Title: Cryptographic Protocols in a Quantum World

Date: Apr 25, 2007 04:00 PM

URL: http://pirsa.org/07040029

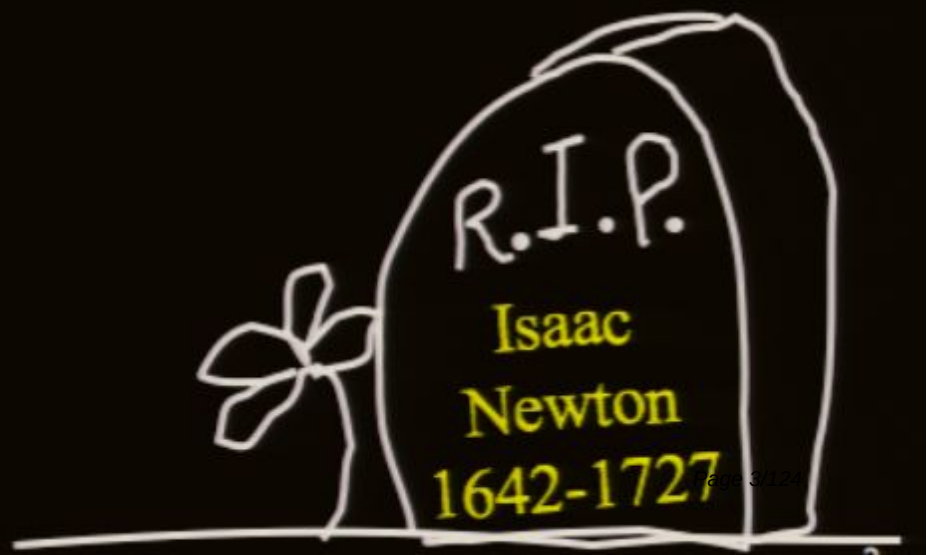
Abstract: I will survey recent feasibility results on building multi-party cryptographic protocols which manipulate quantum data or are secure against quantum adversaries. The focus will be protocols for secure evaluation of quantum circuits. Along the way, I'll discuss how quantum machines can (and can't) prove knowledge of a secret to a distrustful partner. The talk is based on recent unpublished results, as well as older joint work with subsets of Michael Ben-Or, Claude Crepeau, Daniel Gottesman, and Avinatan Hasidim (STOC '02, FOCS '02, Eurocrypt '05, FOCS '06).

Cryptography with Quantum Data

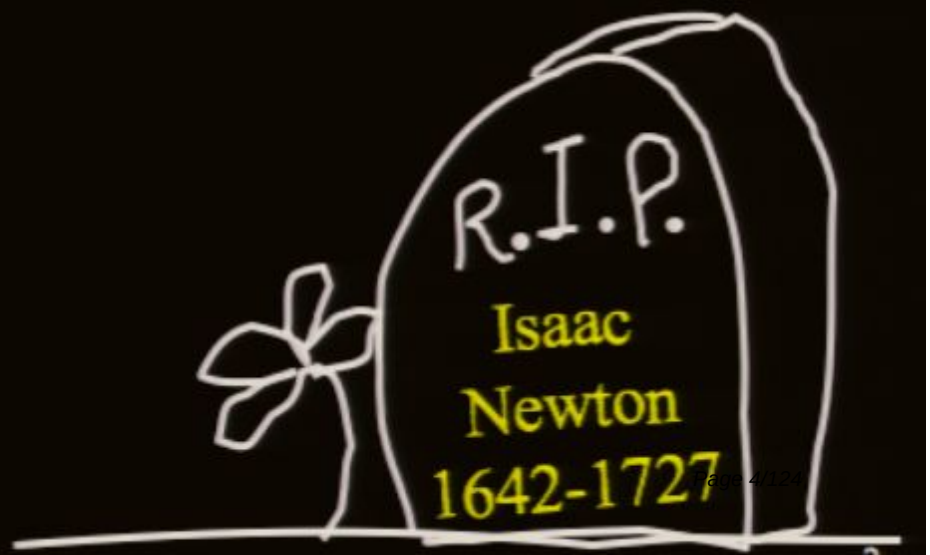
Adam Smith
Penn State

University of Waterloo
April 25, 2007

Cryptography in a Quantum World

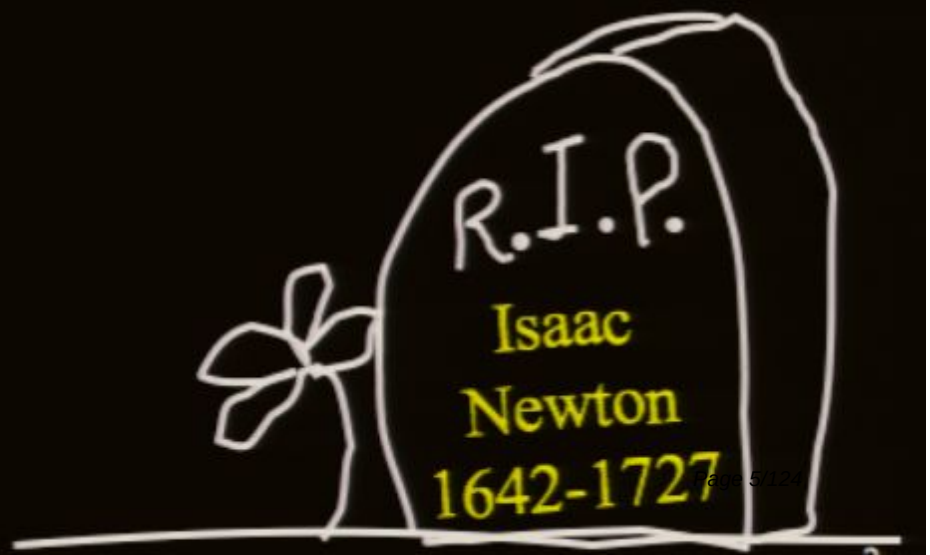


Cryptography in a Quantum World



Cryptography in a Quantum World

- Landscape changes!
  - New features appear
  - New difficulties arise
  - Some key pieces unchanged

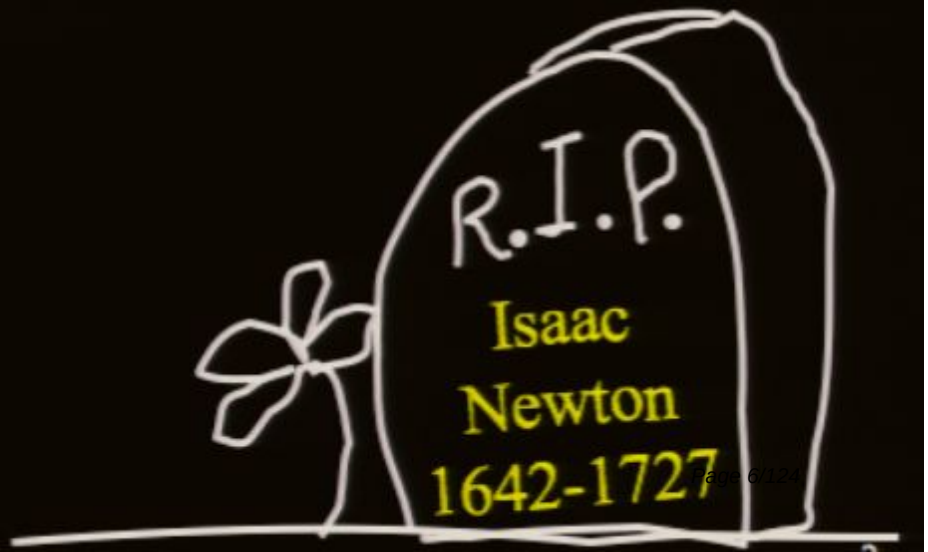


Cryptography in a Quantum World

- Landscape changes!
  - New features appear
  - New difficulties arise
  - Some key pieces unchanged

- Needed:

  Tools and language for reasoning about quantum adversaries



Cryptography in a Quantum World

- Landscape changes!
  - New features appear
  - New difficulties arise
  - Some key pieces unchanged

- Needed:

  Tools and language for reasoning about quantum adversaries

- The field is still very young
  - Some successes…
  - … occasional mistakes
  - Lots of questions!

Some Things That Change

Some Things That Change

- Statistically-secure key exchange [BB84,...]

Some Things That Change

- Statistically-secure key exchange [BB84,...]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]

Some Things That Change

- Statistically-secure key exchange [BB84,...]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]
- Weak 2-party unconditional primitives
  - coin flipping [ATVY,Amb]
  - string commitment [BCHLW]

Some Things That Change

- Statistically-secure key exchange [BB84,...]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]
- Weak 2-party unconditional primitives
  - coin flipping [ATVY,Amb]
  - string commitment [BCHLW]
- Some multi-prover commitments insecure [CST]

Some Things That Change

- Statistically-secure key exchange [BB84,…]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]
- Weak 2-party unconditional primitives
  - coin flipping [ATVY,Amb]
  - string commitment [BCHLW]
- Some multi-prover commitments insecure [CST]
- Some "extractors" fail vs quantum memory [IKW]
  - But some are OK [KMR,…]

Some Things That Change

- Statistically-secure key exchange [BB84,...]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]
- Weak 2-party unconditional primitives
  - coin flipping [ATVY,Amb]
  - string commitment [BCHLW]
- Some multi-prover commitments insecure [CST]
- Some "extractors" fail vs quantum memory [IKW]
  - But some are OK [KMR,...]
- Some simulators for ZK proofs fail
  - but new ones can sometimes be built [Watrous]

Some Things That Change

- Statistically-secure key exchange [BB84,...]
- Factoring + DL broken [Shor]
  - And several other number-theory based schemes [Hallgren]
- Weak 2-party unconditional primitives
  - coin flipping [ATVY,Amb]
  - string commitment [BCHLW]
- Some multi-prover commitments insecure [CST]
- Some "extractors" fail vs quantum memory [IKW]
  - But some are OK [KMR,...]
- Some simulators for ZK proofs fail
  - but new ones can sometimes be built [Watrous]
- Bounded Storage Model more Powerful [DFSS]

= incomplete and biased

This talk: Salient Features (a partial* list)

- Multiparty Quantum Computing
  - Parties hold quantum inputs
  - Want to evaluate a quantum circuit
  - Generalizes classical multiparty computing
- Two Feasibility results
  - Statistical MPQC ⇔ cheating minority
    à la [RB'89]
  - Computational MPQC for arbitrary subsets
    à la [GMW'87] under non-standard (false?) assumption

= incomplete and biased

This talk: Salient Features (a partial* list)

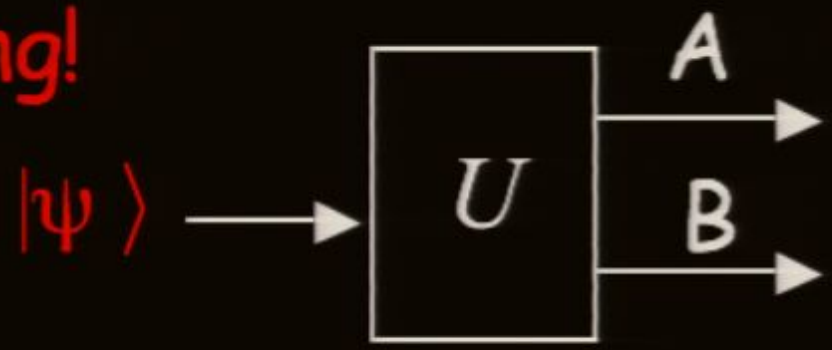
- Multiparty Quantum Computing
  - Parties hold quantum inputs
  - Want to evaluate a quantum circuit
  - Generalizes classical multiparty computing
- Two Feasibility results
  - Statistical MPQC ⇔ cheating minority
    à la [RB'89]
  - Computational MPQC for arbitrary subsets
    à la [GMW'87] under non-standard (false?) assumption
- Along the way:
  - Some infeasibility results
  - Authentication and Approximate Error-Correction
  - ZK Proofs of Knowledge

Common Thread: Information versus Disturbance

- Important principle of quantum mechanics
- Consequence: No cloning!

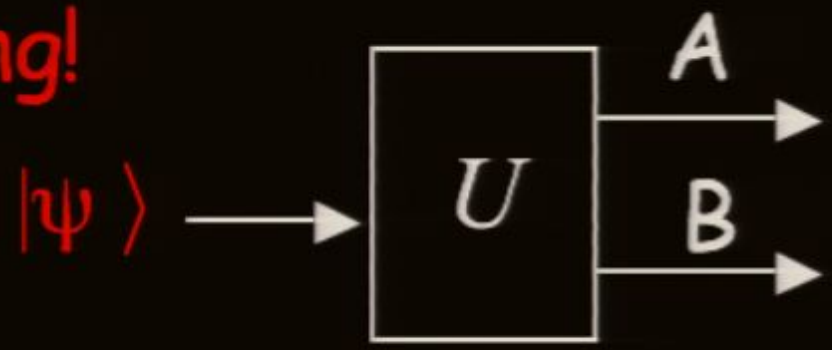
Common Thread: Information versus Disturbance

- Important principle of quantum mechanics
- Consequence: No cloning!



Common Thread: Information versus Disturbance

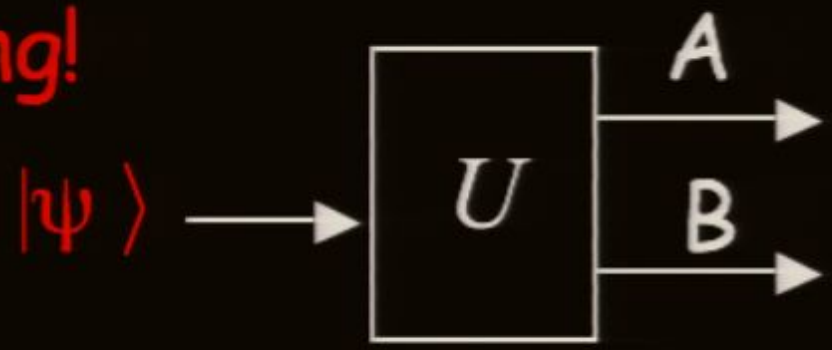
- Important principle of quantum mechanics
- Consequence: No cloning!



- **Theorem:** If $A = |\psi\rangle$ for *all* inputs $|\psi\rangle$ then B is independent of $|\psi\rangle$

Common Thread: Information versus Disturbance

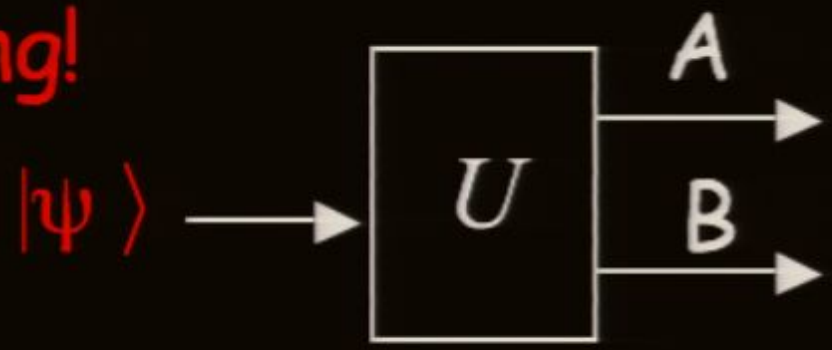
- Important principle of quantum mechanics
- Consequence: No cloning!



- **Theorem:** If $A = |\psi\rangle$ for *all* inputs $|\psi\rangle$
  then B is independent of $|\psi\rangle$
- Information $\Rightarrow$ Disturbance

Common Thread: Information versus Disturbance

- Important principle of quantum mechanics
- Consequence: No cloning!



- **Theorem:** If $A = |\psi\rangle$ for *all* inputs $|\psi\rangle$
  then B is independent of $|\psi\rangle$
- Information $\Rightarrow$ Disturbance

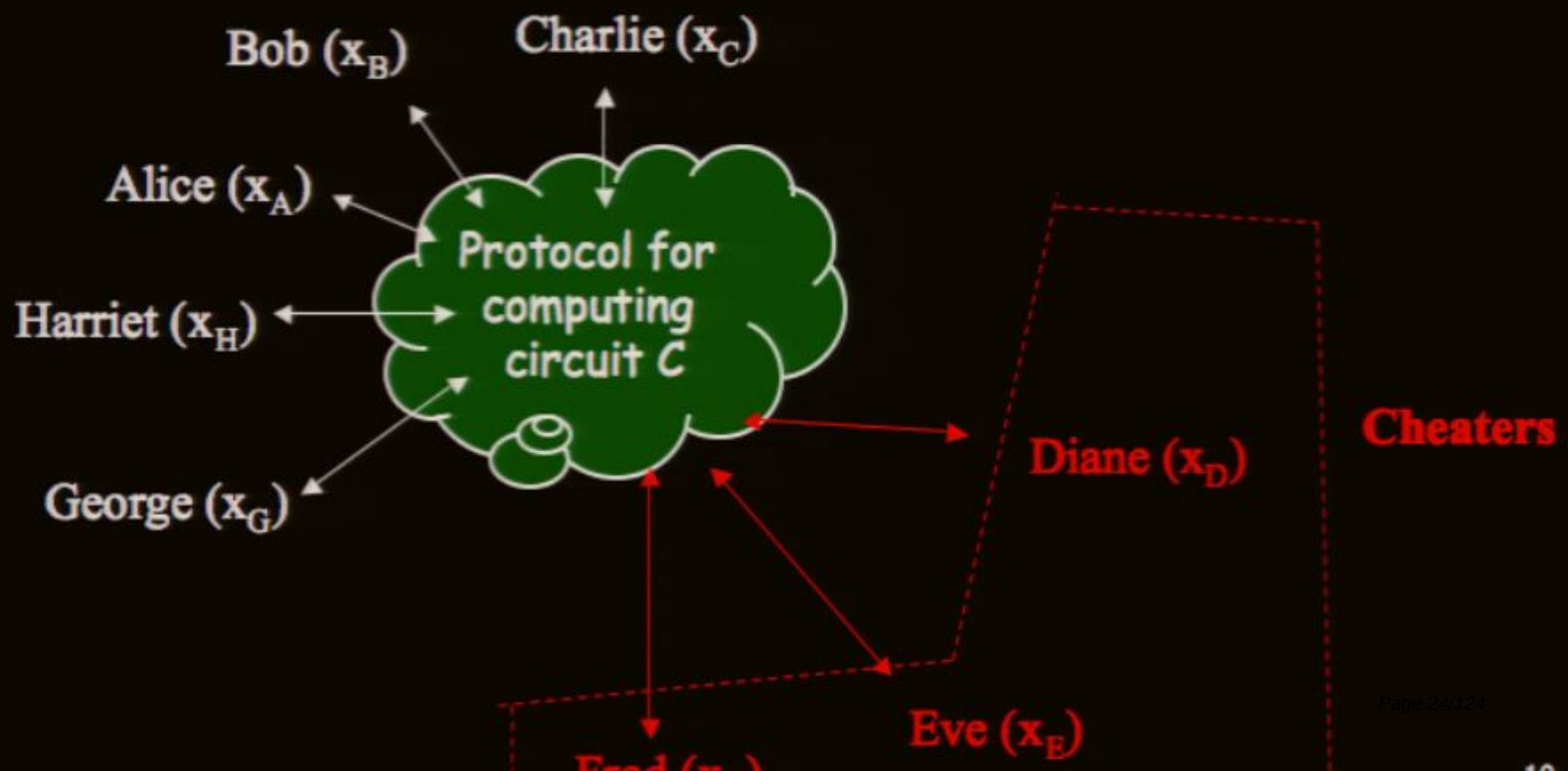
Secrecy	$\Leftarrow$	Resilience to errors

This Talk

- Intro
- Multiparty Quantum Computing
- Codes and Authentication
- MPQC with a cheating minority
- Beyond a faulty minority: 2-party QC
  - Proofs of knowledge for quantum adversaries

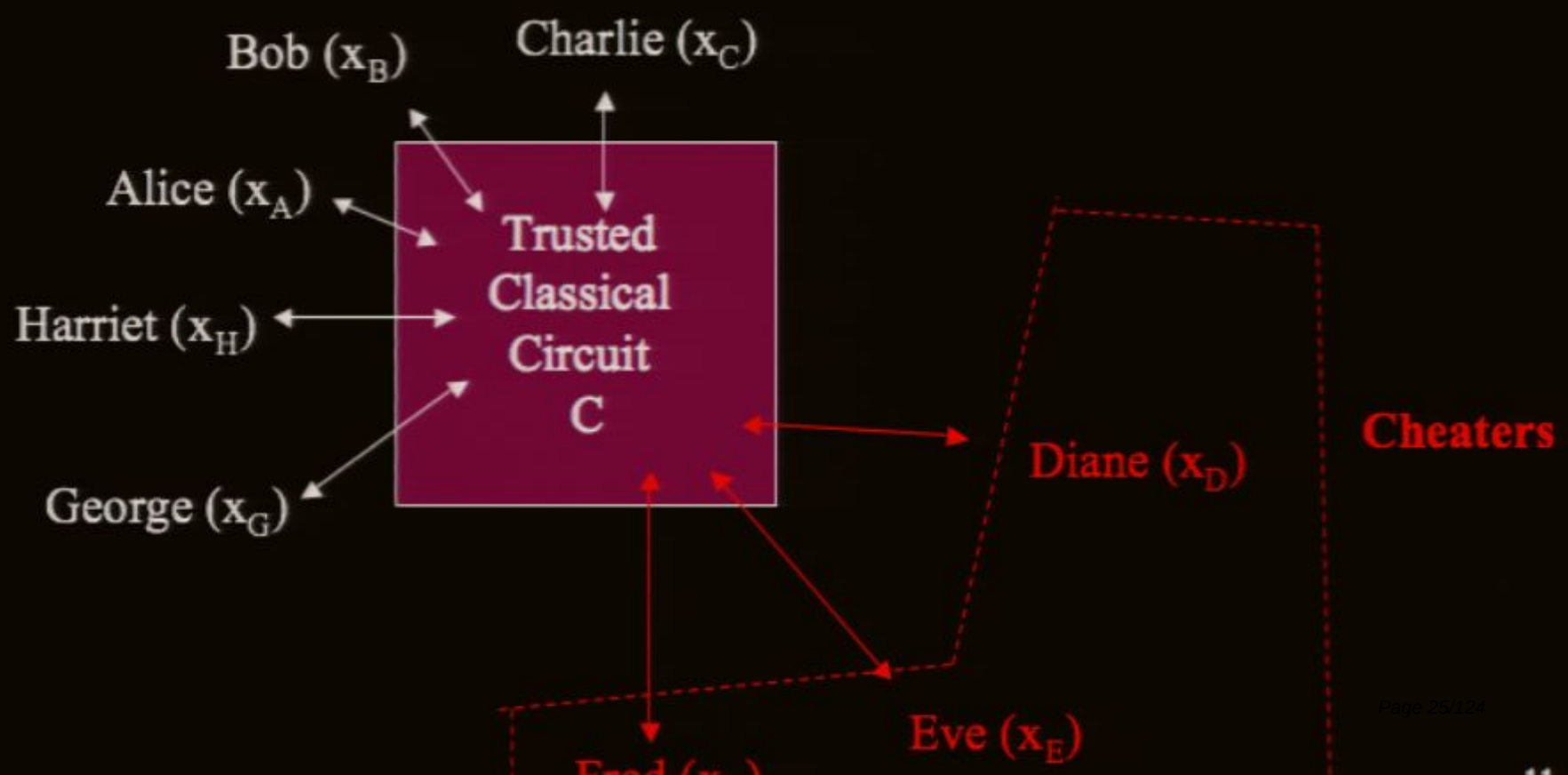
Classical Multiparty Computation (SFE)

- Each party i has input x_i
- Everyone wants to learn output of circuit $C(x_1,\ldots,x_n)$
- Cheaters want to learn more!



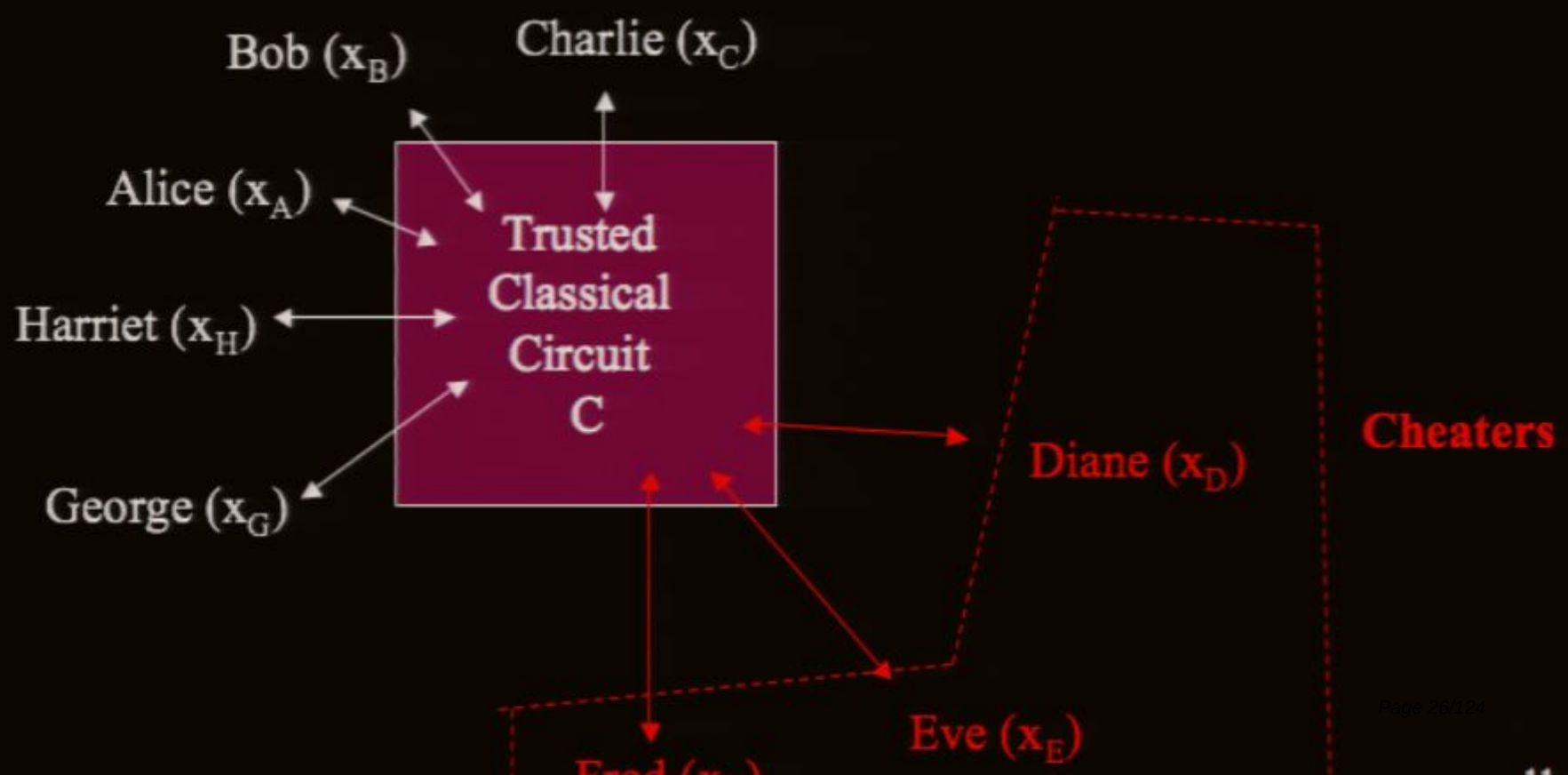
Classical Multiparty Computation (SFE)

- Goal: protocol which simulates trusted party
  - Protocol should behave like the ideal model



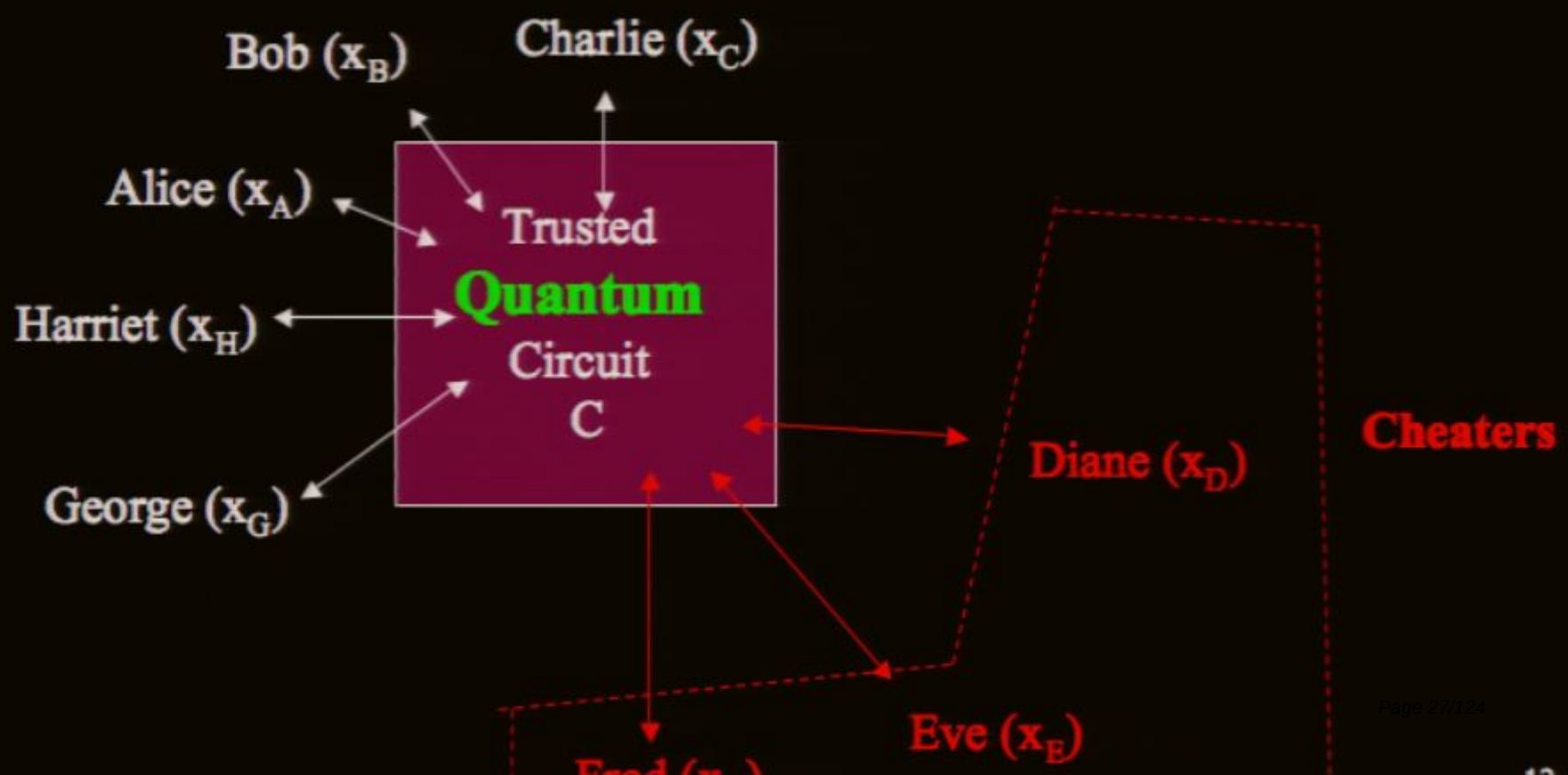
Classical Multiparty Computation (SFE)

- Goal: protocol which simulates trusted party
  - Protocol should behave like the ideal model
- Resource: number of honest players



Quantum Multiparty Computation

- Each player sends quantum input
- Receives quantum output



Quantum Multiparty Computation

- Each player sends quantum input
- Receives quantum output
- Generalizes Classical MPC
- New techniques are needed
  - Players cannot keep copies of their input
  - Rewinding may not be possible
  - Need to operate on encoded / encrypted quantum states

Some Terminology

Some Terminology

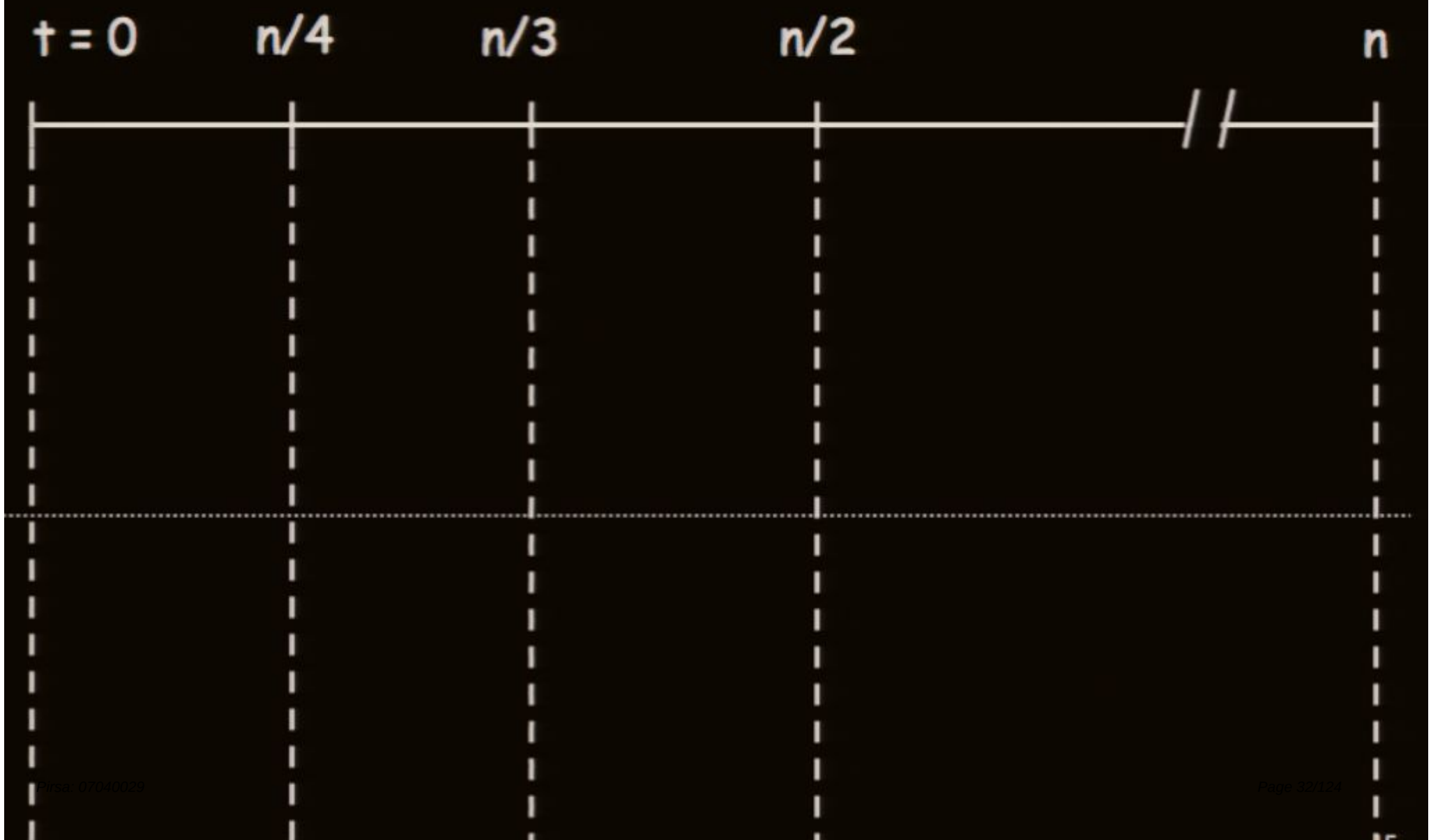
- With Abort?
  - Abort = honest players all stop and output "abort"
  - Sometimes, cheaters can force abort
  - This talk: unfair abort (based on cheaters' output)

Some Terminology

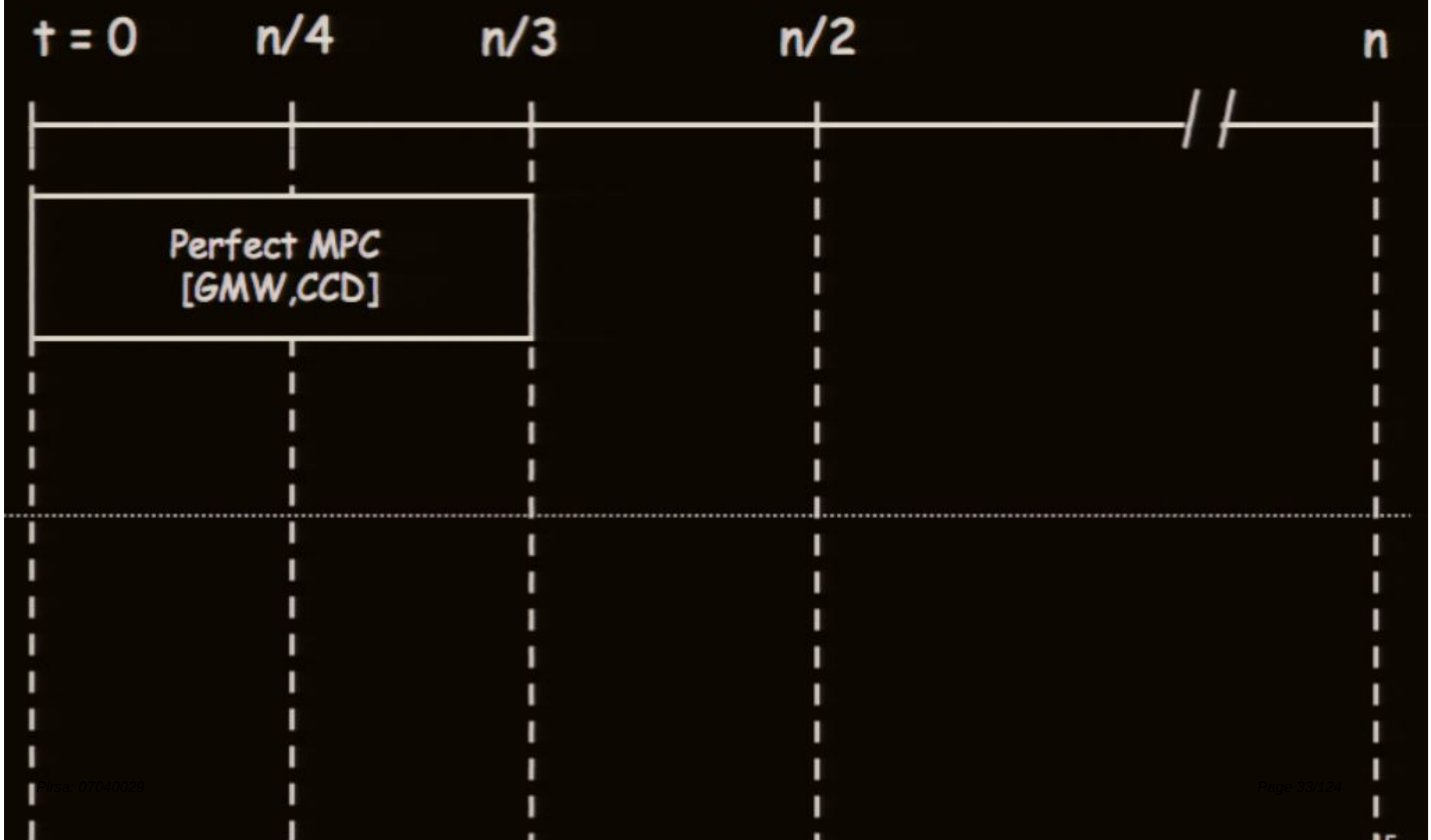
- With Abort?
  - Abort = honest players all stop and output "abort"
  - Sometimes, cheaters can force abort
  - This talk: unfair abort (based on cheaters' output)

- Strengths of security
  - Computational: with overwhelming probability, poly-time adversary learns nothing
  - Statistical: with overwhelming probability, unbounded adversary learns nothing
  - Perfect: with probability 1, unbounded adversary learns nothing

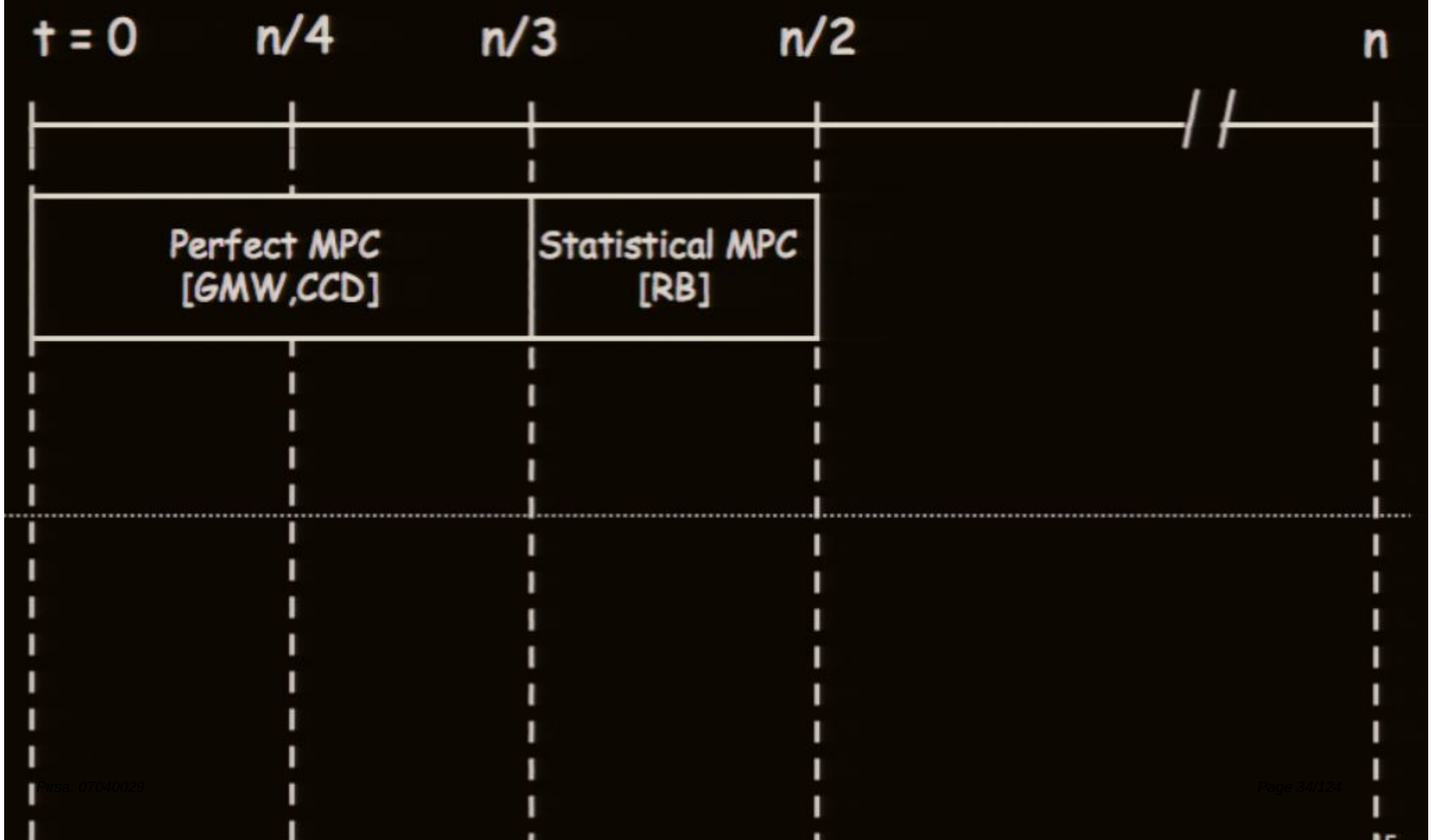
Basic Feasibility Results (assuming broadcast)



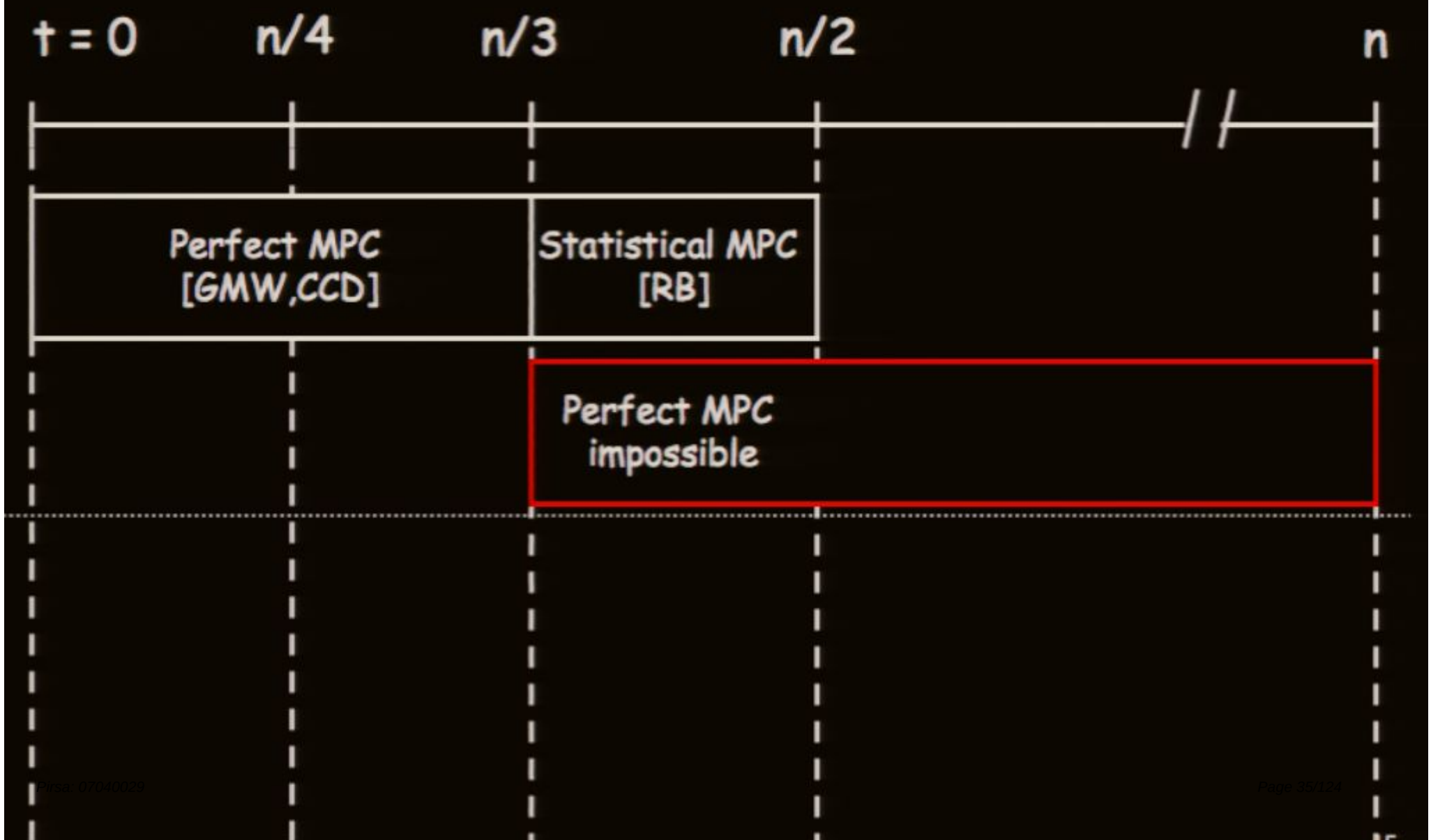
Basic Feasibility Results (assuming broadcast)



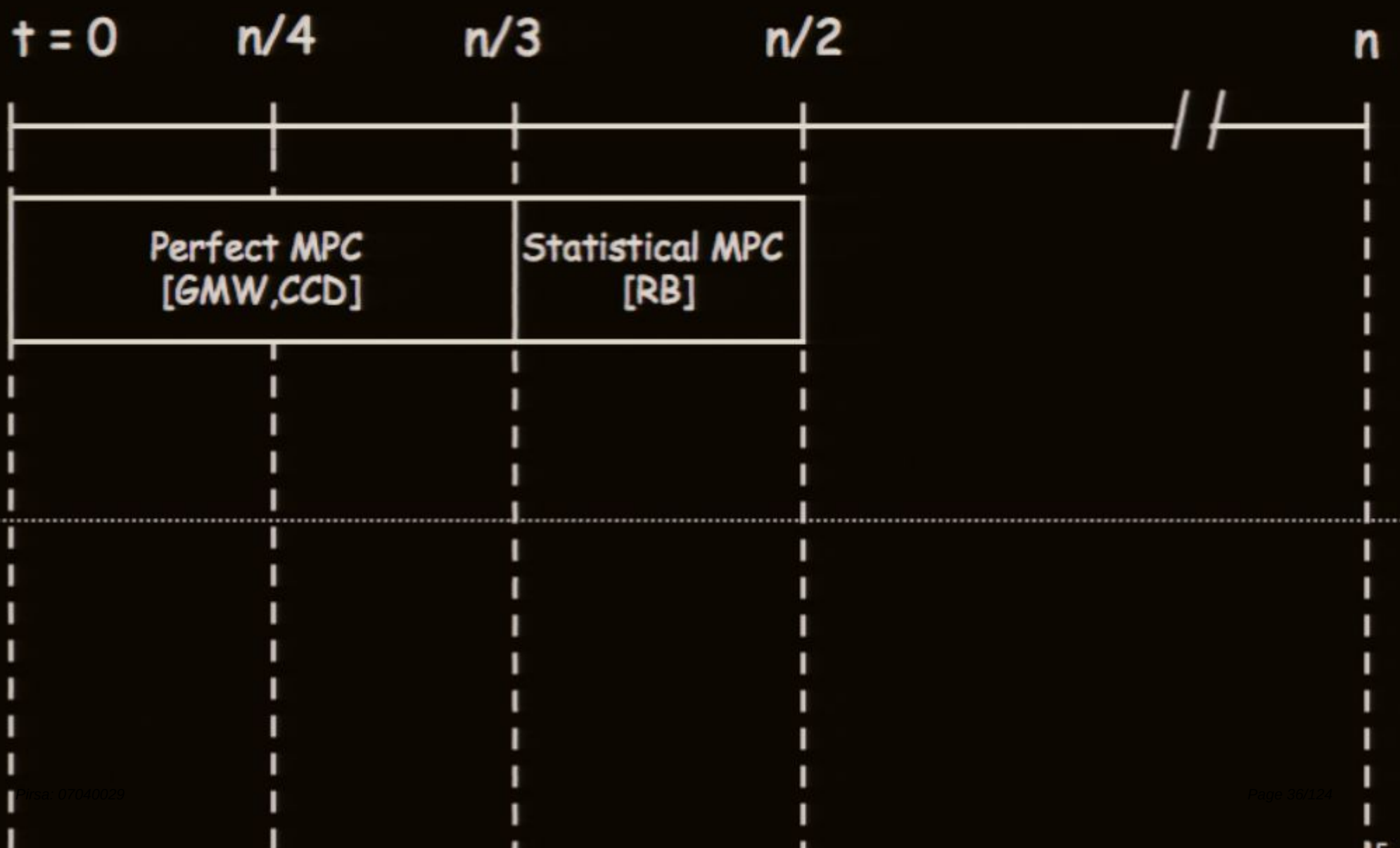
Basic Feasibility Results (assuming broadcast)



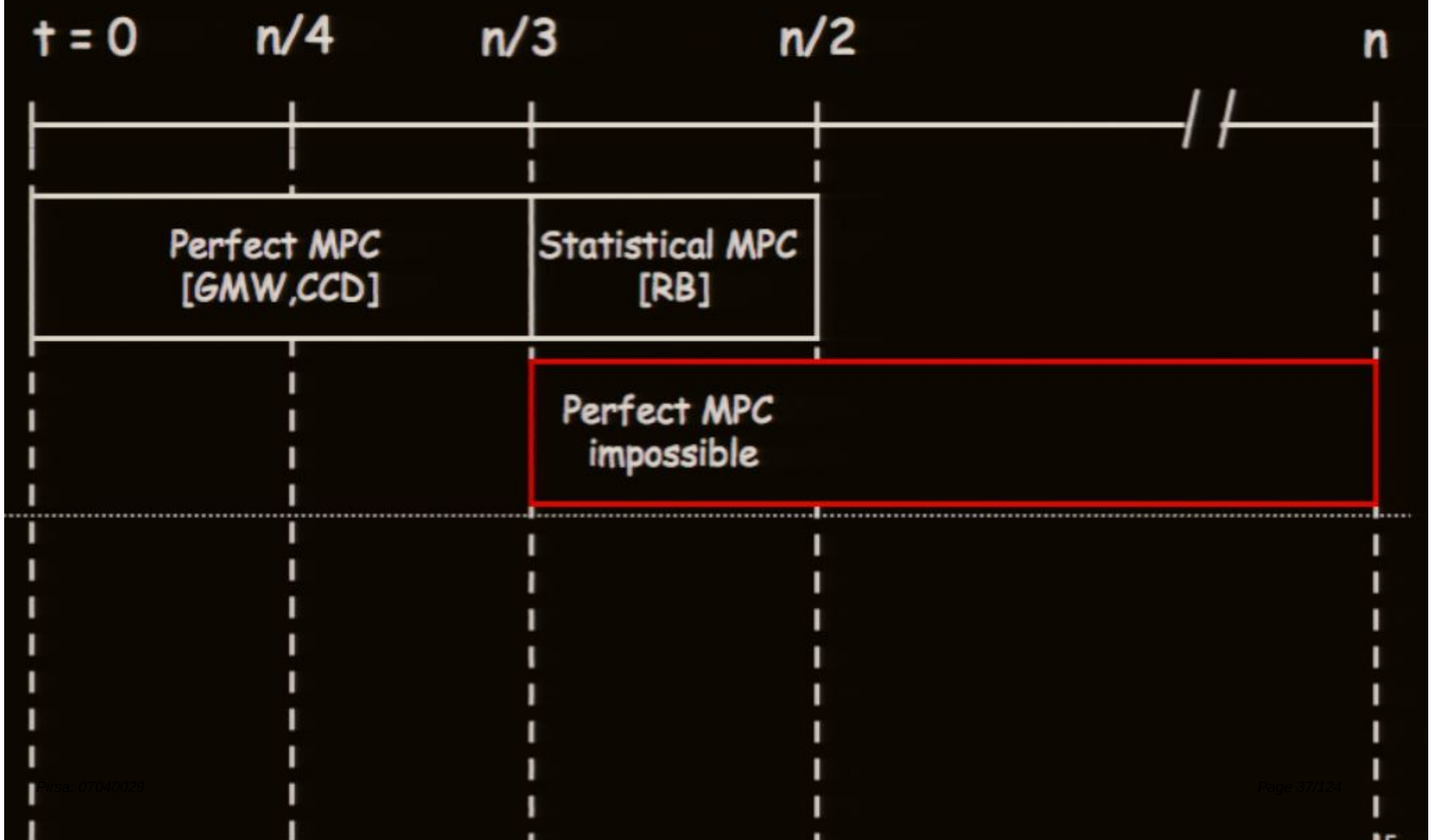
Basic Feasibility Results (assuming broadcast)



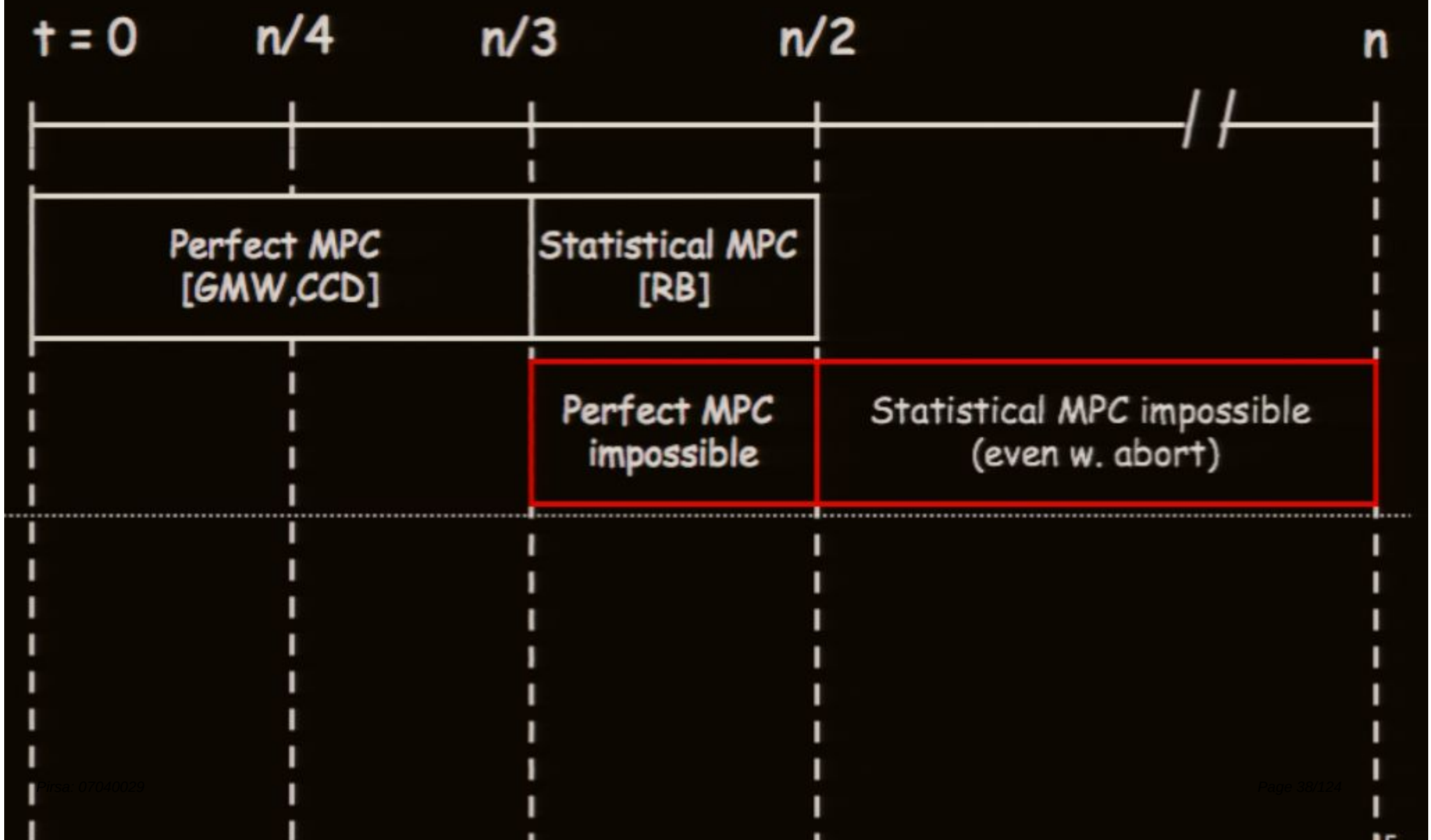
Basic Feasibility Results (assuming broadcast)



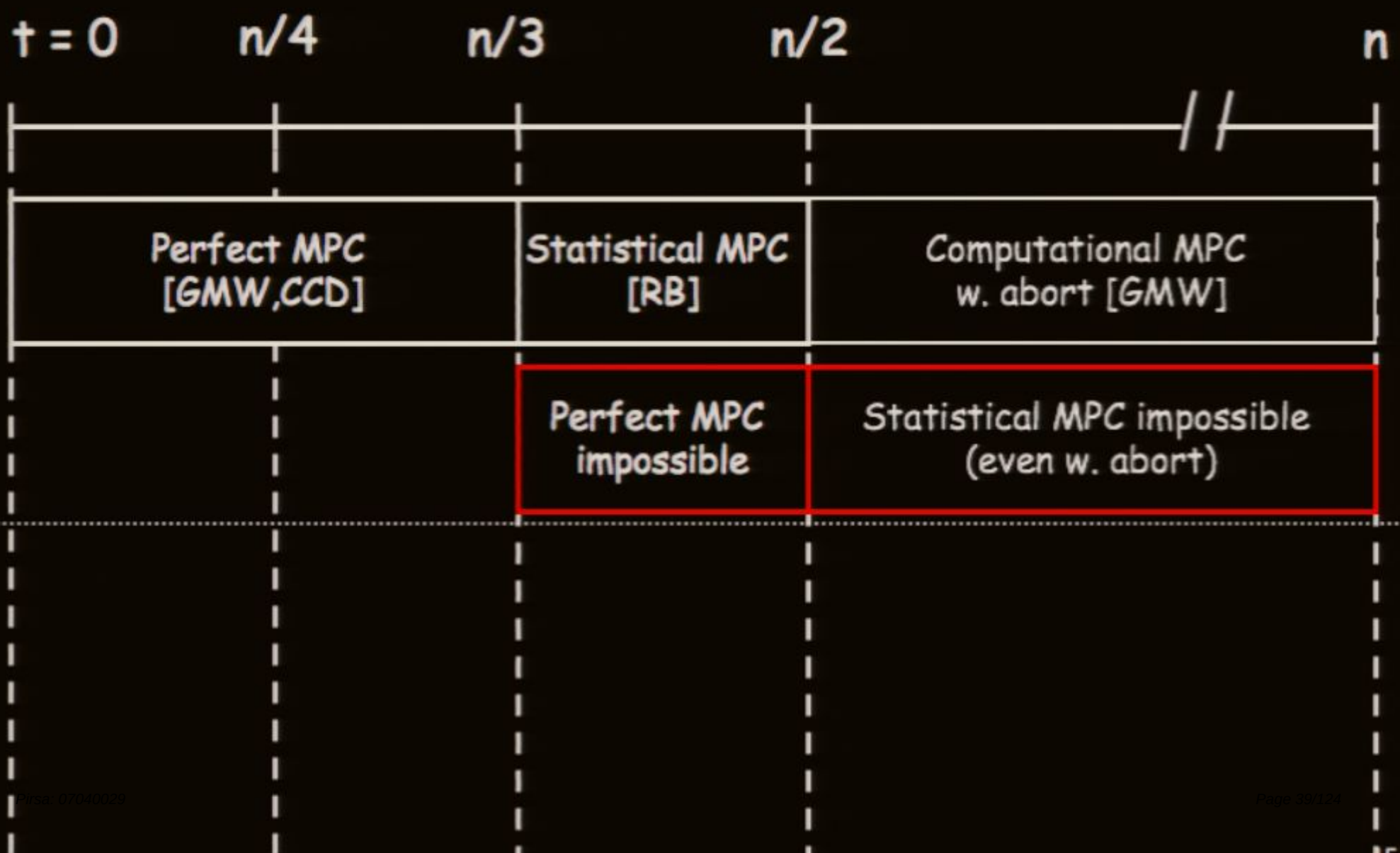
Basic Feasibility Results (assuming broadcast)



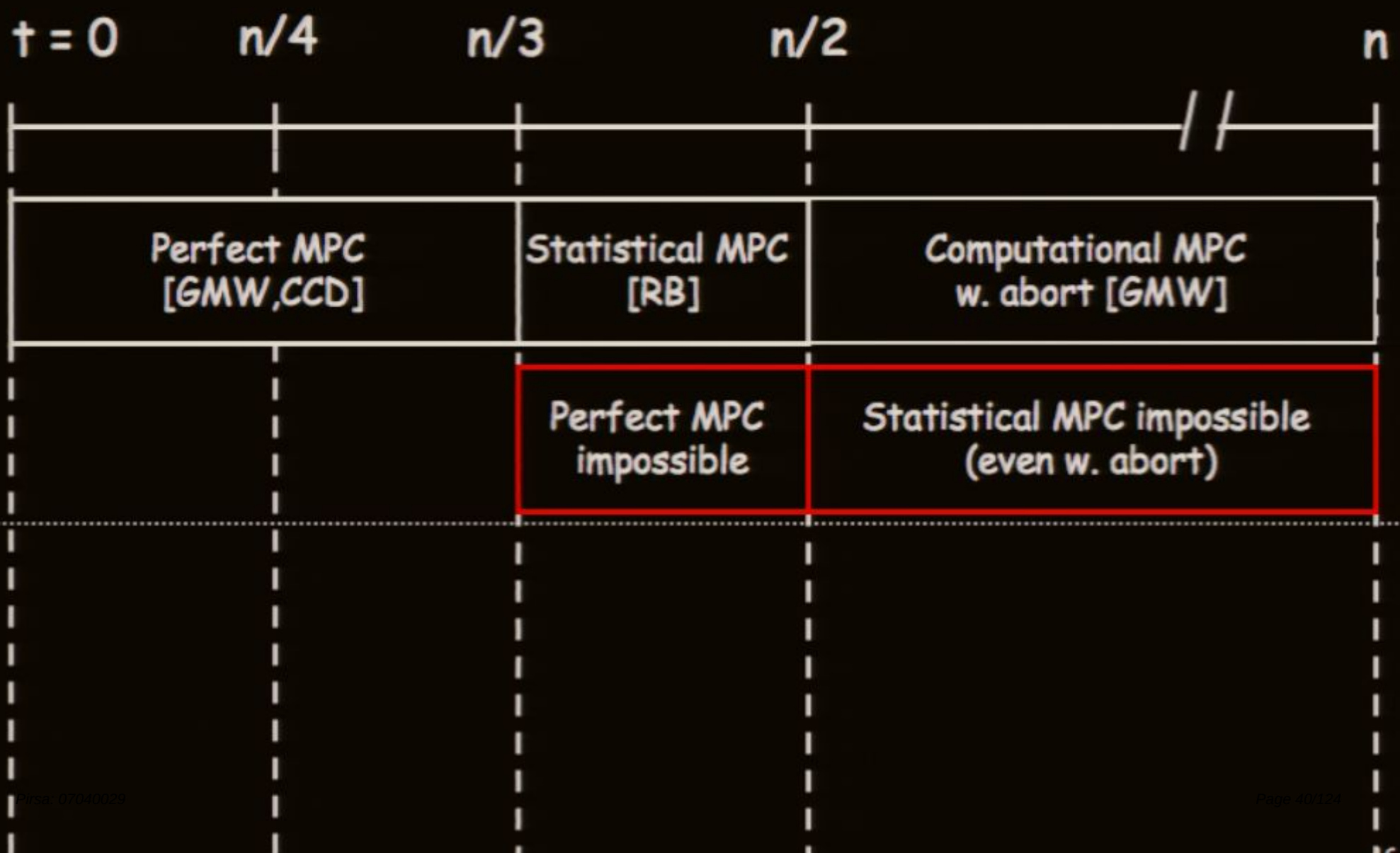
Basic Feasibility Results (assuming broadcast)



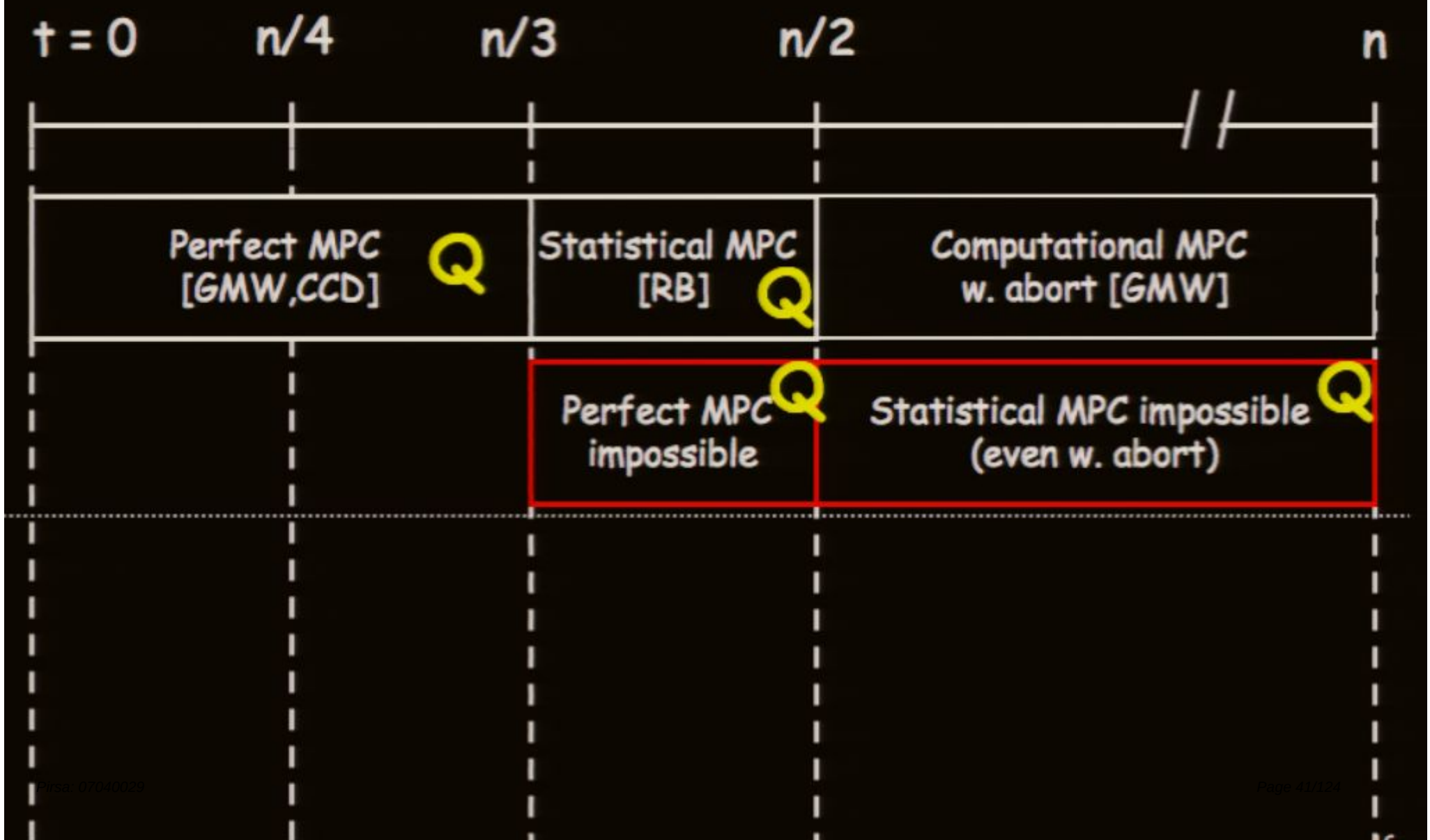
Basic Feasibility Results (assuming broadcast)



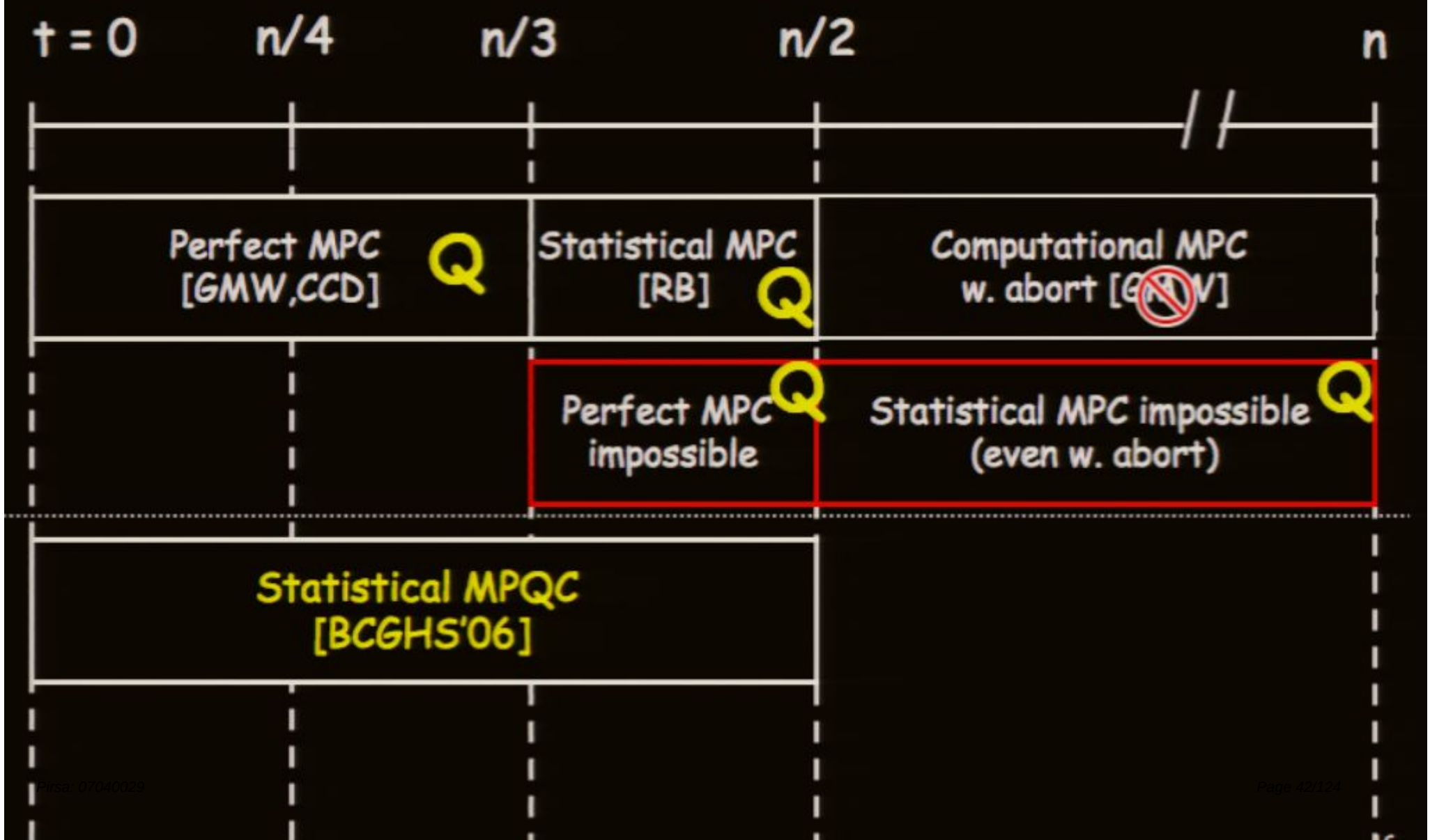
Basic Feasibility Results (assuming broadcast)



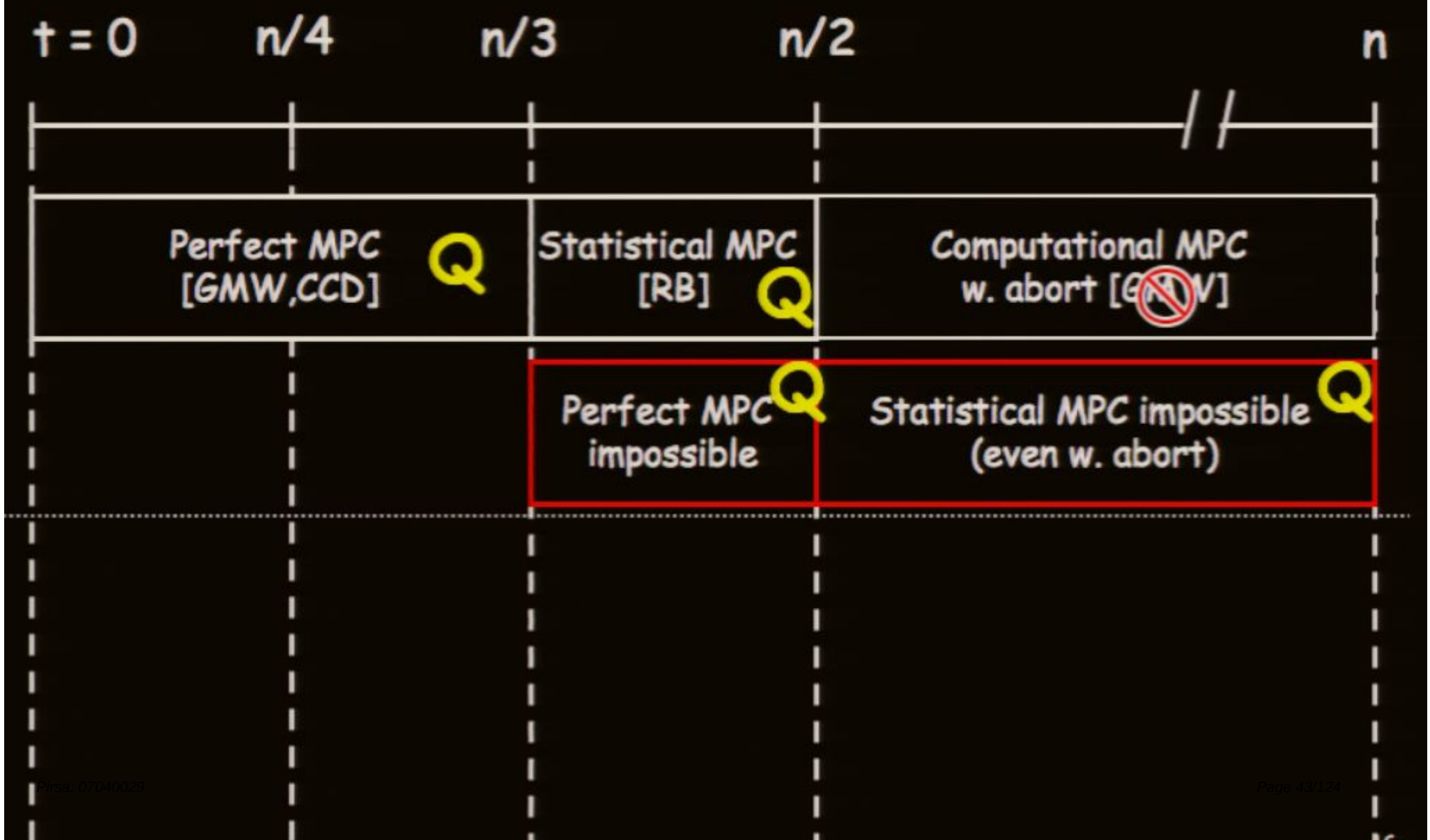
Basic Feasibility Results (assuming broadcast)



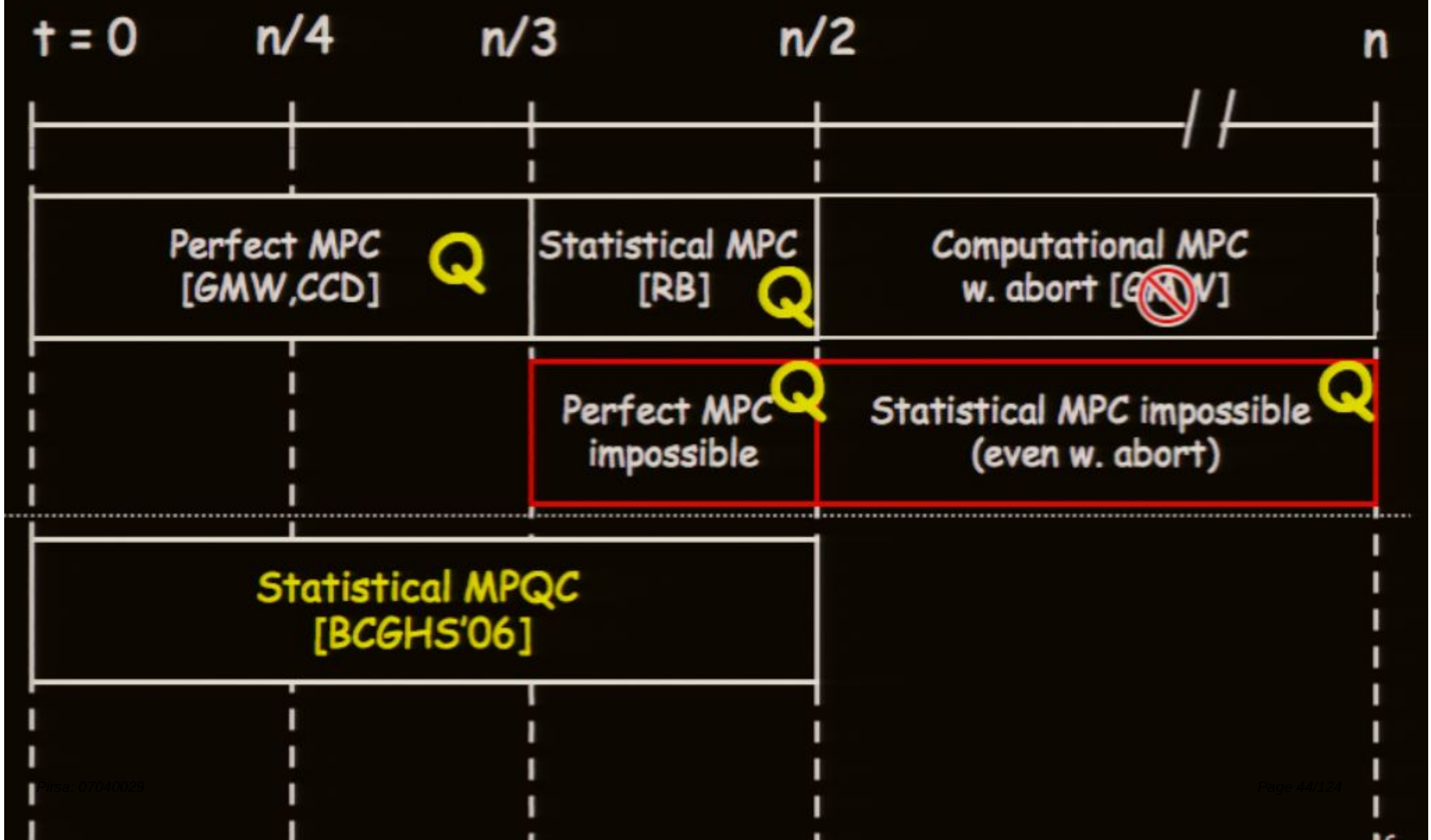
Basic Feasibility Results (assuming broadcast)



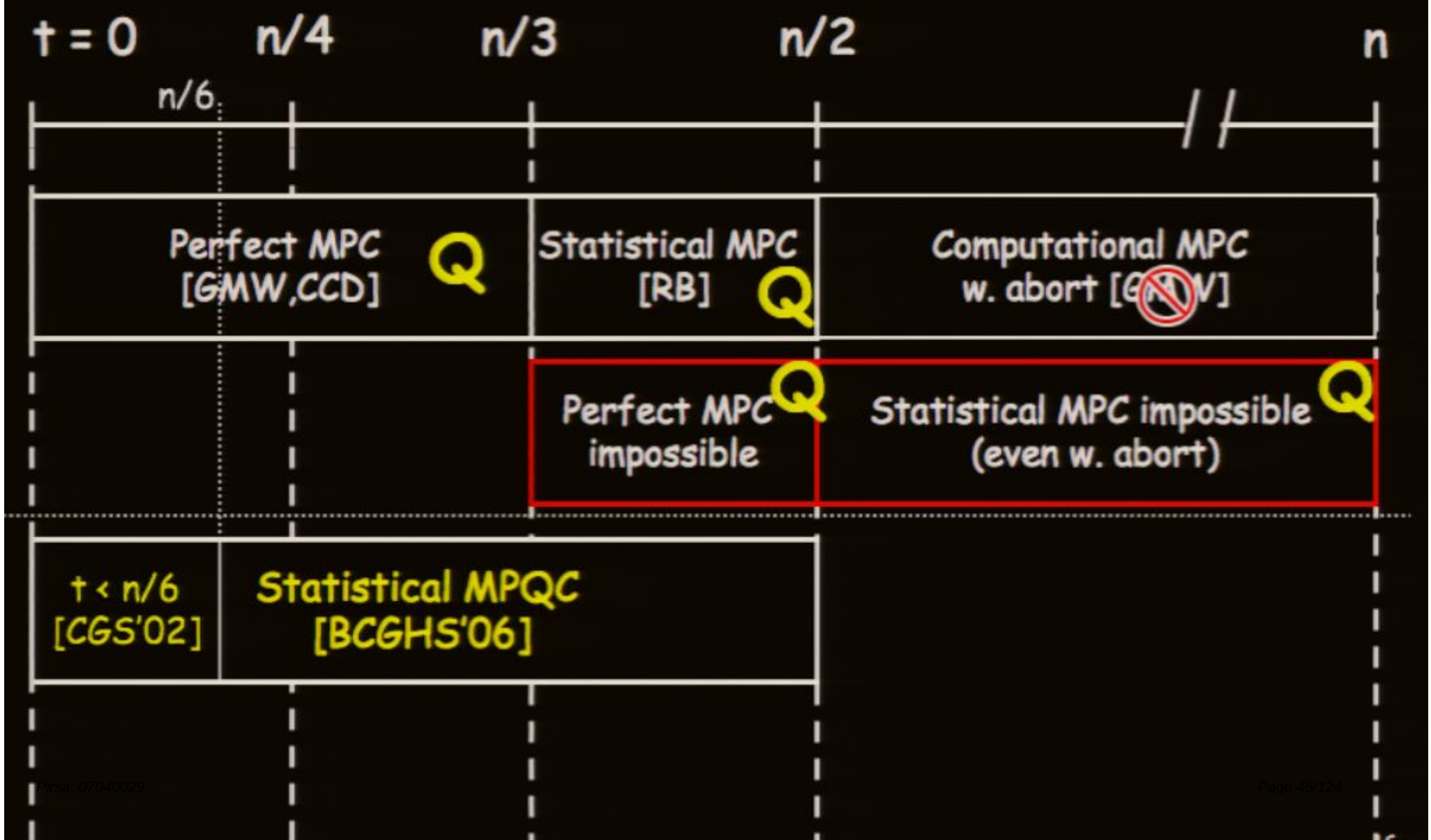
Basic Feasibility Results (assuming broadcast)



Basic Feasibility Results (assuming broadcast)

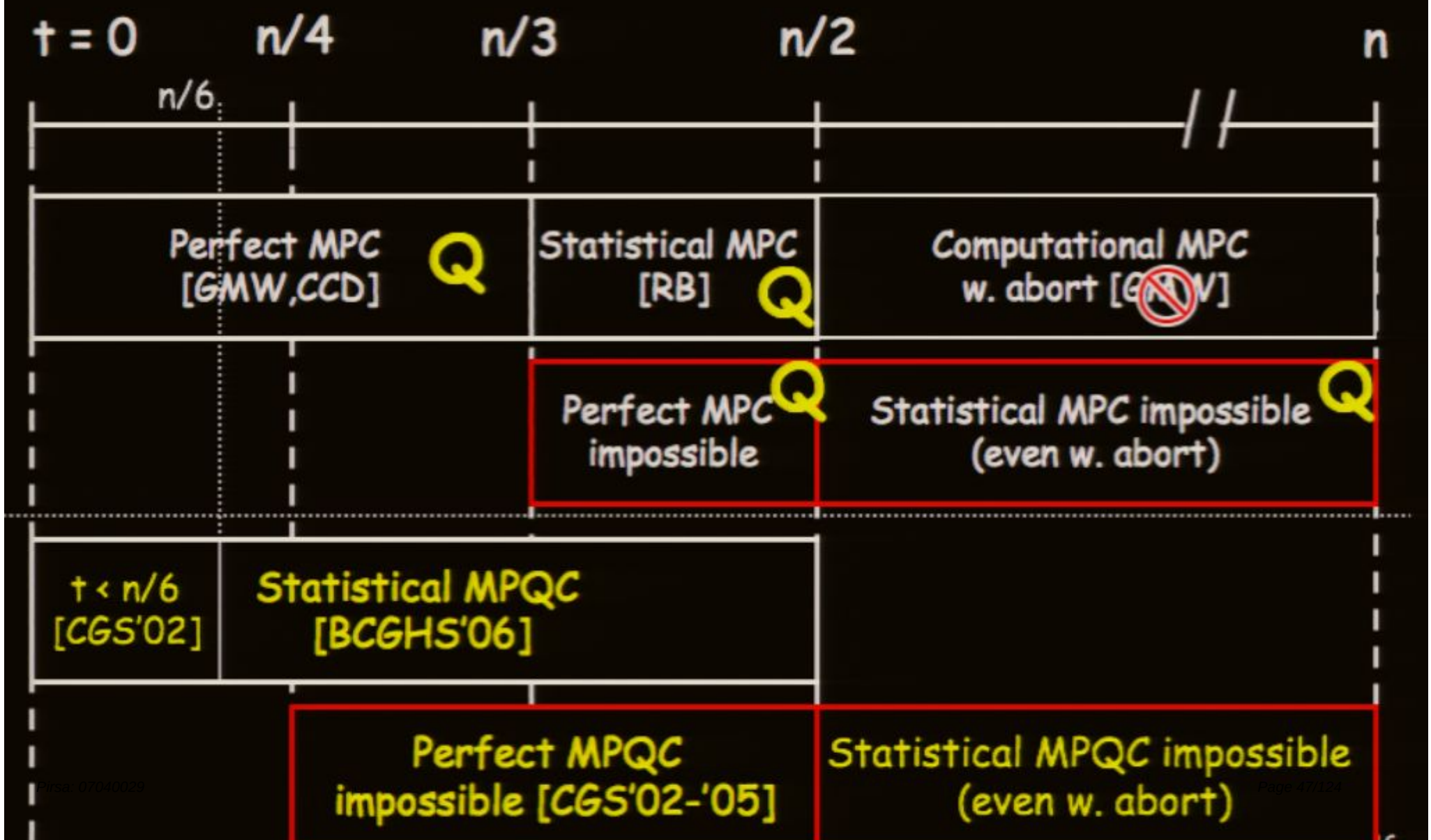


Basic Feasibility Results (assuming broadcast)

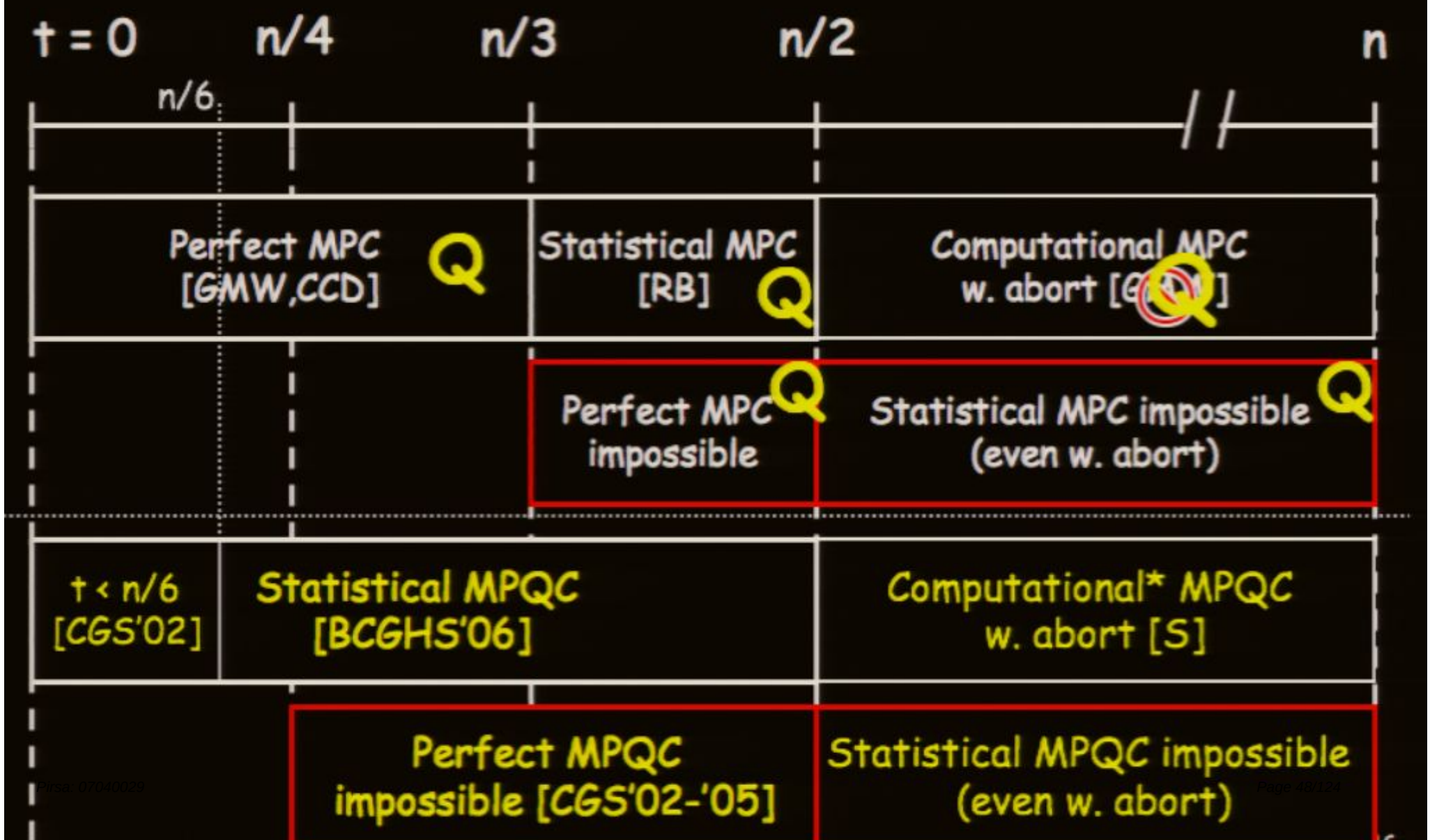


Basic Feasibility Results (assuming broadcast)

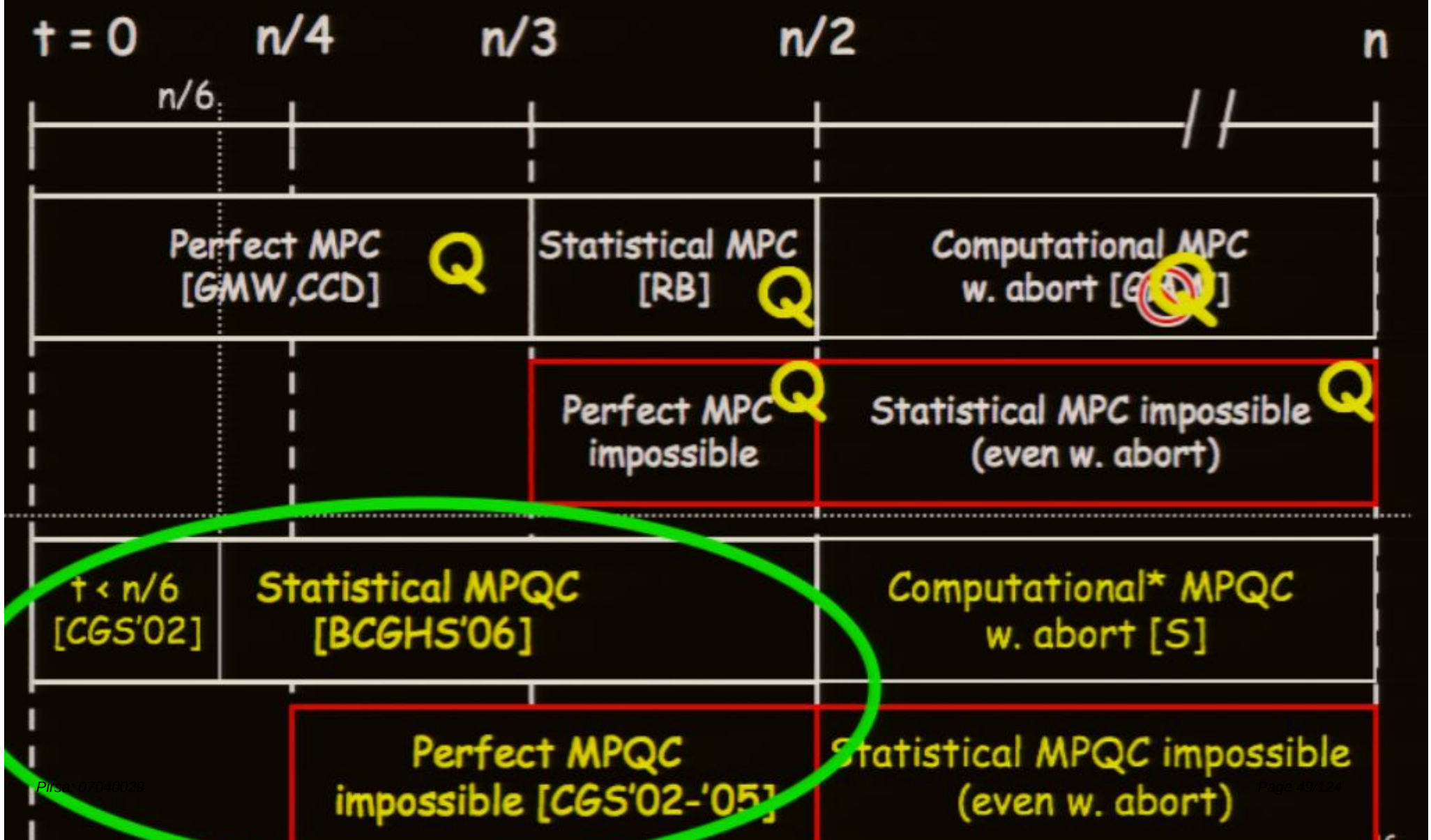
Basic Feasibility Results (assuming broadcast)



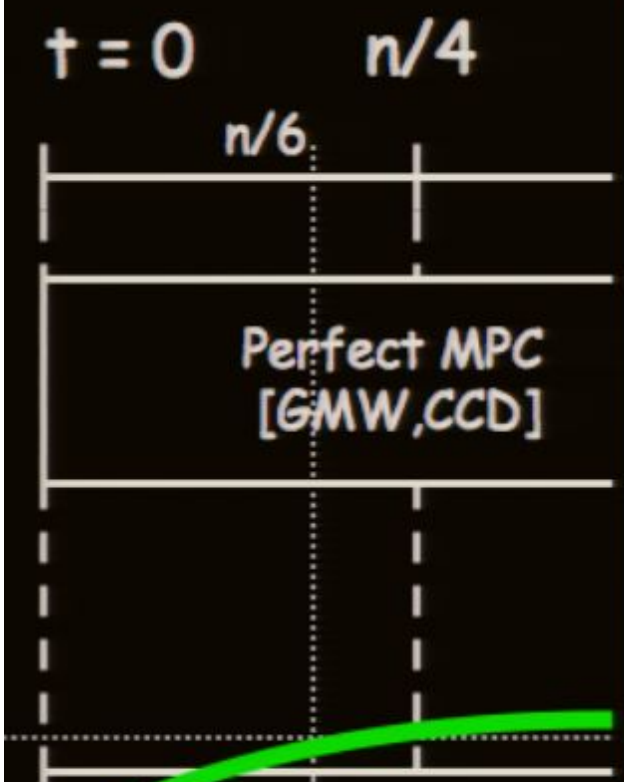
Basic Feasibility Results (assuming broadcast)



Basic Feasibility Results (assuming broadcast)



Basic Feasibility Results (assuming broadcast)



- [CGS'02]: use error-correcting codes and fault-tolerant circuits [AB]
  - 2nd real proof of quantum security?
- Barrier at n/4 : quantum codes [KL]
- Authentication codes [BCGST '02] give
  - approximate codes [CGS '05]
  - reduction to computation on keys

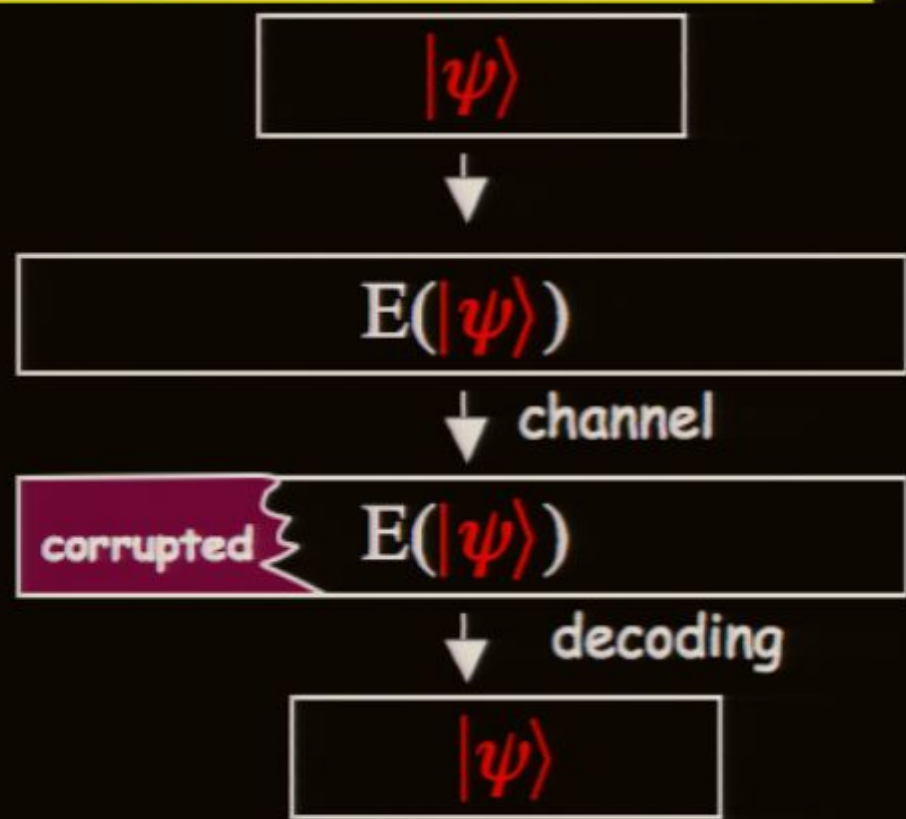
t < n/6 [CGS'02]	Statistical MPQC [BCGHS'06]	Computational* MPQC w. abort [S]
	Perfect MPQC impossible [CGS'02-'05]	Statistical MPQC impossible (even w. abort)

This Talk

- Intro
- Multiparty Quantum Computing
- Codes and Authentication
  - Quantum error-correcting codes
  - A spurious lower bound
  - Authentication
  - Approximate Codes and Secret Sharing
- MPQC with a cheating minority
- Beyond a faulty minority: 2-party QC
  - Proofs of knowledge for quantum adversaries

Error Correcting Codes

- Map k qubits → n qubits
  - introduce redundancy
- If few qubits corrupted or erased, decoder recovers input exactly
- Tricky because of no cloning
  - repetition code doesn't work
- Good codes exist [CSS]
  Over large alphabet [AB99]:
  - Correct (n-1)/4 errors
    or (n-1)/2 erasures

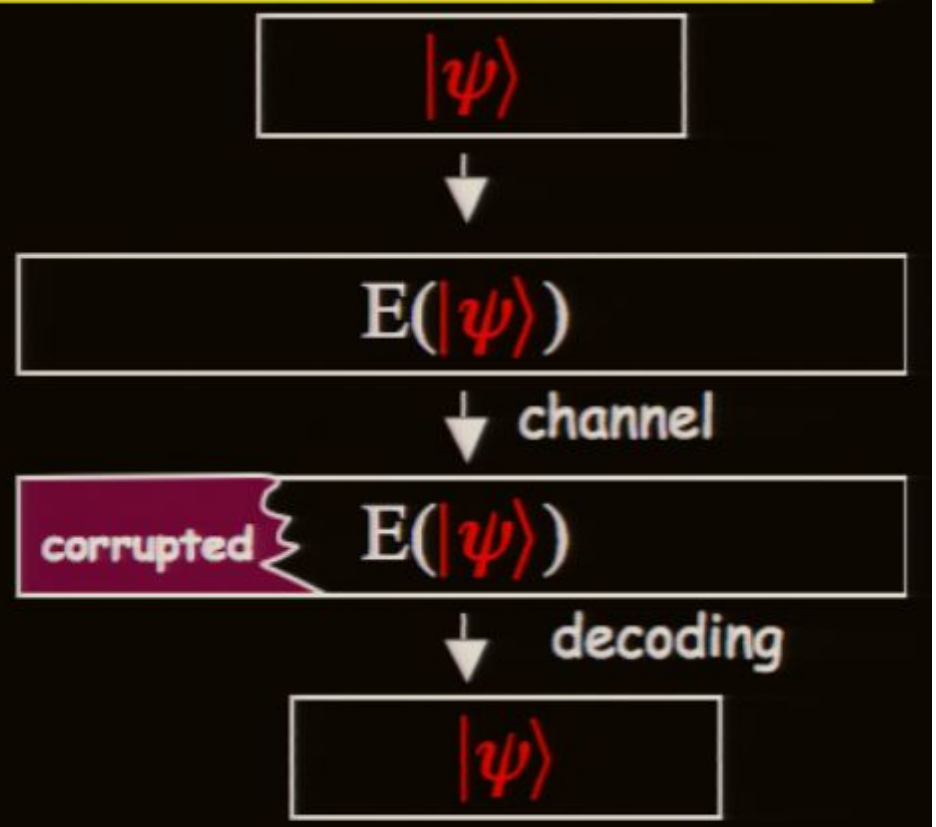


Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct $2t+1$ erasures

Error Correcting Codes

- Map k qubits → n qubits
  - introduce redundancy
- If few qubits corrupted or erased, decoder recovers input exactly
- Tricky because of no cloning
  - repetition code doesn't work
- Good codes exist [CSS]
  Over large alphabet [AB99]:
  - Correct (n-1)/4 errors
    or (n-1)/2 erasures

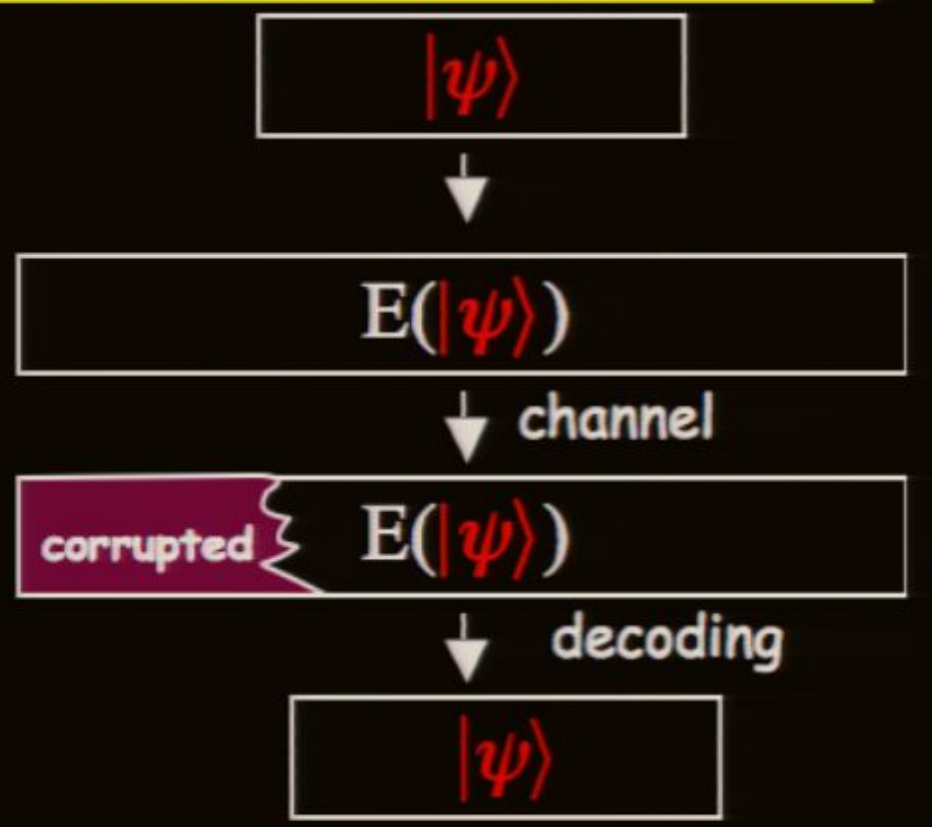


Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct $2t+1$ erasures

Error Correcting Codes

- Map k qubits → n qubits
  - introduce redundancy
- If few qubits corrupted or erased, decoder recovers input exactly
- Tricky because of no cloning
  - repetition code doesn't work
- Good codes exist [CSS]
  Over large alphabet [AB99]:
  - Correct (n-1)/4 errors
    or (n-1)/2 erasures

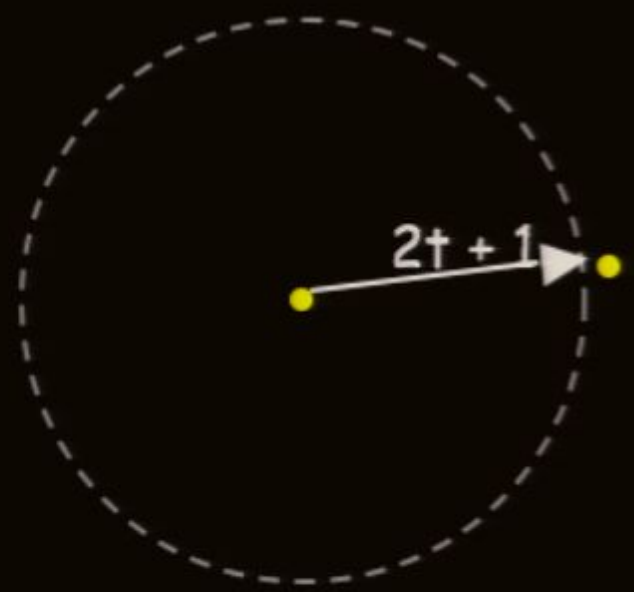


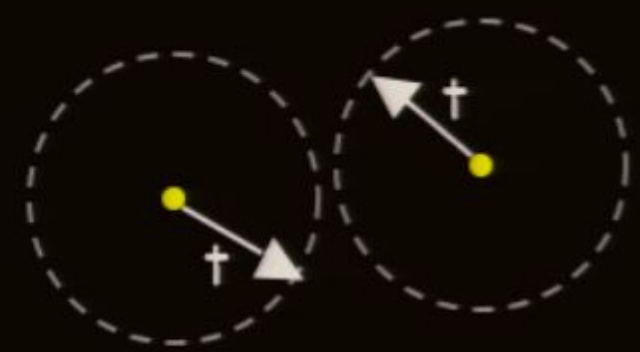
Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct $2t+1$ erasures

Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct $2t+1$ erasures





Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct $2t+1$ erasures

Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors $\Leftrightarrow$ correct 2t+1 erasures

- Quantum codes cannot
  correct n/2 erasures

Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors ⇔ correct 2t+1 erasures

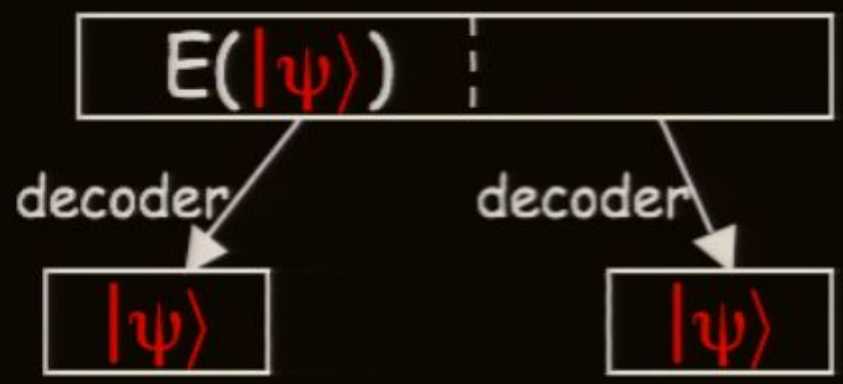
- Quantum codes cannot correct n/2 erasures

$E(|\psi\rangle)$

Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors ⇔ correct 2t+1 erasures

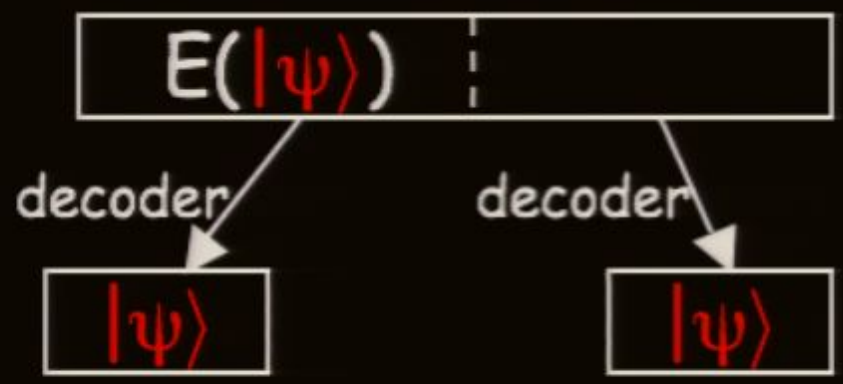
- Quantum codes cannot correct n/2 erasures



Quantum codes cannot correct n/4 errors

- As in the classical case:
  correct t errors ⇔ correct 2t+1 erasures

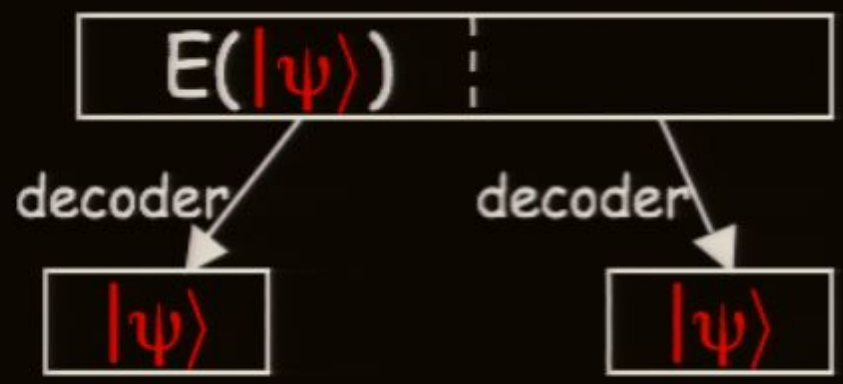
- Quantum codes cannot correct n/2 erasures
  - No cloning ~~Dolly~~



Quantum codes cannot correct n/4 errors

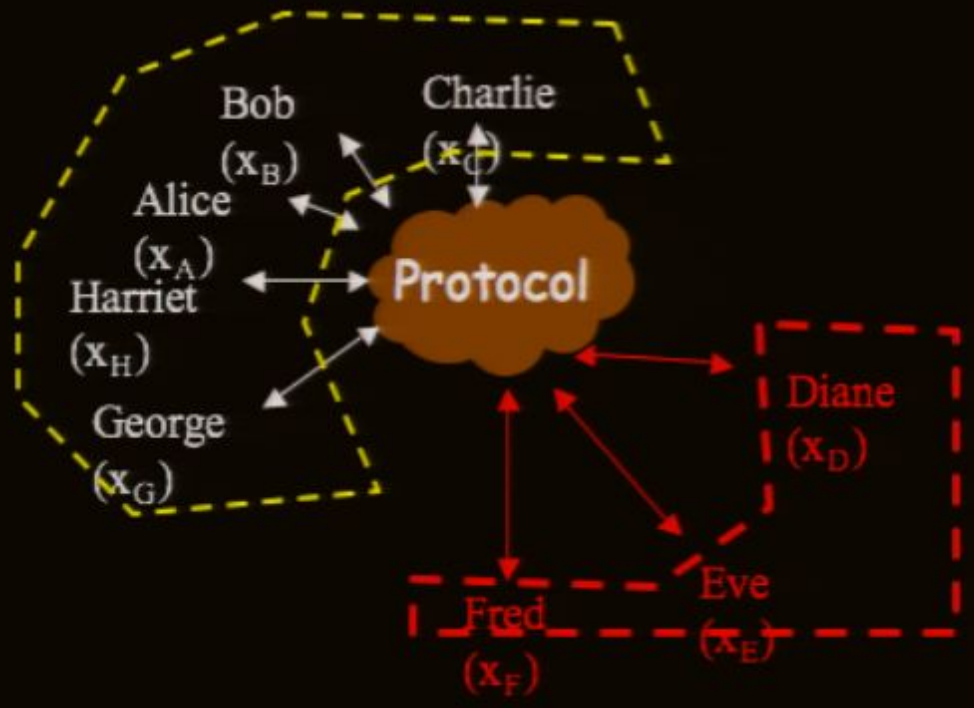
- As in the classical case:
  correct t errors ⇔ correct 2t+1 erasures

- Quantum codes cannot correct n/2 erasures
  - No cloning ~~Dolly~~



⇒ Quantum codes cannot correct n/4 errors
(not true of classical codes – repetition)

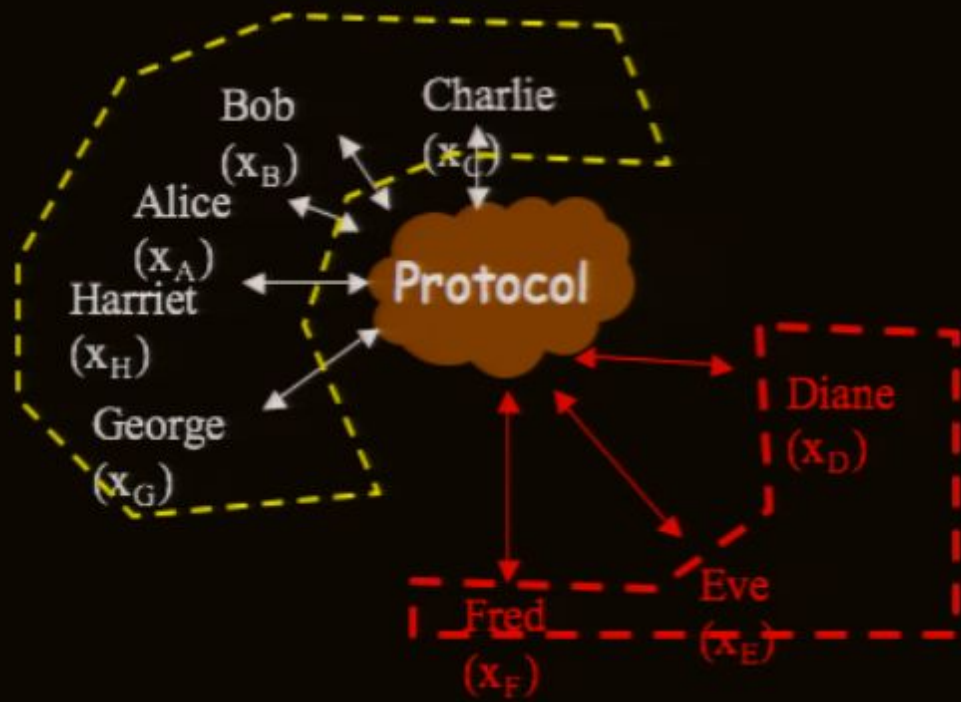
A spurious lower bound



A spurious lower bound

Lemma: Every MPQC protocol tolerating t cheaters implies existence of a code correcting t errors with high fidelity

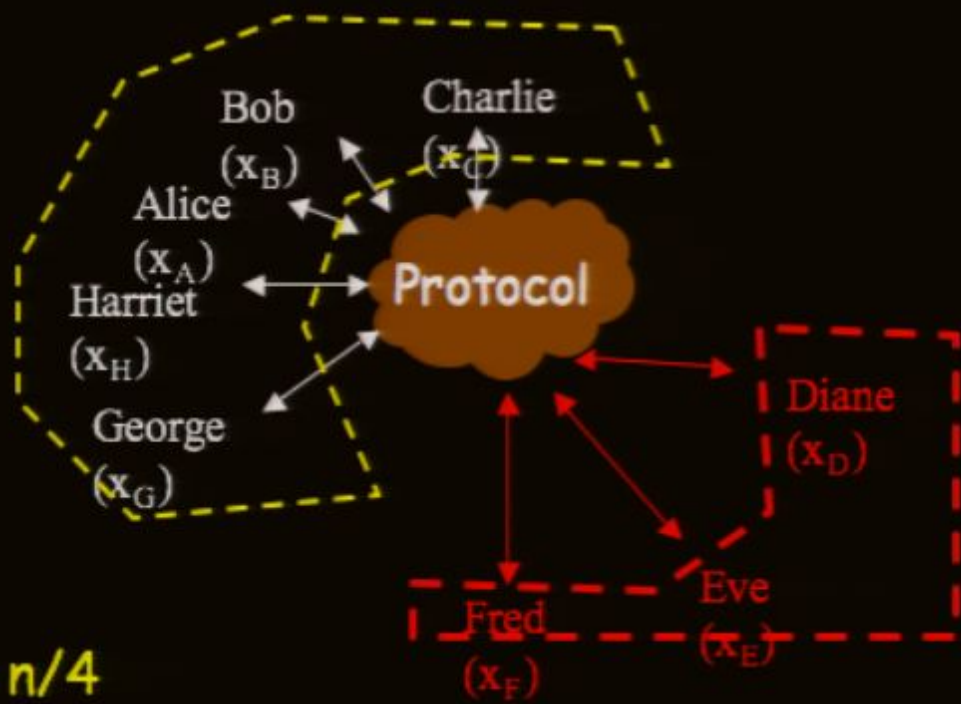
- Honest players should be able to reconstruct output



A spurious lower bound

Lemma: Every MPQC protocol tolerating t cheaters implies existence of a code correcting t errors with high fidelity

- Honest players should be able to reconstruct output

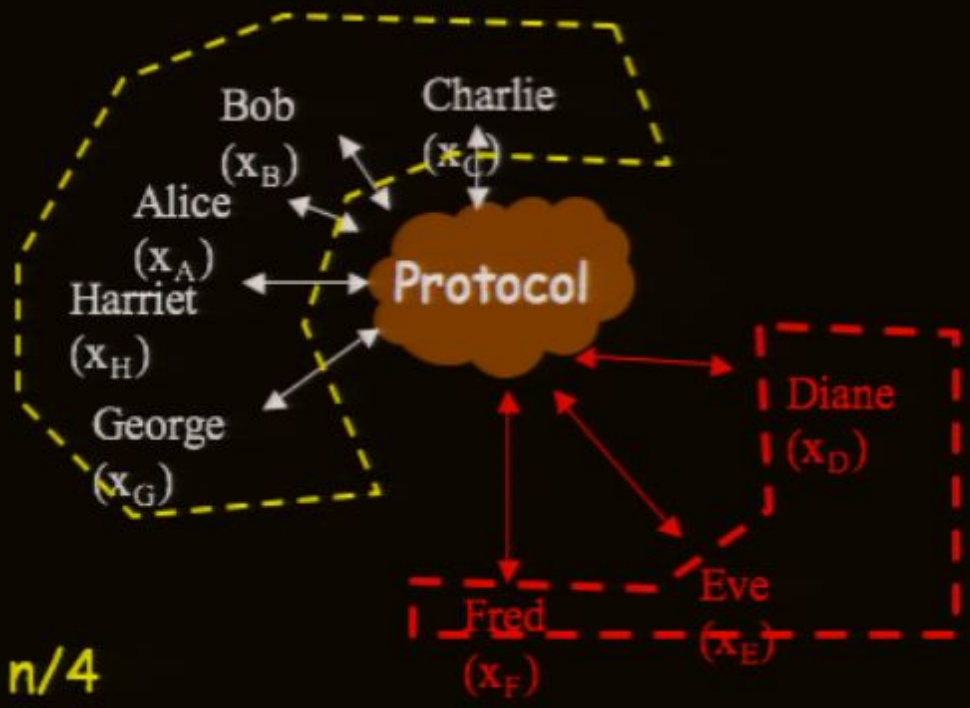


- [CGS'02] MPQC is impossible for t< n/4

A spurious lower bound

Lemma: Every MPQC protocol tolerating t cheaters implies existence of a code correcting t errors with high fidelity

- Honest players should be able to reconstruct output



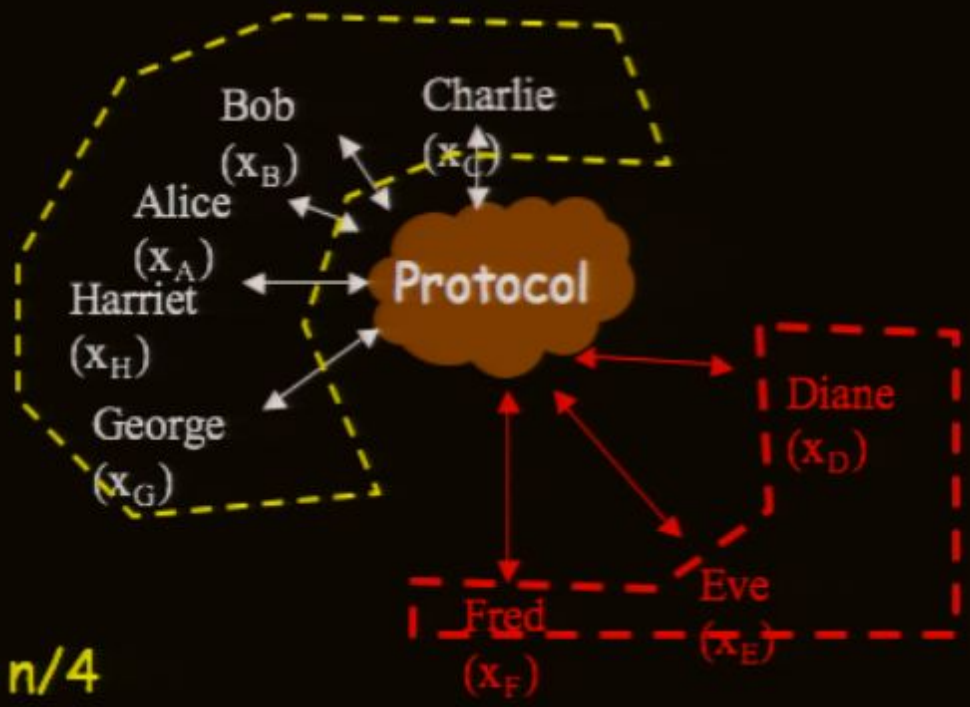
- [CGS'02] MPQC is impossible for t< n/4

Perfect
[CGS'05]

A spurious lower bound

Lemma: Every MPQC protocol tolerating t cheaters implies existence of a code correcting t errors with high fidelity

- Honest players should be able to reconstruct output



- [CGS'02] MPQC is impossible for t< n/4

Perfect
[CGS'05]

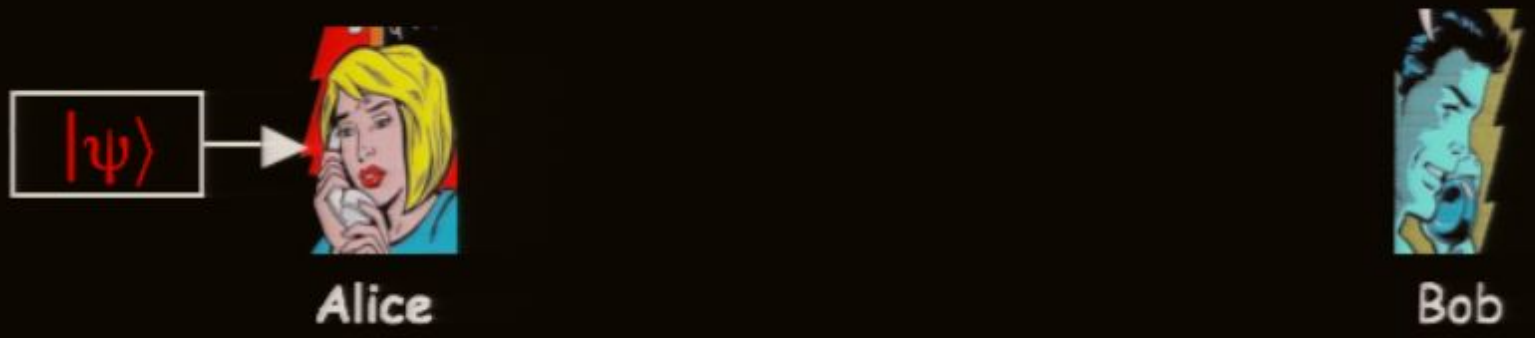
- How do we get around this?
  - Authenticating Quantum States [BCGST]
  - Approximate QECC break n/4 bound
  - Connection to secret sharing

Authenticating Quantum Messages [BCGST]

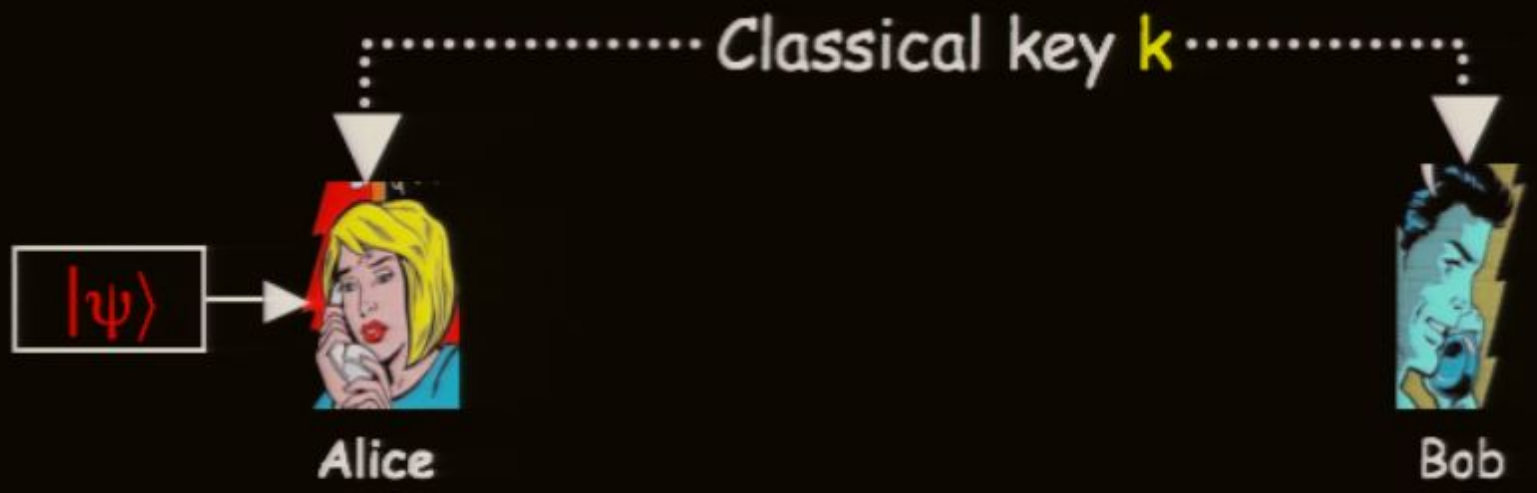
Authenticating Quantum Messages [BCGST]

- How does Alice know it's Bob?
  - classical MACs
- What if he needs to send her qubits?

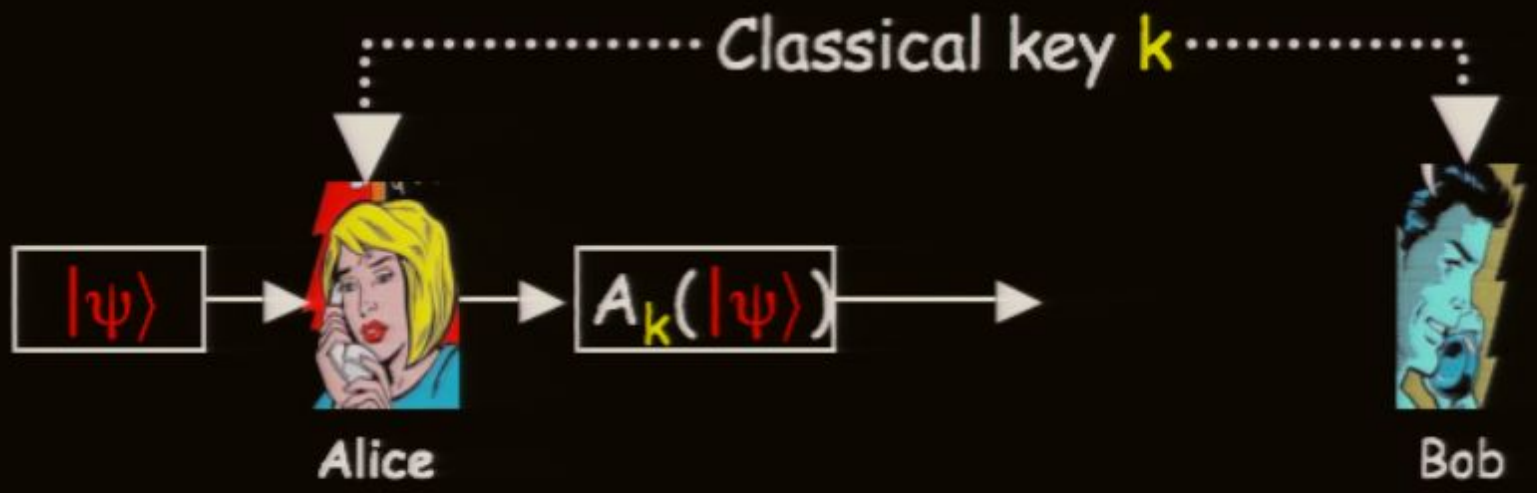
Authenticating Quantum Messages [BCGST]



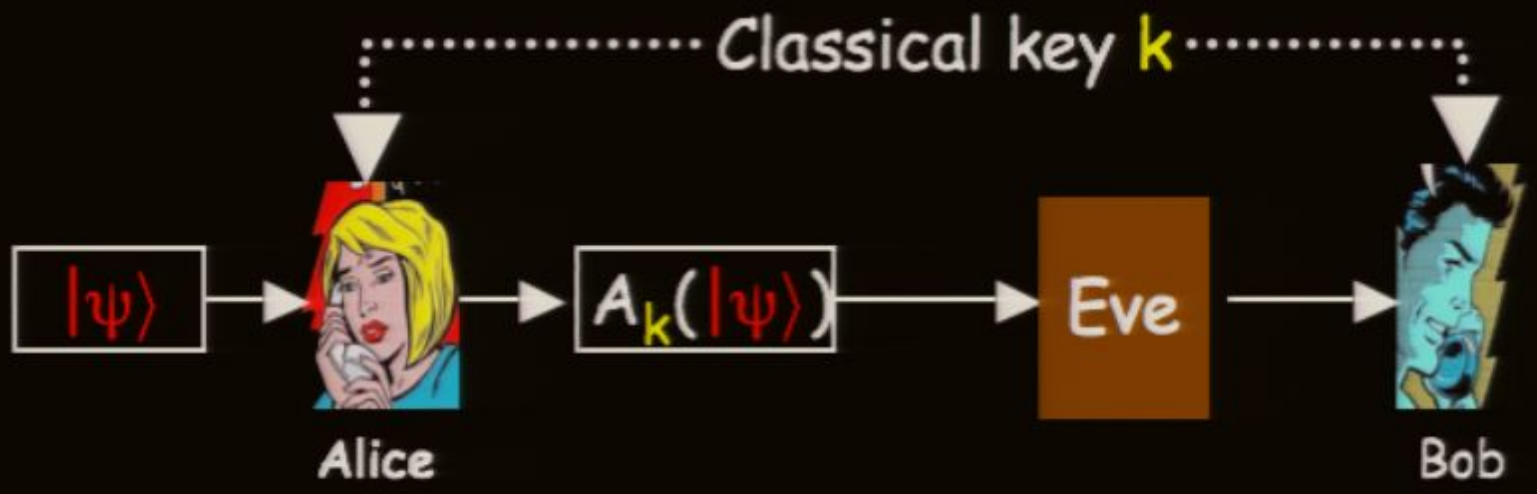
Authenticating Quantum Messages [BCGST]



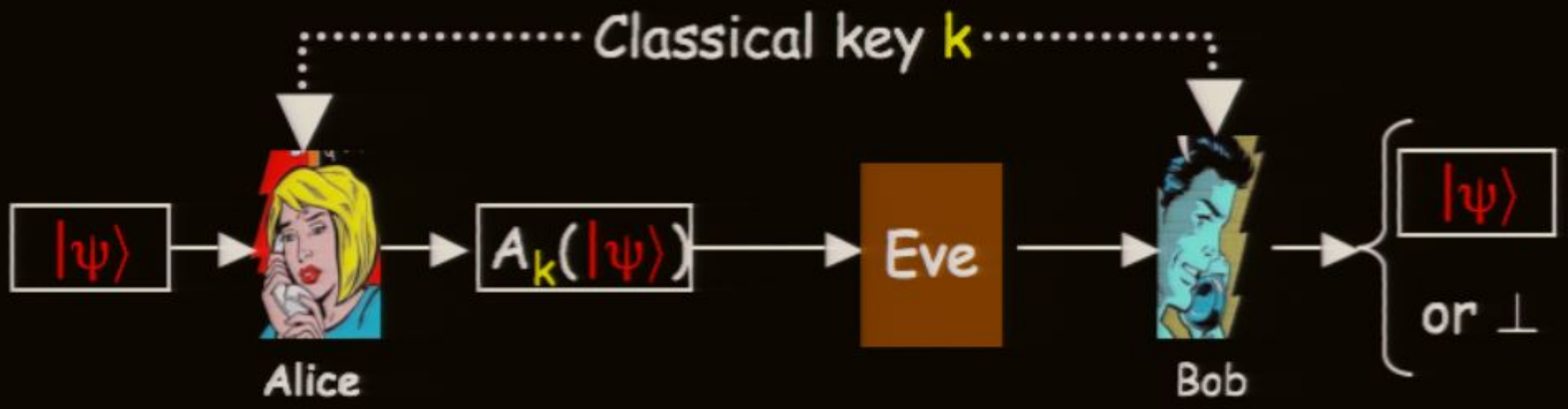
Authenticating Quantum Messages [BCGST]



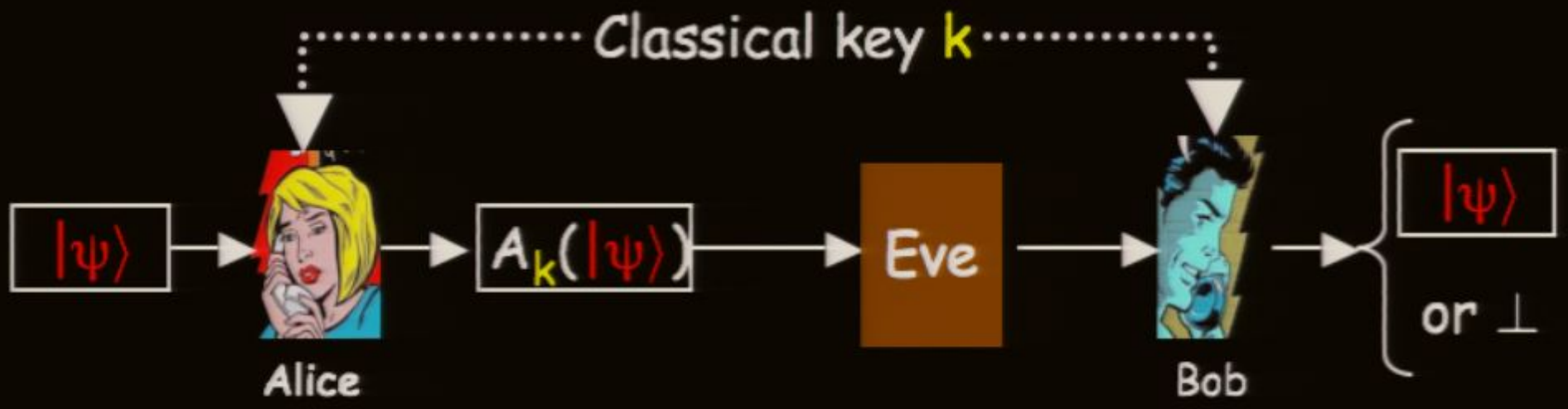
Authenticating Quantum Messages [BCGST]



Authenticating Quantum Messages [BCGST]

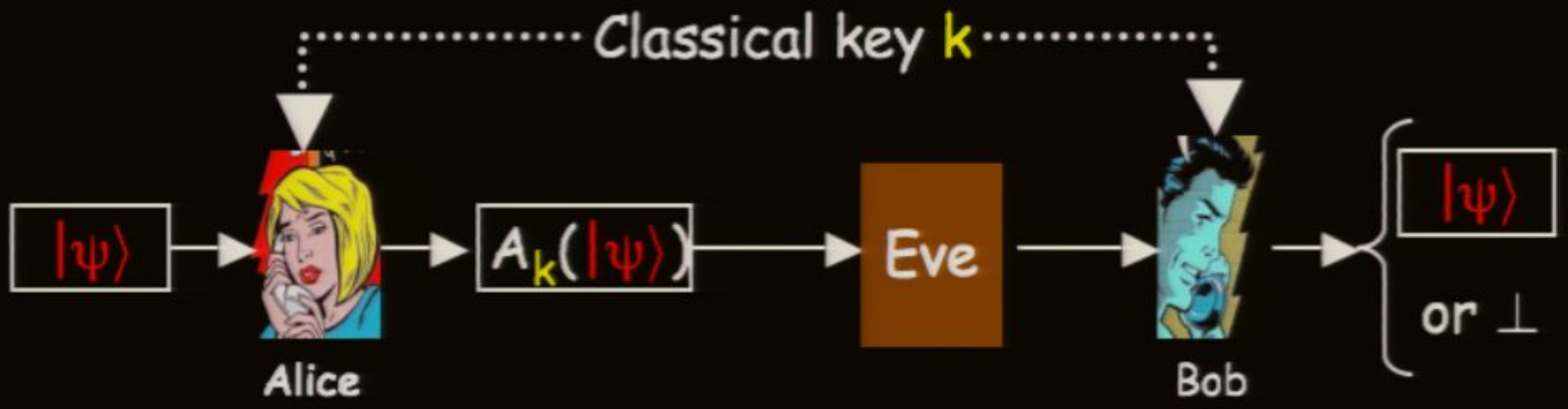


Authenticating Quantum Messages [BCGST]



- System behaves like "channel with veto"
  - Eve inputs one bit (accept/reject)
  - No cloning ⇒ If Bob accepts, Eve learns nothing
  - In fact, Eve learns nothing. Ever.
  - Authentication ⇒ encryption

Authenticating Quantum Messages [BCGST]



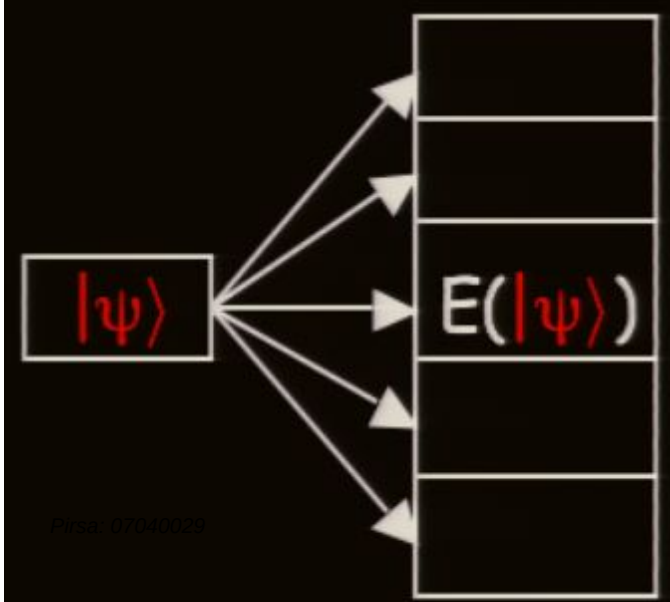
- System behaves like "channel with veto"
  - Eve inputs one bit (accept/reject)
  - No cloning ⇒ If Bob accepts, Eve learns nothing
  - In fact, Eve learns nothing. Ever.
  - Authentication ⇒ encryption
- [BCGST'02] poly-time protocols
  - m qubits ⇝ 2m + 2log (m/ε) bits of key

Approximate Codes [CGS'05]

- Code "correcting" n-1/2 errors
- Start with (n-1)/2 erasure-correcting code
  - Authenticate each piece
  - Secret-share keys
  - Use classical MACs to authenticate keys

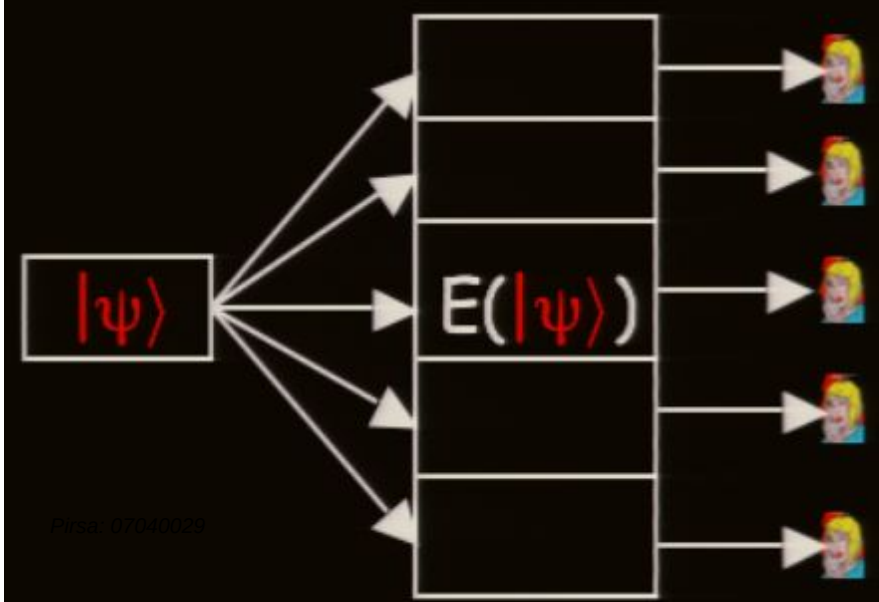
Approximate Codes [CGS'05]

- Code "correcting" n-1/2 errors
- Start with (n-1)/2 erasure-correcting code
  - Authenticate each piece
  - Secret-share keys
  - Use classical MACs to authenticate keys



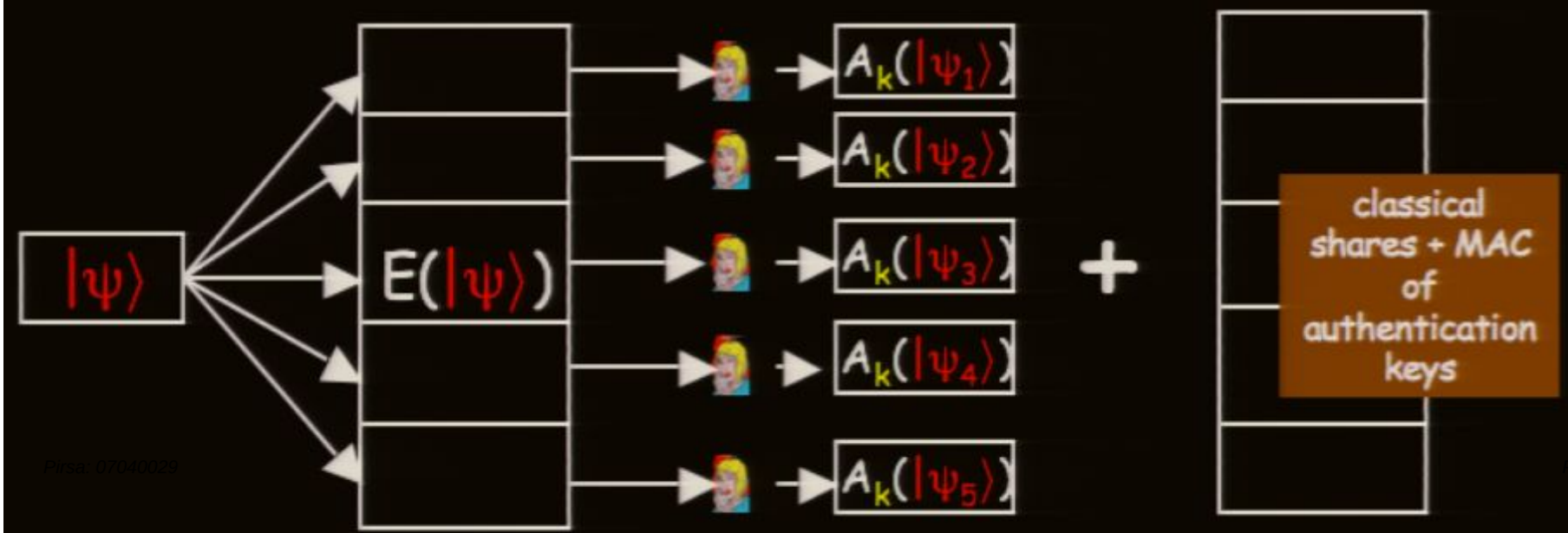
Approximate Codes [CGS'05]

- Code "correcting" n-1/2 errors
- Start with (n-1)/2 erasure-correcting code
  - Authenticate each piece
  - Secret-share keys
  - Use classical MACs to authenticate keys



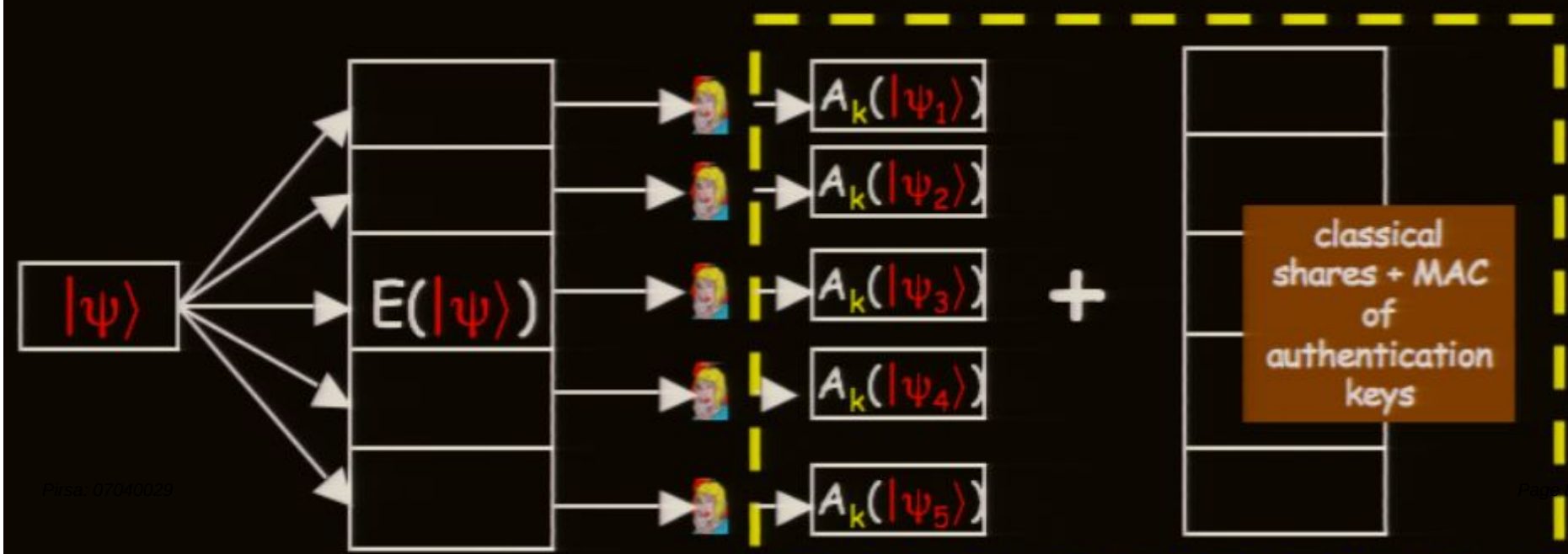
Approximate Codes [CGS'05]

- Code "correcting" n-1/2 errors
- Start with (n-1)/2 erasure-correcting code
  - Authenticate each piece
  - Secret-share keys
  - Use classical MACs to authenticate keys



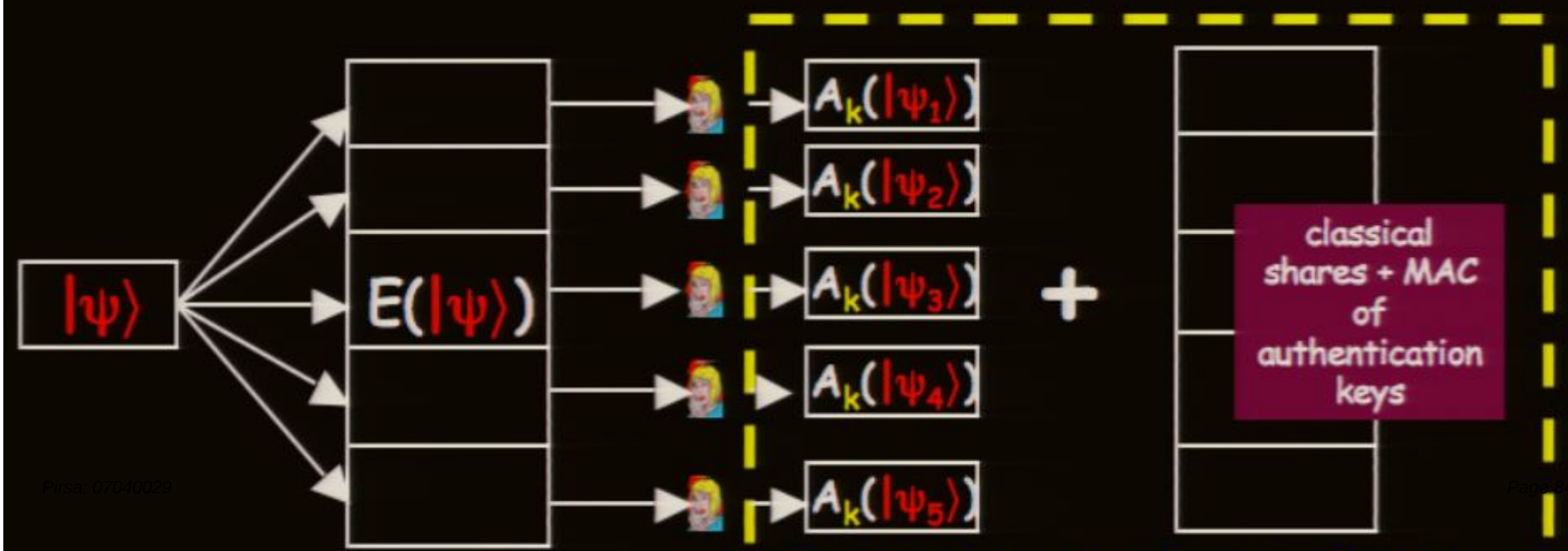
Approximate Codes [CGS'05]

- Code "correcting" n-1/2 errors
- Start with (n-1)/2 erasure-correcting code
  - Authenticate each piece
  - Secret-share keys
  - Use classical MACs to authenticate keys



Approximate Codes [CGS'05]

- AQECC "correcting" n-1/2 errors
  - If any majority of pieces untouched
  - Then original state recovered approximately
  - Correct twice as many errors
  - No classical analogue in codes...



Secret Sharing and Quantum Codes

Secret Sharing and Quantum Codes

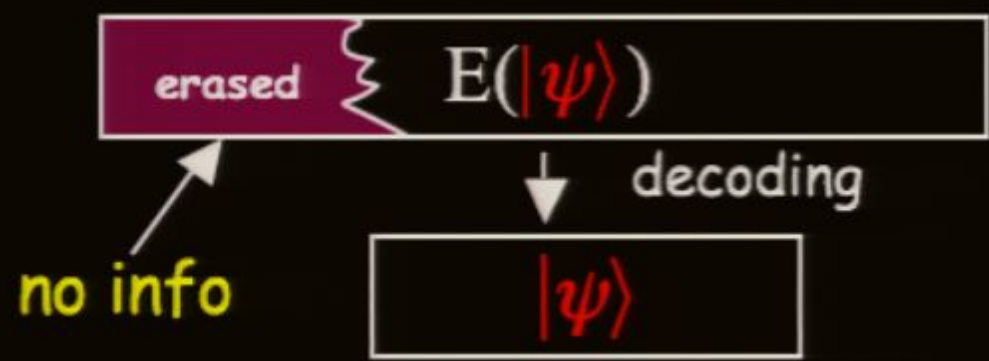
- AQECC smell like secret sharing
  - Similar to Rabin – Ben-Or '89

Secret Sharing and Quantum Codes

- AQECC smell like secret sharing
  - Similar to Rabin – Ben-Or '89
- [CGL] Every quantum code is a SS scheme
  - ~~Dolly~~

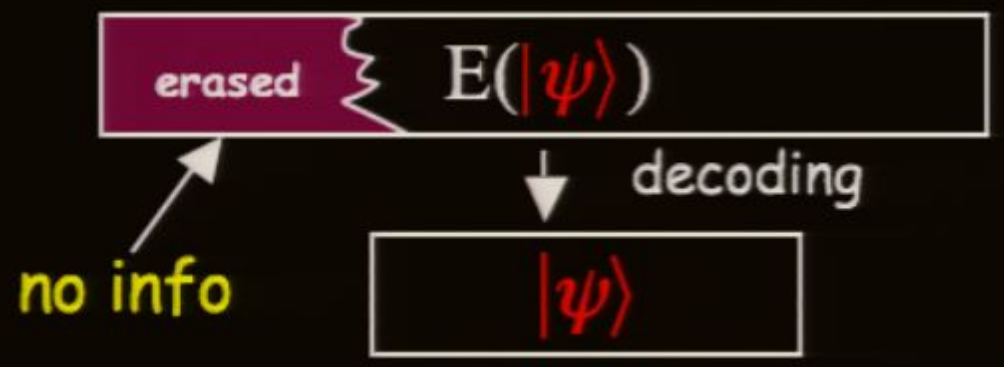
Secret Sharing and Quantum Codes

- AQECC smell like secret sharing
  - Similar to Rabin – Ben-Or '89
- [CGL] Every quantum code is a SS scheme
  - ~~Dolly~~



Secret Sharing and Quantum Codes

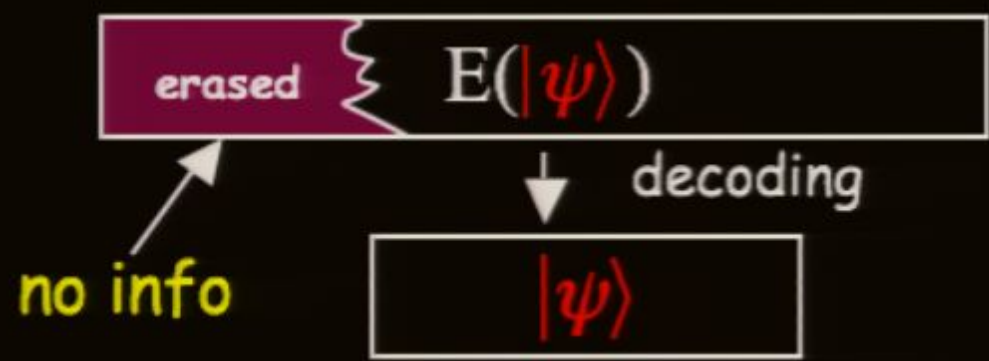
- AQECC smell like secret sharing
  - Similar to Rabin – Ben-Or '89
- [CGL] Every quantum code is a SS scheme
  - ~~Dolly~~



- Lesson of AQECC:
  - best viewed as robust SS (a.k.a. PSMT)
  - secret sharing is the right classical analogue of quantum error-correction

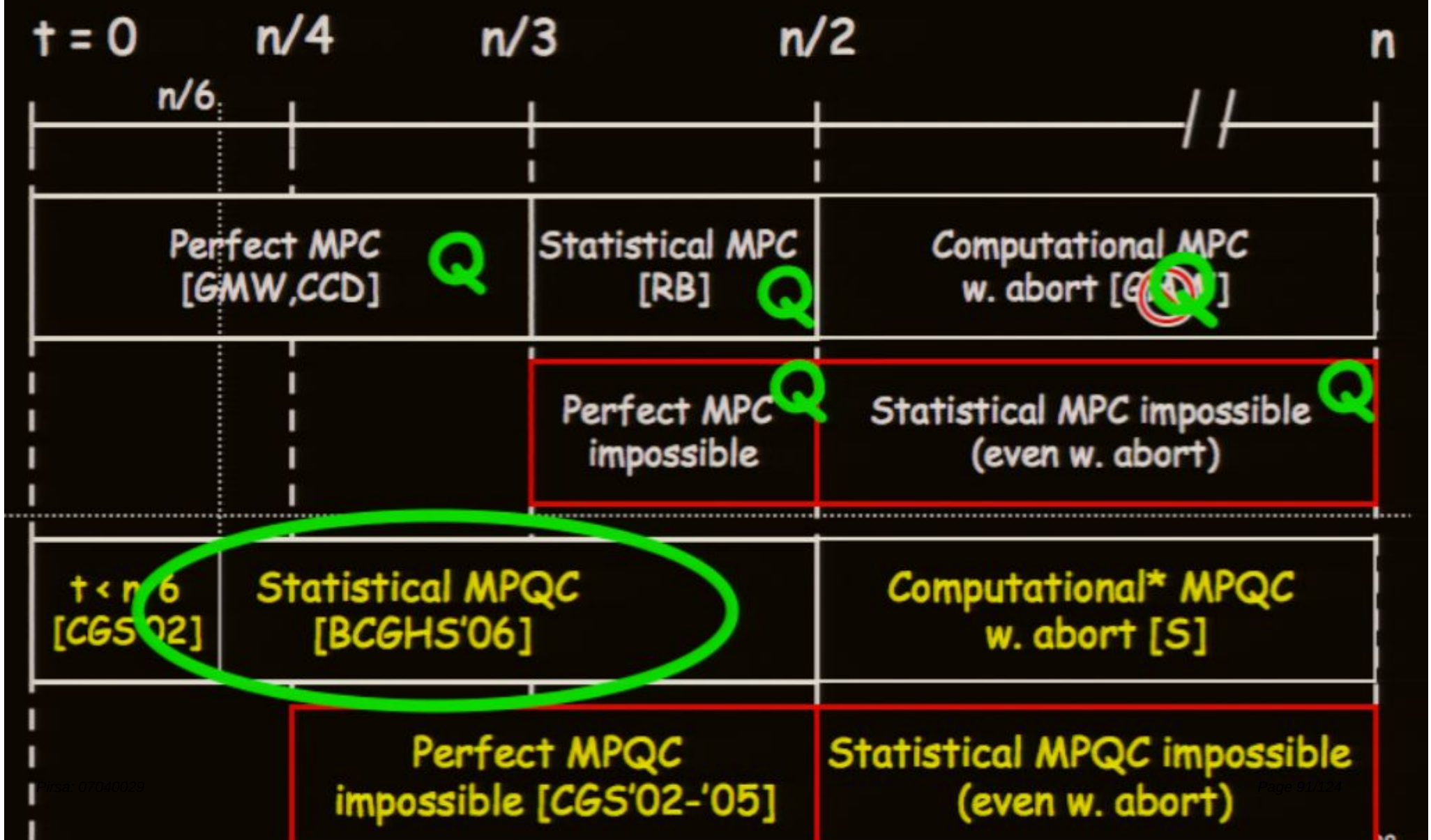
Secret Sharing and Quantum Codes

- AQECC smell like secret sharing
  - Similar to Rabin – Ben-Or '89
- [CGL] Every quantum code is a SS scheme
  - ~~Dolly~~



- Lesson of AQECC:
  - best viewed as robust SS (a.k.a. PSMT)
  - secret sharing is the right classical analogue of quantum error-correction
  - "Cryptography is everything!" (S. Micali)

Basic Feasibility Results (assuming broadcast)



MPQC with a cheating minority

- AQECC is basic underlying code
  - Need to operate on encoded states
- Protocol:
  - Share inputs
    - Authenticate quantum states
    - Share classical keys
  - Compute
    - Reduce computations on quantum states to computations on classical keys
    - Use classical MPC to manipulate keys
  - Distribute outputs

MPQC with a cheating minority

- AQECC is basic underlying code
  - Need to operate on encoded states
- Protocol:
  - Share inputs
    - Authenticate quantum states
    - Share classical keys
  - Compute
    - Reduce computations on quantum states to computations on classical keys
    - Use classical MPC to manipulate keys
  - Distribute outputs

work goes here

A fault-tolerance lemma

- Suppose we can do Clifford gates reliably
  - To get full gate set, Toffoli states suffice

    $\Sigma_{a,b} |a\rangle|b\rangle|ab\rangle$
  - What if an adversary prepares the Toffoli states $T_1,\ldots,T_k$?

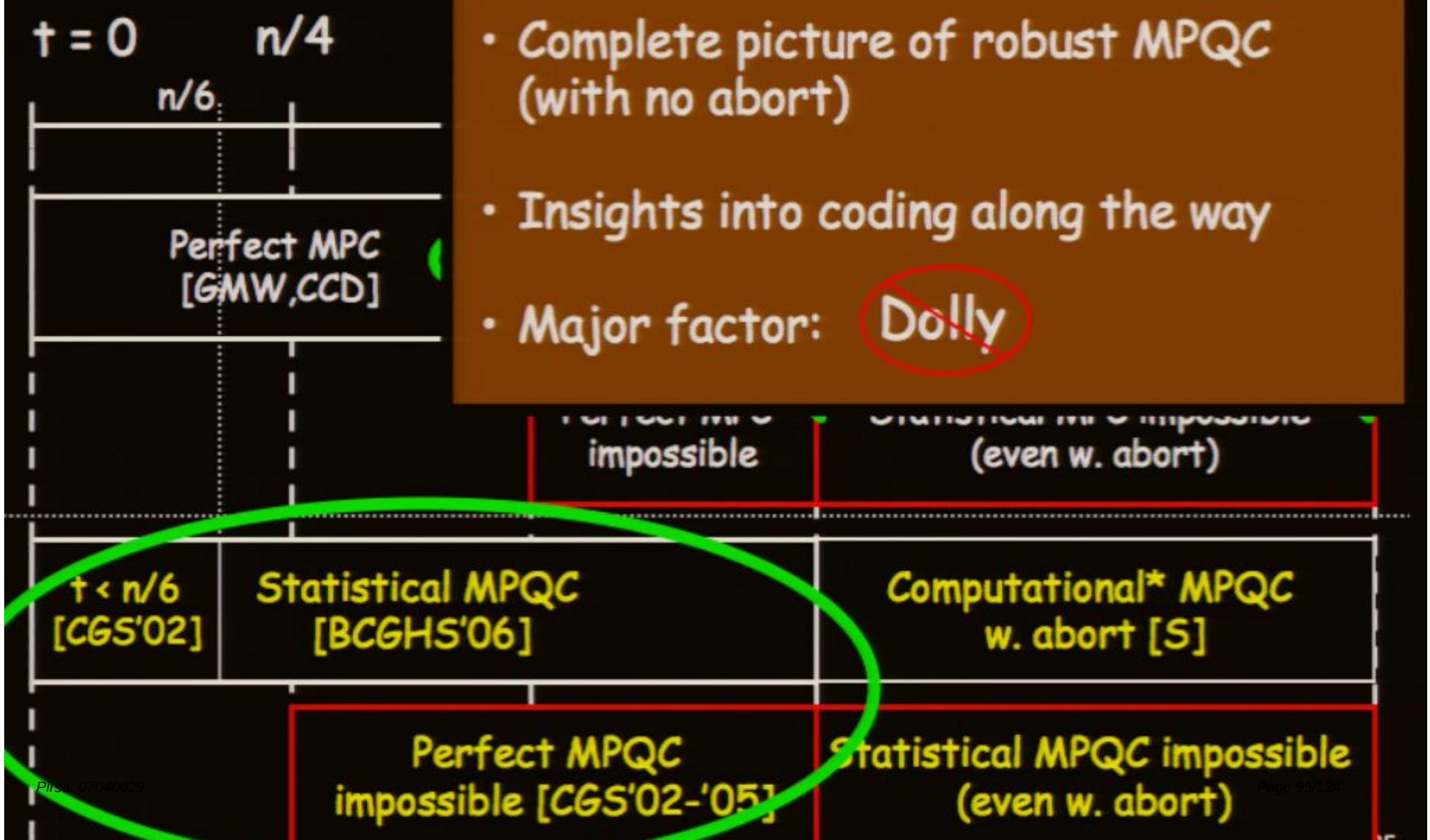
Lemma: There is a Clifford circuit that takes k (possibly faulty) Toffoli states and either

- accepts and outputs $k'<k$ pure Toffoli states or
- aborts.

If $T_1,\ldots,T_k$ were good to start with, circuit accepts.

Basic Feasibility Results (assuming broadcast)

- Complete picture of robust MPQC (with no abort)
- Insights into coding along the way
- Major factor: ~~Dolly~~



This Talk

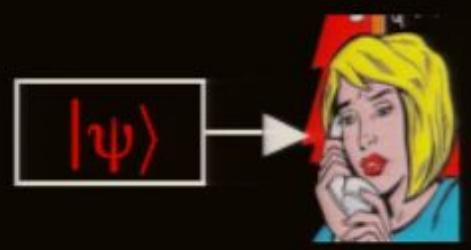
- Intro
- Multiparty Quantum Computing
- Codes and Authentication
- MPQC with a cheating minority
- Beyond a faulty minority: 2-party QC
  - Proofs of knowledge for quantum adversaries

This Talk

- Intro
- Multiparty Quantum Computing
- Codes and Authentication
- MPQC with a cheating minority
- Beyond a faulty minority: 2-party QC
  - Proofs of knowledge for quantum adversaries

Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment

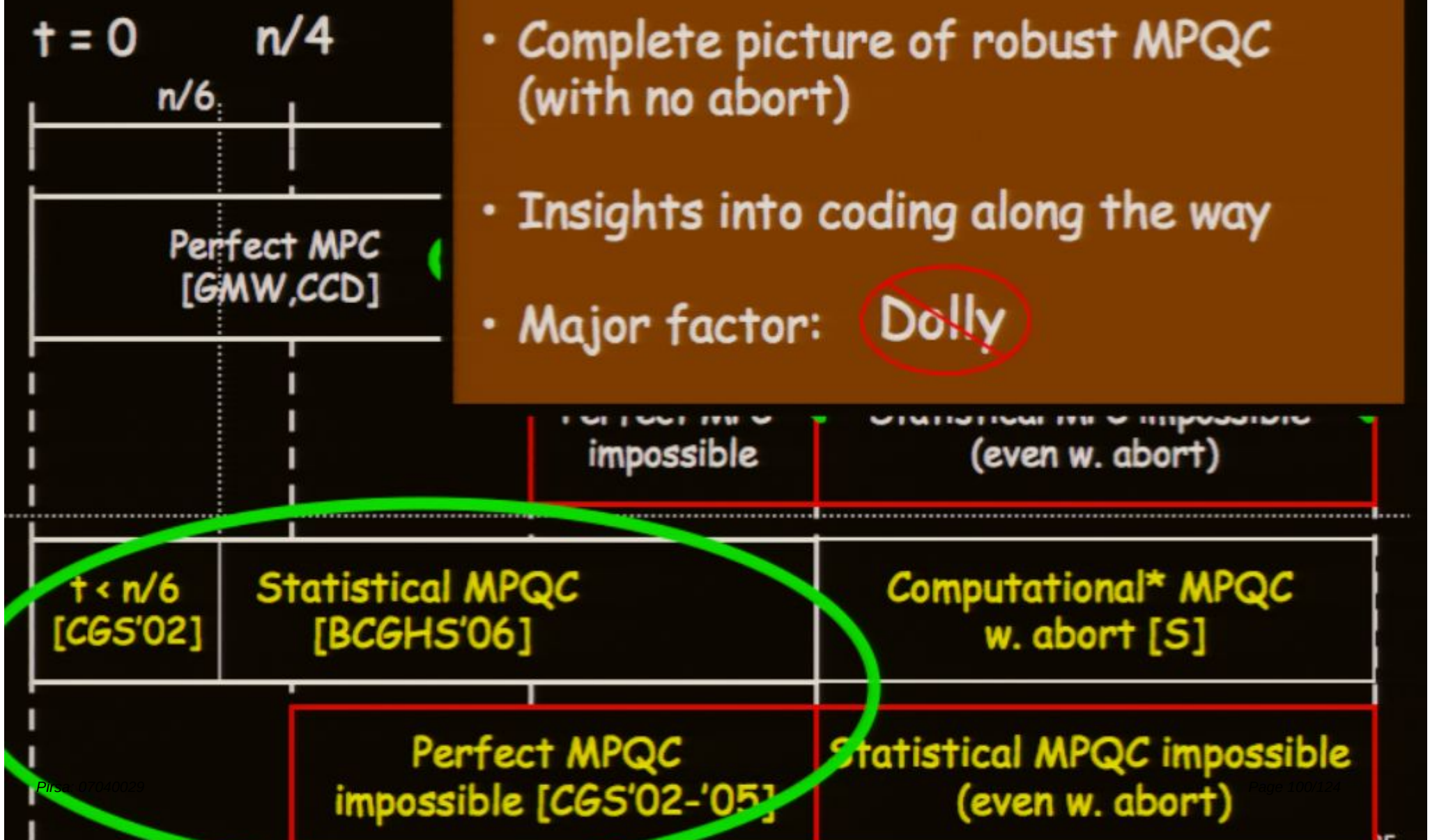


This Talk

- Intro
- Multiparty Quantum Computing
- Codes and Authentication
- MPQC with a cheating minority
- Beyond a faulty minority: 2-party QC
  - Proofs of knowledge for quantum adversaries

Basic Feasibility Results (assuming broadcast)

- Complete picture of robust MPQC (with no abort)
- Insights into coding along the way
- Major factor: ~~Dolly~~

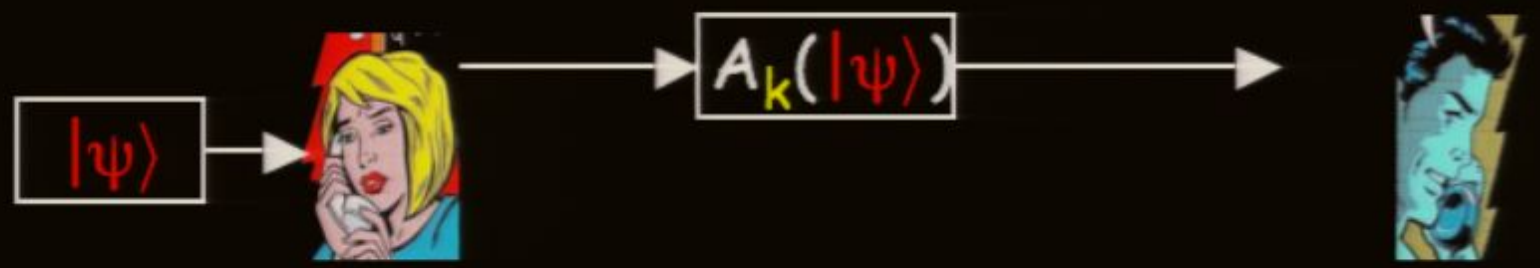


Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment

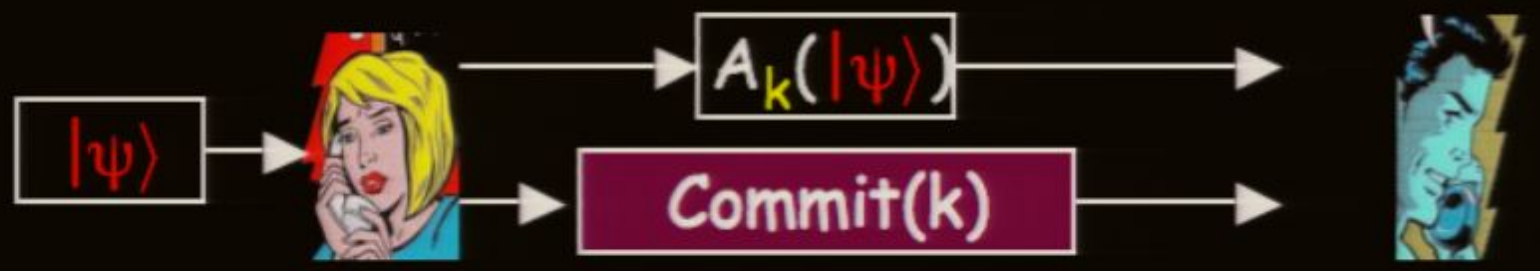
Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment



Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment



Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment

- As before: operate on classical keys
  - Previous reduction still works

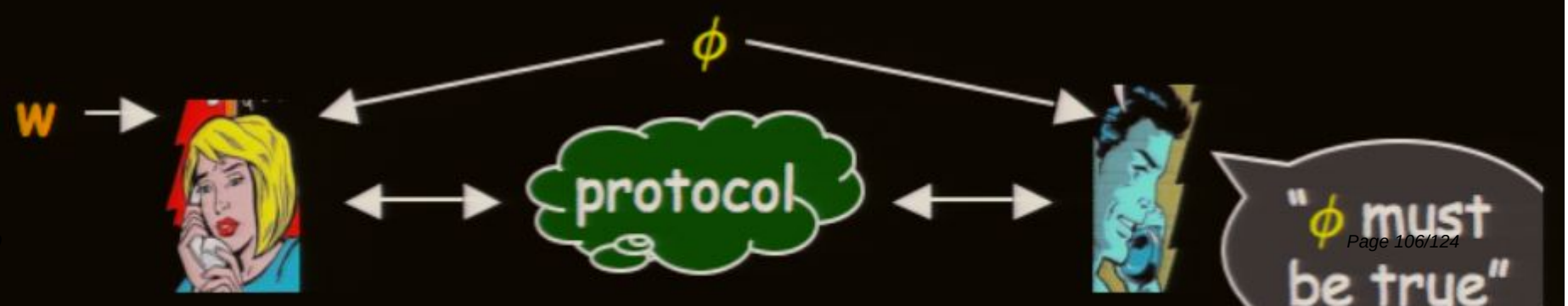
Two-party Quantum Computation

- Many ideas of MPQC can apply here
- AQECC replaced by commitment

- As before: operate on classical keys
  - Previous reduction still works
- Need classical 2-party secure computation
  - Quantum adversary!
  - Sufficient to construct zero-knowledge proofs of knowledge

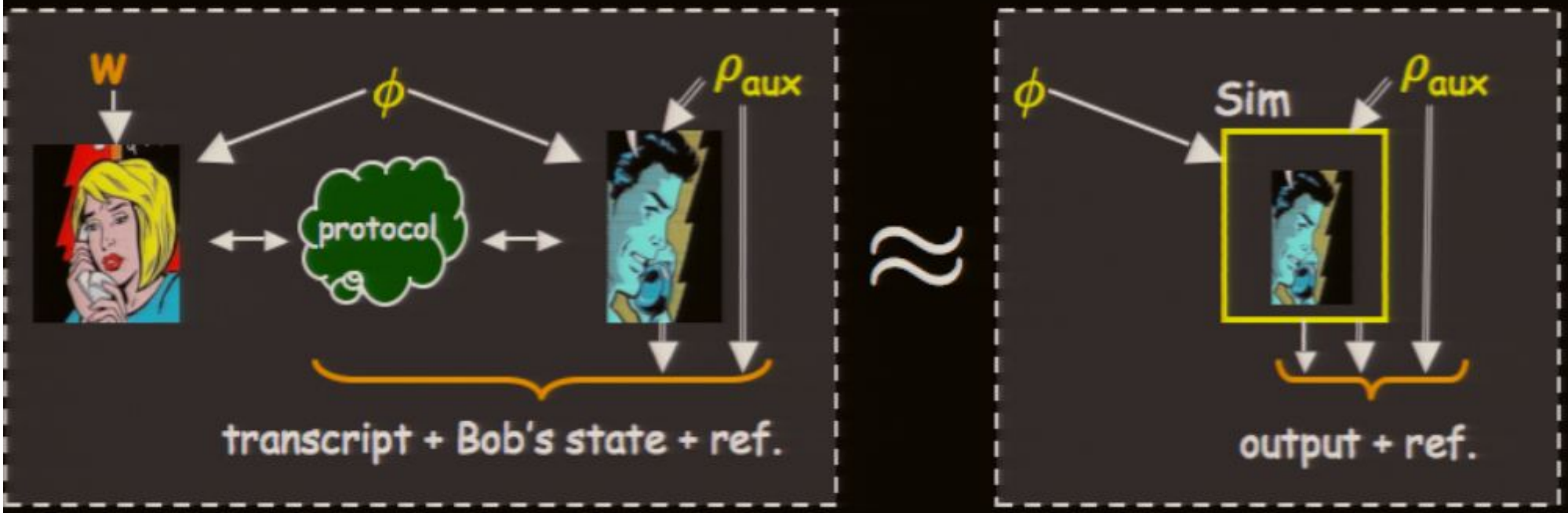
ZK "Proofs of Knowledge"

- Given: boolean formula ϕ
- Alice wants to prove to Bob that ϕ is satisfiable
  - Satisfiable: $\exists$ "witness" w: $\phi(w)=1$
  - This encodes statement "Alice has followed the protocol so far"
- Goals:
  - Alice doesn't want Bob to learn w
  - Bob wants to be sure Alice has some real w in mind



Formalizing Zero-Knowledge

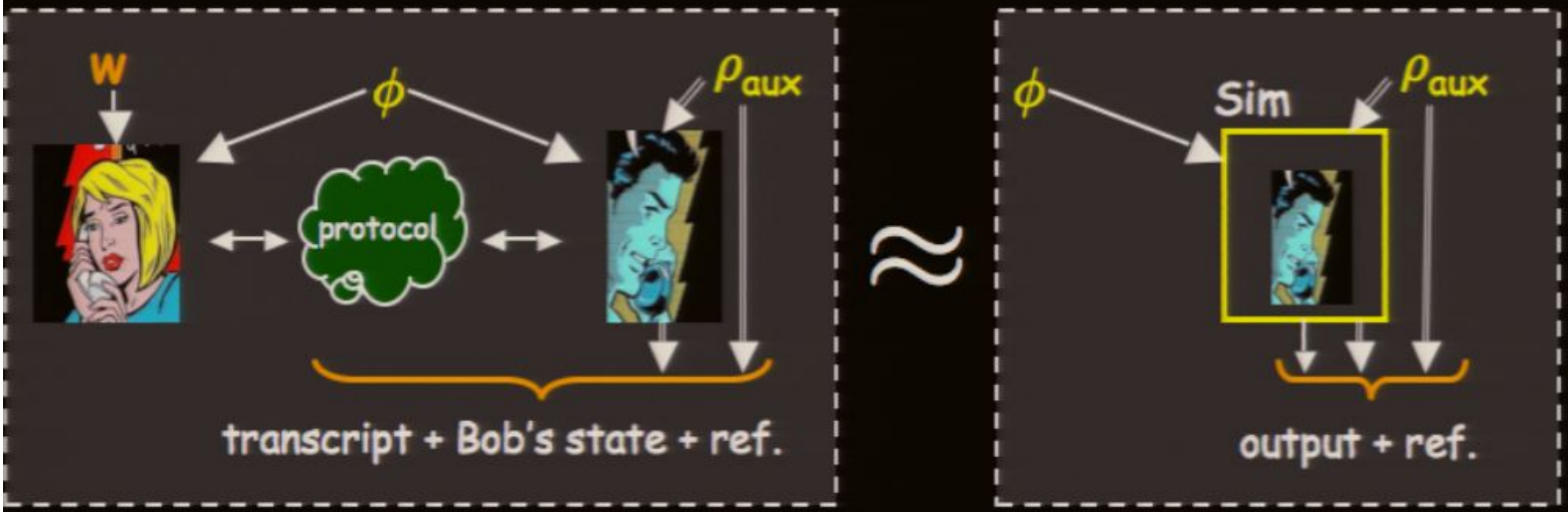
- ∀ Bob, ∃ Simulator such that ∀ ρ_{aux}:



- **Idea**: Bob learns "nothing" since he could have simulated the conversation knowing only that ϕ is satisfiable

Formalizing Zero-Knowledge

- $\forall$ Bob, $\exists$ Simulator such that $\forall\ \rho_{aux}$:

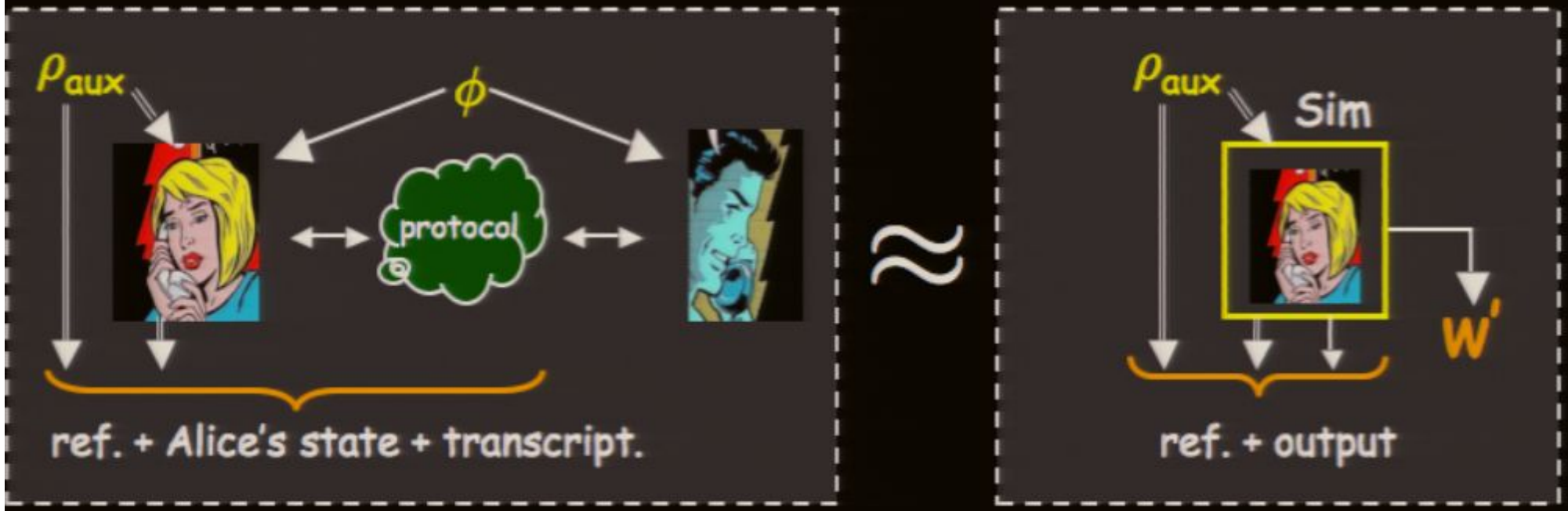


Theorem [Watrous]: There exists a **sound** ZK proof system for satisfiability (i.e. NP) secure against quantum verifiers.

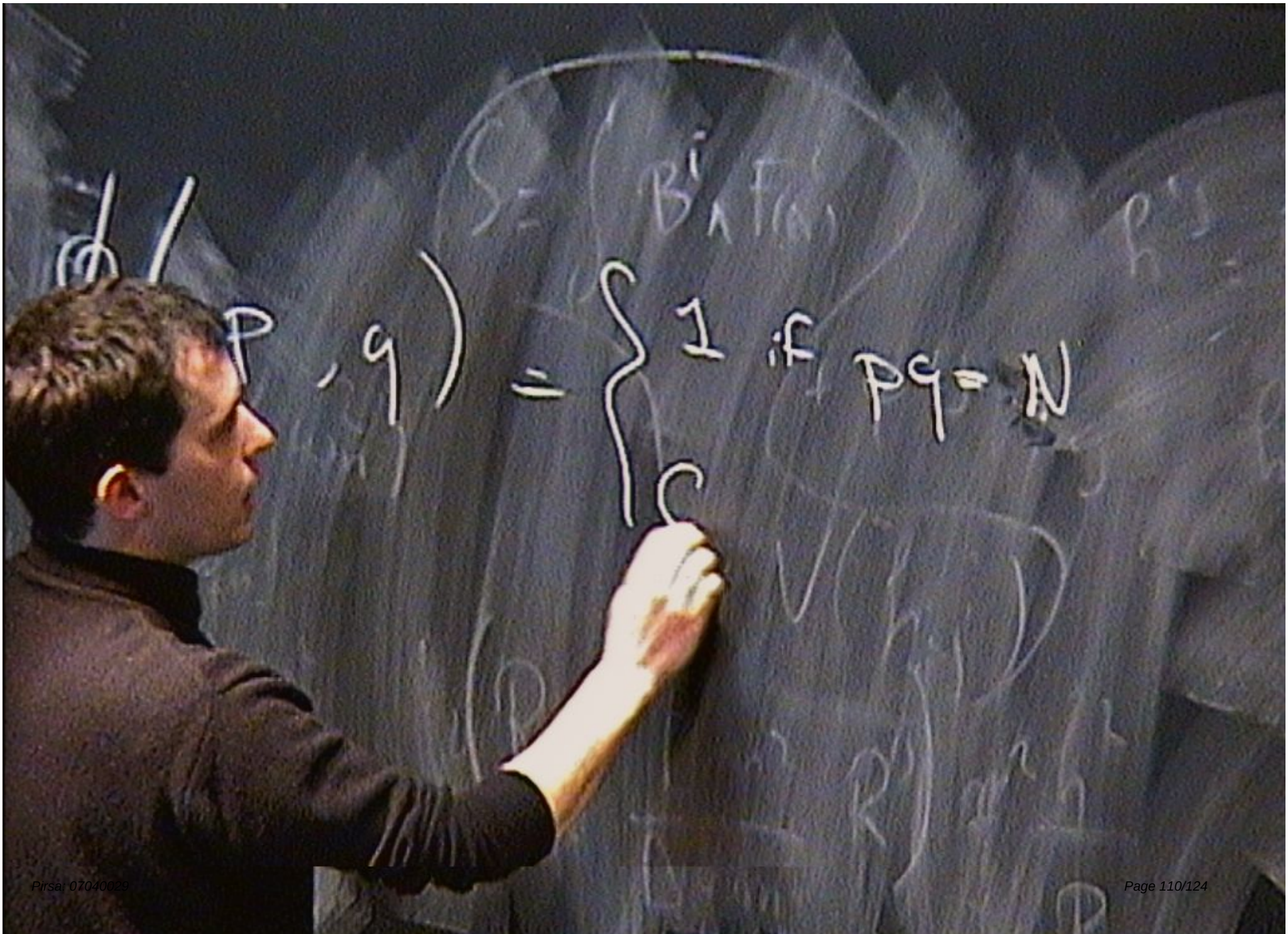
Problem: May not be a proof of knowledge.

Formalizing Proofs of Knowledge

- ∀ Alice, ∃ Simulator such that ∀ ρ_{aux}



- Extra condition on simulator: if simulated transcript accepts, then $\phi(w')=1$
  - Alice "knows" a witness


p, q) = { 1 if pq = N

$$\phi_N(p, q) = \begin{cases} 1 & \text{if } pq = N \\ 0 & \text{otherwise} \end{cases}$$

$$\phi_N(p, q) = \begin{cases} 1 & \text{if } pq = N \text{ and } p > 1, q > 1 \\ 0 & \text{otherwise} \end{cases}$$

Two-party Quantum Computation

- Problem: standard ZK simulation + extraction arguments may not work in quantum world
  - Rewinding = cloning auxiliary info ~~Dolly~~
  - Sequential composition is lost

Two-party Quantum Computation

- Problem: standard ZK simulation + extraction arguments may not work in quantum world
  - Rewinding = cloning auxiliary info ~~Dolly~~
  - Sequential composition is lost

Two-party Quantum Computation

- Problem: standard ZK simulation + extraction arguments may not work in quantum world
  - Rewinding = cloning auxiliary info

  - Sequential composition is lost

- Big step: Watrous' simulator for 3-round ZK
  - Does not give knowledge extractor

Two-party Quantum Computation

- Problem: standard ZK simulation + extraction arguments may not work in quantum world
  - Rewinding = cloning auxiliary info

  - Sequential composition is lost
- Big step: Watrous' simulator for 3-round ZK
  - Does not give knowledge extractor
- Idea: We can lie, need to read minds
  - Attach special preamble

Protocol

w

ϕ

$c = \text{Commit}(a)$

b

a

ZK Proof that Decommit(c) =a

$pk = a+b$

(interpret as public key for special encryption scheme)

$e = \text{Encrypt}_{pk}(w)$

ZK Proof that e encodes a witness for ϕ

Properties of the encryption scheme

- There exists a set $S \subseteq \{0,1\}^{|pk|}$ such that
  - $|S| \ll 2^{|pk|}$
  - $[\, pk \leftarrow S \,] \approx_{QPT} [\, pk \leftarrow \{0,1\}^{|pk|} \,]$
  - If pk not in S, then for all w_1, w_2:

    $$\text{Encrypt}_{pk}(w_1) \equiv \text{Encrypt}_{pk}(w_2)$$

    (identical distributions)
  - If $pk \in S$, then for all w_1, w_2:

    $$\text{Encrypt}_{pk}(w_1) \cap \text{Encrypt}_{pk}(w_2) = \emptyset$$

    - And we can efficiently sample (pk, SK) where $pk \leftarrow S$ and SK is a decryption key for pk

Example: If E is a mult. homomorphic encryption scheme, then let $pk' = (pk, c)$ where $c = E_{pk}(r)$ and let

$$\text{Encrypt}_{pk'} = E_{pk}(w) \cdot c^a \text{ where } a \text{ is random}$$

- Question: examples that are not obviously insecure?

$$p, q) = \begin{cases} 1 & \text{if } pq = \mathbb{N} \text{ and } p = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\boxed{pk \in S \iff c = E_{pk}(1)}$$

Properties of the encryption scheme

- There exists a set $S \subseteq \{0,1\}^{|pk|}$ such that
  - $|S| \ll 2^{|pk|}$
  - $[\, pk \leftarrow S \,] \approx_{QPT} [\, pk \leftarrow \{0,1\}^{|pk|} \,]$
  - If pk not in S, then for all w_1, w_2:

$$\text{Encrypt}_{pk}(w_1) \equiv \text{Encrypt}_{pk}(w_2)$$

(identical distributions)

  - If $pk \in S$, then for all w_1, w_2:

$$\text{Encrypt}_{pk}(w_1) \cap \text{Encrypt}_{pk}(w_2) = \emptyset$$

    - And we can efficiently sample (pk, SK) where $pk \leftarrow S$ and SK is a decryption key for pk

Example: If E is a mult. homomorphic encryption scheme, then let $pk' = (pk, c)$ where $c = E_{pk}(r)$ and let

$$\text{Encrypt}_{pk'} = E_{pk}(w) \cdot c^a \text{ where } a \text{ is random}$$

- Question: examples that are not obviously insecure?

Protocol

w

ϕ

$c = \text{Commit}(a)$

b

a

ZK Proof that Decommit(c) =a

$pk = a+b$

(interpret as public key for special encryption scheme)

$e = \text{Encrypt}_{pk}(w)$

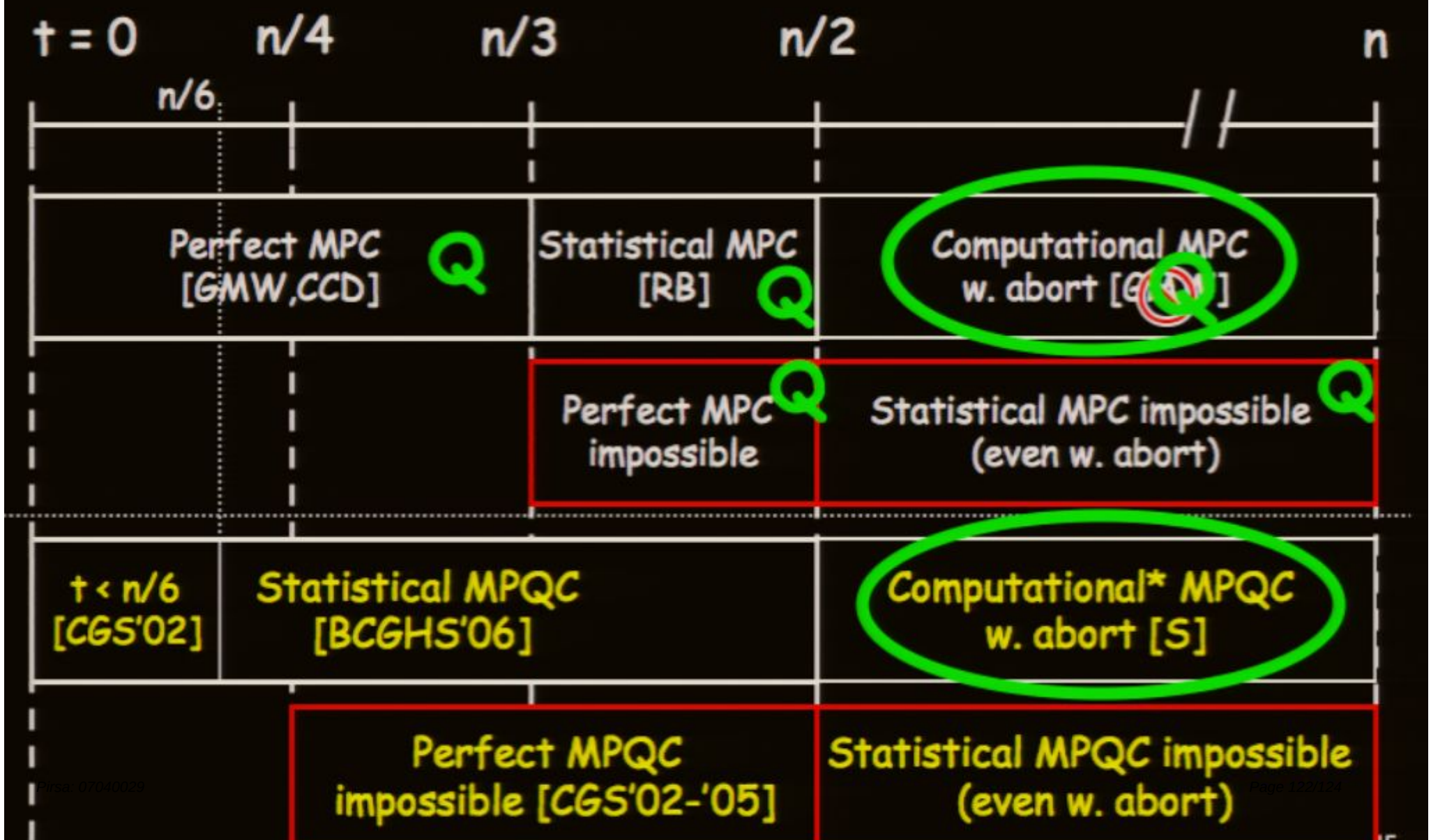
ZK Proof that e encodes a witness for ϕ

Coin flipping where
- Simulated verifier can control coin flip [Wat]
- Simulated prover just knows coin will be random.

- In a real execution, this leaks no information (w.h.p.).
- Simulated verifier controls PK so can decrypt

- Simulated prover can does not need to know a witness

Basic Feasibility Results (assuming broadcast)



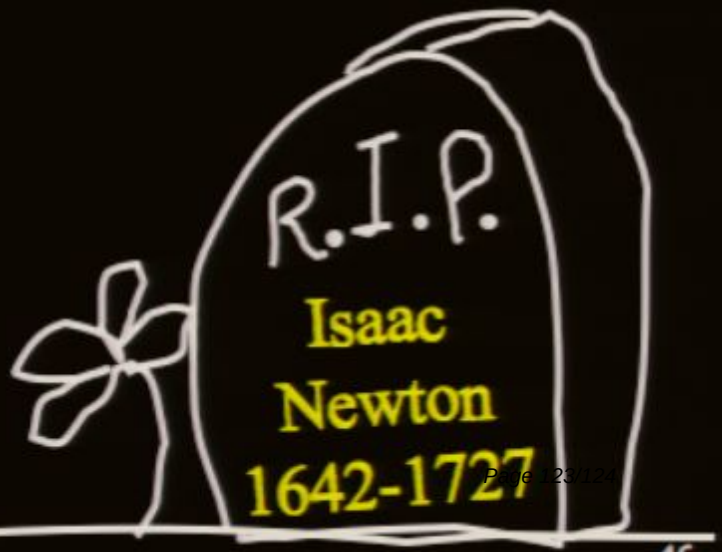
Cryptography in a Quantum World

- Landscape changes!
  - New features appear
  - New difficulties arise
  - Some key pieces unchanged

- Needed:

  Tools and language for reasoning about quantum adversaries

- The field is still very young
  - Some successes…
  - … occasional mistakes
  - Lots of questions!



Dolly

Thanks

Co-authors:

Howard Barnum (LANL),
Michael Ben-Or (HUJI),
Claude Crépeau (McGill),
Daniel Gottesman (Perimeter),
Avinatan Hasidim (HUJI),
Alain Tapp (Montreal)

Discussions: Boaz Barak, Louis Salvail, Jon Katz, …