CS6160 Assignment 2

Gautam Singh
CS21BTECH11018

1) Note that

$$B\left(g^{\alpha}\right) \triangleq g^{\alpha^2} = g^{\alpha^2+\alpha-\alpha} \tag{1}$$
$$= \frac{g^{\alpha(\alpha+1)}}{g^{\alpha}} \tag{2}$$
$$= \frac{A\left(g^{\frac{1}{\alpha(\alpha+1)}}\right)}{g^{\alpha}} \tag{3}$$
$$= \frac{1}{g^{\alpha}}A\left(\frac{g^{\frac{1}{\alpha}}}{g^{\frac{1}{\alpha+1}}}\right) \tag{4}$$
$$= \frac{1}{g^{\alpha}}A\left(\frac{A\left(g^{\alpha}\right)}{A\left(g^{\alpha+1}\right)}\right) \tag{5}$$

can be computed since g, p, q, g^{α} are known. From (5), we compute

$$C\left(g^{\alpha}, g^{\beta}\right) \triangleq \frac{B\left(g^{\alpha+\beta}\right)}{B\left(g^{\alpha}\right)B\left(g^{\beta}\right)} \tag{6}$$
$$= g^{(\alpha+\beta)^2-\alpha^2-\beta^2} = g^{2\alpha\beta}. \tag{7}$$

Finally, we compute using (7),

$$F\left(g^{\alpha}, g^{\beta}\right) \triangleq A\left(\left(A\left(C\left(g^{\alpha}, g^{\beta}\right)\right)\right)^2\right) \tag{8}$$
$$= A\left(\left(A\left(g^{2\alpha\beta}\right)\right)^2\right) \tag{9}$$
$$= A\left(g^{\frac{1}{\alpha\beta}}\right) = g^{\alpha\beta}. \tag{10}$$

2) Using the *Chinese Remainder Theorem*, we can solve the system of congruences

$$r^3 \equiv c_1 \pmod{N_1} \tag{11}$$
$$r^3 \equiv c_2 \pmod{N_2} \tag{12}$$
$$r^3 \equiv c_3 \pmod{N_3} \tag{13}$$

modulo $N_1N_2N_3$, since the N_i are pairwise coprime (if this was not the case, then the RSA public keys could be factored out by taking a GCD). Further, since $r \in \mathbb{Z}_{N_1}$, we have $r < N_1 < N_2 < N_3$, we have $r^3 < N_1N_2N_3$, thus our unique solution is indeed equal to r^3. Taking a cube root of this solution gives us r.
Having found r, we can now compute $H(r)$ and recover $H(r) \oplus (H(r) \oplus m) = m$.

3) a) Given $(i, \mathrm{Sign}(i)) = \left(i, f^{(n-i)}(x)\right)$, the receiver can verify the signature by computing

$$f^{(i)}\left(f^{(n-i)}(x)\right) = f^{(n)}(x) \tag{14}$$

and verifying that it is equal to the public key. If not, then the signature is invalid for the given i.

b) Notice that when $f^{(n-i)}(x)$ is computed, from the above, we also compute the values of $f^{(j)}(x)$ for $n-i \leq j \leq n$. Setting $i = n$, we see that we obtain $f^{(i)}(x)$ for all $1 \leq i \leq n$, hence we can forge every message in $\mathcal{M}$ after knowing the tag for message n.

4) a) For the scheme to be one-time secure, f must be *subset-free*, that is, there do not exist $m_1 \neq m_2$ such that $f(m_1) \subset f(m_2)$. Since f maps messages to subsets of size k, it follows that no two images can be subsets of each other. Thus, for being subset-free, we must have

$$2^n \leq \binom{2t}{k}. \tag{15}$$

Hence, the values of k are

$$S_k = \left\{k : k \in \{0, 1, \ldots, 2t\},\ 2^n \leq \binom{2t}{k}\right\}. \tag{16}$$

b) From (15), we have

$$2^n \leq \binom{2t}{k} \leq \binom{2t}{t}. \tag{17}$$

Asymptotically, for large t,

$$2^n \leq \frac{4^t}{\sqrt{\pi t}} \tag{18}$$

$$\implies n \leq 2t - \frac{1}{2}\log(\pi t) \tag{19}$$

$$= \mathcal{O}(t - \log t)\,. \tag{20}$$