Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

Kurzes Inhaltsverzeichnis

→

Kryptographische Eignung elliptischer Kurven:

K22: Elliptische Kurven über $\mathbb{Q}$ und $\mathbb{C}$
K23: Elliptische Kurven über endlichen Körpern
K24: Der Schoof-Algorithmus
K25: Sichere Kryptographie mit elliptischen Kurven
K26: El Gamal für elliptische Kurven, ECDSA
K27: Angriffe auf ECC