UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea in Ingegneria Elettronica

Utilizzo degli FPGA in ambito cybersecurity per creare moduli HW dedicati

Relatore:
Prof. Daniele Vogrig

Laureando:
Martarello Luca
1216279

Anno Accademico 2022/2023

28/09/2023

Indice

ABSTRACT

Nell'ambito cybersecurity, spesso si pone maggiore attenzione agli aspetti software ma un'adeguata sicurezza di un dispositivo dipende anche dalla scelta dell'hardware. Questa tesi fornisce una panoramica sulle FPGA (Field Programmable Gate Arrays) e il loro ruolo nella sicurezza informatica.

L'elaborato inizia con un'introduzione a questi dispositivi, presentando le loro caratteristiche principali e il metodo di programmazione. Successivamente, vengono esposte le vulnerabilità più comuni delle FPGA: vengono illustrate diverse tipologie di attacchi, accompagnate da possibili soluzioni per garantire la sicurezza e prevenire minacce esterne che potrebbero compromettere il funzionamento delle schede FPGA. Una volta compreso come proteggere questi dispositivi da minacce esterne, la tesi si concentra sull'utilizzo di FPGA, SoC e moduli di sicurezza hardware (HSM) in ambito di cybersecurity.

Infine viene esposto un interessante esempio concreto di utilizzo di questi dispositivi.

L'obiettivo di questo elaborato è di presentare come le caratteristiche delle FPGA vengano sfruttate nell'ambito della sicurezza informatica per avere una protezione che non riguardi solo il software ma anche la parte hardware.

1. FPGA

Gli FPGA, acronimo di Field Programmable Gate Arrays, sono dispositivi logici programmabili proposti per la prima volta da Xilinx nel 1984.

Questi dispositivi sono composti da un insieme di blocchi logici configurabili, Configurable Logic Block (CLB), in cui le funzioni svolte vengono definite dopo la fabbricazione, quindi dall'utente finale non dal produttore, da questo il nome programmazione "sul campo"; inoltre possono essere riconfigurate anche dopo la prima programmazione.

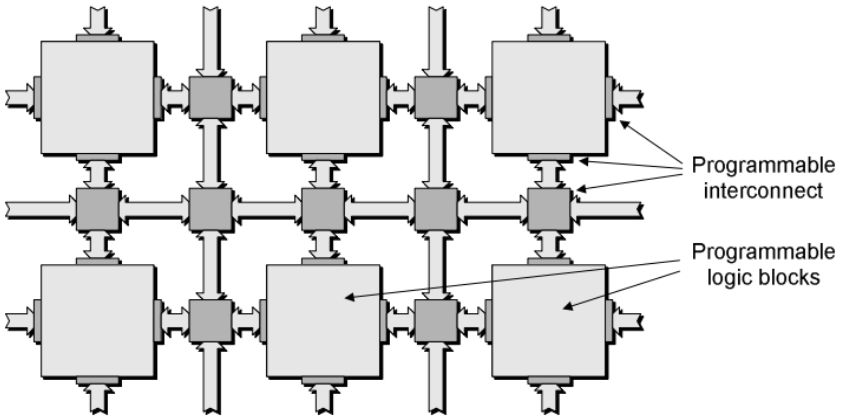

Figura 1: Configurable Logic Block (CLB) [1]

Questi blocchi riescono a realizzare qualsiasi funzione combinatoria grazie alle LUT (look-up table) accompagnata solitamente da un registro dove salvare il risultato di quest'ultima. Questi blocchi logici sono collegati tra loro da interconnessioni programmabili consentendo di realizzare funzioni complesse in modo più semplice e conveniente rispetto ai microprocessori.

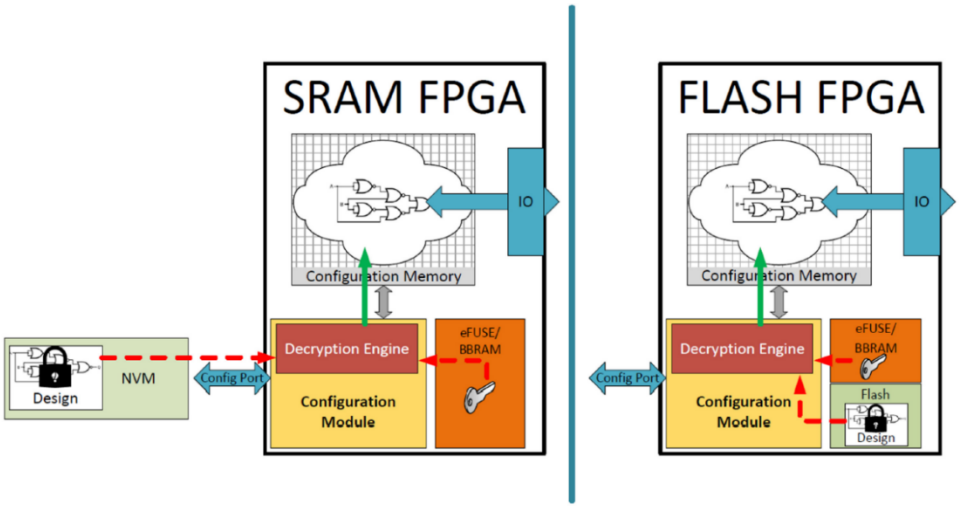

Figura 2 : FPGA SRAM e FLASH [2]

Oggi sul mercato esistono varie tecnologie di FPGA. In figura 2 possiamo vedere due tipologie di FPGA: basate su memoria SRAM e basate su memoria FLASH.

Un aspetto importante delle FPGA è che possono essere riconfigurate anche dopo la prima programmazione.

Gli FPGA basati su SRAM necessitano una memoria non volatile esterna per mantenere le specifiche di configurazione quando il dispositivo è spento, a causa della volatilità della SRAM. Tuttavia, in alcune circostanze, board molto complesse possono prevedere un meccanismo di boot che, attraverso un microcontrollore, riprogramma le FPGA ad ogni avvio, senza richiedere l'utilizzo di una memoria non volatile.

I dispositivi basati su memoria FLASH mantengono il loro design all'interno della memoria flash integrata fino ad una nuova riprogrammazione.

Un'altra variante di dispositivi FPGA in commercio riguarda le FPGA ad antifusibile. La configurazione dei circuiti viene stabilita attraverso dei collegamenti fisici, detti fusibili. Durante la programmazione alcuni fusibili vengono bruciati per creare collegamenti permanenti tra i componenti interni della FPGA. In questi dispositivi i fusibili non possono essere ripristinati o sostituiti, rendendo il design del dispositivo permanente.

Il mercato, secondo uno studio di mercato svolto nel 2019 da Gartner [2], è dominato da 4 produttori principali: i produttori principali sono AMD-Xilinx con il 51,1% e Intel con il 35,8% e producono FPGA basate su SRAM, mentre Microsemi con il 6,6% e Lattice con il 5,0% producono dispositivi FPGA basati su flash. Quindi nel mercato attuale i prodotti basati su SRAM sono i più comuni e utilizzati, mentre le FPGA a memoria FLASH e ad antifusibile sono impiegate in applicazioni con specifiche richieste di configurazione e nella sicurezza.

L'utilizzo dei diversi tipi di FPGA dipende dal tipo di esigenze richieste dal progetto.

Grazie alla loro programmabilità e alla facilità di interfacciamento con l'esterno tramite i blocchi di input/output per comunicare con altri chip o per segnali esterni, gli FPGA sono utilizzati in molti settori come: nell'automazione industriale, delle telecomunicazioni, dell'elettronica di consumo, dell'informatica ad alte prestazioni e della ricerca scientifica. Vengono utilizzati per l'elaborazione di segnali digitali, la comunicazione di rete, l'elaborazione di immagini, la crittografia e la sicurezza informatica, l'intelligenza artificiale, il calcolo ad alte prestazioni e altro ancora.

1.1 Progettazione

La programmazione degli FPGA si basa su strumenti di sviluppo software (EDA, Electronic Design Automation) che consentono di eseguire due operazioni principali la sintesi e la simulazione.
La sintesi è il processo di traduzione delle specifiche di progetto in una implementazione reale, mentre la simulazione serve a verificare che l'implementazione eseguita segua le specifiche imposte.

Le specifiche possono essere rappresentate attraverso il disegno dello schema progettuale oppure in forma testuale utilizzando un linguaggio di descrizione hardware ad alto livello (HDL), come VHDL o Verilog;

Un HDL non è uno strumento per progettare circuiti elettronici ma è un linguaggio hardware utilizzato per descrivere la struttura e il comportamento di progetti già ideati.

Si distinguono dai linguaggi di programmazione tradizionali anche perché non hanno il concetto di esecuzione sequenziale delle istruzioni del codice, ma descrivono il comportamento simultaneo dei componenti hardware.

Dopo la **sintesi**, il design viene **mappato** nella FPGA, questo processo assegna le diverse parti del design come funzioni logiche e registri ai blocchi logici configurabili CLB, tenendo conto delle risorse disponibili e cercando di ottimizzare il più possibile il loro utilizzo.

Mappato il design, tocca alla fase chiamata **place-and-route**. Questo processo determina la posizione fisica delle risorse interne stabilendone le interconnessioni tra essere, ottimizzandole per ridurre i ritardi e massimizzare le prestazioni.

Dopo il place-and-route, viene **generato il bitstream**, utilizzando strumenti di sviluppo forniti dai produttori.

Successivamente viene **caricato il bitstream** nella FPGA per configurarla, rendendola pronta per eseguire il design programmato.

La possibilità di modificare il comportamento della FPGA senza modificare l'hardware è uno dei principali vantaggi di questi dispositivi.

2. VULNERABILITA’

In questa sezione presenteremo le vulnerabilità delle FPGA.

Queste vulnerabilità includono potenziali attacchi alla catena di fornitura, inserimento di backdoor nel design o nel bitstream, attacchi di tipo side-channel, iniezione di guasti e il rischio di reverse engineering.

La comprensione di queste vulnerabilità è fondamentale per proteggere l’integrità e la sicurezza delle FPGA e prevenire potenziali minacce alla loro funzionalità.

Nell’ambito della cybersecurity, gli attacchi vengono raggruppati in due tipologie: attacchi attivi e attacchi passivi. Entrambi i tipi di attacchi hanno come obiettivo minare la riservatezza, l’integrità e la disponibilità di un dispositivo.

In particolare, gli attacchi **attivi** cercano di compromettere un dispositivo perturbandone la normale funzione creando dei danni, nel tentativo di scoprire informazioni riservate sul prodotto attaccato.

Al contrario, gli attacchi **passivi** cercano di estrarre informazioni da un prodotto senza interagire con la sua normale operazione.

Sfruttando attacchi attivi e passivi, gli attaccanti maligni possono rappresentare varie minacce per i dispositivi FPGA. La scelta dell'attacco dipende spesso dal tempo a disposizione, denaro e accessibilità fisica al dispositivo.

In questa sezione tratteremo le tipologie di attacco più frequenti:

- Cloning attack
- Reverse engineering
- Hardware Trojan
- Side-channel attack

2.1 Cloning attack

L'obiettivo di un attacco di clonazione è copiare il design della FPGA. Utilizzando il bitstream scoperto di un dispositivo uguale e gli hacker possono poi venderlo come proprio.

Questo attacco può riguardare l'intero design del prodotto o anche una parte di questo.

La clonazione è considerata la vulnerabilità più comune, per combatterla esistono diverse tecniche di difesa:

2.1.1. Identificazione Friend o Foe

È una tecnica semplice per evitare la clonazione del bitstream di configurazione della FPGA. Il funzionamento si basa sull'utilizzo di un dispositivo di sicurezza esterno utilizzato per memorizzare una chiave univoca diversa per ogni dispositivo FPGA.

In pratica, la chiave conosciuta solo da questo dispositivo viene richiesta nel flusso di bit della FPGA e quest'ultima verifica l'esistenza effettiva di questo dispositivo esterno. Se viene indentificato come AMICO/FRIEND l'FPGA continua a funzionare, al contrario se viene riconosciuto come NEMICO/FOE l'FPGA smette di funzionare.

2.1.2. Crittografia del bitstream

La crittografia del bitstream è una delle tecniche di protezione IP più diffuse contro la clonazione della configurazione delle FPGA.

Il metodo di base consiste nel crittografare i file bitstream di configurazione FPGA mediante lo strumento EDA e quindi decifrarli utilizzando algoritmi di decrittazione sicura standardizzati con una chiave non volatile memorizzata nella memoria FPGA.

La protezione del file di configurazione FPGA dipende interamente dai fornitori di FPGA.

2.1.3. PUF

Acronimo di Physically Unclonable Function, è un componente hardware che sfrutta le variazioni fisiche interne di una FPGA per generare una risposta univoca impossibile da clonare. È noto che la tensione di soglia e lo spessore dell'ossido di gate su ciascuna porta logica potrebbero non essere gli stessi, il che significa che i chip costruiti nelle stesse condizioni saranno diversi in termini di metriche prestazionali come ritardo e potenza a causa di questa

variazione di fabbricazione. Sebbene la variazione non sia sufficiente per influenzare le funzionalità del circuito, può essere utilizzata per distinguere i chip.

Esistono tre principali PUF definiti dalle caratteristiche fisiche che li generano. Sono PUF elettronici analogici, PUF basati sulla memoria e PUF basati sul ritardo. Prenderemo in considerazione un tipico PUF basato sul ritardo denominato Ring Oscillator (RO) PUF, mostrato in figura.

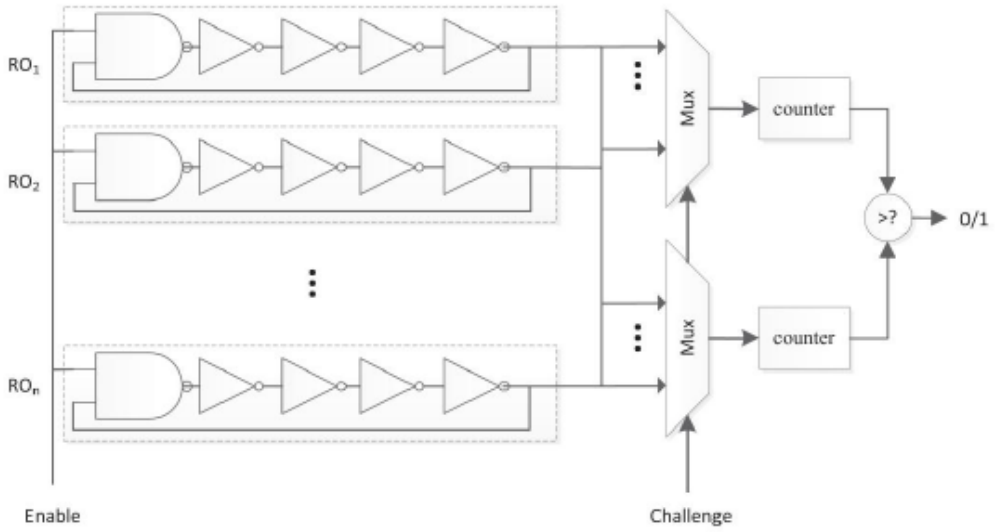

Figura 3: Struttura di PUF Ring Oscillator (RO) [3]

Il RO PUF si basa sulle variazioni nelle frequenze di oscillazione dei Ring Oscillator per generare una risposta unica.

La struttura è formata da un insieme di Ring Oscillator ognuno composto da un anello di porte logiche (in questo caso inverter) collegate in un loop che oscilla con una particolare frequenza.

La frequenza dipende dal ritardo di ciascuna porta logica e dai collegamenti, impossibile da conoscere a causa del processo di produzione e di altri fattori incerti.

La forma più semplice di PUF genera l'uscita logico-0 o logico-1 confrontando le frequenze dei circuiti oscillatori con multiplexer.

A causa dell'unicità e della non clonabilità, il PUF ha un ampio utilizzo nell'area della sicurezza hardware, come protezione IP, generazione di chiavi, condivisione di chiavi e autenticazione a due fattori. Inoltre, PUF può essere applicato anche nell'area della sicurezza del software.

2.2 Reverse engineering

Il reverse engineering è un processo di analisi di un dispositivo con lo scopo di identificare i dettagli della sua progettazione. Viene svolto per diversi motivi, come studiare un prodotto concorrente, analizzare la sicurezza o recuperare le informazioni di un dispositivo ormai obsoleto e privo di documentazione.

Il reverse engineering viene utilizzato in modo improprio da produttori o individui con intenzioni maligne per rubare o clonare un dispositivo FPGA.

In particolare per le FPGA il processo di reverse engineering richiede due passaggi principali: ottenere il file di bitstream non crittografato e successivamente decodificarlo.

Per prima cosa si deve ottenere il file del bitstream.

L'FPGA basato su SRAM perderà i dati quando si spegne. Pertanto, l'FPGA di solito utilizza memorie non volatili esterne (come la memoria flash) per archiviare i file di bitstream di configurazione e inizializzare la SRAM.

La separazione del file bitstream e del chip FPGA semplifica la clonazione del bitstream perché potrebbe venire monitorata la comunicazione tra l'FPGA e la memoria flash all'avvio del sistema.

Per decodificare i bitstream in netlist a livello di gate, dobbiamo prima conoscere la struttura del file bitstream, solitamente fornita dai fornitori di FPGA.

In questo passaggio si mira a identificare la relazione tra il file di bitstream e la netlist a livello di gate.

Un metodo basato sulle immagini interne del dispositivo può fornire immagini di ogni strato del chip. Le immagini vengono scattate da un microscopio elettronico a scansione o da un microscopio elettronico a trasmissione e, infine, lo strumento EDA viene utilizzato per gestire le immagini per generare la netlist a livello di gate.

Per prevenire il reverse engineering ci sono tre tecniche principali: il camuffamento, l’occultamento e l’offuscamento.

2.2.1. Camuffamento

L'idea chiave è che diverse unità logiche standard verranno riprogettate nella stessa architettura fisica e alcune unità logiche inutili verranno aggiunte in alcune posizioni vuote.

Ad esempio, come mostrato nella Figura 4 (a), nel circuito semplice, G1 e G4 sono sostituiti da porte camuffate e il tipo di porta non può essere riconosciuto.

Tuttavia, questa tecnica aumenta notevolmente la complessità della progettazione, inoltre, le porte mimetizzate e le unità logiche inutili aggiunte in posizioni vuote aumenteranno notevolmente il sovraccarico di risorse della progettazione di circuiti integrati.

.

2.2.2. Offuscamento

L'offuscamento consiste nel nascondere la funzionalità di un progetto inserendo ulteriori porte logiche combinatorie o stati FSM ridondanti. Senza la chiave corretta, il sistema non funzionerà correttamente.

Come mostrato in Figura 4(b), le porte logiche G1(XNOR) e G4(XOR) sono inserite nel circuito e controllate dai controlli K_1 e K_2. Pertanto, senza i corretti K_1 e K_2, il circuito non svolge le funzioni logiche corrette.

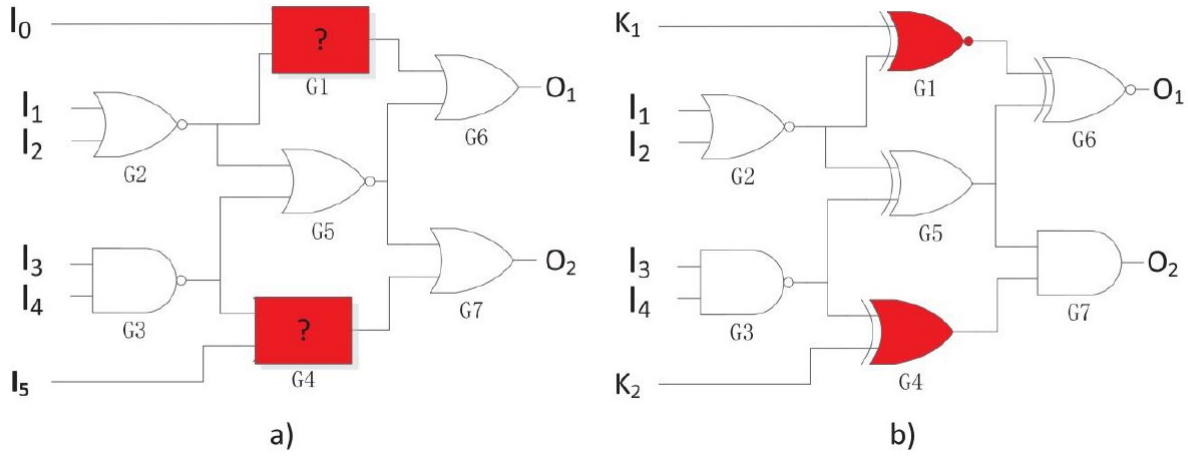

Figura 4: Esempi di Camuffamento (a) e Offuscamento (b) [3]

2.2.3. Occultamento

La tecnica di occultamento si basa sulla divisione del bitstream: una parte di bitstream di configurazione (ad es. core IP) viene archiviato nella memoria flash dell'FPGA, mentre altre parti di bitstream di configurazione non critiche vengono archiviate nella memoria esterna. In questo modo, solo informazioni parziali inutili sulla relazione di mappatura FPGA verranno divulgate agli intercettatori, il che aumenta significativamente la difficoltà del reverse engineering del bitstream.

Queste tecniche di protezione vengono applicate nelle FPGA a memoria SRAM perché l'FPGA con memoria flash e l'FPGA antifusibile non necessitano di memoria di configurazione esterna; pertanto, il download di bitstream dall'esterno non è necessario all'avvio del sistema. Il reverse engineering della memoria flash e della memoria antifusibile richiede attrezzature specifiche, quindi è difficile leggere il contenuto della memoria.

2.3 Hardware trojan

Un hardware trojan è una minaccia alla sicurezza viene inserito un circuito dannoso all'interno del design della FPGA, con l'obiettivo di compromettere il normale funzionamento o rubare preziose informazioni riguardanti la progettazione della FPGA.

Con la popolarità dell'esternalizzazione della produzione dei circuiti integrati e del riutilizzo dell'IP, c'è la possibilità che la sicurezza venga compromessa con l'implementazione di circuiti dannosi nell'hardware [3].

Un tipico scopo di queste minacce è l'invecchiamento più veloce del dispositivo.

Bisogna dire però che l'FPGA fornisce autonomamente una protezione contro i trojan hardware poiché il progettista configura il dispositivo in modo tale che certe informazioni non siano disponibili per gli esterni.

Il modo migliore per proteggersi è mettere in atto controlli di autenticazione e integrità utilizzando chiavi segrete per garantire che non vengano apportate modifiche al circuito. Una recente tecnica ha dimostrato di poter rilevare questi Trojan in base ai valori di temperatura e tensione ottenuti da diversi benchmark standard dell'algoritmo di crittografia.

2.4 Side-channel attack

Questo tipo di attacco sfrutta le grandezze misurabili dal circuito, queste quantità misurate possono fornire informazioni sul design del circuito interno.

Questi attacchi per esempio analizzano la potenza, la temporizzazione o l'emanazione elettromagnetica.

Monitorando la corrente assorbita dai pin di alimentazione del circuito possiamo misurare la **potenza** statica e dinamica.

La potenza statica è la potenza dissipata dal dispositivo anche in assenza di commutazioni, dovuta principalmente alle correnti di perdita dei componenti reali; la potenza dinamica o di commutazione, invece, è la potenza generata quando lo stato di una porta passa da un valore a quello successivo; Queste potenze ci posso fornire informazioni sul tipo di gate e sulle operazioni eseguite durante l'esecuzione di operazioni crittografiche.

Analizzando la **temporizzazione** si è in grado di capire la tipologia del gate e i valori segreti che vengono elaborati dalle porte. Per contrastare queste misure i produttori possono utilizzare due contromisure efficaci:

1) la randomizzazione, in modo che l'impatto di un calcolo non possa essere facilmente distinto tra le molte operazioni

2) l'equalizzazione, in modo tale che tutti i calcoli consumino la stessa quantità di energia.

Un'altra analisi utile per rubare informazioni dal circuito riguarda lo studio del **campo elettromagnetico** generato dal chip.

Durante lo svolgimento dei calcoli della FPGA il movimento degli elettroni genera un campo elettromagnetico che può essere misurato esternamente posizionando le antenne all'esterno del chip.

Le contromisure per queste tipologie di attacco sono basate principalmente sul disturbo del campo EM modificando le proprietà del dispositivo.

Il vantaggio degli attacchi side-channel è che possono sfruttare i dati accessibili senza lasciare alcuna traccia; infatti, rappresentano la principale minaccia per gli attuali dispositivi di cifratura.

L'attacco side-channel più efficace e invasivo è chiamato **Fault Injection**. Sfrutta il glitch di tensione, alterando il clock e la tensione di alimentazione per iniettare guasti che disturberanno

il normale funzionamento del dispositivo e aiuteranno a scoprire informazione sul chip sotto attacco.

Un aspetto importante per questi attacchi è che combinando più tipologie diverse di attacchi side-channel si può essere in grado di attaccare il dispositivo in maniera più potente e rubare informazioni più complete possibili.

3. CYBERSECURITY

3.1 Sicurezza a più livelli

Le minacce informatiche sono in continua evoluzione, con conseguenze spesso gravi. Molte aziende investono in hacking etico o in "test di penetrazione" per individuare falle nei propri dispositivi, ma purtroppo non esiste una procedura che garantisca piena sicurezza sotto ogni aspetto.

L'approccio più efficace è la sicurezza a più livelli, una strategia basata su diversi livelli di sicurezza, per garantire che ogni controllo difenda un'area specifica vulnerabile alle minacce esterne. I livelli di sicurezza sono Hardware, Design e Dati.

Figura 5: Sicurezza a più livelli [5]

La **sicurezza dell'Hardwa**re riveste un ruolo fondamentale, richiedendo una selezione accurata dell'hardware adatto alle diverse tipologie di applicazioni, nonché la garanzia da parte del produttore che il prodotto fornito sul mercato sia stato realizzato con una produzione crittograficamente sicura.

La **sicurezza del design** si basa sull'hardware, fornendo la sicurezza contro gli attacchi fisici e garantendo la riservatezza e autenticità al progetto. In caso di un tentativo di manomissione, i dispositivi devono essere in grado di individuare l'accesso non autorizzato e resettare a zero tutti i valori, preservando l'integrità del sistema.

L'ultimo aspetto trattato con questo approccio riguarda la **sicurezza dei dati,** che può essere suddivisa in due categorie in base alla posizione dei dati: i dati in trasmissione e i dati memorizzati sul dispositivo.

Le varie reti o cloud utilizzati per la trasmissione di dati hanno dei protocolli di sicurezza che forniscono già protezione a questi dati, riducendo la responsabilità dell'utente. Invece, i dati memorizzati nel dispositivo, compresa la parte software, richiedono protezione per garantire la riservatezza e l'integrità delle operazioni.

In cybersecurity, in particolare per questa strategia, le FPGA sono molto utili per i primi due livelli di sicurezza, Hardware e Design, grazie alla loro **resistenza agli attacchi informatici**, come visto nel capitolo precedente.

3.2 FPGA

In cybersecurity le FPGA giocano un ruolo fondamentale per le loro caratteristiche. La loro **flessibilità** permette agli esperti di sicurezza informatica di adattare il dispositivo alle esigenze di sicurezza richieste, consentendo inoltre di aggiornare e modificare più volte il codice senza dover sostituire l'intero dispositivo.

La **rapida prototipazione** è un ulteriore vantaggio, in quanto essendo riprogrammabili, è possibile implementare e testare nuove configurazioni senza dover aspettare la produzione di un nuovo chip personalizzato. Questa capacità di rapida prototipazione consente di esplorare nuove soluzioni di sicurezza e di valutarne l'efficacia in modo tempestivo.

Le FPGA sono particolarmente utili nelle operazioni di crittografia, consentendo l'implementazione di funzionalità di protezione come la crittografia delle comunicazioni o la gestione sicura delle chiavi.

Vengono utilizzate anche per **accelerare operazioni crittografiche** o lunghe elaborazioni di dati. Implementando algoritmi crittografici su una FPGA, è possibile ottenere un aumento significativo delle prestazioni, ciò consente di migliorare la velocità e l'efficienza delle operazioni di crittografia, fondamentali per garantire la sicurezza delle comunicazioni e dei dati, rendendo più efficienti e veloci le operazioni di sicurezza sui dati sensibili.

Le FPGA possono essere utilizzate per implementare funzionalità **di monitoraggio e analisi** avanzate all'interno di un sistema di sicurezza. Ad esempio, è possibile utilizzare una FPGA per analizzare e filtrare il traffico di rete in tempo reale, individuare anomalie o rilevare intrusioni. La capacità di elaborazione parallela delle FPGA le rende adatte per queste applicazioni ad alta intensità computazionale.

3.3 SoC

Un ruolo significativo nel campo della cybersecurity viene svolto dagli SoC FPGA.

I SoC FPGA (System-on-chip) sono dei dispositivi che integrano nello stesso dispositivo una o più CPU insieme ad una FPGA.

La CPU si occupa del controllo e della gestione del sistema e di fornire una piattaforma software per le applicazioni, mentre la logica programmabile offre la possibilità di creare funzioni hardware personalizzate, come algoritmi crittografici, accelerazioni di operazioni o per svolgere delle funzioni di sicurezza su misura.

Le operazioni ad alta intensità computazione e le funzioni specifiche possono essere svolte dalla FPGA, togliendo alla CPU compiti pesanti per svolgere le operazioni di controllo e le operazioni di calcolo generali. Questa combinazione di tecnologie offre un sistema più performante e affidabile con basso consumo e minori dimensioni.

I SoC grazie alle loro elevate prestazioni sono molto utilizzati in ambiti come l'elettronica industriale, l'automotive, l'Internet of Things (IoT) e la sicurezza informatica. In quest'ultimo campo vengono utilizzati per proteggere le comunicazioni, le reti e gli accessi ad esse, possono integrare degli acceleratori hardware consentendo un'elaborazione sicura dei dati e infine possono venire utilizzati per implementare delle funzioni di monitoraggio della sicurezza del dispositivo rilevando in tempo reale possibili attacchi esterni.

L'approccio alla sicurezza informatica di questi dispositivi inizia dal produttore, con una gestione sicura della supply chain anche utilizzando moduli di sicurezza hardware (HSM) durante il test e il confezionamento dei wafer.

Per affrontare le minacce esterne i SoC FPGA al loro interno integrano numerosi rilevatori di manomissione, tra cui monitor di tensione, sensori di temperatura, rilevatori di glitch del clock e della frequenza di clock, rilevatore attivo JTAG e rilevatore attivo di rete a maglie

Ulteriori protezioni sono date da contromisure di cifratura con standard di crittografia avanzata come AES-256, da PUF integrati per la memorizzazione delle chiavi e da funzionalità di azzeramento per l'FPGA e per tutte le memorie sul chip.

Attraverso l'uso di SoC FPGA, è possibile creare moduli hardware dedicati sviluppati per rispondere a richieste di sicurezza su misura.

3.4 Moduli di sicurezza hardware (HSM)

Un modulo di sicurezza hardware (HSM) è un dispositivo fisico utilizzato per fornire ulteriore sicurezza a un sistema. Possono essere schede interne o dispositivi esterni in grado di collegarsi direttamente a un dispositivo o anche a server di rete.

Gli HSM rappresentano una soluzione sicura per svolgere funzioni avanzate come la gestione delle operazioni di crittografia e delle chiavi, per l'autenticazione e la firma digitale, per algoritmi di rilevamento delle intrusioni, controllo di accesso sicuro e altre operazioni di sicurezza.

Il Global Encryption Trends Study del 2021, cioè l'indagine più importante nel settore della crittografia, ha individuato i 10 casi di utilizzo dei moduli di sicurezza hardware più diffusi nel 2021. In figura sottostante troviamo i dati.

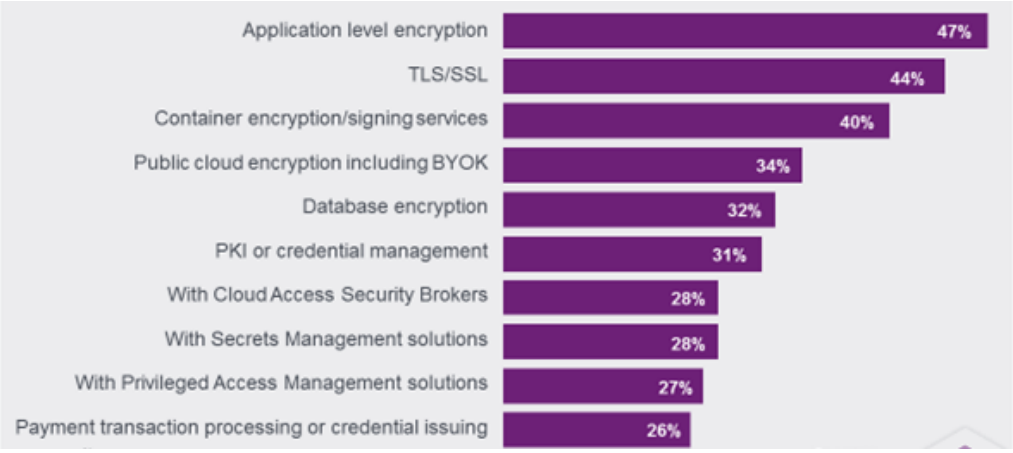

Figura 6: I primi 10 casi d'uso degli HSM nel 2021 [14]

Dalla figura si può notare che i casi di applicazione più frequenti sono le operazioni di crittografia, di firma digitale e per stabilire connessioni sicure su Internet con i protocolli TLS/SSL.

Il vantaggio per cui questi HSM sono molto utilizzati è l'accesso fisico al modulo, da parte dei criminali informatici, per riuscire ad arrivare ai dati all'interno del dispositivo. Questi moduli sono forniti con meccanismi di sicurezza come sensori di tensione o temperatura con lo scopo di individuare e bloccare eventuali minacce esterne.

I moduli HSM possono essere suddivisi in due macrogruppi: quelli per uso generico e quelli per la protezione di pagamenti e transazioni.

I primi sono utilizzati nelle applicazioni più comuni con lo scopo di rafforzare gli algoritmi di crittografia e proteggere i dati sensibili del sistema; invece, quelli che riguardano i pagamenti e le transazioni sono utilizzati da organizzazioni finanziarie o da sistemi di pagamento per proteggere i dati, le transazioni e i pagamenti elettronici da malintenzionati.

Uno dei migliori provider di HSM è Thales, azienda leader nel settore della cybersecurity, offrendo una vasta gamma di moduli altamente affidabili. I dispositivi Thales sono tra i più diffusi per i loro alti standard di sicurezza, per questo sono utilizzati da Microsoft, AWS e IBM.

Thales offre entrambe le tipologie di moduli di sicurezza hardware: gli HSM Luna generici e quelli per i pagamenti.

I moduli Luna generici sono sviluppati per ottimizzare la sicurezza delle chiavi crittografiche, custodite al sicuro all'interno dell'hardware stesso a prova di attacchi esterni. Questi moduli gestiscono le chiavi al loro interno senza mai farle uscire e comunicando con le applicazioni tramite un client sicuro garantendo massima sicurezza. La sicurezza dei dispositivi Luna è rafforzata da certificazioni come FIPS 140-2 e Common Criteria EAL 4+, da un dispositivo di autenticazione a due fattori che offre una gestione sicura anche da remoto e da una funzione di blocco per fornire massima sicurezza anche durante gli spostamenti in altri server o uffici.

I dispositivi HSM specifici per la gestione sicura dei pagamenti offrono sicurezza alle transazioni e alle applicazioni di pagamenti online garantendo ai consumatori l'integrità ad ogni operazione. Devono rispettare le norme e gli standard governativi del settore, ma Thales mira a superare queste aspettative di sicurezza, per prevenire nuove tecniche di manomissione. La loro funzione principale è proteggere le chiavi crittografiche e i dati sensibili dei consumatori con la massima sicurezza possibile, fornendo le applicazioni e l'occorrente per effettuare i pagamenti oltre che a processi di transazioni altamente sicuri.

Thales è una delle aziende ai vertici del settore dei moduli di sicurezza hardware, sviluppando dispositivi che combinano sicurezza, alte prestazioni e facilità d'uso; ma la maggior parte dei produttori di FPGA offre al mercato anche moduli di sicurezza hardware, un esempio è Xilinx con il suo Xilinx Zynq UltraScale+ MPSoC descritto alla sezione successiva.

3.5 Xilinx Zynq UltraScale+ MPSoC

Il Xilinx Zynq UltraScale+ MPSoC è un System-on-Chip (SoC) avanzato e versatile che unisce l'architettura FPGA di Xilinx con un sistema di elaborazione basato su processori ARM che include un quad-core Cortex-A53 e un real-time dual-core Cortex-R5F.

Inoltre, offre alcune interfacce di comunicazione per consentire una connettività avanzata e l'iterazione con il mondo esterno come Ethernet o USB.

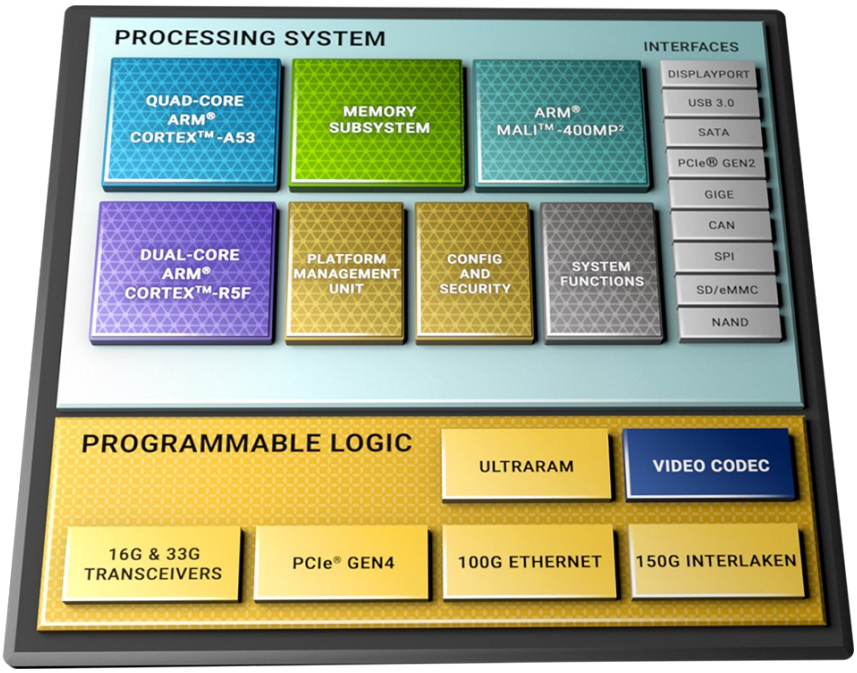

Figura 7: Architettura Zynq UltraScale+ MPSoC [6]

Questa combinazione unica di FPGA e CPU offre elevate prestazioni di elaborazione, flessibilità di configurazione e capacità di implementare funzionalità hardware personalizzate. In questo capitolo, esploreremo le caratteristiche principali del Xilinx Zynq UltraScale+ MPSoC e il suo ruolo nell'ambito della sicurezza informatica.

All'interno del Zynq UltraScale+ MPSoC, l'unità di configurazione della sicurezza (CSU) riveste il ruolo centrale nella sicurezza del sistema.

L'unita di configurazione della sicurezza (CSU) è costituita da due blocchi principali, il blocco di sicurezza del processore (SPB) e il blocco dell'interfaccia crittografica (CIB), rispettivamente illustrati a sinistra e a destra nella figura 8.

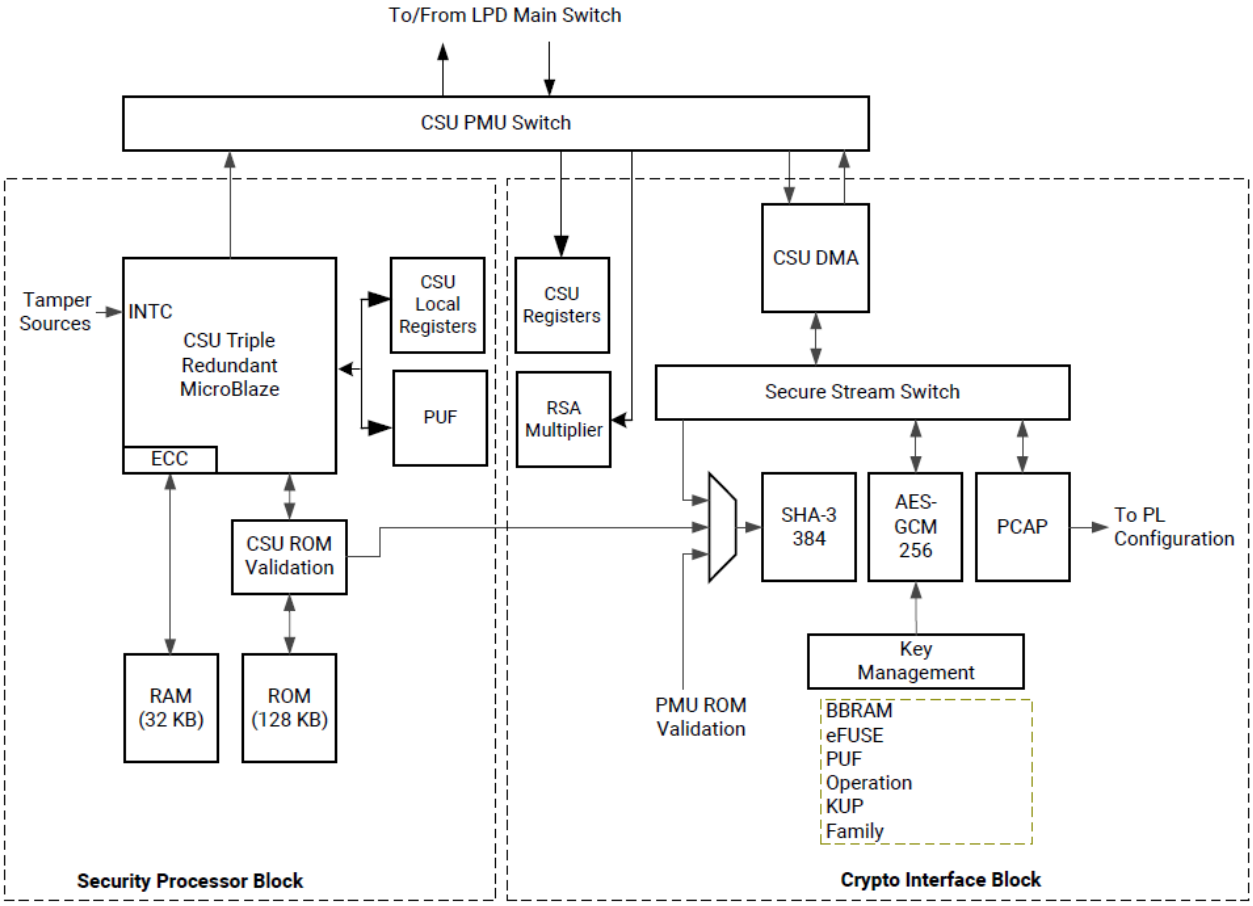

Figura 8: Unità di configurazione della sicurezza (CSU) Zynq UltraScale+ MPSoC [7]

Il blocco di sicurezza del processore (SPB) ospita alcuni componenti chiave, tra cui un processore MicroBlazer a tripla ridondanza per il controllo delle operazioni di avvio, una ROM, una piccola RAM privata, un PUF[1] e i registri necessari per il controllo.

Mentre il blocco dell'interfaccia crittografica (CIB) contiene degli elementi per supportare e accelerare le operazioni crittografiche, tra cui AES-GCM, SHA-3 e RSA, inoltre presenta l'accesso diretto alla memoria DMA e l'interfaccia della porta di accesso alla configurazione del processore (PCAP).

Il Zynq UltraScale+ MPSoC è stato ideato con funzioni incentrate nella sicurezza informatica.

[1] È un componente hardware utile per la sicurezza dei dispositivi, viene illustrato al capitolo 2.1.3.

Grazie all'integrazione del processore ARM Cortex-R5 e alla logica programmabile dell'FPGA, il dispositivo riesce a fornire un **Hardware sicuro** per eseguire operazioni crittografiche e gestire chiavi crittografiche.

L'FPGA consente inoltre di accelerare le operazioni di crittografia e decrittografia in modo efficiente e sicuro.

La combinazione dei due processori ARM, Cortex-A53 e Cortex-R5, consente una migliore gestione della sicurezza, rilevando e bloccando le minacce informatiche.

Il Zynq UltraScale+ MPSoC trova diverse applicazioni nell'ambito della cybersecurity, tra cui l'implementazione di firewall e sistemi di sicurezza di rete, la criptografia e la sicurezza dei dati, in aggiunta a sistemi di controllo sicuri.

Questo dispositivo per le funzioni di sicurezza è aiutato da alcuni moduli di sicurezza hardware, tra cui il modulo HSM IP, un dispositivo sviluppato da Secure-IC (partner Xilinx) che offre ulteriore sicurezza al Zynq UltraScale+ MPSoC sia nell'ambiente hardware che software.

Per quanto riguarda l'hardware offre autenticazione crittografica, riservatezza dei dati in transito, una gestione delle chiavi sicura, un'avanzata protezione contro gli attacchi fisici soprattutto per i Side-Channel e Fault Injection; mentre per l'ambiente software questo modulo di sicurezza hardware utilizza protocolli di comunicazione sicuri e implementa la funzione di Avvio Sicuro che garantisce l'integrità del firmware di avvio e protegge il sistema da minacce all'avvio.

Un interessante caso di utilizzo del Xilinx Zynq UltraScale+ MPSoC è nell'ambito dello sviluppo di applicazioni di sorveglianza.

Un sistema di sicurezza all'avanguardia richiede la capacità di interfacciarsi con diversi tipi di sensori, implementare tecniche di computer vision e machine learning, e garantire alta risoluzione e velocità dei fotogrammi.

Il sistema necessita di una memoria per il trasferimento delle immagini da uno stadio di elaborazione a quello successivo. L'utilizzo di una memoria condivisa da più risorse può generare un "collo di bottiglia" nell'esecuzione dell'algoritmo di elaborazione. Tuttavia, sfruttando la logica programmabile all'interno del Zynq UltraScale+ MPSoC, i progettisti possono evitare il problema del "collo di bottiglia" eseguendo le sequenze di immagini in parallelo.

Utilizzando CPU e FPGA il sistema risulta più reattivo, riconfigurabile ed ottimizzato per i consumi.
Il SoC permette una connettività universale, cioè consente di utilizzare interfacce standard come HDMI o anche di realizzare interfacce su misura; inoltre permette aggiornamenti per supportare gli ultimi standard di interfacce.

Un aspetto critico in questo sistema è la programmazione, poiché richiede la transizione dal linguaggio ad alto livello a un linguaggio di descrizione hardware come VHDL. Tuttavia, Xilinx offre strumenti e software per affrontare questo problema.

In particolare, ReVision Stack è una componente software fornita da Xilinx per semplificare lo sviluppo e l'ottimizzazione di applicazioni su piattaforme come il Zynq Ultrascale+ MPSoC.

Lo stack ReVision consente agli sviluppatori di implementare in modo semplice e rapido tecniche di computer vision e di machine learning.

Gli ingegneri con nessuna competenza in progettazione hardware possono utilizzare linguaggi ad alto livello come C/C++/OpenCL e librerie come Caffe e OpenCV per creare applicazioni dedicate su un singolo SoC o MPSoC Zynq.

Lo stack ReVision offre tutti gli elementi necessari per implementare ed eseguire gli algoritmi richiesti dai sistemi di sorveglianza ad elevate prestazioni.

Figura 9: Esempio di un sistema di sorveglianza avanzato [8]

Un sistema di sorveglianza basato su Zynq Ultrascale+ MPSoC offre alte prestazioni e una sicurezza adeguata grazie alle performance dei SoC in ambito di sicurezza contro minacce esterne.

Il Xilinx Zynq UltraScale+ MPSoC rappresenta un'importante evoluzione nell'ambito dei System-on-Chip FPGA, con le funzionalità e la capacità di personalizzazione offre interessanti opportunità nell'ambito della cybersecurity, in questo caso offre un sistema di sorveglianza ad alte prestazioni e sicuro contro le minacce esterne.

CONCLUSIONI

In un mondo sempre più interconnesso e digitalizzato, la cybersecurity riveste un ruolo cruciale. Nel corso di questo documento, si esamina in dettaglio il ruolo delle FPGA nell'ambito della sicurezza informatica.

Attraverso un'analisi delle caratteristiche, delle vulnerabilità e delle funzioni delle FPGA è emerso che questi dispositivi sono adatti a garantire sicurezza in ambito hardware.

Le FPGA, grazie alla loro flessibilità e alla capacità di personalizzazione, consentono agli esperti di sicurezza di sviluppare i dispositivi su misura per le esigenze richieste. Questi dispositivi sono molto preziosi per la loro resistenza agli attacchi informatici e la possibilità di implementare operazioni crittografiche e funzioni di monitoraggio.

I SoC FPGA, grazie all'utilizzo combinato di logica programmabile e di CPU, offrono ulteriori vantaggi come l'ottimizzazione delle prestazioni e una maggiore reattività del sistema.

Questi dispositivi sono quindi perfetti per sviluppare moduli di sicurezza hardware (HSM) per svolgere tutte le operazioni di sicurezza richieste da un sistema.

L'esempio dell'Xilinx Zynq UltraScale+ MPSoC dimostra come la combinazione tra logica programmabile e processori ARM offra alte prestazioni, flessibilità e la possibilità di implementare funzioni hardware su misura. L'unità di configurazione della sicurezza (CSU), al suo interno, rafforzata da moduli di sicurezza hardware, come HSM IP, offre una sicurezza integrata a livello hardware per proteggere il dispositivo da possibili minacce esterne. In questa tesi il Xilinx Zynq UltraScale+ MPSoC, con l'aiuto dello ReVision Stack , viene presentato per lo sviluppo di sistemi di sorveglianza, evidenziando come sia in grado di gestire algoritmi di computer vision e machine learning, offrendo alte prestazioni grazie all'utilizzo della logica programmabile che consente l'esecuzione di operazioni in parallelo.

In conclusione, le FPGA e i SoC FPGA rappresentano degli strumenti fondamentali per la cybersecurity di molti dispositivi grazie alle loro caratteristiche uniche. Tuttavia, va riconosciuto che la sicurezza informatica è una sfida in continua evoluzione. La ricerca e lo sviluppo continuo in questo campo sono essenziali per affrontare le nuove minacce e garantire la protezione efficace ai sistemi e ai dati sensibili.

Bibliografia

[1] C. Maxfield; Burlington; 2004; *Chapter 3 – The Origin of FPGAs,* in *The Design Warrior's Guide to FPGAs*; pp 68; https://blog.aku.edu.tr/ismailkoyuncu/files/2017/04/01_ebook.pdf

[2] A. Proulx; J. Chouinard; P. Fortier; A. Milled; 11 March 2023; *A survey on FPGA Cybersecurity design Strategies;* https://dl.acm.org/doi/full/10.1145/3561515

[3] J. Zhang; G. Qu; Agosto 2019; *Recent attack and defenses on FPGA-based systems*; https://www.researchgate.net/publication/334729327_Recent_Attacks_and_Defenses_on_FPGA-based_Systems

[4] M. Majzoobi; F. Koushanfar; M. Potkonjak; *FPGA-oriented Security;* http://web.cs.ucla.edu/~miodrag/papers/Majzoobi_2011.pdf

[5] P. Pickle; Elettronica-plus.it; 24 febbraio 2017*; FPGA a prova di attacchi informatici*; https://elettronica-plus.it/fpga-a-prova-di-attacchi-informatici_88644/

[6]] Xilinx Zynq™ UltraScale+™ MPSoC https://www.xilinx.com/products/silicon-devices/soc/zynq-ultrascale-mpsoc.html

[7] Zynq UltraScale+ MPSoC; WP543 (v1.0); 4 febbraio 2022, Xilinx White Paper https://www.xilinx.com/support/documents/white_papers/wp543-fips-140-3-primer.pdf

[8] N. Ni; A. Taylor; *Automazione e Strumentazione*; pag. 66, Gennaio/Febbraio 2018 *Sistemi integrati per la sorveglianza intelligente*; https://automazione-plus.it/brochure/as/1-2018/files/assets/common/downloads/publication.pdf

[9] Redazione, *Elettronica In*; 18 Marzo 2017; *Si espandono con reVISION di Xilinx le applicazioni di Machine Learning basate sulla visione;* https://ei.futuranet.it/2017/03/18/si-espandono-con-revision-di-xilinx-le-applicazioni-di-machine-learning-basate-sulla-visione/

[10] Microchip; *Secure FPGAs and SoC FPGAs*; https://www.microchip.com/en-us/products/security/secure-fpgas-and-soc-fpgas#secure-hardware

[11] Xilinx, Zynq UltraScale+ MPSoC Software Developer Guide (UG1137) https://docs.xilinx.com/r/en-US/ug1137-zynq-ultrascale-mpsoc-swdev/Security

[12] Thales; *Hardware Security Modules (HSM);* https://cpl.thalesgroup.com/it/encryption/hardware-security-modules

[13] Secure-iC; *SecuryzrTM Hardware Security Modules;* https://www.secure-ic.com/products/securyzr/root-of-trust/hardware-security-modules/

[14] Entrust; *Che cosa sono i moduli di sicurezza hardware (HSM)?;* https://www.entrust.com/it/resources/hsm/faq/what-are-hardware-security-modules

[15] SLL Top; *Hardware security Modules (HSM): cos'è e a cosa serve;* https://www.top-ssl.it/hardware-security-module-hsm-cose-e-a-cosa-serve/