ECRYPT

http://www.ecrypt.eu.org

International Approaches to Cryptology

Prof. Bart Preneel
COSIC, K.U.Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel

June 2012

Cryptology

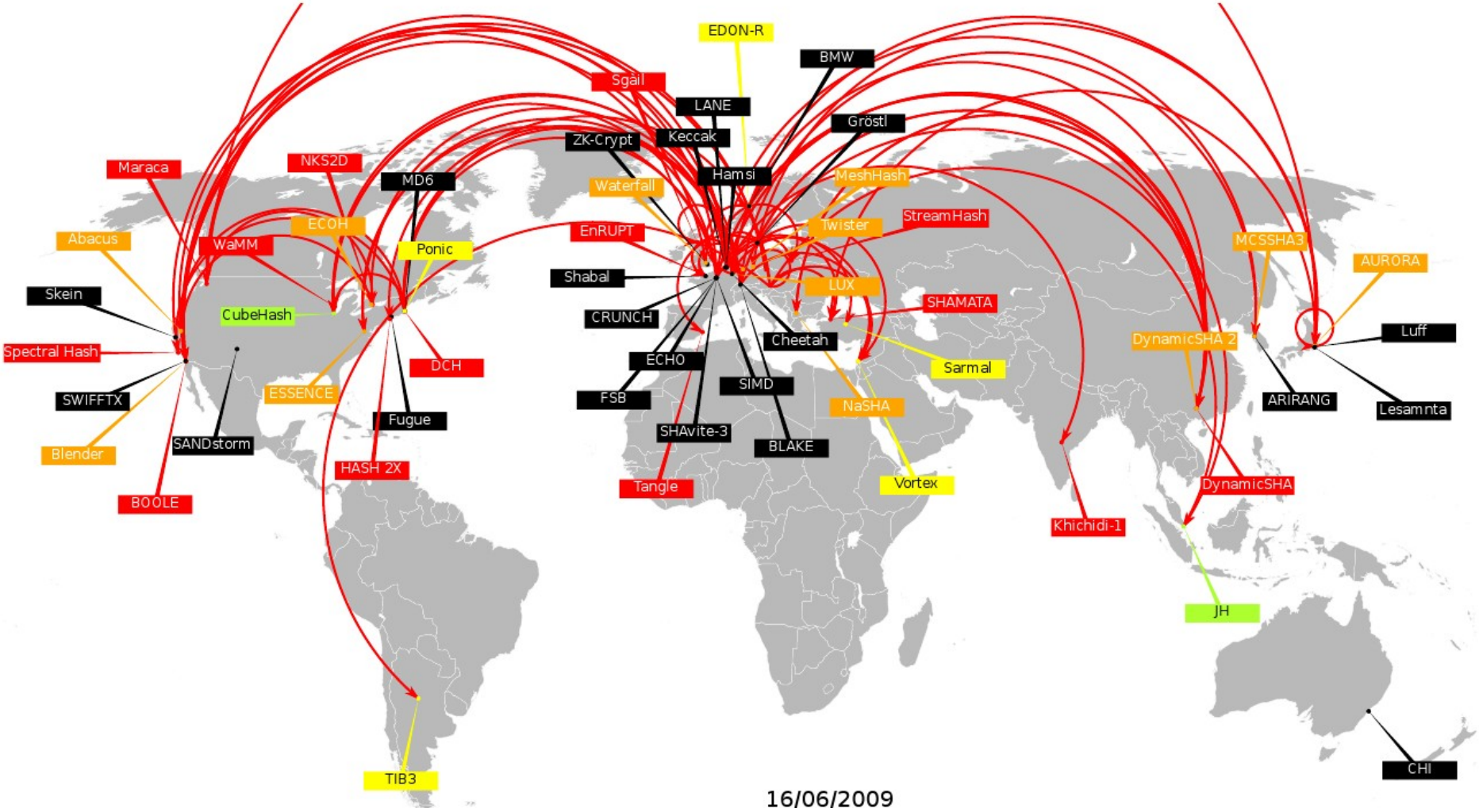
- Strong international integration
- IACR: 1600 members
- ECRYPT II (www.ecrypt.eu.org)
  - Strong network of European players
  - Leading position internationally
  - Key length and algorithms paper
- Standardization: driven by NIST (US)
- Individual member states set their own crypto policies

Independent evaluation efforts
(mostly symmetric algorithms

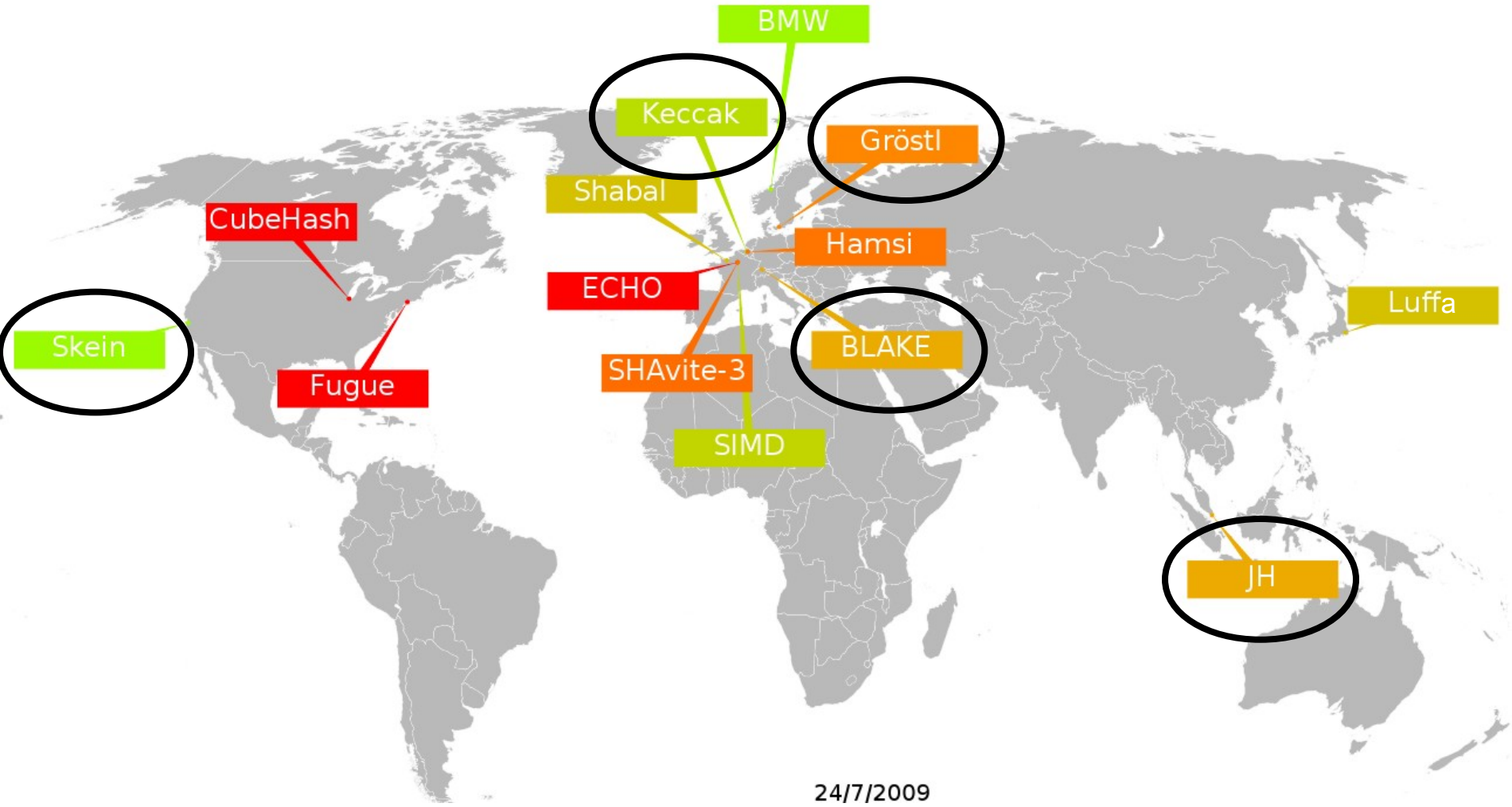
- NIST AES competition (US) (1997-2001): block cipher
- CRYPTREC (Japan) (2000-2003 and 2010-2012): cryptographic algorithms and protocols for government use in Japan
- IST-NESSIE Project (EU) (2000-2003): new cryptographic primitives
- EU ECRYPT: eSTREAM (2004-2008): stream ciphers
- NIST SHA-3 competition (US) (2007-2012): hash function

- ? Authenticated encryption ?
- ? Lightweight cryptography?

SHA-3 Preliminary Cryptanalysis



SHA-3: 5 Finalists

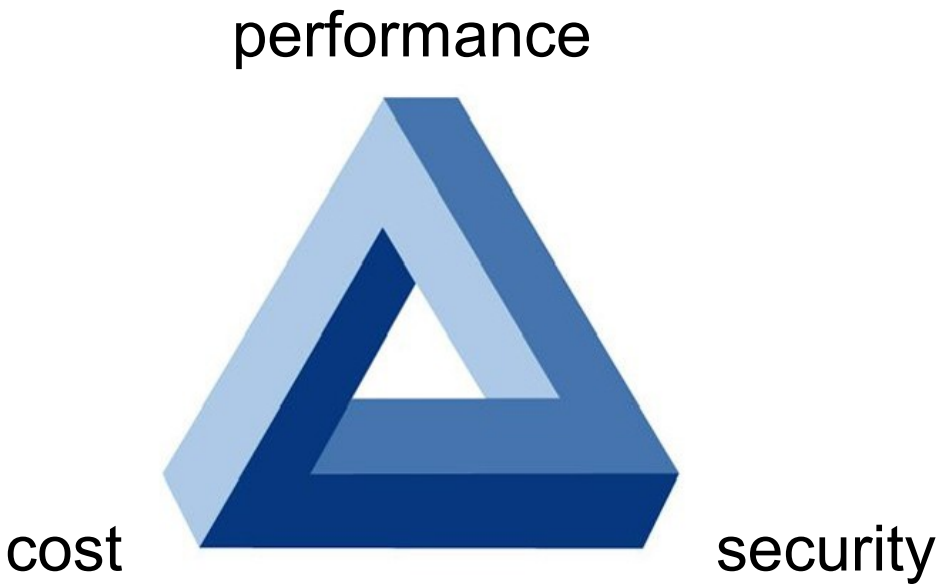


Challenges for crypto

- security for 50-100 years (post-quantum)
- authenticated encryption of Terabit/s networks
- ultra-low footprint/power/energy

secure software and hardware implementations

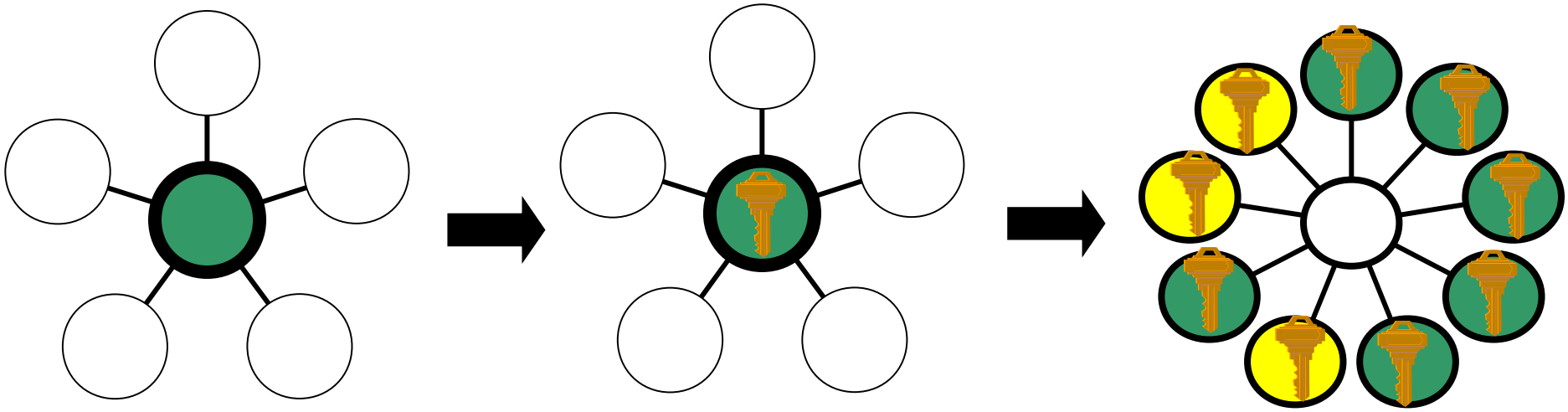
algorithm agility



Distributed computing

multiparty computation and fully homomorphic encryption

- Data can be centralized but in protected (encrypted) form
  - still allows limited processing
- Data can be stored and processed locally
  - example: road pricing



Specific targets for collaboration

- Cryptography for the Internet of Things (IoT)
  - lightweight crypto
  - authenticated encryption
- Cryptography for the cloud
  - Privacy-friendly data processing
  - E-voting
- Tools
  - secure implementations
  - cryptanalysis