La salvaguardia delle proprietà intellettuali integrate in un progetto è un aspetto che riveste un'importanza sempre maggiore. L'adozione di una tecnologia antifusibile come ViaLink di QuickLogic, oltre ad assicurare un notevole livello di sicurezza, permette di sfruttare i vantaggi tipici delle logiche programmabili: elevata velocità, flessibilità e consumi ridotti

La sicurezza nei progetti FPGA

Mehul Kochar
Application Engineering Group – QuickLogic

Durante lo sviluppo di un progetto, un elemento che va acquisendo una sempre maggiore importanza è quello della sicurezza. Il grado di vulnerabilità di un design infatti, cresce di pari passo con l'aumento dell'utilizzo di FPGA. La sempre più diffusa popolarità di questi componenti programmabili è imputabile in larga misura al fatto che la loro adozione comporta una sensibile riduzione dei tempi di sviluppo.
I design possono essere infatti programmati all'interno di un FPGA direttamente dalla scrivania del progettista e collaudati alla massima velocità prevista dal progetto stesso. La modifica di un design è un'operazione che richiede alcune ore o, al massimo, pochi giorni. Si tratta, come si può vedere, di un approccio completamente diverso da quello impiegato per i circuiti ASIC: in questo caso il progetto deve essere spedito a un produttore di ASIC o a una fonderia e bisogna attendere non meno di sei settimane prima che venga riconsegnato. Nel caso sia necessario apportare delle modifiche, i tempi si dilatano ulteriormente. Tutto ciò si riflette sfavorevolmente sui tempi di sviluppo: in questo caso si corre il serio rischio di perdere la "finestra temporale" di introduzione sul mercato di un prodotto e quindi le maggiori opportunità di business. Nella fretta di arrivare per primi sul mercato, alcuni sviluppatori tendono a trascurare il rischio legato alla presenza di concorrenti che potrebbero copiare i loro progetti sfruttando tecniche di "reverse engineering" e guadagnare quindi un significativo margine di vantaggio.

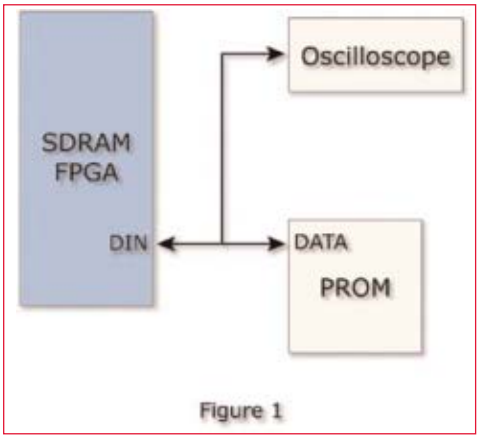

Fig. 1 – Ponendo un oscilloscopio tra una memoria PROM e una FPGA basata su SRAM è possibile acquisire il bit stream di configurazione

Il problema del reverse engineering

Grazie alle tecniche di reverse engineering (ovvero che seguono un percorso inverso rispetto a quello che ha portato alla realizzazione del chip), che possono interessare tanto la parte hardware quanto quella software, è possibile generare specifiche desunte dall'analisi del prodotto di interesse. Tali specifiche vengono quindi sfruttate per generare una copia del prodotto stesso. Un approccio di tale tipo viene talvolta utilizzato da coloro che vogliono continuare a usare un determinato tipo di prodotto non più reperibile per varie ragioni (ad esempio obsolescenza del prodotto stesso). Molto più spesso, invece, tali tecniche sono impiegate da aziende concorrenti per realizzare un prodotto analogo in tempi brevi o da concorrenti sleali che vogliono semplicemente copiare e vendere un prodotto identico a un prezzo notevolmente inferiore.
Il primo passo che viene effettuato nel corso di un'operazione di reverse engineering è quello di penetrare attraverso lo strato di incapsulante del chip mediante processi di incisione (etching) di tipo chimico al fine di evitare di danneggiare la superficie del chip. Mediante un microscopio a contrasto è possibile eseguire la scansione del chip durante il funzionamento e determinare le variazioni di tensione, che forniscono un'indicazione attendibile del funzionamento dei livelli superiori, spesso dei bus delle istruzioni e dei dati.
A questo punto è possibile passare all'analisi di stripping, che consiste nel fotografare gli strati in successione in modo da comprendere la struttura delle interconnessioni e quindi quella dei transistor nel substrato. Le fotografie possono essere analizzate mediante un opportuno softwa-

re di pattern recognition (riconoscimento di forme) allo scopo di generare una netlist e quindi lo schema circuitale necessario per la realizzazione del chip. Sono parecchie le società in grado di offrire, legalmente, questo tipo di servizio. Tali aziende fanno rilevare che esiste sempre un modo per far breccia nelle difese di un chip: tutto dipende dal prezzo (che può variare da 10.000 dollari a diversi milioni). Val comunque la pena sottolineare il fatto che esistono mezzi grazie ai quali è possibile "ostacolare" le operazioni di "reverse engineering" oppure fare in modo che risulti un'operazione troppo costosa per risultare appetibile.

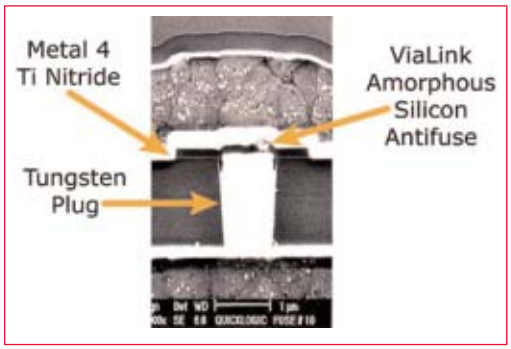

Fig. 2 - La tecnologia ViaLink sviluppata da QuickLogic per i suoi FPGA

La sicurezza di un progetto

Storicamente, il problema della sicurezza di un progetto riguardava solamente alcuni settori specifici, come ad esempio quello militare o dei prodotti di costo elevato. Al giorno d'oggi l'aspetto sicurezza interessa numerosi altri comparti, come ad esempio quello delle reti wireless.

Il principale problema degli FPGA basate su SRAM deriva dal fatto che i dati relativi alla configurazione devono essere introdotti nell'FPGA durante la fase di bootstrap (ovvero la sequenza di operazioni iniziali) del sistema. Semplicemente posizionando un oscilloscopio tra la PROM di bootstrap e l'FPGA (Fig. 1) è possibile ottenere il bitstream di configurazione, che a questo punto può essere copiato e utilizzato in un sistema concorrente. Dopo tutto, l'acquisto di FPGA e chip di memoria è un'operazione banale. La memoria PROM può essere copiata direttamente, così da dar vita a un perfetto clone del sistema.

Una possibile soluzione è il ricorso a una batteria di backup. In questo caso il bitstream viene caricato nell'FPGA direttamente sulla linea di produzione e mantenuto alimentato mediante la batteria di backup anche quanto il sistema non è in funzione. In questo modo è possibile risolvere il problema legato alla vulnerabilità della PROM. Un tale approccio non è comunque esente da svantaggi: da un lato il costo è più elevato, a causa della presenza della batteria, e dall'altro la necessità di dover rimandare il sistema in fabbrica per la riprogrammazione nel caso la batteria di scarichi o si guasti.

La medesima situazione si presenta nel caso in cui si faccia ricorso alla cifratura del bitstream per aumentare il grado di sicurezza del sistema. La chiave per decifrare il bitstream deve risiedere nell'FPGA che a sua volta deve essere mantenuta alimentata da sempre da una batteria di backup.

Per gli FPGA che utilizzano una memoria flash lo scenario si presenta un po' più semplice. Queste memorie sono di tipo non volatile e utilizzano un gate flottante che viene caricato o scaricato per impostare lo stato di uno switch tra due linee di metallizzazione, in modo da non richiedere la presenza di un bitstream per la configurazione. Anche queste memorie, comunque, non sono invulnerabili. Mediante un'opportuna operazione di "spelatura" dello strato di interconnessione nel dispositivo, è possibile eseguire il probing (sondaggio) dei gate nel singolo livello del substrato per stabilire se essi siano o meno caricati e determinare il livello di tensione. Queste informazioni, unitamente alla conoscenza dell'architettura, possono consentire la realizzazione della mappa di configurazione.

Un altro metodo consiste nel porre il chip nudo in una camera a vuoto e alimentarlo, rilevando le emissioni con un microscopio elettronico al fine di costruire la mappa della configurazione.

A livello di grado di sicurezza offerto, i dispositivi ASIC stanno a metà tra gli FPGA basati su SRAM e quelli basati su flash. L'operazione di reverse engineering su un circuito ASIC, seppur costosa, è comunque fattibile.

Una tecnica che può essere utilizzata nei confronti sia dei chip standard sia dei circuiti ASIC prevede la rimozione di ciascuno strato fino ad arrivare a gli strati drogati di tipo P e di tipo N.

A questo punto è possibile applicare un film sottile di metallo per creare un diodo Schottky che può essere osservato con un microscopio elettronico. I micrografici elettronici di ciascun strato vengono quindi trasferiti a un PC su cui gira un software per l'elaborazione delle immagini in modo da ottenere una chiara rappresentazione poligonale e identificare le caratteristiche comuni presenti nell'architettura. Questa tecnica, a prima vista molto complessa, è stata impiegata per eseguire l'operazione di "riverse engineering" di un processore 386 di Intel. Esistono altre tecniche, meno invasive, che possono venire

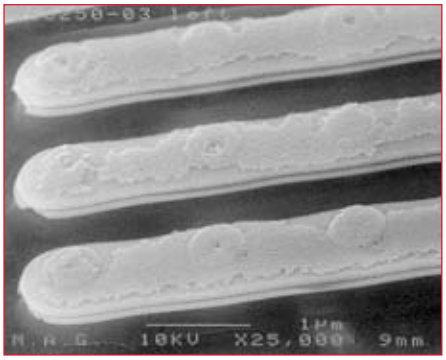

Fig. 3 - Il profilo superficiale di un dispositivo QuickLogic è identico per tutte le connessioni, che siano o meno programmate

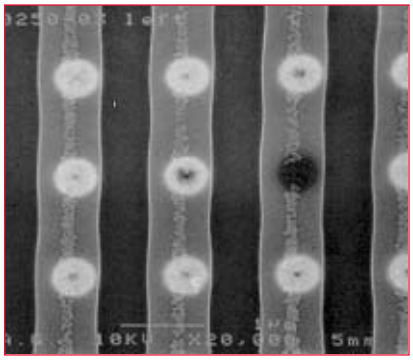

Fig. 4 - Un'ulteriore operazione di rimozione effettuata per cercare di determinare lo stato conduce alla distruzione della via dell'antifusibile

impiegate nel caso siano richiesti dati particolari. Un chip di una smart card per uso bancario può essere decifrata mediante l'analisi termica. Impiegando un rivelatore a infrarossi sulla parte posteriore del chip, è possibile rilevare l'attività sul bus dati e nelle unità di esecuzione principali: l'analisi di queste attività, unitamente alle informazioni desunte dal datasheet, conducono alla chiave di cifratura.

Una valida soluzione: la tecnologia ViaLink

Un metodo per evitare questi problemi e proteggere il sistema dagli attacchi è il ricorso a una tecnologia intrinsecamente sicura. La tecnologia ViaLink sviluppata da QuickLogic per i suoi FPGA (Fig. 2) prevede il ricorso a un antifusibile in silicio amorfo non volatile che agisce come elemento programmabile tra le interconnessioni metalliche. L'adozione di questa tecnologia comporta indubbi vantaggi. Poiché le connessioni ViaLink necessarie vengono settate per mezzo di un impulso di tensione nella fase di programmazione iniziale, non è necessario un bitstream seriale in fase di accensione, e quindi neppure la batteria di backup. Tutti i dati sono interni all'FPGA, codificati in modo passivo sotto forma di interconnessioni, per cui risulta impossibile leggere per via elettronica il design che è stato programmato. Per quanto concerne la programmazione, il software di sbroglio genera un file ASCII contenente le informazioni relative ai link che devono essere programmati e il programmatore hardware confronta questo file con i dati di un database che converte ciascun nome di un link in una locazione sul die e indica le modalità di accesso. Il solo modo per clonare il dispositivo è accedere a questo file di programmazione per generare un nuovo dispositivo. Non esiste alcuna possibilità di analizzare il dispositivo attraverso un punto vulnerabile come la porta JTAG. Essa permette l'accesso ai registri interni al chip per l'esecuzione di operazioni di collaudo ma, come si può facilmente intuire, può essere anche impiegata per determinare la configurazione del chip. QuickLogic utilizza un bit di sicurezza che, una volta programmato, impedisce l'accesso a queste porte interne. Poiché la connessione ViaLink è di tipo volatile e irreversibile, il bit di sicurezza resta impostato e non può essere manomesso in alcun modo.

Ciò non avviene nel caso delle FPGA, sia di tipo SRAM sia basate su flash, dove il bit può essere resettato, e neppure nel caso dei circuiti ASIC, dove è richiesto l'accesso alla porta JTAG per il debug e potrebbe risultare troppo oneroso rimandare il sistema in fabbrica per il settaggio di un solo bit.

Con una tecnologia come ViaLink è anche difficile adoperare la tecnica di stripping per eseguire il "reverse engineering" di circuiti ASIC. Quando non è programmata, la connessione ViaLink è caratterizzata da una resistenza molto elevata, per cui gli strati di metallizzazione risultano isolati: nel momento in cui viene programmata cambia stato e il suo valore di resistenza diventa equiparabile a quella dell'interconnessione di metallo. Le dimensioni sono estremamente ridotte – il diametro è di circa 0,3 micron – e la parte superiore dei collegamenti è molto simile a quella del metallo. In altre parole, il profilo superficiale di un dispositivo QuickLogic è identico per tutte le connessioni, che siano o meno programmate, in modo da non fornire indicazioni circa lo stato del link (Fig. 3). Un'ulteriore operazione di rimozione effettuata per cercare di determinare lo stato conduce alla distruzione della via dell'antifusibile (Fig. 4). Il solo modo di osservare lo stato di ciascun antifusibile è tagliare una sezione trasversale mediante una fresa a fascio ionico focalizzato (FIB - Focused Ion Beam), operazione che comporta praticamente la distruzione del dispositivo. Si tratta comunque di una tecnica molto costosa e l'hacker dovrebbe conoscere la locazione dei link potenzialmente programmati (Fig. 5).

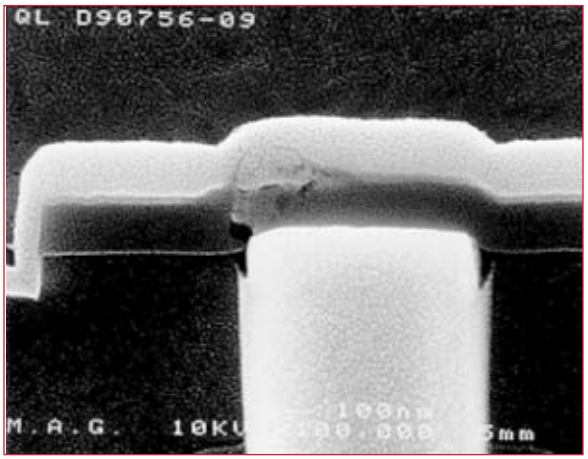

Fig. 5 - Il solo modo di osservare lo stato di ciascun antifusibile è tagliare una sezione trasversale mediante una fresa FIB

Un gran numero di vantaggi

Per generare un design è necessario programmare un numero veramente ridotto di connessioni. Per esempio il dispositivo QL7180 della serie Eclipse Plus dispone di circa 8 milioni di connessioni ViaLink e in un progetto tipico ne vengono usate solo il 4%. Un potenziale hacker deve andare alla ricerca di 80.000 antifusibili programmati su un totale di 8 milioni che sono praticamente indistinguibili gli uni dagli altri. Senza dimenticare il fatto che il progetto stesso diventa inutilizzabile se anche uno solo dei link programmati non viene identificato.

L'approccio di tipo antifusibile comporta numerosi altri vantaggi. Grazie all'architettura di interconnessione, il tasso di utilizzazione delle risorse logiche sfiora il 100%, per cui è possibile far ricorso a logica sparsa per rendere più difficoltoso il lavoro degli hacker. Tale tecnica risulta particolarmente utile per contrabattere i tentativi di intrusione condotti per mezzo dell'analisi termica. Questa logica può essere ubicata deliberatamente in posizioni differenti per evitare di creare raggruppamenti (clustering) che generano punti caldi: inoltre è possibile sfruttarla per creare "motori" che gestiscono chiavi di cifratura false e quindi depistare gli hacker. In definitiva l'impiego di una tecnologia come ViaLink garantisce un livello di sicurezza estremamente elevato, garantendo nel contempo tutti i vantaggi – in termini di elevata velocità, consumi ridotti e flessibilità – tipici delle logiche programmabili.

QuickLogic **www.quicklogic.com**