CO21BTECH11002
Aayush Kumar
Assignment 2

1) Known: g, g^{α}, g^{β}

Given: $A \to A(g^{\alpha}) = g^{1/\alpha}$

We perform the following operations:-

$g_1 = g^{\alpha} \cdot g = g^{\alpha+1}$ $\quad$ $g_2 = g^{\beta} \cdot g = g^{\beta+1}$

$g_3 = A(g_1) = g^{\frac{1}{\alpha+1}}$ $\quad$ $g_4 = A(g_2) = g^{\frac{1}{\beta+1}}$

$g_5 = g_3 g_4 = g^{\frac{1}{\alpha+1} + \frac{1}{\beta+1}} = g^{\frac{\alpha+\beta+2}{1+\alpha+\beta+\alpha\beta}}$

$g_6 = A(g_5) = g^{\frac{1+\alpha+\beta+\alpha\beta}{\alpha+\beta+2}}$

$g_7 = g_6 \cdot g^{-1} = g^{\frac{\alpha\beta-1}{\alpha+\beta+2}}$

$g_8 = g^{\alpha} \cdot g^{\beta} \cdot g^{2} = g^{\alpha+\beta+2}$

$g_9 = A(g_8) = g^{\frac{1}{\alpha+\beta+2}}$

$g_{10} = g_7 \cdot g_9 = g^{\frac{\alpha\beta}{\alpha+\beta+2}}$

$g_{11} = A(g_{10}) = g^{\frac{\alpha+\beta+2}{\alpha\beta}} = g^{\frac{1}{\alpha}+\frac{1}{\beta}+\frac{2}{\alpha\beta}}$

$g_{12} = A(g^{\alpha}) = g^{1/\alpha}$ $\quad$ $g_{13} = A(g^{\beta}) = g^{1/\beta}$

$g_{14} = g_{11} \cdot g_{12}^{-1} \cdot g_{13}^{-1} = g^{2/\alpha\beta}$

$g_{15} = A(g_{14}) = g^{\frac{\alpha\beta}{2}}$

$$\boxed{g_{16} = g_{15}^{\,2} = g^{\alpha\beta}}$$

2) $e = 3$, $N_1 < N_2 < N_3$

Ciphertext :- $(r^3 \bmod N_1,\ r^3 \bmod N_2,\ r^3 \bmod N_3,\ H(r) \oplus m)$

If for any pair of N_1, N_2, N_3, their gcd is not equal to 1, the adversary will be able to factorize the pair and hence calculate r.

If for any pair (N_i, N_j), $\gcd(N_i, N_j) = 1$ then we have the following equations :-

$$r^3 \% N_1 = m_1$$
$$r^3 \% N_2 = m_2$$
$$r^3 \% N_3 = m_3$$

The system can be solved to obtain solutions of the form

$r^3,\ r^3 + N_1N_2N_3,\ r^3 + 2N_1N_2N_3, \ldots$

So we take the ~~sm~~ smallest solution and find r from it.

Knowing r, ~~an~~ adversary can now find m as $H(r) \oplus (H(r) \oplus m) = m$.

3) $\text{Sign}(i) = f^{(n-i)}(x)$

- $f^{(n)}(x) \rightarrow$ public

a) To verify sign(i), the receiver can apply the function f to Sign(i) i times. If $f^{(i)}(\text{Sign}(i)) = f^{n}(x)$ then the signature is valid, since

$$f^{i}(f^{(n-i)}(x)) = f^{(n)}(x)$$

b) The scheme is not one time secure since knowing Sign(i), an adversary can find Sign(i-1), Sign(i-2), ... & Sign(0).

$$\text{Sign}(i-1) = f^{(n-i+1)}(x) = f(f^{(n-i)}(x))$$
$$= f(\text{Sign}(i))$$

$$\text{Sign}(i-2) = f(\text{Sign}(i-1))$$

And so on.

4)

a) For the scheme to be one-time secure, value of K should be such that total no. of possible susets of $2t$ keys should be greater than or equal to message space size.

Hence, $\boxed{{}^{2t}C_K \geq 2^n}$

b) $2^n \leq {}^{2t}C_K$

For max value of n, $K = t$ since ${}^{2t}C_K$ achieves max value at $K = t$

$\Rightarrow \quad 2^n = {}^{2t}C_t$

$$\Rightarrow \boxed{n = \log_2 {}^{2t}C_t}$$