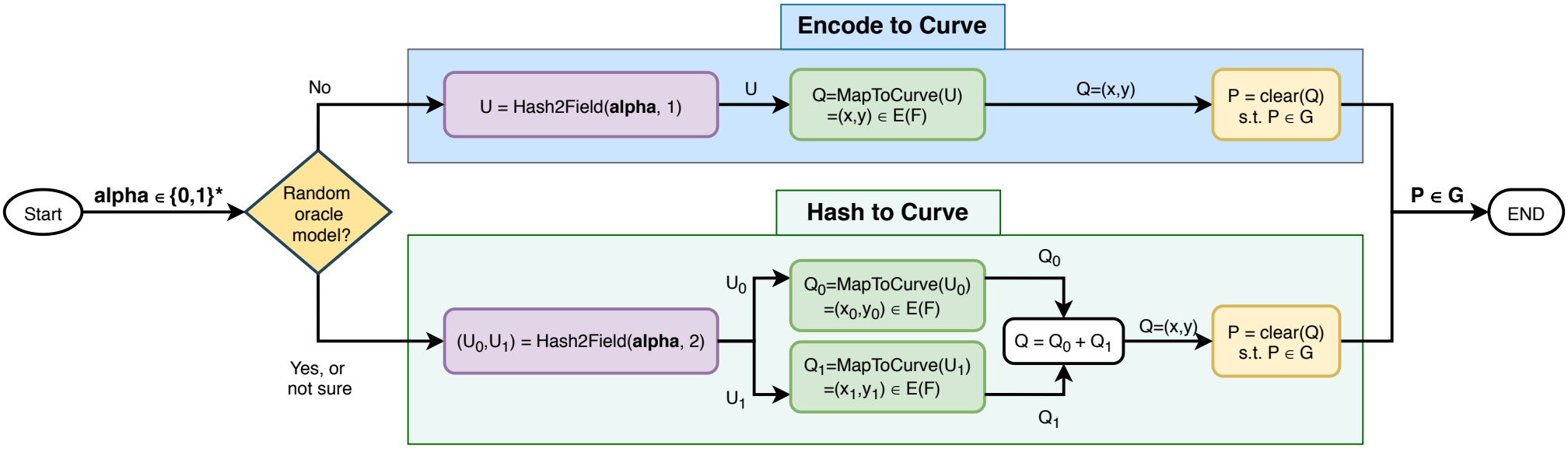
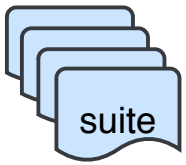
Hashing to Elliptic Curves

https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/

A. Faz-Hernandez, S. Scott, N. Sullivan, R. S. Wahby, C. A. Wood.



A **suite** is a concrete set of algorithms and parameters for an elliptic curve group.



The document provides a set of suites for encoding or hashing messages into elliptic curve points.

Parameters

(F, q, p, m) : A finite field of characteristic p and q=p^m elements.
(E, n) : An elliptic curve E defined over F with n points.
(r, h, h') : Let n=h*r, where r is the order of prime subgroup, h is the cofactor, and h' is a multiple of h.
(G) : Group (or subgroup) of E(F).
(H, b) : A cryptographic hash function H that outputs b bits.