Cryptography is a *tool* and often times only part of a solution.

Examples:
- Public key encryption in TLS ECH, MLS, and OHTTP
- PAKE in WhatsApp end-to-end encrypted backups
- Privacy Pass in Apple’s Private Access Tokens
- Signatures with selective disclosure in Verifiable Credentials

Briefly survey high-level features and usage considerations for some new cryptography and security specifications.
Tool: Public Key Encryption

Purpose: encrypt application data under a public key
Tool: Public Key Encryption

Examples: TLS ECH, MLS, OHTTP / ODoH, DAP

Considerations:
  How to authenticate the public key?
  How to distribute the public key?

Reference: RFC 9180 (CFRG)
Purpose: establish a shared secret authenticated by a password

Protocol: PAKE
Protocol: PAKE

Examples: Device pairing (Thread / Matter), end-to-end encrypted backup (WhatsApp), secure channel establishment

Considerations:
  Would public key authentication be better?
  Do both parties need the password (for policy enforcement)?
  Is the attacker able to brute force “login” attempts?

References: draft-irtf-cfrg-opaque, draft-irtf-cfrg-cpace (CFRG)
Protocol: Private Aggregation

Purpose: privately compute aggregate functions without learning individual aggregate inputs
Protocol: Private Aggregation

Examples: Private aggregation (DiviiUp), Exposure Notification Private Analytics (Apple / Google)

Considerations:
- How are non-collusion requirements guaranteed?
- How does the aggregate function fit into the privacy threat model?
- How are aggregation parameters configured and distributed?

References: draft-ietf-ppm-dap (PPM)
Protocol: Private Authorization

Purpose: authorize clients without revealing unique client information
Protocol: Private Authorization

Examples: CAPTCHA solution signal (Cloudflare Privacy Pass), Private Access Tokens (Apple), Sybil attack prevention (Distributed Aggregation Protocol)

Considerations:
  What signal is the client providing when authorizing?
  Are replay and token hoarding attacks a concern?

References: draft-ietf-privacypass-architecture
Purpose: selectively disclose a subset of attributes authorized by an issuer.

Data Controllers should be able to disclose only the claims required by a Data Processor.
Protocol: Selective Disclosure

Examples:
- Digital Driver's License
- Proof of Vaccinations
- Redacted Trade / Supply Chain Documents

References:
- draft-ietf-oauth-selective-disclosure-jwt
- vc-jose-cose (W3C)
- imda.gov.sg/.../international-trade-and-logistics/tradetrust
- ISO mDoc
Cryptography is a *tool*, and tools can be harmful

Anti-patterns:
1. “How can I implement and deploy the cryptography I found in this new paper?”
   → Focus on problems, not solutions
2. “We can just plug in <X> and it should be fine”
   → Demand formal security analysis when using these tools
3. “If we modify things like <X> then tool <Y> will work for us”
   → Collaborate with people working on standards!