The following contents are provied by the authors of [54] (Zhang, M., Shi, T., Wu, W., Sui, H.: Optimized quantum circuit of AES with interlacing-uncompute structure. IEEE Transactions on Computers (2024))

Width:

Unfortunately, ProjectQ, like Q#, also suffers from similar issues when estimating width—it outputs conflicting width and depth optimizations. This appears to be related to the way parameters are passed. Below are two code simulations of QAND gates:

```
def QAND(eng, control1, control2, target):
    ancilla = eng.allocate_qureg(1)

    H | target
    CNOT | (control2, ancilla[0])
    CNOT | (target, control1)
    CNOT | (target, control2)
    CNOT | (control1, ancilla[0])
    Tdag | control1
    Tdag | control2
    T | target
    T | ancilla[0]
    CNOT | (control1, ancilla[0])
    CNOT | (target, control2)
    CNOT | (target, control1)
    CNOT | (control2, ancilla[0])
    H | target
    S | target
```

Fig. 1. Code1

```
def QAND(control1, control2, target, ancilla):
    H | target
    CNOT | (control2, ancilla)
    CNOT | (target, control1)
    CNOT | (target, control2)
    CNOT | (control1, ancilla)
    Tdag | control1
    Tdag | control2
    T | target
    T | ancilla
    CNOT | (control1, ancilla)
    CNOT | (target, control2)
    CNOT | (target, control1)
    CNOT | (control2, ancilla)
    H | target
    S | target
```

Fig. 2. Code2

The difference between the two lies in Code1's use of a new qubit called within the function as the ancilla qubit for QAND gate, while Code2 explicitly specifies the four registers. When we parallelly invoke these two types of QAND gates in the quantum circuit of the S-box, it leads to completely different width results. Taking the example of the S-box C*-circuit with T-depth 3:

```
Gate counts:
    Allocate : 166
    CX : 1109
    Deallocate : 66
    H : 305
    Measure^\dagger : 65
    S : 66
    T : 132
    T^\dagger : 132
    X : 75

Max. width (number of qubits) : 101.
depth_of_dag: 79
```

Fig. 3. Estimation results based on Code1.

```
Gate counts:
    Allocate : 129
    CX : 1109
    Deallocate : 29
    H : 305
    Measure^\dagger : 65
    S : 66
    T : 132
    T^\dagger : 132
    X : 75

Max. width (number of qubits) : 129.
depth_of_dag: 79
```

Fig. 4. Estimation results based on Code2.

The width estimation results in Fig. 4 are consistent with our previous findings. However, the result in Fig. 3 seems incorrect: in our T-depth-3 S-box circuit, there are a total of 28 parallel QAND gates in the third QAND-layer. Since each QAND gate requires 4 qubits, the width of the circuit should be at least $28 \times 4 = 112$.

We attempt to illustrate this issue because the ProjectQ code in [28] is based on the QAND implementation in Fig. 1 (see: GitHub - QunLiu-sdu/Improved-Quantum-Circuits-for-AES: This is the code for the paper: Improved Quantum Circuits for AES: Reducing the Depth and

the Number of Qubits accepted by ASIACRYPT 2023.). Therefore, we remain skeptical about their width conclusions.

However, even when specifying the registers used by the function, there are still issues with the width estimation results in the case of multi-level nested calls. Therefore, for the width parameter, we choose to rely on manually estimated results.