ETH zürich

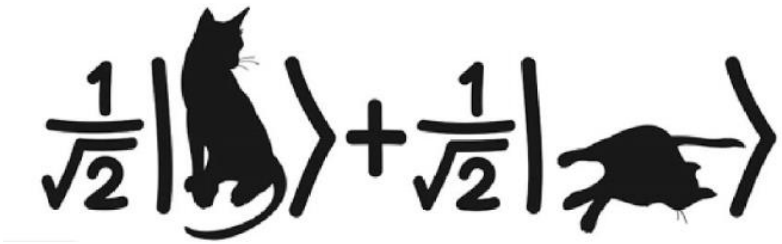
D-INFK, Information Security, Applied Crypto

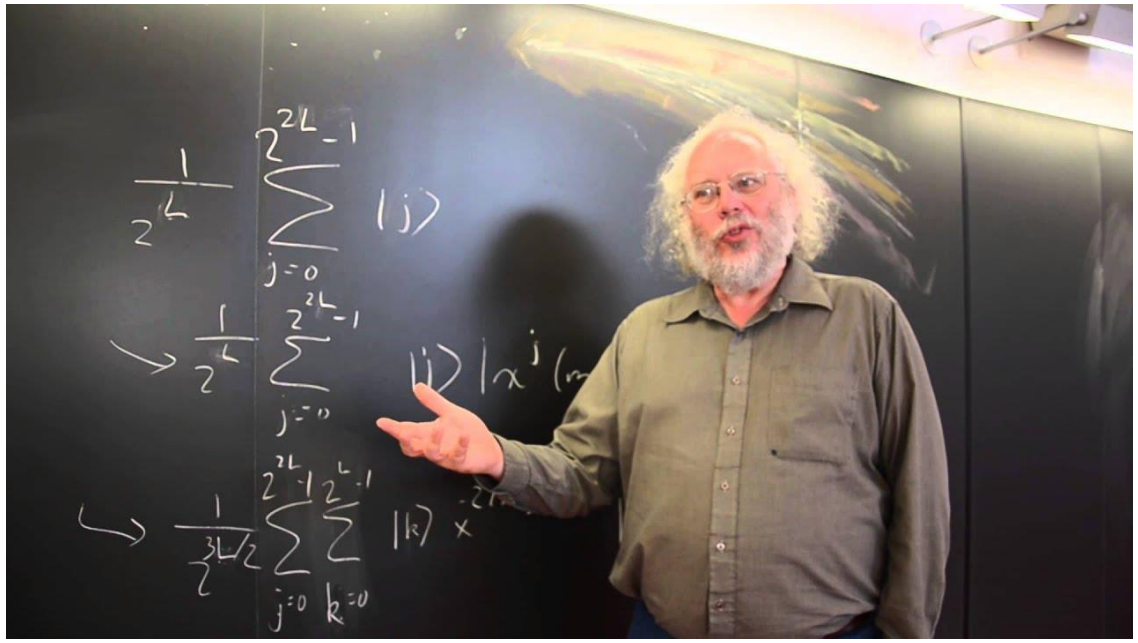
Internet Security in the Quantum Era

Prof. Kenny Paterson

(D-INFK, Institute of Information Security, Applied Cryptography Group)

Quantum Computing – Shor's Algorithm



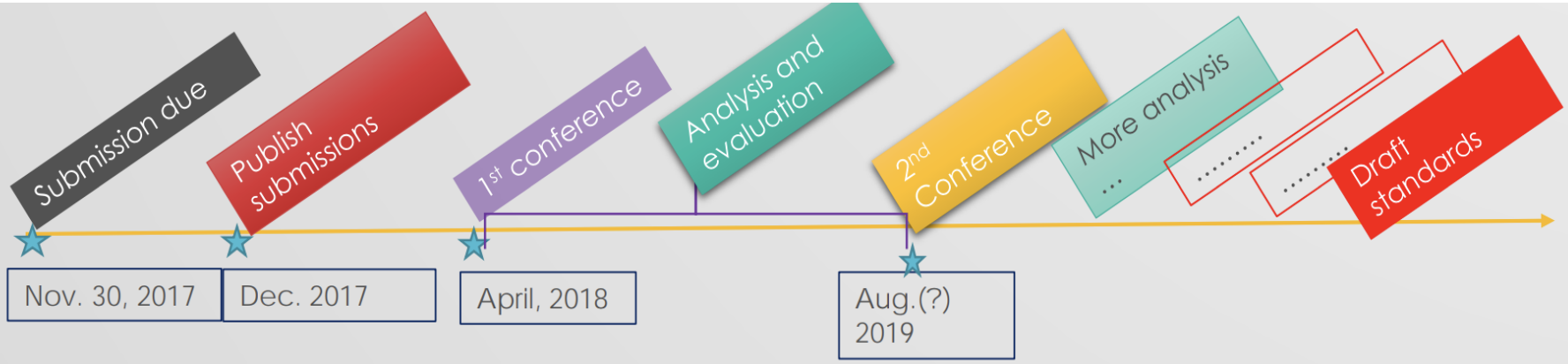


Basic tenet of quantum physics: superposition

https://www.youtube.com/watch?v=hOlOY7NyMfs

Quantum Computing and Classical Cryptography

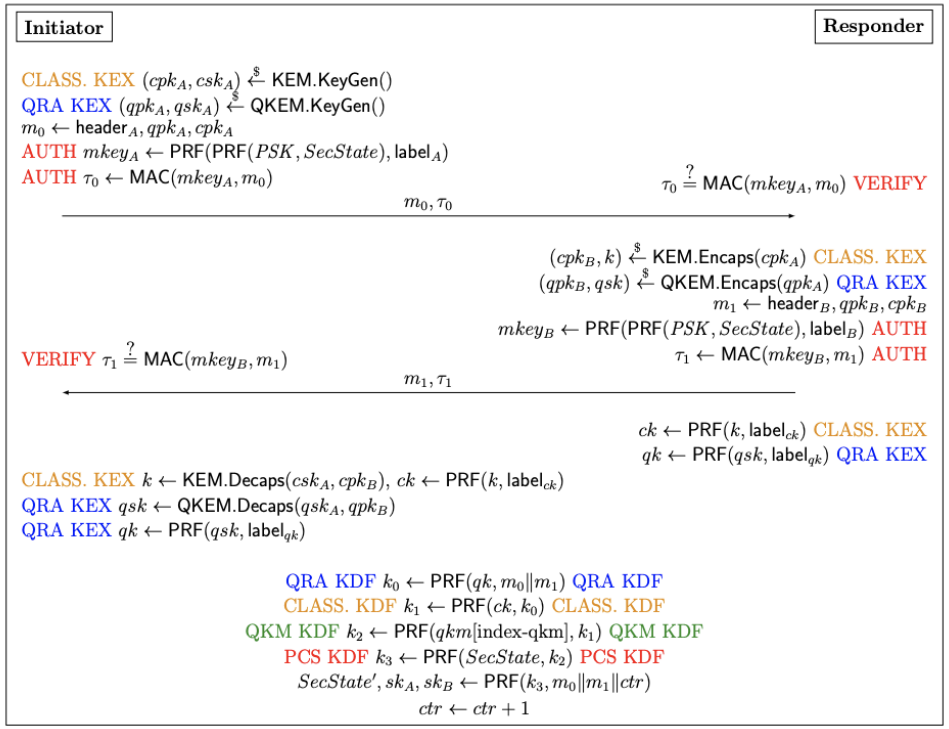
- Everyday life as we know it depends heavily on public-key cryptography.
- Shor's algorithm breaks all currently-deployed public-key cryptographic algorithms.
- The advent of large scale quantum computing would be catastrophic for Internet security.
- A global effort is underway to research and prepare for deployment a new generation of cryptographic algorithms.
- The process is led by US government National Institute of Standards and Technology (NIST).



https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

ETH Involvement: Applied Cryptography Group

- We are co-designers of one of the finalist algorithms, «merged classic McEliece», see:
  - https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement
- We are developing *hybrid* approaches to safely and smoothly integrate the new algorithms into existing Internet security protocols, see:
  - https://www.research-collection.ethz.ch/handle/20.500.11850/399145
- We are active in IETF/IRTF, the bodies responsible for maintaining specifications for Internet procotols:
  - https://www.ietf.org/
  - https://irtf.org/cfrg



$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{HAKE},\mathsf{clean}_{\mathsf{cHAKE}},\mathcal{A}}_{\mathsf{Muckle},n_P,n_S,n_T}(\lambda) \leq \\
&2 \cdot n_P^2 n_S n_T \cdot \left(\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{A}}(\lambda) + \mathsf{Adv}^{\mathsf{eufcma}}_{\mathsf{MAC},\mathcal{A}}(\lambda)\right) \\
&+ n_P^2 n_S^2 n_T \cdot \left(\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{KEM},\mathcal{A}}(\lambda) + (13 + 2 \cdot n_T) \cdot \mathsf{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{A}}(\lambda)\right. \\
&\left. + \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{KEM},\mathcal{A}}(\lambda) + (13 + 2 \cdot n_T) \cdot \mathsf{Adv}^{\mathsf{dual\text{-}prf}}_{\mathsf{PRF},\mathcal{A}}(\lambda)\right)
\end{aligned}$$

ETH zürich

Thank you for your attention!

Professor Kenny Paterson
kenny.paterson@inf.ethz.ch

ETH Zürich
Applied Cryptography Group
CNB E 104
Universitätstrasse 6
8092 Zurich, Switzerland

www.appliedcrypto.ethz.ch