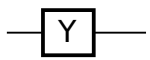
Intervenants

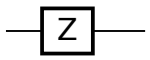
- **Benoît Valiron** (responsable du cours - benoit.valiron@centralesupelec.fr - remplacé par BM)
- **Bertrand Marchand** (bertrand.marchand@lix.polytechnique.fr - TP 1)
- **Simon Martiel** (simon.martiel@atos.net - TP 2)

Usual gates

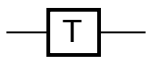
Hadamard  $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

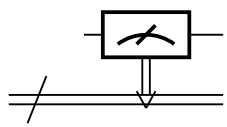
Pauli-X  $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

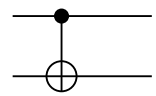
Pauli-Y  $\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$

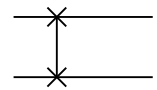
Pauli-Z  $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$

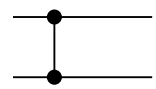
Phase  $\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$

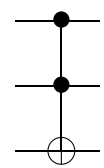
$\pi/8$  $\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

measurement 

controlled-X  $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

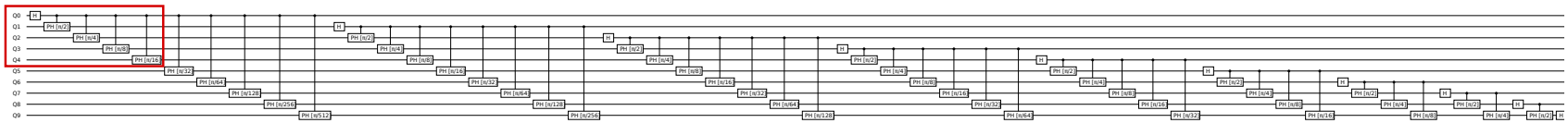
swap  $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$

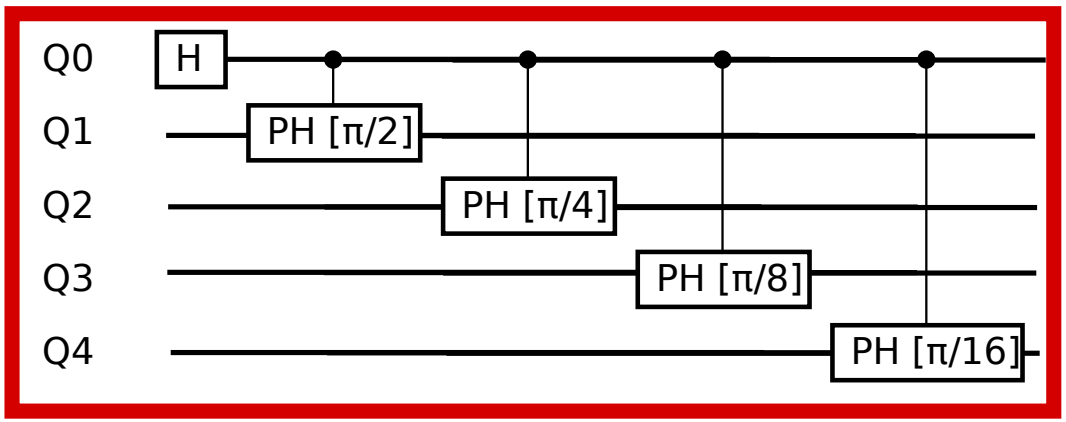
controlled-Z  $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix}$

Toffoli 

$$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$$

Example of a quantum circuit: QFT





Oracle for SHA256

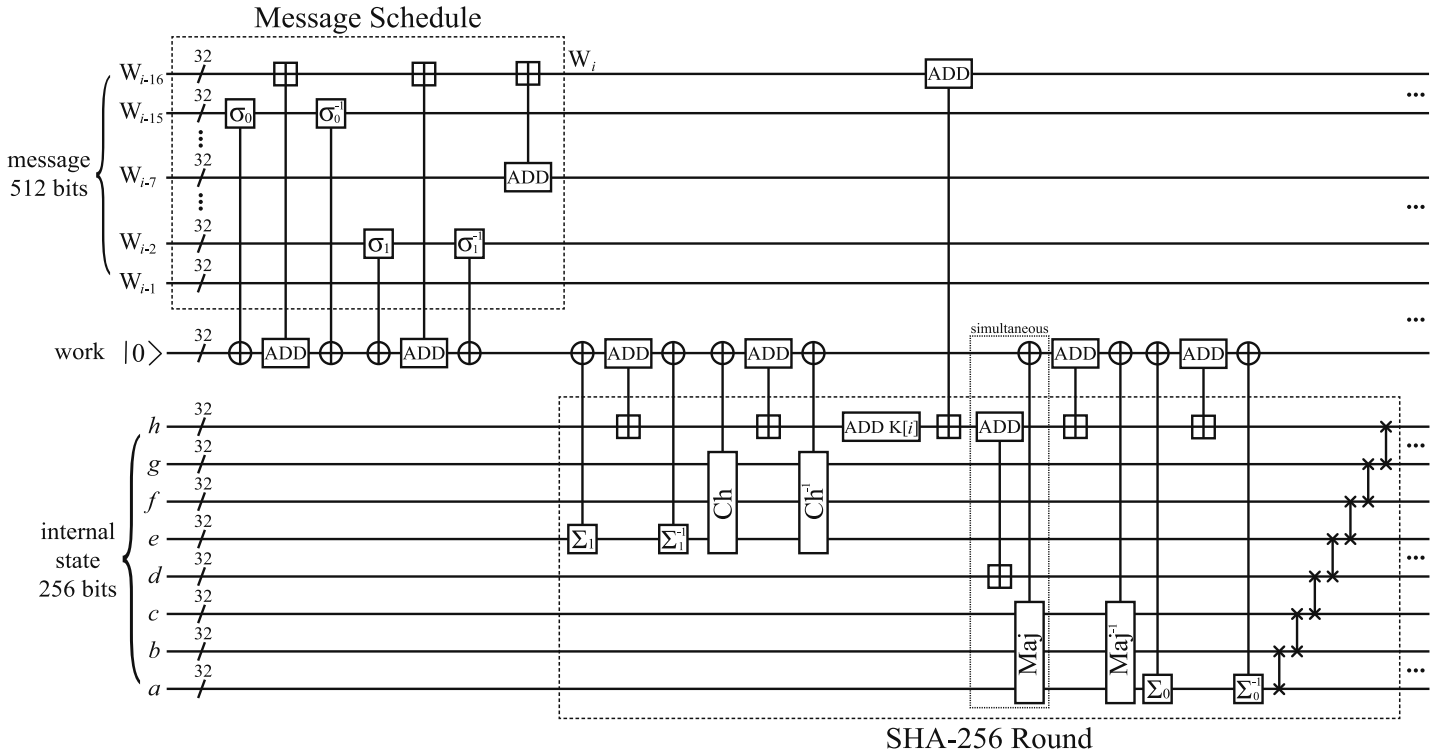


Fig. 10 Reversible circuit for serial implementation of SHA-256 message schedule and round function. The message block consisting of 16 words is recursively updated in place. Note that it is straightforward to make message schedule and round functions work in parallel by expanding the work space. Seven two-qubit gates at the end of round are SWAP gates. The symbol $\boxplus$ is addition modulo 2^{32}

from *Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2*, Kim et al., 2018.

Overview of quantum algorithms

- **Quantum search algorithms** Use $O(\sqrt{N})$ calls to an oracle O_f to identify elements with $f(x) = 1$ in a list of N elements.
  $\rightarrow$ generalizations: **quantum walks**
- **QFT-based algorithms**
  - **Shor's algorithm** to factor integers and other **order-finding algorithms**
  - **Quantum chemistry** (and the solving of other Physics/Chemistry problems) through phase estimation.
  - **Quantum linear algebra** and machine learning or other applications.