

Clover is a hash algorithm that's based on rhodonea curves. The algorithm supports outputs of varying sizes.

A description of the algorithm follows.

Let **B**, **H**, and **R** be arrays of **N** bytes, where $32 \leq N \leq 128$. Let **a** and **p** be arrays of $N / 8$ 64-bit unsigned integers.

1. Convert **B** into a set of 64-bit unsigned integers. Let **a** represent the integer set.
2. For **h** in (13, 26, 39, ..., 75):
 1. For **i** in (0, 1, ..., $N / 8$):
 1. Set **b** to $a_i / (\max(64\text{-bit unsigned integer})) * h * \pi$.
 2. Set x_0 to $\max(64\text{-bit unsigned integer}) * \cos(b * h) * \cos(b) / 2$.
 3. Set y_0 to $\max(64\text{-bit unsigned integer}) * \cos(b * h) * \sin(b) / 2$.
 4. Set **x** to $\text{round}(\text{ceiling}(x_0))$.
 5. Set **y** to $\text{round}(\text{ceiling}(y_0))$.
 6. Set p_i to $x \wedge y$.
 7. Set a_i to p_i .
 2. Let **H** represent the output hash. Compute H_i as follows ($0 \leq i < N$, $0 \leq j < N / 8$):
 1. $H_i = a_j$.
 2. $H_i = a_j \ll 11$.
 3. $H_i = a_j \ll 13$.
 4. $H_i = a_j \ll 17$.
3. Store **p** into **R**.
4. Recompute **H** as follows:
 1. $H_i \wedge= R_i$.