Design Security in Nonvolatile Flash and Antifuse FPGAs

Security Backgrounder

Table of Contents

1. Introduction

FPGAs continue to grow in density and capability, enabling users to implement more complex and valuable designs. With today's larger format wafers and smaller process geometries, mask costs continue to rise while minimum lot sizes have also increased in orders of magnitude. As a result, cost-effective user-customized PLD products have displaced incumbent ASIC technology as the solution of choice for today's most complex design tasks. Fundamentally, this shift has created the need for secure programmable logic solutions to protect expensive and proprietary intellectual property. This poses a problem since presently, FPGA design security is poorly understood. This white paper describes the problem of silicon design security as it exists today along with the various merits and drawbacks of the dominant solutions currently available.

2. Design Security Concerns

Design theft has historically been the greatest concern with military projects. However, as programmable logic's integration capability and performance rise and as cost per gate plummets, the potential for cloning and reverse-engineering becomes a concern for an increasing number and variety of broader-based applications. Many new PLD-based systems that previously utilized ASIC technology are now attracting the attention of a new generation of hackers.[1]

Hackers or "Crackers" as they are often called, target not only FPGA designs, but also the information contained within a data stream being sent to or from a system. As a result, when considering security, there are two distinct classes of design security needs to consider:

1. Intellectual property (IP) security: the designer/vendor wants to protect a product or design (their IP) embedded in an FPGA or ASIC platform from being "cloned" or reverse engineered.
2. Data security: the designer/vendor wants to protect the integrity and confidentiality of a data stream being sent to or from an FPGA or ASIC. Users are concerned with preventing device designs from being copied, corrupted, or otherwise interfered with.

IP Security is the primary concern of companies or IP developers whose competitive advantage is derived from their ability to implement complex proprietary designs. It is also the primary concern for manufacturers of mid-to-high volume consumer electronics whose market share and profitability may be eroded by cloned or counterfeit versions of their product.

Data security is the primary concern in cryptographic or financial applications. Users of such applications include the military (nuclear weapon systems or communication systems), financial institutions (automated bank tellers), consumer electronics manufacturers (pay TV and set-top boxes) and corporations sensitive to copyright infringement (game manufacturers).

Design Security: Some Likely Scenarios

The following examples detail typical security breeches that affect users of FPGAs. They have been broken out to distinguish between the protection of the design and the protection of the data within a system. There are many complex issues involved in the subject of design security. This paper focuses on the most common security problems for today's designers.

1. *Dipert, Brian, "Cunning Circuits Confound Crooks," EDN [online] (12 October 2000, 103-112.[Cited 12 August 2002]); available from http://www.e-insite.net/ednmag/contents/images/21df2.pdf.*

IP Security

Run-on Counterfeit

Run-on fraud is the largest single source of counterfeit goods, and almost the sole source in many sectors. Typically, an OEM contracts production of a design to an independent assembly house, who in turn, over runs the build for resale through grey market importers. The finished goods are often identical in every way to the OEM's production units but are usually re-sold at discounted rates serving to erode margins and profitability of the original designer. The broad use of contract manufacturers in today's business environment creates many opportunities for unscrupulous OEMs to capitalize on almost any designer's valuable IP. As a result, OEMs need a mechanism to stop unauthorized overproduction.

In certain industries key ingredients and packaging are sourced from multiple suppliers whose identities may be kept secret from the contract manufacturer. Unfortunately, today most consumer electronics systems typically utilize a readily available, easily identified standard product offering for all board-level content. To further compound the problem, in many new systems the FPGA is used to tie together a board full of ASSPs (Application Specific Standard Products). In other words, the ease with which a system can be copied results from how easily any particular PLD can be cloned. One common strategy to limit production to authorized quantities is to use a secure PLD technology and do all programming in-house and supply only programmed units to a contract manufacturer.

Reverse Engineering and Cloning

Currently, many people consider reverse engineering a design process, and many engineering schools offer it as a standard course of study. Reverse engineering was originally used as a means of improving on a competitor's product while avoiding the original design effort.[2] Today, reverse engineering is a big business with many companies specializing in providing in-depth analysis using a variety of means, from simple observation and test, through the most advanced intrusive optical and electromagnetic surveys. Conventional wisdom recognizes that no silicon solution is totally secure. Once a function is hard-wired into a chip, it can eventually be defeated. IP security depends upon three factors:

1. The value of the design or secret being protected. This can range from nearly infinite (securing a trigger for a nuclear device) to very low (the stored value on a single phone card). Often the value has a time component (the market window for a consumer product or the usable life of a set-top box).
2. The cost to implement security measures. These can range from zero (do nothing) to very high (epoxy encased circuit boards installed in locked chassis with round-the-clock surveillance or a cryptographic key infrastructure).
3. The expected cost to attack or defeat security measures. These can vary from very low (cost of copying a boot device for an SRAM FPGA) to prohibitive (evading surveillance to remove and reverse engineer an epoxy encased circuit board).

The general position of the design community has held that the price a designer is willing to pay for security is proportional to the value of the design. Though increasingly, market trends are converging to drive down cost and effort necessary to clone many FPGA designs that were previously unnoticed and safe from attack. If designers are uncomfortable with the thought of their code being placed in the public domain, they potentially have a security problem with certain types of PLD architectures. The reality is that many designers using SRAM-based FPGAs fail to recognize the vulnerabilities of the technology.

As previously stated, through reverse engineering, a competitor copies a design by essentially reconstructing a "schematic" level representation from the physical device. In the process, he understands how the design works, how to improve it, and how to disguise it so that it no longer looks like your original work. An even greater concern is cloning. Cloning requires something that is easily copied. This is

2. *Shankar, Nitin K., "Can Reverse Engineering Answer Your Design and Prototyping Needs?" [online], (India: Brown and Sharp, [cited 12 August 2002]); available from http://www.brownandsharpe.com/mfg/mfg7/mfg7ar10.html.*

the situation with SRAM-based FPGA designs (Figure 1). A competitor either makes a copy of the boot prom or intercepts the bitstream from the on-board processor and copies the code. He does not know how your design works, nor does he need that information. He is able to steal the entire design merely by copying the external bitstream, which is always required for an SRAM FPGA.

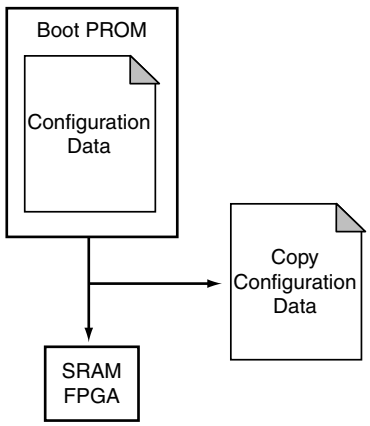

Figure 1 • *Cloning an SRAM FPGA*

Data Security

Service denial: Denial of Service (DoS) is consistently ranked as the single greatest security problem for IT professionals. DoS attacks deny service to valid users trying to access a site. For example, an attacker might flood a web server with requests, rendering the web server temporarily unavailable or unusable. DoS attacks are problematic because they are easy to achieve and can be anonymous. Typically, these attacks have been viewed exclusively as an IT problem, but increasingly, researchers and designers are looking into this problem from a hardware design perspective. There are four main types of denial of service attacks: CPU starvation, memory starvation, resource (or disk space) starvation, and network bandwidth starvation.[3] In each of these scenarios, the attacker is trying to get an application to run in an endless loop until the specified resource is used up, preventing valid users from accessing the site.

Researchers and hardware designers are now looking at another possible means of DoS attack that targets systems using a reconfigurable FPGA. In this scenario, a hostile party could intercept a bitstream being downloaded into a customer device and leave the ID unchanged but replace the rest of the bitstream with random bits. The likely result is an internal electrical conflict that may destroy the device. (Such a problem arose with an FPGA vendor whose customer accidentally destroyed their FPGA by downloading bad ciphertext in error). This method could be used as a service-denial attack on a vendor by a competitor or enemy, on a larger scale by one country against another, or possibly as a means of terrorist attack against a widely used product or service.

Theft of Service

Consumer electronics are shrinking in size while growing in capability. The latest wired and wireless e-appliances have enabled consumers to process instant secure transactions and purchase a variety of goods and services anywhere at anytime. The cornerstone of these subscriptions and pay per use models have been subsidized by hardware like set-top boxes or mobile phones that are associated with extended service contracts. The problem is that grey market traders buy goods in countries where the consumer

3. *Microsoft MSDN Library, "Preventing Denial of Service Attacks," [online] (Microsoft Corporation, 2002 [cited 12 August 2002]); available from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securecode_vyyk.asp.*

hardware is subsidized. They make the necessary software changes and resell the appliances in areas where they are not subsidized. Past attempts to prevent grey exports were circumvented by pirates in a matter of weeks. Economies of scale effectively prevent entry into the market of building cloned units so the focus of the pirates has been on beating the security in existing hardware. As a result, merchants in this market place cannot afford to deliver easily compromised hardware. In considering the problem of theft of service, OEMs recently invested efforts to explore solutions similar to a software dongle that might prevent the pirates from compromising rewriteable circuits in the base stations mobile handsets.[4,5] Security measures for critical infrastructure can be beaten by inadequate solutions on the consumer POS terminals. It is necessary to thoroughly evaluate all points of origin for invasive attacks that can compromise a secure network or service.

3. Intellectual Property and IP Theft

As the world moves from the industrial age to the information age, the global economy is increasingly dependent on the production and distribution of creative, technical, and intellectual products. These valuable products, collectively known as "Intellectual Property" (IP), are becoming the primary fuel of the global economic engine. The International Anti-Counterfeiting Coalition recently reported that the combined U.S. copyright industries and derivative businesses account for more than $433 billion, or 5.68%, of the U.S. Gross National Product, which is more than any other single manufacturing sector. The Bureau of Labor Statistics reported that between 1977 and 1996 the growth in the IP segment of the economy was nearly twice that of the U.S. economy as a whole.

Like any other valuable product, IP is eagerly sought by criminals. IP theft has grown dramatically in recent years resulting in enormous economic losses. These losses not only undermine the position of those who create and own IP, but they also pose a significant threat to the health and viability of the global economy. The International Anti-Counterfeiting Coalition estimated that U.S. companies lost $200 billion in 1997 due to worldwide copyright, trademark, and trade secret infringement. On the law enforcement front, the United States Customs Service reported that it seized more than $70 million in IP-infringing merchandise, which was intended for sale in America in 1998.[6]

4. Key Accelerators: FPGA Security

The rapid acceptance of programmable logic solutions, and their subsequent proliferation in the market has created a host of new security concerns for system-level designers. With virtually limitless liability at stake, OEMs are racing against a number of convergent forces.

Migration from ASICs to PLDs

The increased complexity and density offered to today's logic designers has allowed FPGAs to move to the core of many new systems that had previously been occupied by ASICs or other standard cell solutions. No longer exclusively a peripheral or "glue" logic, FPGAs are being used to perform highly complex timing control functions, and implement high speed interconnect solutions and even state of the art cryptography designs. These advances have enabled relatively low cost flexible solutions that allow designers to bring products to market faster than ever before, but there is a price. The security limitations of SRAM-based FPGA technology are well known, as the devices are easily cloned by copying a bitstream sourced to the SRAM FPGA by either a nonvolatile boot PROM, a microprocessor, or Flash Cache (Figure 2 on page 9).[7]

4. *Anderson, Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems (New York: John Wiley and Sons, 2001).*

5. *Tecnocad S.r.1., "Keylock 2: An Electronic Key for Software Protection is Improved by FPGA Technology Allowing New Features," [online] (Italy: Tecnocad S.r.1., [cited 12 August 2002]); available from http://www.fuse-network.com/fuse/demonstration/30/24566/index.html.*

6. *Federal Bureau of Investigation the Financial Institution Fraud Unit, "Financial Institution Fraud," in About Intellectual Property Crimes [online] (Washington D.C.: FBI, [cited 12 August 2002]); available from http://www.fbi.gov/hq/cid/fc/fifu/about/about_ipc.htm.*

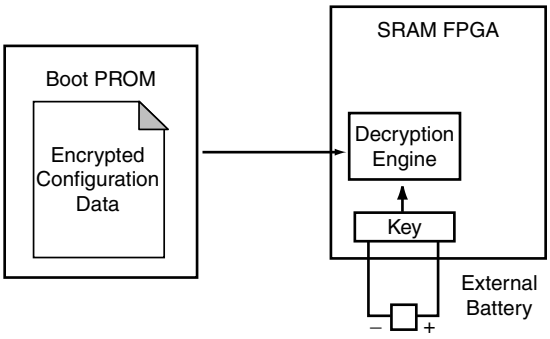

Figure 2 • SRAM FPGA with On-Chip Bitstream Decryption

Hacking on the Rise

Cyber crime and other electronic attacks against our nation's critical infrastructure are on the rise. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites or systems. Thus, while attack tools have become more sophisticated, they have also become easier to use. As the technology becomes more accessible, so does the means to use it for far more nefarious activities. The FBI has documented an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. Beyond criminal threats in cyberspace, we also face a variety of significant national security threats. Terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that "terrorist. . .organization[s] are using computerized files, e-mail, and encryption to support their operations."[8]

In addition to these typical cases, there are several recent publications describing other types of intrusive hacking that targets board-level components. In their report entitled, "Online Viruses," Hadzic, Udani, and Smith discuss the possibilities for "FPGA Viruses." They explore the possibilities open to bitstreams from a malicious source, which could create electrical conflicts that destroy the device.[9] More familiar information security threats include inducing behaviors that causes neighboring devices to fail and replication of a malicious code either using hardware or software as an intermediary. Kean suggests a number of higher-layer protocols for IP management so that separate IP cores could be purchased and downloaded under keys installed at the factory.[10]

7. *Some SRAM FPGA manufacturers have acknowledged this inherent limitation by incorporating a defense against this cloning attack in their latest generation devices. This defense is compromised of an on-chip bitstream decryption engine with an on-chip key that is loaded into battery powered on-chip memory on the board by the board manufacturer. An inefficient solution at best, this approach is difficult to implement and raises a number of challenging board-level design considerations. Furthermore, the use of a battery introduces the possibility of system malfunctions and the need for redundancy, further increasing the total cost of a system.*
8. *FBI Congressional Statement, Statement for the Record of Guadalupe Gonzalez Special Agent in Charge, Phoenix Field Division Federal Bureau of Investigation on Cybercrime [online] (Washington, D.C.: FBI, [cited 12 August 2002]); available from http://www.fbi.gov/congress/congress00/gonza042100.htm.*
9. *Hadzic, I., S.K. Udani, and J.M. Smith, "FPGA Viruses," [online] (Philadelphia, PA: University of Pennsylvania, [cited 2002 August 12]); available from http://www.cis.upenn.edu/~boosters/fpgavirus.ps.*
10. *Kean, T., "Crypto Rights Management of FPGA Intellectual Property Cores FPGA," [online] [cited 12 August 2002]; available from http://www.ecs.umass.edu/ece/fpga2002/.*

Dissemination of Information

The burgeoning problem of cyber intrusions, viruses, and DoS attacks poses unique challenges in an age when virtually all information, on any subject, can be made instantly available to anyone around the world. It also poses significant difficulty for those who would determine the source of a particular attack. This stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. As long as the Internet remains rife with vulnerabilities and allows easy anonymity and concealment, these attacks will continue to create problems. This anonymity also proliferates through damaging and malicious activities, which involve the posting and broadcast of sensitive or proprietary intellectual property. This means, potential damages from criminal intrusion are no longer limited to the single instance of compromise. If your system is vulnerable to outside attackers, the details of the hack combined with any valuable IP stolen, can now be easily and anonymously placed in the public domain, increasing the potential damage from any single attack to nearly infinite levels.

5. Defending a Design From Attack

The ability of adversaries to reverse engineer an integrated circuit can be rated on three different levels. Each level corresponds to varying degrees of security discussed in Abraham et al's article, "Transaction Security System," from the IBM Systems Journal. Adversaries are grouped into three classes, in ascending order, depending on their expected abilities and attack strengths:

Class I: (clever outsiders) A knowledgeable individual using low cost, easily available tools or services could reverse engineer a design in a short period of time. These low security solutions are usually included in products such as phone cards, debit cards, and set-top boxes.

Class II: (knowledgeable insiders) A skilled individual or team with access to expensive sophisticated equipment could reverse engineer a design given sufficient time. Individuals involved in reverse engineering at this level are usually associated with a commercial enterprise such as a game copier or other cloned consumer electronics.

Class III: (funded organizations) A highly skilled team, using equipment not commonly available in the commercial market and with substantial time could reverse engineer a design. This third category is largely limited to government agencies like the NSA with nearly unlimited funds available for their activities.[11]

ASICs are Susceptible to a Class II Attack

On its own, ASIC technology (also standard cells and gate arrays) is thought to be vulnerable to a class II attack. In applications requiring security from perpetrators with access to class II capabilities, traditional methods have employed ASICS with additional measures such as epoxy encasing and tamper sensitive explosive devices. There are many commercially available alternatives to the individual or organization interested in reverse engineering an ASIC, and you only need to look as far as the world wide web to find then.

Methods of attacking ASIC technology, cited in Blythe et al's article, "Layout Reconstruction of Complex Silicon Chips," involve expensive equipment and tools, including:

- Cleanly imaging and etching away successive layers of a device and post-processing the images to render clean polygon images of the circuitry. This technique was employed to reverse engineer an Intel 80386 in two weeks.[12]
- Building on the above techniques, Chipworks Inc. has developed software to automatically generate circuit schematics from the polygon images.[13]

11. *Abraham, D.G., G.M. Dolan, G.P. Double, and J.V. Stevens, "Transaction Security System," IBM Systems Journal (vol. 30, no. 2) (1991: 206-229).*

12. *Blythe, S., B. Fraboni, S. Lall, H. Ahmed, U. de Riu, "Layout Reconstruction of Complex Silicon Chips," IEEE Journal of Solid-State Circuits (vol. 28, no. 2) (Feb. 1993: 138-145).*

SRAM FPGAs are Susceptible to a Class I Attack

As mentioned earlier, a number of factors have contributing to the rise of FPGAs over competing ASIC technologies. However, this shift has also introduced higher levels of risk to the security of a design. As the value of the designs implemented in FPGAs increases, security limitations of the dominant SRAM-based FPGA technology begins to limit market penetration and, ultimately, revenue growth potential. SRAM FPGAs are classified as Level I security because the devices are easily cloned by intercepting and copying the bitstream.[14]

The classic method of reverse-engineering a programmable-logic design involves cycling through all possible device input combinations and capturing the corresponding output bit patterns. Essentially, by using a huge Karnaugh map (often with high-powered computer help) or through visual inspection of data patterns, a thief can derive the Boolean equations that define the internal logic. A more common loop-hole with SRAM FPGAs is for a pirate to simply capture and copy the device's configuration data.

All SRAM FPGAs come with a security back-door that leaves designs vulnerable to compromise. Internet news groups regularly detail the ease with which one can simply read back the internal configuration bitstream through a chip's JTAG or proprietary programming interface.[15]

Today's largest suppliers now integrate a variety of security settings in all FPGAs, but unfortunately, even "locking" your SRAM chip with the vendor's security bit might not be good enough to prevent theft. It is easy to surmount some device families' security safeguards by applying high-voltage sequences to certain pins. This action puts the chips into manufacturing test modes, which re-enable internal-device-state access.[16] With these inherent holes in device security, some SRAM vendors have had to resort to novel solutions to try and beat determined hackers.

As previously outlined, SRAM manufacturers have proposed a novel solution requiring a board-level battery to maintain the integrity of a securely programmed device. While this defense is effective when it works, it does come with significant costs to implement, including:

- Cost of implementation and maintenance: Using this method requires overhead in terms of personnel and process to maintain an encryption key database and the necessary infrastructure at the board manufacturer.
- Reliability cost: Due to the battery-powered key storage mechanism. If the battery fails in the field, the board will fail. Raising the question of further redundancy for system integrity.

Nonvolatile Flash and Antifuse FPGAs are More Secure than ASICs

In contrast to the inadequate, easily cloned, SRAM FPGAs, there are two nonvolatile FPGA technologies that are even more secure than competing ASIC technologies. They are antifuse-based FPGAs and Flash-based FPGAs. These two technologies derive their security from:

- Nonvolatility, which enables them to be configured before they are shipped to the end-user. Unlike SRAM technology, there is no bitstream that can be intercepted.
- Difficulty in determining the state (on or off) of the programming elements on a programmed part. In contrast with easily visible vias on an ASIC, it is very difficult to determine whether a given programmable antifuse or Flash switch element is on or off.
- A large number of switch elements (millions on the largest devices). Given that the state of a single switch is difficult to determine, trying to determine the state of millions is prohibitive.

---

13. *Chipworks, (2002 [cited 12 August 2002]), available from http://www.chipworks.com/.*
14. *Algotronics, "Secure Configuration of Field Programmable Gate Arrays."*
15. *Dipert, Brian, "Cunning Circuits Confound Crooks."*
16. *Ibid.*

Direct Physical Attack of Antifuse FPGAs

As previously stated, compromising an antifuse FPGA is exceedingly difficult. Antifuse PLDs do not require a bitstream for configuration, which means all the design data is internal to the chip. In addition, it is impractical and, in many cases, impossible to compromise an antifuse device with invasive methods, making the devices even more secure than ASICs. Antifuse technology uses a layer of amorphous silicon in the via, which causes an isolation between the metal layers. In the unprogrammed state, the amorphous silicon has very high resistance, thus isolating the metal layers. When a programming voltage is applied, the amorphous silicon changes to a low impedance state, creating a metal-to-metal interconnect.

Using traditional techniques to reverse engineer antifuse FPGAs are useless. Etching away the surface will only reveal the top of the vias and not the state of the amorphous silicon. One way to identify a programmed link would be with the use of a SEM (Scanning Electron Microscope) to view each of the antifuse links. Millions of links are on a single antifuse FPGA and only a small fraction (2-3%) are actually programmed. It would take years to scan each link to identify its programming state. To put it in perspective, Actel's AX2000 antifuse FPGA contains approximately 53,000,000 antifuse elements in a single device (Figure 3).

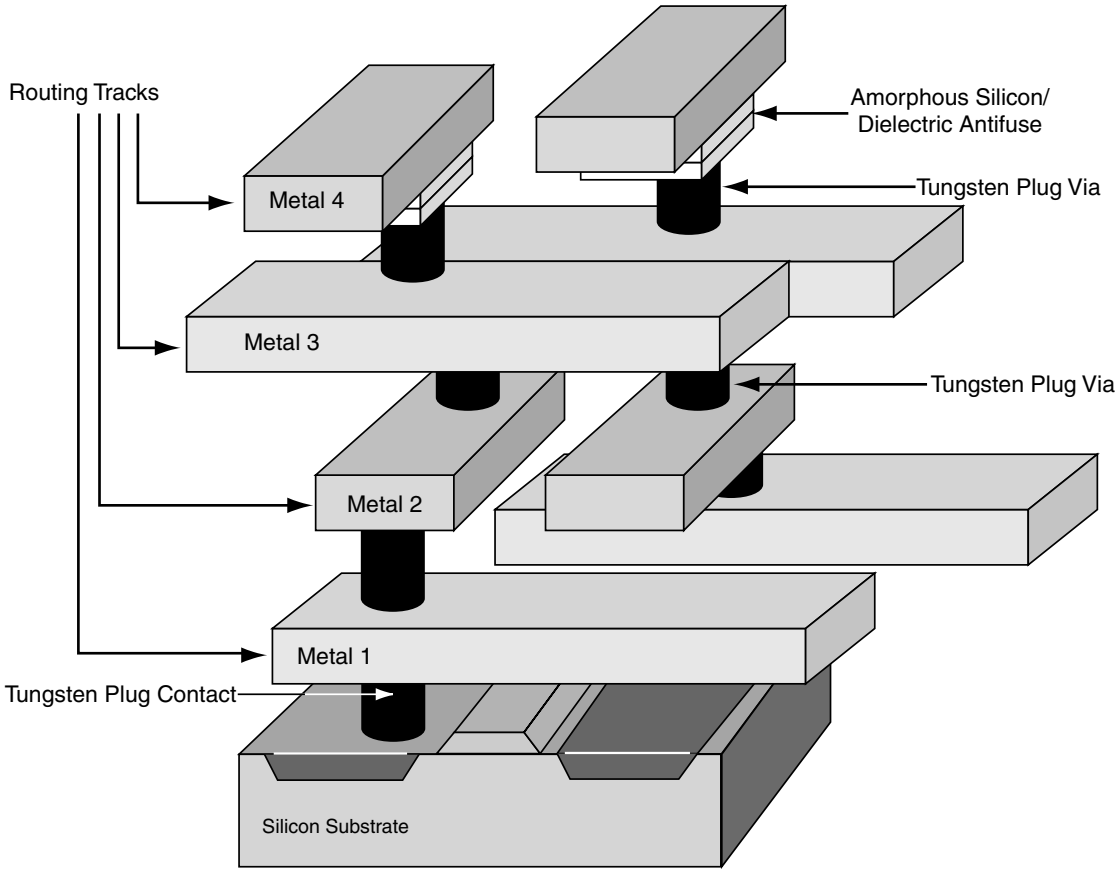

Figure 3 • *Cross Section of a Programmer Antifuse*

Direct Physical Attack of Flash-based FPGAS

As with antifuse-based FPGAs, Flash-based FPGAs utilize switches to connect and disconnect intersecting metal lines. A single-floating gate is charged or discharged to set the state of a switch that connects two metal lines. Since there is no physical change in the programming device or switch device, there is nothing to detect by material analysis.; There is only a change in the number of electrons on the floating gates. Because there is no observable change in the Flash-based switch when programmed, a Flash-based FPGA is extremely difficult to reverse engineer using any form of invasive survey to determine the state of each switch.

Fundamentally, the Flash architecture also offers higher levels of security when compared to other reprogrammable FPGAs. Because the Flash architecture does not require an external configuration device after being programmed, Flash-based ProASIC^{PLUS} devices do not rely on an external bitstream. Programming can easily be done in a secure environment to offer a nonvolatile, single-chip solution that can be incorporated into system-level designs with high levels of danger from reverse engineering.

6. Other Methods of Attack

It has been shown that ASICs can be physically attacked in a straightforward manner that relies on the visibility of connections or vias between metal layers. It has also been proven that such a direct attack is extremely difficult, if not impossible, against antifuse or Flash-based FPGAs due to the difficulty in physically observing the state of millions of switches. Several other advanced methods of attack have been developed that may be employed against any technology but with considerable expense and/or difficulty:

- IBM developed a very advanced technology that allows one to actually look at the logic states of the metal lines.[17] This is accomplished by placing a crystal of lithium niobate over the feature whose voltage is to be monitored. The refractive index of this substance varies with the applied electric field, and the potential of the underlying metal can be read out using an ultraviolet laser beam passed through the crystal at grazing incidence. This technique allows a 5V signal of up to 25 MHz to be read.
- Another technique (recently declassified) developed at Sandia Laboratories utilizes an infrared laser to which the silicon is transparent. It is then possible to shine the laser from the backside to induce photocurrents that are affected by the logic state and thus determine the logic state of a specific transistor.[18] (Inspired by this methodology, other researches are now attempting to duplicate these results using controlled electromagnetic fields to achieve the same results).

Finally, both antifuse and Flash-based devices are architecturally designed to prevent attack on a programmed device with a programmer or by other electronic means. Typically, both contain circuitry to lock the device by disabling the programming and readback capabilities after configuration. Care can be taken in the design to make the locking circuitry difficult to defeat through either electronic or direct physical attack. In antifuse FPGAs, as fuses are programmed, it becomes impossible to uniquely address previously programmed fuses, making programming essentially a one-way function. Therefore, the architecture of the antifuse-based devices makes electronic readback impossible, even if the locking mechanism is not used. Flash is also highly resistant to invasive attacks. Decapping and stripping only reveal the structure of the device, not the actual content of the Flash cell, as no physical change occurs in the device. Flash also enables designers to dispense with extra batteries and vulnerable configuration devices that may introduce multiple points of weakness into a system.

---

17. Wiesenfeld, J.M., "Electro-optic Sampling of High Speed Devices and Integrated Circuits," IBM Journal of Research and Development (vol. 34, no. 2/3) (New York: International Machines Business Corporation: 1991): 141-161.

18. Ajluni, C., "Two New Imaging Techniques Promise to Improve IC Defect Identification," Electronic Design (vol. 43 no. 14) (10 July 1995: 37-38).

7. Preventing Design Theft

As corporations continually expand their mission-critical enterprises, security is becoming increasingly vital in preventing corruption and intrusion. Without precautions, corporations could experience major security breaches, resulting in serious damages and losses. Maintaining a high level of security for your systems, products, and designs requires a continuous cycle of efforts. Establishing a security policy that defines security goals is a critical first step.[19] When planning a silicon design security program, consider the following:

- Take steps at the designer level to ensure designs do not leave with an employee but remain company property
- If employees are allowed to work remotely, ensure design work is done using a secure centrally accessed server that also serves as a depository for any relevant EDA tools
- Implement procedures to track IP and programming codes as necessary to limit exposure of your designs in the manufacturing channel. Limit access to designs whenever possible
- Use design techniques that prevent a simple I/O scan from revealing the circuit structure
- Use trusted silicon vendors to implement the design (all Actel in-house programming is done at the corporate headquarters in our Sunnyvale factory to ensure the security of our customers designs)
- Utilize the most secure technology available to minimize potential attacks at the physical level
- Assess your security regularly

If security is an important parameter, be sure to select a secure FPGA solution for your next design. It is much cheaper to protect your design up front than to try and recover losses through the courts.

8. Unique Business Models with Secure Nonvolatile FPGAs

As FPGAs are used in more and more diverse applications, FPGA security becomes a more complex topic. Trust relationships between vendors, customers, regulators, and competitors can be extremely involved and contested. Intellectual property is at risk from a variety of sources: external invasive type attacks, internal malicious attacks, accidental exposure caused by an incompetent employee and a host of other possibilities. The last decade has seen a dramatic shift in the semiconductor industry from a few horizontally integrated companies to dozens of fabless semiconductor companies using the services of silicon foundries.

The next big shift expected was continued vertical fragmentation with hundreds of design services and intellectual property companies providing their services to system-level architects and integrators. That expectation has failed to materialize, and the design services and intellectual property providers are still struggling with how to capture their share of the value chain.

Secure nonvolatile FPGAs offer solutions to overcome two large barriers in this struggle. The first barrier is simply security. The risk that the design services company has by losing their intellectual property sets in motion legal and administrative activities and costs that, in the end, prove too high to justify all but the largest engagements. The industry has spent great effort developing design encryption schemes that protect the design at the netlist level, but it is still exposed to a trivial cloning attack if implemented in an SRAM FPGA. In contrast, a nonvolatile antifuse or Flash-based FPGA prevents such an attack and offers better security than an ASIC implementation.

The second barrier to growth is that the design service companies lack a reliable mechanism to charge a royalty for their services. All the money must be made up-front in licensing fees that, again, can only be justified in the largest engagements. With secure nonvolatile FPGA technologies, an IP developer can

19. *Cisco Systems Inc., "A Beginner's Guide to Network Security 2001 Cisco Systems," [online] (Cisco Systems Inc., 2001 [cited 12 August 2002]); available from http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf.*

become a virtual ASIC company and ship pre-programmed FPGAs with only a nominal mark-up or royalty charge above the cost of the unprogrammed FPGA. Antifuse FPGA vendors could conceivably serve as a type of virtual foundry for the designers. This would effectively eliminate operational costs for the design services companies while allowing a per-unit royalty based scheme without any of the security risks associated with SRAM-based products.

9. Conclusions

As the complexity of FPGAs continues to increase, so does the value of the designs they hold. IP theft, and specifically the cloning of component and system-level designs, is one of the largest economic threats in modern global business models employed today. SRAM FPGAs are typically considered susceptible to a Level 1 attack and consistently prove inadequate for providing effective design security. On the other hand, nonvolatile Flash and antifuse FPGAs are even more secure against attack than the ASIC technologies they are often targeted to replace.

As a result, assessment of your particular security requirements often comes down to the value of your IP and the potential risk of having your design compromised. While it may seem inherently easy to recognize that security for the launch control on a nuclear missile is more critical than a small CPLD design in a video game cartridge, all IP has value, and there are often significant repercussions should it be compromised. In order to off set the potential damages of IP theft, it is recommended that designers select a nonvolatile Flash or antifuse-based FPGA, which will have minimum impact on total system cost while providing higher levels of overall design security.

10. Bibliography

Abraham, D.G., G.M. Dolan, G.P. Double, and J.V. Stevens. 1991. Transaction Security System. *IBM Systems Journal* vol. 30 no. 2 New York: International Machines Business Corporation: 206-229.

Ajluni, C. 1995 Two New Imaging Techniques Promise to Improve IC Defect Identification. *Electronic Design* vol. 43 no. 14 (10 July 1995): 37-38.

Algotronics. Secure Configuration of Field Programmable Gate Arrays.

Anderson, Ross J. 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: John Wiley and Sons.

Blythe, S., B. Fraboni, S. Lall, H. Ahmed, U. de Riu. 1993. Layout Reconstruction of Complex Silicon Chips. *IEEE Journal of Solid-State Circuits* vol. 28 no. 2 (Feb. 1993): 138-145.

Chipworks. 2002. [cited 12 August 2002] Available from World Wide Web: http://www.chipworks.com/.

Cisco Systems Inc. 2001. A Beginner's Guide to Network Security 2001 Cisco Systems [online]. Cisco Systems Inc. [cited 12 August 2002]. Available from World Wide Web: http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf.

Dipert, Brian. 2002. Cunning Circuits Confound Crooks. *EDN* (12 October 2000): 103-112. [cited 12 August 2002]. http://www.e-insite.net/ednmag/contents/images/21df2.pdf.

FBI Congressional Statement. 2000. Statement for the Record of Guadalupe Gonzalez Special Agent In Charge, Phoenix Field Division Federal Bureau of Investigation on Cybercrime. [online]. Washington, D.C.: FBI. [cited 12 August 2002] Available from World Wide Web: http://www.fbi.gov/congress/congress00/gonza042100.htm.

Federal Bureau of Investigation the Financial Institution Fraud Unit. 2002. Financial Institution Fraud. In A*bout Intellectual Property Crimes* [online]. Washington D.C.: FBI, [cited 12 August 2002] Available from World Wide Web: http://www.fbi.gov/hq/cid/fc/fifu/about/about_ipc.htm.

Hadzic, I., S.K. Udani, and J.M. Smith. 2002. FPGA Viruses. [online]. Philadelphia, PA: University of Pennsylvania, [cited 2002 August 12]. Available from World Wide Web: http://www.cis.upenn.edu/~boosters/fpgavirus.ps.

Kean, T. 2002. Crypto Rights Management of FPGA Intellectual Property Cores FPGA. [online] [cited 12 August 2002] Available from World Wide Web: http://www.ecs.umass.edu/ece/fpga2002/.

Microsoft MSDN Library. 2002. Preventing Denial of Service Attacks. [online] Microsoft Corporation, 2002 [cited 12 August 2002]. Available from World Wide Web: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securecode_vyyk.asp.

Shankar, Nitin K. 2002. Can Reverse Engineering Answer your Design and Prototyping Needs? [online] India: Brown and Sharp. [cited 12 August 2002] Available from World Wide Web: http://www.brownandsharpe.com/mfg/mfg7/mfg7ar10.html.

Tecnocad S.r.1. 1998. Keylock 2: An Electronic Key for Software Protection is Improved by FPGA Technology Allowing New Features. [online] Italy: Tecnocad S.r.1. [cited 12 August 2002] Available from World Wide Web: at http://www.fuse-network.com/fuse/demonstration/30/24566/index.html.

Wiesenfeld, J.M. 1991. Electro-optic Sampling of High Speed Devices and Integrated Circuits. *IBM Journal of Research and Development*. vol. 34 no. 2/3 New York: International Machines Business Corporation: 141-161.

http://www.actel.com

Actel Europe Ltd.
Maxfli Court, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Tel: +44 (0)1276 401450
Fax: +44 (0)1276 401490

Actel Corporation
955 East Arques Avenue
Sunnyvale, California 94086
USA
Tel: (408) 739-1010
Fax: (408) 739-1540

Actel Asia-Pacific
EXOS Ebisu Bldg. 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150 Japan
Tel: +81 03-3445-7671
Fax: +81 03-3445-7668

5172163-1/8.02