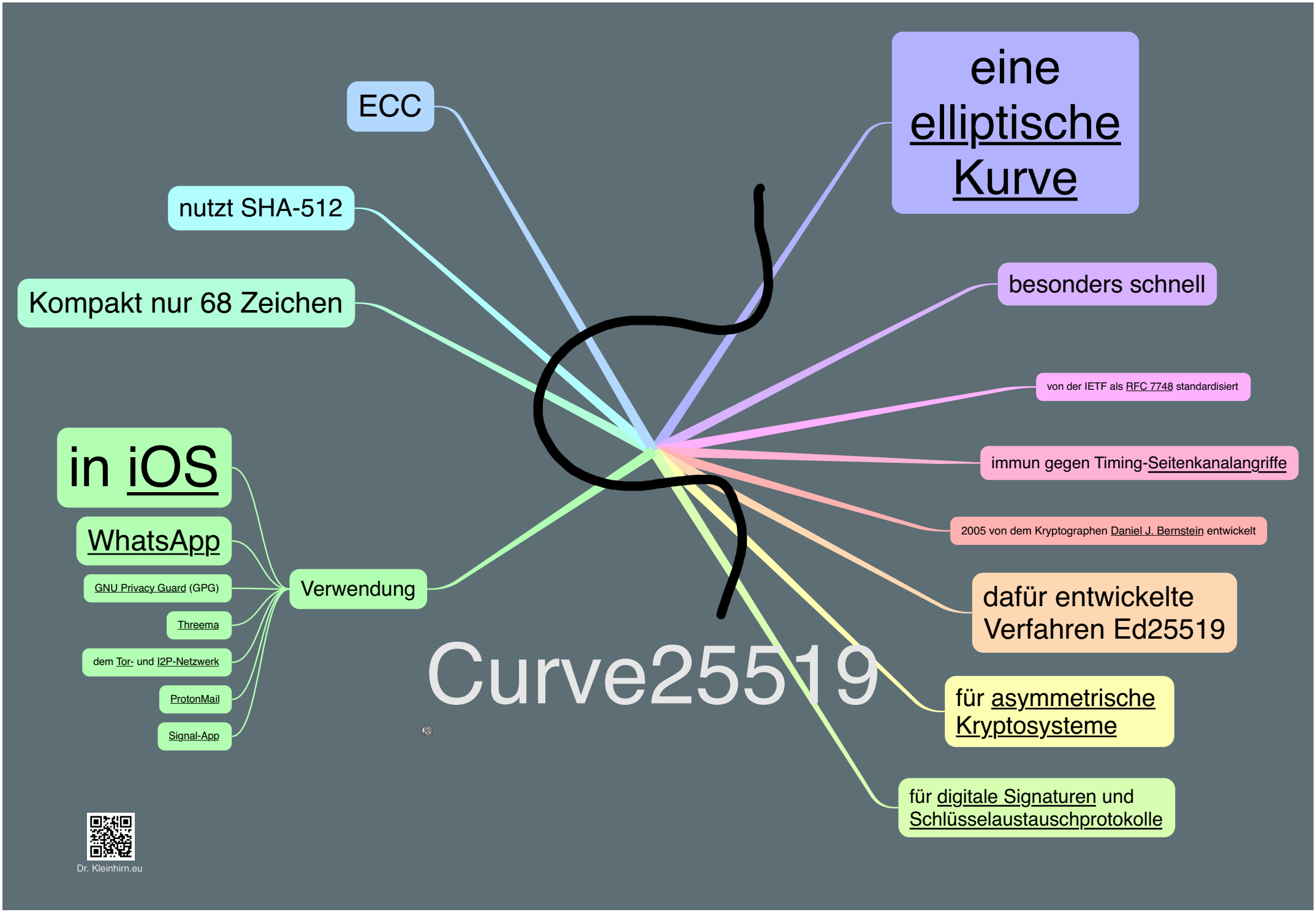
Curve25519
ECC
nutzt SHA-512
Kompakt nur 68 Zeichen
Verwendung
in iOS
WhatsApp
GNU Privacy Guard (GPG)
Threema
dem Tor- und I2P-Netzwerk
ProtonMail
Signal-App
eine elliptische Kurve
besonders schnell
von der IETF als RFC 7748 standardisiert
immun gegen Timing-Seitenkanalangriffe
2005 von dem Kryptographen Daniel J. Bernstein entwickelt
dafür entwickelte Verfahren Ed25519
für asymmetrische Kryptosysteme
für digitale Signaturen und Schlüsselaustauschprotokolle
Dr. Kleinhirn.eu