Introduzione

Con il termine *proprietà intellettuale* (da ora in avanti IP, dall'inglese *intellectual properties*) ci si riferisce genericamente ai frutti dell'attività creativa/inventiva umana ai quali vengono riconosciuti determinati diritti. Formalmente, una proprietà intellettuale è definita come "*un lavoro originale e creativo che si manifesta in una forma tangibile tale da poter essere legalmente protetto*" [**?**]. Le norme in materia garantiscono ai proprietari di IP un assoluto controllo sulla gestione della propria creazione. In particolare, laddove non si optasse per un utilizzo esclusivo della *proprietà*, questa può essere ceduta a terzi tramite cessione su licenza o stipulazione di affiliazioni commerciali (fanchising). Di conseguenza la protezione delle proprietà intellettuali è un meccanismo complesso che può spaziare su più ambiti differenti, quali ad esempio il diritto giuridico, le tecnologie informatiche e le risorse umane.
In riferimento alle tecnologie informatiche, le minacce maggiori sono costituite dalla pirateria dei *core* delle proprietà intellettuali e dalla produzione di componenti contraffatti. In particolare il termine *core* è adoperato in rifermento a progetti software o hardware che possono essere eseguiti o sintetizzati su circuiti integrati. In questo lavoro di tesi con il termine *software IP core* ci riferiamo ad applicazioni eseguibili prodotte tramite le primitive di un qualsiasi linguaggio di programmazione, mentre con il termine *hardware IP core* ci riferiamo a progetti sintetizzati a livello di porte logiche e direttamente implementabili in hardware.
Tradizionalmente grande attenzione è stata riposta nel proteggere proprietà intellettuali rendendo sicuri a livello software i sistemi di elaborazione. D'altro canto

la pirateria software ha da sempre riscosso un maggior interesse rispetto a quella hardware per motivi prettamente economici: essendo meno esosa in termini di costi e richiedendo strumenti generalmente economici, la pirateria software ha potuto abbracciare nel tempo una fetta nettamente maggiore di pubblico potenziale. Tuttavia, dal momento che i circuiti integrati sono fondamenta un di qualsiasi dispositivo elettronico, la pirateria hardware e la produzione di componenti contraffatti sono elementi ancora più cruciali rispetto alla sicurezza del software [**?**]. In aggiunta, la protezione dell'hardware diventa ancora più critica se si considera che le aziende che effettuano progettazione hardware si rivolgono a fonderie esterne per la produzione dei propri design. Sebbene venga stipulato un accordo di riservatezza tra le aziende coinvolte, questo meccanismo introduce un problema di fiducia tra le due parti. In particolare, una fonderia potrebbe sovra produrre i circuiti integrati o clonare il progetto originale affidatogli, in modo tale da trarne ulteriore profitto sul *mercato nero*. Tali problematiche trovano riscontro nella realtà, tanto che i componenti hardware dei computer, delle periferiche e dei sistemi embedded sono le proprietà intellettuali più contraffatte sul mercato [**?**], come dimostra il rapporto dell'IHS che stima in circa 169 miliardi di dollari le perdite che l'industria elettronica deve affrontare annualmente a causa della contraffazione della componentistica. [**?**].

Con l'avvento e la crescita dei *field-programmable gate arrays* (FPGAs) sono nate ulteriori preoccupazioni riguardanti la sicurezza hardware e la protezione delle proprietà intellettuali. Infatti è possibile sfruttare la capacità di riprogrammazione degli FPGA in modo tale da permettere ad un progettista di poter riusare IP cores sviluppati da terze parti. Inoltre i moderni FPGA hanno estremamente ridotto il gap con gli *application specific integrated circuits* (ASICs) grazie all'introduzione all'interno dello stesso chip di un *Processing System*, definendo così *Systems on Programmable Chips* (SoPCs). Di conseguenza è nato un nuovo segmento di mercato del cosiddetto *reconfigurable computing*, che sfrutta principalmente le potenzialità della tecnologia FPGA in modo tale da fornire acceleratori hardware per task tipi-

camente progettati per essere eseguiti a livello software. Pertanto diventa cruciale proteggere sia i software IP cores, che sono eseguiti sui SoPC, sia gli hardware IP cores, che sono sintetizzati sugli FPGA. Di conseguenza è chiaro il bisogno di nuovi schemi di protezione e di meccanismi di difesa atti a garantire il rispetto dei diritti riconosciuti ai proprietari di IP.

Tipicamente per prevenire la pirateria delle proprietà intellettuali, i venditori di IP stipulano con i propri clienti un accordo di licenza vincolante, incorporando un meccanismo di protezione all'interno dei propri progetti o cifrando gli stessi IP cores. Quest'ultimo approccio è maggiormente prevalente nei progetti FPGA-based [**?**] e si basa su una terza parte fidata che agisce come intermediario tra il venditore di IP e i suoi clienti. In particolare i venditori di IP vendono e rilasciano i propri hardware IP cores utilizzando file di bitstream cifrati, i quali contengono la nuova configurazione relativa all'hardware IP core che assumerà la FPGA quando verrà riprogrammata. Utilizzando questo schema di protezione, la terza parte assume quindi il ruolo di autorità fidata che non solo è a conoscenza della chiave crittografica, ma si occupa anche di inserirla all'interno del dispositivo FPGA.

Recentemente è stato introdotto un nuovo approccio basato sullo sviluppo di un'infrastruttura per il Digital Right Management (DRM) in grado di garantire protezione, distribuzione, modifica e applicazione dei diritti connessi all'utilizzo di contenuti digitali. Le implementazioni del DRM sono spesso basate su piattaforme fidate di elaborazione che forniscono nativamente i meccanismi appena descritti. Tali piattaforme integrano al loro interno un chip addizionale, il Trusted Platform Module (TPM), che fornisce primitive per la sicurezza, come attestazione della piattaforma e archiviazione protetta, in modo tale da validare la configurazione dell'hardware e, all'occorreza, del software della piattaforma stessa [**?**].

La sicurezza dei meccanismi di protezione appena descritti può essere ulteriormente aumentata sfruttando le Physically Unclonable Functions (PUFs), le quali forniscono firme digitali uniche prodotte sfruttando le proprietà fisiche del dispositivo in cui

sono integrate. Utilizzando le loro eccezionali caratteristiche di non clonabilità, impredicibilità e resistenza (le PUFs vengono considerate a tutti gli effetti un sistema anti-manomissione), è possibile sviluppare nuovi meccanismi maggiormente sicuri per la protezione di proprietà intellettuali. Inoltre, siccome le PUF sono implementabili su qualsiasi dispositivo, è possibile sfruttarle anche su FPGA a basso costo che non dispongono di meccanismi integrati di cifratura. Difatti, in letteratura si trovano ampie testimonianze su possibili implementazioni di PUF e di protocolli per la protezione di proprietà intellettuali, sia per ASIC che per FPGA.

Contributo della Tesi

L'obiettivo di questo lavoro di tesi è fornire un'analisi sui meccanismi disponibili per la protezione di proprietà intellettuali, e di contribuire con soluzioni innovative per FPGA e SoPC che sfruttano le caratteristiche delle PUF.
Parte del lavoro di tesi è stato pubblicato e discusso in conferenze accademiche. Di seguito riportiamo la lista degli articoli prodotti:

- M. Barbareschi, P. Bagnasco, and A. Mazzeo, "Supply voltage variation impact on anderson puf quality", in *Design & Technology of Integrated Systems In Nanoscale Era (DTIS). 2015 10th IEEE International Conference On.* IEEE, 2015, pp. 1–6.

- M. Barbareschi, A. Mazzeo, and P. Bagnasco, "Implementing reliable mechanisms for ip protection on low-end fpga devices", March 2015. URL `http://www.date-conference.com/conference/workshop-w10`. DATE W10 TRUDEVICE 2015, online publication.

Organizzazione della Tesi

La struttura della tesi è riportata di seguito:

- Il Capitolo 1 presenta le attuali minacce alla sicurezza hardware che sfruttano le vulnerabilità della tecnologia FPGA, e le relative contromisure disponibili;
- Il Capitolo 2 fornisce un'ampia analisi sulle proprietà delle silicon PUF e sulle implementazioni disponibili per la tecnologia FPGA;
- Il Capitolo 3 introduce i meccanismi di sicurezza e i protocolli di protezione presenti in letteratura che sfruttano le PUF;
- Nel Capitolo 4 definiamo e implementiamo nuove soluzioni che, mediante le PUF, forniscono meccanismi per la protezione di proprietà intellettuali. In particolare presentiamo diversi implementazioni per il licensing e la protezione di IP cores sia per FPGA a basso costo che per dispositivi più complessi. Tali meccanismi sfruttano l'offuscamento, la crittografia e il TPM. Inoltre, presentiamo uno schema innovativo di *enrollment*, il quale permette ad una terza parte di estendere dinamicamente e remotamente l'iniziale set di challenge-response di una PUF;
- Il Capitolo 5 conclude la tesi, e fornisce indicazioni riguardanti futuri sviluppi;
- La Appendice A presenta un'analisi dettaglia della PUF di Anderson, descrivendo il procedimento di *porting* per la FPGA Xilinx Spartan-3E, e stimando sperimentalmente le sue qualità al variare delle condizioni ambientali.