Uncloneable Encryption

Daniel Gottesman

Cloning Attack

Alice: message m, key k

1) Encrypt message $E_k(m)$

$\longrightarrow$ Eve

2) Copy message $E_k(m)$

$\longrightarrow$ Bob: key k'

3) Bob receives message, decrypts m

4) Eve learns key k'

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

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

Uncloneable Encryption

Classical message m

Key k

Uncloneable encryption is secure vs. cloning attack:

$m \longmapsto E_k(m)$ (quantum state)

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

Bob receives $tr_E\, \rho_k^{BE}(m)$

Eve keeps $\rho_k(m) = tr_B\, \rho_k^{BE}(m)$

$\forall\, m, m'$ $\forall$ 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 $|\psi\rangle$

Key k

Authentication scheme $A_k(|\psi\rangle)$

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

$\forall$ strategies by Eve, either

Bob almost always detects her

or the final decoded state has

high fidelity to $|\psi\rangle$

Note:

Quantum authentication scheme

must encrypt message $|\psi\rangle$

Encryption is necessary

Suppose Eve can distinguish (almost) messages $|0\rangle$ and $|1\rangle$ (sent as ρ_0, ρ_1)

Then $\rho_0 = \left(\begin{array}{c|c} V_0 & 0 \\ \hline 0 & 0 \end{array}\right)$, $\rho_1 = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & V_1 \end{array}\right)$ (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 ρ_0 (representing $|0\rangle$) and ρ_1 (for $|1\rangle$) by ϵ. (e.g. trace distance)

$\Rightarrow \rho_0^{\otimes t}$ & $\rho_1^{\otimes t}$ 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
$\Rightarrow$ Uncloneable Encryption

Classical message m (basis state $|m\rangle$)
Key k
Authentication scheme $A_k(\cdot)$

Security of authentication $\Rightarrow$

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

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

Linearity $\Rightarrow$

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

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

Quantum Authentication

authenticate basis state

?

Need not authenticate classical message

Uncloneable Encryption

encrypt, then announce "key"

?

No analogue of B92

Quantum Key Distribution

Practical Uncloneable 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

Uncloneable 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