Quantum non-malleability and authentication – Information theoretic security + ~~sneak preview~~ teaser

based on arXiv:1610.04214 and arXiv:1709.06539

Christian Majenz
QuSoft/University of Amsterdam
Joint work with Gorjan Alagic, NIST and University of Maryland,
and Tommaso Gagliardoni, IBM Zurich

Quantum Innovators, IQC, University of Waterloo

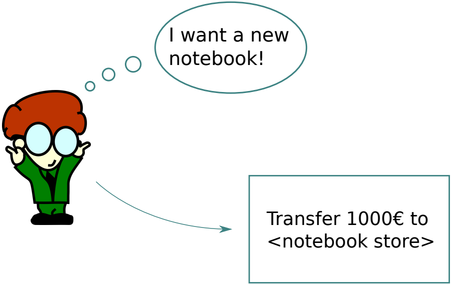
20.09.2017

Motivation: a classical story...

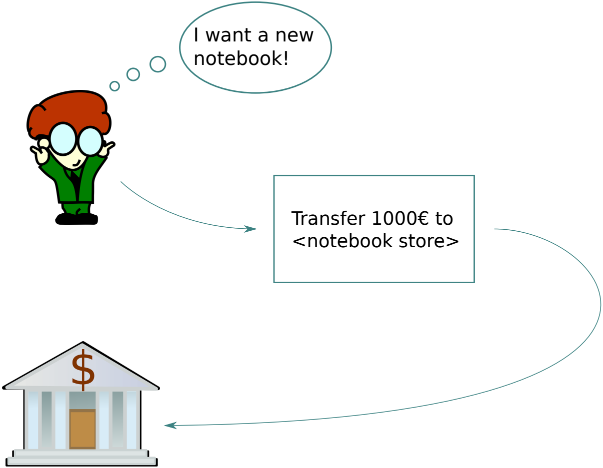
Crypto for bank transfers

Crypto for bank transfers

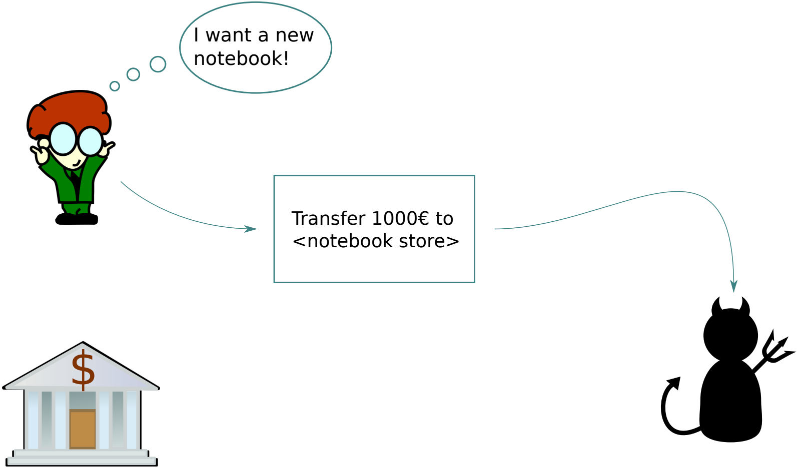
Crypto for bank transfers



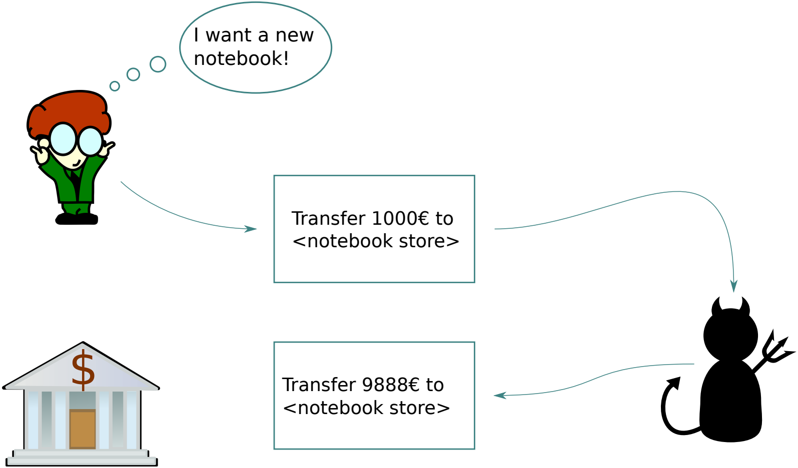
Crypto for bank transfers



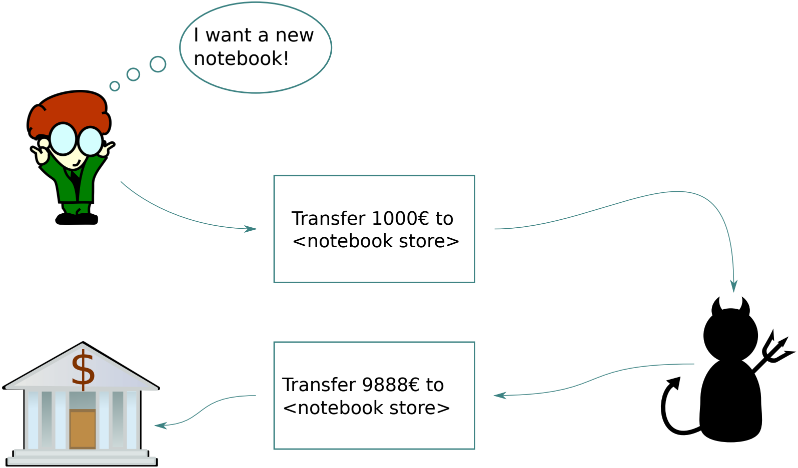
Crypto for bank transfers



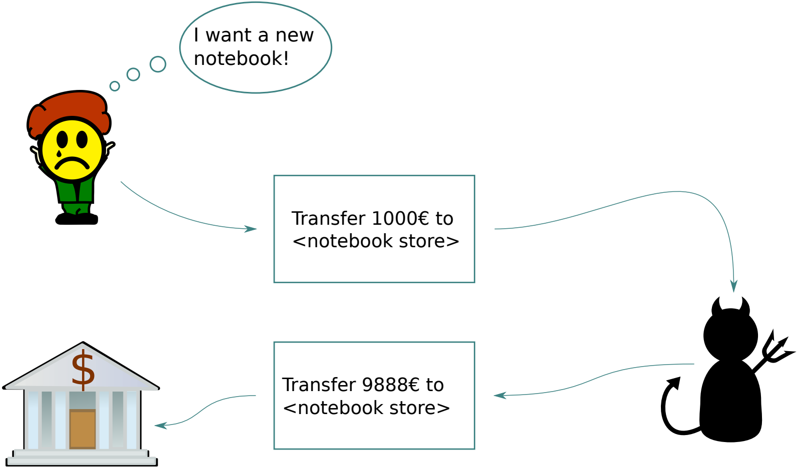
Crypto for bank transfers



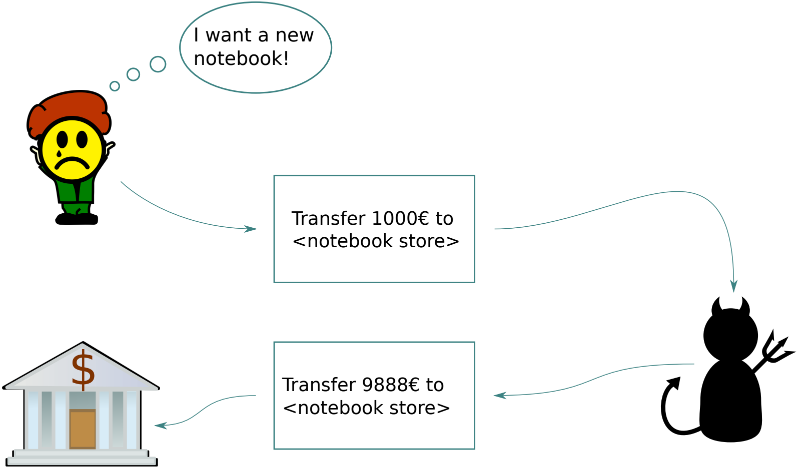
Crypto for bank transfers



Crypto for bank transfers



Crypto for bank transfers



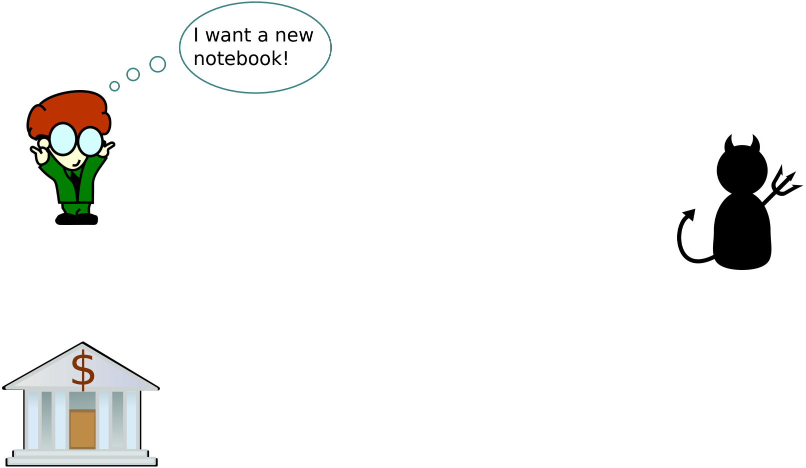
- What cryptographic security notions would fix this problem?

Non-malleability

- One solution is non-malleable encryption:

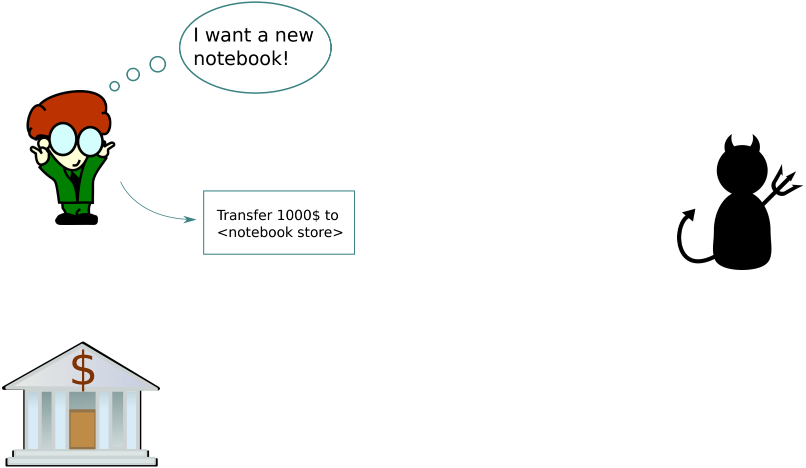
Non-malleability

- One solution is non-malleable encryption:



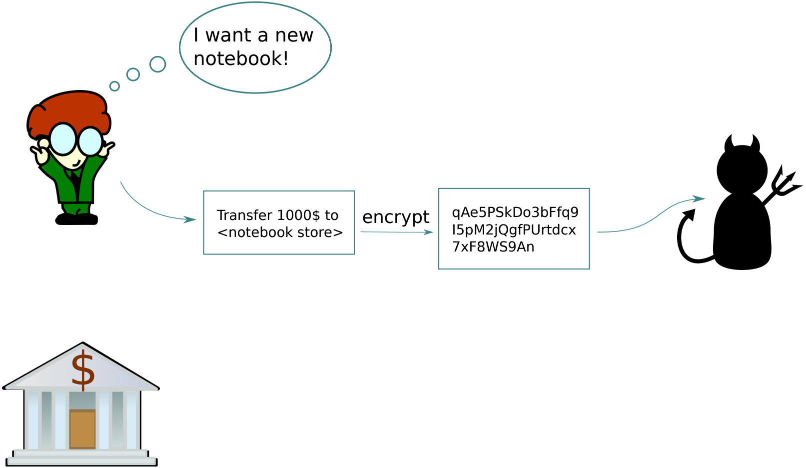
Non-malleability

- One solution is non-malleable encryption:



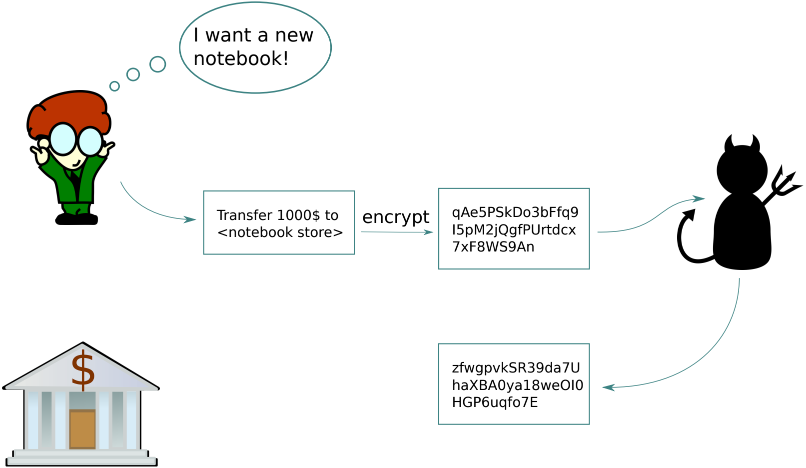
Non-malleability

- One solution is non-malleable encryption:



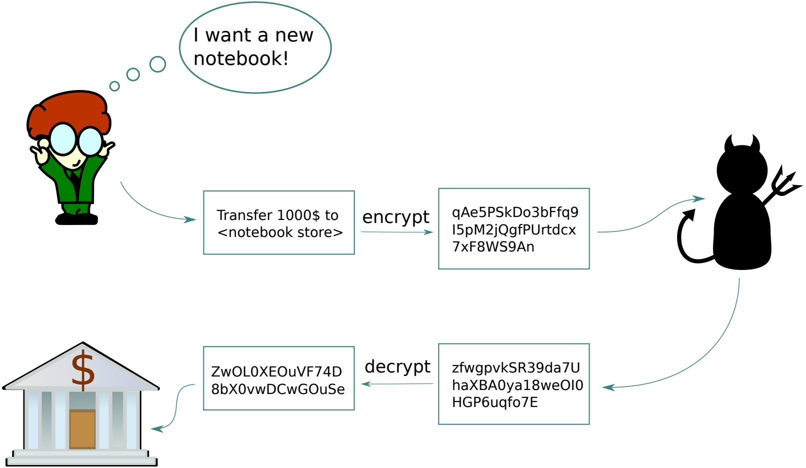
Non-malleability

- One solution is non-malleable encryption:



Non-malleability

- One solution is non-malleable encryption:



Outline

Non-malleability

classical non-malleability (NM)

- NM first defined in the context of public key cryptography (Dolev, Dwork, Naor '95):

classical non-malleability (NM)

- NM first defined in the context of public key cryptography (Dolev, Dwork, Naor '95):

Definition (informal)

An encryption scheme is non-malleable if for any relation R on plaintexts, getting an encryption of x does not help with producing an encryption of $x' \neq x$ such that $R(x, x')$.

classical non-malleability (NM)

- NM first defined in the context of public key cryptography (Dolev, Dwork, Naor '95):

Definition (informal)

An encryption scheme is non-malleable if for any relation R on plaintexts, getting an encryption of x does not help with producing an encryption of $x' \neq x$ such that $R(x, x')$.

Example: Adversary wants to increase amount, relation is "$\leq$"

classical non-malleability (NM)

- NM first defined in the context of public key cryptography (Dolev, Dwork, Naor '95):

Definition (informal)

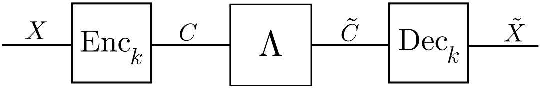
An encryption scheme is non-malleable if for any relation R on plaintexts, getting an encryption of x does not help with producing an encryption of $x' \neq x$ such that $R(x, x')$.

Example: Adversary wants to increase amount, relation is "$\leq$"

- Information theoretic definition using entropy:
  (X, C), $(\tilde{X}, \tilde{C})$ two plaintext ciphertext pairs, $C \neq \tilde{C}$

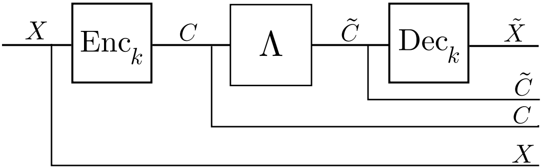
def: scheme is NM if $I(\tilde{X} : \tilde{C}|XC) = 0$ (Hanaoka et al. '02)

- Classical NM:



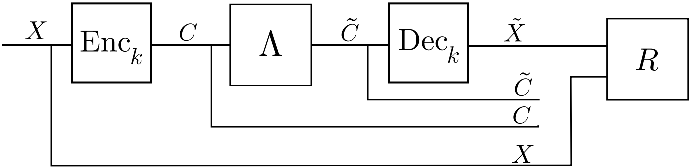
the no-cloning problem

- Classical NM:

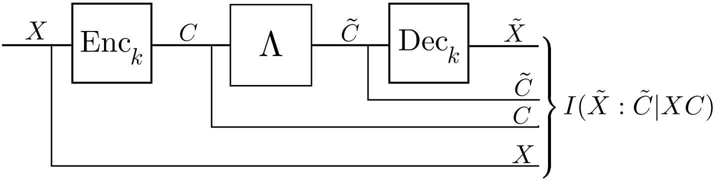


the no-cloning problem

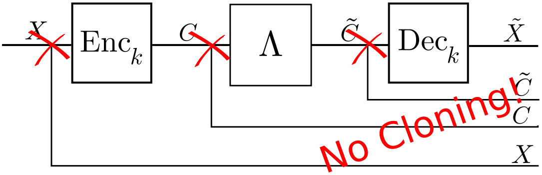
- Classical NM:



- Classical NM:



- Quantum NM:



X
Enc_k
C
Λ
$\tilde{C}$
Dec_k
$\tilde{X}$
$\tilde{C}$
C
X
No Cloning!

Quantum symmetric key encryption

def: Quantum encryption scheme: $(\mathrm{Enc}_k, \mathrm{Dec}_k)$

- classical uniformly random key k
- encryption map $(\mathrm{Enc}_k)_{A \to C}$, decryption map $(\mathrm{Dec}_k)_{C \to \bar{A}}$

Quantum symmetric key encryption

def: Quantum encryption scheme: $(\mathrm{Enc}_k, \mathrm{Dec}_k)$

- classical uniformly random key k
- encryption map $(\mathrm{Enc}_k)_{A \to C}$, decryption map $(\mathrm{Dec}_k)_{C \to \bar{A}}$
- $\mathcal{H}_{\bar{A}} = \mathcal{H}_A \oplus \mathbb{C} \ket{\perp}$

Quantum symmetric key encryption

def: Quantum encryption scheme: $(\mathrm{Enc}_k, \mathrm{Dec}_k)$

- classical uniformly random key k
- encryption map $(\mathrm{Enc}_k)_{A\to C}$, decryption map $(\mathrm{Dec}_k)_{C\to\bar{A}}$
- $\mathcal{H}_{\bar{A}} = \mathcal{H}_A \oplus \mathbb{C}\,|\perp\rangle$
- correctness: $\mathrm{Dec}_k \circ \mathrm{Enc}_k = \mathrm{id}_A$

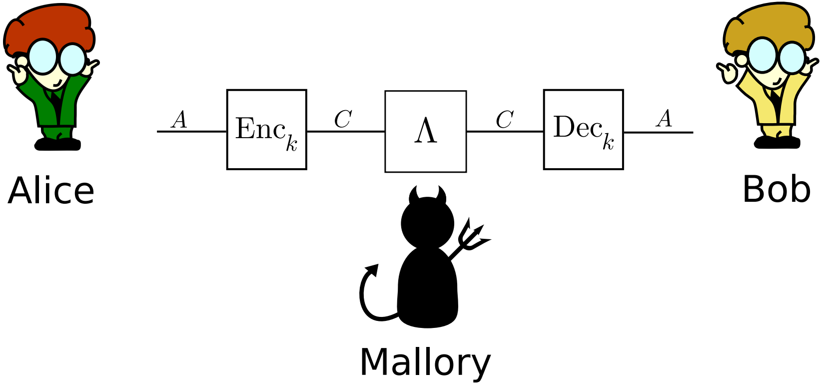
Quantum symmetric key encryption

def: Quantum encryption scheme: $(\mathrm{Enc}_k, \mathrm{Dec}_k)$

- classical uniformly random key k
- encryption map $(\mathrm{Enc}_k)_{A\to C}$, decryption map $(\mathrm{Dec}_k)_{C\to\bar{A}}$
- $\mathcal{H}_{\bar{A}} = \mathcal{H}_A \oplus \mathbb{C}\,|\perp\rangle$
- correctness: $\mathrm{Dec}_k \circ \mathrm{Enc}_k = \mathrm{id}_A$
- average encryption map: $\mathrm{Enc}_K = \mathbb{E}_k \mathrm{Enc}_k$

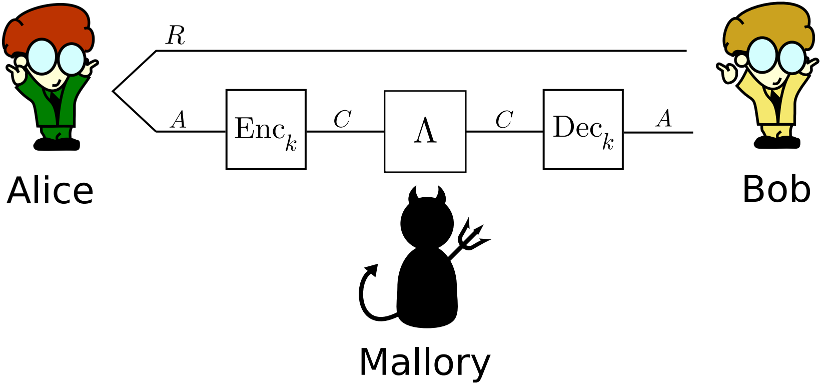
Setup for q-non-malleability

- Recall: classical non-malleability setup



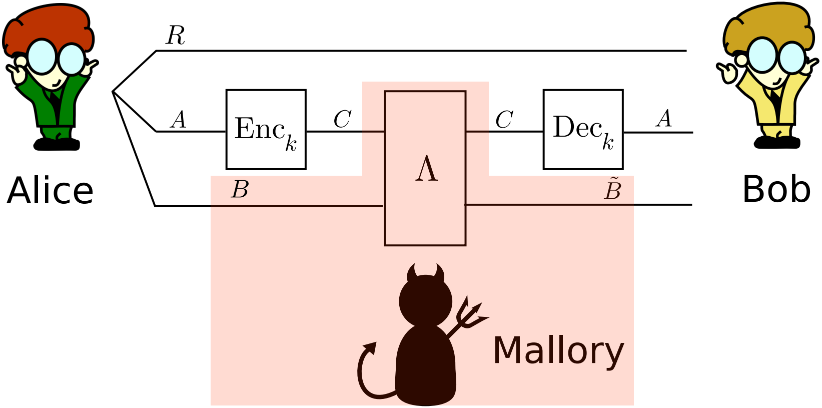
Setup for q-non-malleability

- Recall: classical non-malleability setup
- add reference system



Setup for q-non-malleability

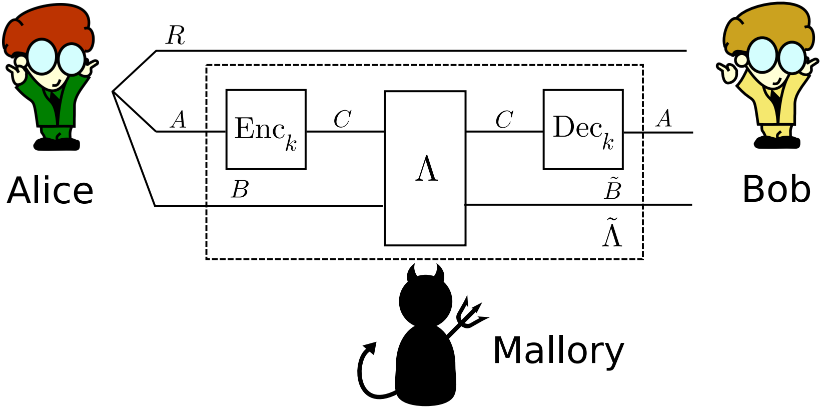
- Recall: classical non-malleability setup
- add reference system
- allow side info for adversary



Setup for q-non-malleability

- Recall: classical non-malleability setup
- add reference system
- allow side info for adversary

def: effective map on plaintexts and side info
$\tilde{\Lambda} = \mathbb{E}_k[\mathrm{Dec}_k \circ \Lambda \circ \mathrm{Enc}_k]$



The unavoidable attack

- Mallory can decide whether to intervene or not

The unavoidable attack

- Mallory can decide whether to intervene or not
- example:

$$\Lambda_{C\to C\tilde{B}} = p\,\mathrm{id}_C \otimes |0\rangle\langle 0|_{\tilde{B}} + (1-p)U_C(\cdot)U_C^\dagger \otimes |1\rangle\langle 1|_{\tilde{B}},$$

  Mallory tampers with the message with probability $1-p$, and records her choice.

The unavoidable attack

- Mallory can decide whether to intervene or not
- example:

$$\Lambda_{C\to C\tilde{B}} = p\,\mathrm{id}_C \otimes |0\rangle\langle 0|_{\tilde{B}} + (1-p)U_C(\cdot)U_C^\dagger \otimes |1\rangle\langle 1|_{\tilde{B}},$$

  Mallory tampers with the message with probability $1-p$, and records her choice.
- definition:

$$\begin{aligned} p_{=}(\Lambda_{CB\to C\tilde{B}}, \rho) =& \mathrm{tr}\left[(\phi^+_{CC'} \otimes \mathbb{1}_{\tilde{B}})\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'} \otimes \rho_B)\right] \\ =& F(\mathrm{tr}_{\tilde{B}}\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'} \otimes \rho_B), \phi^+_{CC'})^2 \end{aligned}$$

The unavoidable attack

- Mallory can decide whether to intervene or not
- example:

$$\Lambda_{C\to C\tilde{B}} = p\,\mathrm{id}_C \otimes |0\rangle\langle 0|_{\tilde{B}} + (1-p)U_C(\cdot)U_C^\dagger \otimes |1\rangle\langle 1|_{\tilde{B}},$$

  Mallory tampers with the message with probability $1-p$, and records her choice.
- definition:

$$\begin{aligned} p_=(\Lambda_{CB\to C\tilde{B}},\rho) =& \mathrm{tr}\left[(\phi^+_{CC'}\otimes \mathbb{1}_{\tilde{B}})\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes\rho_B)\right] \\ =& F(\mathrm{tr}_{\tilde{B}}\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes\rho_B),\phi^+_{CC'})^2 \end{aligned}$$

- "probability of Λ acting as the identity on C"

The unavoidable attack

- Mallory can decide whether to intervene or not
- example:

$$\Lambda_{C\to C\tilde{B}} = p\,\mathrm{id}_C \otimes |0\rangle\langle 0|_{\tilde{B}} + (1-p)U_C(\cdot)U_C^\dagger \otimes |1\rangle\langle 1|_{\tilde{B}},$$

  Mallory tampers with the message with probability $1-p$, and records her choice.
- definition:

$$\begin{aligned} p_=(\Lambda_{CB\to C\tilde{B}},\rho) =& \mathrm{tr}\left[(\phi^+_{CC'}\otimes \mathbb{1}_{\tilde{B}})\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes\rho_B)\right] \\ =& F(\mathrm{tr}_{\tilde{B}}\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes\rho_B),\phi^+_{CC'})^2 \end{aligned}$$

- "probability of Λ acting as the identity on C"

$\Rightarrow$ $p_=(\Lambda) = p$ for the example if $\mathrm{tr}(U_C) = 0$.

New definition

- idea: define NM such that Mallory cannot increase her correlations with the honest parties, except by the unavoidable attack

New definition

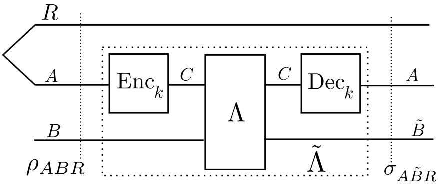
- idea: define NM such that Mallory cannot increase her correlations with the honest parties, except by the unavoidable attack

Definition (Quantum non-malleability (qNM))

A scheme $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *is non-malleable, if for all states* ρ_{ABR} *and all attacks* $\Lambda_{CB \to C\tilde{B}}$,

$$I(AR : \tilde{B})_\sigma \leq I(AR : B)_\rho$$

with $\sigma_{A\tilde{B}R} = \tilde{\Lambda}_{AB \to A\tilde{B}}(\rho_{ABR})$.



New definition

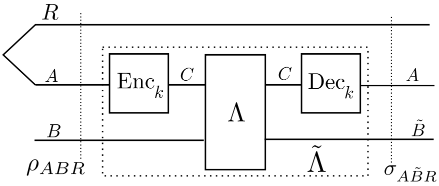
- idea: define NM such that Mallory cannot increase her correlations with the honest parties, except by the unavoidable attack

Definition (Quantum non-malleability (qNM))

A scheme $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *is non-malleable, if for all states* ρ_{ABR} *and all attacks* $\Lambda_{CB \to C\tilde{B}}$,

$$I(AR : \tilde{B})_\sigma \leq I(AR : B)_\rho + h(p_=(\Lambda, \rho)),$$

with $\sigma_{A\tilde{B}R} = \tilde{\Lambda}_{AB \to A\tilde{B}}(\rho_{ABR})$.

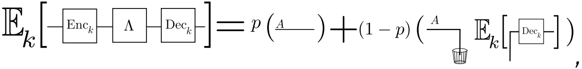


$$p_=(\Lambda, \rho) = F(\mathrm{tr}_{\tilde{B}} \Lambda_{CB \to C\tilde{B}}(|\phi^+\rangle\langle\phi^+|_{CC'} \otimes \rho_B), |\phi^+\rangle\langle\phi^+|_{CC'})^2$$

Comparison to previous definition

Definition (ABW-NM, Ambainis, Bouda, Winter '09)

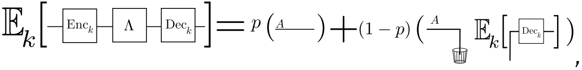
Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *be a quantum encryption scheme.* Π *is ABW-NM if*



for some probability p.

Definition (ABW-NM, Ambainis, Bouda, Winter '09)

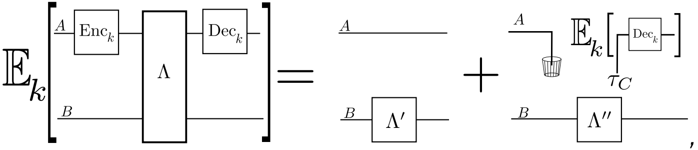
Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *be a quantum encryption scheme.* Π *is ABW-NM if*



for some probability p.

Theorem (Alagic, CM)

Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *be a quantum encryption scheme.* Π *is qNM if and only if*

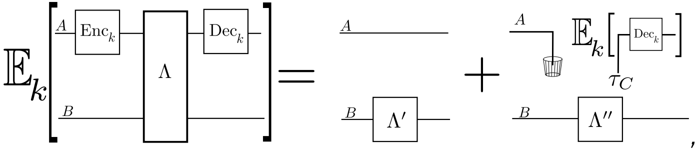


where Λ' *and* Λ'' *are explicitly given in terms of* Λ.

Comparison to previous definition (ctd.)

Theorem (Alagic, CM)

Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *be a quantum encryption scheme.* Π *is qNM if and only if*

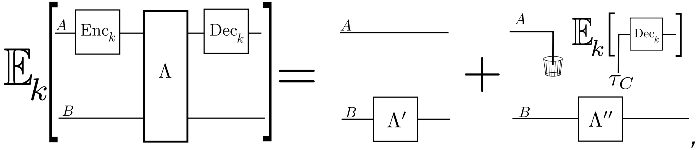


where Λ' *and* Λ'' *are explicitly given in terms of* Λ*.*

Comparison to previous definition (ctd.)

Theorem (Alagic, CM)

Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ be a quantum encryption scheme. Π is qNM if and only if



where Λ' and Λ'' are explicitly given in terms of Λ.

$$\Lambda'_{B\to\tilde{B}} = \langle\phi+|_{CC'}\,\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes(\cdot)_B)\,\left|\phi^+\right\rangle_{CC'}$$

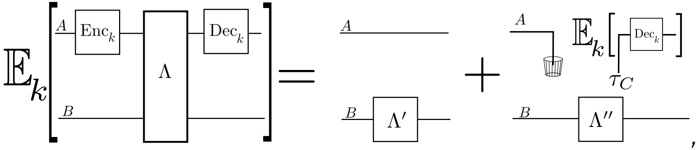
$$\Lambda''_{B\to\tilde{B}} = \mathrm{tr}_C\Lambda(\tau_C\otimes(\cdot)_B) - \Lambda'$$

$$p_=(\Lambda,\rho) = \mathrm{tr}\Lambda'(\rho_B)$$

Comparison to previous definition (ctd.)

Theorem (Alagic, CM)

Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ be a quantum encryption scheme. Π is qNM if and only if



where Λ' and Λ'' are explicitly given in terms of Λ.

$$\begin{aligned}
\Lambda'_{B\to\tilde B} &= \langle \phi+|_{CC'}\, \Lambda_{CB\to C\tilde B}(\phi^+_{CC'} \otimes (\cdot)_B)\, |\phi^+\rangle_{CC'} \\
\Lambda''_{B\to\tilde B} &= \mathrm{tr}_C \Lambda(\tau_C \otimes (\cdot)_B) - \Lambda' \\
p_=(\Lambda,\rho) &= \mathrm{tr}\Lambda'(\rho_B)
\end{aligned}$$

$\Rightarrow$ Ciphertext non-malleability!

Improvements

The new definition

... allows adversaries with side information

... prevents plaintext injection attack

... provides *ciphertext* non-malleability

while ABW-NM does not.

More Properties

$$\begin{aligned}\Lambda'_{B\to\tilde{B}} =& \langle\phi+|_{CC'}\,\Lambda_{CB\to C\tilde{B}}(\phi^+_{CC'}\otimes(\cdot)_B)\left|\phi^+\right\rangle_{CC'}\\ \Lambda''_{B\to\tilde{B}} =& \mathrm{tr}_C\Lambda(\tau_C\otimes(\cdot)_B)-\Lambda'\end{aligned}$$

More Properties

$$\Lambda'_{B\to\tilde{B}} = \langle \phi+|_{CC'} \Lambda_{CB\to C\tilde{B}}(\phi^{+}_{CC'} \otimes (\cdot)_B) \left|\phi^{+}\right\rangle_{CC'}$$
$$\Lambda''_{B\to\tilde{B}} = \mathrm{tr}_C \Lambda(\tau_C \otimes (\cdot)_B) - \Lambda'$$

- Unitary encryption maps:
  qNM$\Leftrightarrow$ $\{\mathrm{Enc}_k\}_k$ is *unitary 2-design*($\Leftrightarrow$ ABW-NM, Ambainis et al.)

More Properties

$$\begin{aligned}\Lambda'_{B\to\tilde{B}} =& \langle\phi+|_{CC'}\,\Lambda_{CB\to C\tilde{B}}(\phi^{+}_{CC'}\otimes(\cdot)_B)\left|\phi^{+}\right\rangle_{CC'}\\ \Lambda''_{B\to\tilde{B}} =& \mathrm{tr}_C\Lambda(\tau_C\otimes(\cdot)_B)-\Lambda'\end{aligned}$$

- Unitary encryption maps:
  qNM$\Leftrightarrow$ $\{\mathrm{Enc}_k\}_k$ is *unitary 2-design*($\Leftrightarrow$ ABW-NM, Ambainis et al.)
- non-unitary schemes are interesting, e.g. for authentication.

More Properties

$$\begin{aligned}\Lambda'_{B\to\tilde B} =& \langle\phi+|_{CC'}\,\Lambda_{CB\to C\tilde B}(\phi^+_{CC'}\otimes(\cdot)_B)\left|\phi^+\right\rangle_{CC'}\\ \Lambda''_{B\to\tilde B} =& \mathrm{tr}_C\Lambda(\tau_C\otimes(\cdot)_B)-\Lambda'\end{aligned}$$

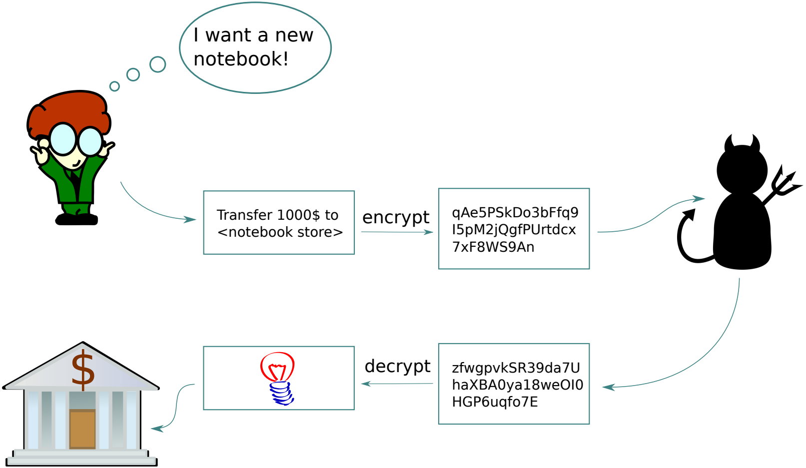
- Unitary encryption maps: qNM$\Leftrightarrow$ $\{\mathrm{Enc}_k\}_k$ is *unitary 2-design*($\Leftrightarrow$ ABW-NM, Ambainis et al.)
- non-unitary schemes are interesting, e.g. for authentication.
- qNM serves as primitive for quantum authentication schemes $\Rightarrow$ second part of the talk

Summary non-malleability

	ABW-NM	qNM
assumes secrecy	✓	✗
implies secrecy	✗	✓
secure against plaintext injection	✗	✓
primitive for authentication	✗	✓

Authentication

Authentication



Quantum authentication

- First studied by Barnum et al. '02

Quantum authentication

- First studied by Barnum et al. '02
- Most used definition by Dupuis, Nielsen and Salvail '10

Quantum authentication

- First studied by Barnum et al. '02
- Most used definition by Dupuis, Nielsen and Salvail '10
- New definition by Garg, Yuen and Zhandry '16:

Quantum authentication

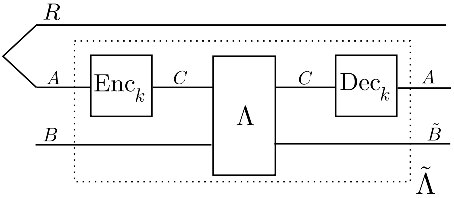
- First studied by Barnum et al. '02
- Most used definition by Dupuis, Nielsen and Salvail '10
- New definition by Garg, Yuen and Zhandry '16:

Definition (GYZ Authentication; Garg, Yuen and Zhandry)

$\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *is* ε*-GYZ-authenticating if, for any attack* $\Lambda_{CB \to CB'}$, *there exists* $\Lambda^{acc}_{B \to \tilde{B}}$ *such that for all* ρ_{AB}

$$\mathbb{E}_k \left[\left\| \Pi_{acc} \left[\mathrm{Dec}_k \circ \Lambda \circ \mathrm{Enc}_k(\rho_{AB}) \right] \Pi_{acc} - \left(\mathrm{id}_A \otimes \Lambda^{acc} \right)(\rho_{AB}) \right\|_1 \right] \leq \varepsilon$$

with $\Pi_{acc} = \mathbb{1} - \perp$.



GYZ-authentication with 2-designs

- GYZ authenticating scheme from 8-designs (GYZ '16)

GYZ-authentication with 2-designs

- GYZ authenticating scheme from 8-designs (GYZ '16)
- Using representation-theoretic analysis:

Theorem (Alagic, CM)

Adding a constant tag to a quantum message and applying a random element from a 2-design provides GYZ authentication.

GYZ-authentication with 2-designs

- GYZ authenticating scheme from 8-designs (GYZ '16)
- Using representation-theoretic analysis:

Theorem (Alagic, CM)

Adding a constant tag to a quantum message and applying a random element from a 2-design provides GYZ authentication.

- Independently proven by Portmann '16

GYZ-authentication with 2-designs

- GYZ authenticating scheme from 8-designs (GYZ '16)
- Using representation-theoretic analysis:

Theorem (Alagic, CM)

Adding a constant tag to a quantum message and applying a random element from a 2-design provides GYZ authentication.

- Independently proven by Portmann '16
- advantages: shorter keys, nice constructions (Clifford group)

Proof sketch

want to ”decouple the adversary”

Proof sketch

want to "decouple the adversary"

consider pure states and attack isometries (Stinespring)

Proof sketch

want to "decouple the adversary"

consider pure states and attack isometries (Stinespring)

Simulator for an attack isometry $V_{CB\to C\tilde{B}}$:

$$\Gamma^V_{B\to\tilde{B}} = \mathrm{tr}_C V_{CB\to C\tilde{B}}$$

Proof sketch

want to "decouple the adversary"

consider pure states and attack isometries (Stinespring)

Simulator for an attack isometry $V_{CB\to C\tilde{B}}$:

$$\Gamma^{V}_{B\to\tilde{B}} = \mathrm{tr}_C V_{CB\to C\tilde{B}}$$

same simulator as used by GYZ, introduced by Broadbent and Wainewright '16

Proof sketch

want to "decouple the adversary"

consider pure states and attack isometries (Stinespring)

Simulator for an attack isometry $V_{CB\to C\tilde{B}}$:

$$\Gamma^V_{B\to\tilde{B}} = \mathrm{tr}_C V_{CB\to C\tilde{B}}$$

same simulator as used by GYZ, introduced by Broadbent and Wainewright '16

want to bound

$$\mathbb{E}_k\left[\left\|\langle 0|_T\, U_k^\dagger V_{CB\to C\tilde{B}} U_k\left(|\psi\rangle_{AB}\otimes|0\rangle_T\right) - \mathbb{1}_A\otimes\Gamma^V_{B\to\tilde{B}}\,|\psi\rangle_{AB}\right\|_2^2\right]$$

Proof sketch

want to "decouple the adversary"

consider pure states and attack isometries (Stinespring)

Simulator for an attack isometry $V_{CB\to C\tilde{B}}$:

$$\Gamma^V_{B\to\tilde{B}} = \mathrm{tr}_C V_{CB\to C\tilde{B}}$$

same simulator as used by GYZ, introduced by Broadbent and Wainewright '16

want to bound

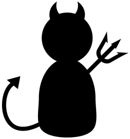
$$\mathbb{E}_k\left[\left\|\langle 0|_T\, U_k^\dagger V_{CB\to C\tilde{B}} U_k\left(|\psi\rangle_{AB}\otimes|0\rangle_T\right) - \mathbb{1}_A\otimes\Gamma^V_{B\to\tilde{B}}|\psi\rangle_{AB}\right\|_2^2\right]$$

Use "swap trick" $\mathrm{tr} A_X B_X = \mathrm{tr} S_{XX'} A_X \otimes B_{X'}$ and Schur's lemma for $U \mapsto U\otimes U$

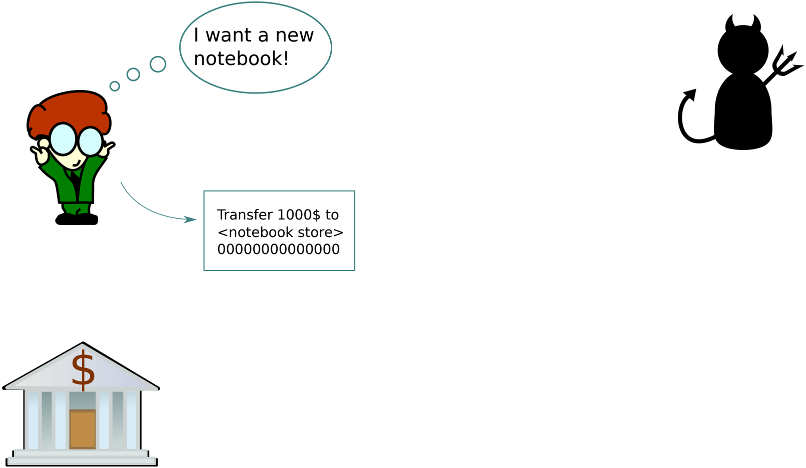
Authentication from NM: Intuition

I want a new notebook!

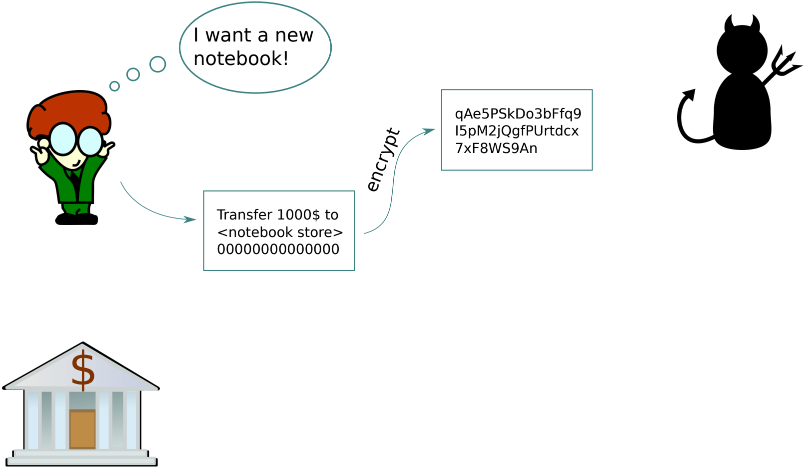
Transfer 1000$ to <notebook store>



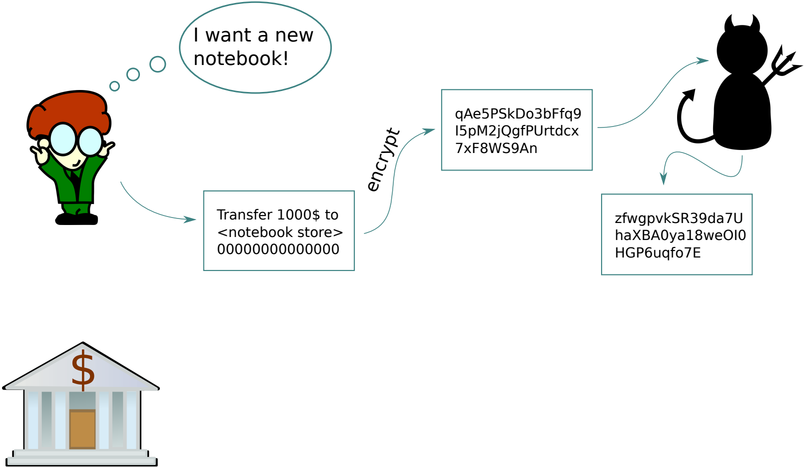
Authentication from NM: Intuition



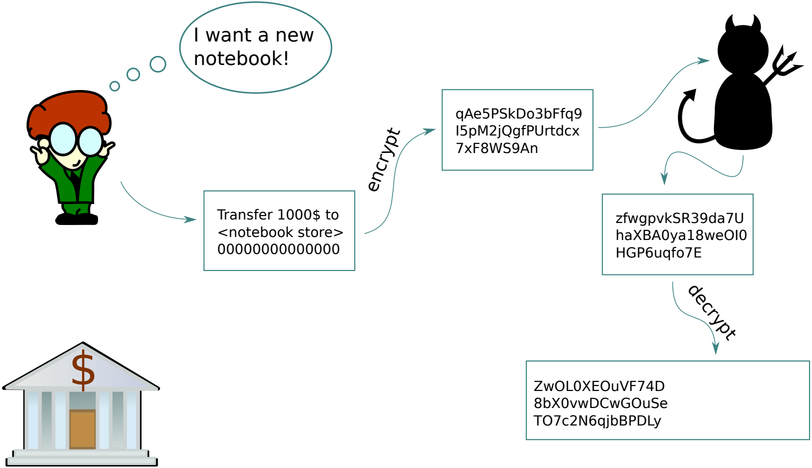
Authentication from NM: Intuition



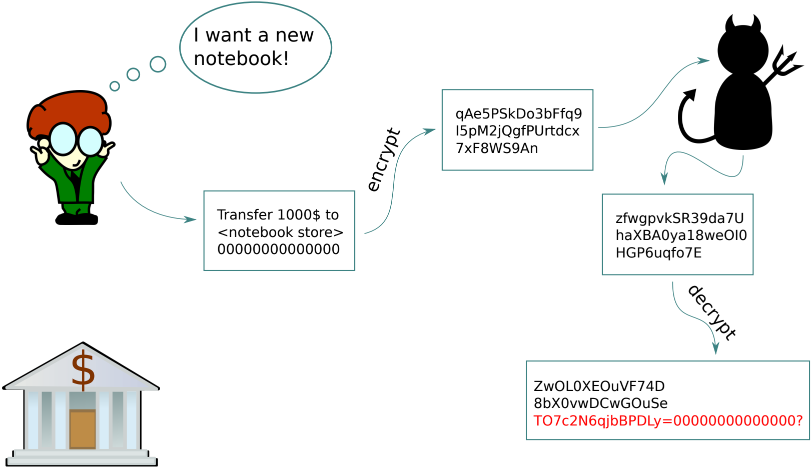
Authentication from NM: Intuition



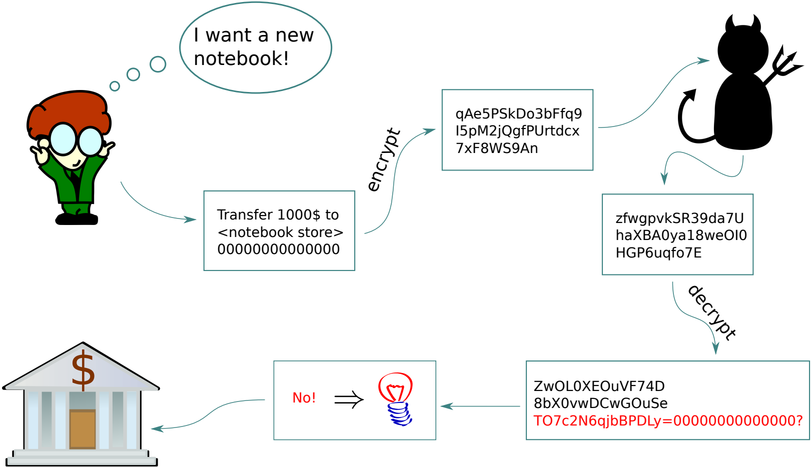
Authentication from NM: Intuition



Authentication from NM: Intuition



Authentication from NM: Intuition



Authentication from qNM

Theorem (Alagic, CM)

Adding a constant tag to a quantum message and encrypting it with an qNM scheme achieves DNS-authentication

Summary authentication

- ✓ DNS authentication from qNM schemes via tagging
- ✓ GYZ authentication from 2-designs instead of 8-designs

Teaser: Unforgeable quantum encryption

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!
- real life threat

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!
- real life threat
- model: $\mathcal{A}^{\mathrm{Enc}_k}$, adversary with oracle access to Enc_k

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!
- real life threat
- model: $\mathcal{A}^{\mathrm{Enc}_k}$, adversary with oracle access to Enc_k
- security against chosen plaintext attacks (IND-CPA) requires randomized schemes, computational assumptions.

Adversaries with oracles

- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!
- real life threat
- model: $\mathcal{A}^{\mathrm{Enc}_k}$, adversary with oracle access to Enc_k
- security against chosen plaintext attacks (IND-CPA) requires randomized schemes, computational assumptions.
- asymptotic framework: encryption and decryption poly time, secure against poly time adversaries

Adversaries with oracles

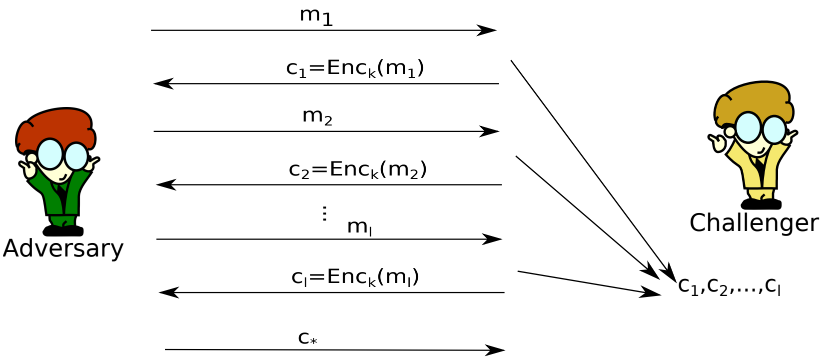
- one-time pad: $\mathrm{Enc}_k(m) = m \oplus k$, $\mathrm{Dec}_k(c) = c \oplus k$
- chosen plaintext attack (CPA): $\mathrm{Enc}_k(0^n) = k$!
- real life threat
- model: $\mathcal{A}^{\mathrm{Enc}_k}$, adversary with oracle access to Enc_k
- security against chosen plaintext attacks (IND-CPA) requires randomized schemes, computational assumptions.
- asymptotic framework: encryption and decryption poly time, secure against poly time adversaries
- quantum case: Alagic, Broadbent, Fefferman, Gagliardoni, Schaffner, St. Jules '16

CPA-ciphertext unforgeability

- Authentication against chosen plaintext attacks?

CPA-ciphertext unforgeability

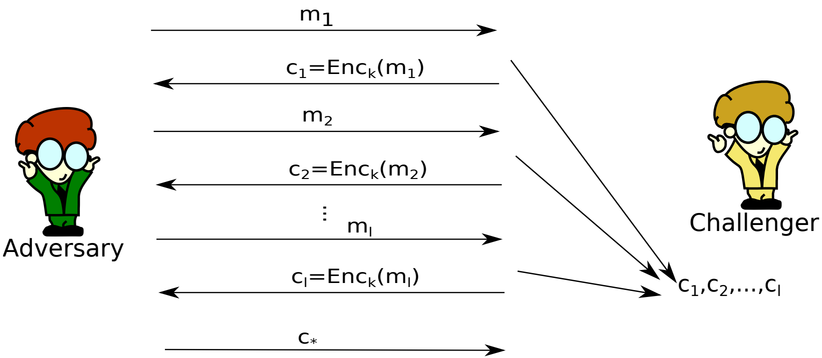
- Authentication against chosen plaintext attacks?
- Forge game:



- Adversary wins if $\mathrm{Dec}_k(c_*) \neq \perp$ and $c_* \neq c_i$ for all $i = 1, ..., l$

CPA-ciphertext unforgeability

- Authentication against chosen plaintext attacks?
- Forge game:



- Adversary wins if $\mathrm{Dec}_k(c_*) \neq \perp$ and $c_* \neq c_i$ for all $i = 1, \ldots, l$
- No-cloning problem 2.0!

Quantum plaintext unforgeability

Recall: authentication implies secrecy

Quantum plaintext unforgeability

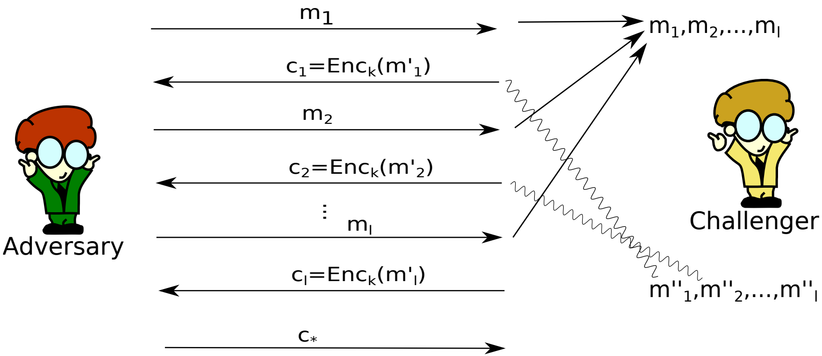
Recall: authentication implies secrecy

expect Quantum ciphertext authentication to imply IND-CPA

Quantum plaintext unforgeability

Recall: authentication implies secrecy

expect Quantum ciphertext authentication to imply IND-CPA



- Adversary wins if $m_* = \mathrm{Dec}_k(c_*) \neq \perp$ and measurement $|\phi\rangle\langle\phi|^+_{m_* m''_i}$ vs $\mathbb{1} - |\phi\rangle\langle\phi|^+_{m_* m''_i}$ yields the second outcome for all i

Disturbance?

- what if the adversary cheated by submitting c_I?

Disturbance?

- what if the adversary cheated by submitting c_I?
- Asymptotic setting, exponential message space dimension

Disturbance?

- what if the adversary cheated by submitting c_I?
- Asymptotic setting, exponential message space dimension
- Gentle measurment lemma $\Rightarrow$ negligible disturbance!

Disturbance?

- what if the adversary cheated by submitting c_l?
- Asymptotic setting, exponential message space dimension
- Gentle measurment lemma $\Rightarrow$ negligible disturbance!
- problem only arises in plaintext unforgeability scenario

What more

- Enc_k is invertible on its image with CPTP inverse Dec_k

$\Rightarrow$ $\mathrm{Enc}_k(X) = U_k(X \otimes \sigma_k)U_k^\dagger$

What more

- Enc_k is invertible on its image with CPTP inverse Dec_k

$\Rightarrow$ $\mathrm{Enc}_k(X) = U_k(X \otimes \sigma_k)U_k^\dagger$

- use to define quantum ciphertext unforgeability (QUF)

What more

- Enc_k is invertible on its image with CPTP inverse Dec_k

$\Rightarrow$ $\mathrm{Enc}_k(X) = U_k(X \otimes \sigma_k)U_k^\dagger$

- use to define quantum ciphertext unforgeability (QUF)
- works for small message sizes (no disturbance problem)
- same techniques: quantum indistinguishability under adaptive chosen ciphertext attacks, quantum authenticated encryption

Open questions

- Q quantum non-malleability with high probability?
- Q How powerful is QUF? It does not consider side information with forgery...
- Q Public key encryption? Obvious problem with digital signatures...

Open questions

- Q quantum non-malleability with high probability?
- Q How powerful is QUF? It does not consider side information with forgery...
- Q Public key encryption? Obvious problem with digital signatures...

Thanks!