$$
\begin{aligned}
CA_i \oplus CX_i &= \mod (PA_i^* + t \times u_i) \oplus u_i \\
&\oplus \mod (PA_i^*, 256) \oplus u_i
\end{aligned} \tag{1}
$$