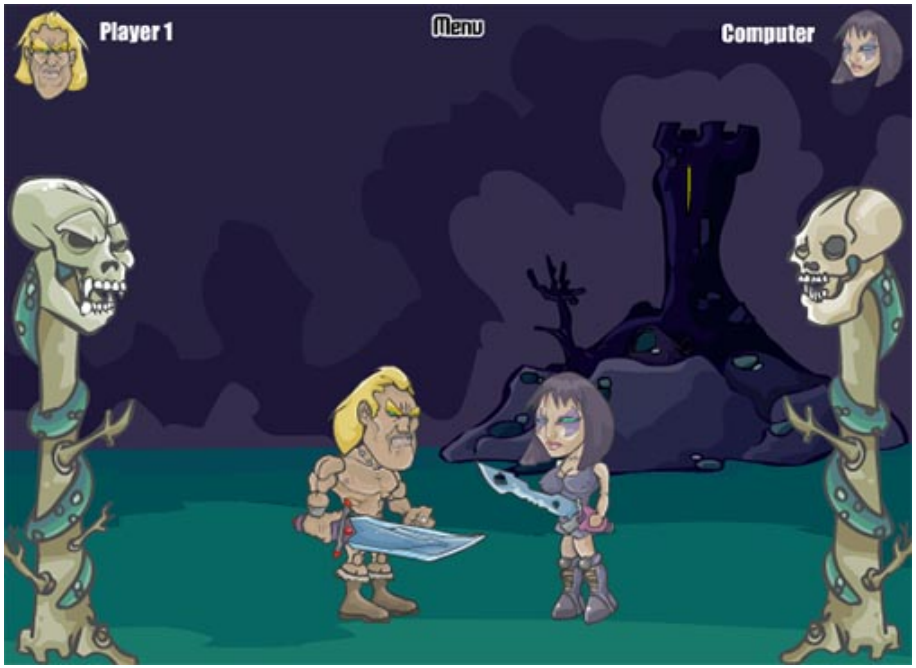
An epistemic measurement system for quantum security

Mehrnoosh Sadrzadeh
joint work with Elham Kashefi

School of Electronics and Computer Science, University of Southampton

Computing Laboratory, University of Oxford

Reasoning about quantum security protocols



Matrix vs Logic

Logic: `proving properties and discovering attacks`

A logical view:

security protocol `is`

a sequence of actions,

`after which a certain` knowledge property holds.

After A sends a **secure** message m to B, they share a secret.

sharing `data`

$$\begin{cases} A \text{ knows } m \\ B \text{ knows } m \\ A \text{ knows that } B \text{ knows } m \\ B \text{ knows that } A \text{ knows } m \\ \vdots \\ \text{It is common knowledge between } A, B \text{ that } m \end{cases}$$

secrecy `of data`

$\forall C \neq A, B$ C does not know that m

secrecy `of sharing data`

$\forall C \neq A, B$ C does not know it is CK between A, B that m

A logic to reason about these properties

after a sequence of actions, some agents know some data.

$$[\pi]\Box_A\, m$$

A logic to reason about these properties

after a sequence of `actions`, some agents know some `data`.

$$[\pi]\Box_A\, m$$

dynamics and epistemics

$[-]$ $\Box_A$

`action` and `data`

π m

After A sends a **secure** message m to B, they share a secret.

sharing `data`

$$\begin{cases} [!m]\Box_A\, m \\ [!m]\Box_B\, m \\ [!m]\Box_A\Box_B\, m \\ [!m]\Box_B\Box_A\, m \\ \vdots \\ [!m]\Box^*_{A,B}\, m \end{cases}$$

secrecy `of data`

$$\forall C \neq A, B \qquad \neg[!m]\Box_C\, m$$

secrecy `of sharing data`

$$\forall C \neq A, B \qquad \neg[!m]\Box_C\Box^*_{A,B}\, m$$

How do we get a logic to reason about these properties?

Start with a logic of dynamics then enrich it with epistemics

$$(M, Q)$$

Lattice of data, Quantale of actions

$$\begin{array}{rcl} m \leq m' & , & a \leq a' \\ m \wedge m' & , & a ; a' \\ m \vee m' & , & a \vee a' \\ \top, \bot & , & \top, \bot, 1 \end{array}$$

$$m ; a, \quad [a]m$$

$[a]m$: after doing action q proposition m holds.

We add epistemics to this logic (M, Q)

$$(M, Q)$$

$$\Downarrow$$

$$(M, Q, \{f_A\}_{A \in \mathcal{A}})$$

$$f_A = (f_A^M : M \to M, f_A^Q : Q \to Q)$$

How do we interpret these?

M: data

$f_A(m)$: appearance of agent A about data m

$\Box_A(m)$: agent A believes that m holds

Q: actions

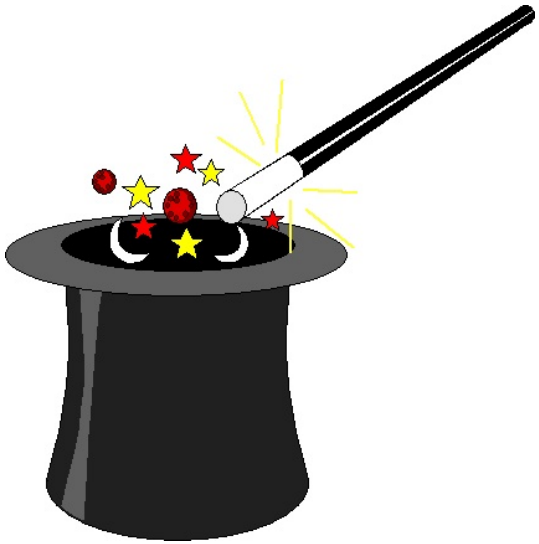
$f_A(a)$: appearance of agent A about action a

$\Box_A(a)$: agent A believes that action a has happened

$$[a]\Box_A m$$

after doing action a,
agent A believes that proposition m holds.

How does the whole thing work?



adjunction

A typical security property

$$m_0 \leq [a; a'] \Box_A m$$

A typical security reasoning

$$\begin{aligned} m_0 &\leq [a; a']\Box_A\, m \\ m_0; a; a' &\leq \Box_A\, m \end{aligned}$$

A typical security reasoning

$$\begin{aligned} m_0 &\leq [a; a']\Box_A\, m \\ m_0; a; a' &\leq \Box_A\, m \\ f_A(m_0; a; a') &\leq m \end{aligned}$$

A typical security reasoning

$$\begin{aligned} m_0 &\leq [a; a']\Box_A\, m \\ m_0; a; a' &\leq \Box_A\, m \\ f_A(m_0; a; a') &\leq m \\ f_A(m); f_A(a); f_A(a') &\leq m \end{aligned}$$

A typical security reasoning

$$\begin{aligned} m_0 &\leq [a; a']\Box_A\, m \\ m_0; a; a' &\leq \Box_A\, m \\ f_A(m_0; a; a') &\leq m \\ f_A(m); f_A(a); f_A(a') &\leq m \end{aligned}$$

Appeal to assumptions about

$$\begin{cases} \text{appearances of actions} & f_A(a), f_A(a') \\ \text{appearances of propositions} & f_A(m_0) \\ \text{concrete axioms} & \text{relating the two} \end{cases}$$

Logic:

$$(M, Q, \{f_A\}_{A\in\mathcal{A}})^{\mathcal{QM}}$$

$$M: \begin{cases} \mathcal{B} & \text{classical data} \\ \mathcal{H} & \text{quantum data} \end{cases}$$

$$Q: \begin{cases} \mathcal{Q}_c & \text{communication actions} \begin{cases} \text{classical} \\ \text{quantum} \end{cases} \\ \mathcal{H} & \text{quantum actions} \begin{cases} \text{preparation} \\ \text{projection} \\ \text{entanglement} \end{cases} \end{cases}$$

Language:

`measurement-calculus-like`

Appearances:

f_A: are set as in the classical case

$$f_A(P_1^{A,\alpha}) = P_1^{A,\alpha}, \qquad f_A(P_1^{B,\alpha}) = P_1^{B,\alpha} \vee P_1^{B,-\alpha} \vee P_1^{B,\beta} \vee \dots$$

$$f_A(N_1^{A,\alpha}) = N_1^{A,\alpha}, \qquad f_A(N_1^{B,\alpha}) = N_1^{B,\alpha} \vee N_1^{B,-\alpha} \vee N_1^{B,\beta} \vee \dots$$

$$f_A(E_{1,2}^{A,B}) = E_{1,2}^{A,B} \vee E_{1,2}^{A,C} \vee E_{1,3}^{A,B} \vee \dots$$

`owners are certain, non-owners are suspicious.`

Issue: what is the min or canonical set of appearances?

$\mathcal{QM}$ **axioms** (`so far`)

Projection

If $\Gamma(q_i); P_i^{\alpha}$ then s_i^0

Entanglement

If $\Gamma(q_i \otimes q_j; E_{i,j}^{A,B}; P_i^{A,\alpha}; P_j^{B,\alpha})$ then $s_i^0 \wedge s_j^0$

If $\Gamma(q_i \otimes q_j; E_{i,j}^{A,B}; P_i^{A,-\alpha}; P_j^{B,-\alpha})$ then $s_i^1 \wedge s_j^1$

Preparation

If $\Gamma(N_i^{A,|\alpha,0>})$ and $P_i^{B,\alpha}$ then $s_i^0 \wedge s_{i-1}^0$

If $\Gamma(N_i^{A,|-\alpha,0>})$ and $P_i^{B,-\alpha}$ then $s_i^1 \wedge s_{i-1}^1$

Ekert'91

Agents A and B share a Bell pair, they randomly choose a base and measure their qbit. Then they communicate their bases using a safe classical channel.

If the run is **successful**

$$A\text{'s base} = B\text{'s base},$$

then they share a secret.

Assume the successful run is

$$r := E^{A,B}_{1,2}; P^{A,Z}_1; P^{B,Z}_2; Z!$$

Knowledge properties for sharing

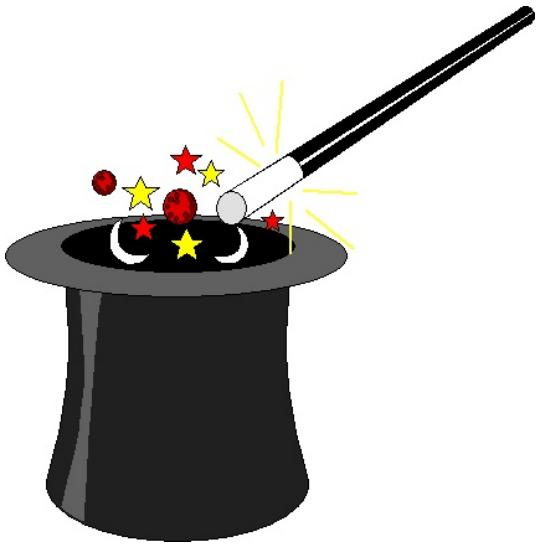
$$\begin{aligned} q_1 \otimes q_2 &\leq [r]\Box_A(s^0_1 \wedge s^0_2) \\ q_1 \otimes q_2 &\leq [r]\Box_B(s^0_1 \wedge s^0_2) \\ q_1 \otimes q_2 &\leq [r]\Box^*_{A,B}(s^0_1 \wedge s^0_2) \end{aligned}$$

Knowledge properties for secrecy

$$q_1 \otimes q_2 \leq [r]\Box_C(s^0_1 \vee s^0_2 \vee s^1_1 \vee s^1_2)$$

Consider the property

$$q_1 \otimes q_2 \leq [r]\Box_A(s_1^0 \wedge s_2^0)$$



$$q_1 \otimes q_2; f_A(E_{1,2}^{A,B}); f_A(P_1^{A,Z}); f_A(P_2^{B,Z}); f_A(Z!) \leq (s_1^0 \wedge s_2^0)$$

How do we set the Appearances?

we have

$$f_A(P_1^{A,Z}) = P_1^{A,Z}$$

we need to specify

$$f_A(Z!)$$

and

$$f_A(P_2^{B,Z})$$

and

$$f_A(E_{1,2}^{A,B})$$

The communication channel is assumed to be safe

$$f_A(Z!) = Z!$$

There are only two possible bases, so B guesses

$$f_A(P_2^{B,Z}) = P_2^{B,Z} \vee P_2^{B,-Z} \vee P_2^{B,X}; P_2^{B,-X}$$

But, does A trust the source of entanglement?

$$f_A(E_{1,2}^{A,B}) = E_{1,2}^{A,B}$$

ATTACK !

`Quantum crypto solves the problem by data screening.`

Sketch of proof

Given the safety of classical channel and trust between A and B, we substitute B's guess and have to prove

$$q_1 \otimes q_2; E^{A,B}_{1,2}; P^{A,Z}_1; P^{B,-Z}_2; Z! \;\leq\; s^0_1 \wedge s^0_2$$

$$q_1 \otimes q_2; E^{A,B}_{1,2}; P^{A,Z}_1; P^{B,Z}_2; Z! \;\leq\; s^0_1 \wedge s^0_2$$

$$q_1 \otimes q_2; E^{A,B}_{1,2}; P^{A,Z}_1; P^{B,-X}_2; Z! \;\leq\; s^0_1 \wedge s^0_2$$

$$q_1 \otimes q_2; E^{A,B}_{1,2}; P^{A,Z}_1; P^{B,X}_2; Z! \;\leq\; s^0_1 \wedge s^0_2$$

The first two follow by quantum entanglement, the second two by classical precondition.

Some questions arise

(1) How can we model data screening?

Need iteration for the rounds and probabilities.

(2) How can we prove these properties without rounds,
that is modularly?

```
some thing like a quantum digital signature;
first they trust the source using one protocol,
then they share a key using another protocol.
```

BB'84: key-dist

A picks a base X or Z and prepares a photon in $|0>$ or $|1>$ state and sends it to B over a safe quantum channel. Upon receipt, B picks a base and measures it. If the two bases are the same, they share a secret. In order to realize that, they both announce their base.

If the run is **successful**

prepared base = measured base = announced base

then they realize that they share a secret.

BB'84: key-dist

Given a successful run

$$r := N_1^{A,|Z,0>}; !q_1; P_1^{B,Z}; !Z$$

Let's consider the following sharing properties

$$q_1 \leq [r]\Box_A(s_0^0 \wedge s_1^0)$$

$$q_1 \leq [r]\Box_B(s_0^0 \wedge s_1^0)$$

s_0^0 for the classical value of the prepared data is 0.

BB'84: key-dist

For the first one we have to decide about

$$f_A(Z!) =?. \qquad f_B(Z!) =? \qquad f_B(q!) =?$$

Need:

safety of classical channel

$$f_A(Z!) = Z!. \qquad f_B(Z!) = Z!$$

safety of quantum channel

$$f_B(q!) = q!$$

BB'84: key-dist

For the second one we have to decide about

$$f_B(N_1^{A,|Z,0>}) = ?$$

Mayer's attack !

Possibilities are

$$f_B(N_1^{A,|Z,0>}) = N_1^{A,|Z,0>} \vee N_1^{A,|-Z,0>} \vee N_1^{A,|X,0>} \vee N_1^{A,|-X,0>} \vee \dots$$

Mayer's attack is solved, again, by data screening.
Can it be done modularly?

BB'84: bit-commit

Answer: A picks a base X or Z and prepares a photon in $|0>$ or $|1>$ state and sends it to B over a safe quantum channel. Upon receipt, B picks a base and measures it. A then announces her basis and the classical bit of her preparation. If these match with B's base and bit, B knows that he can trust A. That is if A had lied, B would figure it out.

BB'84: bit-commit

If A lies about **her basis** , thus the following run:

$$r := N_1^{A,|X,0>}; !q_1; P_1^{B,Z}; !_A Z; !_A 0$$

we detect it: B will figure it our since we can prove

$$\top \leq [r]\Box_B(s_0^0 \wedge s_1^1)$$

Also, if A lies about **her classical data**, thus

$$r := N_1^{A,|Z,1>}; !q_1; P_1^{B,Z}; !_A Z; !_A 0$$

we detect it: B will figure it our since we can prove

$$\top \leq [r]\Box_B(s_0^1 \wedge s_1^0)$$

But if we assume A lies about **her prepared bit**, thus

$$r := E_{1,2}^{A,B}; !q_1; P_1^{B,Z}; !_A Z; !_A 0$$

we can detect it only by `making` B `suspect it`.

Algebraic logic for verification of Q protocols

proving properties and discovering attacks

Strength

- no probabilities
- QM axioms

Weakness of our approach:

- no probabilities
- QM axioms

Related work:

- Distributed measurement calculus by DDKP

  equivalence relation on configurations leads to strong knowledge: no attacks are discovered.

  our mysterious f_A

- Gay et al and Mateus et al

  probabilities are there, but the setting is so complicated that they cannot prove any useful property.

  our simple axiomatics