ZKboo

Henrique José Carvalho Faria

03 21, 2022

Performance Report

Results

The first jasmin implementation of ZKBoo started with a performance deficit of 50 times the original C version. The following results and description explain the modifications undertaken during the process of increasing the jasmin performance beyond the current C version.

The most important modificiation conssisted of replacing the used arrays arrangement. In the first version the arrays were divided between players, and inside each player's part into rounds. In the new version the arrays were divided by rounds and only then by player.

In function commit the array w was filled by round instead of by player (Switched the while loops).

The resulting array went from:

$P_1(0-80)\ P_2(80-160)\ P_3(160-240) \Rightarrow R_1(0-3)\ R_2(3-6)\ ...\ R_{136}(237-240)$

Modified the mpc_ADD() function on the type of the variable i from u64 to inline int allowing the change on bit shifts in the get_bit/set_bit functions. Stopped using a while loop and started using shift directly.

From:

```
n = i;
while(n > 0) {
    x = x >> 1;
    n = n - 1;
}
```

To:

```
x = x >> i;
```

In function prove() the variables were accessed using u64 instead of u8.

Both jasmin functions H() and H3() share several functions. Regarding the function that

updates the data buffer using a 8-bit value at a time, it was split into two: one to update the buffer using 32-bit values at a time and another to update the buffer using 64-bit values at a time.

Phase	Encrypt									
	Shares_xor		Commit		H		H3		Prove	
	C	J	C	J	C	J	C	J	C	J
1	12	3	57572	686848	2217	13584	89	563	85	300
6	18	4	60781	51829	2051	11137	100	464	87	85

Table 1: Encrypt performance enhancement.