HDRL: Homogeneous Dual-Rail Logic For DPA Attack Resistive Secure Circuit Design

Tech ID: 21209 / UC Case 2011-151-0

BRIEF DESCRIPTION

HDRL (Homogeneous Dual-Rail Logic) is a standard cell level DPA (Differential Power Analysis) attack countermeasure that theoretically guarantees fully-balanced power consumption and has been shown to significantly improve the DPA attack resistivity of hardware with low energy overhead and no delay overhead over conventional countermeasures.

FULL DESCRIPTION

Differential Power Analysis (DPA) side-channel attacks pose serious threats for embedded system security. Wave Dynamic Differential Logic (WDDL) was proposed as a countermeasure that can be incorporated into a conventional ASIC design flow using standard cells. However, simulations show that DPA attacks on WDDL still leak secret keys to adversaries. To respond to this critical industry need, UCI researchers have created Homogeneous Dual-Rail Logic (HDRL), a standard cell level DPA attack countermeasure that theoretically guarantees fully balanced power consumption and significantly improves the DPA attack resistivity of hardware. Experimental results on the AES S-Box circuit show that HDRL successfully prevent DPA attacks in all cases. In addition, HDRL achieves such higher security with only 100.0% energy overhead while WDDL incurs 231.7% energy overhead. Also, HDRL requires the same area overhead as WDDL. HDRL's better resistivity and lower energy overhead make it a promising countermeasure for standard cell based crypto-applications.

SUGGESTED USES

HDRL is applicable to any standard cell-based crypto-LSI that deals with personal information. Possible applications include smart cards, mobile devices, SIM cards, and health monitoring devices. When one designs LSIs for such applications, the designer is able to achieve high DPA (Differential Power Analysis) attack resistivity using HDRL.

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	9,240,786	01/19/2016	2011-151
United States Of America	Issued Patent	8,395,408	03/12/2013	2011-151

CONTACT

Ben Chu
ben.chu@uci.edu
tel: .

INVENTORS

- Dutt, Nikil D.
- Tanimura, Kazuyuki

OTHER INFORMATION

CATEGORIZED AS

- **Computer**
  - Security
- **Security and Defense**
  - Cyber security

RELATED CASES

2011-151-0

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- DNN-Assisted Sensor for ECG Monitoring

UCI Beall
Applied Innovation

5270 California Avenue / Irvine,CA
92697-7700 / Tel: 949.824.2683

© 2010 - 2016, The Regents of the University of California
Terms of use
Privacy Notice