A Story of “United Nations” of Post Quantum Cryptogrpahy

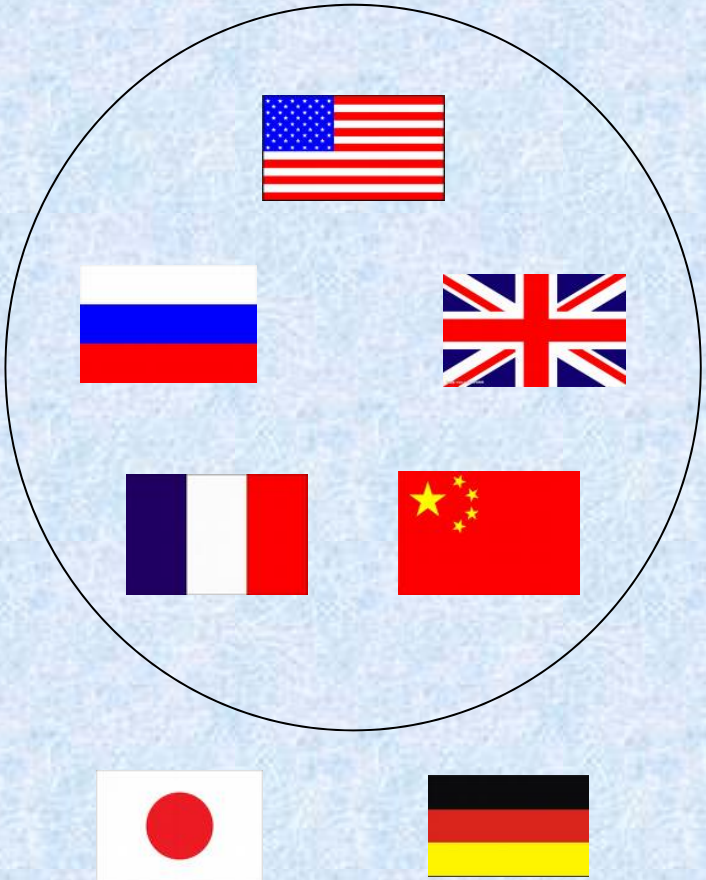
— Direct dialogue between quantum alg. & braid Crypt.

Licheng Wang and Lihua Wang

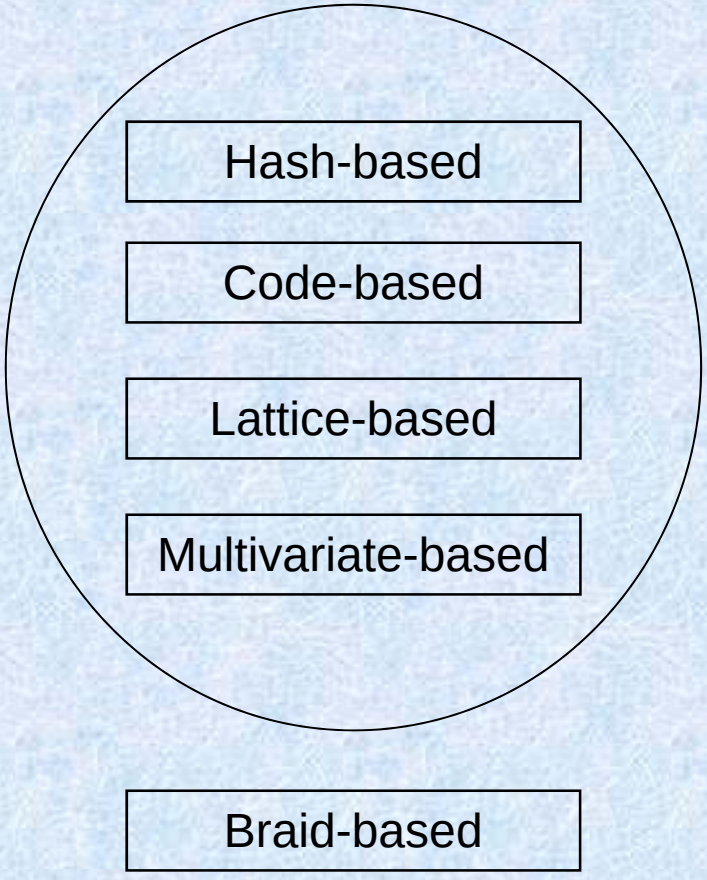
National Institute of Information and Communications Technology

Story of two “United Nations”

- PMS of UN S. C.

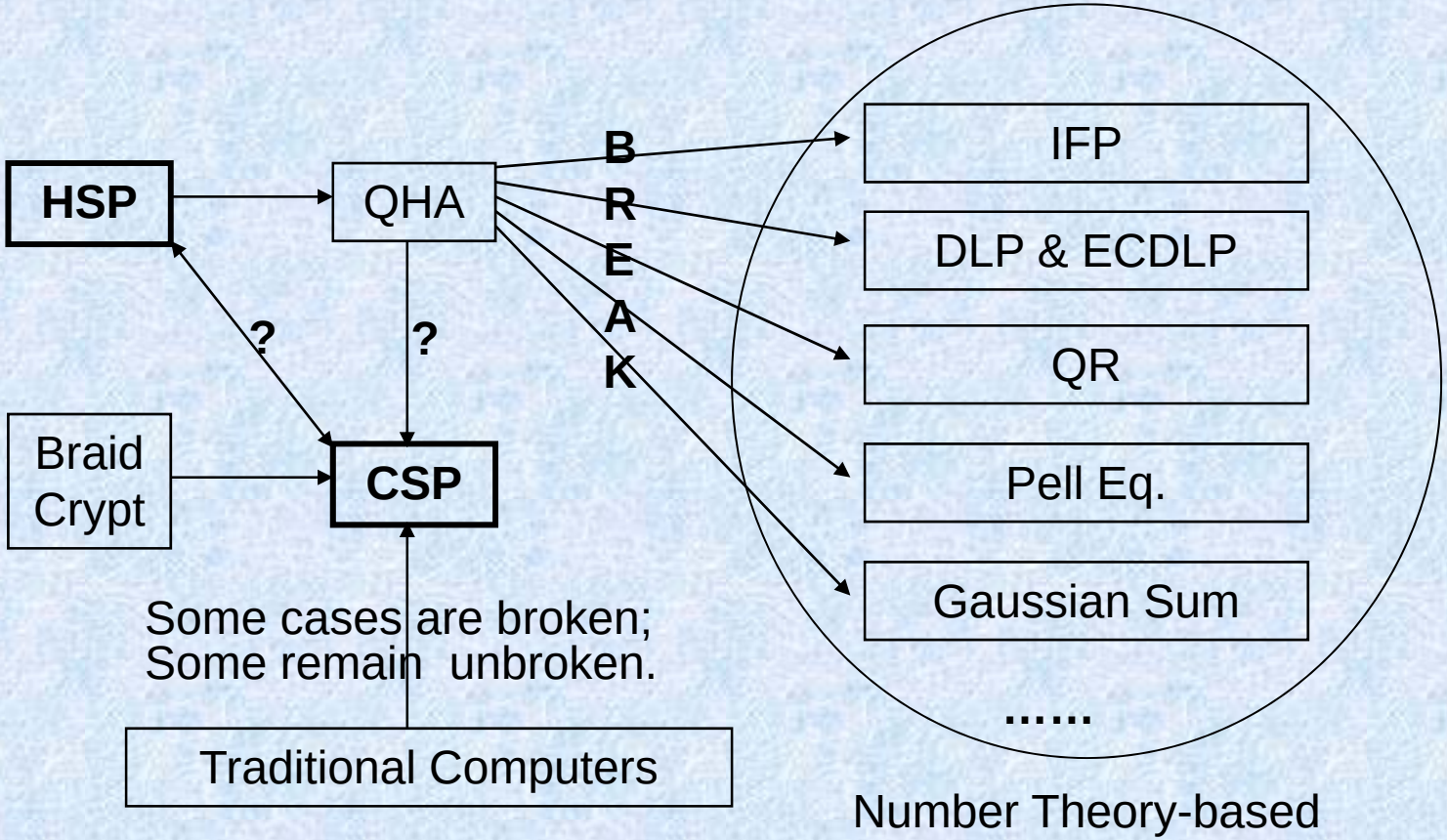


- “UN” of PQCrypt.



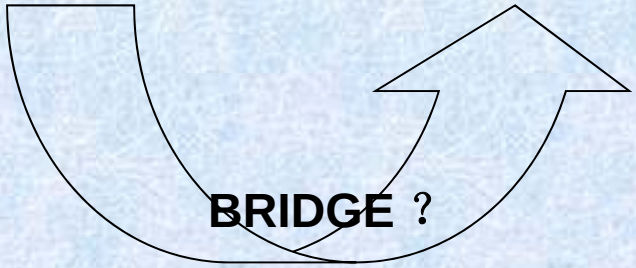
Criterion of Being Selected

- Quantum Alg. vs. Fundamental Assumptions



HSP vs. CSP

- Hidden Subgroup P.
  - Instance:
    - f: G→S, black-box
    - f constant on gH
  - Objective:
    - Find H
- Conjugator Search P.
  - Instance:
    - x
    - $y = zxz^{-1}$
  - Objective:
    - Find z (or z' s.t. $y=z'xz'^{-1}$)



HSP⊃HCSP vs. CSP

- Hidden Conjugate Subgroup P.
  - Instance:
    - f: G→S, black-box
    - H<G
    - f constant on $H^g=gHg^{-1}$
  - Objective:
    - Find H^g or.

    eq. find g

- Conjugator Search P.
  - Instance:
    - x
    - $y = zxz^{-1}$
  - Objective:
    - Find z (or z' s.t. $y=z'xz'^{-1}$)

HSP⊃HCSP vs. CSP

- Hidden Conjugate Subgroup P.
  - Instance:
    - f: G→S, black-box
    - H<G
    - f constant on $H^g=gHg^{-1}$
  - Objective:
    - Find H^g or.

      eq. find g

- Conjugator Search P.
  - Instance:
    - <x>
    - <y> = z<x>z^{-1}
  - Objective:
    - Find z (or z' s.t. y=z'xz'$^{-1}$)

CSP⊄ HCSP ?

⇑

Finding <y>≠ Finding z

-where if f?

-what is the obj.?

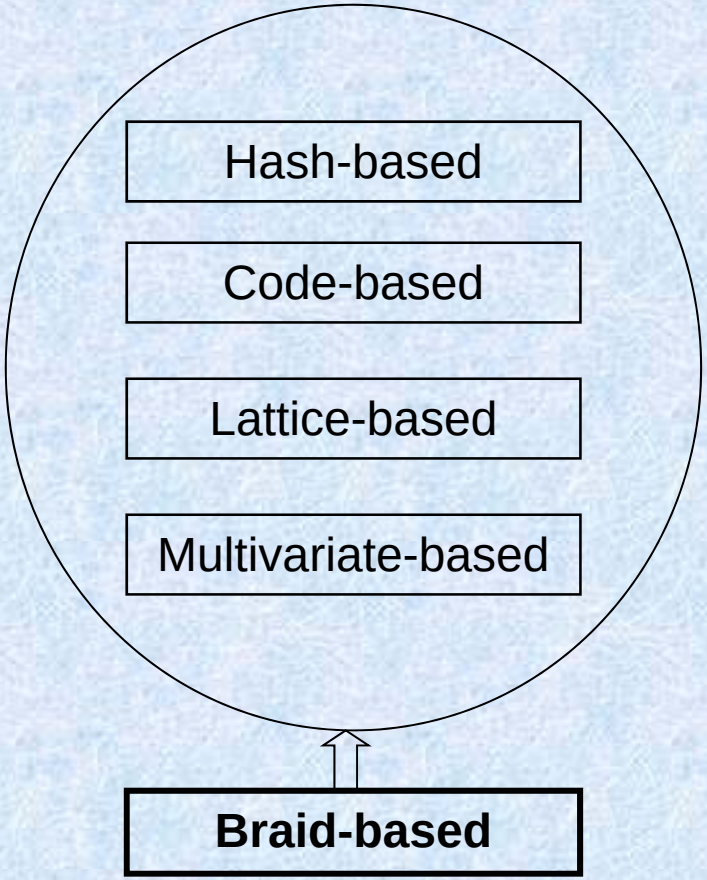
<y> is given!

Qualification Applying

- Statements
  - Advantages
    - Resist to existing Q.A.: QHA in Sn(<Bn) is inefficient [1]
    - Relations between CSP and lattice were found [2]
    - High Efficiency & Security
  - Disadvantages
    - Some immature schemes were broken
    - Large size of keys

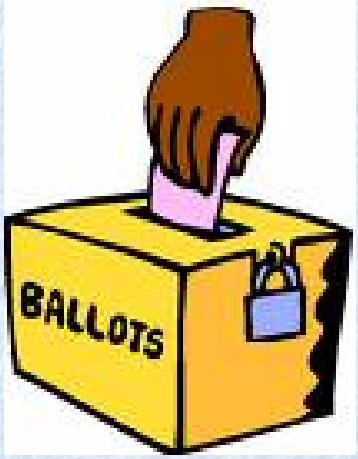
Similar to MPKE

- "UN" of PQCrypt.



Voting Invitation

- Qualified Voters
  - All cryptographers seeing this invitation
- Ballot Box
  - wanglc.cn@gmail.com



Main References:

[2] A. Denney et al. Finding conjugate stabilizer subgroups of PSL(2; q). Report, arXiv: 0809.2445, 2009.

[1]L. Wang et al. New Cryptosystems From CSP-based Self-Distributive Systems, Report, Cryptology ePrint Archive: 2009/566