TTP   **FO**

1. Chooses *Salt* and calculates
   Salted = Salt XOR R_r

$$\xrightarrow{\{Salted, C_r\}}$$

2. Calculates R_r and
   Salt = Salted XOR R_r,
   and stores *Salt*

3. Chooses C_{i+1}

$$\xrightarrow{C_{i+1}}$$

4. Calculates R_{i+1} and
   $Salted_{R_{i+1}} = Salt\ XOR\ R_{i+1}$

$$\xleftarrow{Salted_{R_{i+1}}}$$
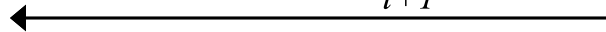
5. Calculates
   $R_{i+1} = Salt\ XOR\ Salted_{R_{i+1}}$,
   and stores $\{C_{i+1}, R_{i+1}\}$