SHA-3 Keccak-f

cpprhtn

2023-11-28

1 Keccak-f 함수 정의

1.1 Theta 함수 정의:

$$C[x] = A[x] \oplus A[x+5] \oplus A[x+10] \oplus A[x+15] \oplus A[x+20]$$

$$D[x] = C[(x+4) \mod 5] \oplus \text{ROTL64}(C[(x+1) \mod 5], 1)$$

$$A[x+5\cdot y] \doteq A[x+5\cdot y] \oplus D[x]$$

```
void theta(uint64 *A) {
    uint64 C[5], D[5];
    for (size_t i = 0; i < 5; i++) {
        C[i] = A[i] ^ A[i + 5] ^ A[i + 10] ^ A[i + 15] ^ A[i + 20];
    }

    for (size_t i = 0; i < 5; i++) {
        D[i] = C[(i + 4) % 5] ^ ROTL64(C[(i + 1) % 5], 1);
    }

    for (size_t i = 0; i < 5; i++) {
        for (size_t j = 0; j < 5; j++) {
            A[i + 5 * j] ^= D[i];
        }
    }
}
```

Listing 1: Theta 함수

1.2 Rho 함수 정의:

$$A[x] \doteq \text{ROTL64}(A[x], \text{RHO}[x])$$

```
void rho(uint64 *A) {
    for (size_t i = 0; i < 25; i++) {
        A[i] = ROTL64(A[i], RHO[i]);
    }
}
```

Listing 2: Rho 함수

1.3 Pi 함수 정의:

$$B[x] = A[y]$$

$$A[x] \doteq B[x]$$

```
void pi(uint64 *A) {
    uint64 B[25];
    for (size_t i = 0; i < 25; i++) {
        size_t x = i % 5;
        size_t y = (2 * i + 3 * (i / 5)) % 5;
        size_t index = 5 * x + y;
        B[index] = A[i];
    }
    memcpy(A, B, sizeof(B));
}
```

Listing 3: Pi 함수

1.4 Chi 함수 정의:

$$B[x] = A[x] \oplus (\neg A[5 \cdot x + ((y+1) \mod 5)] \wedge A[5 \cdot x + ((y+2) \mod 5)])$$

$$A[x] \doteq B[x]$$

```
void chi(uint64 *A) {
    uint64 B[25];
    for (size_t i = 0; i < 25; i++) {
        size_t x = i % 5;
        size_t y = (2 * i + 3 * (i / 5)) % 5;
        size_t index = 5 * x + y;
        B[index] = A[index] ^ ((~A[5 * x + ((y + 1) % 5)]) & A[5 * x + ((y + 2) % 5)]);
    }
    memcpy(A, B, sizeof(B));
}
```

Listing 4: Chi 함수

1.5 Iota 함수 정의:

$$A[0] \doteq A[0] \oplus \mathrm{RC}[\mathrm{round}]$$

```
void iota(uint64 *A, size_t round) {
    A[0] ^= RC[round];
}
```

Listing 5: Iota 함수

1.6 Keccak-f 함수 정의:

```
void keccakF(uint64 *A) {
    for (size_t round = 0; round < KECCAK_ROUNDS; round++) {
        theta(A);
        rho(A);
        pi(A);
        chi(A);
        iota(A, round);
    }
}
```

Listing 6: Iota 함수