KEM SABER VS DS FALCON

KEM SABER è considerato più semplice da implementare rispetto a **DS FALCON**. Le operazioni aritmetiche di base di SABER (come la convoluzione di polinomi e l'arrotondamento) sono meno complesse rispetto alla gestione delle trasformate di Fourier e delle operazioni su reticoli necessarie per FALCON.

Implementazione Efficiente di Saber su ESP32

Questo documento descrive un'implementazione efficiente di Saber, uno schema di incapsulamento delle chiavi post-quantistico basato su lattice CCA-sicuro[Un algoritmo si dice CCA-sicuro se è sicuro contro attacchi di tipo Chosen Ciphertext Attack (CCA). Questo tipo di sicurezza implica che l'algoritmo rimane sicuro anche se l'attaccante ha la possibilità di ottenere la decrittazione di testi cifrati scelti.], sul microcontrollore ESP32. Saber è stato selezionato come uno degli algoritmi candidati per la standardizzazione della crittografia post-quantistica dal National Institute of Standards and Technology (NIST) degli Stati Uniti.

Punti Chiave del Documento:

Moltiplicazione Polinomiale: Le prestazioni di Saber dipendono fortemente dalla velocità della moltiplicazione polinomiale. Il documento presenta un'implementazione ottimizzata che utilizza il coprocessore per interi di grandi dimensioni presente sull'ESP32 per accelerare questo processo. Viene utilizzata una combinazione di tecniche come la sostituzione di Kronecker, l'algoritmo di Karatsuba e l'algoritmo di Toom-Cook per suddividere le

moltiplicazioni polinomiali in operazioni più piccole che possono essere gestite dal coprocessore.

Utilizzo del Tempo di Inattività della CPU: Durante l'esecuzione del coprocessore, la CPU è generalmente inattiva. Il documento propone strategie per utilizzare questo tempo di inattività per preparare i dati per le successive moltiplicazioni, riducendo ulteriormente il tempo di calcolo complessivo. Queste strategie includono il pre-calcolo delle somme ponderate dei polinomi di input, la riorganizzazione dei passaggi di interpolazione e l'allineamento preventivo degli input per il coprocessore.

Accelerazione Dual-Core: L'ESP32 è dotato di due core CPU. Il documento descrive come lo schema Saber può essere suddiviso in attività più piccole che possono essere eseguite in parallelo sui due core, migliorando ulteriormente le prestazioni.

Risultati Principali:

L'implementazione ottimizzata di Saber sull'ESP32 supera significativamente le implementazioni precedenti in termini di velocità. La versione dual-core è più veloce di un fattore 10.5x, 10.1x e 13.2x per la generazione delle chiavi, l'incapsulamento e il decapsulamento, rispettivamente, rispetto all'implementazione di riferimento.

Il documento dimostra che il coprocessore per interi di grandi dimensioni, originariamente progettato per l'accelerazione di RSA o ECC, può essere utilizzato efficacemente per accelerare le moltiplicazioni polinomiali nella crittografia basata su reticolo.

Limitazioni:

L'accelerazione dual-core è limitata dalla natura sequenziale dell'algoritmo Saber e dal fatto che l'ESP32 ha un solo coprocessore per interi di grandi dimensioni e un solo generatore di numeri casuali.