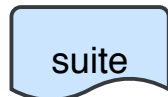
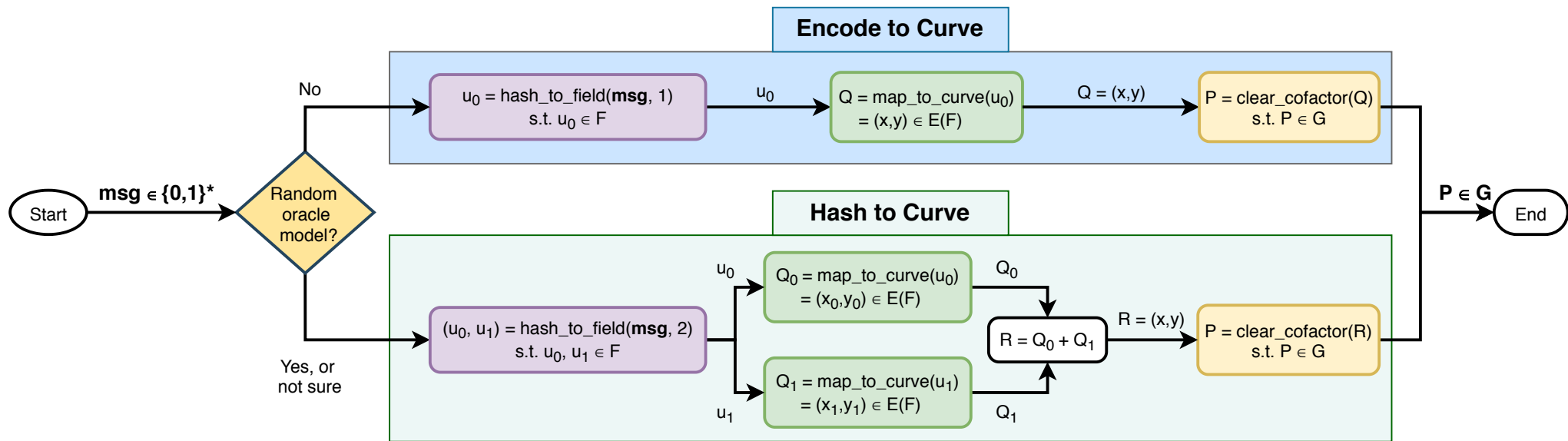


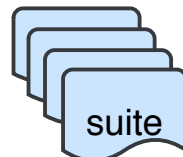
# Hashing to Elliptic Curves

<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

$F$  : A finite field.

$E$  : An elliptic curve  $E$  defined over  $F$ .

$E(F)$  : The group of points generated by  $E$ .

$G$  : A prime order subgroup of  $E(F)$ .