Projekt

Teoretyczna

- Kontekst: Dlaczego Keccak został wybrany jako SHA-3? Krótka historia konkursu NIST
- Krótka charakterystyka pozostałych finalistów konkursu SHA-3

Szczegółowe wyjaśnienie stanu (state) jako tablicy $5 \times 5 \times w$ bitów (gdzie w to długość słowa).

Standardowo Keccak-f[1600] ma stan $5 \times 5 \times 64 = 1600$ bitów

- Liczba rund (n_r): Wyjaśnienie, dlaczego jest ich 24 w Keccak-f[1600]
- Dokładne opisanie każdej z pięciu operacji rundy, wyjaśniając jej cel (np. dyfuzja, nieliniowość):
    - Theta (θ): Mieszanie bitów w kolumnach.
    - Rho (ρ) i Pi (π): Permutacje/przesunięcia.
    - Chi (χ): Nieliniowa operacja (kluczowa dla bezpieczeństwa).
    - Iota (ι): Dodanie stałej rundy.

Analityczna

1. Właściwości kryptograficzne
    - Dyfuzja: Jak szybko zmiana jednego bitu wejściowego rozprzestrzenia się w stanie. Można to zilustrować wizualnie (np. po 1, 2, 4, 8 rundach).
    - Nieliniowość (operacja χ): Dlaczego jest kluczowa w ochronie przed atakami liniowymi i różnicowymi.
    - Rezystancja wobec Ataków: Krótka analiza, jak Keccak-f chroni przed:
        - Atakami różnicowymi (Differential Cryptanalysis).
        - Atakami liniowymi (Linear Cryptanalysis).
        - Atakami kryptoanalizy algebraicznej.
2. Omówienie i praktyczna weryfikacja, jak parametry stanu (np. Keccak-f[800], Keccak-f[400]) wpływają na bezpieczeństwo i wydajność.
3. Analiza konstrukcji Sponge, fazy absorbing i sqeezing, diagram blokowy
4. Zestawienie SHA-3 vs SHA-2

Praktyczna

- język: Python

1. Implementacja:

- implementacja samego Keccak-f: głównie implementacja funkcji permutacji P(S) (24 rundy operacji $\theta,\rho,\pi,\chi,\iota$) - użycie znanych wektorów testowych z dokumentacji Keccak aby sprawdzić czy działa 2. Wizualizacja i pomiar
  - zmienić 1 bit wejściowego stanu S
  - przeprowadzenie permutacji Keccak-f na obu stanach (S i S') i po każdej rundzie (lub co kilka rund) policzenie liczbę bitów, które się zmieniły (odległość Hamminga).
  - prezentacja na wykresie: liczba rund vs odległość Hamminga (powinien to być wykres rosnący)

2. Implementacja ataku kolizji na SHA-3 ze zrredukowaną ilością rund

Harmonogram

- 11 grudnia: Koncepcja, szczegóły Keccaka
- 15 stycznia: zbliżanie się do finału