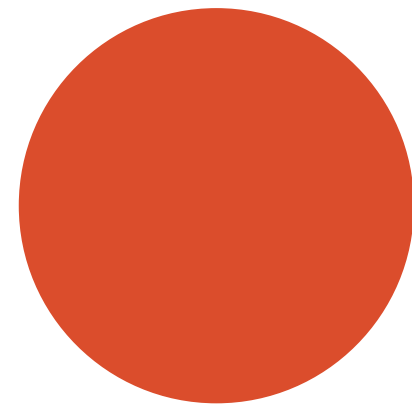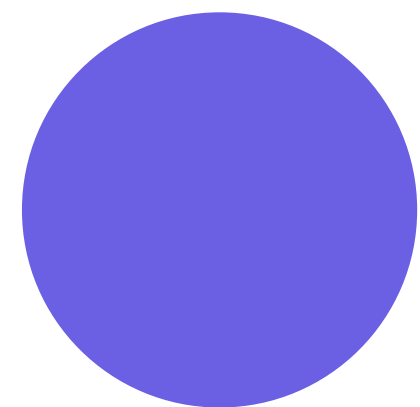#333333
rgba(51, 51, 51, 1);
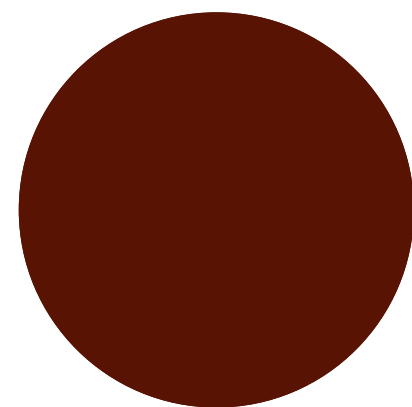
#db4d2c
rgba(219, 77, 44, 1)

#faf9f5
rgba(250, 249, 245, 1)

#6b60e3
rgba(107, 96, 227, 1)

#581303
rgba(219, 77, 44, 1)

Sigsum

https://outfit.io/outfit-font

A free and open source software project that brings transparency to cryptographic key-usage

Add your use-case

Sigsum outfit

For security we need a collision resistant hash function and an unforgeable signature scheme. We also assume that at most a threshold of independent witnesses stop following protocol to protect against a malicious log that attempts split-view and slow-down attacks. An attacker can at best deny service with these assumptions.