Abstract. Constructive cryptography, an alternative paradigm for designing cryptographic protocols and proving their security, is reviewed in this talk and contrasted with other approaches. In constructive cryptography, a cryptographic scheme (e.g. encryption) is seen as constructing a certain resource (e.g. a secure channel) from another resource (e.g. an authenticated channel and a secret key), for a well-defined notion of construction. The construction notion is composable, which allows to design complex protocols in a modular, layered manner. The security proofs of the modules (e.g. encryption, authentication, key agreement, or signatures) directly compose to a security proof for the entire protocol. A treatment in constructive cryptography comes with several advantages, among them:

- Simplicity and reusability due to the modular design.
- The semantics of security definitions are clear in the sense that one knows how a scheme satisfying a given definition can be used. This allows to compare security definitions.
- The treatment is at an abstract level, freed from artefacts like Turing machines, asymptotics, polynomial-time, communication tapes, etc.
- Information-theoretic and computational security are different instantiations of the same security statement.
- It appears better amenable to a treatment by formal methods.