# 1 Implementation

In this section we present an implementation of hash function using the three parallel call block cipher based compression function. The implementation uses a four-core Intel Westmere CPU and makes use of the AES instruction set [**?**]. Finally we use cycles per bytes to benchmark our implementation and we compare it with the other implementation that used only two parallel call of a block cipher. The measure are done as described in [**?**].

## 1.1 Overview

To implement the hash function by making use of the block cipher based compression function we apply the Merkle-Damgård construction.

## 1.2 Parallelization

Let us describe more in detailed how we parallelized the hash function over a four-core CPU.

## 1.3 Benchmarking