$\mathcal{A}_m(K_{pub}^m, K_{pri}^m)$

$\mathcal{A}_{m+1}(K_{pub}^{m+1}, K_{pri}^{m+1})$

A) $\mathcal{A}_m$ Send attack mode vote $\mathcal{V}_m$ to $\mathcal{A}_{m+1}$

B) $\mathcal{A}_{m+1}$ Collect all vote $\mathcal{V}_{m\in G}$ determine attack mode m_t

I

C) $\mathcal{A}_m$ calculate uncertainty score u_{tar}^m of x_{tar}^m

D) $\mathcal{A}_m$ evaluate attack value of x_{tar}^m

E) $\mathcal{A}_m$ send high attack value uncertainty score u_{tar}^m

II

F) $\mathcal{A}_m$ randomly selects a large random number x

G) $\mathcal{A}_m$ calculates $E(K_{pub}^m, x) - u_{tar}^m$ send to $\mathcal{A}_{m+1}$

III

H) $\mathcal{A}_{m+1}$ Select N numbers
and randomly select a large prime number P

$y_u = D(E(x) - i + u), u = 1,2, \ldots . N$

$z_u = y_u \bmod p, u = 1,2, \ldots . N$

IV

I) $\mathcal{A}_{m+1}$ Verify if $0 \le a \ne b \le N - 1$
Satify $||z_a - z_b|| \ge 2$

V

J) $\mathcal{A}_{m+1}$ send $p\ z_u, u = 1, \ldots N$ to $\mathcal{A}_m$

VI

K) $\mathcal{A}_m$ verify if $z_i \equiv mod\ p$
then $u_{tar}^m \le u_{tar}^{m+1}$ else $u_{tar}^m \ge u_{tar}^{m+1}$

VII

Local Computation **Message Sending**