Somethings Never Change

Claudia Diaz, Nele Mentens, Bart Preneel, Vincent Rijmen, Nigel Smart,
Ingrid Verbauwhede, Fre Vercauteren

Including my spelling ability

Some Things Never Change

Claudia Diaz, Nele Mentens, Bart Preneel, Vincent Rijmen, Nigel Smart,
Ingrid Verbauwhede, Fre Vercauteren

Somethings in Cryptography are constant….

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore’s Law) will soon end.

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore’s Law) will soon end.
- CRYPTO will be held in Santa Barbara

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore’s Law) will soon end.
- CRYPTO will be held in Santa Barbara
  - With prawns on Sunday
  - Margerita’s on Wednesday
  - Bagels and Waffles for breakfast

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore’s Law) will soon end.
- CRYPTO will be held in Santa Barbara
- The (all) government(s) want(s) access to your keys

Somethings in Cryptography are constant….

- ❑ The expected number of years until a quantum computer is built
- ❑ Computer performance improvement (Moore’s Law) will soon end.
- ❑ CRYPTO will be held in Santa Barbara
- ❑ The (all) government(s) want(s) access to your keys
- ❑ Papers on obfuscation are obfuscated for mere mortals

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore's Law) will soon end.
- CRYPTO will be held in Santa Barbara
- The (all) government(s) want(s) access to your keys
- Papers on obfuscation are obfuscated for mere mortals
- Car key fobs with 40-bit keys

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore’s Law) will soon end.
- CRYPTO will be held in Santa Barbara
- The (all) government(s) want(s) access to your keys
- Papers on obfuscation are obfuscated for mere mortals
- Car key fobs with 40-bit keys
- Academic papers with 1024 bit RSA and 80 bit symmetric key sizes

Somethings in Cryptography are constant….

- ❑ The expected number of years until a quantum computer is built
- ❑ Computer performance improvement (Moore’s Law) will soon end.
- ❑ CRYPTO will be held in Santa Barbara
- ❑ The (all) government(s) want(s) access to your keys
- ❑ Papers on obfuscation are obfuscated for mere mortals
- ❑ Car key fobs with 40-bit keys
- ❑ Academic papers with 1024 bit RSA and 80 bit symmetric key sizes
- ❑ Belgium wins a NIST completion for a crypto standard

Somethings in Cryptography are constant….

- The expected number of years until a quantum computer is built
- Computer performance improvement (Moore's Law) will soon end.
- CRYPTO will be held in Santa Barbara
- The (all) government(s) want(s) access to your keys
- Papers on obfuscation are obfuscated for mere mortals
- Ca key fobs with 40-bit keys
- Academic papers with 1024 bit RSA and 80 bit symmetric key sizes
- Belgium wins a NIST completion for a crypto standard

- And some people always seeming to need more staff…….

Bristol is Hiring……

B[illegible] is Hiring……

LEUVEN

We are hiring many PhDs and PostDocs

We have current jobs in the following areas

- Machine Learning for Network Intrusion (PhD)
- Protocol Design and Analysis (PhD/PostDoc)
- Applied MPC (PhD/PostDoc)
- Secure Positioning (PhD)
- Secure Distance Bounding (PhD/PostDoc)
- V2X Security (PhD/PostDoc)
- Security and Privacy in P2P Electricity Trading (PhD/PostDoc)
- Provable Security for Lightweight Symmetric Cryptography (PhD)
- Distributed Consensus and Blockchains (PhD/PostDoc)
- Cryptography Secured Against Physical Attacks (PhD)

With more to come in next few weeks

More details

https://www.esat.kuleuven.be/cosic/vacancies/