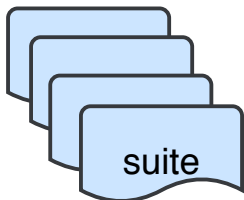
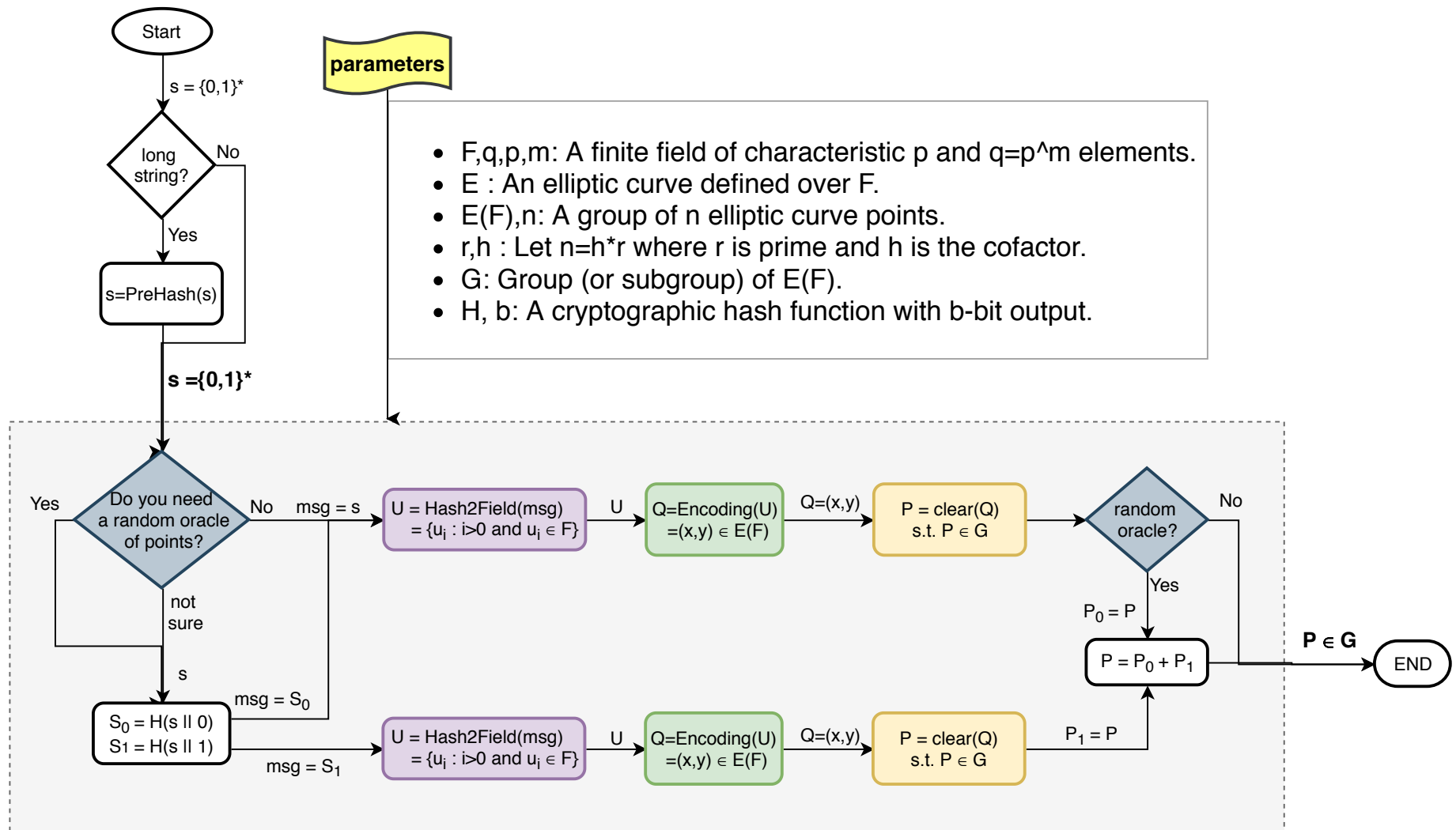


Hashing to Elliptic Curve Points

$f : \{0,1\}^* \rightarrow G$



<https://tools.ietf.org/html/draft-irtf-cfrg-hash-to-curve-03>

- Document provides a set of suites for hashing to curve.
- Each **suite** is a specification of algorithms and parameters for a particular elliptic curve group.
- Elliptic curve groups not covered can define suites following these recommendations.