Table 1. Possible alternate camouflaged logic functions for selected one and two-input logic gates in an example foundry logic cell library

Physical Appearance	Possible Alternate Camo Functions
XOR2	11 (XNOR2, AND2, NAND2, NOR2, OR2, INV A, INV B, BUF A, BUF B, VDD, VSS)
XNOR2	11 (XOR2, AND2, NAND2, NOR2, OR2, INV A, INV B, BUF A, BUF B, VDD, VSS)
AND2	9 (OR2, NAND2, NOR2, INV A, INV B, BUF A, BUF B, VDD, VSS)
OR2	9 (AND2, NAND2, NOR2, INV A, INV B, BUF A, BUF B, VDD, VSS)
NAND2	7 (NOR2, INV A, INV B, BUF A, BUF B, VDD, VSS)
NOR2	7 (NAND2, INV A, INV B, BUF A, BUF B, VDD, VSS)
BUF	3 (INV, VDD, VSS)
INV	2 (VDD, VSS)

When faced with the possibility that the device under analysis contains camouflaged logic cells, an attacker must consider alternate functions for each gate in the design. Figure 6 below shows the example circuit from Figure 5, with logic gates replaced by boxes representing the number of possible functions for consideration. The number of possible functions for a given logic gate is the number of possible alternate functions from Table 1 plus 1, the apparent function of the gate.

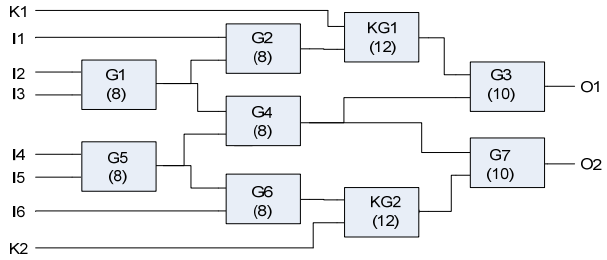

Figure 6. Possible logic functions to consider when resolving functional differences between the extracted netlist (Figure 5) and the fabricated device.

To arrive at the total number of possible configurations for the 9-gate netlist in Figure 6, one would multiply together the number of possible functions for each gate. In this example the number of configuraitons would be $5.9*10^7$ (8*8*8*8*12*12*10*10). This far exceeds the total number of possible input patterns, even considering the key inputs (6 input bits plus 2 key bits allows for 2^8, or 64 possible input combinations). It would be easier for the attacker to analyze the device as a black box with brute force.

Power, Area, and Delay Overheads: Overhead for power and area are highly design dependent. For an implementation using camouflaged foundry logic cells, camouflaged cells have similar power, area, and delay characteristics to the reference foundry library. Non-switching circuitry, such as a gate with a static output, is an area and static power overhead. Partially non-switching circuitry, such as an inverter that is designed to look like a NAND gate, is also an area and static power overhead because one is using a larger footprint than necessary to perform a given logic function. However, camouflaged gates whose actual function is of the same complexity as its apparent function do not incur an area overhead. Highly effective levels of circuit camouflage can be attained with 1-5% extraneous circuitry. Camouflaged cell timing is highly layout-dependent. Some camouflaged cells will have similar timing characteristics to their foundry counterparts, and some may be slower. If critical paths are avoided when placing camouflaged cells, there is effectively no timing penalty.

For a fully camouflaged circuit, one is comparing camouflaged versus non-camouflaged standard cell libraries at a given technology node. Since camouflaged cell design techniques don't inherently impose power, area, or timing penalties, it's not possible to generalize these overheads. However, when comparing a fully camouflaged circuit against an implementation using camouflaged foundry logic cells, the fully camouflaged circuit needs no extraneous circuitry because every logic gate is already camouflaged.

Conclusions

Use of camouflaged gates in a design containing logic encryption is an effective means to harden the circuit against circuit analyses that would lead to extraction of logic encryption key data, as well as providing an independent layer of security against reverse engineering.

References

1. Roy, J.A., Koushanfar, F., and Markov, I.L., "Ending Piracy of Integrated Circuits", *Design, Automation, and Test in Europe*, 2008.
2. Subramanyan, P., Ray, S., and Malik, S., "Evaluating the Security of Logic Encryption Algorithms", *Hardware Oriented Security and Trust,* 2015.
3. Rajendran J., Pino, Y., Sinanoglu, O., Karri, R., "Security Analysis of Logic Obfuscation", *Proceedings of the 49th Annual Design Automation Conference*, 2012.
4. "Circuit Camouflage Technology, SMI IP Protection and Anti-Tamper Technologies", www.smi.tv/ SMI_SypherMedia_Library_Intro.pdf.
5. Cocchi, R., Baukus, P., Chow, L.W., Wang, B., "Circuit Camouflage for Hardware IP Protection", *Proceedings of the 51st Annual Design Automation Conference*, 2014.