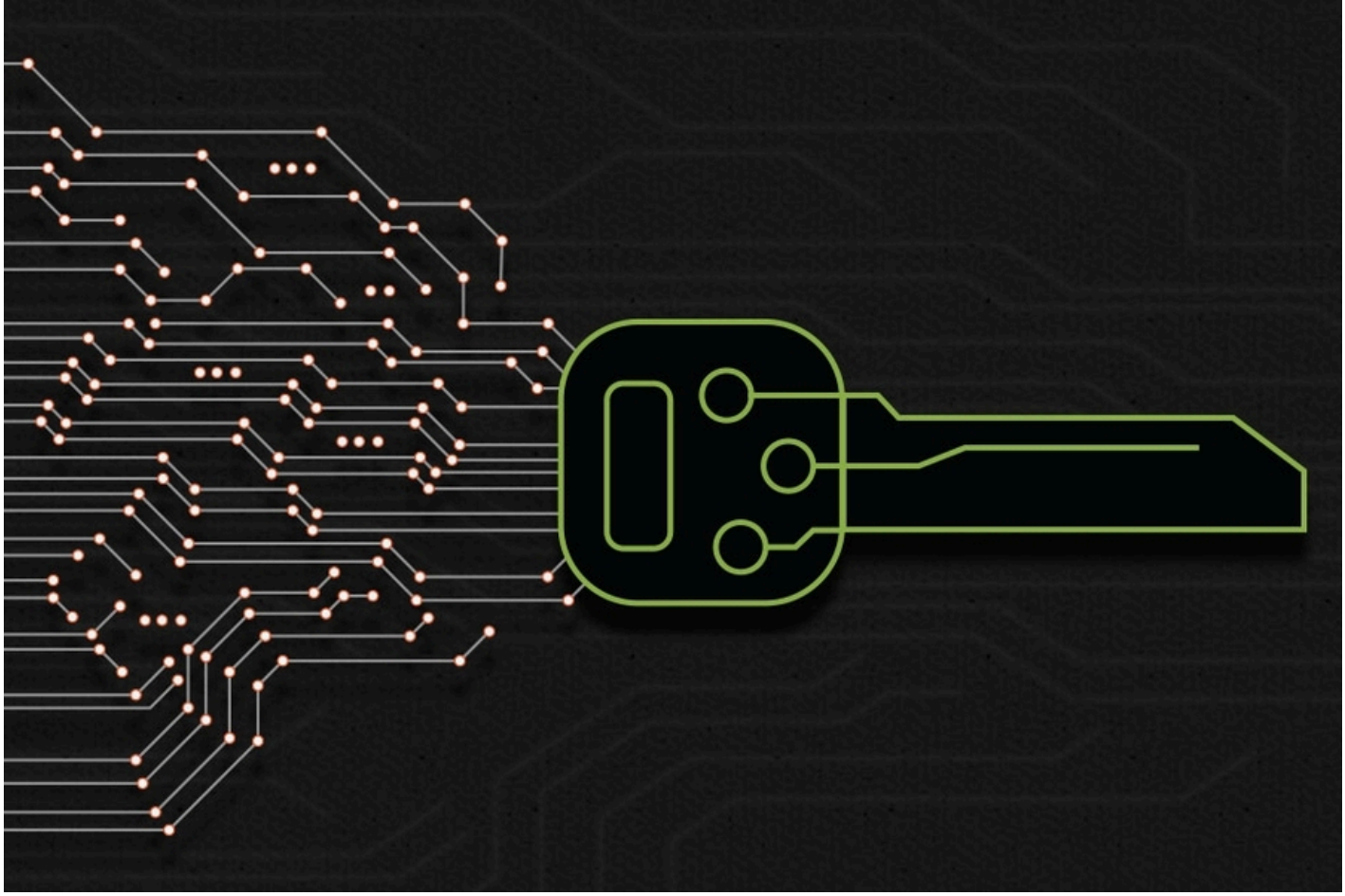

Encrypted Systems

EECS 498/598, Winter 2022

Instructor: Paul Grubbs (www.paulgrubbs.net)

Computer systems play a central role - both positive and negative - in our society. They are used to help heal people, but also harass them; for teaching, but also transmitting misinformation; democracy, but also demagoguery; privacy, but also pervasive surveillance; connection, but also control.

Because of this, it is vital to ask how we can design computer systems that are difficult, or impossible, to misuse for ill ends. Cryptography offers a powerful set of theoretical tools - encryption, digital signatures, multi-party computation, zero-knowledge proofs, blockchains, and more - that can be applied to build misuse-resistant *encrypted systems*. Integrating cryptography into systems is challenging, and raises mathematical, engineering, social, and ethical questions.

The aim of this course is fourfold: first, to understand the cryptographic tools that have proven useful in encrypted systems, and how to design new ones; second, to study how encrypted systems have used them (successfully or not); third, to identify "design patterns" for encrypted systems; fourth, to navigate the complex ethical questions that can arise in encrypted systems research.

Advised prerequisites: 475/575 or 388