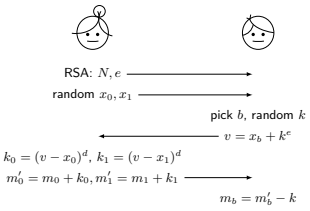
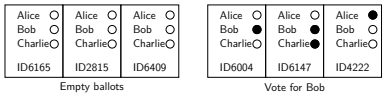
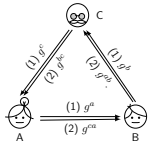
1outof2



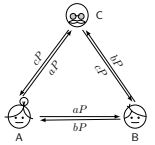
3ballot



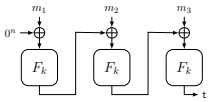
3parties-DHKE



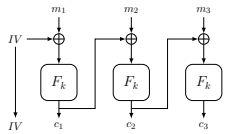
3parties-JOUX



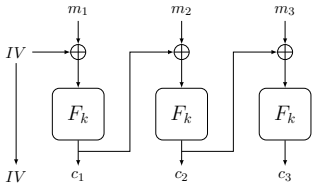
CBC-MAC



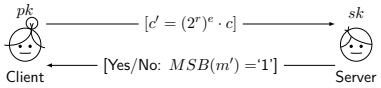
CBC-small



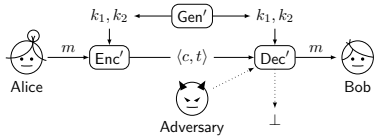
CBC



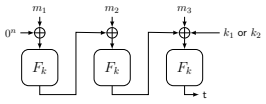
CCA-PKCS



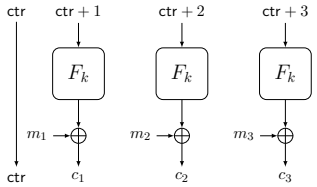
CCA



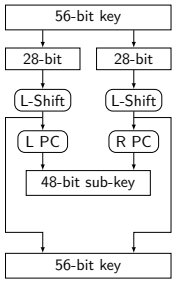
CMAC



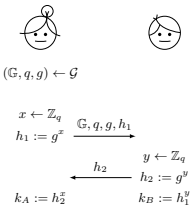
CTR



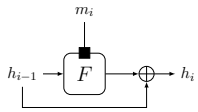
DESkey



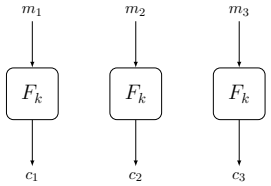
DHkey



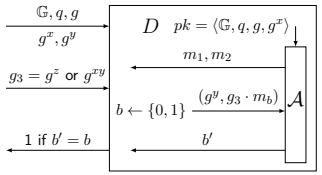
Davies-Meyer



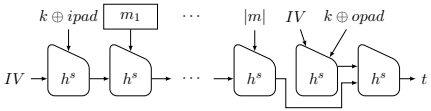
ECB



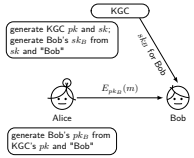
ElGamal



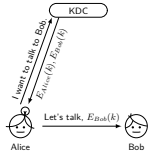
HMAC



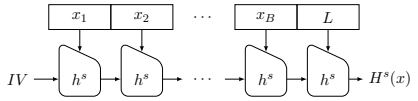
IBE



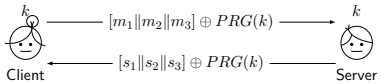
KDC



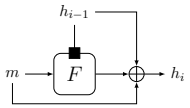
MDtransform



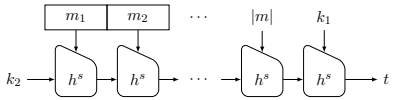
MS-PPTP



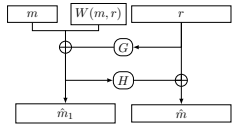
Miyaguchi-Preneel



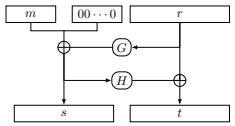
NMAC



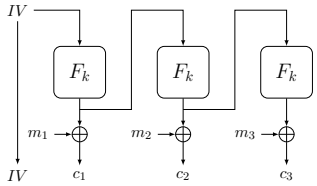
OAEP-plus



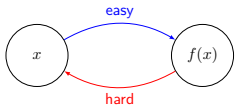
OAEP



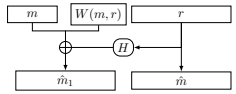
OFB



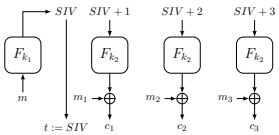
OWF



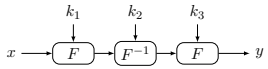
SAEP-plus



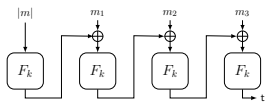
SIV-CTR



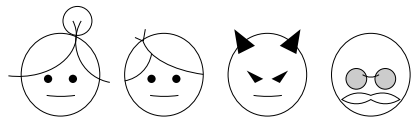
TDES



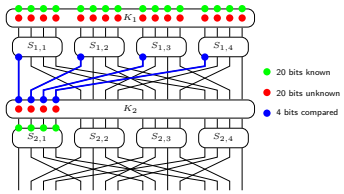
VCBC-MAC



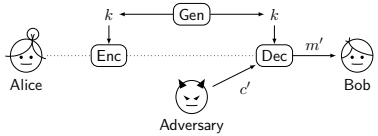
alice



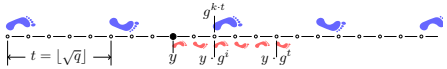
attack-spn



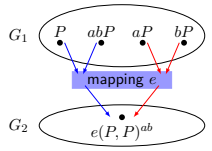
authentication



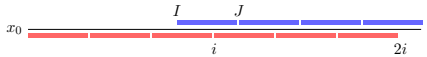
baby-giant



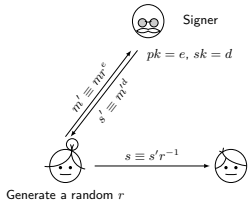
bilinear-map



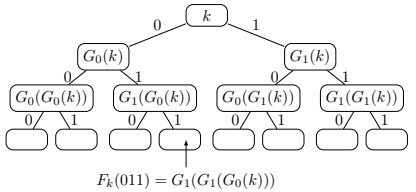
birthdayattack



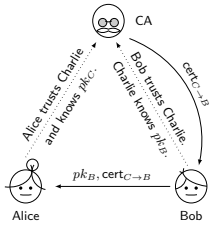
blindsignature



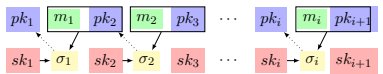
cPRF



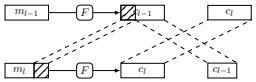
certificates



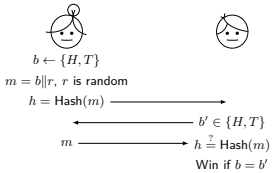
chain-sig



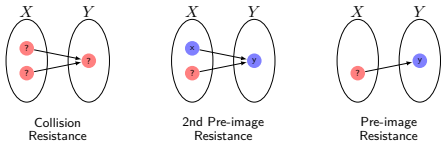
cipher-stealing



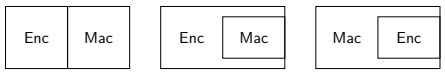
coinflipping



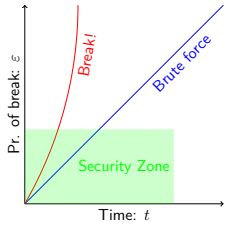
collision



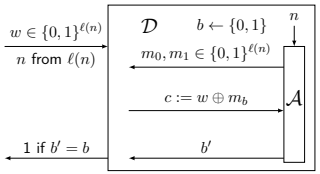
combination



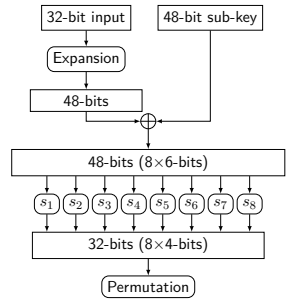
compute-sec



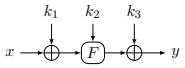
constructD



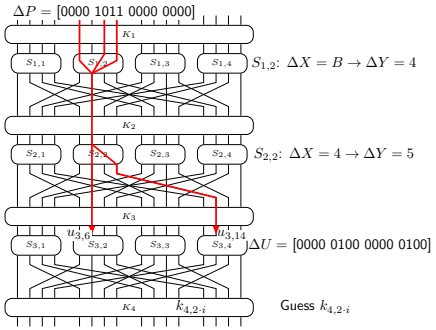
des



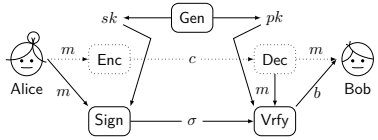
desx



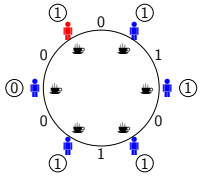
differential



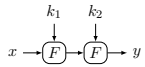
digitalsignature



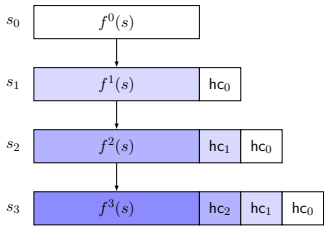
dining



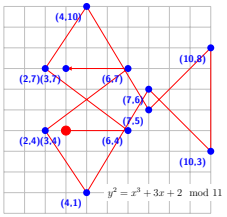
doubleE



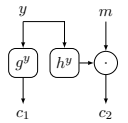
ePRG



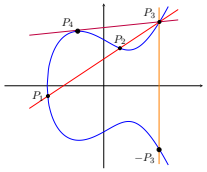
ecdhke



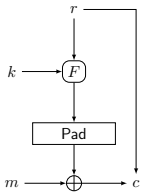
elgamal-con



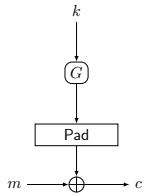
ellipticcurve



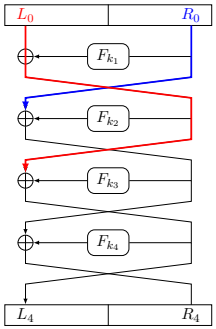
encryptionwithpf



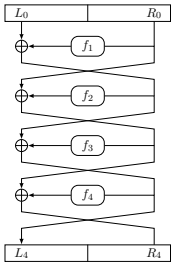
encryptionwithpg



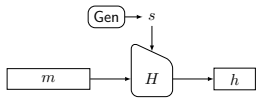
feistel-prp



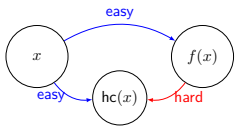
feistel



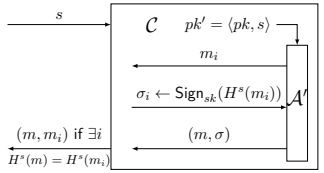
hash



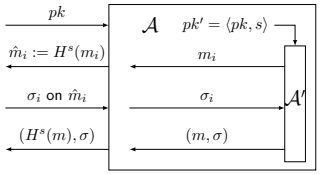
hcp



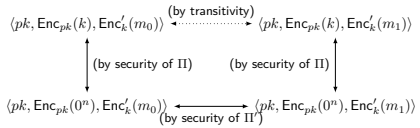
hs-reduce-1



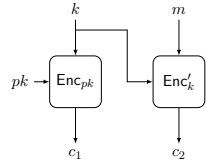
hs-reduce-2



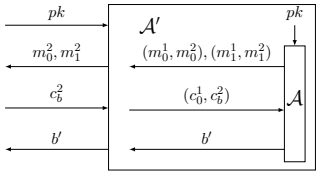
hybrid-enc-proof



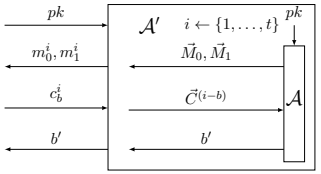
hybrid-encrypt



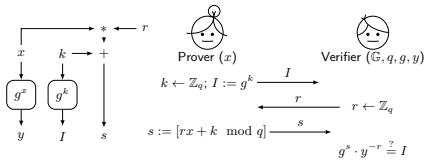
hybrideg



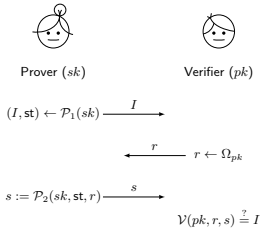
hybridproof



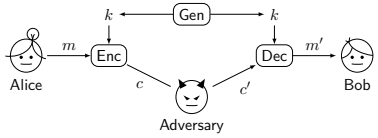
identification-schnorr



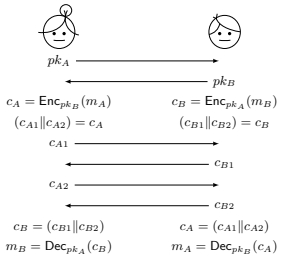
identification



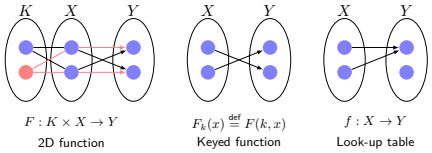
integrity



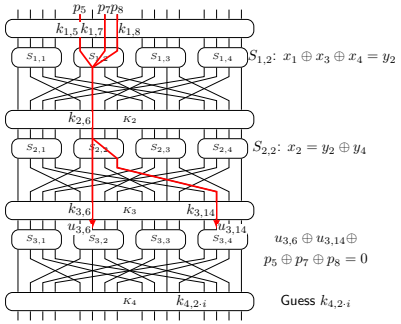
interlock



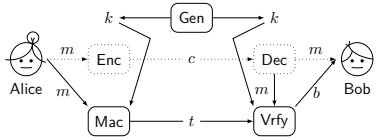
keyed-func



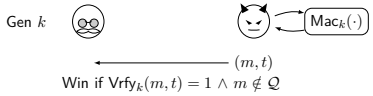
linear



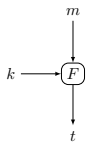
mac



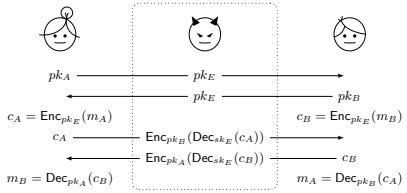
macforge-exp



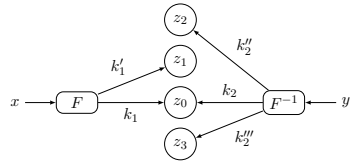
macwithprf



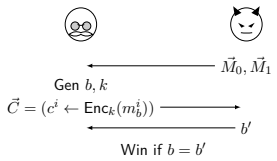
man-in-middle



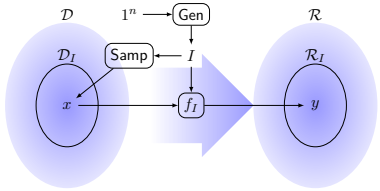
meet-in-middle



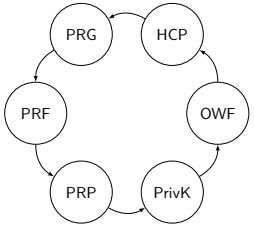
multiple-enc-exp



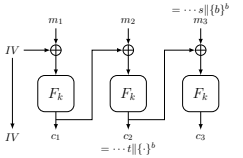
owff



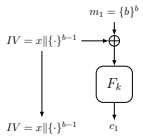
owfover



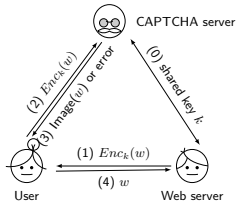
padding-oracle-lastbyte



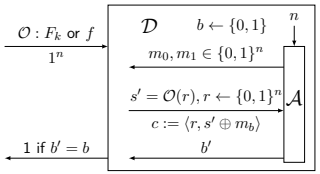
padding-oracle-null



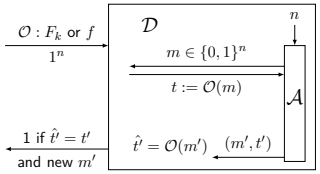
padding-oracle



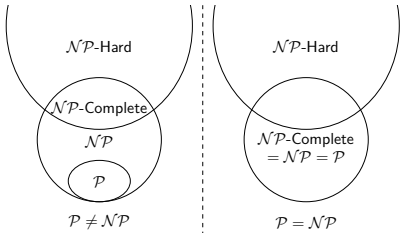
pgfD



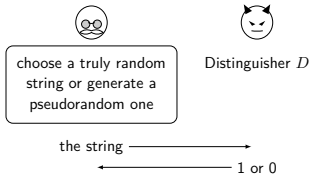
pgfMAC



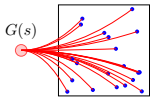
pnp



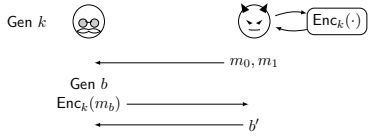
prg-distinguisher



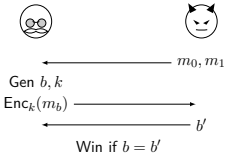
prg-sparse



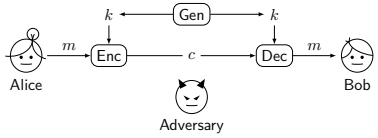
pri-cpa-exp



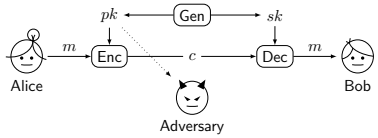
pri-eav-exp



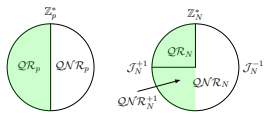
private-key



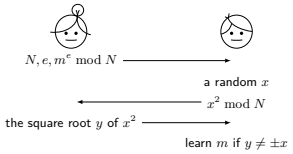
public-key



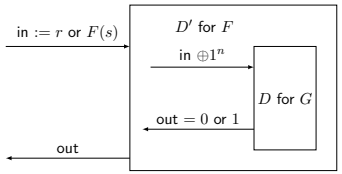
qr-qnr



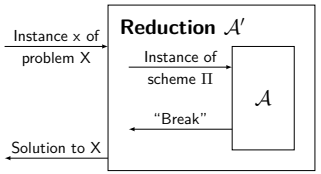
rabinOT



reduction-prg



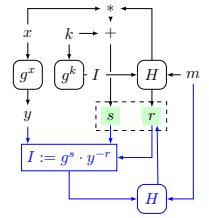
reduction



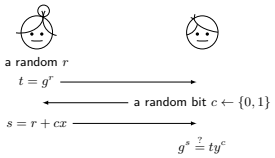
schnorr-signature

Sign: $k \leftarrow \mathbb{Z}_q$,
compute $I := g^k$,
$r := H(I, m)$,
$s := [rx + k \mod q]$
and output (r, s)

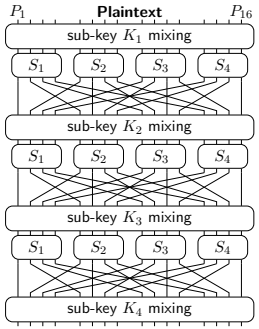
Vrfy: Compute I and
output 1 $\iff H(I, m) \stackrel{?}{=} r$.



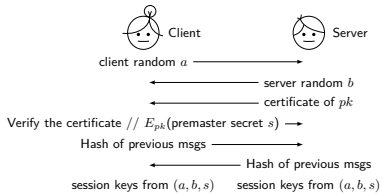
schnorr



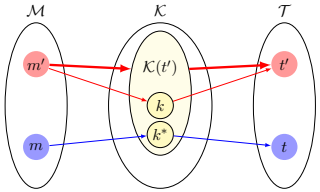
spn



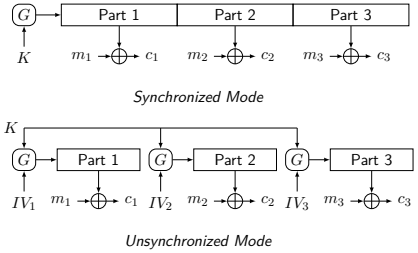
ssl



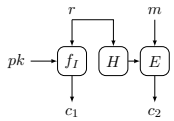
suf-mac



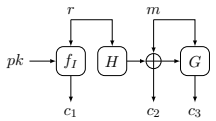
synchronizedmode



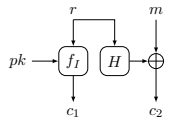
tdp-cca1



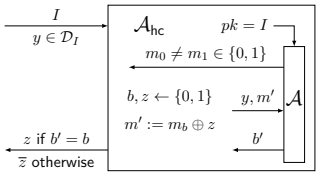
tdp-cca2



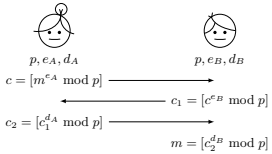
tdp-cpa



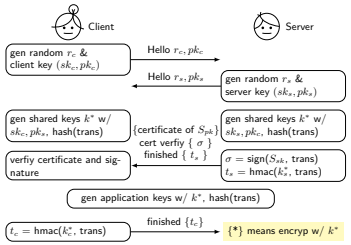
tdp-pk



threepass

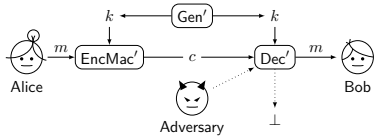


tls13hs

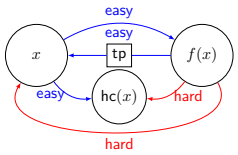


toy-OT

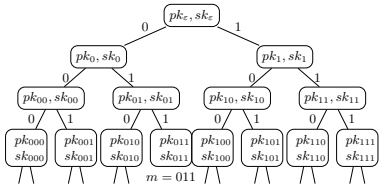
transmission



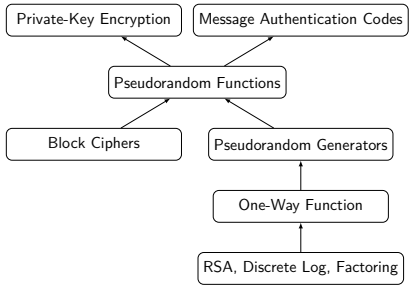
trapdoor



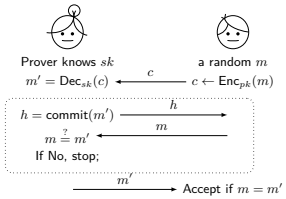
tree-sig



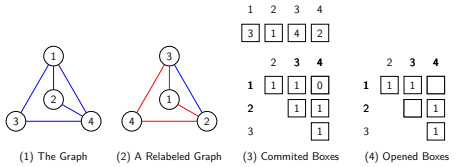
worldofpk



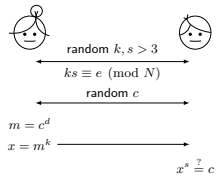
zkp-commitment



zkp-hanmilton



zkp-rsa



zkp