



SAPIENZA
UNIVERSITÀ DI ROMA

***Effetti dell'hardware nella valutazione di
funzioni di sicurezza comunque
realizzate (HW, FW, SW)***

Dipartimento di Ingegneria Elettronica (DIE)

Università di Roma "La Sapienza"

Fondazione Ugo Bordoni

Relatore

Prof. Alessandro Trifiletti

Controrelatore

Prof. Mauro Olivieri

Dottorando

Francesco Trotta

XXV ciclo

Ambito di ricerca (I)

- ❑ **Attacchi a funzioni di sicurezza (crittografia) basati sulla vulnerabilità dell'hardware (*hardware attacks*) e relative contromisure**
- ❑ **Alcuni attacchi all'hardware (*side channel attacks*) si basano su osservazione del comportamento fisico del dispositivo che realizza la funzione di sicurezza.**

Side Channel Attacks:

- ❑ **Categoria di attacchi non invasivi che, utilizzando varie tecniche di inferenza statistica, producono una stima del valore dei segreti (P. es. password, chiave di codifica) sulla base dell'osservazione di grandezze fisiche, ad esempio:**
 - ❑ **Potenza assorbita (*power attacks*)**
 - ❑ **Potenza irradiata (*electromagnetic attacks*)**
 - ❑ **Tempo di esecuzione (*timing attacks*).**
- ❑ **L'attacco richiede la raccolta di un elevato numero di tracce, corrispondenti a parole opportunamente scelte inviata in ingresso al dispositivo crittografico.**

Ambito di ricerca (II)

Esempi di Contromisure

- ❑ **Stili logici diversi dal CMOS classico:**
- ❑ Non manifestano variazioni apprezzabili dell'assorbimento di corrente in funzione delle operazioni effettuate e/o dei dati trattati.
- ❑ **Tecniche che agiscono sull'algoritmo di codifica:**
- ❑ inserimento di operazioni "dummy" su dati generati casualmente.
- ❑ "mascheramento" dei dati trattati internamente combinandoli con valori generati "casualmente" ad ogni nuova esecuzione dell'algoritmo.

Obiettivi

- ❑ **Messa a punto di un "setup" di misura per l'esecuzione di attacchi side-channel;**
- ❑ **Proposta di nuove metodologie per attacchi side channel**
- ❑ **Proposta di contromisure rispetto agli attacchi side-channel noti in letteratura**
- ❑ **Studio di una metodologia che consenta di validare l'efficacia delle contromisure.**

Attività svolte

- ❑ **E' stato perfezionato il setup di misura, in particolare l'interfaccia tra core crittografico e computer.**
 - ❑ Precedentemente si era previsto l'uso di una interfaccia USB, ma la sua implementazione si è rivelata problematica quindi si è optato per una più semplice interfaccia seriale.
 - ❑ Con opportune modifiche tale interfaccia è stata adattata a diversi core crittografici.
- ❑ **Sono stati eseguiti attacchi a correlazione (CPA) su diversi core crittografici**
 - ❑ Tali attacchi hanno comportato l'acquisizione di tracce in differenti modalità, variando l'intervallo di acquisizione e il numero di punti per traccia.
 - ❑ Il numero di tracce acquisite varia da poche decine di migliaia a diverse centinaia di migliaia.
 - ❑ L'esperimento di maggior durata (400000 tracce) ha richiesto un tempo di acquisizione di 6 giorni
 - ❑ L'analisi dei dati è stata effettuata tramite un software precedentemente sviluppato all'interno del dipartimento.
- ❑ **Sono stati individuati gli elementi (registri e logica combinatoria) responsabili del leakage.**
- ❑ **E' stata implementata e testata una contromisura a mascheramento su uno dei core.**

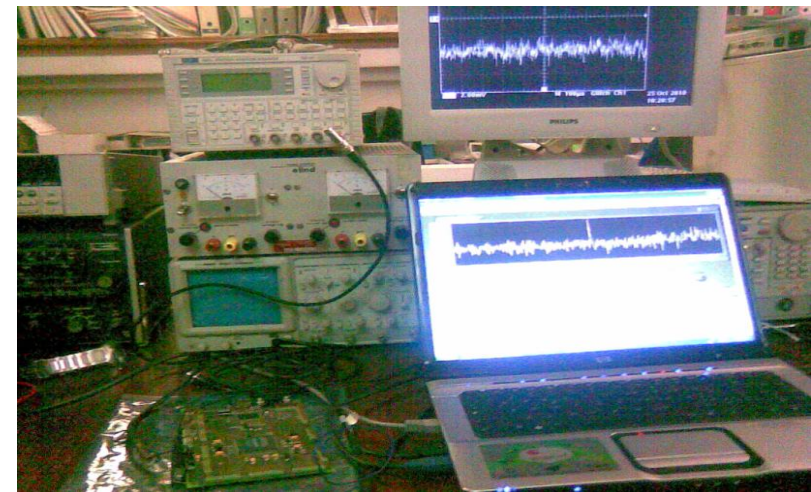
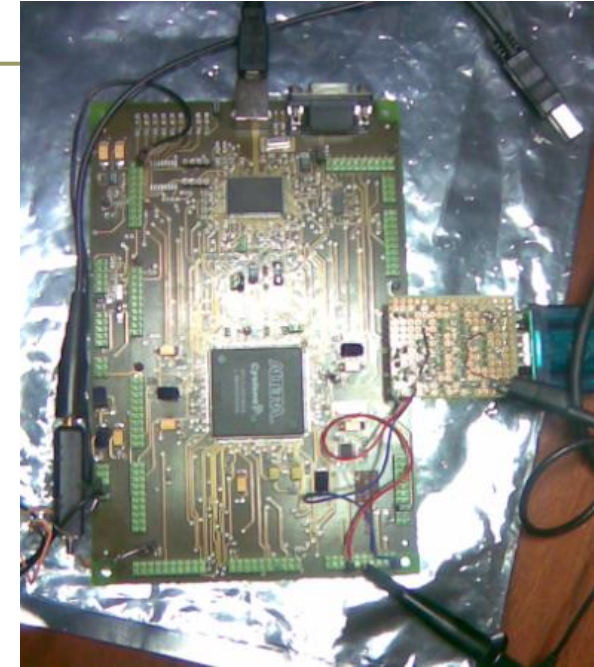
Setup di misura

Hardware

- ❑ Oscilloscopio digitale Tektronix TDS520;
- ❑ scheda FPGA basata su ALTERA Cyclone I e su microcontrollore Cypress per l'interfaccia USB;
- ❑ Collegamento al PC tramite:
 - ❑ USB per il caricamento del codice
 - ❑ Porta seriale per lo scambio di dati (plaintext e cyphertext)
- ❑ Sonda di corrente Tektronix TC-1
- ❑ PC con installato l'ambiente di sviluppo Labview;
- ❑ interfaccia USB – GPIB

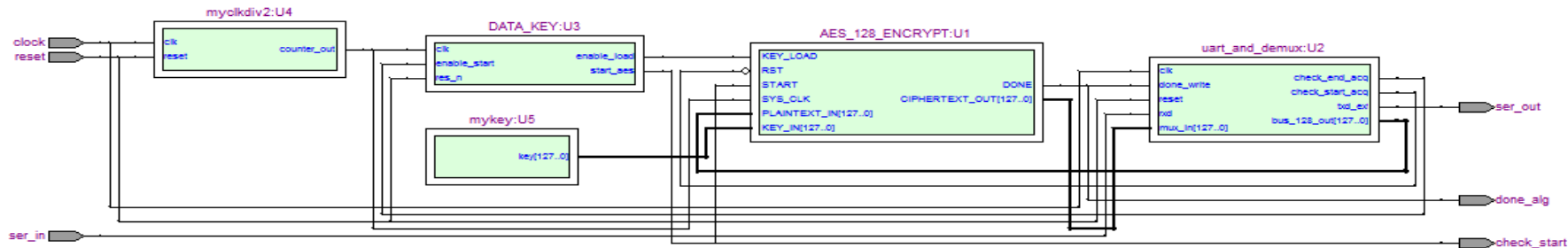
Software

- ❑ Programma di acquisizione delle tracce scritto in linguaggio Labview;
- ❑ Matlab;
- ❑ Programma di analisi delle tracce (per il momento è il programma "Gemini" realizzato in dipartimento);

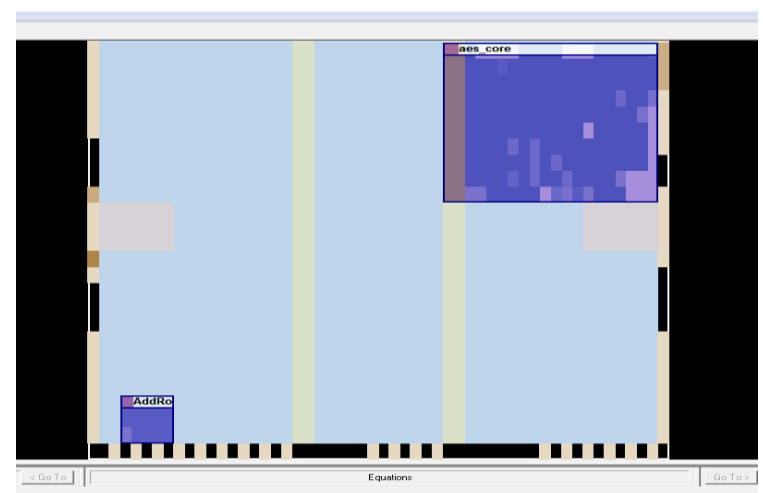
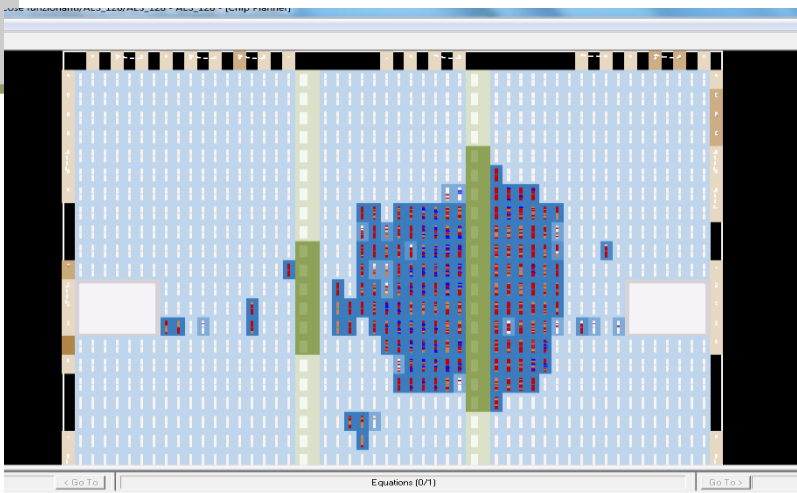


Gestione funzionamento core AES

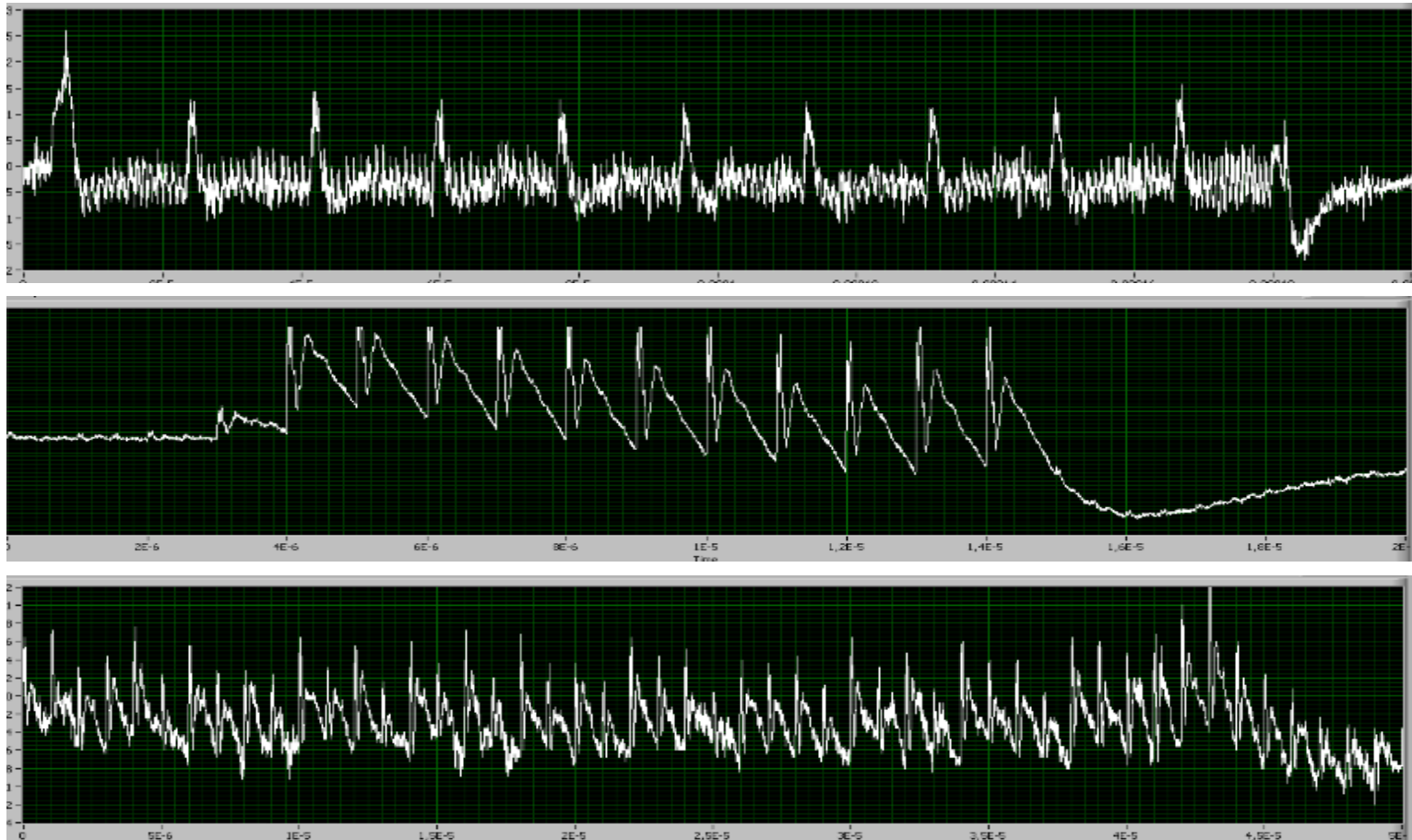
■ Esempio di diagramma RTL di core crittografico più relative interfacce I/O



- E' possibile decidere dove piazzare i diversi blocchi funzionali, ciò permette ad esempio, di separare fisicamente le varie funzioni.
- In questo è possibile verificare se e come cambia il leakage di informazione al variare della disposizione dei blocchi.
- Inoltre questo può rendere più agevole un eventuale attacco con sonda EM.



Esempi di tracce



□ Esempi di tracce: nei primi due casi sono ben visibili le 10 iterazioni dell'algoritmo di codifica AES

Acquisizione delle tracce

- All'interno della FPGA è caricato il core crittografico AES.**
 - Caricamento del codice tramite USB.
 - Interfaccia di comunicazione seriale asincrona per il caricamento dei dati da criptare (plaintext) e l'invio dei dati criptati.

- Il programma Labview gestisce l'acquisizione**
 - Genera casualmente le parole da 128 bit del plaintext e le invia al core, contemporaneamente le salva in un file txt.
 - Al termine dell'invio di ogni parola da 128 bit, viene fatta partire la codifica AES, mediante un segnale di start prodotto dalla logica di interfaccia seriale.
 - Tale segnale è utilizzato anche dall'oscilloscopio come trigger.
 - Terminata la codifica i dati vengono inviati in uscita e il sistema si pone in attesa di un'altra parola da codificare.

- La misura della traccia di assorbimento viene effettuata tramite la sonda di corrente induttiva.**

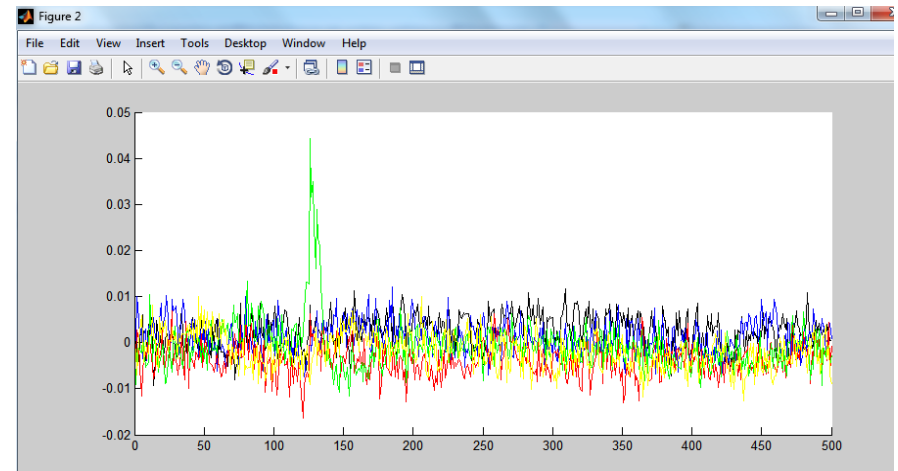
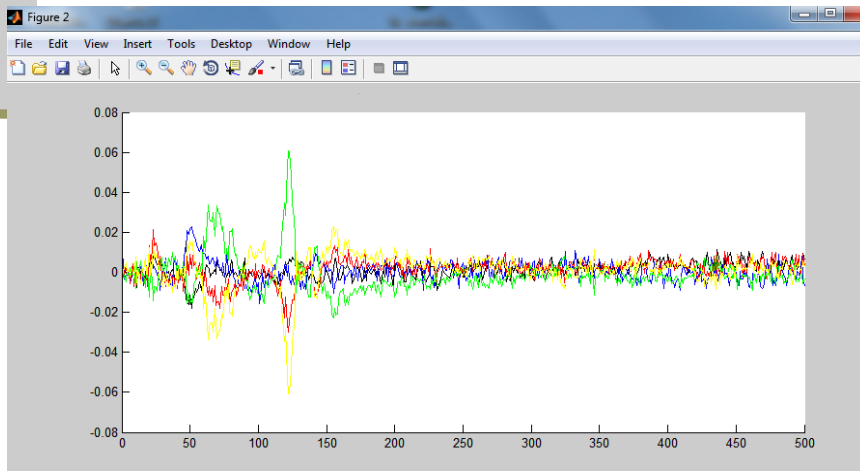
- L'oscilloscopio acquisisce la traccia e la invia al PC tramite GPIB.**

- Il programma Labview riceve i dati dall'oscilloscopio e li immagazzina in un file txt.**

- Si ha un file per ogni traccia acquisita.**

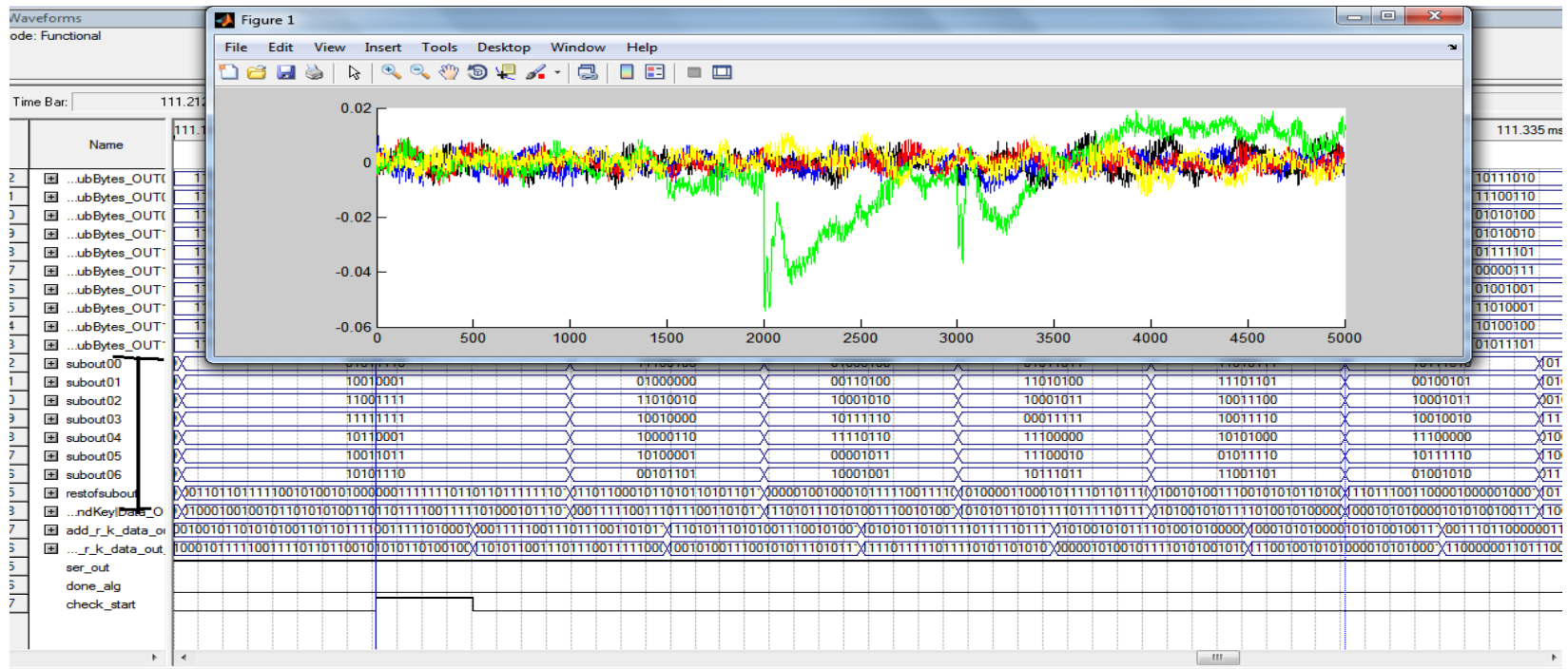
Analisi dei dati

- ❑ **Analisi effettuata tramite software prodotto all'interno al dipartimento.**
- ❑ **Analisi a correlazione.**
- ❑ Si considera il peso di hamming dei valori dei dati intermedi.
- ❑ **Obiettivo: primo round dell'algoritmo AES, in particolare:**
- ❑ Operazione di xor tra dato in ingresso e chiave
- ❑ Uscita dalla sbox al primo round di elaborazione
- ❑ **Il software di analisi produce in uscita un file che viene poi elaborato mediante Matlab.**
- ❑ Il risultato è un grafico della funzione di correlazione, che presenta un picco nel caso di previsione di chiave corretta.
- ❑ **Dalla posizione del picco si vede inoltre a che punto (ossia quando) avviene l'operazione che ha causato il leakage.**



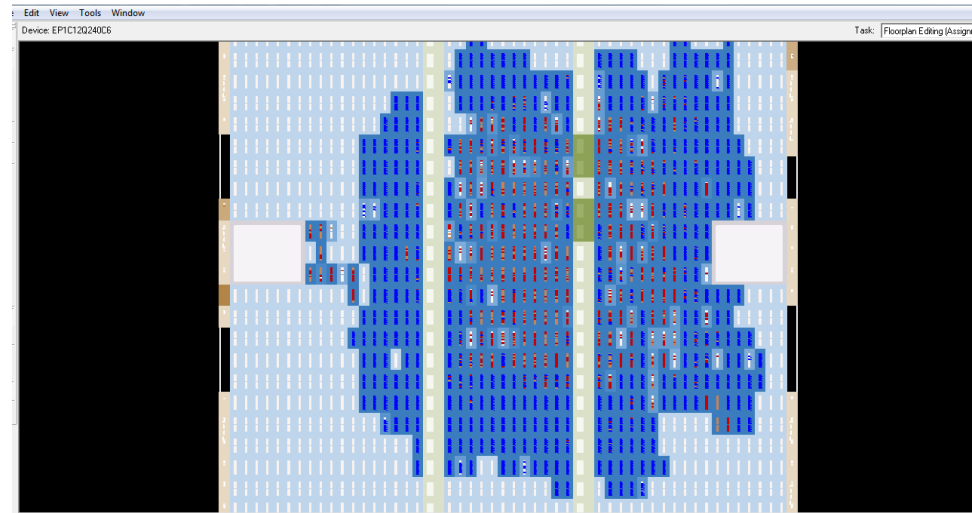
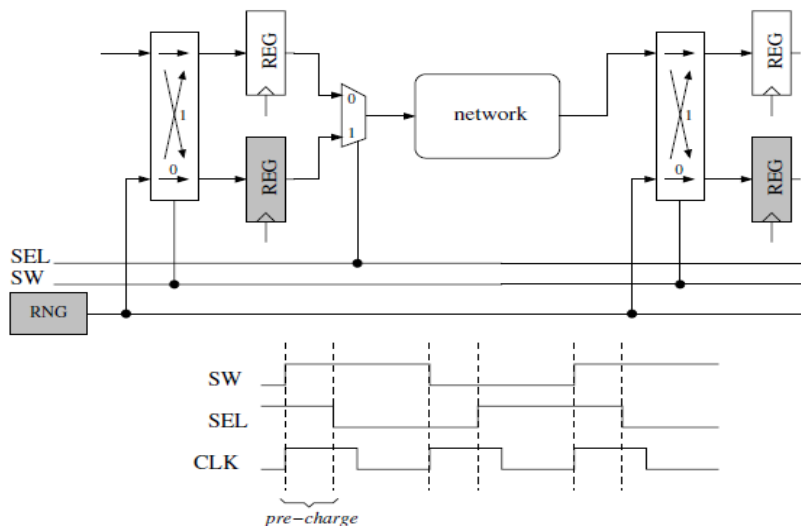
Dove avviene il leakage

- ❑ **Le tracce acquisite negli attacchi a core1 e core3 sono state confrontate con le simulazioni (simulatore di Quartus II) di detti core.**
- ❑ Si è confrontato l'andamento della funzione di correlazione, e i picchi relativi alla chiave corretta, con le forme d'onda di determinati blocchi funzionali, in particolare i registri.
- ❑ L'intento era di verificare quali componenti commutano in corrispondenza dei picchi.
- ❑ Di seguito un esempio di grafico.



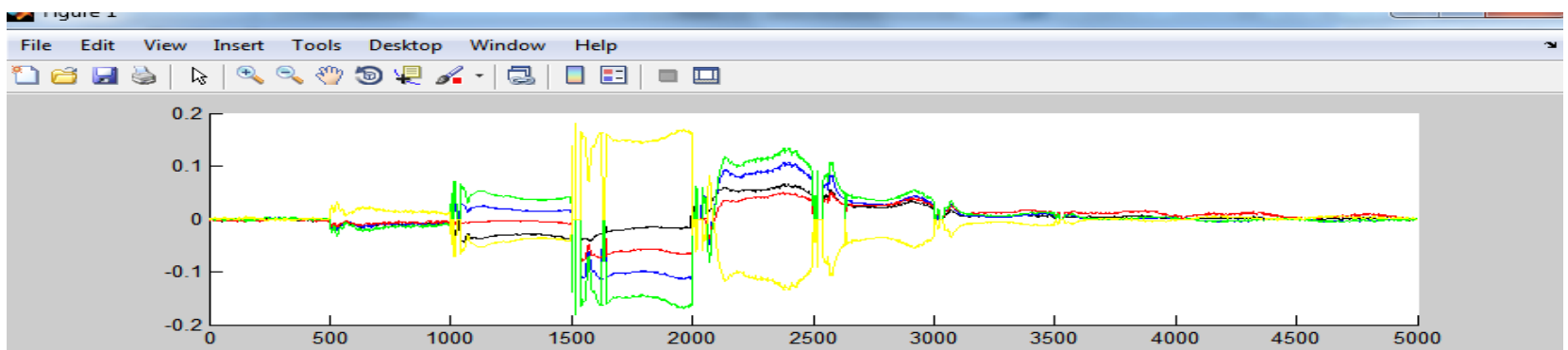
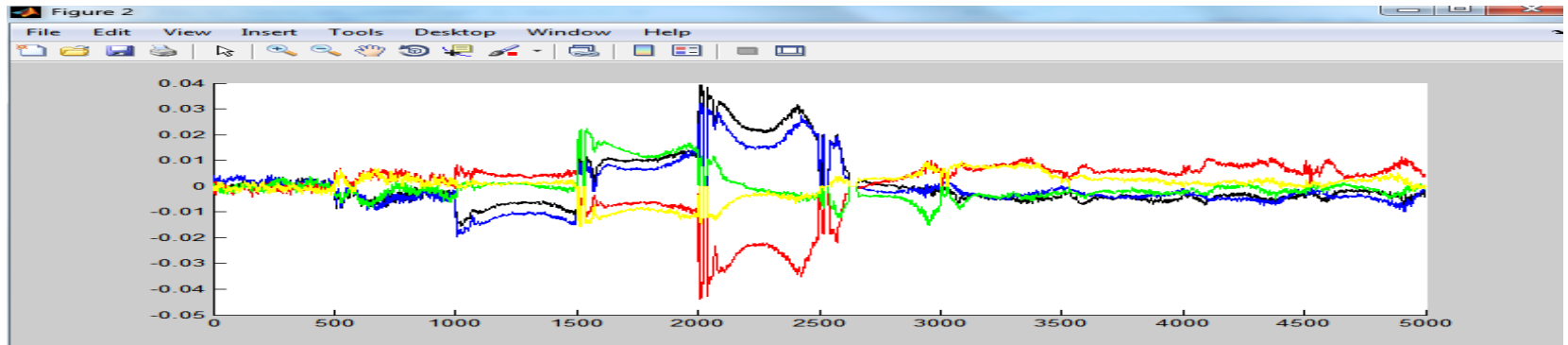
Implementazione Contromisura

- ❑ **E' stata implementata una contromisura sviluppata dal dipartimento.**
- ❑ Descritta nell'articolo di Bucci, Guglielmo, Luzzi e Trifiletti (*A power consumption randomization countermeasure for DPA-resistant cryptographic processors*).
- ❑ **Questo è un esempio di contromisura a mascheramento basata sul principio del random precharging dei registri.**
- ❑ **Il core cui è stata applicata è uno di quelli reperiti in rete e già attaccato con successo nella versione originale.**
- ❑ **Si paga un prezzo in termini di area occupata e assorbimento di corrente.**



Esperimento su contromisura

- ❑ **Il core contromisurato è stato sottoposto ad attacco**
- ❑ Raccolte 400000 tracce di assorbimento di corrente.
- ❑ L'attacco verso l'uscita della sbx (Subbyte) non ha avuto successo, mentre ha avuto successo quello verso lo xor (AddRoundKey).



In alto, correlazione su sbx, in basso, correlazione su xor, in verde la chiave corretta

Risultati

Messa a punto del setup di misura

Realizzazione di esperimenti di attacchi side channel su più dispositivi

- Il core sviluppato nel dipartimento, strettamente sequenziale e privo di contromisure è molto facile da attaccare, mentre gli altri core, dotati un certo grado di parallelismo, benché privi di contromisure richiedono un numero molto elevato di tracce e un tempo di acquisizione molto più lungo.

Validazione del setup di misura

- L'esecuzione di esperimenti con diversi dispositivi crittografici e con diverse modalità ha fornito un'ulteriore prova della bontà del setup di misura.

Esperimenti su diverse implementazioni su FPGA dello stesso dispositivo.

- Analisi dell'attaccabilità in funzione della disposizione fisica dei blocchi funzionali.

Esperimenti su implementazione di contromisura a mascheramento

- Validazione su un particolare stadio (subByte).

Considerazioni

- Per il II anno gli obiettivi erano:**
 - Effettuare dei veri attacchi DPA (Differential Power Analysis) sia su dispositivi standard che contromisurati.
 - Estendere tali attacchi anche ad altri parametri fisici (E.M.).
 - Raffinare ulteriormente il sistema di acquisizione.
 - Elaborazione dei dati tramite opportuno software
- Di tali obiettivi non è stata realizzata l'estensione alla misura di emissione e.m.**
- In compenso sono stati eseguiti attacchi su diversi core, che rispetto a quello sviluppato nel dipartimento sono più simili a quelli comunemente impiegati.**
- Si è cominciato ad indagare su come alcuni parametri implementativi influenzano la vulnerabilità agli attacchi.**
- E' stata implementata e testata una contromisura a mascheramento su uno dei core utilizzati.**

Attività da svolgere nel III anno

- ❑ **Confrontare i risultati sperimentali con quelli ottenuti in simulazioni svolte precedentemente da altri all'interno del dipartimento, al fine di capire nel dettaglio quali parti dei dispositivi sono maggiormente implicate nel leakage, in modo da elaborare un efficace metodo di contromisura.**
- ❑ **In tali simulazioni era stato provato anche un core contromisurato sviluppato all'interno del dipartimento. Sarà utile effettuare anche su di esso degli esperimenti al fine sia di validare la contromisura sia di elaborarne una migliore.**
- ❑ **Come ulteriore altra attività si propone di ritornare sull'argomento degli attacchi E.M. Questi richiedono l'acquisizione di un enorme numero di tracce, e la possibilità di posizionare la sonda esattamente sopra la parte del dispositivo che si ritiene responsabile del leakage. Una sonda E.M. (artigianale e dalle prestazioni da verificare) è già disponibile nel laboratorio.**



SAPIENZA
UNIVERSITÀ DI ROMA

Grazie per l'attenzione!