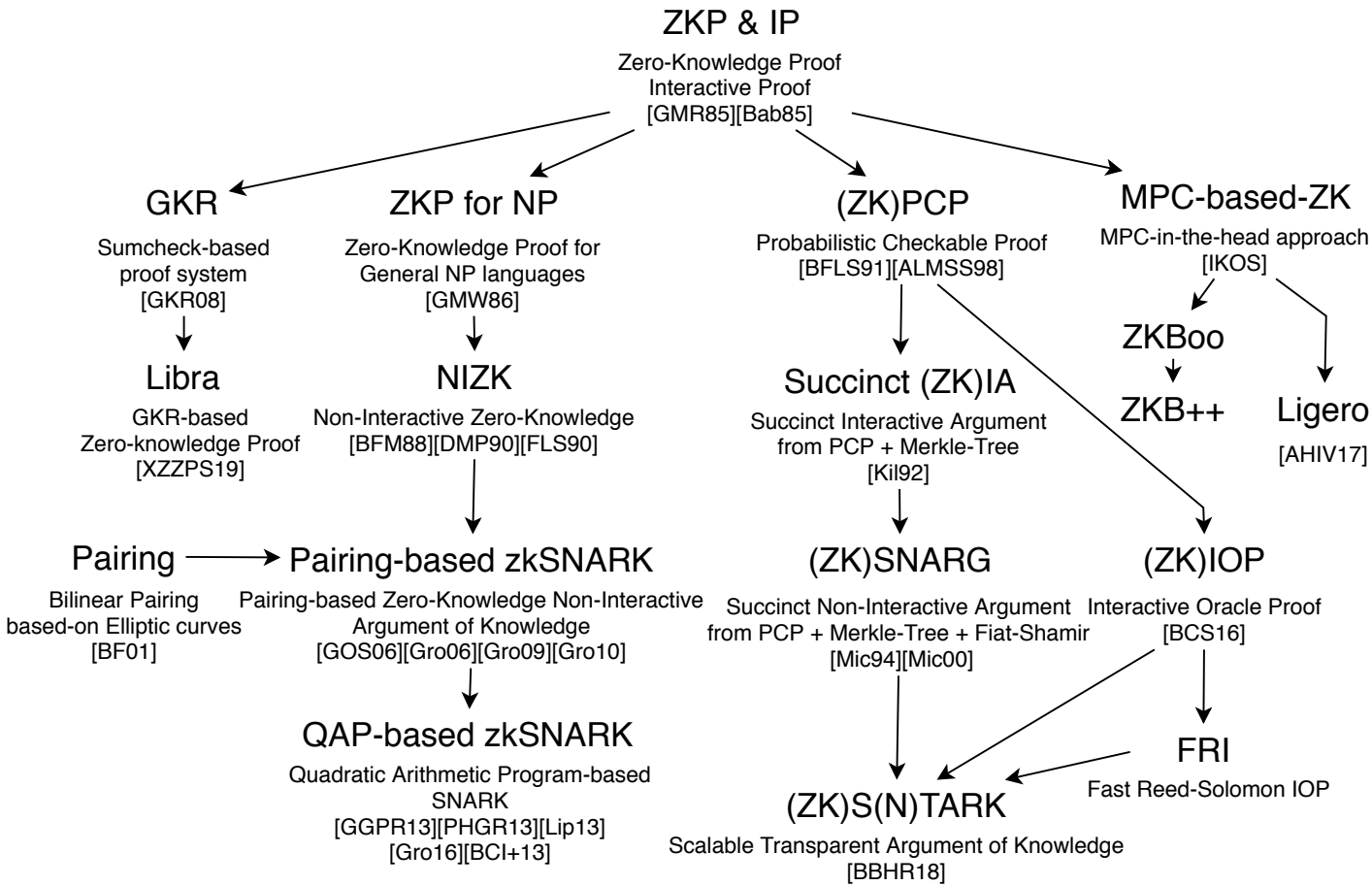
ZKP & IP
Zero-Knowledge Proof
Interactive Proof
[GMR85][Bab85]
GKR
Sumcheck-based
proof system
[GKR08]
Libra
GKR-based
Zero-knowledge Proof
[XZZPS19]
ZKP for NP
Zero-Knowledge Proof for
General NP languages
[GMW86]
NIZK
Non-Interactive Zero-Knowledge
[BFM88][DMP90][FLS90]
Pairing
Bilinear Pairing
based-on Elliptic curves
[BF01]
Pairing-based zkSNARK
Pairing-based Zero-Knowledge Non-Interactive
Argument of Knowledge
[GOS06][Gro06][Gro09][Gro10]
QAP-based zkSNARK
Quadratic Arithmetic Program-based
SNARK
[GGPR13][PHGR13][Lip13]
[Gro16][BCI+13]
(ZK)PCP
Probabilistic Checkable Proof
[BFLS91][ALMSS98]
Succinct (ZK)IA
Succinct Interactive Argument
from PCP + Merkle-Tree
[Kil92]
(ZK)SNARG
Succinct Non-Interactive Argument
from PCP + Merkle-Tree + Fiat-Shamir
[Mic94][Mic00]
MPC-based-ZK
MPC-in-the-head approach
[IKOS]
ZKBoo
ZKB++
Ligero
[AHIV17]
(ZK)IOP
Interactive Oracle Proof
[BCS16]
FRI
Fast Reed-Solomon IOP
(ZK)S(N)TARK
Scalable Transparent Argument of Knowledge
[BBHR18]