SECURE COMMUNICATION IN THE QUANTUM ERA

NATO SPS programme- Project Number: G5448

Kick-off meeting

Malta, September 30th- October 3rd, 2018

STEP 2-A: IDENTIFY CANDIDATE PROTOCOL (LEAD: URJC, CONTRIBUTORS: FAU)

IDENTIFY CANDIDATE PROTOCOLS: TWO STRATEGIES

- Compiled solutions:
  - "classical" compilers for going from 2-party to group can be used (on top of pq-AKE)
  - Construct new compilers (complying with pq-security models from 1-A)
- Dedicated designs:
  - Implementation goals: low communication complexity
  - Optimized computational costs
  - Advanced/Not-standard security goals

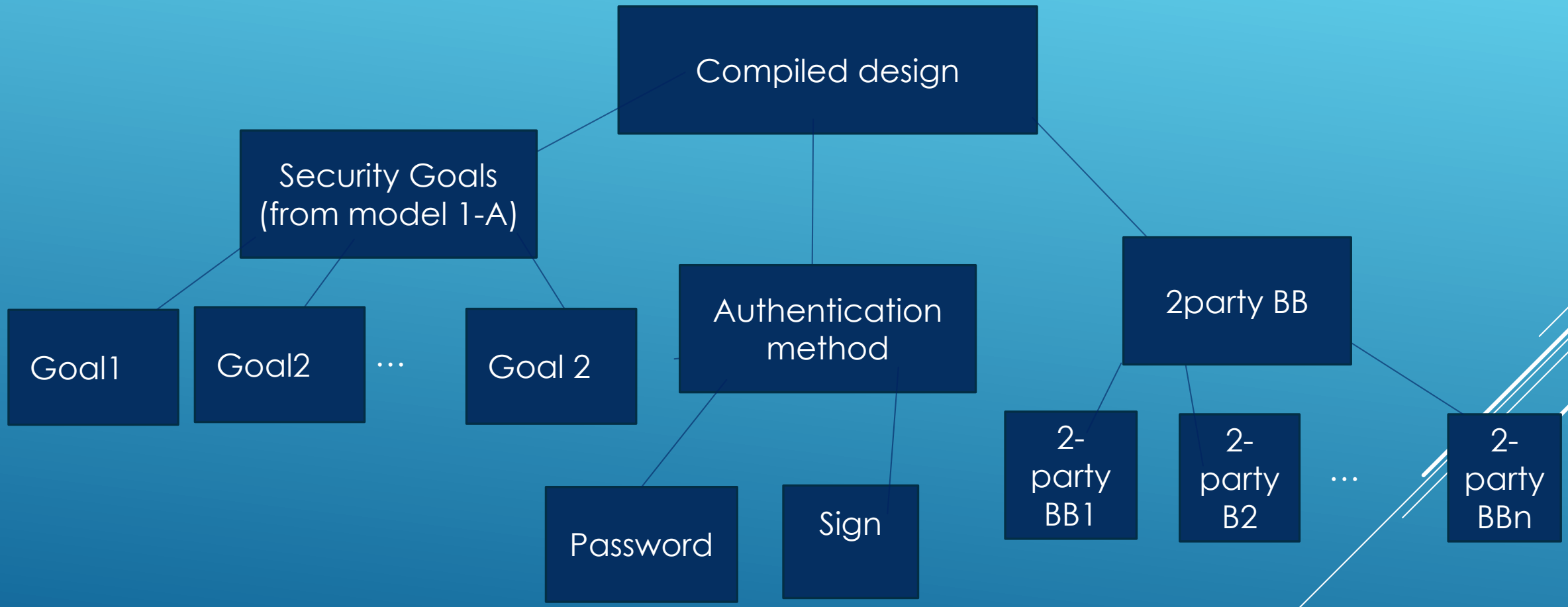
AUTHENTICATION:

- Password based:
  - Exploit existing constructions (no risky preQ assumptions)
  - Obtain privacy properties/ad-hoc designs for non-homogeneus groups
- Signature based
  - PQ (potentially) very expensive → number of signatures must be reduced by design
  - Short term: use pre-quantum signature + forward secrecy

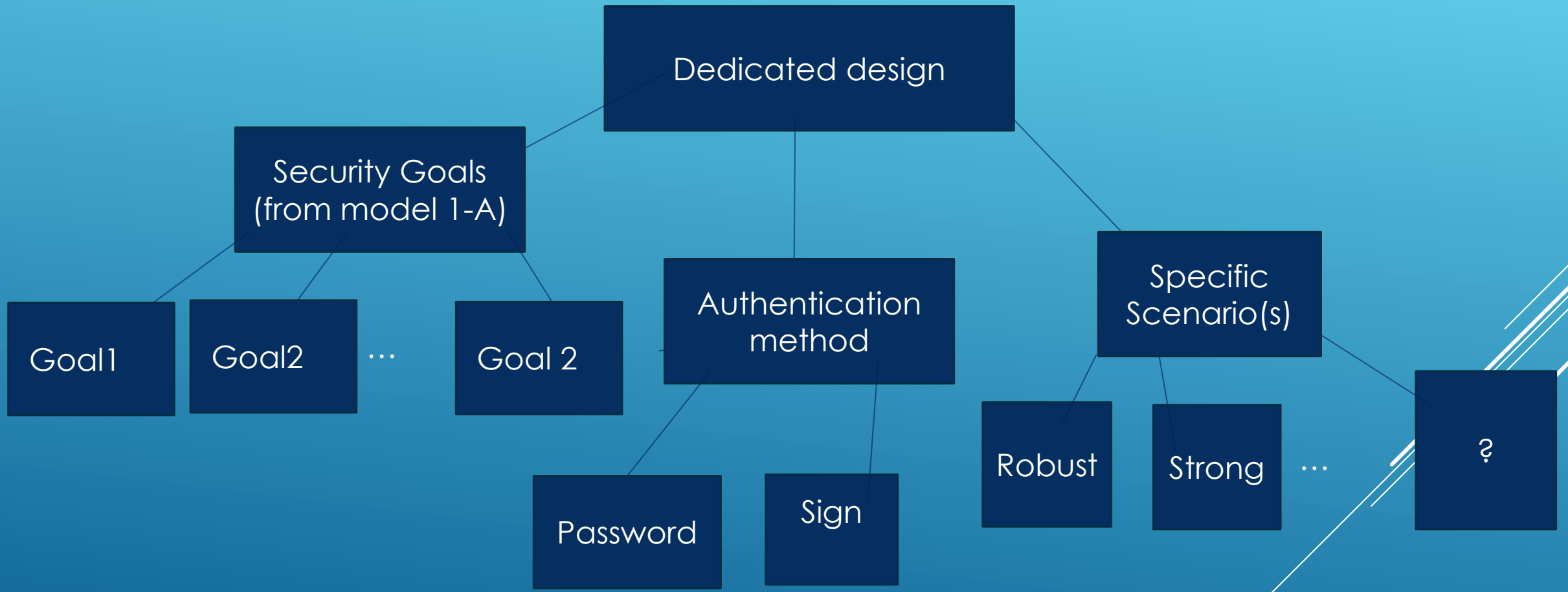
ASSUMPTIONS

- "Pure" PQ: LWE, Code Based, isogenies…
- Hybrid: based on two assumptions (secure as one assumption is)

DECISION TREE (COMPILED)



DECISION TREE (DEDICATED)



OUTCOME (D3)
2ND YR, 4TH QR (JULY/SEPT 2020)

Complete proposal for a quantum-safe AGKE protocol, including:

- High level description
- Detailed constructions
- Security analysis
- Implementation guidance