Abstract: Some cryptographic schemes like RSA have the remarkable property that the leakage of a constant fraction of the secret key allows an attacker to recover the complete key in polynomial time. Other scheme as e.g. discrete-log based schemes seem to be resistant to this kind of partial key exposure attacks.

We review some classic results, and then turn our focus to modern post-quantum cryptographic schemes. As opposed to the common belief, modern post-quantum schemes such as e.g. McEliece, BIKE and also lattice-based schemes allow for efficient recovery of the secret key from partial information.