- cryptosystem libraries
  → OpenSSL:
      RSA: public key cryptosystem
      DSA: digital signature algorithm
      DH: Diffie-Hellman key agreement
      …
  → Crypto++:
      RSA (LUCRSA)
      DSA
      ElGamal (LUCELG, DLIES)
      Nyberg-Rüppel: digital signature
      Rabin
      ESIGN
      …
  → Paillier library: Paillier cryptosystem from University of Texas - Austin

- DFT/FFT in the encrypted domain
  → 3 interrelated articles on DFT encryption, by Tiziano Bianchi et al.
    “Comparison of Different FFT Implementations in the Encrypted Domain”
    “Implementing the Discrete Fourier Transform in the Encrypted Domain”

- implementation of Paillier cryptosystem
  → based on algorithms described on Wikipedia, simplifications due to length(p)=length(q)
  → use of OpenSSL for random (prime) number generation, modular multiplicative inverse
  → work in progress, to be completed early next week