managing the risks of counterfeiting in the information technology industry. A White Paper by KPMG and the Alliance for Gray Market and Counterfeit Abatement (AGMA). http://www.agmaglobal.org/press_events/press_docs/Counterfeit_WhitePaper_Final.pdf

Alkabani, Y.M. and F. Koushanfar, 2007. Active hardware metering for intellectual property protection and security. Proceedings of 16th USENIX Symposium on Security, August 6-10, 2007, Boston, USA., pp: 291-306.

Alkabani, Y., F. Koushanfar and M. Potkonjak, 2007. Remote activation of ICs for piracy prevention and digital right management. Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, November 4-8, 2007, San Jose, USA., pp: 674-677.

Busch, H., M. Sotakova, S. Katzenbeisser and R. Sion, 2010. The PUF promise. Proceedings of the 3rd Conference on Trust and Trustworthy Computing, June 21-23, 2010, Berlin, Germany, pp: 290-297.

Huang, J. and J. Lach, 2008. IC activation and user authentication for security-sensitive systems. Proceedings of the International Workshop on Hardware-Oriented Security and Trust, June 9, 2008, Anaheim, USA., pp: 76-80.

Koushanfar, F. and G. Qu, 2001. Hardware metering. Proceddings of the 38th Annual Conference on Design Automation, June 18-22, 2001, LasVagas, USA., pp: 490-493.

Koushanfar, F., G. Qu and M. Potkonjak, 2001. Intellectual property metering. Proceedings of the 4th International Workshop on Information Hiding, April 25-27, 2001, Pittsburgh, USA., pp: 81-95.

Majzoobi, M., F. Koushanfar and M. Potkonjak, 2008a. Lightweight secure PUFs. Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, November 10-13, 2008, San Jose, USA., pp: 670-673.

Majzoobi, M., F. Koushanfar and M. Potkonjak, 2008b. Testing techniques for hardware security. Proceedings of the International Conference on Test, October 28-30, 2008, Santa Clara, USA., pp: 1-10.

Yu, M.D. and S. Devadas, 2010. Secure and robust error correction for physical unclonable functions. IEEE Design Test Comput., 27: 48-65.

Zhang, J., Y. Lin, Q. Wu and W. Che, 2012a. Watermarking FPGA bitfile for intellectual property protection. Radioengineering, 21: 764-771.

Zhang, J., Y. Lin, W. Che, Q. Wu, Y. Lu and K. Zhao, 2012b. Efficient verification of IP watermarks in FPGA designs through lookup table content extracting. IEICE Electron. Express, 9: 1735-1741.