mpc core tss algorithms

protocols	usage	algorithms	remark	code reference
cmp20/cggmp21 threshold key generation	m out of n keygen	ecdsa key geneation eddsa key generation hash commitment schnorr zk proof	N/A	tsslib
cmp20/cggmp21 threshold sign	m out of n sign	ecdsa /eddsa sign Paillier Encryption Enc Range zk proof Paillier affine group zk proof	N/A	tsslib
frost eddsa threshold sign	m out of n eddsa sign	eddsa sign	N/A	tsslib
cmp20/cggmp21 auxiliary	auxiliary	Paillier Encryption Ring Pederson zk proof Paillier Blum Modules zk proof No samll Factor zk proof	N/A	tsslib

mpc crypto table

algorithm	usage	remark	code reference
ECIES Encrypt	Private Key Share Encryption User key backup	use KMS	local ; go-etheruem ;github.com/ecies/go/v2
AES (GCM/CBC)	For Communication Security; Hardware wallet to server ;	generate random key	local / golang std lib

algorithm	usage	remark	code reference
	mpc node to server ; encrypt transaction ;	for every session	
SHA256 /SHA3	Common Hashing	N/A	local / golang std lib
pbkdf2	Password based key derivation for Bip39	N/A	local / golang std lib
HMAC-SHA512	Bip32 key derivation	N/A	local / golang std lib
Google Auth	Running Server in Production	N/A	
ECDH	For key agreement ; node to server communication	N/A	local / golang std lib
Ed25519 Signature	For node to server communication authentication	N/A	local / golang std lib
RSA Signature	sign wallet address ; sign request to HBC Business	N/A	local / golang std lib
RSA Encryption	Encrypt wallet backup key; Server TLS Certification	N/A	local / golang std lib
JWT with AES encryption	For user to server communication authentication	N/A	local / golang std lib
KMS	store private key share	Aliyun KMS	