



UNITYFVG

United Universities of FVG
Technology Transfer

CHIP PIÙ SICURI CON LE PHYSICALLY UNCLONABLE FUNCTIONS

Dispositivo integrabile per l'implementazione di Physically Unclonable Functions



Settore:

Elettronica

Titolarietà del brevetto:

Università di Udine

Inventori:

R. Bernardini, R. Rinaldo

Data di priorità:

1/10/2014

Numero brevetto:

PD2014A000253

Status legale del brevetto:

Brevetto esteso a livello internazionale

Disponibilità alla licenza:

Sì

Contatti:

Ufficio Trasferimento Tecnologico - Università di Udine

brevetti@uniud.it - tel. 0432 556384

In cosa consiste?

La soluzione proposta consiste in un **circuito sviluppato ad hoc per integrare una PUF**, potenzialmente utilizzabile su **chip di diversi produttori**.

A che bisogno risponde?

La ricerca si è orientata alla realizzazione di chip dotati di "chiavi private", uniche e non replicabili, basate sulle caratteristiche fisiche del singolo chip derivanti da imprecisioni legate alla fase di produzione (*PUF-Physically Unclonable Functions*).

La tecnologia proposta è un **circuito sviluppato per implementare una PUF perfettamente stabile**, evitando la necessità di costosi meccanismi di stabilizzazione.

Dispositivi basati sulle PUF infatti sono utilizzati per proteggere la proprietà intellettuale di *software embedded*, per consentire la comunicazione sicura *machine to machine* o per sistemi di pagamento basati su lettori di *smart cards* e carte di credito *chip-based*. Le soluzioni attualmente offerte sono "instabili": nonostante la PUF integrata in un dispositivo generi la stessa parola segreta, occasionalmente può produrre bit sbagliati e rendere il sistema inusabile. Per proteggersi dall'instabilità si ricorre a schemi "stabilizzanti" che però aumentano complessità (e costo) del dispositivo.

Che vantaggi ha?

Rispetto ad altre tecnologie (es. basate sull'utilizzo di SRAM), il dispositivo proposto:

- ✓ non richiede circuiti stabilizzatori aggiuntivi
- ✓ semplifica il processo e riduce i costi di produzione.

Qual è il mercato di riferimento?

La tecnologia s'inserisce nel segmento di mercato della **sicurezza hardware**, parte del mercato più ampio della produzione di semiconduttori, chip e componenti.

La diffusione di dispositivi elettronici portatili, di tecnologie di comunicazione *machine to machine* e la richiesta di sicurezza a livello hardware subiranno un significativo **trend di crescita**. Il valore globale del mercato dei chip per applicazioni industriali ha raggiunto nel 2013 un valore di 33 miliardi di dollari, con crescita dell'11% rispetto al 2012. Si prevede che entro il 2018 il fatturato del mercato raggiungerà i 45 miliardi di dollari.

Si tratta di un mercato dinamico, con **altissimi tassi di innovazione** a livello di prodotto e di standard settoriali. Grossi player controllano gran parte del mercato della produzione di chip e microprocessori, ma vi sono possibili segmenti di ingresso in altre aree della catena del valore.

La tecnologia proposta si rivolge ai **produttori di chip e microprocessori**, a OEMs e aziende produttrici di **dispositivi elettronici integrati e software embedded** ed è di interesse per aziende attive nel settore della **sicurezza hardware** (*smart card, chip* per sistemi di pagamento ecc.).

Stato di avanzamento

La tecnologia è stata validata attraverso **studi analitici e simulazioni**. La fase di sviluppo successiva prevede l'avvio della validazione sperimentale e la realizzazione dei primi prototipi applicativi.

Università degli Studi di Trieste

Industrial Liaison Office
Piazzale Europa 1, 34127 Trieste

Università degli Studi di Udine

Ufficio trasferimento tecnologico
Vicolo Florio 4, 33100 Udine

Scuola Internazionale Superiore di Studi Avanzati

Servizio trasferimento tecnologico
Via Bonomea 265, 34136 Trieste