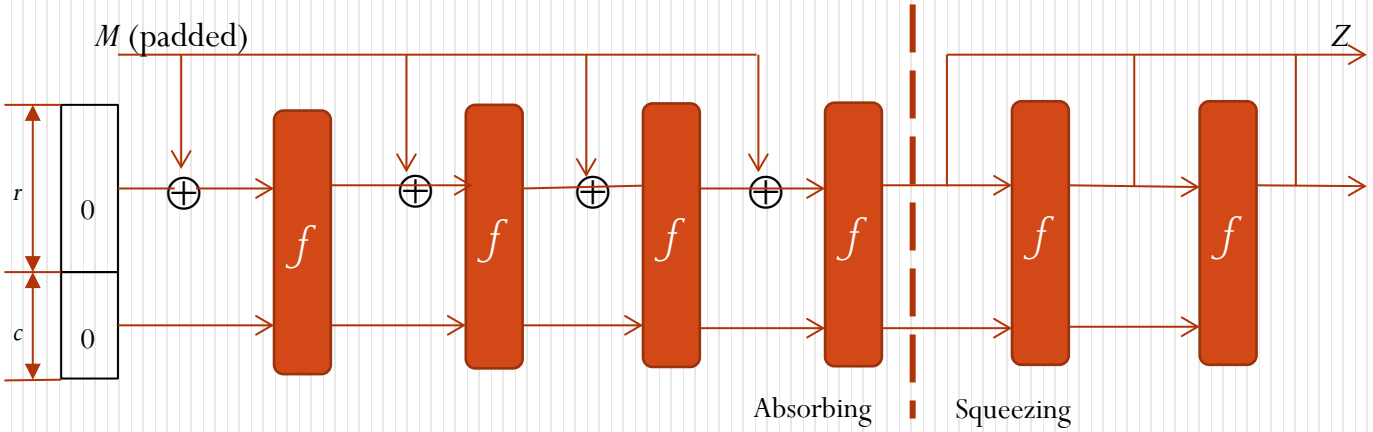
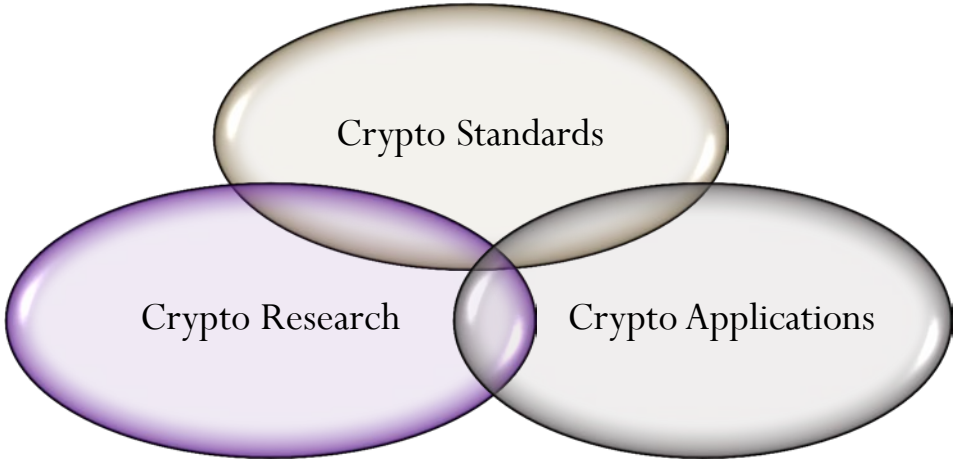
Cryptographic Technology Group

Lily Chen, Acting Manager of CTG

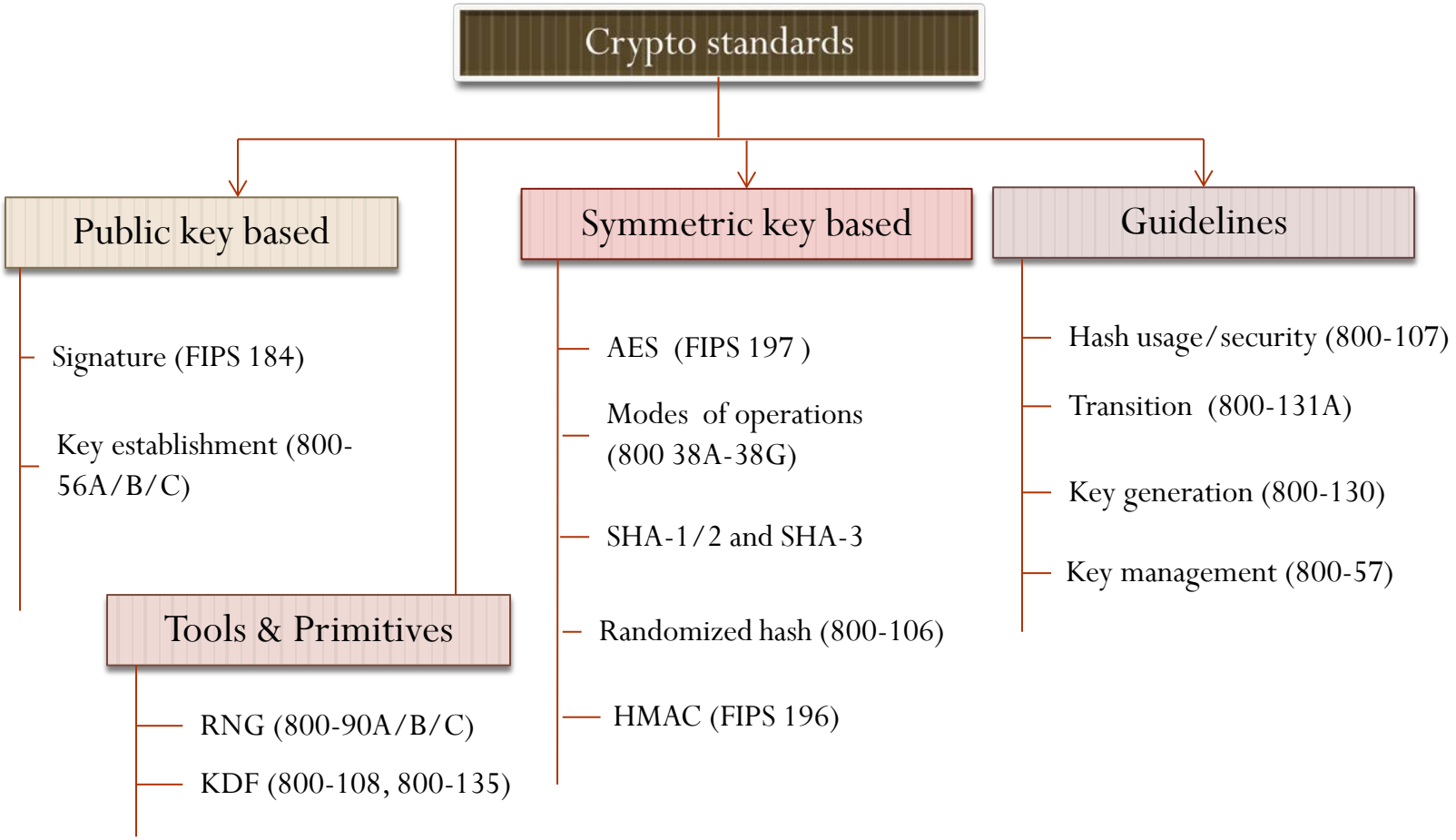
June 4, 2013



We are working on three areas



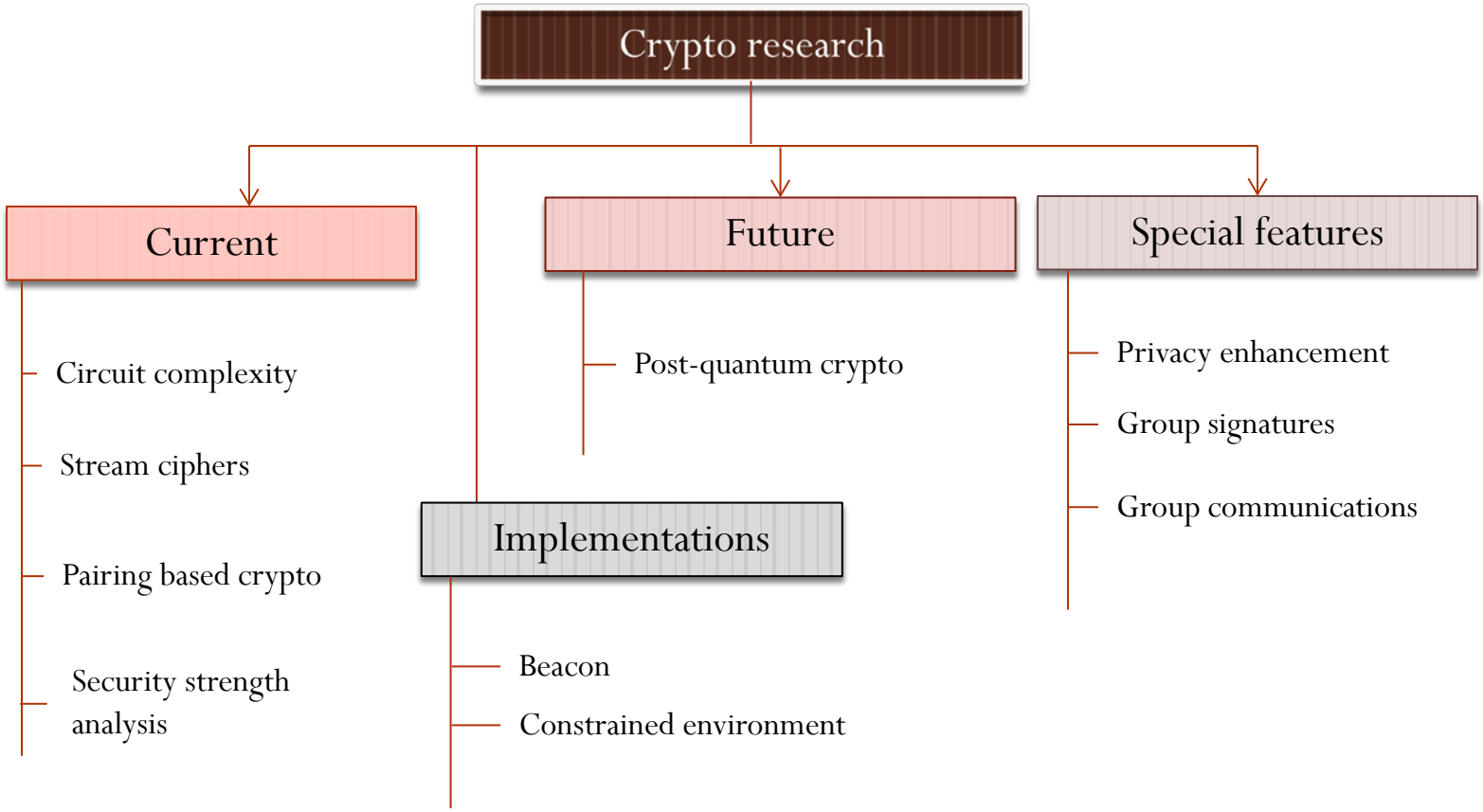
Crypto standards – At a glance



Crypto standards – Highlights

- SHA-3 Competition: After a five-year competition, Keccak was selected as SHA-3 in the fall of 2012.
  - SHA-3 is to be standardized in a FIPS.
  - Continue to invest the special features of SHA-3 such as tree hash, authenticated encryption, PRF mode, etc..
- New modes of operations: SP 800-38F for key wrapping.
- Random number generation: SP 800-90A/B/C for deterministic and non-deterministic random number generators, essential components for crypto implementations.
- Key management standards:
  - 800-131A Recommendation for key length and algorithm transition provides timeline for retiring and adopting.
  - 800-56A/B revision.

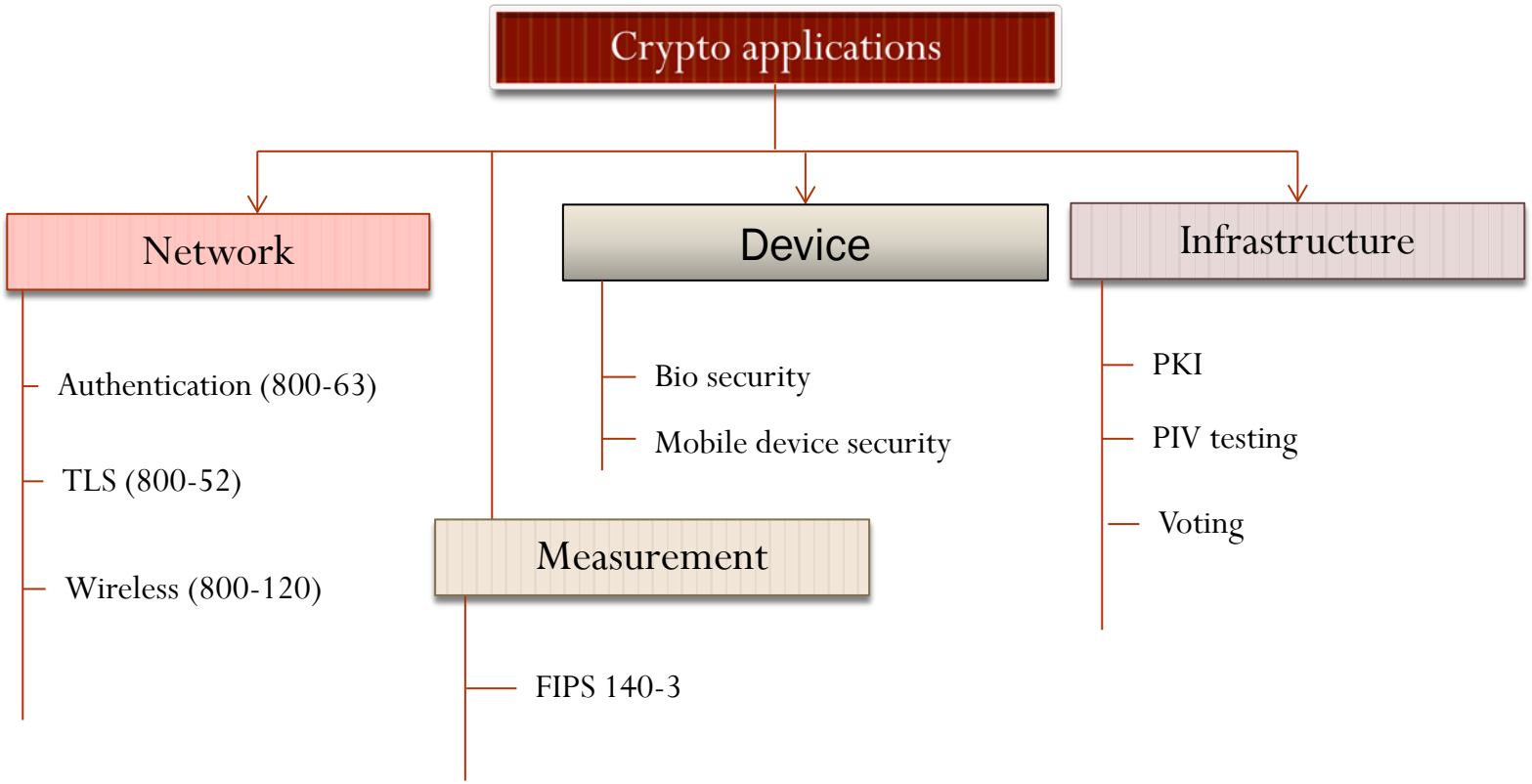
Crypto research – At a glance



Crypto research – Highlights

- Post-quantum cryptography (PQC) deals with quantum computing challenges to the current cryptosystems such as RSA, DH, and DSA.
  - Look into different PQC schemes such as lattice based, coding based, multivariate, etc., the schemes believed resistant to quantum computing.
  - Understand the security assessment on these schemes.
  - Explore the impact to existing security infrastructure and applications.
- Privacy enhancing crypto research explores cryptographic tools for protecting user privacy.
  - support of the National Strategy for Trusted Identities in Cyberspace (NSTIC).
- Beacon is a secure randomness source that broadcasts full entropy bit-strings.

Crypto applications – At a glance



Crypto applications – Highlights

- SP 800-52 provides guidelines for TLS usage.
  - It is under a major revision to reflect the newer version(s) of TLS and dealing with the attacks identified recently. The new version is expected to be released for public comments by the end of 2013.
- Continue to improve trust infrastructure.
  - Held a workshop to discuss increasing trust online by improving the Public Key Infrastructure (PKI) certificate marketplace supporting Secure Socket Layer (SSL) and Transport Layer Security (TLS).
- Introduce hardware roots of trust to support reliable device authentication and establish a trust base for system measurement (Draft SP 800-164)
- FIPS 140-3, the revision of Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is in the final stage to prepare for publications.

Last but not least, we collaborate with other CSD groups

- For example,
  - With components and mechanisms group for trusted mobile devices;
  - With systems and applications group for PIV testing and authentication protocols;
  - With outreach and integration group for crypto standards applications in various areas such as smart grid;
  - With testing, validation, and measurement group for algorithm testing (CAVP) and for FIPS 140 development (CMVP).