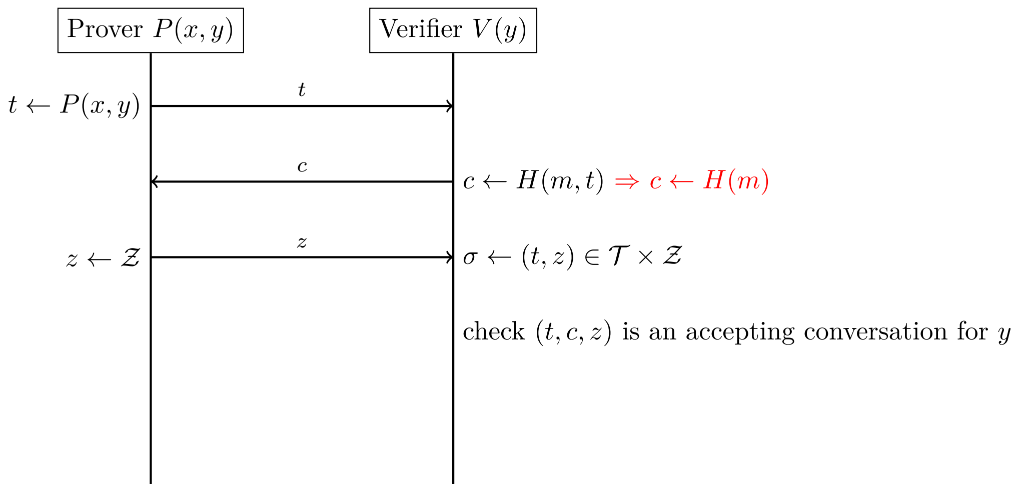
CSCI968 Advance Network Security: Assignment #2

Mei Wangzhihui 2019124044

Problem 1

Fiat-Shamir signature scheme

$pk = y \in \mathcal{Y}, sk = (x, y) \in \mathcal{R}$

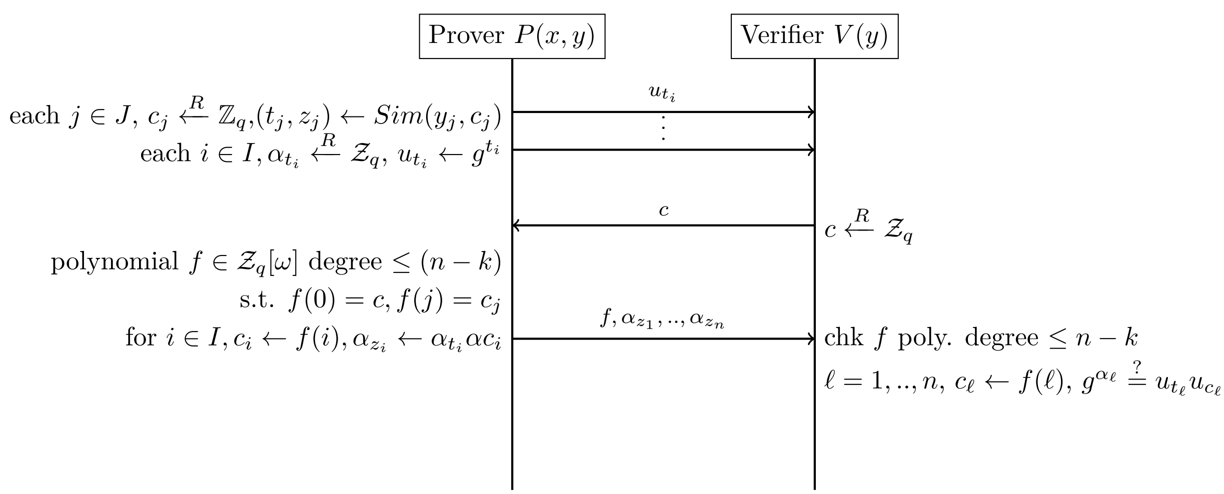


t from prover is used to generate c, If the simulator has an legal pair (t, c, z) it can hash any message $c_i = H(m_i)$ by itself. The (t, c_i, z_i) can be accepted. It is insecure. so the probability of obtaining secret key α is not negligible.

Problem 2

OR-proof

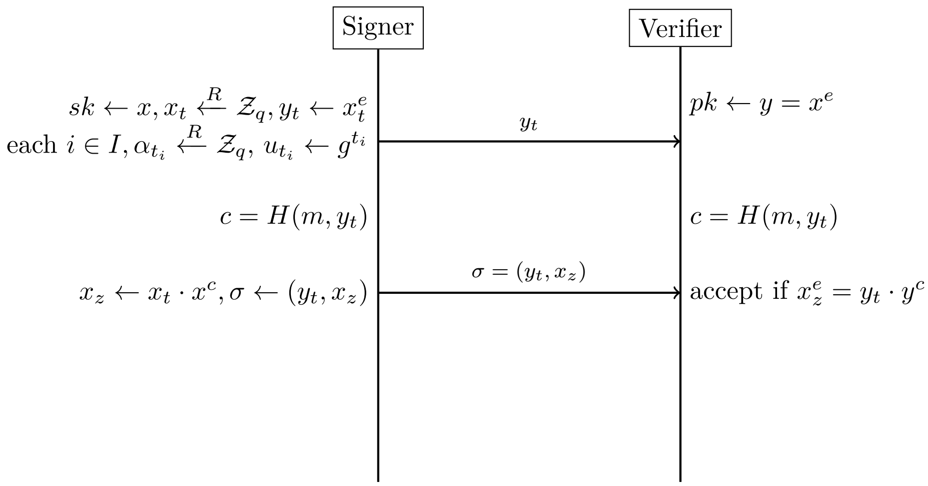
$((x_1, x_2, .., x_n), (y_1, y_2, .., y_n)) \in ((\mathcal{X} \cup \perp)^n \times \mathcal{Y}^n) : |i \in \{1, ..., n\} : (x_i, y_i) \in \mathcal{R}| \geq k$



Problem 3

GQ signature scheme

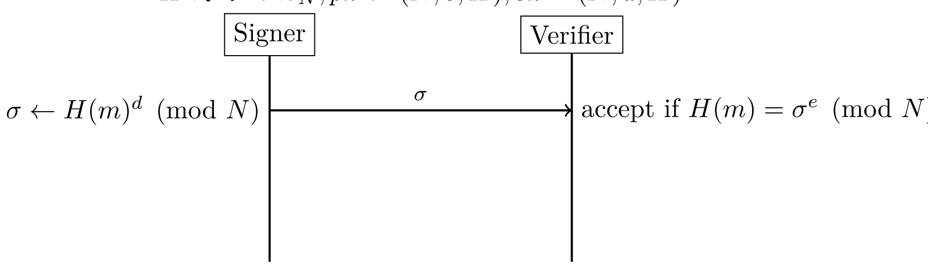
$x \xleftarrow{R} \mathcal{Z}_q, y \leftarrow x^e pk = y, sk = (x, y)$



RSA Full Domain Hash

$G() : N = pq, e \cdot d = 1 mod \varphi(N)$

$H : \mathcal{M} \rightarrow \mathcal{Z}_N, pk \leftarrow (N, e, H), sk = (N, d, H)$



Fiat-Shamir heuristic GQ signature doesn't need the involvement of d, thus no need of computing it. The Fiat-Shamir heuristic GQ signature is more efficient than RSA-FDH signature.