EMERGING CHALLENGES AND TRENDS IN FPGA SECURITY

Shweta Priya[1], Neetu Sagar[2]

[1,2]UG, Department of Electronics &Communication Engineering,
Raj Kumar Goel Institute of Technology for Women,
Gautam Buddh Technical University, Lucknow, (India)

ABSTRACT

Field-Programmable Gate Arrays (FPGAs) have become one of the key digital circuit implementation media over the last decade. A crucial part of their creation lies in their architecture, which governs the nature of their programmable logic functionality and their programmable interconnect. FPGA architecture has a dramatic effect on the quality of the final device's speed performance, area efficiency, and power consumption. This survey reviews the historical development of programmable logic devices, the fundamental programming technologies that the programmability is built on, and then describes the basic understandings extracted from research on architectures. Here the design and data security concerns regarding FPGA based designs, security features of different FPGA technologies and trends in advanced security architecture and countermeasures has been discussed. We include a survey of the key elements of modern commercial FPGA architecture, and look toward future trends in the field.

Keywords-FPGA,cSoC,Eavesdropping,Anti-fuse programming.

I INTRODUCTION

Field-Programmable Gate Arrays (FPGAs) are pre-fabricated silicon devices that can be electrically programmed to become almost any kind of digital circuit or system. Available in a variety of different sizes and arrangements, these can be programmed to perform almost any logic function from small to large. The tightedly coupled general-purpose microprocessor and associated sub-system of the customisable system-on-chip(cSoC) can be programmed with firmware to perform tasks best suited for sequential execution. The ever expanding number of surrounding dedicated logic blocks, memories and interfaces, SRAM, Non-volatile memory and high speed serialiser-deserialiser (SERDES) interfaces complete this almost infinitely versatile device.

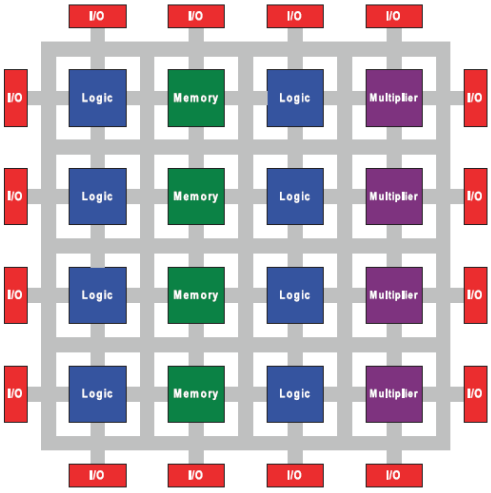

Fig-1 Basic FPGA structure

an array of programmable logic blocks of potentially different types, including general logic, memory and multiplier blocks, surrounded by a programmable routing fabric that allows blocks to be programmably interconnected. The array is surrounded by programmable input/output blocks, labelled I/O in the figure-1, that connect the chip to the outside world. The "programmable" term in FPGA indicates an ability to program a function into the chip after silicon fabrication is complete. This customization is made possible by the programming technology, which is a method that can cause a change in the behaviour of the pre-fabricated chip after fabrication, in the "field," where system users create designs. Every FPGA relies on an underlying programming technology that is used to control the programmable switches that give FPGAs their Programmability. SRAM-based FPGAs can use the latest CMOS technology available and, therefore, benefit from the increased integration, the higher speeds and the lower dynamic power consumption of new processes with smaller minimum geometries.Traditionally, FPGA and cSoC security is broken down into two distinct concepts design security and data security.

1.1 Design Security

In design security, the objective is to protect the interest of the IP honour-usually the original equipment manufacturer (OEM)-whose engineers designed the soft logic and firmware used to configure the device at the board or system-level manufacturing step. Because of the investment in creating the FPGA or cSoC soft IP, the OEM wishes to keep its design confidential so that it can't be copied or cloned. Another design security concern is overbuilding. Overbuilding is where unscrupulous contract manufacturer or his employees build more systems than the number authorised or received by the EOM,and then sell the excess systems for their own profit. FPGA can actually help reduce the occurrence of overbuilding. EOM, the risk of untrusted IP is largely moved to the configuration step rather than the foundry step. But a very real risk is the entry into the supply chain of used parts ,or parts that are remarked- from authentic but less expensive versions to more expensive

devices that should be designed or screened to faster speed grids, high temperature ranges or higher reliability levels.

1.2 Data Security

Data security moves the focus from the OEM's IP to the data processed by the device. This is typically data owned by the OEM's customer, or the customer's customer, rather than the IP owned by the OEM. An FPGA or cSoC without solid design security is not a good candidate for data security applications. In many projects data security is only a miner concern, but in some applications, such as financial payment and military communication system, data security is paramount.

1.3 Eavesdropping

Tampering can occur at the device level or system level. This is where an attacker tries to gain some advantage by finding out information to which he should not have access. This may be by eavesdropping on signals that where intended to be confidential. Network attacks rightly get allot of attention since poorly designed protocol or network protection such as firewalls may allow an adversary to steal information from the comfort of an internet café halfway around the world. There are attacks that get right down to the hardware level, and try to steal the IP right out of a device. This may involve first extracting cryptographic keys from the device that are used to protect the IP, perhaps together with capturing a new configuration file being downloaded to a device in field. Extracting processor firmware and reverse engineering it is another real threat. With the keys, it is usually possible than, and in some cases easy, to decrypt the bit stream. The device can emit or respond to light but the silicon device is not mechanically disturbed. Generally, as an attack becomes more invasive, it is more expensive to mount, requiring expensive equipment like electron microscopes and focussed ion beam machines.

1.4 Different Technologies Used

There are two main technologies used for commercial FPGAs: SRAM and Flash. In addition, anti-fuse FPGAs are still used in space applications, which require enhanced tolerance to background radiation.

1.4.1 SRAM Based FPGAs

SRAM FPGAs, including those from Xilink and Altera, hold device configuration bits in volatile SRAM cells. These bits determine the logic function that the FPGA performance, since the configuration memory is volatile. In low-end devices, the configuration bit stream moves from the external non-volatile memory where it is held, to the SRAM FPGA, in unencrypted form. This provides virtually no security, as anyone with a storage scope or logic analyser can easily record the data.

1.4.2 FLASH Based FPGAs

In flash-based FPGAs, configuration bits are held in non-volatile flash memory. Thus the configuration needs to be loaded only once-typically during the board assembly process, since flash memory is also re programmable, flash FPGAs can be reconfigured multiple times over their lifetime. Flash-based cSoC devices also have on-chip embedded non-volatile memory (eNVM) for holding the processor firmware securely on-chip. For secure field upgrades of the FPGA fabric configuration and/or eNVM array, most flash FPGAs also offer

built-in bit stream decryption functionality. One alternative that addresses some of the shortcomings of SRAM based technology is the use of floating gate programming technologies that inject charge onto a gate that "floats" above the transistor. This approach is used in flash or EEPROM memory cells. These cells are non-volatile; they do not lose information when the device is powered down.

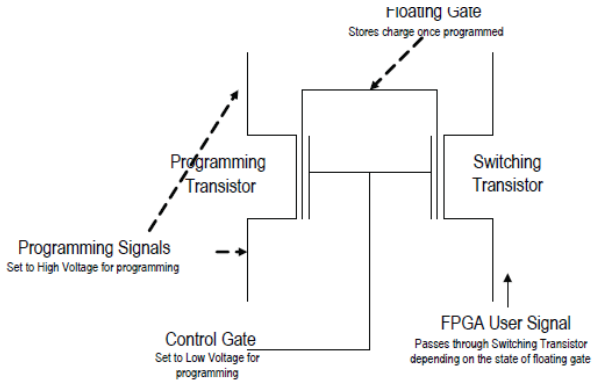

Fig 1.2 Floating gate transistor

1.4.3 Anti-Fuse Programming Technology

An alternative to SRAM and floating gate-based technologies is anti fuse programming technology. This technology is based on structures which exhibit very high-resistance under normal circumstances but can be programmably "blown" (in reality, connected) to create a low resistance link. Unlike SRAM or floating gate programming technologies.

Table 1 Programming technologies summary

	SRAM	**Flash**	**Anti-fuse**
Volatile	Yes	No	No
Reprogrammable	Yes	Yes	No
Area(storage element size)	High (6 transistors	Moderate(4 transistors)	Low(0 transistor)
Manufacturing process?	Standard CMOS	Flash process	Needs special development
In-system programmable?	Yes	Yes	No
Switch resistance	~500-1000Ω	~500-1000Ω	20-100Ω

II TRENDS IN ADVANCED SECURITY ARCHITECTURE AND COUNTERMEASURES

The threat environment is daunting, but all hope is not lost. No security is absolute, but with proper architecture and design, next-generation FPGAs will be significantly stronger than those security on the market. Next-generation FPGAs and cSoCs would incorporate DPA countermeasures for all built-in 'bit stream' cryptographic operations. It is expected that deployment of DPA countermeasures will become the norm in the FPGA industry, as in the case with mirco-controllers used in financial applications, set-top box and the trusted platform module chips used in computers.

Over the next few years, we can expect to see the protocols used to initially configure and upgrade FPGAs and cSoCs improvement to provide more features and improved security. New use models that help reduce costs will become available, especially where security demands are elevated, such as when board and system manufacturing is done by contract manufactures, or is more sensitive applications such as system used for national defence or home security.

III CONCLUSION

The threat level for FPGA and cSoCs will continue to increase as attacks get better. At the same time, more applications are demanding enhanced data security. for example industrial control and data security.For example, industrial control and medical devices that in past barely considered security are more and more considering it a prime design requirement.This trend is being accelerated by machine –to-machine applications and the internet of things.

IV ACKNOWLEDGEMENT

This survey has explored many issues in the complex and rapidly evolving world of pre-fabricated FPGA architectures. While these devices have changed dramatically in last two decades, it is clear that many fundamental questions remain, driven by rapid changes in technology and applications.

REFERENCES

[1] Actel Corporation, *"ACT 1seriesFPGAs," http://www.actel.com/* documents/ACT1 DS.pdf, April 1996.

[2] Actel Corporation, "*Axcelerator family FPGAs*," http://www.actel.com/ documents/AX DS.pdf, May 2005.

[3] Actel Corporation, "*ProASIC3 flash family FPGAs*," http://www.actel. com/documents/PA3 DS.pdf, October 2005.

[4] Actel Corporation, "*Single-event effects in FPGAs*," http://www.actel. com/documents/FirmErrorPIB.pdf, 2007.

[5] Actel Corporation, "*SX-A family FPGAs v5.3*," http://www.actel.com/ documents/SXA DS.pdf, February

2007.

[6] A. Aggarwal and D. Lewis, "*Routing architectures for hierarchical fieldprogrammable gate arrays*," in IEEE International Conference on Computer Design, pp. 475–478, October 1994.

[7] E. Ahmed, The Effect of Logic Block Granularity on Deep-Submicron FPGA Performance and Density. Master's thesis, University of Toronto, Department of Electrical and Computer Engineering, 2001.

[8] E. Ahmed and J. Rose, "The effect of LUT and cluster size on deep-submicron FPGA.