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
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

\[
\begin{aligned}
A & \text{ knows } m \\
B & \text{ knows } m \\
A & \text{ knows that } B \text{ knows } m \\
B & \text{ knows that } A \text{ knows } m \\
& \vdots \\
\text{It is common knowledge between } A, B \text{ that } m
\end{aligned}
\]

secrecy of data

\[
\forall C \neq A, B \quad C \text{ does not know that } m
\]

secrecy of sharing data

\[
\forall C \neq A, B \quad C \text{ does not know it is CK between } A, B \text{ that } m
\]
A logic to reason about these properties

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

\[ [\pi] \square_A m \]
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

$$\pi \quad m$$
After $A$ sends a **secure** message $m$ to $B$, they **share** a secret.

**Sharing** data

\[
\begin{align*}
[m]_{A}^{A} m \\
[m]_{B}^{B} m \\
[m]_{A}^{A} [m]_{B}^{B} m \\
[m]_{B}^{B} [m]_{A}^{A} m \\
\vdots \\
[m]_{A,B}^{A,B} m
\end{align*}
\]

**Secrecy** of data

\[
\forall C \neq A, B \quad \neg [m]_{C} m
\]

**Secrecy** of sharing data

\[
\forall C \neq A, B \quad \neg [m]_{C}^{A,B} m
\]
How do we get a logic to reason about these properties?

Start with a logic of dynamics then enrich it with epistemics.

$\mathcal{(M, Q)}$

Lattice of data, Quantale of actions

$[a]m$ : after doing action $a$ proposition $m$ holds.
We add epistemics to this logic \((\mathcal{M}, \mathcal{Q})\) \(\uparrow\) \((\mathcal{M}, \mathcal{Q}, \{f_A\}_{A \in A})\)

\[ f_A = (f^M_A : \mathcal{M} \rightarrow \mathcal{M}, f^Q_A : \mathcal{Q} \rightarrow \mathcal{Q}) \]
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

\[ m_0 \leq [a; a'] \square_A m \]
\[ m_0; a; a' \leq \square_A m \]
A typical security reasoning

\[
m_0 \leq [a; a'] \square_A m
\]
\[
m_0; a; a' \leq \square_A m
\]
\[
f_A(m_0; a; a') \leq m
\]
A typical security reasoning

\[
\begin{align*}
    m_0 & \leq [a; a'] \Box_A m \\
    m_0; a; a' & \leq \Box_A m \\
    f_A(m_0; a; a') & \leq m \\
    f_A(m); f_A(a); f_A(a') & \leq m
\end{align*}
\]
A typical security reasoning

\[ m_0 \leq [a; a'] \Box_A m \]
\[ m_0; a; a' \leq \Box_A m \]
\[ f_A(m_0; a; a') \leq m \]
\[ f_A(m); f_A(a); f_A(a') \leq m \]

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:

\[ (M, Q, \{ f_A \}_{A \in A})_{QM} \]

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

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

measurement-calculus-like

Appearances:

\[ f_A : \text{are set as in the classical case} \]

\[ f_A(P_1^{A,\alpha}) = P_1^{A,\alpha}, \quad f_A(P_1^{B,\alpha}) = P_1^{B,\alpha} \vee P_1^{B,-\alpha} \vee P_1^{B,\beta} \vee \ldots \]

\[ f_A(N_1^{A,\alpha}) = N_1^{A,\alpha}, \quad f_A(N_1^{B,\alpha}) = N_1^{B,\alpha} \vee N_1^{B,-\alpha} \vee N_1^{B,\beta} \vee \ldots \]

\[ f_A(E_{1,2}^{A,B}) = E_{1,2}^{A,B} \vee E_{1,2}^{A,C} \vee E_{1,3}^{A,B} \vee \ldots \]

owners are certain, non-owners are suspicious.

Issue: what is the min or canonical set of appearances?
**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 $s_i^0 \land s_j^0$
If $\Gamma(q_i \otimes q_j; E_{i,j}^{A,B}; P_{i}^{A,-\alpha}; P_{j}^{B,-\alpha})$ then $s_i^1 \land s_j^1$

**Preparation**
If $\Gamma(N_i^A,|\alpha,0\rangle)$ and $P_{i}^{B,\alpha}$ then $s_i^0 \land s_{i-1}^0$
If $\Gamma(N_i^A,|\alpha,0\rangle)$ and $P_{i}^{B,-\alpha}$ then $s_i^1 \land s_{i-1}^1$
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**

\[ A’s \text{ base} = B’s \text{ base}, \]

then they **share** a **secret**.
Assume the successful run is 

\[ r := E_{1,2}^{A,B} ; P_1^{A,Z} ; P_2^{B,Z} ; Z! \]

Knowledge properties for sharing

\[ q_1 \otimes q_2 \leq [r] \Box_A (s_1^0 \land s_2^0) \]
\[ q_1 \otimes q_2 \leq [r] \Box_B (s_1^0 \land s_2^0) \]
\[ q_1 \otimes q_2 \leq [r] \Box^*_{A,B} (s_1^0 \land s_2^0) \]

Knowledge properties for secrecy

\[ q_1 \otimes q_2 \leq [r] \Box_C (s_1^0 \lor s_2^0 \lor s_1^1 \lor s_2^1) \]
Consider the property

\[ q_1 \otimes q_2 \leq [r] \square_A (s_1^0 \land s_2^0) \]

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

\[ f_A(P^{B,Z}_2) = P^{B,Z}_2 \lor P^{B,-Z}_2 \lor P^{B,X}_2 \lor P^{B,-X}_2 \]

But, does \( A \) trust the source of entanglement?

\[ f_A(E^{A,B}_{1,2}) = E^{A,B}_{1,2} \]

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

\[ q_1 \otimes q_2; E_{1,2}^{A,B}; P_1^{A,Z}; P_2^{B,-Z}; Z! \leq s_1^0 \wedge s_2^0 \]

\[ q_1 \otimes q_2; E_{1,2}^{A,B}; P_1^{A,Z}; P_2^{B,Z}; Z! \leq s_1^0 \wedge s_2^0 \]

\[ q_1 \otimes q_2; E_{1,2}^{A,B}; P_1^{A,Z}; P_2^{B,-X}; Z! \leq s_1^0 \wedge s_2^0 \]

\[ q_1 \otimes q_2; E_{1,2}^{A,B}; P_1^{A,Z}; P_2^{B,X}; Z! \leq s_1^0 \wedge s_2^0 \]

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**

\[
\text{prepared base} = \text{measured base} = \text{announced base}
\]

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

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

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

\( s_0^0 \) for the classical value of the prepared data is 0.
BB’84: key-dist

For the first one we have to decide about

\[ f_A(Z!) = ?, \quad f_B(Z!) = ?, \quad f_B(q!) = ? \]

Need:

\textit{safety of classical channel}

\[ f_A(Z!) = Z!, \quad f_B(Z!) = Z! \]

\textit{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

$$f_B(N_1^A,|Z,0>) = N_1^A,|Z,0> \lor N_1^A,|-Z,0> \lor N_1^A,|X,0> \lor N_1^A,|-X,0> \lor \ldots$$

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:

\[
\begin{align*}
\begin{array}{l}
r := N^A_1|X,0>; {q}_1; P^{B,Z}_1; !AZ; !A0 \\
\end{array}
\end{align*}
\]
we detect it: \( B \) will figure it our since we can prove

\[
\top \leq [r] □_B (s^0_0 \land s^1_1)
\]

Also, if \( A \) lies about her classical data, thus

\[
\begin{align*}
\begin{array}{l}
r := N^A_1|Z,1>; {q}_1; P^{B,Z}_1; !AZ; !A0 \\
\end{array}
\end{align*}
\]
we detect it: \( B \) will figure it our since we can prove

\[
\top \leq [r] □_B (s^1_0 \land s^0_1)
\]

But if we assume \( A \) lies about her prepared bit, thus

\[
\begin{align*}
\begin{array}{l}
r := E^{A,B}_1; {q}_1; P^{B,Z}_1; !AZ; !A0 \\
\end{array}
\end{align*}
\]
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
Our simple axiomatics

...they cannot prove any useful property.

Gay et al. and Mateus et al.

Our mysterious

edge: no attacks are discovered.

Equivalence relation on configurations leads to strong knowledge.

Distributed measurement calculus by DDKP

Related work: