# SECURITY ASPECTS OF LATTICE SEMICONDUCTOR iCE40 MOBILE FPGA DEVICES

## DISCUSSION OF NONVOLATILE AND VOLATILE MEMORY WITHIN LATTICE SEMICONDUCTOR iCE40 PRODUCTS

A Lattice Semiconductor White Paper

September 2013

Lattice Semiconductor
5555 Northeast Moore Ct.
Hillsboro, Oregon 97124 USA
Telephone: (503) 268-8000
www.latticesemi.com

**ABSTRACT:**

There are no ways known to Lattice Semiconductor to physically or electronically read the Non-Volatile Configuration Memory (NVCM), or to trace its path to the Configuration RAM (CRAM) or Block RAM (BRAM) memory areas, or to otherwise extract digital information stored in NVCM or CRAM memory areas.

In addition to superior physical on-chip security, mobileFPGA™ devices lower the risk and associated cost of obsolete inventory in the case of Mask ROM products, and the cost and security weaknesses of external memory required to configure standard FPGA products.

# Security Aspects of Lattice Semiconductor iCE40 mobileFPGA™ Devices

## Introduction

Product piracy is of strong concern to major companies around the world. R&D costs are very high for leading companies. Therefore, companies plan to recoup these R&D costs by sale of their proprietary products. If pirates are able to steal or copy the final design, or countermand the security systems of these proprietary products, the market will become flooded with low cost alternatives. As a final consequence, major companies will find themselves unable to recover their high development costs, and will lose valuable profits.

One way in which companies protect their products is by incorporating digital security keys. From Blue- Ray DVDs to camera batteries, we find many items are encoded so that the products which use or read them can determine legitimate ones from pirated copies. Smartcard chips, which interface to banking systems, likewise incorporate techniques to prevent internal calculations from being deciphered by pirates.

## Secure Custom Mobile Devices by Lattice Semiconductor

At Lattice Semiconductor, we have engineered particularly useful iCE40 mobileFPGA devices -- products which are well adapted to mobile, handheld electronics. Our iCE40 mobileFPGA products contain the fabric of familiar FPGAs enabling complex logical calculations to proceed rapidly in parallel. The configuration of this logic fabric would be insecure if installed in the standard way via external RAM such as Flash. During external configuration, the serial bitstream could be detected by an oscilloscope or logic analyzer attached to the serial input line. With effort, the bitstream could be deciphered into the configuration of the FPGA itself, and might be able to be copied to other FPGA devices.

Lattice Semiconductor iCE40 products defeat this method of piracy. In Lattice Semiconductor iCE40 products, logic fabric configuration data can be incorporated

within the chip itself in a dense block of transistor memory. The transfer of this digital data to the configuration of the chip is hidden within the chip and does not appear at any external port. After the NVCM data is written by the customer or Lattice Semiconductor, a security flag can be set which locks the NVCM memory. Once this security flag is set, it cannot be reset and the NVCM cannot be adjusted or directly read.

## Security of the iCE40 On-Chip NVCM Memory

The physical nature of the NVCM memory provides itself an extremely high level of security. This memory does not use floating gates, such as common in Flash or EPROM memories, whose data can be revealed by voltage contrast methods. There is no charge on the gates of the programmed or unprogrammed memory cells. In the technologies used to produce Lattice Semiconductor products, modern lithographies of 65nm or smaller are employed. Our memory transistors are below $1/10^{th}$ the wavelength of visible light (400nm to 700nm from violet to red). Additionally, the memory cells are buried below 8 or more layers of metal interconnect wiring, further obscuring any nondestructive direct optical inspection. In general, our NVCM binary 1 or 0 memory cells cannot be distinguished by either visual or SEM means. Even chemical stripback and decoration methods will falsely reveal erroneous "1" and "0" valued cells in the collection of nearly a half million memory cells used to configure Lattice Semiconductor products.

The NVCM memory is programmed by slightly changing the insulating properties of the core transistor gate dielectric. These changes in conductivity are thought to occur due to changes in the chemical bonding in atomically sized regions of the gate dielectric. There is no change to the chemistry of the material itself - the same atoms remain in position. Unlike earlier technologies which vaporized metal or non-metal fuses, the Lattice Semiconductor method does not result in physical material transport. Consequently, there is no way known to the Lattice Semiconductor Technologies to chemically or physically detect the logical state of each of the nearly half-million memory cells.

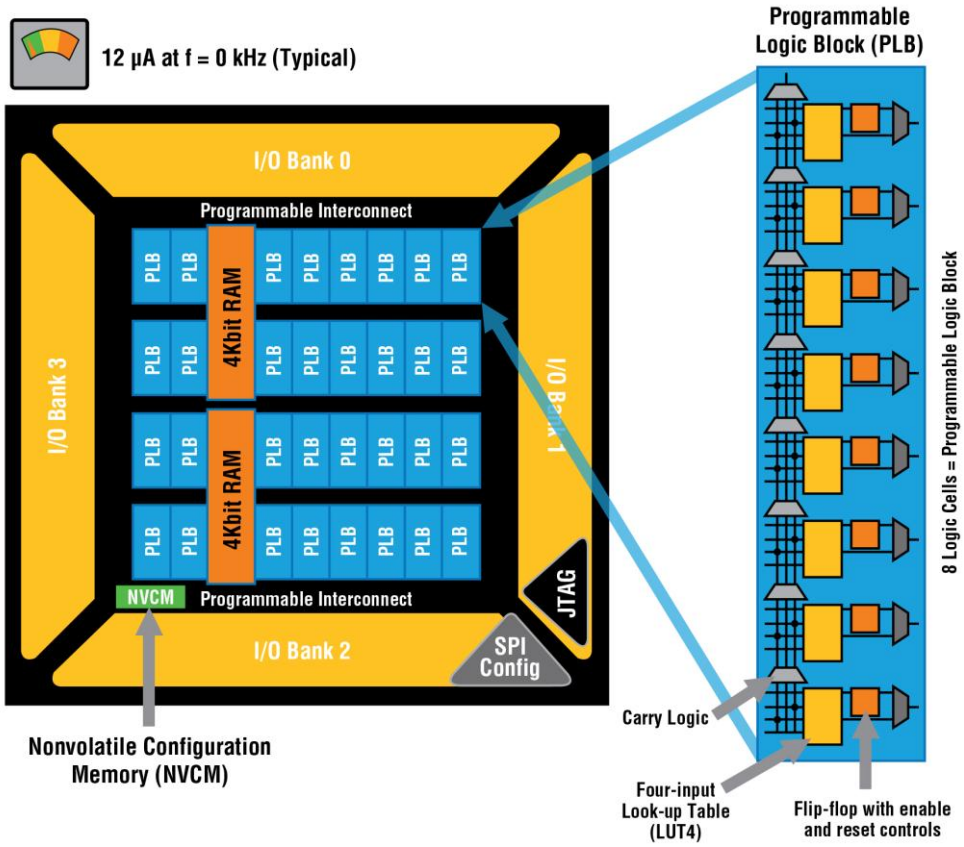


**Figure 1: Block diagram of mobileFPGA showing NVCM in lower left, Block RAM labelled here 4kbit RAM sections, and CRAM located in every PLB block throughout the chip.**

## Security of the Transfer of On-Chip NVCM Memory to On-Chip CRAM and BRAM

Even if one could invent a way to see the logical state of the NVCM memory cells themselves, the NVCM memory cells are not connected in a straightforward manner directly to the CRAM or BRAM memory blocks. Memory cells from separate sections of the NVCM memory block are combined by the on-chip Finite State Machine (FSM). The FSM mathematically combines bits from different parts of the NVCM memory, and then stores a final digital value in various RAM blocks of the chip. The other RAM blocks are known as Configuration RAM (CRAM) and Block RAM (BRAM). The CRAM is ordinarily used to hold the logical switching information necessary to tell the logical unit (LUT) cells what type of logical operation to perform and whether to be connected

to other LUTs. The BRAM is ordinarily used to hold calculation data. However, calculation data can be stored in CRAM as well.

## Security of the On-Chip CRAM and BRAM

As long as the NVCM data is sent to the CRAM memory block, there is no way to externally read that data from the chip. NVCM data which is sent to the internal Block RAM (BRAM) can possibly be read later by cleverly manipulating the chip after a Configuration Reset with power still applied to the chip, so secure data should not be stored in BRAM memory. In contrast to BRAM memory, all data stored in the CRAM memory block is completely erased during a Configuration Reset.

On resetting the product with power still applied, it is possible to insert a new program in CRAM that will read the BRAM data out. However, on resetting the product, the CRAM memory itself is fully erased and there is no possible way to read the CRAM data externally. Therefore, storing Digital Key data in the NVCM with the protection flag set, and then sending that secure data to the CRAM memory of the chip, there is no way to extract it.

## Conclusion: Security of Lattice Semiconductor iCE40 mobileFPGA™ Devices

Consequently, by storing any digital secure data, such as a secure digital key or algorithm, in NVCM and then specifying that data to be transferred only to CRAM, the data cannot be externally read from Lattice Semiconductor products. There are no ways known to Lattice Semiconductor to physically read the NVCM memory or to trace its path to the Configuration or Block RAM memory areas. Lattice Semiconductor internal engineering cannot conceive of any way to reverse engineer or read back the physical or logical memory locations within the NVCM or CRAM areas. Only the BRAM area can be conceived as an area of memory that can be accessed with expert knowledge of the chip, but there is no need for secure digital key or algorithm information to be stored in that insecure location.