Energy and Area Saving Effect of Dynamic Partial Reconfiguration on a 28-nm Process FPGA

Yohei Hori, Toshihiro Katashita, and Kazukuni Kobara
National Institute of Advanced Industrial Science and Technology (AIST)
1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
Email: {hori.y,t-katashita,k-kobara}@aist.go.jp

Abstract—**We empirically evaluated the energy- and area-saving effect of Dynamic Partial Reconfiguration (DPR) of a 28-nm process FPGA. DPR is a technology where a portion of the entire circuit is replaced with another one, while the other parts of the circuit still continue running. Using DPR, different functionalities are not necessarily implemented at once; only required modules need be implemented on the FPGA. Therefore, a DPR system requires less hardware resources, and consequently, can save the power consumption of the system. We explored the effectiveness of DPR in saving energy and area of a multi-algorithm cryptoprocessor on Kintex-7 FPGA on SASEBO-GIII board. The cryptoprocessor supports the six ISO/IEC 18033-3 block cipher algorithms: AES, Camellia, SEED, TDEA, MISTY1, and CAST-128. In a DPR cryptoprocessor, only one cipher module is implemented at once, and it is overwritten when a different algorithm is required. Compared to the non-DPR cryptoprocessor, the DPR cryptoprocessor can reduce up to 74% hardware resource (slice) and 3.4% energy consumption.**

I. Introduction

As battery-driven mobile devices such as a cell phone, tablet computers and multi-media players have been widely used in daily lives, energy-saving and size reduction techniques of LSI have become more and more important in consumer electronics. The **dynamic partial reconfiguration (DPR)** of a field-programmable gate arrays (FPGAs) can be one of such energy- and area-saving techniques. DPR can replace a portion of the entire circuit while the other parts of the circuit continue running. Some FPGA can be partially reconfigured under the control of itself, and this type of DPR is called **Self-DPR** (We hereafter call Self-DPR just DPR). Using DPR, the functionality of the system can be altered according to, for example, user applications, performance requirements and environmental changes. In a DPR system, all modules are not necessarily implemented at the same time; a module can be downloaded when it is necessary and dynamically configured on the chip without halting the system. DPR can reduce the circuit size, and consequently, reduce the power consumption of the chip.

There are several reports regarding the energy- and area-saving effect of DPR [1], [2], but the effectiveness of DPR in 28-nm process FPGA has not been clarified yet. Therefore, we investigate the power consumption of a DPR system by developing a real DPR application on the 28-nm Kintex-7 [3]. Our DPR system is a multi-algorithm cryptoprocessor that supports the six ISO/IEC 18033-3 symmetric block cipher algorithms. The DPR cryptoprocessor implements one cipher module at once, and the module is overwritten when another cipher algorithm is to be executed. On the other hand, the non-DPR cryptoprocessor developed for comparison implements the six cipher modules at once. We compare the resource utilization and power consumption of DPR and non-DPR cryptoprocessors and investigate the effectiveness of DPR as the energy- and area-saving technique.

TABLE I
Key and block size of the cipher algorithms.

Algorithm	Key [bits]	Block [bits]
AES [4]	128, 192, **256**	128
Camellia [5]	128, 192, **256**	128
SEED [6]	**128**	128
TDEA [7]	**56**, **112**, **168**	64
MISTY1 [8]	**128**	64
CAST-128 [9]	40 to **128**	64

(Boldface values are the key size used in this study.)

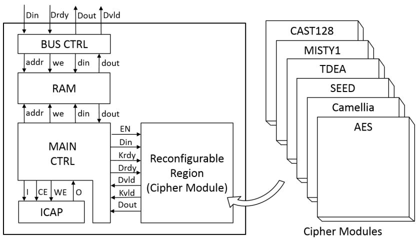

Fig. 1. Block diagram of the DPR cryptoprocessor.

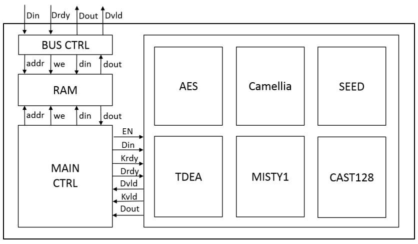

Fig. 2. Block diagram of the non-DPR cryptoprocessor.

II. DPR Cryptoprocessor

Figure 1 and 2 illustrate the architecture of our DPR and non-DPR cryptoprocessors, respectively. Both cryptoprocessor supports the six cipher algorithms shown in Table I. The boldface values are the key size adopted in this study.

As Fig. 1 shows, DPR cryptoprocessor has only one cipher module, while the non-DPR cryptoprocessor simultaneously implements the six cipher modules. In non-DPR cryptoprocessor, only one cipher module is activated using enable signal.

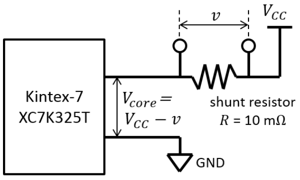

Fig. 3. Power supply line of Kintex-7.

TABLE II
HARDWARE RESOURCE UTILIZATION.

	Slice		Flip-Flop		Look-Up Table	
Non-DPR	**5,581**		**14,556**		**3,734**	
DPR-AES	**1,477**	**(-73.5%)**	**4,492**	**(-69.1%)**	1,449	(-61.2%)
DPR-Camellia	877	(-84.3%)	2,786	(-80.9%)	1,002	(-73.2%)
DPR-SEED	837	(-85.0%)	2,483	(-82.9%)	1,002	(-73.2%)
DPR-TDEA	644	(-88.5%)	1,618	(-88.9%)	797	(-78.7%)
DPR-MISTY1	1,042	(-81.3%)	3,000	(-79.4%)	937	(-74.9%)
DPR-CAST128	1,253	(-77.5%)	3,845	(-73.6%)	**1,529**	**(-59.1%)**

TABLE III
ENERGY CONSUMPTION OF NON-DPR AND DPR PROCESSORS.

Encryption Algorithm		Non-DPR	DPR	
AES	Energy [μJ]	234.1	226.2	-3.40%
	(Power [mW])	(211.9)	(204.7)	
Camellia	Energy [μJ]	463.4	453.6	-2.12%
	(Power [mW])	(209.7)	(205.2)	
SEED	Energy [μJ]	327.3	325.1	-0.675%
	(Power [mW])	(213.9)	(212.5)	
TDEA	Energy [μJ]	904.9	903.5	-0.150%
	(Power [mW])	(208.7)	(208.4)	
MISTY1	Energy [μJ]	201.6	201.9	+0.160%
	(Power [mW])	(215.6)	(215.9)	
CAST128	Energy [μJ]	344.9	346.0	+0.327%
	(Power [mW])	(213.6)	(214.3)	

III. EMPIRICAL EVALUATION

A. Experimental Setup

The DPR and non-DPR cryptoprocessors are implemented on 28-nm Kintex-7 (XC7K160T) on SASEBO-GIII board [10]. The encryption key is set to 0x000102...0F, and the initial plain-text block is 0x001122..FF. After encryption is finished, the output cipher-text is fed back to the input of the next encryption. The encryption is repeated 255 times, and these encryption processes are collectively called *one-set* encryption.

During one-set encryption, the potential difference of the shunt resistor (Fig. 3) is measured using two SMA cables and Agilent Digital Storage Oscilloscope DSO8104A. The resolution of the voltage (vertical) and time (horizontal) axes of the oscilloscope are set to 500 μsec/div and 2.0 mV/div, respectively. The sampling rate of the oscilloscope is 200 MSa/s. The power consumption was calculated from the average wave trace of 1000-set encryption.

B. Results

Table II shows the hardware resource utilization of DPR and non-DPR cryptoprocessors. As the table shows, DPR cryptoprocessor can reduce 73.5% slices, 69.1% flip-flops and 59.1% look-up tables compared to the non-DPR cryptoprocessor. The smallest Xilinx 7-series FPGA that can implement the non-DPR processor is XC7A50T, while XC7A35T is enough for the DPR-processor. Such chip size reduction would be effective for reducing the size, price and power consumption of various systems.

Table III shows the energy and power consumption during encryption on the Non-DPR and DPR cryptoprocessors. Due to the area-saving effect by DPR, power consumptions of AES, Camellia, SEED and TDEA on the DPR processor are reduced compared to the non-DPR processor. However, power consumptions of MISTY1 and CAST128 on the DPR processor slightly increased. This implies that some DPR-specific logic are implemented and working during encryption in the DPR processor, for example *partition pins* that are used for fixing interconnections between static and reconfigurable modules. It is our future plan to conduct more experiments to clarify the reason for the results.

IV. CONCLUSION

The energy- and area-saving effect of Dynamic Partial Reconfiguration (DPR) in a 28-nm process FPGA is empirically evaluated. DPR and non-DPR cryptoprocessors supporting AES, Camellia, SEED, TDEA, MISTY1 and CAST128 are implemented on Kintex-7 on SASEBO-GIII for the evaluation. The results show that the DPR cryptoprocessor can reduce 74% of circuit size and up to 3.4% energy consumption compared to the non-DPR cryptoprocessor. The non-DPR and DPR processors are both implemented on the XC7K160T in this experiments, but in actuality, the DPR processor can be implemented on a smaller chip than non-DPR one. In such case, the power reduction effect of DPR is expected to be more striking.

The future work of this study includes to implement various DPR applications and evaluate their energy- and area-saving effect.

ACKNOWLEDGMENT

A part of this work is performed as the project Core Research for Evolutional Science and Technology (CREST) funded by Japan Science and Technology Agency (JST).

REFERENCES

[1] J. Noguera and I. O. Kennedy, “Power reduction in network equipment through adaptive partial reconfiguration,” in *FPL 2007*, 2007, pp. 240–245.

[2] Y. Hori, H. Sakane, T. Katashita, and K. Toda, “Area and power reduction with dynamic partial reconfiguration of multi-algorithm cryptographic modules,” *IPSJ Trans. ACS*, vol. 1, no. 2, pp. 47–58, 2008.

[3] *7 Series FPGAs Overview, Advanced Product Specification (DS180 v1.13)*, Xilinx, Inc., 2012.

[4] U.S. Department of Commerce/National Institute of Standards and Technology, “Announcing the advanced encryption standard (AES),” FIPS PUB 197, Nov. 2001.

[5] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, *Specification of Camellia —a 128-bit Block Cipher Version 2.0*, NTT and Mitsubishi Electric Corporation, Sep. 2001.

[6] H. J. Lee, S. J. Lee, J. H. Yoon, D. H. Cheon, and J. I. Lee, “SEED algorithm specification, RFC 4269,” 2005.

[7] National Institute of Standards and Technology, “Recommendation for the triple data encryption algorithm (TDEA) block cipher,” May 2004.

[8] M. Matsui, *Specification of MISTY1 —a 64-bit Block Cipher, Version 1.00*, 2000.

[9] C. Adams, *The CAST-128 Encryption Algorithm*, May 1997.

[10] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, “SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA,” in *GCCE 2012*, 2012, pp. 657–660.