Differential Power Analysis Resistant Logic Style
Tech ID: 20209 / UC Case 2004-155-0

SUMMARY

UCLA researchers in the Department of Electrical Engineering have developed and reduced-to-practice a logic style which provides resistance against differential power analysis (DPA) attacks to the encryption chip.

BACKGROUND

Security chips leak information through power consumption, timing, and electro-magnetic radiation although they are secure against mathematical attacks. One of the most effective side channel attacks to the encryption ICs is the differential power analysis attack. In DPA, the attacker measures the power consumption of the chip while it encrypts and by doing a statistical analysis he can extract the secret-key. This is due to the asymmetry of the power consumption in the standard CMOS logic gates since they have power characteristic that is dependent on the input signals. Different techniques have been proposed to prevent this information leakage: interleaved dummy instructions, random power consumption, duplicate logic, etc.; however, all of these methods have been circumvented.

INNOVATION

A novel logic style is developed in which every logic gate consumes constant power independent of the input signal. It is called Wave Dynamic Differential Logic (WDDL) and is DPA resistant. Moreover, a routing scheme is developed that provides constant load capacitance for true and false outputs of the WDDL gates which results in constant power cost. Using these innovations, a design methodology that is suitable for integration in a common automated standard cell ASIC or FPGA design flow is developed.

APPLICATIONS

▶ Smart cards
▶ Any security application that is relying on standard CMOS technology or FPGA design flow.

ADVANTAGES

1. The modification is a technically feasible and systematic modification to what is currently available; and,
2. The approach is flexible to accommodate any silencing gene candidates.

STATE OF DEVELOPMENT

The complete design flow is developed that integrates usage of the WDDL gates and differential routing in the standard CMOS technology and FPGA design flow. About 128 WDDL library cells are designed. This design methodology is used to fabricate an embedded biometric authentication system (ThumbPod) using the 0.18μm CMOS technology. The chip is tested against the DPA attack and it proved to provide resistance against differential power analysis side-channel attack. This case is also related to, [LA 2003-442 ABOUT THE LAB

PATENT STATUS

<table>
<thead>
<tr>
<th>Country</th>
<th>Type</th>
<th>Number</th>
<th>Dated</th>
<th>Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States Of America</td>
<td>Issued Patent</td>
<td>8,324,937</td>
<td>12/04/2012</td>
<td>2004-155</td>
</tr>
</tbody>
</table>

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

▶ Constant Power Design Encryption Technology