ARMv8 Perk, caddq 함수 구현

김상원

https://youtu.be/pqxCLHCNMlo

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Caddq 함수

Caddq 함수 어셈블리

결과

Q & A

Caddq 함수

Perk₩Reference_Implementation₩perk-128-fast-3₩src₩arithmetic.c

```
#define PARAM_Q      1021 /**< Parameter q of the scheme */
```

```
static inline int16_t caddq(int16_t a) {
    a += (a >> 15U) & PARAM_Q;  // NOLINT(hicpp-signed-bitwise): behavior tested in unit tests
    return a;
}
```

```
static inline void caddq(int16_t *a, int size) {
    for (int i=0; i< size; i++){
        a[i] += (a[i] >> 15U) & PARAM_Q;
    }
}

extern void caddqq (int16_t *a, int16_t *b);
```

```
int16_t input[16];
```

```
int16_t output[8];
```

```
caddqq(input,output);
```

Caddq 함수 어셈블리

```
1  .globl caddqq
2  .globl _caddqq
3
4  caddqq:
5  _caddqq:
6
7  mov w3, #1021
8  dup v1.8h, w3
9
10
11 ld1 {v0.8h}, [x0],#16
12 ld1 {v0.8h}, [x0]
13 sshr v2.8h, v0.8h, #15
14 and v2.16b, v2.16b, v1.16b
15 add v2.8h, v2.8h, v0.8h
16 st1 {v2.8h}, [x1]
17
18
19 ret
```

결과

```
Benchmarking caddq function...
output : 800
output : 900
output : 1000
output : 1100
output : 1200
output : 1300
output : 1400
output : 1500
output : 0
output : 100
output : 200
output : 300
output : 400
output : 500
output : 600
output : 700
Total time for 10000 iterations: 0.000014 seconds
Average time per iteration: 0.000000001 seconds
Final output of caddq: 0
Final output of caddq: 100
Final output of caddq: 200
Final output of caddq: 300
Final output of caddq: 400
Final output of caddq: 500
Final output of caddq: 600
Total time for 10000 iterations: 0.000111 seconds
Average time per iteration: 0.000000011 seconds
Program ended with exit code: 0
```

```c
#include <time.h>

start = clock();

    for (int i = 0; i < TEST_LOOP; i++) {
        caddq(input, 7);
}
end = clock();
```

Q & A