Quantum non-malleability and authentication

Christian Majenz
QSoft/University of Amsterdam
Joint work with Gorjan Alagic, NIST and University of Maryland

AQIS 2017, National University of Singapore

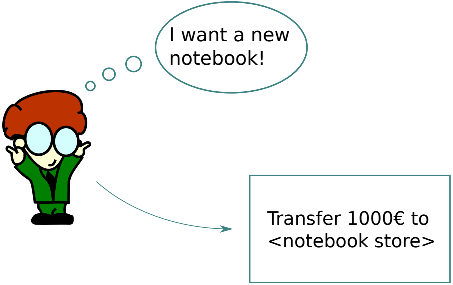
04.09.2017

Motivation: a classical story...

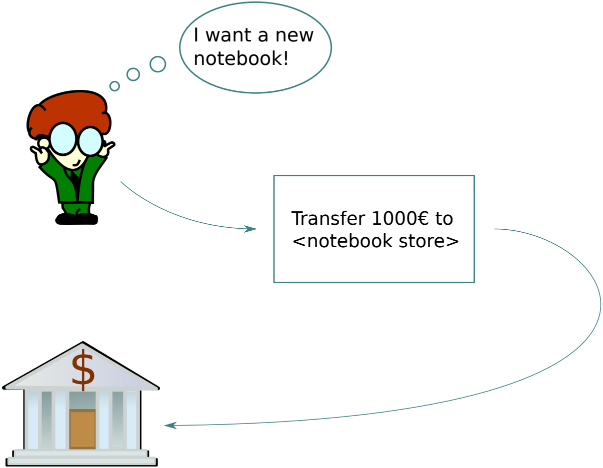
Crypto for bank transfers

Crypto for bank transfers

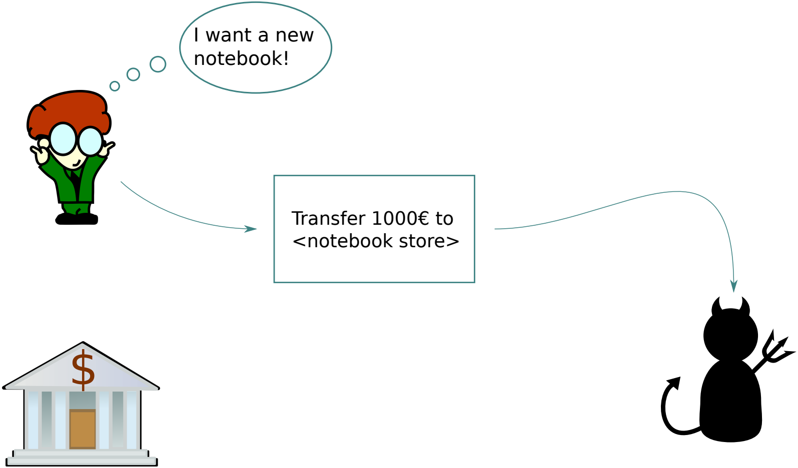
Crypto for bank transfers



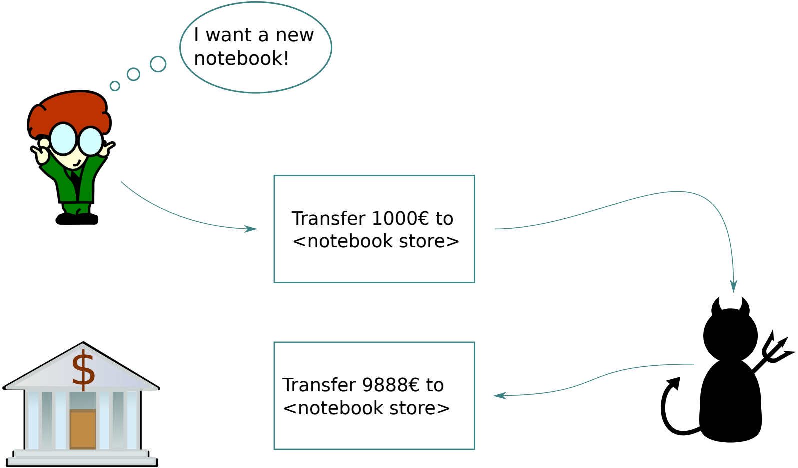
Crypto for bank transfers



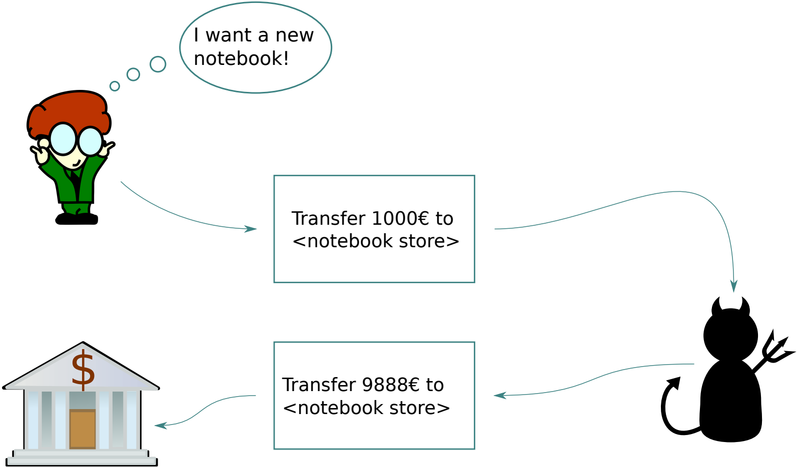
Crypto for bank transfers



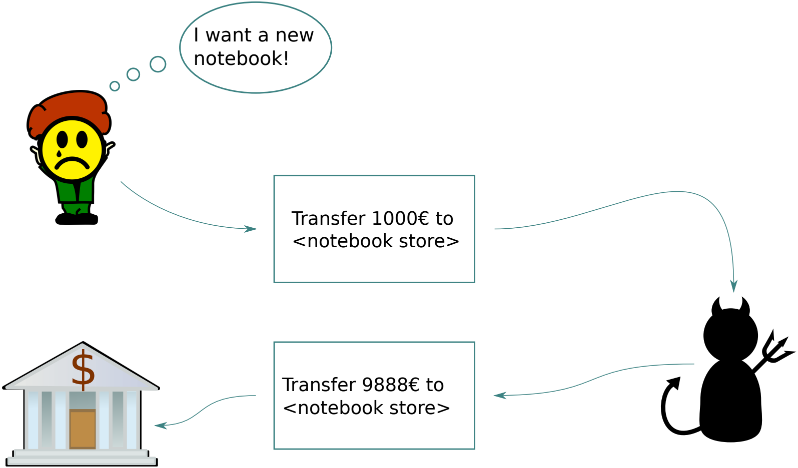
Crypto for bank transfers



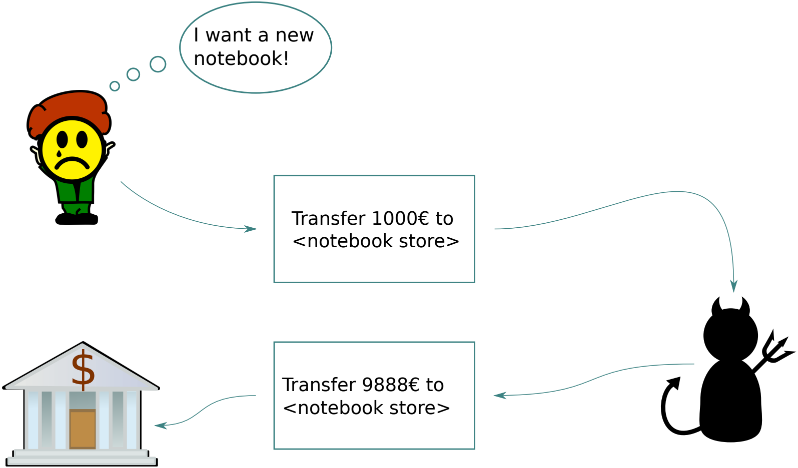
Crypto for bank transfers



Crypto for bank transfers



Crypto for bank transfers



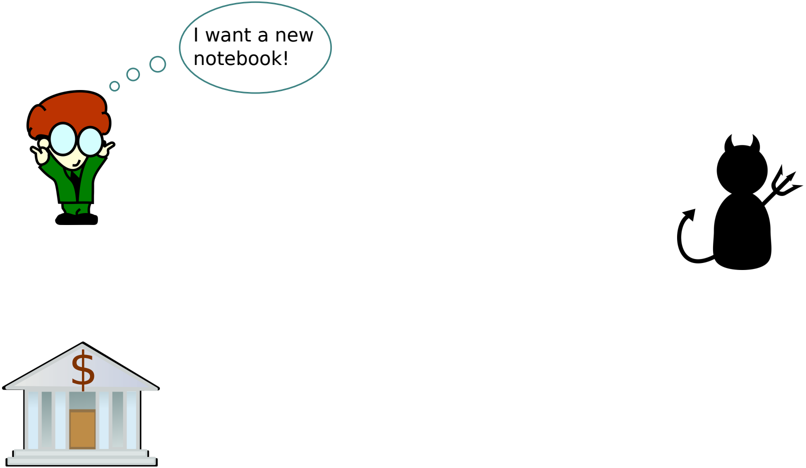
- What cryptographic security notions would fix this problem?

Non-malleability

- One solution is non-malleable encryption:

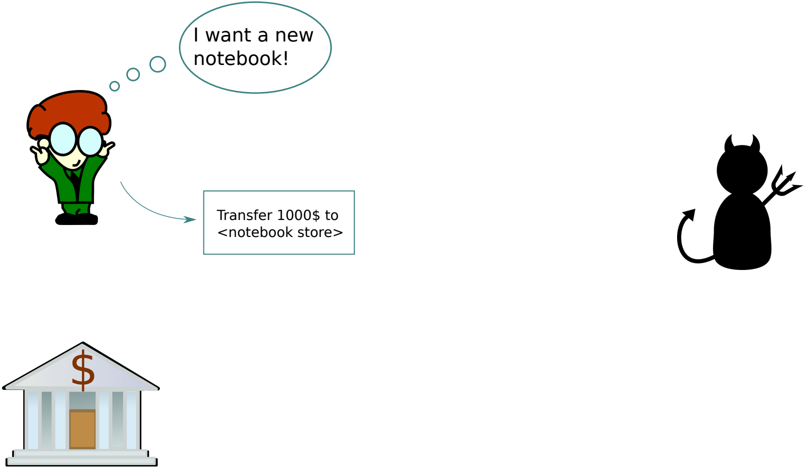
Non-malleability

- One solution is non-malleable encryption:



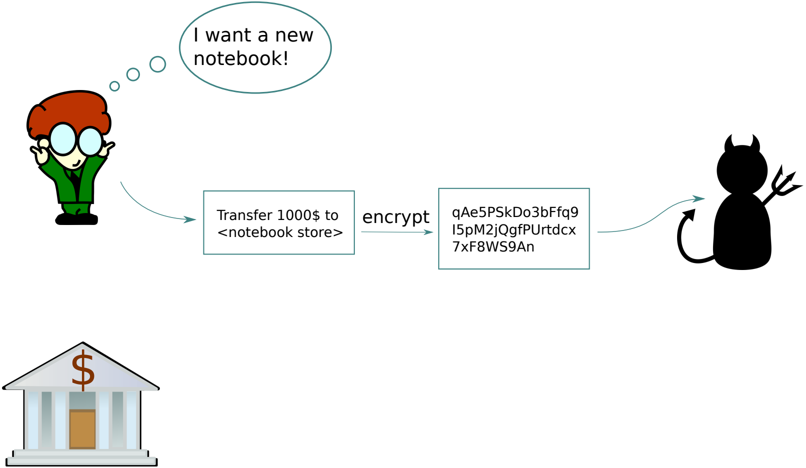
Non-malleability

- One solution is non-malleable encryption:



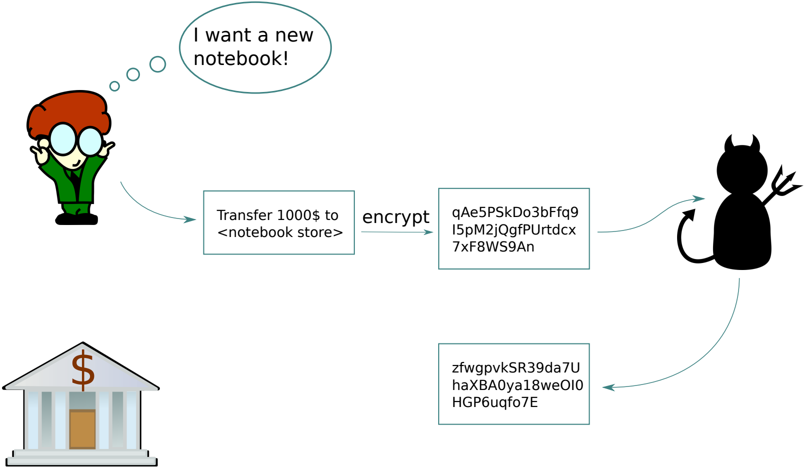
Non-malleability

- One solution is non-malleable encryption:



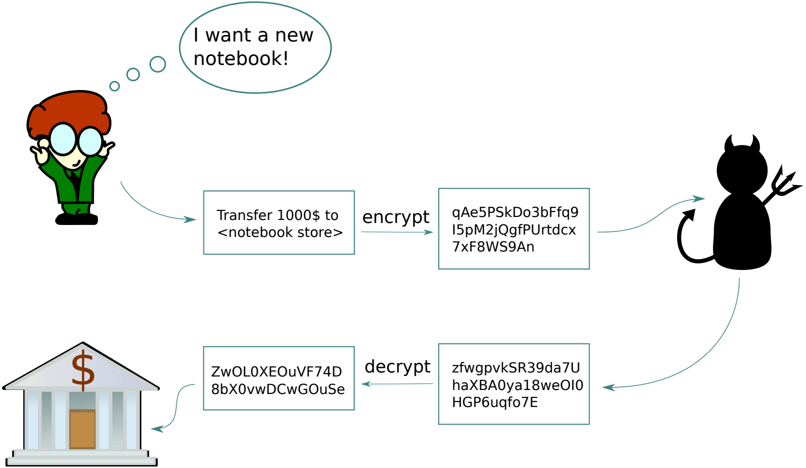
Non-malleability

- One solution is non-malleable encryption:



Non-malleability

- One solution is non-malleable encryption:



Summary of Results

New definition of information-theoretic quantum non-malleability which

Summary of Results

New definition of information-theoretic quantum non-malleability which

- fixes a vulnerability allowed by the previous definition

Summary of Results

New definition of information-theoretic quantum non-malleability which

- fixes a vulnerability allowed by the previous definition
- implies secrecy, analogously to quantum authentication

Summary of Results

New definition of information-theoretic quantum non-malleability which

- fixes a vulnerability allowed by the previous definition
- implies secrecy, analogously to quantum authentication
- serves as a primitive for building quantum authentication

Summary of Results

New definition of information-theoretic quantum non-malleability which

- fixes a vulnerability allowed by the previous definition
- implies secrecy, analogously to quantum authentication
- serves as a primitive for building quantum authentication
- has both a simulation-based and an entropic characterization

Summary of Results

New definition of information-theoretic quantum non-malleability which

- fixes a vulnerability allowed by the previous definition
- implies secrecy, analogously to quantum authentication
- serves as a primitive for building quantum authentication
- has both a simulation-based and an entropic characterization

♠ Additional result: The new definition of quantum authentication with key recycling by Garg, Yuen, Zhandry, '16, can be fulfilled using unitary 2-designs.

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)

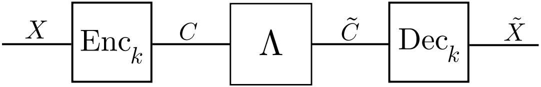
An encryption scheme is non-malleable if for any relation R on plaintexts, getting an encryption of x does not help with producing an encryption of $x' \neq x$ such that $R(x, x')$.

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

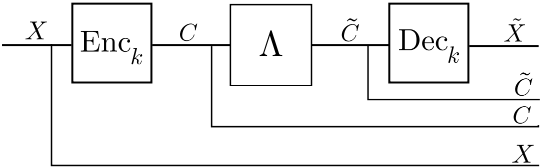
- Information theoretic definition using entropy:
  (X, C), $(\tilde{X}, \tilde{C})$ two plaintext ciphertext pairs, $C \neq \tilde{C}$

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

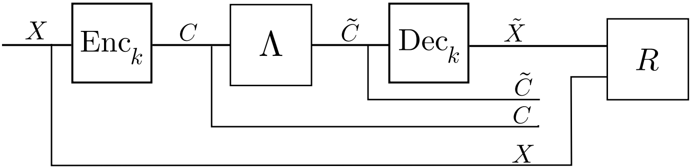
- Classical NM:



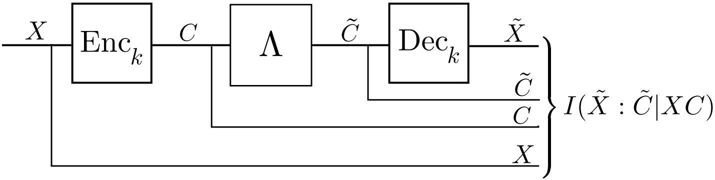
- Classical NM:



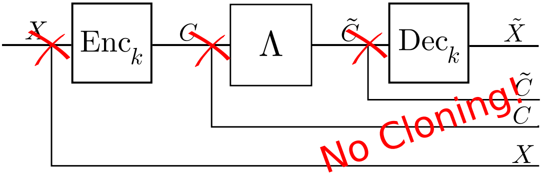
- Classical NM:



- Classical NM:



- Quantum NM:



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 $(\mathrm{Dec}_k)_{C\to\bar{A}}$
- $\mathcal{H}_{\bar{A}} = \mathcal{H}_A \oplus \mathbb{C}\left|\perp\right\rangle$

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 $(\mathrm{Dec}_k)_{C\to\bar{A}}$
- $\mathcal{H}_{\bar{A}} = \mathcal{H}_A \oplus \mathbb{C}\,|\bot\rangle$
- correctness: $\mathrm{Dec}_k \circ \mathrm{Enc}_k = \mathrm{id}_A$

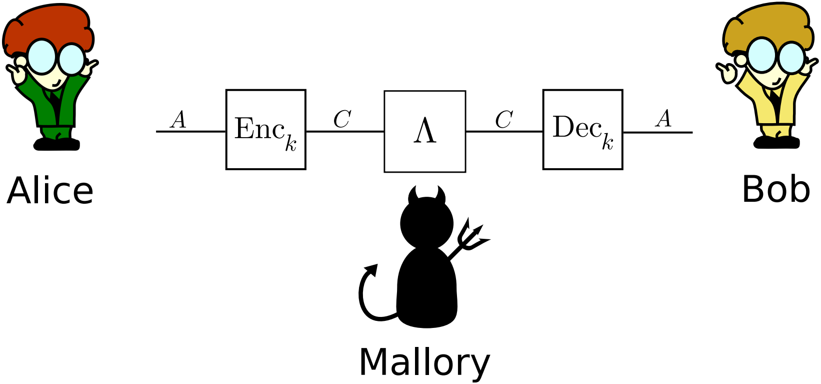
Quantum symmetric key encryption

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

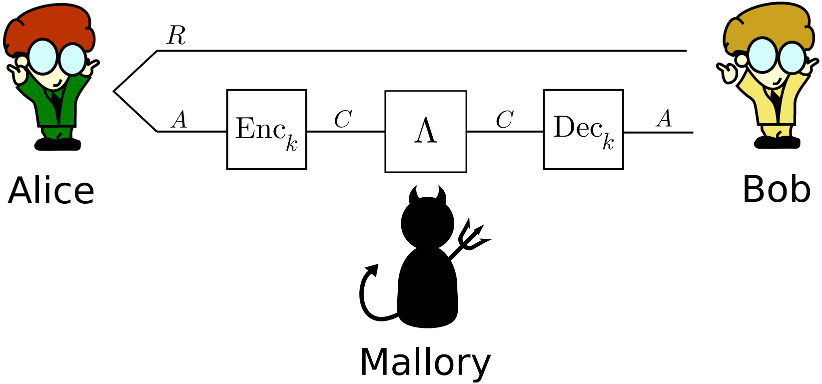
Setup for q-non-malleability

- Recall: classical non-malleability setup



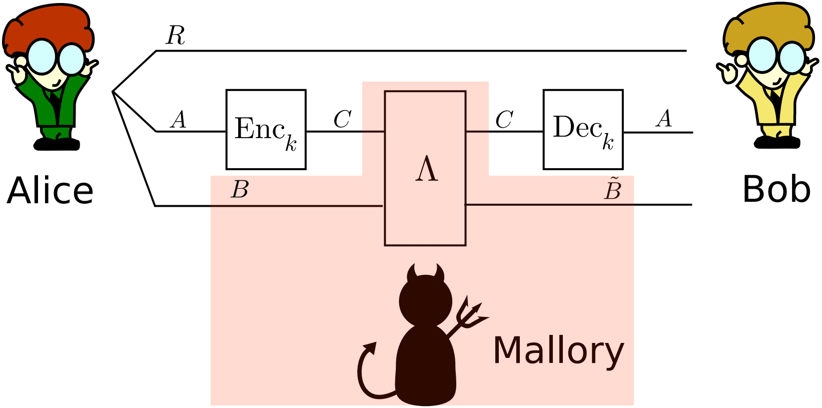
Setup for q-non-malleability

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



Setup for q-non-malleability

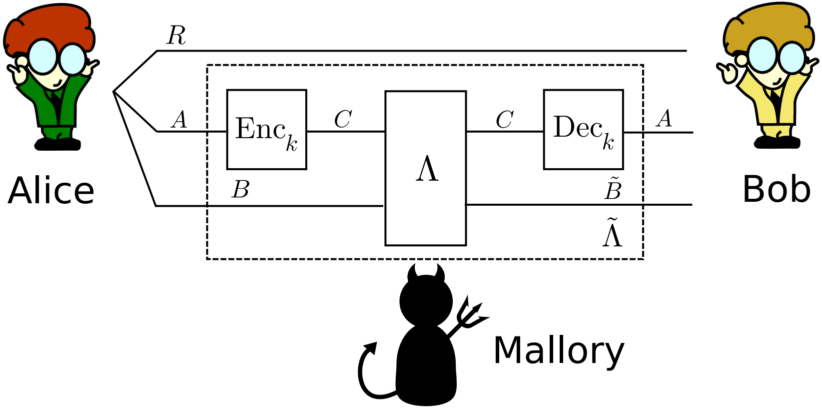
- Recall: classical non-malleability setup
- add reference system
- allow side info for adversary



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

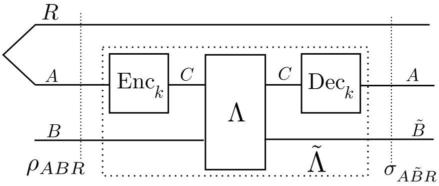
- idea: define NM such that Mallory cannot increase her correlations with the honest parties, except by the unavoidable attack

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

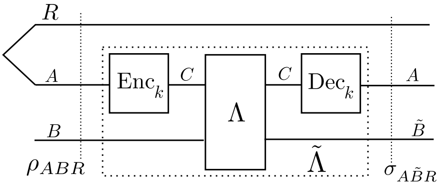
- idea: define NM such that Mallory cannot increase her correlations with the honest parties, except by the unavoidable attack

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* $\Lambda_{CB\to C\tilde{B}}$*,*

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

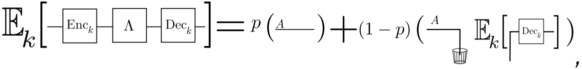
with $\sigma_{A\tilde{B}R} = \tilde{\Lambda}_{AB\to A\tilde{B}}(\rho_{ABR})$*.*



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

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*

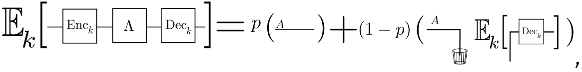


for some probability p.

Comparison to previous definition

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

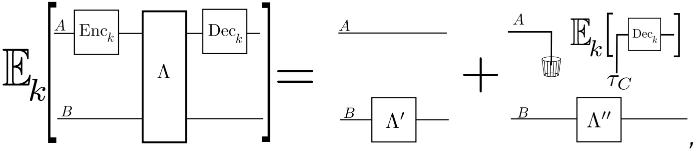
Let $\Pi = (\mathrm{Enc}_k, \mathrm{Dec}_k)$ *be a quantum encryption scheme.* Π *is ABW-NM if*



for some probability p.

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.

Improvements

The new definition

... allows adversaries with side information

... prevents plaintext injection attack

... provides *ciphertext* non-malleability

while ABW-NM does not.

More Properties

- Unitary encryption maps:
  qNM$\Leftrightarrow \{\mathrm{Enc}_k\}_k$ is *unitary 2-design*

More Properties

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

More Properties

! 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

! 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 $\Rightarrow$ information theoretic IND

More Properties

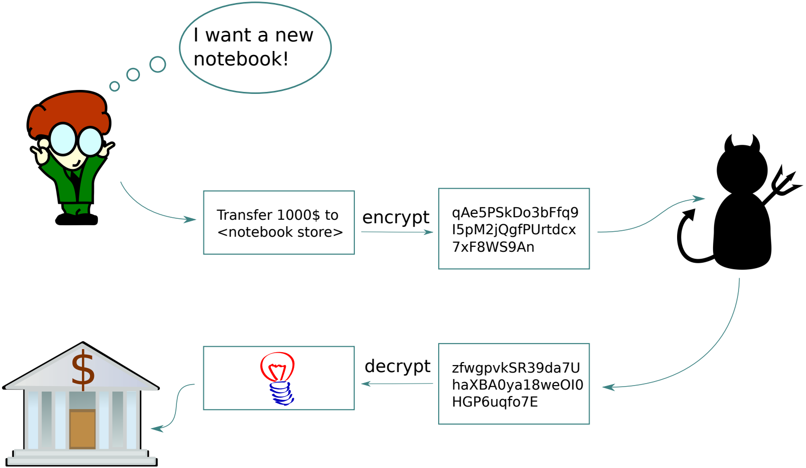
- ! Unitary encryption maps:
  qNM$\Leftrightarrow$ $\{\mathrm{Enc}_k\}_k$ is *unitary 2-design*($\Leftrightarrow$ ABW-NM, Ambainis et al.)
- non-unitary schemes are interesting, e.g. for authentication.
- ! qNM $\Rightarrow$ information theoretic IND
- qNM serves as primitive for quantum authentication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

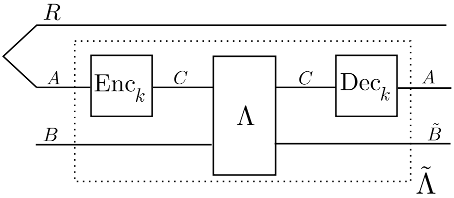
- First studied by Barnum et al. '02
- Most used definition by Dupuis, Nielsen and Salvail '10
- New definition by Garg, Yuen and Zhandry '16:

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

consider pure states and attack isometries (Stinespring)

Proof sketch

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

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

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

$$\mathbb{E}_k\left[\left\|\langle 0|_T\, U_k^\dagger V U_k \left(|\psi\rangle_{AB}\otimes|0\rangle_T\right) - \Gamma^V\,|\psi\rangle_{AB}\right\|_2^2\right]$$

Proof sketch

consider pure states and attack isometries (Stinespring)

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

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

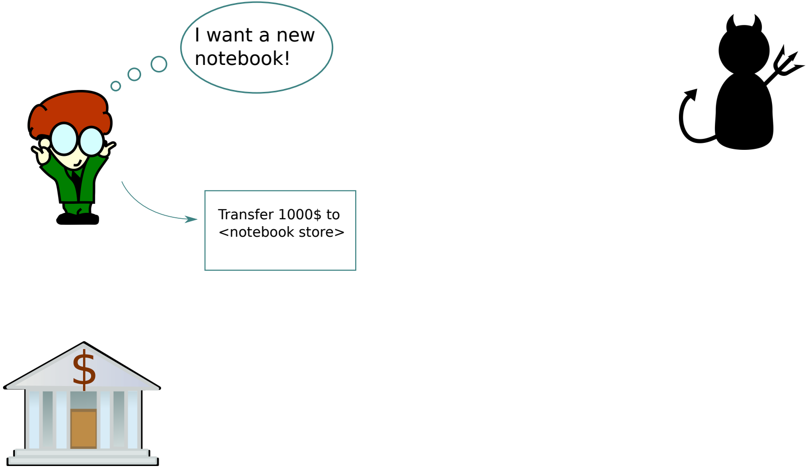
same simulator as used by GYZ, introduced by Broadbent and Wainewright '16

want to bound

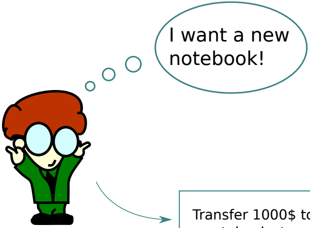
$$\mathbb{E}_k\left[\left\|\langle 0|_T\, U_k^\dagger V U_k\left(|\psi\rangle_{AB}\otimes|0\rangle_T\right) - \Gamma^V|\psi\rangle_{AB}\right\|_2^2\right]$$

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

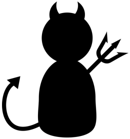
Authentication from NM: Intuition



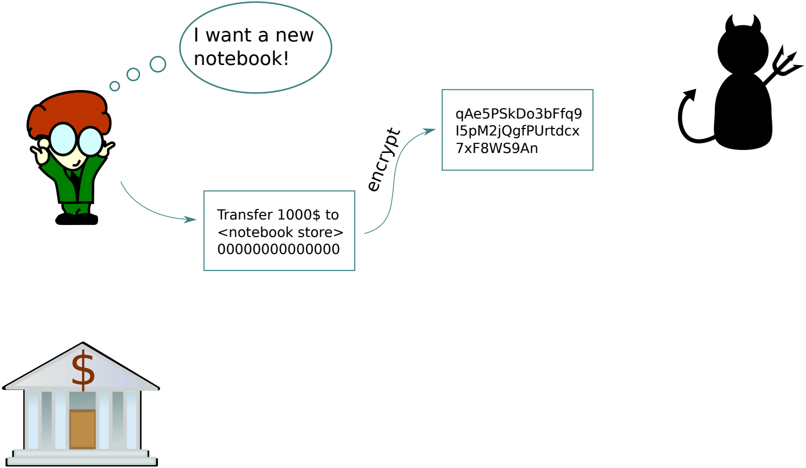
Authentication from NM: Intuition



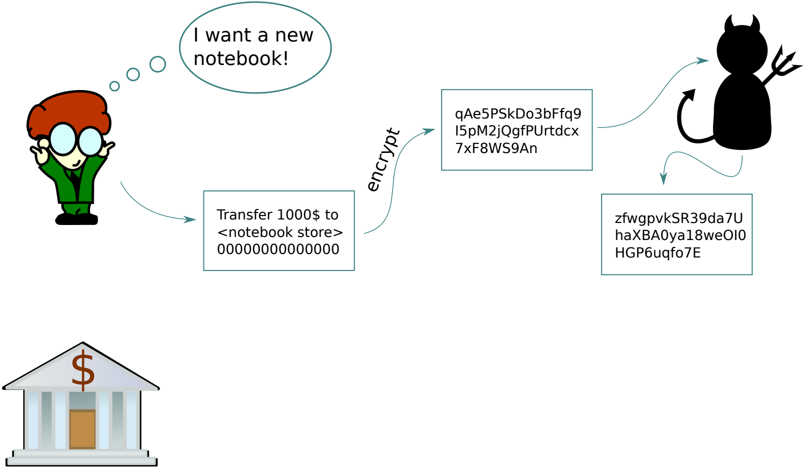
Transfer 1000$ to
<notebook store>
00000000000000



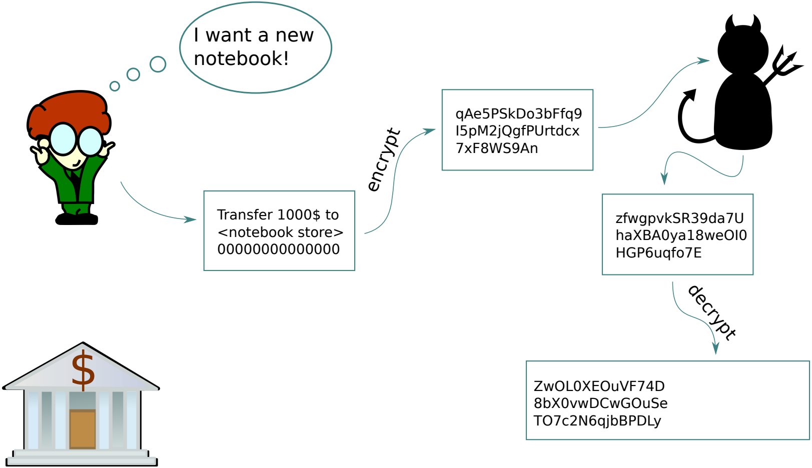
Authentication from NM: Intuition



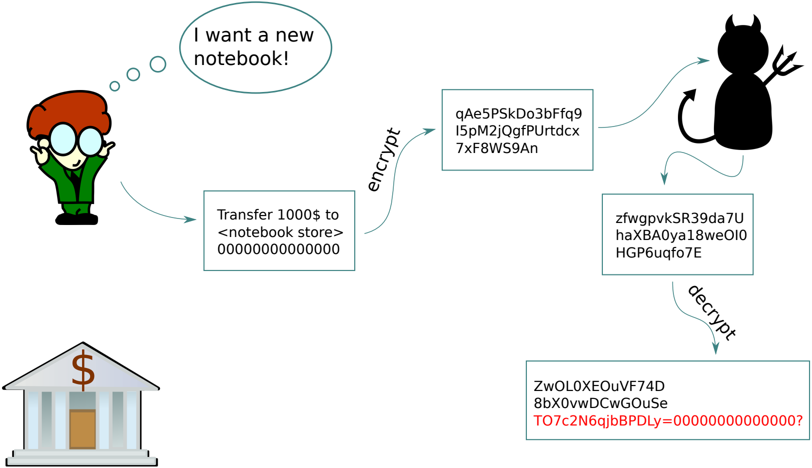
Authentication from NM: Intuition



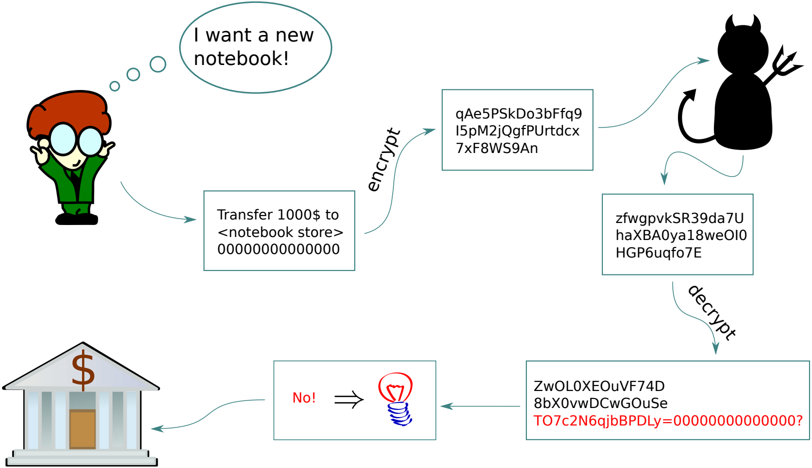
Authentication from NM: Intuition



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

Open questions

Computational security?

Current work with Christian Majenz and Tommaso Gagliardoni

Can we improve the Λ-dependence of NM?

NM with high probability?