量子暗号の形式的検証のための確率双模倣

久保田 貴大[*], 角谷 良彦[*],
加藤 豪[†], 河野 泰人[†], 櫻田 英樹[†]

[*]東京大学情報理工学系研究科,
[†]NTTコミュニケーション科学基礎研究所

量子暗号の形式的検証のための近似双模倣

久保田 貴大[*], 角谷 良彦[*],
加藤 豪[†], 河野 泰人[†], 櫻田 英樹[†]

[*]東京大学情報理工学系研究科,
[†]NTTコミュニケーション科学基礎研究所

背景

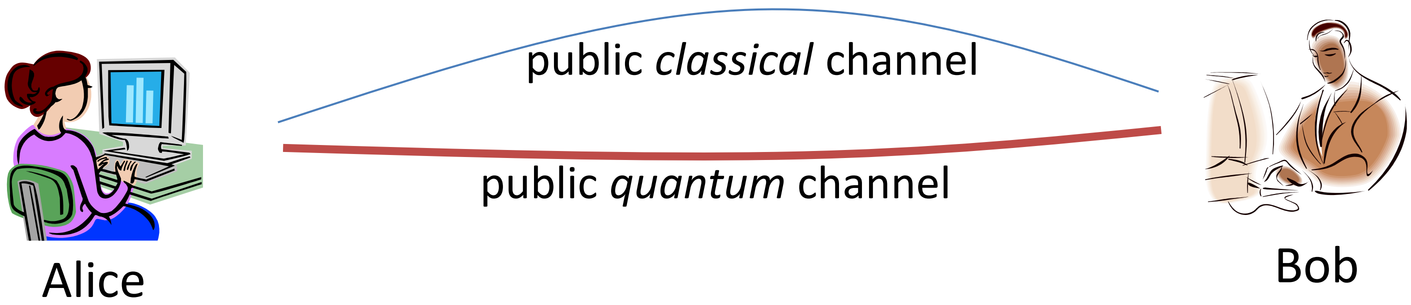
- 暗号安全性証明の検証は難しい
  - 古典暗号に対しては, 検証のための形式体系やツールが開発・適用されている
- 形式的検証は, 量子暗号に対しても有用
  - 複雑な安全性証明がある [Mayers’98]
  - 今後も, さまざまなプロトコルが提案される可能性がある

本研究の目標

- 量子プロセス計算qCCSを,
  Shor-PreskillのBB84の安全性証明に適用すること
  - プロセス計算は並行システムを記述するのに適している
    - qCCSには, プロセスの双模倣の概念がある [Feng+'11]
  - Shor-Preskillの証明は,
    最もシンプルな安全性証明のひとつ [Shor-Preskill'00]

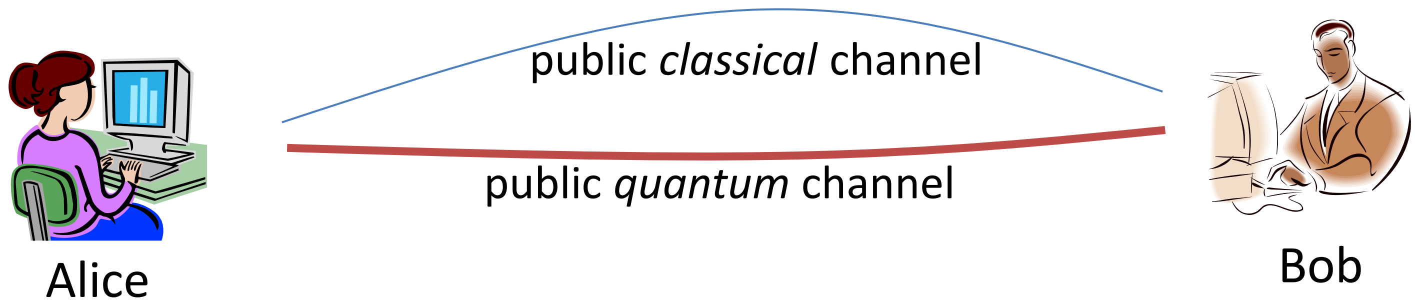
Outline of Shor-Preskill proof of BB84

BB84

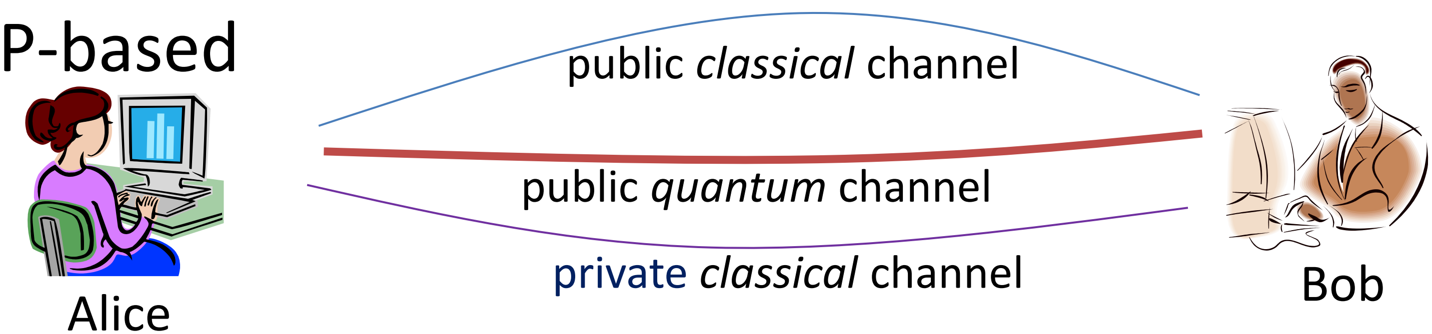


Outline of Shor-Preskill proof of BB84

BB84

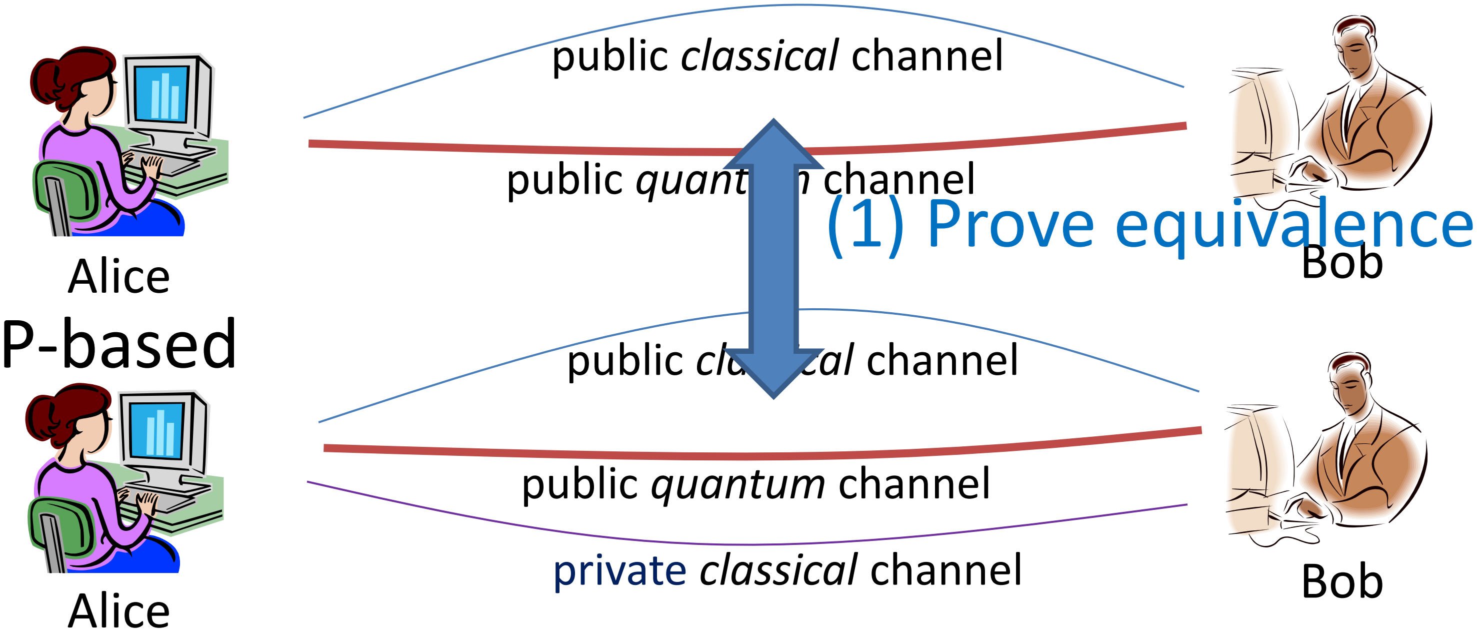


EDP-based



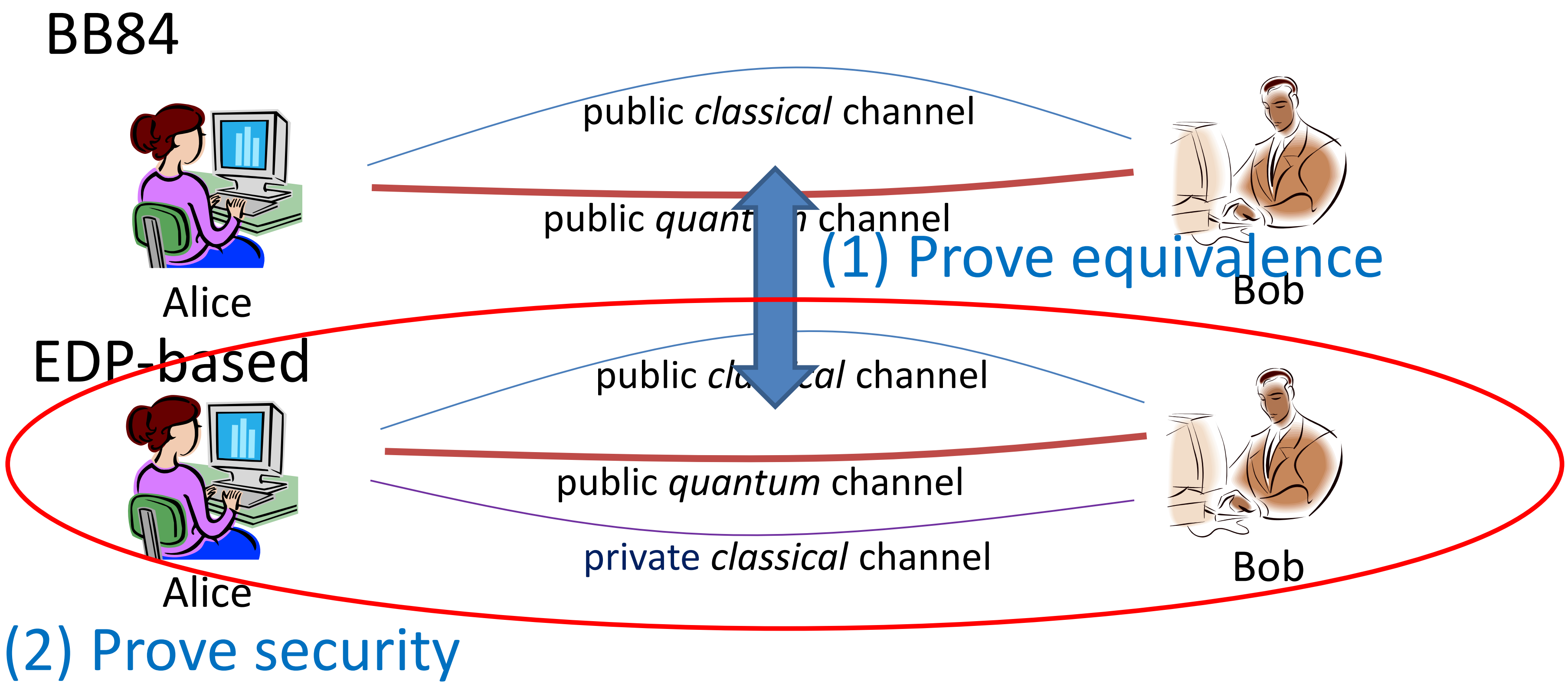
Outline of Shor-Preskill proof of BB84

BB84



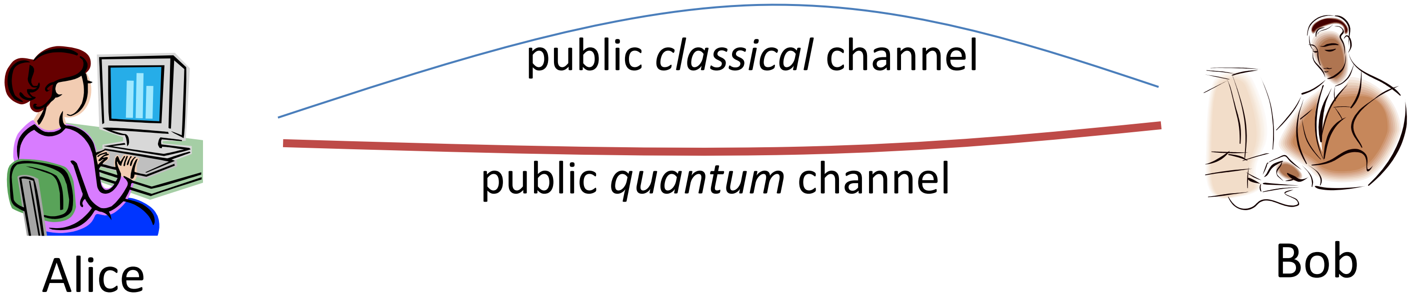
EDP-based

Outline of Shor-Preskill proof of BB84

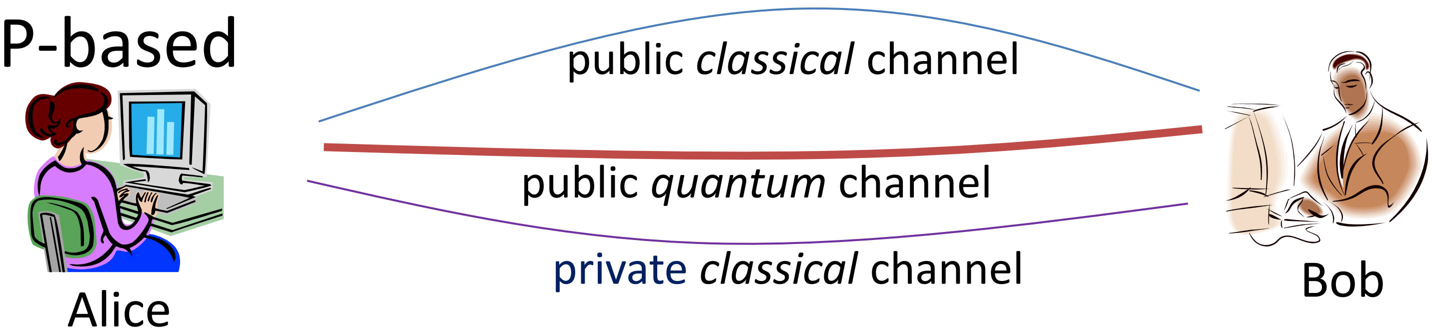


Our formal verification

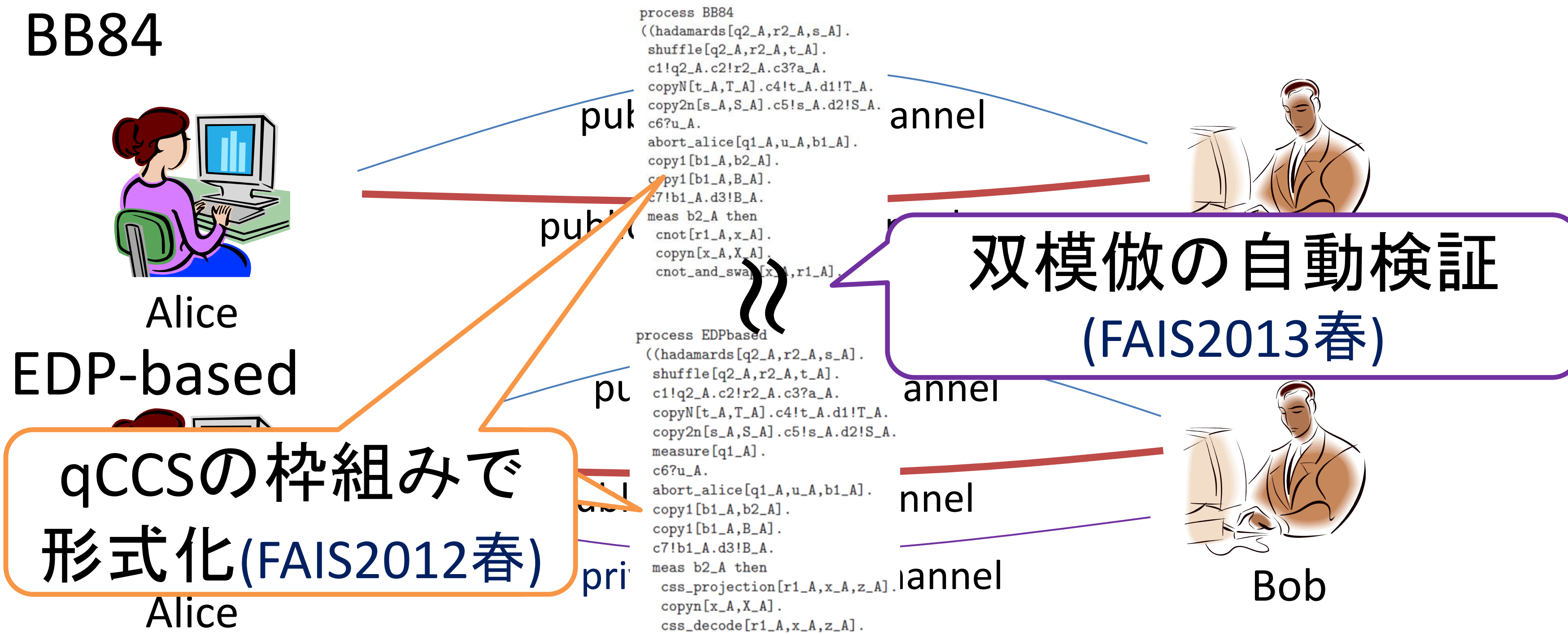
BB84



EDP-based



Our formal verification

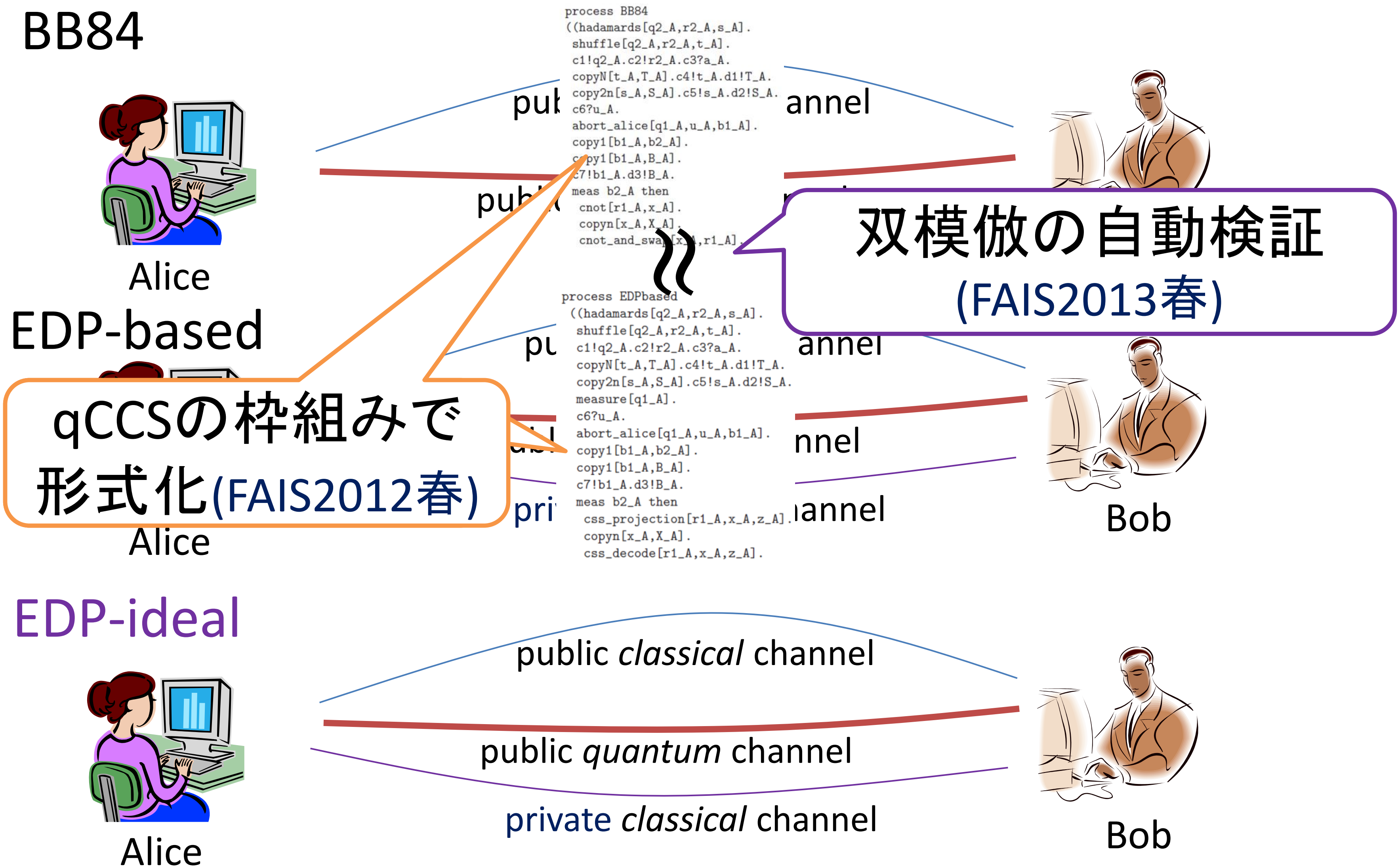



```
process BB84
((hadamards[q2_A,r2_A,s_A].
 shuffle[q2_A,r2_A,t_A].
 c1!q2_A.c2!r2_A.c3?a_A.
 copyN[t_A,T_A].c4!t_A.d1!T_A.
 copy2n[s_A,S_A].c5!s_A.d2!S_A.
 c6?u_A.
 abort_alice[q1_A,u_A,b1_A].
 copy1[b1_A,b2_A].
 copy1[b1_A,B_A].
 c7!b1_A.d3!B_A.
 meas b2_A then
  cnot[r1_A,x_A].
  copyn[x_A,X_A].
  cnot_and_swap[x_A,r1_A].
```

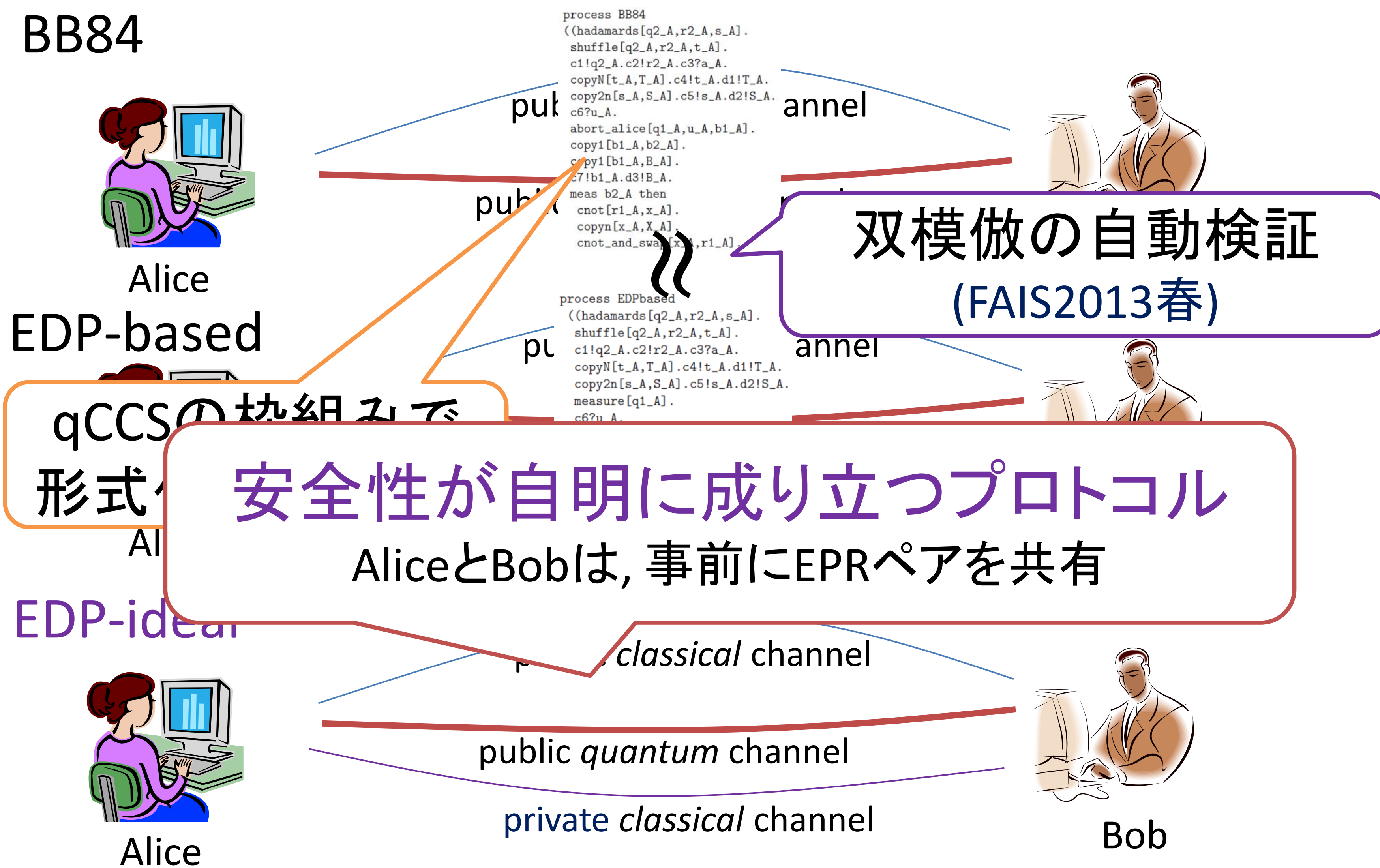
≈

```
process EDPbased
 ((hadamards[q2_A,r2_A,s_A].
  shuffle[q2_A,r2_A,t_A].
  c1!q2_A.c2!r2_A.c3?a_A.
  copyN[t_A,T_A].c4!t_A.d1!T_A.
  copy2n[s_A,S_A].c5!s_A.d2!S_A.
  measure[q1_A].
  c6?u_A.
  abort_alice[q1_A,u_A,b1_A].
  copy1[b1_A,b2_A].
  copy1[b1_A,B_A].
  c7!b1_A.d3!B_A.
  meas b2_A then
   css_projection[r1_A,x_A,z_A].
   copyn[x_A,X_A].
   css_decode[r1_A,x_A,z_A].
```

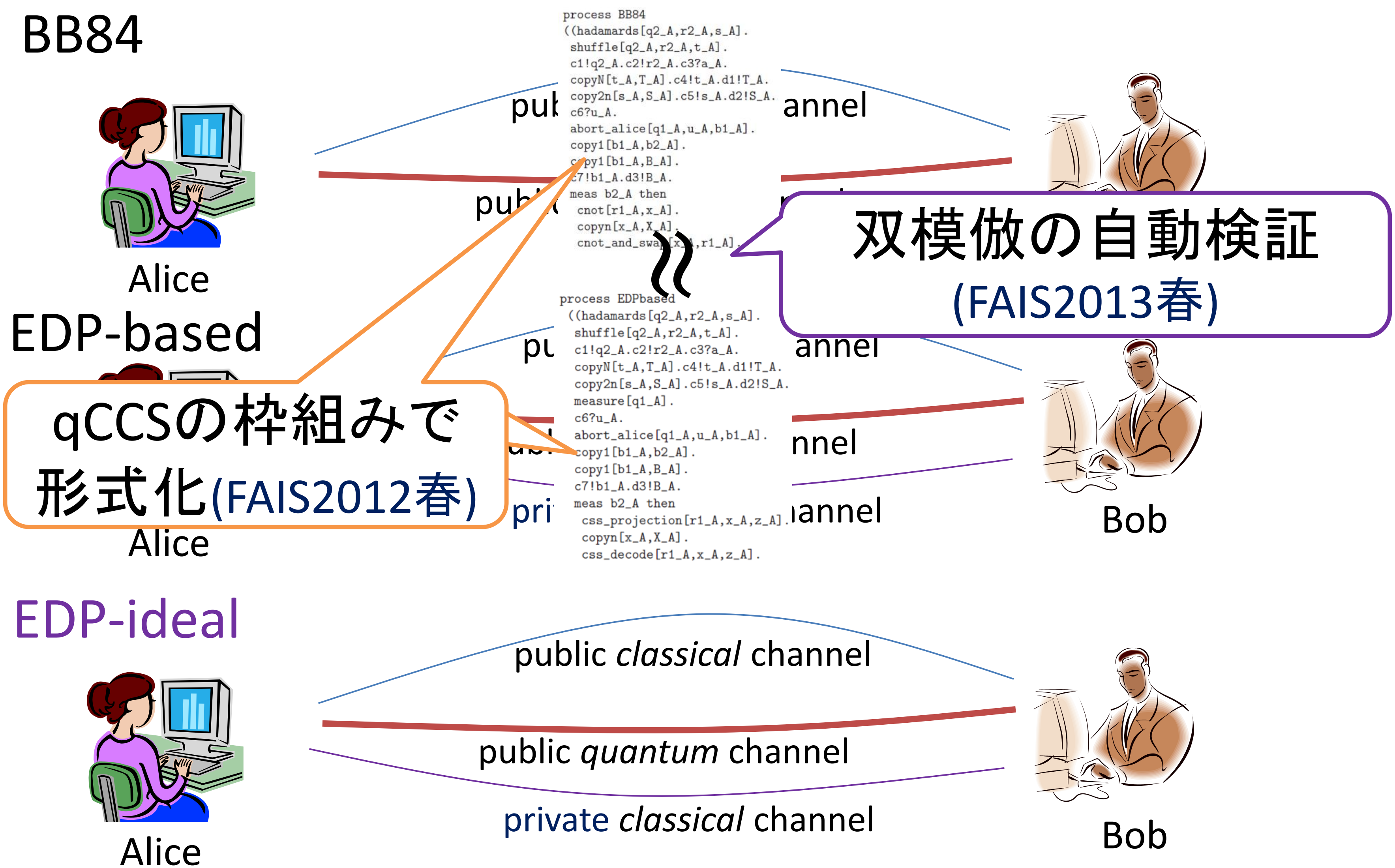
Our formal verification



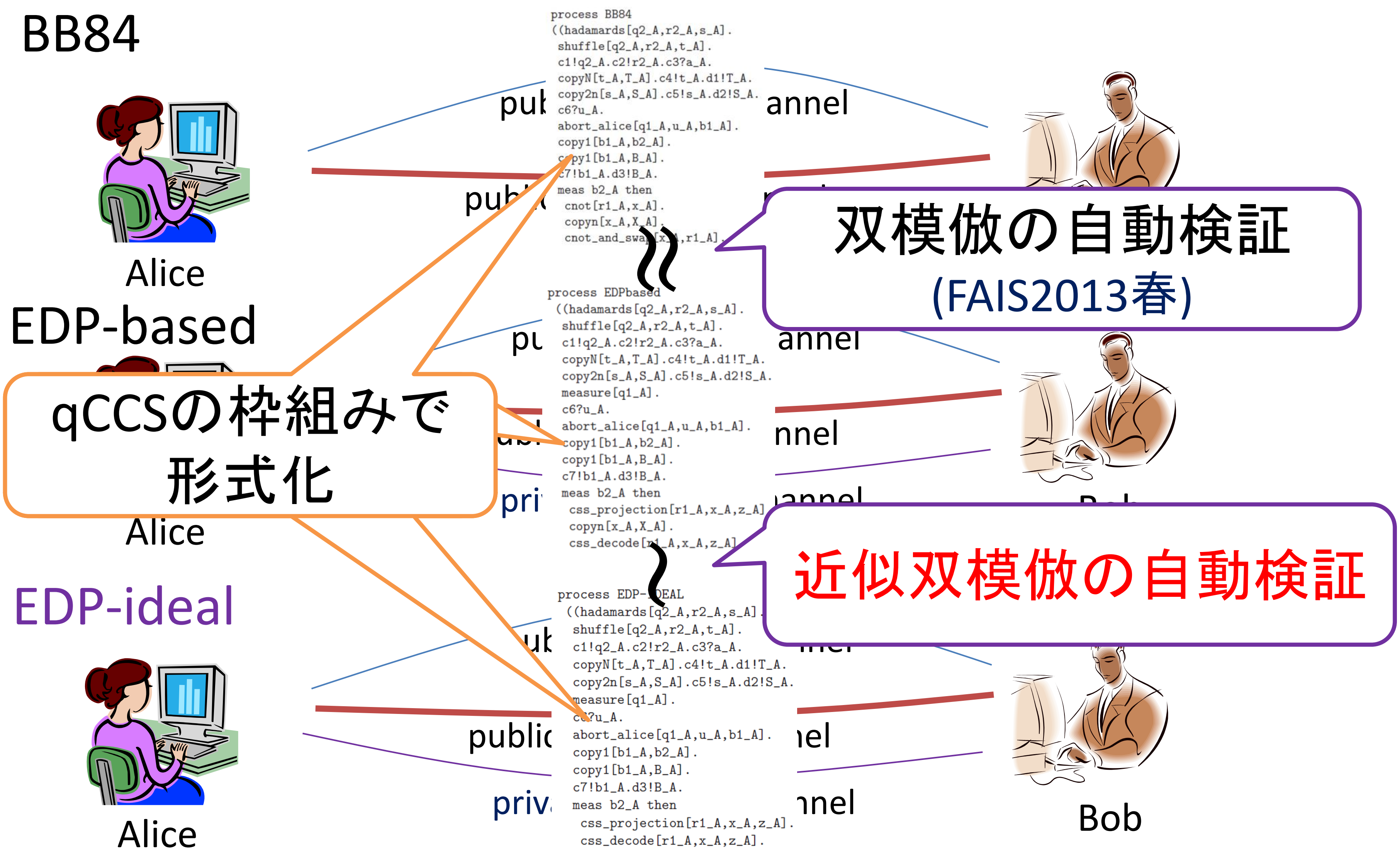
Our formal verification



Our formal verification



Our formal verification



本研究の貢献

qCCSをツール用に
簡略化した枠組み

- 非決定的qCCSのコンフィグレーションたちに対して, 近似双模倣関係を定義した
  - 並行合成に関して閉じている
    - $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$ ならば $\langle P || R, \rho \rangle \sim \langle Q || R, \sigma \rangle$
  - 安全性証明に適用可能
- 検証ツールを拡張し, Shor-Preskillの証明の後半部分に適用した

Outline

- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Outline

- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Syntax of qCCS [Feng+'11]

Quantum communication

$$P, Q ::= \mathtt{nil} \mid c?x.P \mid c!e.P \mid \mathsf{c}?q.P \mid \mathsf{c}!q.P$$

$$\mathtt{if}\ b\ \mathtt{then}\ P\ \mathtt{fi} \mid op[\tilde{q}].P \mid M[\tilde{q}; x].P \mid P||Q \mid P\backslash L$$

Quantum operation

Measurement

e : real expression
b : boolean expression on real numbers
q : quantum variable
M : Hermitian operator
op : TPCP map
$\tilde{q}$: sequence of quantum variables
L : set of channels

Configuration

- A pair $\langle P, \rho \rangle$ of a process P and a quantum state ρ

$$\langle \underbrace{\mathtt{c}!q_B.M[q_A;x].\mathtt{nil}}_{P}, \underbrace{|+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E}_{\rho} \rangle$$

where ρ_E is the outsider's arbitrary state

$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Probabilistic labeled transition

- $\langle P, \rho \rangle \stackrel{\alpha}{\rightarrow} \mu$
  - A configuration $\langle P, \rho \rangle$ performs an action α and transits to a probability distribution μ on configurations

ρ is a distribution on quantum states

μ is a distribution on configurations

Probabilistic labeled transition

1 $\langle \underline{\mathtt{c}!q_B}.M[q_A;x].\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$

Sends q_B to the
outside through **c**

$$\Big\downarrow \; \mathbf{c}!q_B$$

1 $\langle \underline{M[q_A;x]}.\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$

Measures q_A

$\swarrow \tau \qquad \tau \searrow$

1/2 $\langle \mathtt{nil}, |0\rangle\langle 0|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$

1/2 $\langle \mathtt{nil}, |1\rangle\langle 1|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$

Probabilistic labeled transition

$$1 \quad \langle \mathtt{c}!q_B.M[q_A;x].\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$$

$$\Big\downarrow \mathbf{c}!q_B$$

$$1 \quad \langle M[q_A;x].\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$$

$$\swarrow \tau \qquad \tau \searrow$$

Only measurement causes a prob. branch

$$1/2 \quad \langle \mathtt{nil}, |0\rangle\langle 0|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle \qquad 1/2 \quad \langle \mathtt{nil}, |1\rangle\langle 1|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E\rangle$$

Probabilistic labeled transition

$$1 \quad \langle \mathtt{c}!q_B.M[q_A;x].\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E \rangle$$

Visible action
from the outside

$$\Big\downarrow \mathbf{c}!q_B$$

$$1 \quad \langle M[q_A;x].\mathtt{nil}, |+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E \rangle$$

Invisible action
from the outside

$$\swarrow \tau \qquad \tau \searrow$$

1/2

$$\langle \mathtt{nil}, |0\rangle\langle 0|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E \rangle \qquad \langle \mathtt{nil}, |1\rangle\langle 1|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E \rangle$$

Bisimulation Relation

- Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are bisimilar, written $\langle P, \rho \rangle \approx \langle Q, \sigma \rangle$, if
  1. $\mathrm{qv}(P) = \mathrm{qv}(Q)$ and $\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \mathrm{tr}_{\mathrm{qv}(Q)}(\sigma)$ hold

     -- namely, the states that the outsider can access are the same
  2. For any outsider's operation E acting on $qVar - \mathrm{qv}(P)$, Each transition of $\langle P, E\rho \rangle$ is "simulated" by those of $\langle Q, E\sigma \rangle$ up to τ transitions

Bisimulation Relation

- Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are bisimilar, written $\langle P, \rho \rangle \approx \langle Q, \sigma \rangle$, if
  1. $\mathrm{qv}(P) = \mathrm{qv}(Q)$ and $\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \mathrm{tr}_{\mathrm{qv}(Q)}(\sigma)$ hold

     -- namely, the states that the outside ... are the same

     ...P)),

$$\underbrace{\langle \mathtt{c}!q_B.M[q_A;x].\mathtt{nil}}_{P}, \underbrace{|+\rangle\langle+|_{q_A} \otimes |0\rangle\langle 0|_{q_B} \otimes \rho_E}_{\rho} \rangle$$

のとき,

$$\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \rho_E$$

Bisimulation Relation

- Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are bisimilar, written $\langle P, \rho \rangle \approx \langle Q, \sigma \rangle$, if
  1. $\mathrm{qv}(P) = \mathrm{qv}(Q)$ and $\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \mathrm{tr}_{\mathrm{qv}(Q)}(\sigma)$ hold

     -- namely, the states that the outsider can access are the same
  2. For any outsider's operation E acting on $qVar - \mathrm{qv}(P)$,
     Each transition of $\langle P, E\rho \rangle$ is "simulated"
     by those of $\langle Q, E\sigma \rangle$ up to τ transitions

Example of Bisimulation

$$\langle P, \rho \rangle \approx \langle Q, \sigma \rangle$$

Example of Bisimulation

$\langle P, \rho \rangle \qquad \approx \qquad \langle Q, \sigma \rangle$

$\langle P, E\rho \rangle \qquad\qquad \langle Q, E\sigma \rangle$

Example of Bisimulation

$$\begin{tikzcd}
\langle P, \rho \rangle \arrow[rr, phantom, "\approx"] & & \langle Q, \sigma \rangle \\
\langle P, E\rho \rangle \arrow[d, "\mathbf{c}!\, q"] & & \langle Q, E\sigma \rangle \\
\langle P', \rho' \rangle & &
\end{tikzcd}$$

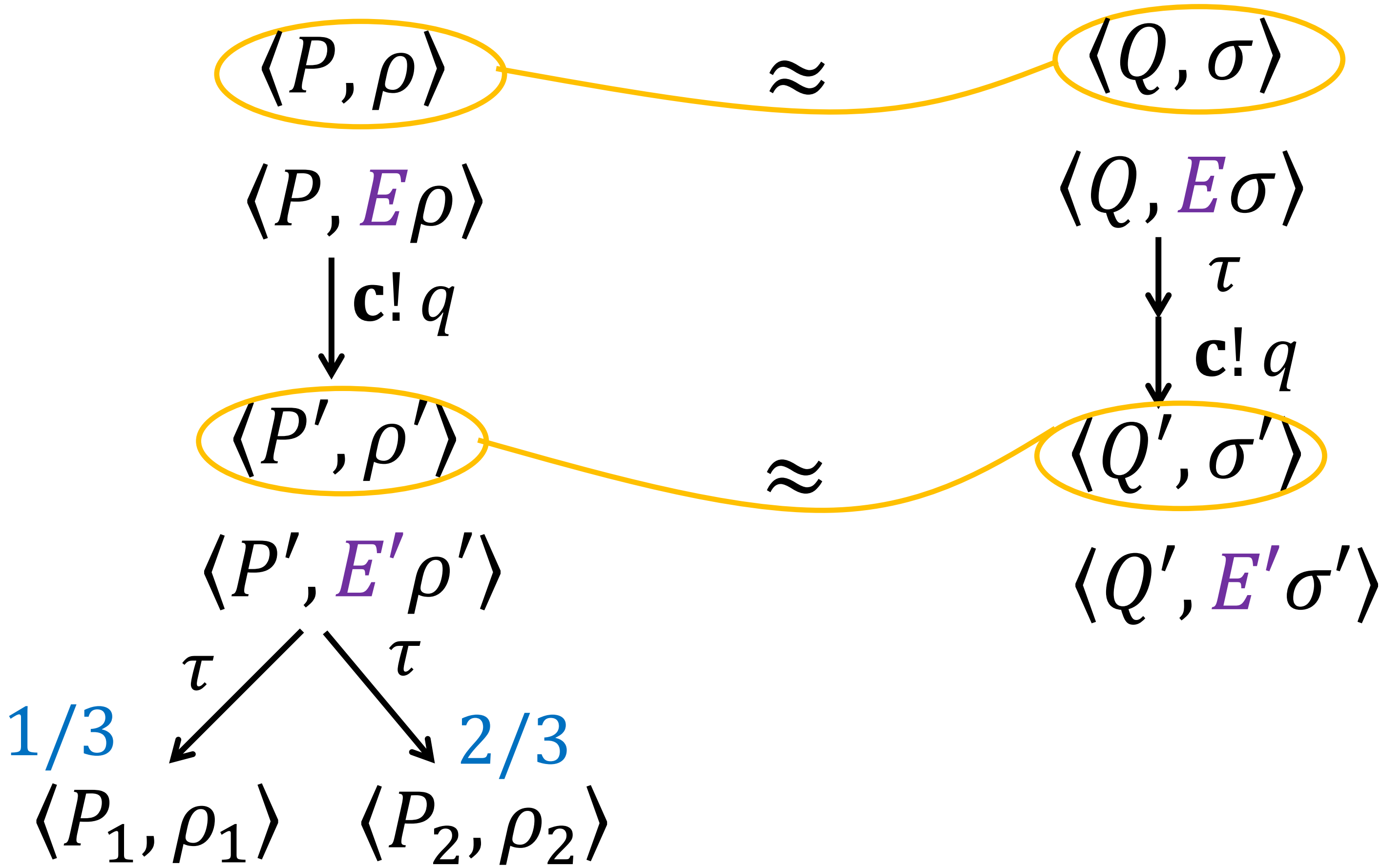
Example of Bisimulation

$$
\begin{tikzcd}
\langle P, \rho \rangle & \approx & \langle Q, \sigma \rangle \\
\langle P, E\rho \rangle \arrow[dd, "\mathbf{c}!\,q"] & & \langle Q, E\sigma \rangle \arrow[d, "\tau"] \\
& & {} \arrow[d, "\mathbf{c}!\,q"] \\
\langle P', \rho' \rangle & \approx & \langle Q', \sigma' \rangle
\end{tikzcd}
$$

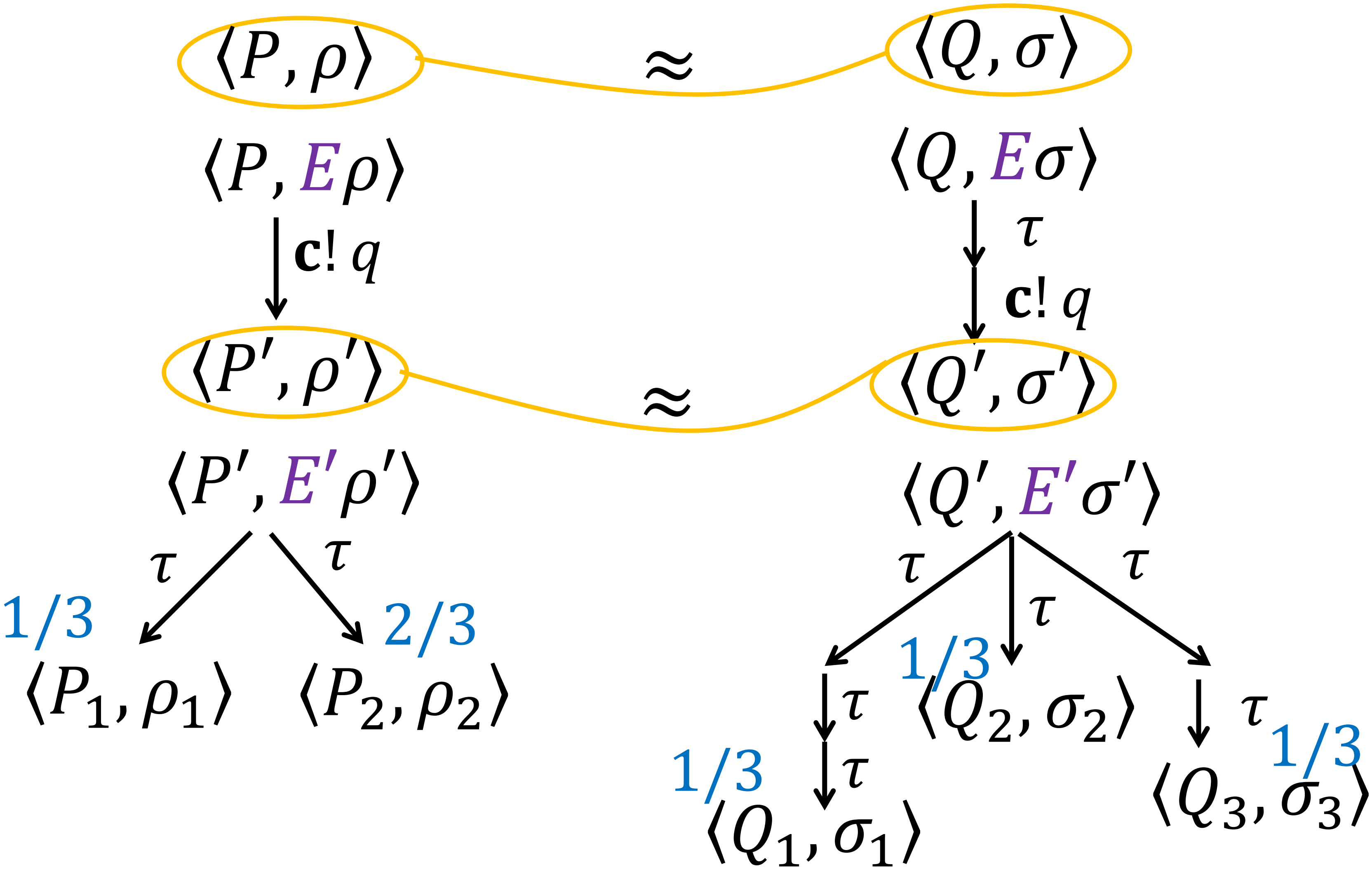
Example of Bisimulation

$$
\begin{tikzcd}
\langle P, \rho \rangle \arrow[rr, phantom, "\approx"] & & \langle Q, \sigma \rangle \\
\langle P, E\rho \rangle \arrow[dd, "\mathbf{c}!\,q"] & & \langle Q, E\sigma \rangle \arrow[d, "\tau"] \\
& & {} \arrow[d, "\mathbf{c}!\,q"] \\
\langle P', \rho' \rangle \arrow[rr, phantom, "\approx"] & & \langle Q', \sigma' \rangle \\
\langle P', E'\rho' \rangle & & \langle Q', E'\sigma' \rangle
\end{tikzcd}
$$

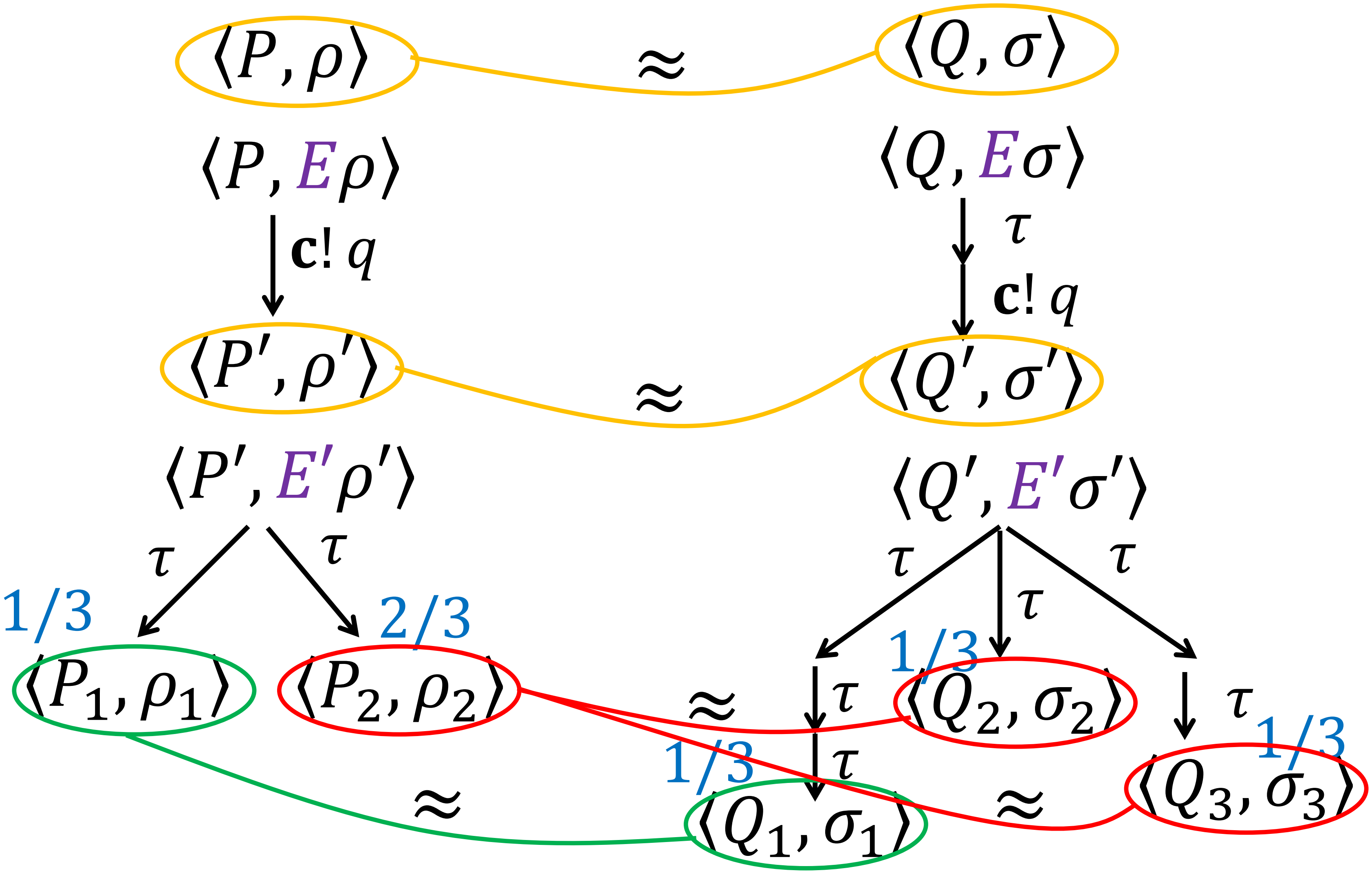
Example of Bisimulation



Example of Bisimulation



Example of Bisimulation



Outline

- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Simplification of Syntax

- $M[q;x]$ and **if** must always be written together

$$M[q;x].\texttt{if}\ x = 1\ \texttt{then}\ P\ \texttt{fi} \Longrightarrow \texttt{meas}\, q\ \texttt{then}\ P\ \texttt{saem}$$

$$\begin{aligned} P, Q ::= {} & \texttt{discard}(\tilde{q}) \mid \texttt{c}!q.P \mid \texttt{c}?q.P \mid op[\tilde{q}].P \\ & \mid P||Q \mid \underline{\texttt{meas}\, q\ \texttt{then}\ P\ \texttt{saem}} \mid P\backslash L \end{aligned}$$

q must be a qubit

Simplification of syntax

$$\begin{tikzcd}[column sep=tiny]
& \langle \texttt{meas}\ q\ \texttt{then}\ \texttt{c!}r.P\ \texttt{saem}, |+0\rangle\langle +0|_{q,r} \otimes \rho_E \rangle \arrow[dl, "\tau"'] \arrow[dr, "\tau"] & \\
1/2\ \ \langle \texttt{discard(r,}\ldots\texttt{)}, |00\rangle\langle 00|_{q,r} \otimes \rho_E \rangle & & 1/2\ \ \langle \texttt{c!r.}P, |10\rangle\langle 10|_{q,r} \otimes \rho_E \rangle \arrow[d, "\texttt{c!r}"] \\
& & 1/2\ \ \langle P, |10\rangle\langle 10|_{q,r} \otimes \rho_E \rangle
\end{tikzcd}$$

Simplification of operational semantics

$$\langle \texttt{meas}\ q\ \texttt{then}\ \texttt{c}!r.P\ \texttt{saem}, |+0\rangle\langle+0|_{q,r} \otimes \rho_E\rangle$$

probability to reach here

$\xrightarrow{\tau}$

1/2

$$\langle \texttt{discard(r},\ldots\texttt{)}, |00\rangle\langle 00|_{q,r} \otimes \rho_E\rangle$$

trace is 1

1/2

$$\langle \texttt{c!r.}P, |10\rangle\langle 10|_{q,r} \otimes \rho_E\rangle$$

$\downarrow$ c!r

1/2 $\langle P, |10\rangle\langle 10|_{q,r} \otimes \rho_E\rangle$

Simplification of operational semantics

- Excluded probability from the transition system by extending the def. of configurations

$$\langle \texttt{meas}\ q\ \texttt{then}\ \texttt{c!}r.P\ \texttt{saem}, |+0\rangle\langle +0|_{q,r} \otimes \rho_E\rangle$$

$\xrightarrow{\tau}$

$$\langle \texttt{discard(r,}\ldots\texttt{)}, 1/2\,(|00\rangle\langle 00|_{q,r} \otimes \rho_E)\rangle$$

trace is 1/2
probability to reach here

$\xrightarrow{\tau}$

$$\langle \texttt{c!r.}P, 1/2\,(|10\rangle\langle 10|_{q,r} \otimes \rho_E)\rangle$$

$\xrightarrow{\texttt{c!r}}$

$$\langle P, 1/2\,(|10\rangle\langle 10|_{q,r} \otimes \rho_E)\rangle$$

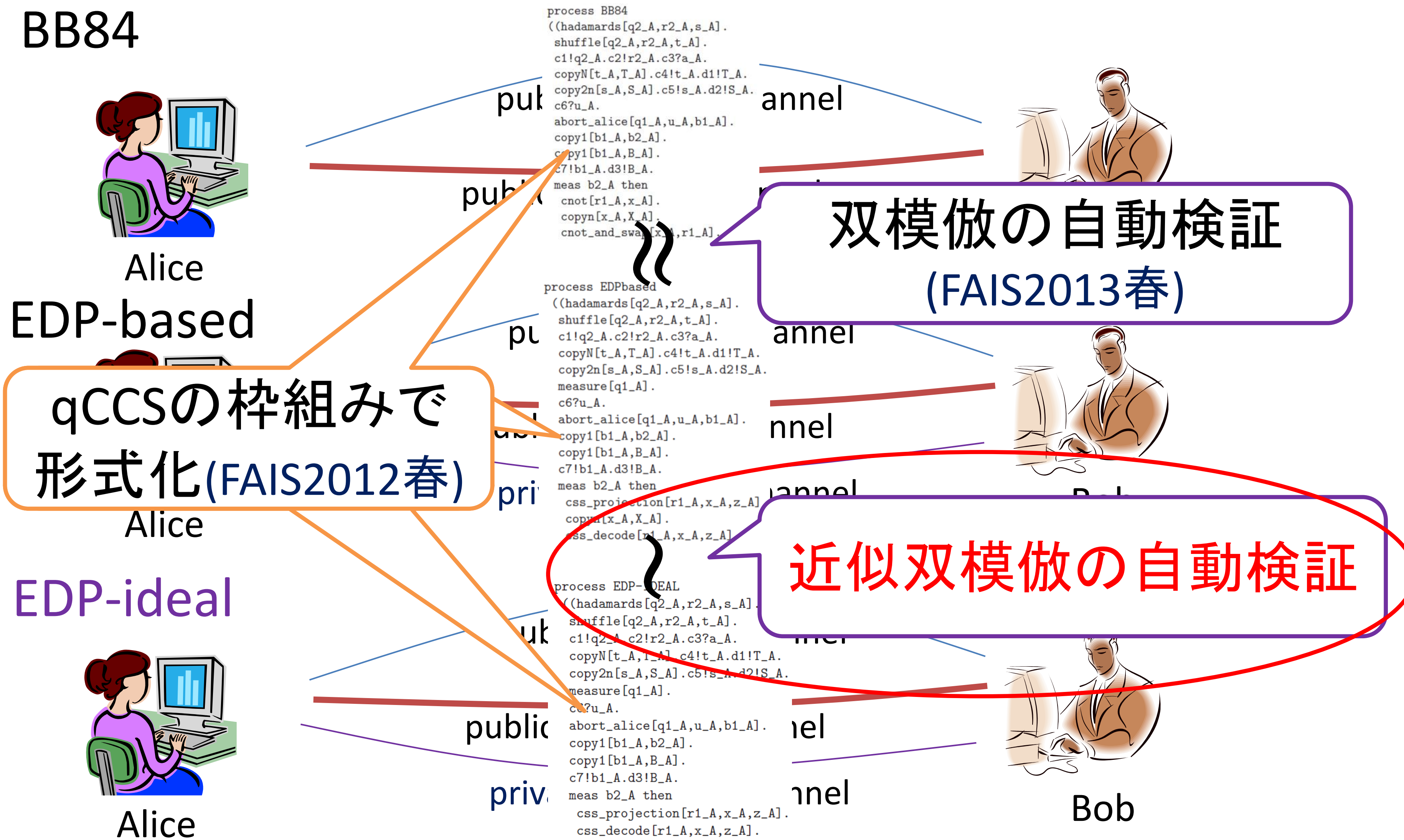
Simplified formal framework

- We call nondeterministic qCCS
- $M[q;x].\mathtt{if}\ x=1\ \mathtt{then}\ P\ \mathtt{fi} \Longrightarrow \mathtt{meas}\, q\ \mathtt{then}\ P\ \mathtt{saem}$
- Transition system is only nondeterministic
  - For a configuration $\langle P, \rho \rangle$,
    $\mathrm{tr}(\rho)$ is the probability to reach it
    and the quantum state is $\frac{\rho}{\mathrm{tr}(\rho)}$

Outline

- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Our formal verification



Trace distance

- $d(\rho, \sigma) \coloneqq \frac{1}{2}\mathrm{tr}|\rho - \sigma|$, where $|A| = \sqrt{A^\dagger A}$
- Examples
  - $d(|0\rangle\langle 0|, |+\rangle\langle +|) = \frac{1}{2}$
  - $d\left(|0\rangle\langle 0|^{\otimes n}, |+\rangle\langle +|^{\otimes n}\right) = 1 - \frac{1}{2^n}$

Approximate Bisimulation

- Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are approximately bisimilar, written $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$, if
  1. $\mathrm{qv}(P) = \mathrm{qv}(Q)$ hold and $d\left(\mathrm{tr}_{\mathrm{qv}(P)}(\rho), \mathrm{tr}_{\mathrm{qv}(Q)}(\sigma)\right)$ is negligible
  2. For any outsider's operation E acting on $qVar - \mathrm{qv}(P)$, $\langle P, E\rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle$ holds and $\mathrm{tr}(\rho')$ is non-negligible, $\langle Q, E\sigma \rangle \xrightarrow{\tau *} \xrightarrow{\widehat{\alpha}} \xrightarrow{\tau *} \langle Q', \sigma' \rangle$ and $\langle P', \rho' \rangle \sim \langle Q', \sigma' \rangle$ hold for some $\langle Q', \sigma' \rangle$, and conversely

Properties of approximate bisimulation

- The relation $\sim$ is an equivalence relation
- If $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$ holds, then $\langle P || R, \rho \rangle \sim \langle Q || R, \sigma \rangle$ holds for all process R

Application of the property

- Multiple session

$\langle P, \rho \otimes \rho_E \rangle \sim \langle Q, \sigma \otimes \rho_E \rangle$ for all ρ_E, and

$\langle P', \rho' \otimes \rho'_E \rangle \sim \langle Q', \sigma' \otimes \rho'_E \rangle$ for all ρ'_E

implies

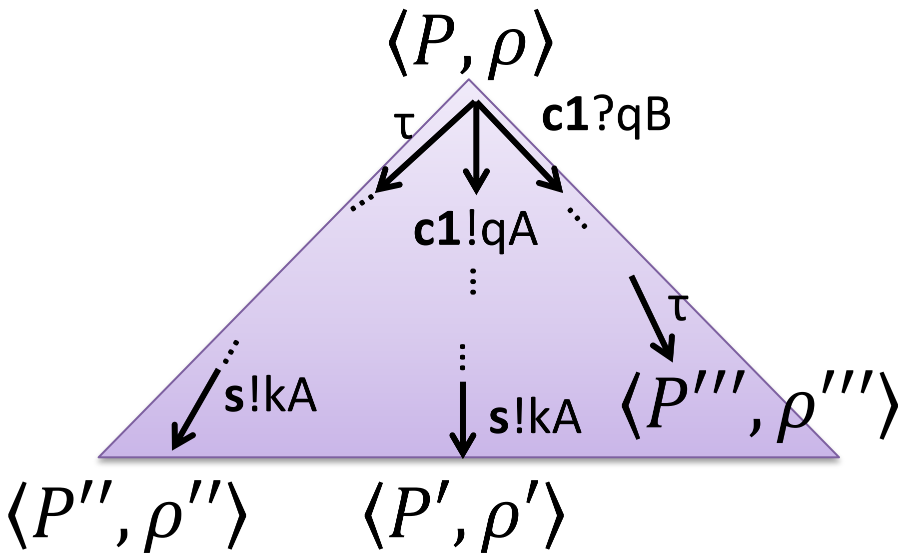
$\langle P || P', \rho \otimes \rho''_E \rangle \sim \langle Q || Q', \sigma \otimes \rho''_E \rangle$ for all ρ''_E

Outline

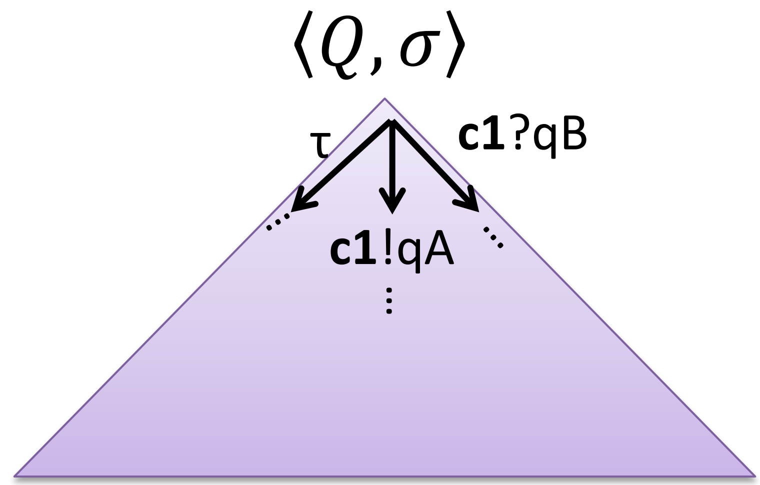
- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Application to QKD protocols

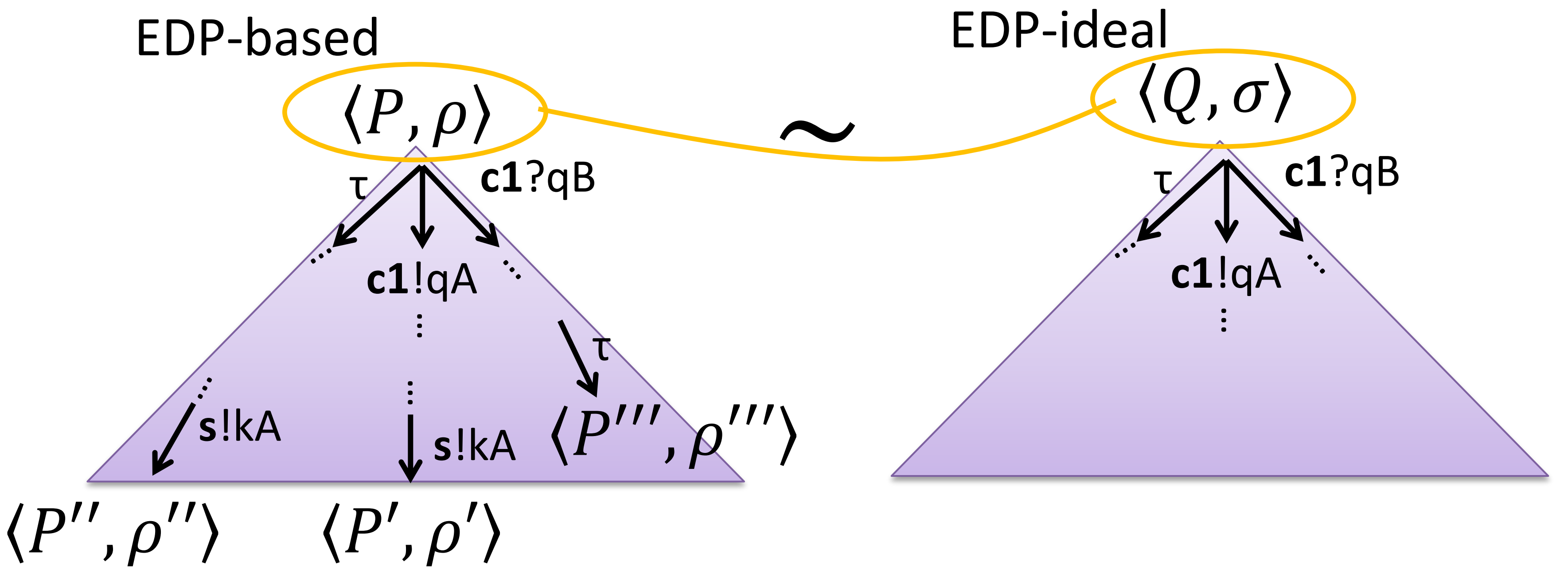
EDP-based



EDP-ideal

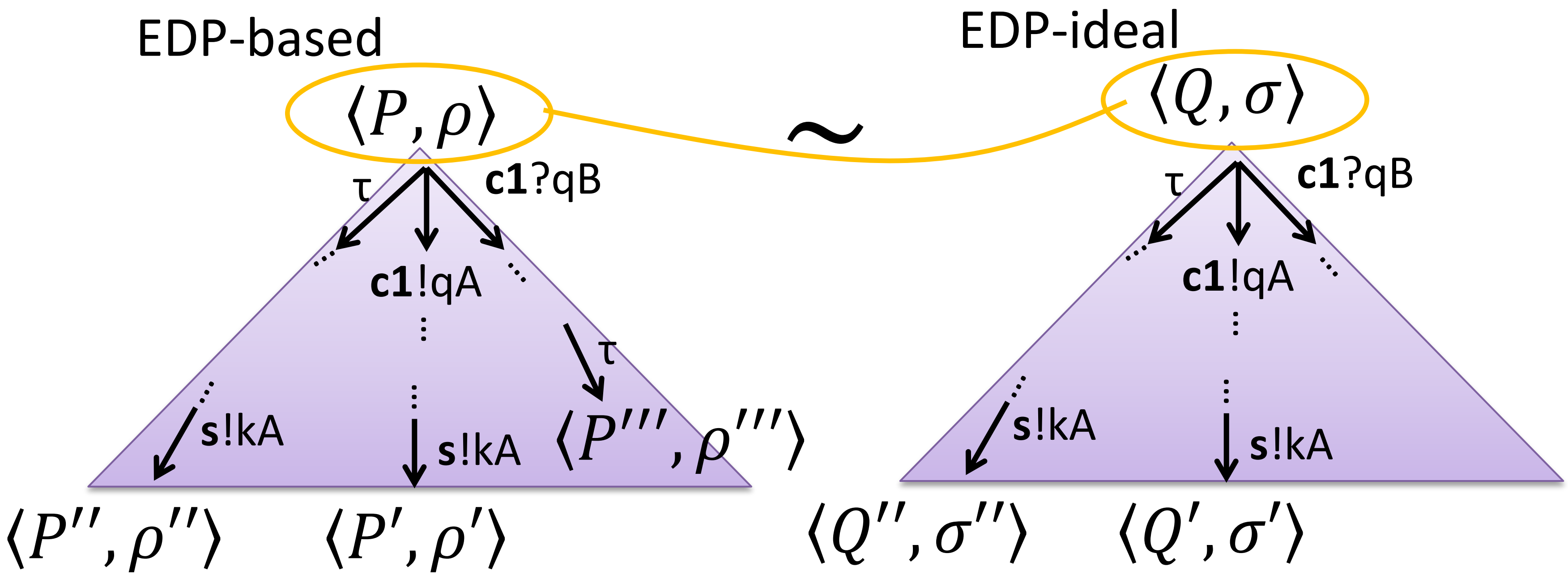


Application to QKD protocols



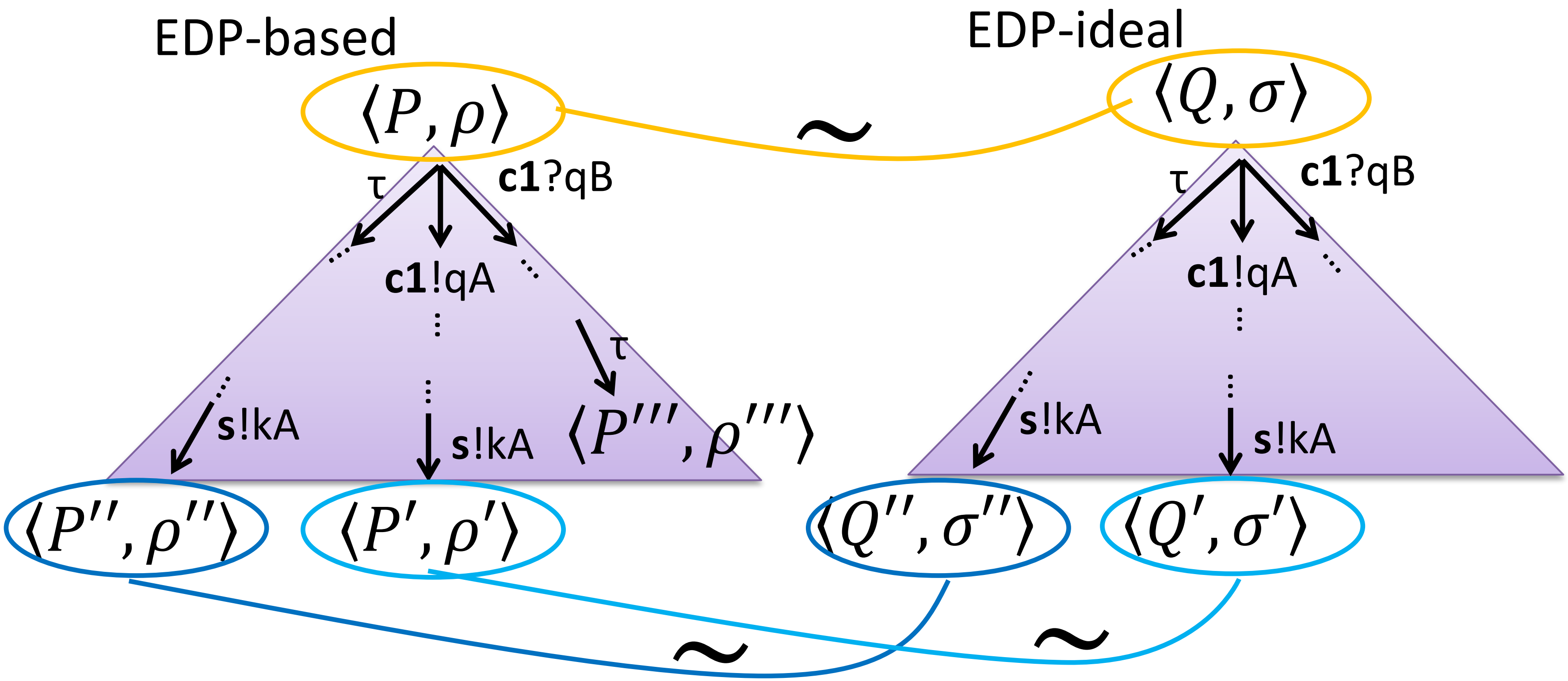
$\mathrm{tr}(\rho')$ is non-neg.
$\mathrm{tr}(\rho'')$ is non-neg.
$\mathrm{tr}(\rho''')$ is neg.

Application to QKD protocols



$\mathrm{tr}(\rho')$ is non-neg.
$\mathrm{tr}(\rho'')$ is non-neg.
$\mathrm{tr}(\rho''')$ is neg.

Application to QKD protocols



$\mathrm{tr}(\rho')$ is non-neg.
$\mathrm{tr}(\rho'')$ is non-neg.
$\mathrm{tr}(\rho''')$ is neg.

Trace distances are negligibly small

Property of distance of probability-weighted density matrices

- If $d(\rho, \sigma)$ is negligible, then $|\mathrm{tr}(\rho) - \mathrm{tr}(\sigma)|$ is negligible and $|\mathrm{tr}(\rho)\mathrm{tr}\left(\pi \frac{\rho}{\mathrm{tr}(\rho)}\right) - \mathrm{tr}(\sigma)\mathrm{tr}\left(\pi \frac{\sigma}{\mathrm{tr}(\sigma)}\right)|$ is negligible for all projector π
  - For a configuration $\langle P, \rho \rangle$,
    - $\mathrm{tr}(\rho)$ is the probability to reach $\langle P, \rho \rangle$
    - $\frac{\rho}{\mathrm{tr}(\rho)}$ is the quantum state

Property of distance of

pr

Joint probability that
the configuration reaches $\langle P, \rho \rangle$ and
obtain the measurement result corresponding to π

- If
$|\mathrm{tr}(\rho) - \mathrm{tr}($ $)|$ is negligible and
$$\left|\boxed{\mathrm{tr}(\rho)\mathrm{tr}\left(\pi \frac{\rho}{\mathrm{tr}(\rho)}\right)} - \mathrm{tr}(\sigma)\mathrm{tr}\left(\pi \frac{\sigma}{\mathrm{tr}(\sigma)}\right)\right|$$ is
negligible for all projector π
  - For a configuration $\langle P, \rho \rangle$,
    - $\mathrm{tr}(\rho)$ is the probability to reach $\langle P, \rho \rangle$
    - $\frac{\rho}{\mathrm{tr}(\rho)}$ is the quantum state

Application to QKD

- If $d(\rho, \sigma)$ is negligible, then
  $|\mathrm{tr}(\rho) - \mathrm{tr}(\sigma)|$ is negligible and
  $|\mathrm{tr}(\rho)\mathrm{tr}\left(\pi_i \frac{\rho}{\mathrm{tr}(\rho)}\right) - \underline{\mathrm{tr}(\sigma)\mathrm{tr}\left(\pi_i \frac{\sigma}{\mathrm{tr}(\sigma)}\right)}|$ is neg.

This is 1/2

Let

ρ : a final state of an execution of EDP-based

σ : a final state of an execution of EDP-ideal

π_i : the projector to the subspace where
i-th bits of Alice's and Eve's key are equal

Application to QKD

- If $d(\rho, \sigma)$ is negligible, then
  $|\mathrm{tr}(\rho) - \mathrm{tr}(\sigma)|$ is negligible and
  $\left|\mathrm{tr}(\rho)\mathrm{tr}\left(\pi_i \frac{\rho}{\mathrm{tr}(\rho)}\right) - \mathrm{tr}(\sigma)\underline{\mathrm{tr}\left(\pi_i \frac{\sigma}{\mathrm{tr}(\sigma)}\right)}\right|$ is neg.

This is 1/2

We can derive that
$|\mathrm{p}(k_{A,i} = k_{E,i}) - 1/2|$ is negligible for all i.

Outline

- Quantum process calculus qCCS
- Nondeterministic qCCS
- Approximate bisimulation
- Application to Shor-Preskill's security proof
- Experiment

Verifier2

- Checks $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$
- Input:
  - $\langle P, \rho \rangle, \langle Q, \sigma \rangle$
  - A set of equations eqs
  - A set of indistinguishability expressions $inds$
- Output: *true* or *false*

プロトコルの形式化

```
process EDPbased
 ((hadamards[q2_A,r2_A,s_A].
   shuffle[q2_A,r2_A,t_A].
   c1!q2_A.c2!r2_A.c3?a_A.
   copyN[t_A,T_A].c4!t_A.d1!T_A.
   copy2n[s_A,S_A].c5!s_A.d2!S_A.
   measure[q1_A].
   c6?u_A.
   abort_alice[q1_A,u_A,b1_A].
   copy1[b1_A,b2_A].
   copy1[b1_A,B_A].
   c7!b1_A.d3!B_A.
   meas b2_A then
    css_projection[r1_A,x_A,z_A].
    copyn[x_A,X_A].
    css_decode[r1_A,x_A,z_A].
    measure[r1_A].
    c8!x_A.d4!X_A.
    c9!z_A.barrier!f_A.
    cka!r1_A.
    discard(q1_A,b2_A,a_A,
            u_A,v1_A,v_B)
   saem
 ||
   c1?q_B.c2?r_B.
   c3!a_B.d5!A_B.
   c4?t_B.unshuffle[q_B,r_B,t_B].
   c5?s_B.hadamards[q_B,r_B,s_B].
   measure[q_B].
   copyn[q_B,Q_B].c6!q_B.d6!Q_B.
   c7?b_B.
   meas b_B then
    c8?x_B.c9?z_B.
    css_syndrome[r_B,x_B,z_B,
                 sx_B,sz_B].
    css_correct[r_B,sx_B,sz_B].
    css_decode[r_B,x_B,z_B].
    measure[r_B].
    barrier?f_B.
    ckb!r_B.
    discard(b_B,s_B,t_B,x_B,
            z_B,sx_B,sz_B,f_B)
   saem)/{c3, c4, c5, c6, c7, c8,
    c9, barrier})
end
```

プロトコルの形式化

```
environment EDPbased_ENV
 EPR[q1_A,q2_A] * EPR[r1_A,r2_A]
 * RND_2n[s_A] * RND_N[t_A] *
 Z_1[b1_A] * Z_1[b2_A] * Z_n[x_A]
 * Z_n[z_A] * Z_2n[S_A] *
 Z_N[T_A] *
 Z_1[B_A] * Z_n[X_A] * Z_1[f_A]
 * Z_1[a_B] * Z_1[A_B] * Z_n[Q_B]
 * Z_n[sx_B] * Z_n[sz_B]
 * EVE[q_E] * Z_n_n[v1_A,v_B]
 * EVE1[q_B] * EVE2[r_B]
end
```

```
configuration EDPbased
 proc EDPbased
 env EDPbased_ENV
end
```

プロトコルの形式化

```
process EDP-IDEAL
 ((hadamards[q2_A,r2_A,s_A].
  shuffle[q2_A,r2_A,t_A].
  c1!q2_A.c2!r2_A.c3?a_A.
  copyN[t_A,T_A].c4!t_A.d1!T_A.
  copy2n[s_A,S_A].c5!s_A.d2!S_A.
  measure[q1_A].
  c6?u_A.
  abort_alice[q1_A,u_A,b1_A].
  copy1[b1_A,b2_A].
  copy1[b1_A,B_A].
  c7!b1_A.d3!B_A.
  meas b2_A then
   css_projection[r1_A,x_A,z_A].
   css_decode[r1_A,x_A,z_A].
   copyn[x_A,X_A].
   measure[r1_A].
   c8!x_A.d4!X_A.
   c9!z_A.
   create_key[rx_A,r1_A].
   barrier!f_A.
   cka!r1_A.
   discard(q1_A,b2_A,
           a_A,u_A,rx_A)
  saem
 ||
  c1?q_B.c2?r_B.
  c3!a_B.d5!A_B.
  c4?t_B.unshuffle[q_B,r_B,t_B].
  c5?s_B.hadamards[q_B,r_B,s_B].
  measure[q_B].
  copyn[q_B,Q_B].c6!q_B.d6!Q_B.
  c7?b_B.
  meas b_B then
   c8?x_B.c9?z_B.
   css_syndrome[r_B,x_B,
                z_B,sx_B,sz_B].
   css_correct[r_B,sx_B,sz_B].
   css_decode[r_B,x_B,z_B].
   measure[r_B].
   create_key[rx_B,r_B].
   barrier?f_B.
   ckb!r_B.
   discard(b_B,s_B,t_B,x_B,z_B,
           sx_B,sz_B,f_B,rx_B)
  saem)/{c3, c4, c5, c6,
         c7, c8, c9, barrier})
end
```

プロトコルの形式化

```
environment EDP-IDEAL_ENV
 EPR[q1_A,q2_A] * EPR[r1_A,r2_A]
 * RND_2n[s_A] * RND_N[t_A]
 * Z_1[b1_A] * Z_1[b2_A]
 * Z_n[x_A]
 * Z_n[z_A] * Z_2n[S_A]
 * Z_N[T_A]
 * Z_1[B_A] * Z_n[X_A] * Z_1[f_A]
 * Z_1[a_B] * Z_1[A_B] * Z_n[Q_B]
 * Z_n[sx_B] * Z_n[sz_B]
 * EVE[q_E]
 * EVE1[q_B] * EVE2[r_B]
 * EPR[rx_A,rx_B]
end

configuration EDP-IDEAL
 proc EDP-IDEAL
 env  EDP-IDEAL_ENV
end
```

ユーザ定義近似式

```
indistinguishable E1 n
 Tr[b1_A,b2_A,q1_A,q_B,r_B,rx_A,rx_B,s_A,t_A,x_A,z_A](
  create_key[rx_A,r1_A](proj1[b1_A](measure[r1_A](
  copyn[x_A,X_A](css_decode[r1_A,x_A,z_A](
  css_projection[r1_A,x_A,z_A](proj1[b2_A](
  copy1[b1_A,B_A](copy1[b1_A,b2_A](
  abort_alice[q1_A,q_B,b1_A](measure[q1_A](
  copyn[q_B,Q_B](measure[q_B](
  hadamards[q_B,r_B,s_A](copy2n[s_A,S_A](
  unshuffle[q_B,r_B,t_A](copyN[t_A, T_A](
  __[q2_A,r2_A,q_E,q_B,r_B](
  shuffle[q2_A,r2_A,t_A](hadamards[q2_A,r2_A,s_A](
    EPR[q1_A,q2_A] * EPR[r1_A,r2_A] * EPR[rx_A,rx_B] *
    RND_2n[s_A] * Z_2n[S_A] * RND_N[t_A] * Z_N[T_A] *
    Z_1[b1_A] * Z_1[b2_A] * Z_1[B_A] * Z_n[Q_B] *
    Z_n[x_A] * Z_n[X_A] * Z_n[z_A] *
    __[q_B] * __[r_B] * __[q_E]
 ))))))))))))))))))))
 =
  Tr[b1_A,b2_A,q1_A,q_B,r_B,s_A,t_A,x_A,z_A](
   proj1[b1_A](measure[r1_A](
   copyn[x_A,X_A](css_decode[r1_A,x_A,z_A](
   css_projection[r1_A,x_A,z_A](proj1[b2_A](
   copy1[b1_A,B_A](copy1[b1_A,b2_A](
   abort_alice[q1_A,q_B,b1_A](measure[q1_A](
   copyn[q_B,Q_B](measure[q_B](
   hadamards[q_B,r_B,s_A](copy2n[s_A,S_A](
   unshuffle[q_B,r_B,t_A](copyN[t_A, T_A](
   __[q2_A,r2_A,q_E,q_B,r_B](
   shuffle[q2_A,r2_A,t_A](hadamards[q2_A,r2_A,s_A](
     EPR[q1_A,q2_A] * EPR[r1_A,r2_A] *
     RND_2n[s_A] * Z_2n[S_A] * RND_N[t_A] * Z_N[T_A] *
     Z_1[b1_A] * Z_1[b2_A] * Z_1[B_A] * Z_n[Q_B] *
     Z_n[x_A] * Z_n[X_A] * Z_n[z_A] *
     __[q_B] * __[r_B] * __[q_E]
   ))))))))))))))))))))
 end
```

Environment of the experiment

- Panasonic CF-J9
  Intel(R) Core(TM) i5 CPU
  M460 @ 2.53GHz, 1GB memory

Results

	BB84∼EDP	EDP∼ideal
eqs	6	0
inds	0	24
time (sec)	39.50	112.50
proc. calls	1039	907

今後の課題

- 等式･近似式の正しさの形式的検証
- qCCSの枠組みにおける近似双模倣関係の定義
- 非決定的qCCSの近似双模倣関係の健全性の考察
- 他のプロトコルへの適用
  - B92, six-state protocol

Approximate Bisimulation

- Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are approximately bisimilar, written $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$, if
  1. $\mathrm{qv}(P) = \mathrm{qv}(Q)$ hold and $d\left(\mathrm{tr}_{\mathrm{qv}(P)}(\rho), \mathrm{tr}_{\mathrm{qv}(Q)}(\sigma)\right)$ is negligible
  2. For any outsider's operation E acting on $qVar - \mathrm{qv}(P)$, $\langle P, E\rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle$ holds and $\mathrm{tr}(\rho')$ is non-negligible, $\langle Q, E\sigma \rangle \xrightarrow{\tau*} \xrightarrow{\widehat{\alpha}} \xrightarrow{\tau*} \langle Q', \sigma' \rangle$ and $\langle P', \rho' \rangle \sim \langle Q', \sigma' \rangle$ hold for some $\langle Q', \sigma' \rangle$, and conversely

Simplification of operational semantics

$$\langle \texttt{meas}\ q\ \texttt{then}\ \texttt{c!}q.P\ \texttt{saem}, |+0\rangle\langle +0|_{q,r} \otimes \rho_E \rangle$$

probability to reach here

1/2 $\langle \texttt{discard(r,}\ldots\texttt{)}, \underbrace{|00\rangle\langle 00|_{q,r} \otimes \rho_E}_{\text{trace is 1}} \rangle$

$\xrightarrow{\tau}$ 1/2 $\langle \texttt{c!r.}P, |10\rangle\langle 10|_{q,r} \otimes \rho_E \rangle$

$\xrightarrow{\texttt{c!r}}$ 1/2 $\langle P, |10\rangle\langle 10|_{q,r} \otimes \rho_E \rangle$

Simplification of operational semantics

- Excluded probability from the transition system by extending the def. of configurations

$$\langle \texttt{meas}\ q\ \texttt{then}\ \texttt{c!}q.P\ \texttt{saem}, |+0\rangle\langle +0|_{q,r} \otimes \rho_E\rangle$$

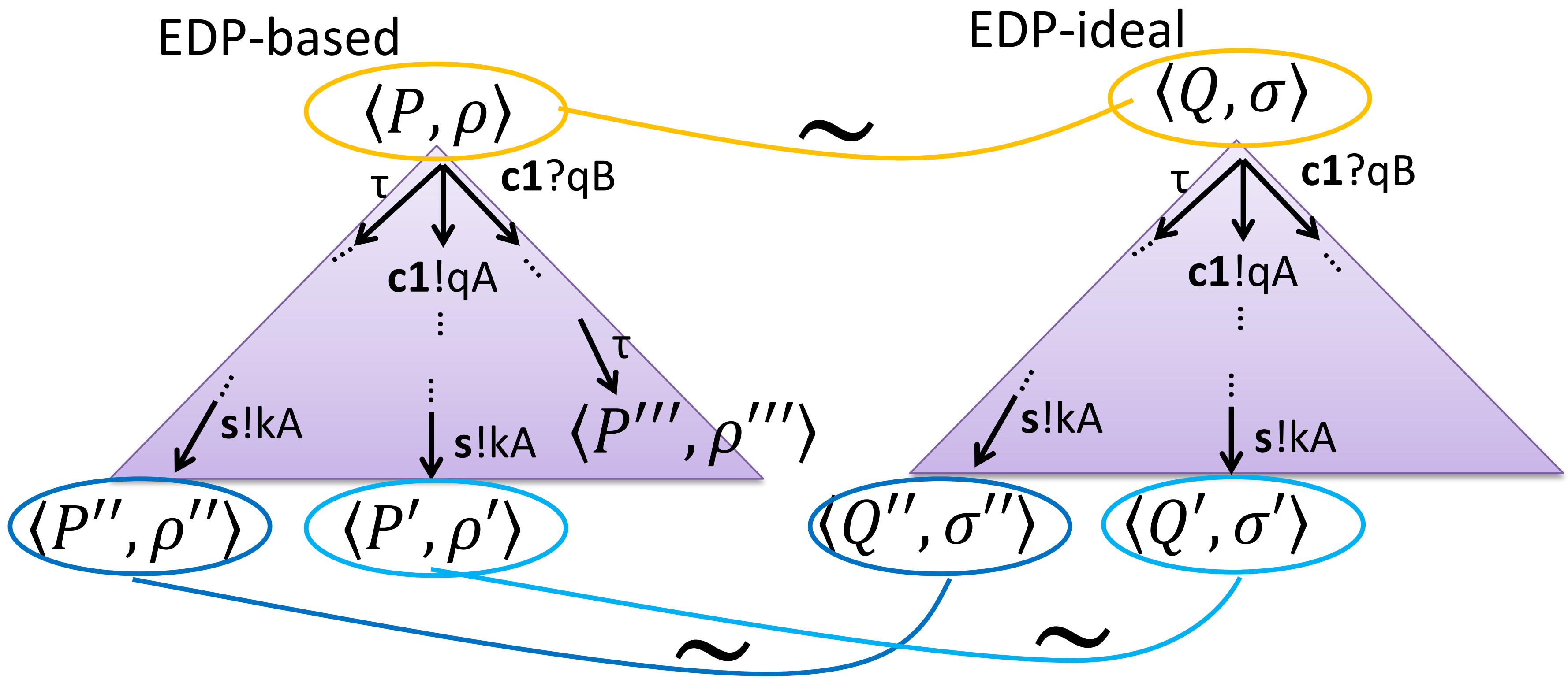
$$\xrightarrow{\tau} \langle \texttt{discard(r},\ldots\texttt{)}, \underline{1/2\,(|00\rangle\langle 00|_{q,r}\otimes\rho_E)}\rangle$$

trace is 1/2
probability to reach here

$$\xrightarrow{\tau} \langle \texttt{c!r}.P, 1/2\,(|10\rangle\langle 10|_{q,r}\otimes\rho_E)\rangle$$

$$\xrightarrow{\texttt{c!r}} \langle P, 1/2\,(|10\rangle\langle 10|_{q,r}\otimes\rho_E)\rangle$$

Application to QKD protocols



$\mathrm{tr}(\rho')$ is non-neg.
$\mathrm{tr}(\rho'')$ is non-neg.
$\mathrm{tr}(\rho''')$ is neg.

Trace distances are negligibly small

Verifier2

If
$$\begin{tikzcd} & \langle P_1, \overline{\rho_1} \rangle \\ \langle P, E[\tilde{r}](\bar{\rho}) \rangle \arrow[ur, "\tau"] \arrow[dr, "\tau"'] & \\ & \langle P_2, \overline{\rho_2} \rangle \end{tikzcd}$$
by measure,

it searches $\langle Q_1, \overline{\sigma_1} \rangle$ and $\langle Q_2, \overline{\sigma_2} \rangle$ such that

$$\left.\begin{array}{l} \langle Q, E[\tilde{r}](\bar{\sigma}) \rangle \xrightarrow{\tau^*} \langle Q_1, \overline{\sigma_1} \rangle \\[2em] \langle Q, E[\tilde{r}](\bar{\sigma}) \rangle \xrightarrow{\tau^*} \langle Q_2, \overline{\sigma_2} \rangle \end{array}\right\} \text{Not limited form}$$

and $\langle P_1, \overline{\rho_1} \rangle \approx_{\mathrm{Verifier2}} \langle Q_1, \overline{\sigma_1} \rangle$ and
$\langle P_2, \overline{\rho_2} \rangle \approx_{\mathrm{Verifier2}} \langle Q_2, \overline{\sigma_2} \rangle$

Verifier1

If
$$\begin{tikzcd} & \langle P_1, \overline{\rho_1} \rangle \\ \langle P, E[\tilde{r}](\bar{\rho}) \rangle \arrow[ur, "\tau"] \arrow[dr, "\tau"'] & \\ & \langle P_2, \overline{\rho_2} \rangle \end{tikzcd}$$
by measure,

it searches $\langle Q_1, \overline{\sigma_1} \rangle$ and $\langle Q_2, \overline{\sigma_2} \rangle$ such that

$$\begin{tikzcd} & & \cdot \arrow[r, "\tau^*"] & \langle Q_1, \overline{\sigma_1} \rangle \\ \langle Q, E[\tilde{r}](\bar{\sigma}) \rangle \arrow[r, "\tau^*"] & \cdot \arrow[ur, "\tau"] \arrow[dr, "\tau"'] & & \\ & & \cdot \arrow[r, "\tau^*"] & \langle Q_2, \overline{\sigma_2} \rangle \end{tikzcd}$$

measure branch

Limited form

and $\langle P_1, \overline{\rho_1} \rangle \approx_{\mathrm{Verifier1}} \langle Q_1, \overline{\sigma_1} \rangle$ and
$\langle P_2, \overline{\rho_2} \rangle \approx_{\mathrm{Verifier1}} \langle Q_2, \overline{\sigma_2} \rangle$