PROGETTO DI INGEGNERIA INFORMATICA

IMPLEMENTAZIONE DI PRIMITIVE CRITTOGRAFICHE RESISTENTI A CALCOLATORI QUANTISTICI (POST QUANTUM)

Anno Accademico: 2023/2024

**Contemi Agostino Dodi Filippo**

Professore: Barenghi Alessandro

Indice

1. Introduzione
   1. Perché SHA3
   2. Keccak
   3. Crittografia post quantum
2. Come è possibile ottimizzare sha
   1. Come è possibile ottimizzarlo
   2. Architetture e loro differenze (no dettagli su intrisics)
   3. AVX
   4. NEON
3. Risultati
   1. Soggetti dei confronti
   2. Dispositivi usati
   3. Processo di validazione e misura dei risultati
   4. Analisi dei risultati
4. Conclusioni
   1. Cosa abbiamo imparato
   2. Pareri degli autori
   3. Ringraziamenti
   4. Citazioni / Bibliografia
5. Introduzione
6. Perché SHA3

* Storia di SHA3
  + Mondo crittografico prima di sha3 (citazione ad attacchi a sha1)
  + NIST e la competizione
  + Vincitori: keccak, autori, su cosa si sono basati
  + SHA3 oggi
* Vantaggi di SHA3
  + Resistenza ad attacchi (attacchi a sha1)
  + Versatilità (sicurezza oppure velocità per es sha3 512 e piu lento ma piu sicuro)
  + Facilità di implementazione
  + Pubblico open source
* Svantaggi di SHA3
  + Lento a morire a meno di implementazione hardware apposite
  + Suscettibilità alle collisioni

1. Keccak

Paragrafo di introduzione generale

* Sponge function
  + Lo stato marxista
  + (init, absorb, finalize, extract)
  + Absorb, padding
  + Squeeze
* Le permutazioni
  + Overview step
  + Theta, Rho, Pi, Chi, Iota

1. Crittografia post quantum

* Cos’è un computer quantistico (3 righe max)
* Perché creano problemi di sicurezza
* Come SHA3 risolve tali problemi
* Vulnerabilità di SHA3 Post quantum (collisione)

1. Com’è possibile ottimizzare SHA
2. Com’è possibile ottimizzarlo

* Cos’è la vettorizzazione/parallelizzazione
* Un paio di esempi di parallelizzazione
* Altre tecniche di ottimizzazione (load e store solo quando serve, ordine di operazioni secondo operandi, loop, valori precalcolati)

1. Architetture e le loro differenze

* x86 e ARM (differenze tra le 2)
* Instrisics cosa sono e perche

1. AVX

* Come funziona (registri, tipi di variabili)
* Istruzioni usate
* Gestione dello stato
* Variabili globali e inizializzazione
* La StateXORBytes
* La StateExtractBytes
* La StatePermute
  + Theta come ottimizziamo
  + Rho
  + Pi chi iota
* Il fastloop

1. NEON

* Come funziona (registri, tipi di variabli)
* Istruzioni usate
* Gestione dello stato
* Interlacciamento
* Le intrisics rallentano l’esecuzione nella permute
* La StateXORBytes e StateExtractBytes

1. Risultati
2. Soggetti del confronto

* SUPERCOP
* CROSS
* Nostre implementazioni

1. Dispositivi usati
2. Processo di validazione e misura dei risultati
3. Analisi dei risultati

* Grafici
* Tabelle di dati
* Spiegazione dei risultati

1. Conclusioni
2. Cosa abbiamo imparato
3. Pareri degli autori
4. Ringraziamenti
5. Citazioni / Bibliografia