1.32GHz High-Throughput Charge-Recovery AES Core with Resistance to DPA Attacks

Shengshuo Lu, Zhengya Zhang, Marios Papaefthymiou
University of Michigan, Ann Arbor, MI, USA

Abstract

A 128-bit Advanced Encryption Standard (AES) core targeted for high-performance security applications is fabricated in a 65nm CMOS technology. A novel charge-recovery logic family, called Bridge Boost Logic (BBL), is introduced in this design to achieve switching-independent energy dissipation for an intrinsic high resistance against Differential Power Analysis (DPA) attacks. Based on measurements, the AES core achieves a throughput of 16.90Gbps and power consumption of 98mW, exhibiting 720x higher DPA resistance and 30% lower power than its conventional CMOS counterpart at the same clock frequency.

Introduction

AES is a popular encryption method that is often implemented in dedicated hardware to achieve high performance and energy efficiency [1-2]. AES chips are vulnerable to side-channel attacks that exploit side-channel information such as power profiling to reveal the secret key used by the chip. Differential Power Analysis (DPA) is one of the most effective side-channel attacks [3]. DPA attacks on conventional CMOS chips exploit the switching-dependent power profile of the chip, which can be easily obtained in an unobtrusive manner by monitoring power supply currents. A statistical analysis is then performed to correlate switching behavior with the data used in the computation, to reveal the cryptographic key [4-6].

Previous AES prototype chips with DPA resistance have been demonstrated at clock rates up to 255MHz. One approach against DPA is to add countermeasure circuits around an unprotected CMOS core to inject noise or erase the information content on the power trace [4,6]. Another effective approach uses gates designed with nearly constant power consumption to diminish the impact of switching activity on the power trace, but these designs incur high performance and power penalties [5].

This paper presents a 128-bit AES core running at 1.32GHz with intrinsic DPA resistance. A new charge-recovery logic, called Bridge Boost Logic (BBL), is proposed for the design of this AES core to ensure a switching-independent power profile that is intrinsically immune to DPA attacks and provides power savings at a GHz speed.

The measured results show that this AES core is the fastest among published DPA-resistant chips [4-6]. Unlike previous approaches toward DPA resistance that incur power overhead or speed degradation [4-6], this DPA-resistant AES core reduces power consumption over its conventional static CMOS counterpart and maintains a high throughput. Running at 16.90Gbps with 98mW, this core is 720x more DPA resistant, and consumes 30% lower power than its static CMOS counterpart operating at the same clock speed.

Bridge Boost Logic

BBL is a dual-rail charge-recovery logic that achieves low energy dissipation by recovering charge from gate fanouts. BBL is a dynamic logic family and enables deep pipelining for high frequency operation. Unlike other charge-recovery topologies, such as [7], BBL gates adopt higher supply voltage than Vth to attain high operating speeds.

As shown in Fig. 1, a BBL gate consists of an evaluation stage and a boost stage. Two sinusoidal power clocks PC and PC_b with 180 degree phase difference are supplied to the logic gate. First, during evaluation phase, while PC is low and PC_b is high, the evaluation stage initiates a voltage difference between two complementary outputs logically based on the inputs. Second, as PC rises, the cross-coupled inverters lock the voltage difference and boost it up to the same level as PC. Since output voltage reaches nominal voltage at the same time as PC, the next gate is driven without degradation to ensure GHz-level operation. As PC falls, the charge from the gate and its fanouts is recycled back to the PC instead of being dumped to ground to improve energy efficiency. After PC falls below Vth, a new evaluation phase begins.

To enhance DPA resistance, a key innovation in BBL is the introduction of a bridge transistor that equalizes currents in the evaluation stage to remove switching-dependent signatures from the power profile. Tied to PC_b, the bridge transistor turns on when the input signal reaches the nominal voltage, shorting the pull-up and pull-down networks on the opposite sides of the evaluation stage to conduct the same current regardless of the previous state. At the end of evaluation, the bridge transistor ensures that the voltage difference of the complementary outputs is independent of switching direction, enabling PC to always boost from about the same voltage level, and thus yielding a switching-independent power profile.

As shown in Fig. 2, the sinusoidal PC is generated from two on-chip inductors resonating with the capacitance of the gates and the clock distribution mesh parasitic capacitance. 72 distributed cross-coupled NMOS transistor pairs are used as negative transconductance to maintain resonating amplitude.

Experimental Evaluation

For comparison, along with the BBL-based DPA-resistant AES core, a conventional CMOS AES core is fabricated using a 65nm static CMOS standard cell library. The CMOS core has the same architecture and target frequency as the BBL-based core.

Fig. 3 shows the measured transient power supply current of the two AES cores. The CMOS current in Fig. 3(a) shows considerable variations due to the switching activity, while the BBL current in Fig. 3(b) shows no appreciable variation to reveal any switching activity.

The results of DPA attacks launched on the MixColumn block of the two cores are shown in Fig. 4. As indicated in Fig. 4(a) and 4(b), the key in the CMOS core is easily disclosed, as within a small number of measurements, the correlation for the correct key is significantly higher than for incorrect keys. As the number of measurements increases, the correct key correlation rises further. Measurements to Disclosure (MTD) of a byte in the key is the number of measurements required for the correlation of the correct key value for that byte to exceed that of any other value [5]. Fig. 4(c) and 4(d) show the difficulty in disclosing the key in BBL core, since the MTD is several hundred thousands, and the peak correlation of the correct key is only marginally higher than the incorrect keys.

Measurements from the two cores are shown in Fig. 5. Both cores attain a maximum clock frequency of 1.32GHz, yielding a throughput of 16.90Gbps. Dissipating 98mW, the BBL core consumes 30% less power than its CMOS counterpart. The logic area of the BBL core is about twice as large as the CMOS core. The inductor overhead is 25% of its logic area. By comparing the MTD of the 1st block, which is defined as the minimum MTD of all 16 key bytes [4], the BBL core offers 720x higher DPA resistance than the CMOS core.

Fig. 6 shows the normalized power dissipation and performance of the BBL core and other published AES designs [4-6,8]. The designs in [4-6] are DPA resistant with MTD of 1st block ranging from 66x to 2500x compared to an unprotected core, and throughput slower than 5Gbps. At 16.90Gbps, the BBL core almost matches the performance of the fastest, but unprotected, AES core published to date [8], while also providing 720x DPA resistance.

References

[1] J. Daemen et al., The Design of Rijndael, Springer, 2002.
[2] U. Nawathe et al., ISSCC, pp.108-109, Feb 2007.
[3] P. Kocher et al., CRYPTO, pp. 388-397, Aug 1999.
[4] C. Tokunaga et al., ISSCC, pp. 64-65, Feb 2009.
[5] D. Hwang et al., JSSC, pp. 781-792, April 2006.
[6] P. Liu et al., ESSCIRC, pp. 71-74, Sept 2011.
[7] W. Ma et al., VLSI Circuits Symp, pp. 202-203, June 2009.
[8] S. Mathew et al., JSSC, pp. 767-776, April 2011.

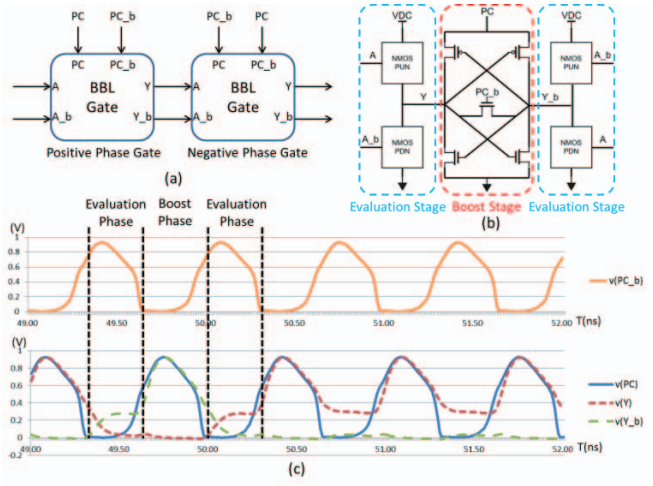


Fig. 1: (a) Cascade of BBL gates, (b) Schematic of a BBL gate, (c) Simulation operating waveforms.

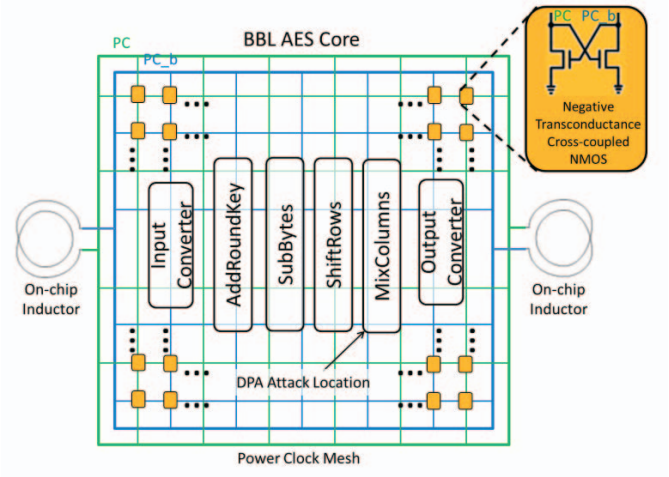
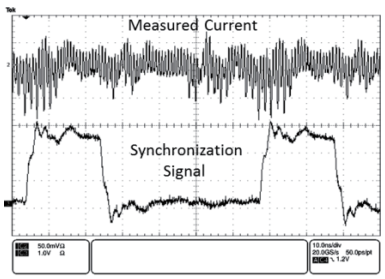
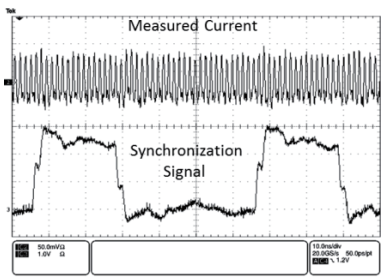


Fig. 2: Power clock generation and distribution.

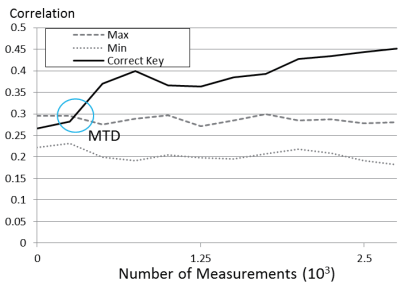


(a)CMOS Core

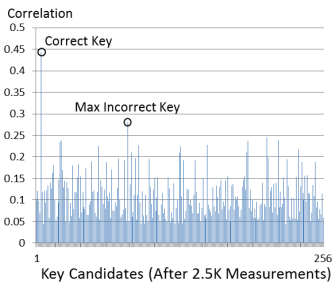


(b)BBL Core

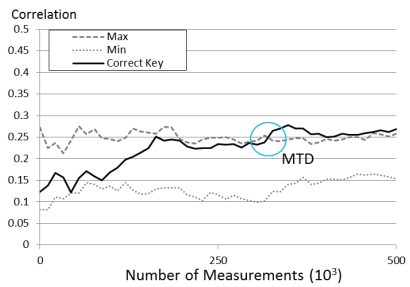
Fig. 3: Transient power supply current (@ 600MHz).



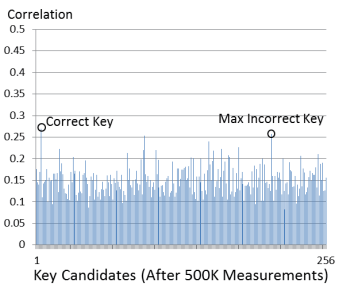
(a) CMOS: Correlation vs. Number of measurements



(b) CMOS: Correlation of different key candidates



(c) BBL: Correlation vs. Number of measurements

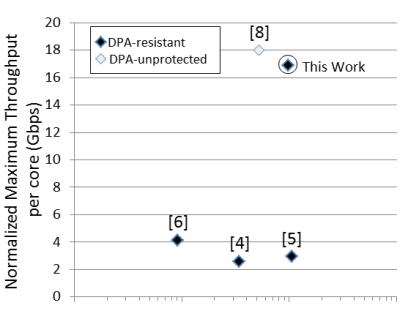


(d) BBL: Correlation of different key candidates

Fig. 4: DPA attack measurements.

Parameter		BBL	CMOS
Technology		65nm	
Supply Voltage (V)		0.41	1
Area(mm^2)	Logic	0.230	0.097
	Logic + Inductors	0.291	
Maximum Frequency (GHz)		1.32	1.32
Maximum Throughput (Gb/s)		16.90	16.90
Power (mW)		98.0	138.1
Measurements to Disclosure Min (1st block) Mean Max (Last block)		 180K 526K 940K	 250 1,360 3,750
DPA Resistance (Ratio of MTD of 1st block)		720x	
Bytes not disclosed (out of 16)		0	0

Fig. 5: AES BBL and CMOS designs characteristics.



Technology scaling from other Tech nodes to 65nm, Vdd=1V:

$$S = \frac{\text{tech node}}{65\text{nm}},\ U = \frac{Vdd}{1V},\ Delay \sim \frac{1}{S},\ Power \sim \frac{1}{U^2}$$

Fig. 6: Comparison with previously published AES chips

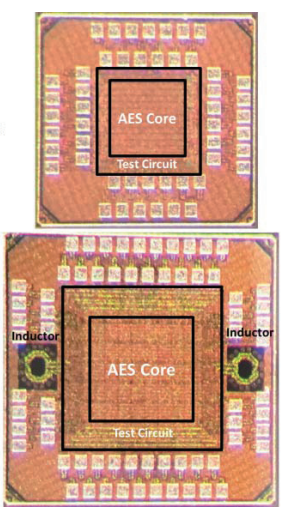


Fig. 7: Die photos