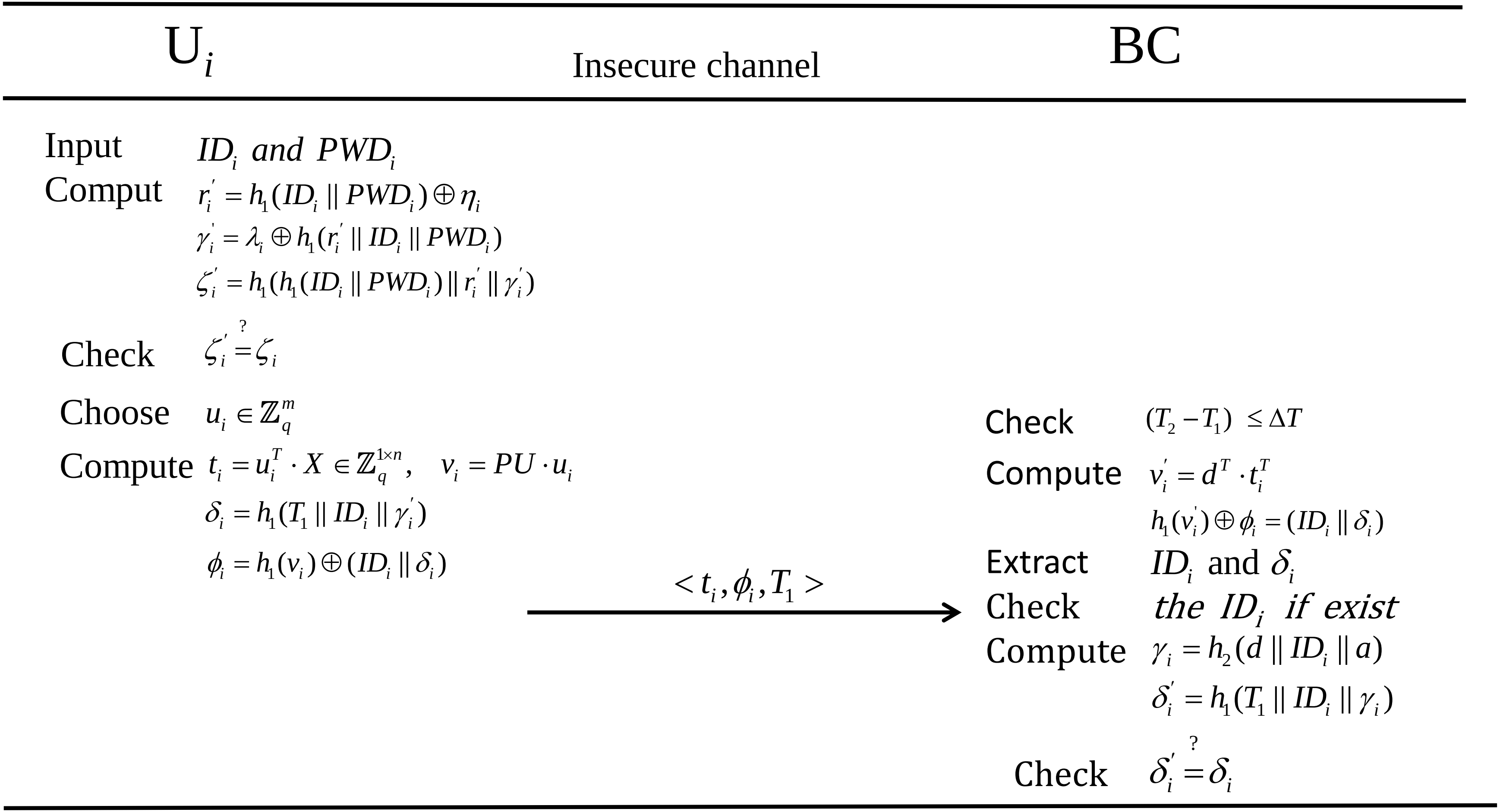

U_i

Insecure channel

BC

Input ID_i *and* PWD_i

Comput $r_i' = h_1(ID_i \| PWD_i) \oplus \eta_i$

$\gamma_i' = \lambda_i \oplus h_1(r_i' \| ID_i \| PWD_i)$

$\zeta_i' = h_1(h_1(ID_i \| PWD_i) \| r_i' \| \gamma_i')$

Check $\zeta_i' \overset{?}{=} \zeta_i$

Choose $u_i \in \mathbb{Z}_q^m$

Compute $t_i = u_i^T \cdot X \in \mathbb{Z}_q^{1\times n}, \quad v_i = PU \cdot u_i$

$\delta_i = h_1(T_1 \| ID_i \| \gamma_i')$

$\phi_i = h_1(v_i) \oplus (ID_i \| \delta_i)$

$$\xrightarrow{< t_i, \phi_i, T_1 >}$$

Check $(T_2 - T_1) \le \Delta T$

Compute $v_i' = d^T \cdot t_i^T$

$h_1(v_i') \oplus \phi_i = (ID_i \| \delta_i)$

Extract ID_i and δ_i

Check *the* ID_i *if exist*

Compute $\gamma_i = h_2(d \| ID_i \| a)$

$\delta_i' = h_1(T_1 \| ID_i \| \gamma_i)$

Check $\delta_i' \overset{?}{=} \delta_i$