



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



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

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

II

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

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
 $y_u = D(E(x) - i + u), u = 1, 2, \dots, N$
 $z_u = y_u \bmod p, u = 1, 2, \dots, N$

IV

I) \mathcal{A}_{m+1} Verify if $0 \leq a \neq b \leq N - 1$
Satisfy $||z_a - z_b|| \geq 2$

V

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

VI

K) \mathcal{A}_m verify if $z_i \equiv \bmod p$
then $u_{tar}^m \leq u_{tar}^{m+1}$ else $u_{tar}^m \geq u_{tar}^{m+1}$

VII

--- ➔ Local Computation ➔ Message Sending