

# Unclooneable Encryption

Daniel Gottesman

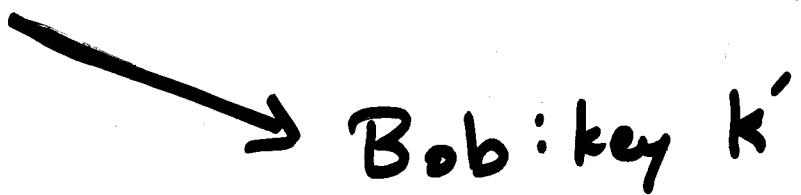
# Cloning Attack

Alice: message  $m$ , key  $k$

1) Encrypt message  $E_k(m)$



2) Copy message  $E_k(m)$



3) Bob receives message, decrypts  $m$

4) Eve learns key  $k'$

$$k' + E_k(m) \rightarrow m$$

(e.g. Eve steals  $k'$ , breaks computational assumption, ...)

# Undoneable Encryption

Classical message  $m$

Key  $k$

Undoneable encryption is secure vs. cloning attack:

$$m \mapsto E_k(m) \quad (\text{quantum state})$$

Eve:  $E_k(m) \mapsto \rho_k^{\text{BE}}(m)$

Bob receives  $\text{tr}_E \rho_k^{\text{BE}}(m)$

Eve keeps  $\rho_k(m) = \text{tr}_B \rho_k^{\text{BE}}(m)$

$\forall m, m'$   $\forall$  attacks, either:

1) Bob detects Eve w/ high prob.

or

2)  $F(\rho_k(m), \rho_k(m')) \geq 1 - \varepsilon$

(Eve's residual state does not depend on  $m$ )

# Quantum Authentication

quant-ph/0205158

Quantum message  $|ψ\rangle$

Key  $k$

Authentication scheme  $A_k(|ψ\rangle)$

Quantum authentication is  
secure if:  $\forall |ψ\rangle,$

$\forall$  strategies by Eve, either  
Bob almost always detects her  
or the final decoded state has  
high fidelity to  $|ψ\rangle$

Note:

Quantum authentication scheme  
must encrypt message  $|ψ\rangle$

# Encryption is necessary

Suppose Eve can distinguish (almost) messages  $|0\rangle$  and  $|1\rangle$  (sent as  $\rho_0, \rho_1$ )

Then  $\rho_0 = \begin{pmatrix} v_0 & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\rho_1 = \begin{pmatrix} 0 & 0 \\ 0 & v_1 \end{pmatrix}$   
(or close)

$\Rightarrow$  Eve maps  $v_0 \mapsto v_0$   
 $v_1 \mapsto (-1)v_1$

Effect: message  $|0\rangle + |1\rangle$   
(almost) becomes  $|0\rangle - |1\rangle$

Eve can change the message.

# Encryption is necessary

Suppose Eve can distinguish  $\rho_0$  (representing  $|0\rangle$ ) and  $\rho_1$  (for  $|1\rangle$ ) by  $\epsilon$ . (e.g. trace distance)

$\Rightarrow \rho_0^{\otimes t} \text{ and } \rho_1^{\otimes t}$  are distinguishable  
by  $\sim t\epsilon$

When  $t \sim 1/\epsilon$ , Eve can change  
message  $|0^{\otimes t}\rangle + |1^{\otimes t}\rangle$  to  
 $|0^{\otimes t}\rangle - |1^{\otimes t}\rangle$

Thm.: Encryption is necessary

Cor.: Digitally signing quantum states  
is impossible (info.-theoretically)

Thm.: Digitally signing quantum states  
is impossible, even with computational  
security.

# Quantum Authentication ⇒ Uncloakable Encryption

Classical message  $m$  (basis state  $|m\rangle$ )

Key  $k$

Authentication scheme  $A_k(\cdot)$

Security of authentication  $\Rightarrow$

$$|m\rangle \mapsto |m\rangle_{\text{Bob}} \otimes |\phi_k(m)\rangle_{\text{Eve}} + O(\epsilon)$$

$$|m'\rangle \mapsto |m'\rangle_{\text{Bob}} \otimes |\phi_k(m')\rangle_{\text{Eve}} + O(\epsilon)$$

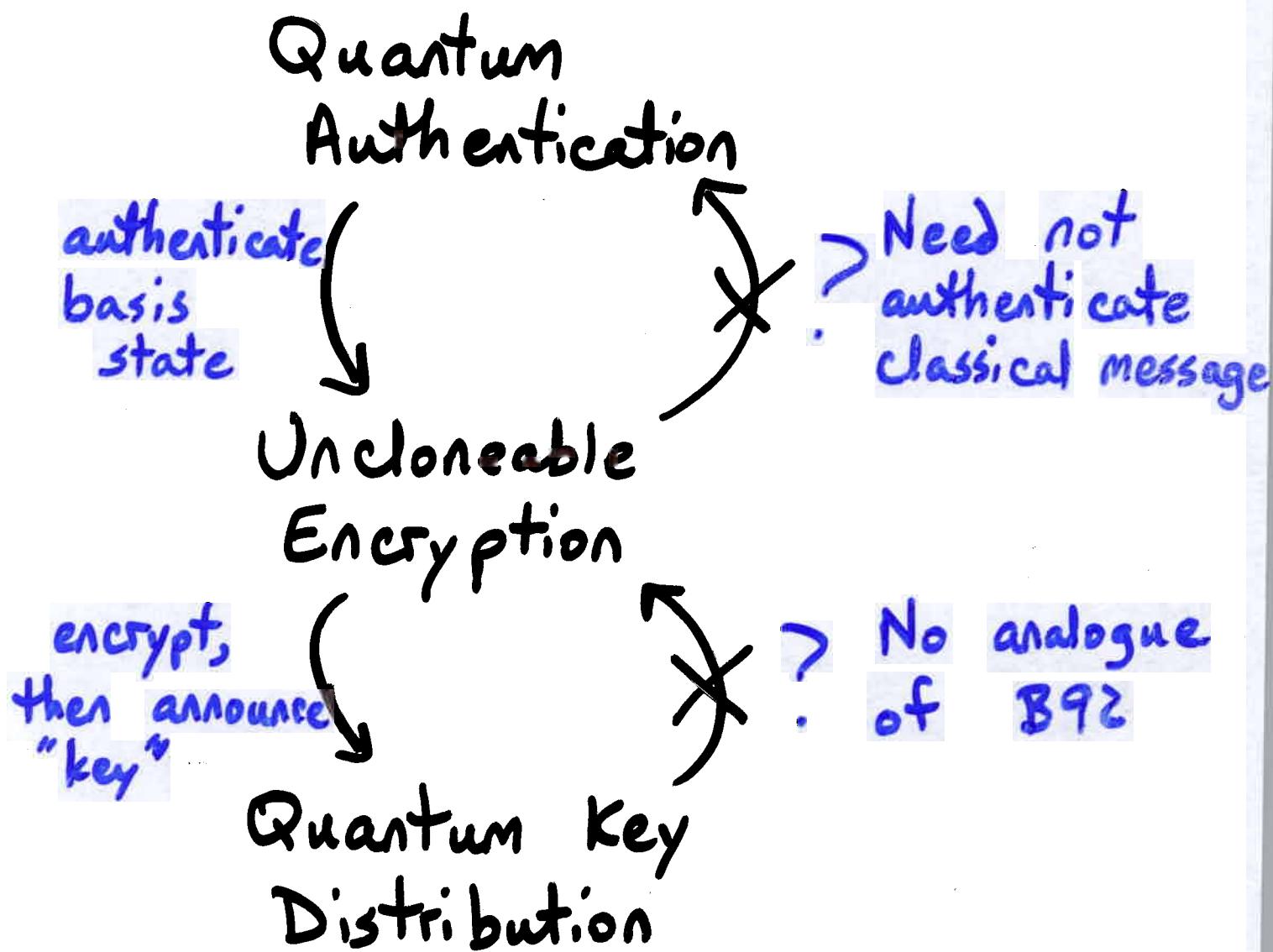
Linearity  $\Rightarrow$

$$|m\rangle + |m'\rangle \mapsto |m\rangle \otimes |\phi_k(m)\rangle + |m'\rangle \otimes |\phi_k(m')\rangle + O(\epsilon)$$

This has high fidelity to  $|m\rangle + |m'\rangle$

$$\Rightarrow \langle \phi_k(m) | \phi_k(m') \rangle \geq 1 - O(\epsilon)$$

# Relationships of Protocols



# Practical Undoable Encryption

BB84 analogue:

- 1) Alice encrypts and authenticates message  $m$ , key  $k_1$
- 2) Alice encodes result with fixed error-correcting code, syndrome  $s$
- 3) Alice adds random bits & multiplies by fixed matrix (code w/ large distance)  
(= inverse privacy amplification)
- 4) Chooses + or X basis for each bit from key  $k_2$
- 5) Sends appropriate quantum states

Bob has key  $k = (k_1, k_2, s)$ , can extract message  $m$

## Improvements vs. QKD

- Noninteractive
- Possible computational security:  
Eve must break computational assumption before Bob receives quantum states
- Efficient key use  
(= random #s, classical communication in QKD)
- Stronger security condition
- More efficient intrusion detection

### Disadvantage:

- Most photons must arrive  
(i.e., good single-photon states, low absorption, efficient detectors)

# Temporary Computational Assumption

Undoneable encryption  $E_k(m)$   
(derived from authentication)

Assume  $k$  is not shared random sequence, but pseudorandom sequence  
(pseudorandom  $\Leftrightarrow$  Eve cannot efficiently distinguish from random)

If Eve can break  $E_k(m)$ , she can break pseudorandom sequence

To distinguish random  $k$  & pseudorandom:

- Eve sends fake message  $|m\rangle + |m'\rangle$
- Attempts to break:  
Failure  $\Rightarrow$  receives  $|m\rangle + |m'\rangle$   
 $\Rightarrow$  random  $k$

Success  $\Rightarrow$  receives mixture  $\{|m\rangle, |m'\rangle\}$   
 $\Rightarrow$  pseudorandom  $k$

## Outlook

- There are new quantum cryptographic protocols other than QKD
- Cryptography for classical data is intimately connected to cryptography for quantum data