Cryptosystem 7.7: Full Domain Hash

Let $k$ be a positive integer; let $\mathcal{F}$ be a family of trapdoor one-way permutations such that $f : \{0, 1\}^k \rightarrow \{0, 1\}^k$ for all $f \in \mathcal{F}$; and let $G : \{0, 1\}^* \rightarrow \{0, 1\}^k$ be a "random" function. Let $\mathcal{P} = \{0, 1\}^*$ and $\mathcal{A} = \{0, 1\}^k$, and define

$$\mathcal{K} = \{(f, f^{-1}, G) : f \in \mathcal{F}\}.$$

Given a key $K = (f, f^{-1}, G)$, $f^{-1}$ is the private key and $(f, G)$ is the public key.

For $K = (f, f^{-1}, G)$ and $x \in \{0, 1\}^*$, define

$$\text{sig}_K(x) = f^{-1}(G(x)).$$

A signature $y = (y_1, \ldots, y_k) \in \{0, 1\}^k$ on the message $x$ is verified as follows:

$$\text{ver}_K(x, y) = \text{true} \iff f(y) = G(x).$$
Algorithm 7.2: FDH-\textsc{Invert}(z_0, q_h)

\begin{verbatim}
external f

procedure SIMG(x)
    if j > q_h
        then return ("failure")
    else if j = j_0
        then z ← z_0
    else let z ∈ \{0, 1\}^k be chosen at random
    j ← j + 1
    return (z)

main
    choose j_0 ∈ \{1, ..., q_h\} at random
    j ← 1
    insert the code for FDH-\textsc{Forge}(f) here
    if FDH-\textsc{Forge}(f) = (x, y)
        then \{ if f(y) = z_0
                     then return (y)
                     else return ("failure") \}
    \end{verbatim}

THEOREM 7.2 Suppose there exists an algorithm FDH-\textsc{Forge} that will output an existential forgery for Full Domain Hash with probability \(\epsilon > 2^{-k}\), using a key-only attack. Then there exists an algorithm FDH-\textsc{Invert} that will find inverses of random elements \(z_0 \in \{0, 1\}^k\) with probability at least \((\epsilon - 2^{-k})/q_h\).