Abstract: The present thesis analyses the proposal of CubeHash with special emphasis on the following papers: “Inside the Hypercube” [1], “Symmetric States and Their Improved Structure” [7] and “Linearisation Framework for Collision Attacks” [6]. The CubeHash algorithm is presented in a concise manner together with a proof that the CubeHash round function $R : \{0,1\}^{32} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ is a permutation. The results of [1] and [7] concerning the CubeHash symmetric states are reviewed, corrected and substantiated by proofs. More precisely, working with a definition of $D$-symmetric state, based on [7], the thesis proves both that for $V = \mathbb{Z}_2^4$ and its linear subspace $D$, there are $2^{2^{16}}$ $D$-symmetric states and an internal state $x$ is $D$-symmetric if and only if the state $R(x)$ is $D$-symmetric. In response to [1], the thesis presents a step-by-step computation of a lower bound for the number of distinct symmetric states, explains why the improved preimage attack does not work as stated and gives a mathematical background for a search for fixed points in $R$. The thesis further points out that the linearisation method from [6] fails to consider the equation $(A \oplus \alpha) + \beta = (A + \beta) \oplus \alpha$ ($\ast$), present during the CubeHash iteration phase. Necessary and sufficient conditions for $A$ being a solution to ($\ast$) are formulated and proven, their implications discussed.