

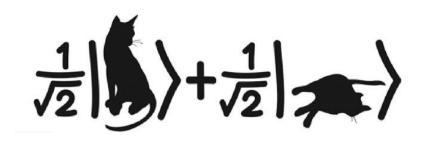
D-INFK, Information Security, Applied Crypto

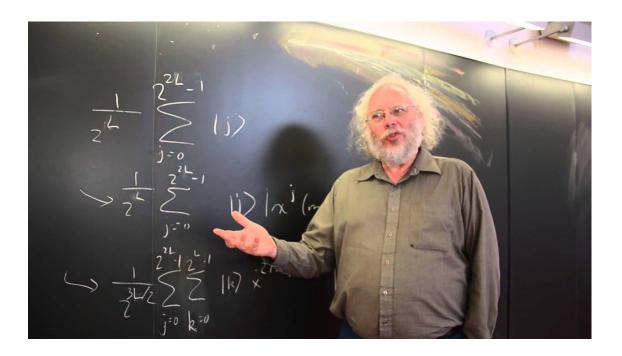
# Internet Security in the Quantum Era

#### **Prof. Kenny Paterson**

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

### Quantum Computing – Shor's Algorithm





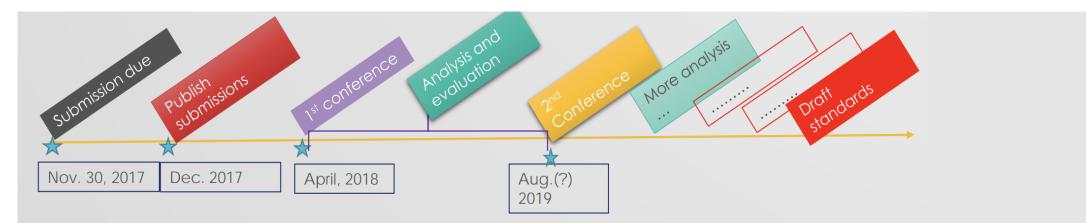
Basic tenet of quantum physics: superposition

#### https://www.youtube.com/watch?v=hOIOY7NyMfs



## 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 zürich Kenny Paterson, D-INFK, Information Security, Applied Crypto Group

## ETH Involvement: Applied Cryptography Group

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

| Initiator  | Responder   |
|--|---|
| Initiator  | Responder   |
| CLASS KEX $(cnk_A, csk_A) \notin KFM KevGen()$   |   |
| CLASS. KEX $(cpk_A, csk_A) \stackrel{\&}{\leftarrow} \text{KEM.KeyGen}()$<br>QRA KEX $(qpk_A, qsk_A) \stackrel{\&}{\leftarrow} \text{QKEM.KeyGen}()$ |   |
| $m_0 \leftarrow \text{header}_A, qpk_A, cpk_A$   |   |
| <b>AUTH</b> $mkey_A \leftarrow PRF(PRF(PSK, SecState), label_A)$   |   |
| $\textbf{AUTH} \ \tau_0 \leftarrow \textsf{MAC}(mkey_A, m_0)$  | $\tau_0 \stackrel{?}{=} MAC(mkey_A, m_0)$ VERIFY  |
| $m_0, 	au_0$   |   |
|  |   |
|  | $(cpk_B, k) \stackrel{\$}{\leftarrow} KEM.Encaps(cpk_A) \ CLASS. \ KEX$   |
|  | $(qpk_B, qsk) \stackrel{\$}{\leftarrow} QKEM.Encaps(qpk_A) \operatorname{QRA} \operatorname{KEX} m_1 \leftarrow header_B, qpk_B, cpk_B$ |
|  | $m_1 \leftarrow \text{Header}_B, q_{PKB}, e_{PKE}$<br>$m_1 \leftarrow \text{Header}_B, q_{PKB}, e_{PKE}$                                |
| <b>VERIFY</b> $\tau_1 \stackrel{?}{=} MAC(mkey_B, m_1)$  | $\tau_1 \leftarrow MAC(mkey_B, m_1)$ AUTE   |
| $m_1, \tau_1$  | ·1····································  |
| 4  |   |
|  | $ck \leftarrow PRF(k, label_{ck}) \ \mathbf{CLASS}. \ \mathbf{KEX}$   |
|  | $qk \leftarrow PRF(qsk, label_{qk}) \ QRA \ KEX$  |
| CLASS. KEX $k \leftarrow KEM.Decaps(csk_A, cpk_B), ck \leftarrow PR$   | $F(k,label_{ck})$   |
| $\mathbf{QRA} \text{ KEX} qsk \leftarrow QKEM.Decaps(qsk_A, qpk_B)$  |   |
| $QRA KEX qk \leftarrow PRF(qsk, label_{qk})$   |   |
| OPA KDE h / DPE/   | $(qk, m_0    m_1)$ QRA KDF  |
| •  | $(ck, m_0  m_1)$ GRA KDF<br>RF $(ck, k_0)$ CLASS. KDF   |
| -  | $[index-qkm], k_1$ QKM KDF  |
|  | SecState, $k_2$ ) PCS KDF   |
|  | $- PRF(k_3, m_0    m_1    ctr)$   |
| , 11, 2  | ctr + 1   |

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

#### **ETH** zürich

## **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

