Chip-level Anti-reverse Engineering using Transformable Interconnects

Shuai Chen, Junlin Chen, Domenic Forte, Jia Di*, Mark Tehranipoor, and Lei Wang
Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269, USA
*Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, AR 72701, USA

***Abstract*—Cloning of integrated circuit (IC) chips have emerged as a significant threat to the semiconductor industry. Unauthorized extraction of design information from IC chips can be carried out in numerous ways. Invasive methods physically disassemble chip package and gain access to the different layers of a die through the low-cost delaying processing. This paper presents a new countermeasure exploiting transformable IC technologies. Transformable ICs are fabricated using materials that not only are electronically active but also change their electrical properties and physical compositions when experiencing invasive attacks. Simulation results demonstrate the proposed approach in improving the complexity of chip reverse engineering without introducing large performance overhead.**

I. Introduction

In recent years, reverse engineering of integrated circuit (IC) chips has become increasingly successful. Revealing the design details and physical implementations of IC chips not only creates opportunities for illegal reproduction, but also makes it easier for IP infringement, tampering, malicious alteration, and counterfeiting. Nowadays, not only various electronic systems such as mobile phones, internet modems/routers, and TV setup boxes are illegally copied and reproduced, many general purpose and custom-designed IC chips are also cloned precisely. Semiconductor Equipment and Materials International (SEMI) published a survey in 2010 about IP infringement. The survey revealed that 90% companies have experienced IP infringement, among 54% of them face serious infringement of their products [1].

Unauthorized extraction of design information from IC chips can be carried out in numerous ways [2]. Invasive methods physically disassemble chip package and gain access to the different layers of a die. Chip layout can be analyzed through the delayering process, which can be done layer by layer using wet/plasma etching, grinding, and polishing. Once a layer is exposed, post processing can extract the circuit schematic through the following steps: (1) image processing, (2) gate-level schematic extraction, (3) schematic analysis and organization, and (4) high-level netlist extraction. Automated instruments (scanning electron microscopes, digital microscopes) can take images of entire layers of ICs. Then, software tools can be used to stitch the images together and synchronize multiple layers including the alignments of contacts and vias. Transistors and other components such as interconnects and wells can be identified. Gate-level netlist can be extracted thereafter, from which a flattened schematic could be created. After the gate-level schematic is derived from the stripped IC, the high-level circuit description can be obtained for analysis and validation of the functionality of the chip.

A number of circuit/chip level countermeasures have been proposed, including obfuscation [3], [4], hardware metering [5]–[7], reconfigurable logic barrier [8], and IC locking [9], etc.. However, most of these techniques target different levels of abstraction other than invasive attacks for chip-level reverse engineering. Other efforts, such as top layer mesh and cell camouflage [10], [11], are effective to hinder the adversaries who want to extract the design of a chip using non-invasive methods such as X-ray imaging and micro-probing. Given the growing number of successful invasive attacks, new countermeasures augmented by process enhancements are needed to address this challenging problem.

In this paper, we propose a design technique exploiting *transformable interconnects* to improve chip-level anti-reverse engineering. The key idea of the proposed approach is to utilize two types of contacts/vias for interconnects: magnesium (Mg) contacts/vias for the real interconnects in the original design of the circuit, and magnesium oxide (MgO) contacts/vias for the dummy interconnects deliberately introduced for the purpose of obfuscation. All the interconnects are deposited with the same material (Al or Cu). When chip reverse engineering is performed, the delayering process causes Mg to quick oxidize into MgO, and thus the dummy interconnects cannot be distinguished from the real ones. Note that creating an oxygen-free environment during reverse engineering and developing steps to identify MgO/Mg contacts/vias will incur huge costs and complexity, which makes the proposed technique a favorable solution. A formal design framework is developed to maximize the complexity of reverse engineering and the penalty to the adversaries while minimizing the incurred performance overhead.

II. Construction of Transformable Interconnects

Transformable interconnects are fabricated using materials that not only are electronically active but also change their electrical properties and physical compositions when being exposed to reverse engineering attacks. In this paper, we will exploit magnesium (Mg) as the material for contacts and vias. Dummy interconnects are deliberately introduced, which are connected through non-conductive magnesium oxide (MgO)

978-1-4799-8606-4/15/$31.00

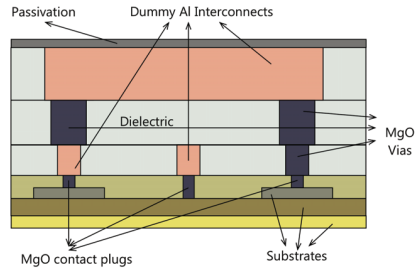


Fig. 1. Cross-section illustration of dummy interconnects.

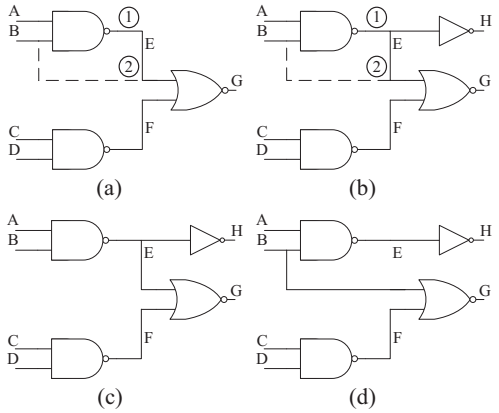


Fig. 2. The impact of fan-outs on chip reverse engineering: (a) with single-fan-out port E being selected, (b) with two-fan-out port E being selected, and (c)–(d) valid reversely engineered circuits after correcting schematic analysis errors.

contacts/vias to certain circuit nodes (see Fig. 1), thereby providing no real connections between these nodes and minimizing the impact on delay and power consumption. During the delayering process, magnesium will completely oxidize into magnesium oxide within a few minutes. Thus, all the real and dummy interconnects are connected by MgO contacts/vias, which obfuscates the original design of a chip. As shown in Section III, this approach greatly increases the complexity of reverse engineering, as it would be extremely difficult, if not impossible, for the adversaries to figure out the actual design. Furthermore, introducing transformable interconnects can also maximize the penalty to the adversaries when the circuit netlist is incorrectly generated (e.g., dummy interconnects are treated as real interconnects).

Mg displays very good electrical conductivity. The resistivity of Mg (44.7 nΩ·m) is lower than tungsten (56.1 nΩ·m)), which is used as the material for contacts/vias [12]. Several works have studied Mg alloys as the promising contact materials relevant to VLSI [13]. Recent work [17] also used Mg as the contact material in transient electronics. Furthermore, the semiconductor industry has a long history of using Mg in silicon-based IC chips. It was once used as the material to improve the adhesion of copper interconnects to the dielectric material at the passive interface. Dual-Damascene process [14] is now widely used in interconnect/contact metallization. If Mg is used for contacts/vias, the "trench first then via" process is suitable for this approach. Regarding electromigration, Mg is more resilient than Cu and Al to electromigration failures. On the other hand, MgO is a perfect insulator; the resistivity of MgO at the room temperature is more than 1014Ω·cm, which is similar to silicon dioxide [15].

One potential issue of transformable interconnects is that Mg has higher resistivity than Al (26.5 nΩ·m) and Cu (17.1 nΩ·m)). This is the reason that the proposed approach only uses Mg for contacts/vias but not changes the interconnect martial. Furthermore, a design optimization technique is proposed in Section III to reduce the performance overhead.

III. Design for Transformable Interconnects

In this section, we present the design technique that utilizes transformable interconnects for chip-level anti-reverse engineering. Intuitively, add more dummy interconnects will make reverse engineering more difficult to accomplish. However, dummy interconnections will consume metal tracks and occupy the limited area for the placement and routing on the chip. Some design metrics, such as timing, will be negatively affected due to the possible changes in circuit topology. Thus, it is important to develop a formal method that can effectively exploit transformable interconnects for maximizing the effectiveness of anti-reverse engineering without introducing large performance overheads.

To make the proposed technique generally applicable to integrate circuits with various functions, we will only consider the structural and behavioral information of a circuit. In other words, the proposed technique is not function-specific. Exploiting functional information for design optimization relevant to transformable interconnects will be a topic for our future work.

A. Structural information

The structural information, or circuit topology and especially the number of fan-outs of logic gates, plays an important role in determining which nodes the dummy interconnects can be inserted. For logic gates with only one fan-out, as the one shown in Fig. 2(a), the dummy interconnect ② links two single-fan-out ports B and E, where B is the output of the previous logic gate. In this case, after delayering the actual interconnect ① and the dummy interconnect ② are indistinguishable because all are connected to MgO contacts/vias. If both are treated as valid interconnects, errors will be generated during the schematic analysis, because multiple signals are driving the same input port. It is relatively easy for the adversaries to detect such errors. The adversaries with moderate circuit design expertise can figure out that ② is an invalid interconnect; otherwise ① will not drive any logic gate and will be useless. As a result, adding dummy interconnects to single-fan-out logic gates can be detected and corrected easily, compromising the anti-reverse engineering effort.

On the other hand, it will be much more difficult to find

out the valid interconnects when dummy interconnects are connected to logic gates with multiple fan-outs, such as node E in Fig. 2(b), which is connected by the dummy interconnect ②. Note that schematic analysis will still report an error as both ① and ② are driving the same input port. However, different from Fig. 2(a), two possible logic connections can be resulted after correcting the schematic analysis error in Fig. 2(b). Both logic connections, as shown in Figs. 2 (c) and (d), are valid if without *a priori* knowledge of the original circuit design, while only one of them is correct. Assume that overall we can insert N dummy interconnects, all linked two-fan-out logic gates, then there are 2^N possible circuit topologies that satisfy the schematic analysis, while only one of them is the correct interconnect structure. Therefore, the difficulty of reverse engineering increases exponentially as the number of dummy interconnects being introduced. It is prohibitively expensive for the adversaries to figure out the correct design of the circuit.

Similarly, when logic gates with more than two fan-outs are connected by the dummy interconnects, the complexity of reverse engineering will be further increased. This scenario is illustrated in Fig. 3(a) for a gate with three fan-outs at node E. After the gate-level schematic extraction, three circuit topologies, as shown in Figs. 3(b)–(c), are all valid. In general, adding dummy interconnects to multi-fan-out gates will lead to higher reverse engineering complexity. Specifically, when the dummy interconnect connects a gate with fan-outs of m ($m \geq 2$), there are m possible circuit topologies satisfying the schematic analysis. If N mummy interconnects are inserted with each linked ports with fan-out of m_i, the number of total valid circuit topologies $\mathcal{N}_m$ can be expressed as,

$$\mathcal{N}_m = \prod_{i=1}^{N} m_i, \qquad m_i \geq 2. \tag{1}$$

As a result, to make chip reverse engineering more difficult, the first step of the proposed technique is to identify gates in the circuit netlist with multiple fan-outs. These gates are the candidate locations where dummy interconnects could be inserted.

B. Behavioral information

In many circuits, only considering the structural information will not deliver an optimal solution of dummy interconnect insertion. This is due to the fact that the circuit netlist usually contains a large number of nodes with multiple fan-outs. Adding dummy interconnects to all these nodes may cause a large performance overhead. Thus, a subset of these nodes has to be selected. Since these nodes may have diverse circuit behaviors, different selections will result in different levels of security enhancement. To achieve the optimal design tradeoff, it is necessary to consider the behavioral information of the circuit. In this paper, two types of behavioral information, switching activity and correlation factor, will be utilized to guide node selection for transformable interconnects.

Switching activity is an important behavioral information commonly used in circuit designs; for example, many CAD

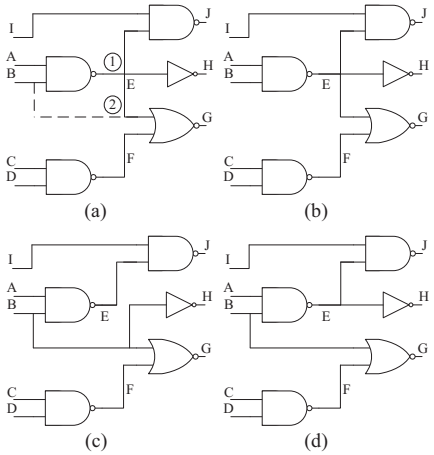
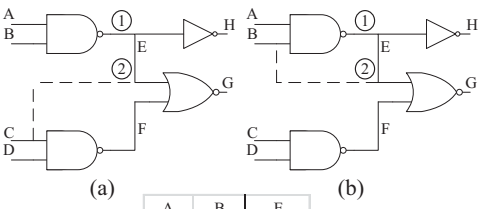


Fig. 3. The impact of multiple fan-outs impact on chip reverse engineering: (a) with three-fan-out port E being selected, and (b)–(d) valid reversely engineered circuits after correcting schematic analysis errors.



A	B	E
0	0	1
0	1	1
1	0	1
1	1	0

(c)

Fig. 4. Selection of dummy interconnects based on correlation coefficients: (a) dummy interconnect between C and E, (b) dummy interconnect between B and E, and (c) the truth table of the NAND gate.

tools estimate the dynamic power consumption based on switching activities. If a node in the netlist has a high switch activity, the workload of this node is high and thus we can reasonably regard it as an important contributor to the overall circuit behavior (though not necessarily to the functionality, which is beyond the scope of this paper). In general, circuit nodes with higher switching activities can propagate signals as well as faults (which may be caused by the incorrect netlist generated by the adversaries) faster than those with low switching activities. Due to these considerations, we will select nodes with multiple fan-outs as well as high switching activities to insert dummy interconnects.

Dummy interconnect will make a false connection between two circuit nodes. The behaviors of these two nodes should be as different as possible in order to increase the effectiveness of anti-reverse engineering. Consider the case where two nodes connected by a dummy interconnect have identical behaviors. For example, these two nodes belong to two sets of address decoders that are connected to the same address bus. They have the same input and perform the same decoding function. If the dummy interconnect is treated as the actual interconnect by

the adversaries, the resulted circuit will still perform correctly as the connection between the two nodes is redundant and won't change the logic function of the circuit. Therefore, we should try to avoid adding dummy interconnects to circuit nodes that are closely correlated. Consider the example in Fig. 4, where a dummy interconnect can be added from node E to either node C or node B. To improve the effectiveness of anti-reverse engineering, we need to choose between C and B. The right choice should be the node having a less probability to be equal to E. For the purpose of illustration, assume that the inputs at nodes A, B, C, and D are independent and uniformly distributed random variables, i.e., $P(A=1)=P(B=1)=P(C=1)=P(D=1)=0.5$. Based on the truth table in Fig. 4(c), we obtain

$$\begin{aligned} P(E=B) =& P(A=0;B=1)=0.25; \\ P(E=C) =& P(A=0;B=0;C=1)+ \\ & P(A=0;B=1;C=1)+ \\ & P(A=1;B=0;C=1)+ \\ & P(A=1;B=1;C=0)=0.5. \end{aligned} \tag{2}$$

From (2), node B should be selected because $P(E=B)$ is much smaller than $P(E=C)$. This guarantees that, if the dummy interconnect is treated as the real interconnect, the resulted circuit will generate more errors statistically.

A formal method to characterize the relationship between a pair of circuit nodes can be derived by using the correlation coefficient, which is a statistical measure defined as [16],

$$\begin{aligned} \gamma_{XY} =& \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X \sigma_Y} \\ =& \frac{\sum_{i=1}^{n}(x_i-\mu_X)(y_i-\mu_Y)}{\sqrt{\sum_{i=1}^{n}(x_i-\mu_X)^2}\sqrt{\sum_{i=1}^{n}(y_i-\mu_Y)^2}}, \end{aligned} \tag{3}$$

where X and Y represent the bitstreams $\{x_i\}$ and $\{y_i\}$, respectively, at two circuit nodes, n is the total number of bits, and μ_X and μ_Y are the average values of these two bitstreams. Note that γ_{XY} can be calculated from the gate-level simulation.

According to (3), the value of γ_{XY} ranges from 1 to -1. When γ_{XY} is close to 1, the two circuit nodes with X and Y as the outputs become strongly correlated. For example, $\gamma_{XY}=1$ indicates that the two circuit nodes have the identical behaviors, such as the input and output of a buffer. Adding dummy interconnects won't help for this case because they won't affect the logic correctness in the reversely engineered chip. On the other hand, $\gamma_{XY}=-1$ means the two circuit nodes are "inversely" identical, i.e., one node is an inverted version of the other node, such as the input and output of an inverter. Adding dummy interconnects between these nodes will completely disable the circuit if these interconnects are treated as true connections in the reversely engineered chip. Ideally, when we choose circuit nodes to introduce dummy interconnects, the correlation coefficients of these nodes should be as negative as possible to maximize the probability of malfunctioning in the reversely engineered chip.

Algorithm 1 Design for Transformable Interconnects

Input:
A fault-free circuit with n nodes (W_i is the ith node in the circuit)($n-1 \geq i > 0$))
Switching activities α_i of W_i ($n-1 \geq i > 0$)
Delay of thel circuit(T)
Output:
P(Transformable interconnect options)

Step 1 - Options for Transformable Interconnects

```
for i ← 0 to n − 1 do
    for j ← 0 to n − 2 − i do
        if α_j < α_{j+1} then
            Swap (α_j, α_{j+1})
            Swap (W_j, W_{j+1})
        end if
    end for
end for
for i ← 0 to [n/10] do
    Add W_j to { F_i } as f_j ← W_j
    Measure the fan-out of elements in { F_i}
    if fan-out of node f_i<2 then
        Delete f_i from { F_i}
    end if
end for
```

Step 2 - Performance Checking for Single Transformable Interconnect

```
% γ_ij(Correlation coefficient between f_i and f_j) is measured.
% Transformable interconnects G_r is built between f_i and f_j.
for i ← 0 to m do
    for j ← 0 to m − 1 − i do
        if γ_j > γ_{j+1} then
            Swap (γ_j, γ_{j+1})
            Swap (G_j, G_{j+1})
        end if
    end for
end for
for i ← 0 to m do
    Measure the delay(t) of the circuit
    if γ_j<0 and t = T then
        Add element G = {[(f_i, f_j), γ_ij]} to { G_i}
    end if
end for
```

Step 3 - Iterative Timing Optimization

```
for r ← 0 to s do
    {D_m}_i ← combntns({G_i}, s)
    for m ← 0 to s do
        Add {G_i}-D_m transformable interconnects into circuit
        Measure the delay(t) of the circuit
        if t≤T then
            P←{G_i}-D_m
            Break;
        else
            Delete {G_i}-D_m transformable interconnects
        end if
    end for
end for
```

Now let us revisit the circuit example in Fig. 4. It can be calculated that $\gamma_{BE}=-0.577$ and $\gamma_{CE}=0$, indicating that the dummy interconnect between B and E is a better choice, which is consistent with the analysis in (2).

C. The proposed transformable interconnect design technique

As discussed above, the design space exploration related to the proposed technique involves selecting circuit nodes with appropriate fan-outs, switching activities, and correlation coefficients. The objective is to increase the number of inserted dummy interconnects so as to maximize the complexity of reverse-engineering (see (1)), while at the same time reduce the design overhead. In terms of the design overhead, we are primarily concerned with the impact on circuit delays due

to the circuit topology change after the insertion of dummy interconnects. Since dummy interconnects are not conductive (as they are connected by MgO contacts/vias), the power overhead is not a primary concern.

The proposed transformable interconnect design technique is summarized in Algorithm 1. In Step 1, the netlist of a circuit is taken as the input, and the numbers of fan-outs are determined for all the circuit nodes. Then, the switching activities of the nodes with multiple fan-outs are estimated through gate-level simulations. A threshold of switching activities can be provided by the designer. For example, if 10% is set as the threshold, nodes having the top 10% switching activity values are collected into the set F. Thus, after Step 1, the set $F = \{f_1, f_2 \cdots, f_N\}$ will only contain circuit nodes $f_1, f_2 \cdots, f_N$ with multiple fan-outs and high switching activities.

In Step 2, the correlation coefficients for all node pairs in the set F are calculated. For the set F containing N nodes, the total number of node pair combinations is $N(N-1)/2$. Then, these node pairs are ranked by their correlation coefficients, and the one with the most negative value is on the top of the list. Starting from the top of the list, each time a dummy interconnect is added between one node pair, the critical path delay of the resulted circuit is checked by full path timing report (e.g., using Synopsys Design Compiler). If the added dummy interconnect won't increase the circuit delay beyond a pre-specific acceptable value, the corresponding node pair is put into a set $G = \{[(f_i, f_j), \gamma_{ij}]\}, 1 \leq i, j \leq N$, where γ_{ij} is the correlation coefficient of the note pair (f_i, f_j). After Step 2, the set G will contain all node pairs that, when adding the dummy interconnect *individually* between them, the resulted circuits have acceptable performance overhead.

In Step 3, dummy interconnects are added to all the node pairs in the set G. It is very likely that the performance overhead of the resulted circuit will be large due to the change in the circuit topology. An iterative optimization procedure will be applied to ensure the acceptable performance while maximizing the number of added dummy interconnects. The optimization procedure first removes one dummy interconnect at a time, starting from the node pair with the least negative correlation coefficient, and then checks the timing of the resulted circuit. If timing is not satisfied by removing one dummy interconnect at a time, two dummy interconnects starting with the least negative correlation coefficients will removed together and the timing is checked again. This procedure continues until at a point that, by removing a set of dummy interconnects, the timing of the resulted circuit meets the requirement. The remaining elements in the set G are the final result, which provides the largest number of dummy interconnects (i.e., the maximum complexity in reverse engineering) with an acceptable performance overhead.

IV. Evaluations

In this section, we apply the proposed technique for the design of transformable interconnects in a number of benchmark circuits. A suite of simulations will be conducted to evaluate the enhancement in anti-reverse engineering as well as the incurred performance overhead. For benchmark circuits, we choose ITC99, which are sequential circuits with various complexities with some industrial design subsets.

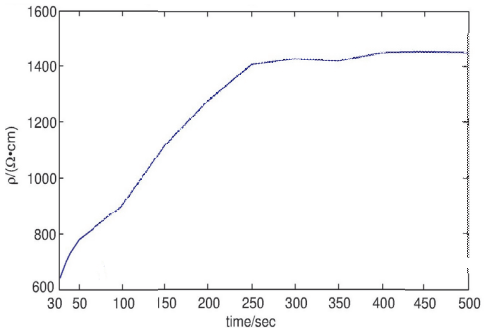


Fig. 5. Measured Mg oxidization process.

We are mainly interested in the timing overhead, i.e., the increase in critical path delays due to the circuit topology change caused by the added dummy interconnects. Note that dummy interconnects with MgO contacts/vias are not conductive (e.g., no additional parasitic capacitance) and thus won't affect the timing directly. All the results were obtained from gate-level simulations, where the switching activities were measured by Synopsys VCS, correlation coefficients were calculated using our numerical simulation tool based on gate-level simulation results, and timing estimation was performed by Synopsys Design Compiler.

We have fabricated some Mg samples and measured the oxidization process. As shown in Fig. 5, the resistivity of Mg increases quickly after being exposed to air. In less than three minutes, the resistivity becomes more than 1000 Ωcm, in the same range of silicon dioxide, indicating that Mg has been completely oxidized into non-conductive MgO. This experiment validate the feasibility of the proposed transformable interconnect approach.

Table I shows the results obtained from the benchmark ITC99, where different values of acceptable timing overhead are presented for illustration. In this table, N is the number of inserted dummy interconnects by using the proposed technique; α_{min} refers to the minimal value of switching activities among the nodes chosen for dummy interconnects; γ_{max} indicates least negative value of correlation coefficients among the selected node pairs. We also provide the complexity of reverse engineering, quantified by $\mathcal{N}_m$ as in (1), i.e., the number of valid circuit topologies due to the insertion of dummy interconnections. A larger value of $\mathcal{N}_m$ means that it is more difficult for the adversaries to reasoning about the original circuit design.

As shown in Table I, when the circuit becomes more complex, it is more likely to introduce transformable interconnects and the complexity of reverse engineering will be increased. For example, there are 5678 gates in the benchmark

TABLE I
TRANFORMABLE INTERCONNECT INSERTION WITH 0, 3% AND 5% TIMING OVERHEADS

ITC99	gates	0% timing overhead				3% timing overhead				5% timing overhead			
		N	$\mathcal{N}_m$	$\alpha\ _{min}$	γ_{max}	N	$\mathcal{N}_m$	$\alpha\ _{min}$	γ_{max}	N	$\mathcal{N}_m$	$\alpha\ _{min}$	γ_{max}
b05	574	7	128	0.218	-0.20	9	512	0.202	-0.20	13	8.20e03	0.183	-0.13
b12	1006	12	3.36e07	0.243	-0.32	22	8.80e12	0.203	-0.32	25	3.36e07	0.136	-0.32
b14	5678	30	1.07e09	0.251	-0.24	36	6.87e10	0.201	-0.10	55	3.60e16	0.201	-0.07
b14_1	6900	33	8.59e09	0.197	-0.23	78	3.02e23	0.197	-0.18	104	2.03e31	0.113	-0.18
b15	7577	38	2.75e11	0.184	-0.27	44	1.76e13	0.166	-0.27	84	1.93e25	0.134	-0.07
b20	12501	48	2.81e14	0.172	-0.22	85	3.87e25	0.172	-0.16	166	9.35e49	0.111	-0.01
b21	12678	54	1.80e16	0.136	-0.15	76	7.56e22	0.150	-0.15	168	3.74e50	0.101	-0.15
b22	18086	76	7.56e22	0.227	-0.43	113	1.04e34	0.207	-0.09	191	3.14e57	0.178	-0.09
b17	24305	92	4.96e27	0.166	-0.28	198	4.02e59	0.132	-0.28	272	7.59e81	0.105	-0.11
b17_1	24571	96	7.92e28	0.149	-0.12	192	6.28e57	0.130	-0.12	294	3.18e88	0.130	-0.02
b18	73243	265	5.93e79	0.215	-0.30	334	3.50e100	0.179	-0.24	518	8.584e155	0.148	-0.01
b18_1	71611	225	5.39e67	0.185	-0.18	303	1.63e91	0.148	-0.18	482	1.25e145	0.112	-0.04
b19	231320	438	7.10e131	0.203	-0.09	583	3.17e175	0.160	-0.09	893	6.60e268	0.129	-0.09

b14, and 30 dummy interconnects can be added without incurring any timing overhead; whereas for benchmark b17 with 24305 gates, adding 92 dummy interconnects causes no timing overhead. For both cases, the circuit structures are changed, but the changes are small as only a few dummy interconnects are added. Thus, the critical path delays are not affected. These results indicate that the proposed technique is more effective when applied to complex circuits.

By relaxing the constraint on timing overhead, more dummy interconnects can be included, thereby further increasing the complexity of reverse engineering. For example, by increasing the timing overhead to 3% and 5%, benchmark b17 (24305 gates) can accept 189 and 272 dummy interconnects, respectively, and the corresponding complexity in reverse engineering increases to $\mathcal{N}_m = 4.02 \times 10^{59}$ and $\mathcal{N}_m = 7.57 \times 10^{81}$, respectively. This is because some relatively less important circuit nodes are also protected, as indicated by the reduction in both α_{min} and $|\gamma_{max}|$.

Note that while other performance metrics are not reported in this paper, we expect they will have a similar trend as the timing results presented in Table I. For example, power consumption will not see significant changes because dummy interconnects are not conductive and thus won't affect the power consumption directly. Also, more accurate results could be obtained through layout-based simulations but this is very time-consuming and usually unnecessary, as it won't change the essence of the proposed technique.

V. CONCLUSION

This paper presents a new technique and the related optimization method for the design of transformable interconnects to achieve better security against chip reverse engineering. We have demonstrated the structure of transformable interconnects and the feasibility of the insertion of dummy interconnects. The effectiveness of the proposed approach was evaluated through a number of benchmark circuits. Design tradeoffs are measured in terms of timing and complexity of reverse engineering. Future work is being directed towards the evaluation of other performance metrics and experimental demonstration of the proposed technique in various IC chips.

REFERENCES

[1] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers," *IEEE Design and Test of Computers*, pp. 66-75, 2010.

[2] S. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM Journal on Emerging Technologies in Computing Systems*, accepted.

[3] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, pp. 709-720, 2013.

[4] R. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation." *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, 2008.

[5] Y. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security." *USENIX Security*. 2007.

[6] S. Wei, A. Nahapetian, and M. Potkonjak, "Robust passive hardware metering." *Proceedings of the International Conference on Computer-Aided Design*. IEEE Press, 2011.

[7] F. Koushanfar, "Integrated circuits metering for piracy protection and digital rights management: an overview." *Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI*. ACM, 2011.

[8] H. Liu and D. D. Coon, "Heterojunction double barrier diodes for logic applications." *Applied physics letters* 50.18 (1987): 1246-1248.

[9] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers." *IEEE Design and Test of Computers* 27.1 (2010): 66-75.

[10] K. Daum, "Structures for preventing reverse engineering of integrated circuits." U.S. Patent No. 5,468,990. 21 Nov. 1995.

[11] R. Cocchi, P. Baukus, and James P. "Circuit camouflage integration for hardware IP protection." *Design Automation Conference (DAC)*, 2014 51st ACM/EDAC/IEEE. IEEE, 2014.

[12] H. Nicholls, M. J. Norrington, and M. K. Thompson, "Method of fabricating a tungsten contact." U.S. Patent No. 5,422,308. 6 Jun. 1995.

[13] Kaneko, Noriyoshi, Fumihiro Honda, and Koichi Nakajima. "Availability of Al-Mg alloys for use as electrical contact resistors." *Components, Packaging, and Manufacturing Technology, Part A, IEEE Transactions on 19.1* (1996): 98-104.

[14] R. J. Huang, A. Hui, R. Cheung, M. Chang, and M. Lin. "Simplified dual damascene process for multi-level metallization and interconnection structure." U.S. Patent No. 5,635,423. 3 Jun. 1997.

[15] K. Chahara, T. Ohno, M. Kasai, and Y. Kozono. "Magnetoresistance in magnetic manganese oxide with intrinsic antiferromagnetic spin structure." *Applied Physics Letters* 63.14 (1993): 1990-1992.

[16] J. Lee Rodgers and W. Alan Nicewander, "Thirteen ways to look at the correlation coefficient." *The American Statistician* 42.1 (1988): 59-66.

[17] Hwang S-W, Tao H, Kim D-H, et al. A Physically Transient Form of Silicon Electronics, With Integrated Sensors, Actuators and Power Supply. *Science (New York, NY).* 2012;337(6102):1640-1644. doi:10.1126/science.1226325.