

Responsive Round Complexity and Concurrent Zero-Knowledge

A Lecture at Asiacrypt 2001

- Tzafrir Cohen (Technion)
- Joe Kilian (Yianilos Labs)
- Erez Petrank (Technion)

Agenda

- Background, definitions, motivation: zero-knowledge proofs
- Concurrent zero-knowledge: Current state-of-the-art
- Responsive-Round-Complexity: a new notion
- Our new proof system (ideas)
- Conclusions

Interactive Proofs

[GOLDWASSER-MICALI-RACKOFF]

An interactive proof system for L :

- Prover (P) tries to convince verifier (V) that $x \in L$
 - **Completeness:** P succeeds on all $x \in L$
 - **Soundness:** Any prover P^* may succeed on any $x \notin L$ with only negligible probability
 - **Efficiency:** V is probabilistic polynomial time

Zero-Knowledge, Black-Box Version

Zero-Knowledge:

[GOLDWASSER-MICALI-RACKOFF],

Black-Box version: [GOLDREICH-OREN]

An interactive proof (P, V) is a black-box zero-knowledge if exists an efficient simulator S such that for any verifier V^* :

If $x \in L$, hard to distinguish betw. $(P, V^*)(x)$ and $S_{V^*}(x)$

- S interacts with V^* as a “black box”
 - S manipulates coin tosses of V^*
- $\Rightarrow S$ can rewind V^* and try various answers

Fundamental Theorem of Zero-Knowledge

[Goldreich-Micali-Wigderson]

If one way functions exist, then there exists a zero-knowledge interactive proof for any language in \mathcal{NP}

- What about multiple proofs?
- How does this work in a modern computing environment?

Concurrent Composition of Proofs

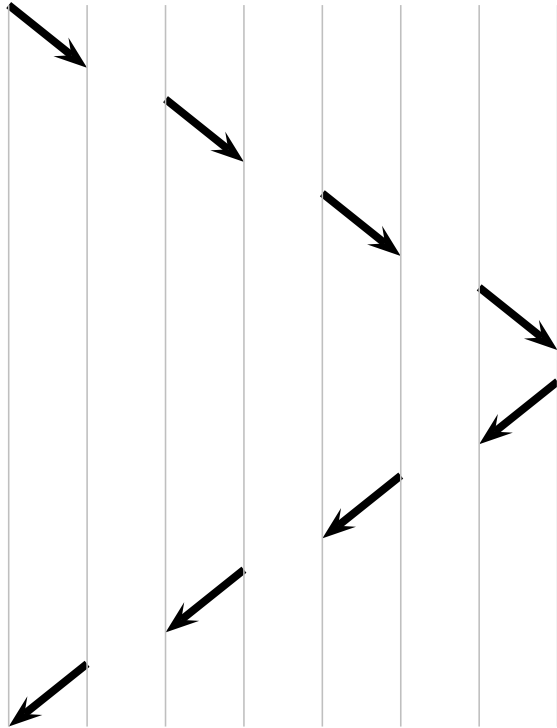
Concurrent: (asynchronous) multiple verifiers (V_i) connect to the prover (P) independently in multiple sessions.

Paranoid Prover: All verifiers are coordinated by a single adversary. Their sole purpose is to extract information from P .

Concurrent Zero-Knowledge: The zero-knowledge property is maintained in concurrent settings.

Main Problem: Pyramid Timing

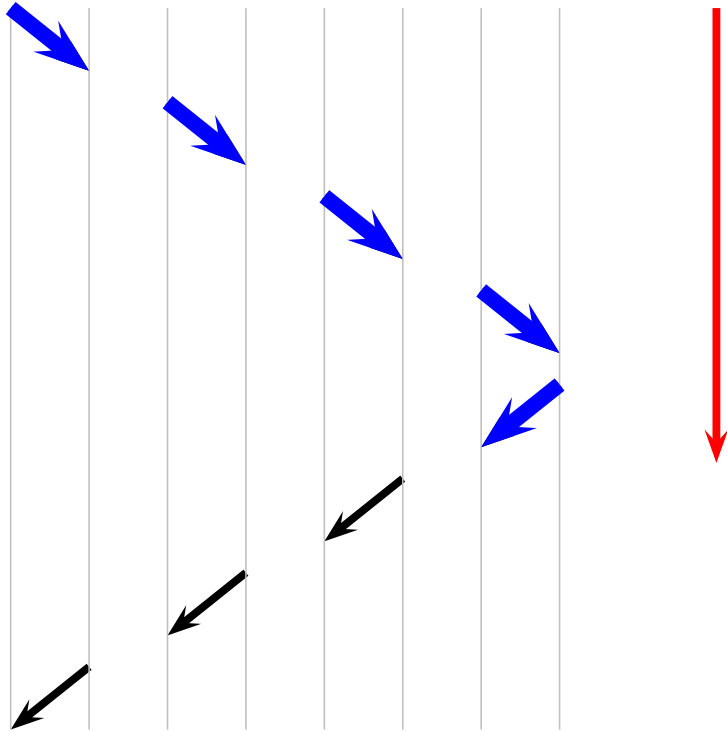
$PV_1 PV_2 PV_3 PV_4$



Next

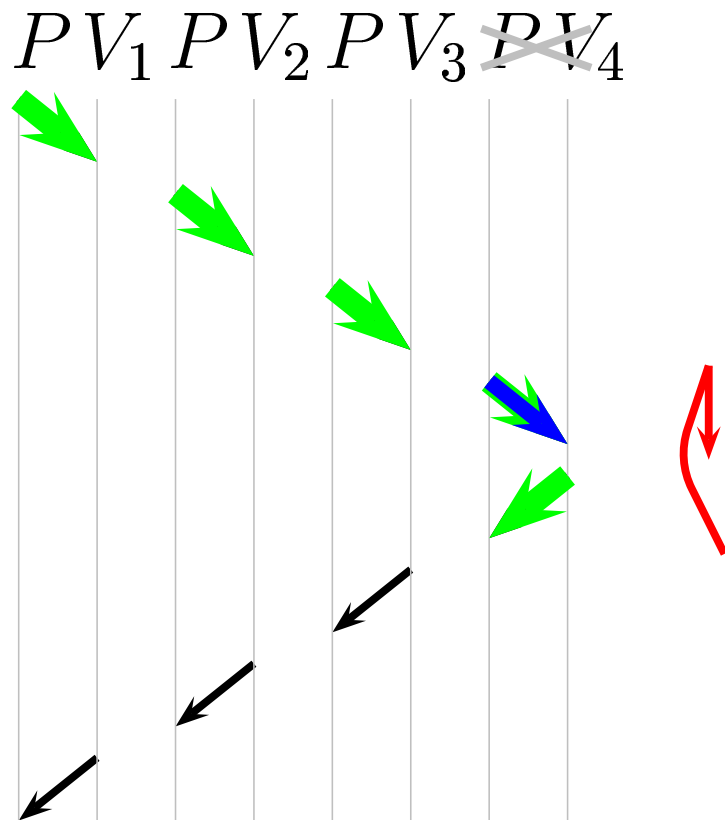
Main Problem: Pyramid Timing

$PV_1 PV_2 PV_3 PV_4$



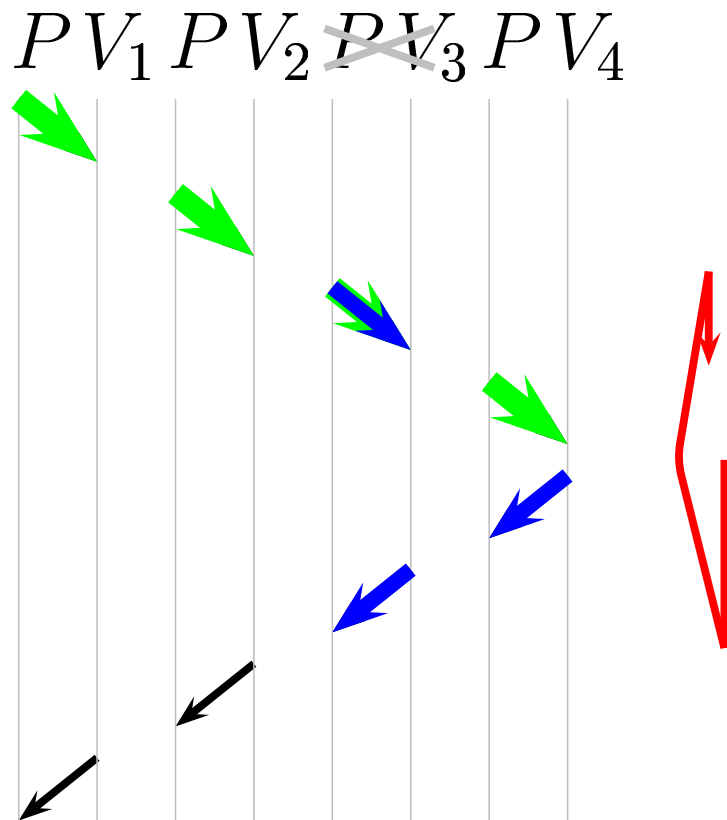
Next

Main Problem: Pyramid Timing



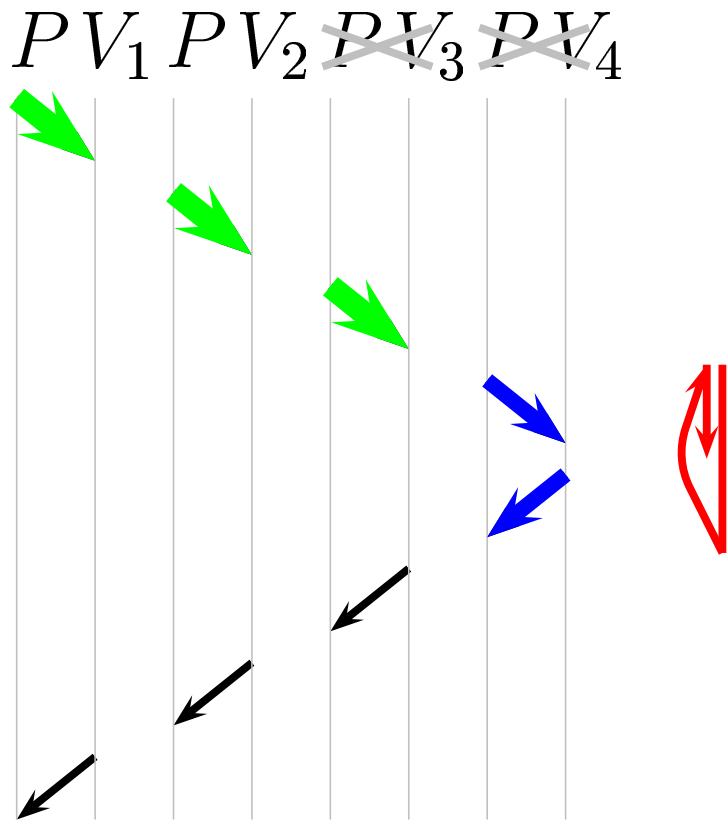
Next

Main Problem: Pyramid Timing



Next

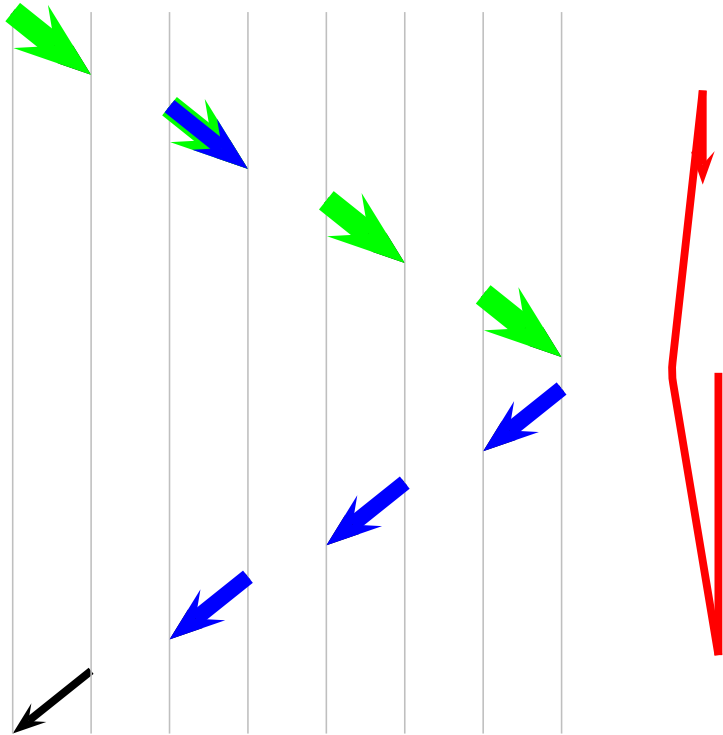
Main Problem: Pyramid Timing



Next

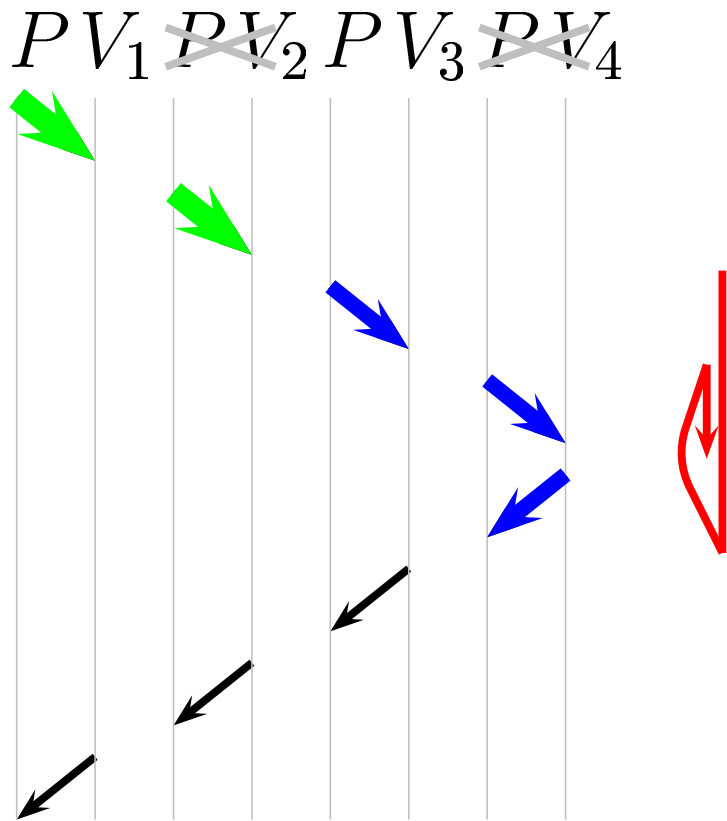
Main Problem: Pyramid Timing

PV_1 ~~PV_2~~ PV_3 PV_4



Next

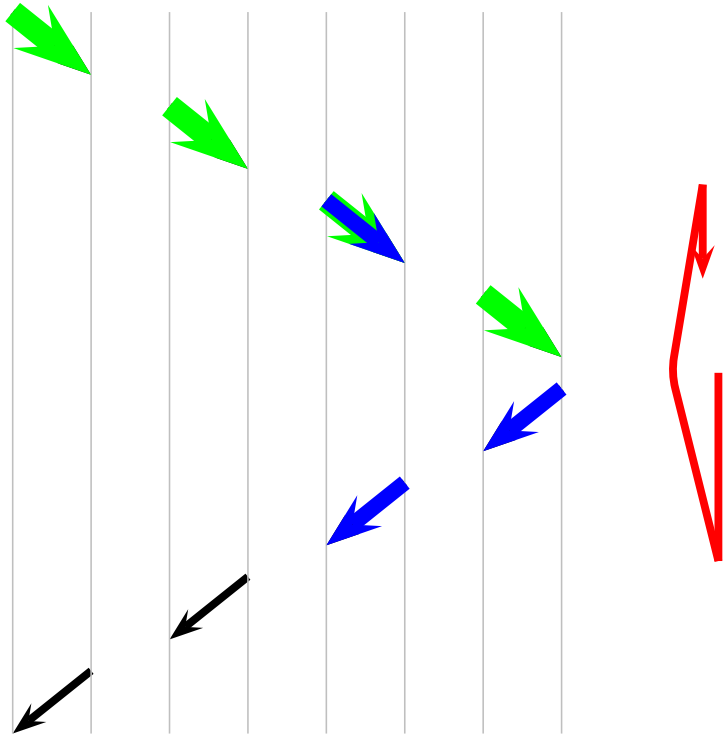
Main Problem: Pyramid Timing



Next

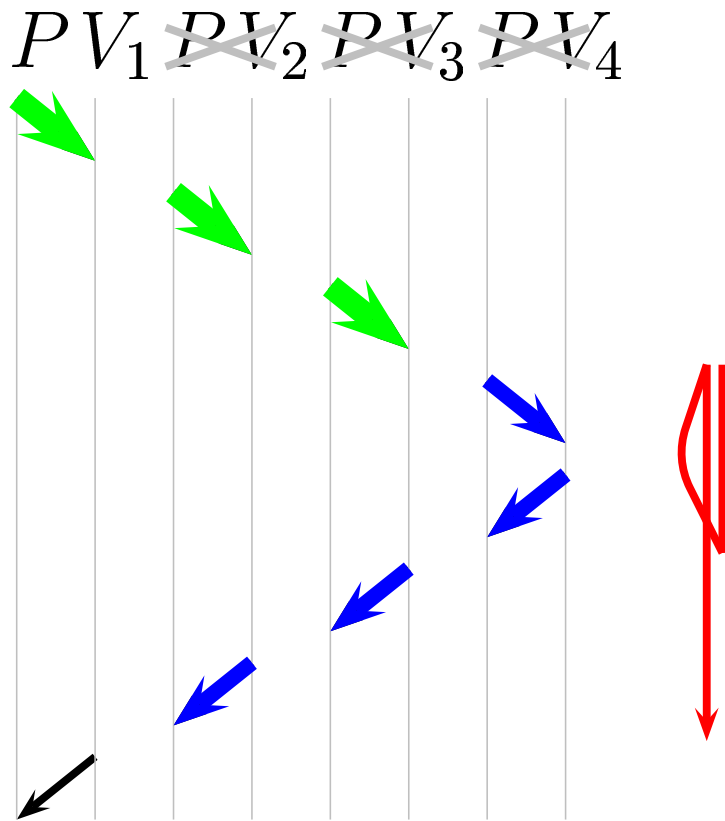
Main Problem: Pyramid Timing

PV_1 ~~PV_2~~ ~~PV_3~~ PV_4



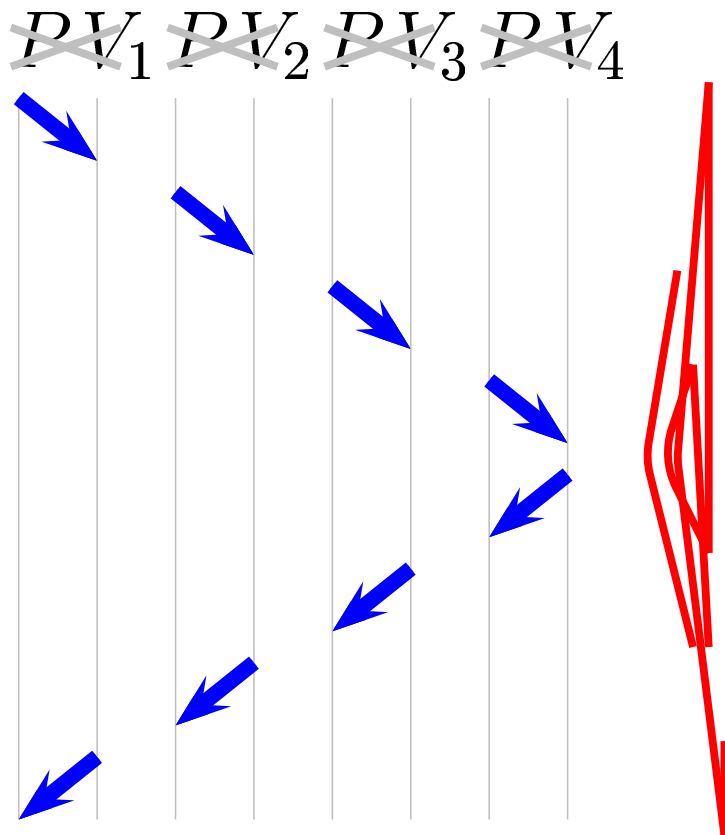
Next

Main Problem: Pyramid Timing



Next

Main Problem: Pyramid Timing



Next

Work is exponential in the number of the verifiers!

Current Lower Bound

As shown by [Canetti-Killian-Petrank-Rosen]

A **black-box** simulation of a proof for a non- \mathcal{BPP} language requires $\tilde{\Omega}(\log n)$ rounds

Current Upper Bound

- [Kilian-Petrank] proposed a Black-box concurrent zero-knowledge for \mathcal{NP} with round complexity $\tilde{O}(\log^2 n)$
- Recent breakthrough [Barak]: non-black-box zero-knowledge proof for \mathcal{NP} with a constant number of rounds.
 - Slight drawback: max number of sessions must be known in advance.
 - length of communication proportional to this number.

Alternative Models

Timing Limitations

- Each session lasts the same time period.
Pyramid-like timing is impossible
([Dwork-Naor-Sahai])
 - Subsequent work has reduced limitations

Settings Assumptions

- Give the prover some information about the verifier.
- Drawbacks: decreased anonymity, trusted authority, users must register in advance.

This Work:

Responsive-Round Complexity

- Motivation for round complexity is time complexity.
- If one round is longer than all the rest, motivation fails.
- Our suggestion:
 - Measure number of rounds by length of longest round.
 - Thus, relate round complexity to time complexity.
 - Intuitively: round complexity (modified) =
$$\frac{\text{overall communication time}}{\text{longest round}}$$

Responsive-Round Definition

Complexity:

- Each party gets a guarantee on overall communication time by how much it delays a message.
- Responsive round complexity m for V_i in a protocol means that:
 - If longest delay of V_i in a run of the protocol is t ,
 - Then overall communication time is at most $m \cdot t$.
- If V_i intentionally delays a message or V_i has slow communication, then its overall guarantee on communication time naturally suffers.

Main Result

Theorem: There exists a concurrent zero-knowledge interactive proof for \mathcal{NP} with responsive round complexity $m = \tilde{O}(\log n)$.

- Proof by construction.
- We use a modified [Richardson-Kilian] protocol with $\tilde{O}(\log n)$ rounds.
- Verifier has associated delay (initially small).
- If verifier fails to answer “in time”, it is reset to start again with double delay.

Ideas in Construction

Complexity

- At most $O(\log n)$ failures (levels)
 - Communication time dominated by highest delay.
 - Each level has $\tilde{O}(\log n)$ rounds.
- \Rightarrow responsive round complexity is $\tilde{O}(\log n)$.

Simulation

- Verifiers with the same delay can be simulated using ideas from [Dwork-Naor-Sahai].
- Combining different levels of delays concurrently requires care and a new rewind schedule for the simulator).

Remarks

- Note the difference from timing-assumptions of [Dwork-Naor-Sahai]: Network is not limited, ZK always guaranteed.
- Round complexity (worst case) is still $\tilde{O}(\log^2 n)$, but responsive round complexity is $\tilde{O}(\log n)$.

Conclusions

Responsive-Round Complexity

- A new measure for complexity
 - Variation of round complexity

A protocol for Concurrent ZK.

The protocol features:

- Effectively $\tilde{O}(\log n)$ rounds
- Good for the general concurrent model

References

- [Barak] Barak, B. (2001). How to get beyond black-box simulator barrier. In *Proceedings of FOCS 2001*.
- [Canetti-Killian-Petrank-Rosen] Canetti, R., Killian, J., Petrank, E., and Rosen, A. (2001). Concurrent zero-knowledge requires $\tilde{\Omega}(\log n)$ rounds. In *Proceedings of the thirty third annual ACM Symposium on Theory of Computing*. ACM Press.
- [Dwork-Naor-Sahai] Dwork, C., Naor, M., and Sahai, A. (1998). Concurrent zero-knowledge. In ACM, editor, *Proceedings of the thirtieth annual ACM Symposium on Theory of Computing: Dallas, Texas, May 23–26, 1998*, pages 409–418, New York, NY, USA. ACM Press.

References (cont'd)

- [Goldreich-Micali-Wigderson] Goldreich, O., Micali, S., and Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *JACM*, 38(3):690–728.
- [Goldreich-Oren] Goldreich, O. and Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32.
- [Goldwasser-Micali-Rackoff] Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive systems. *SIAM Journal of Computing*, 18(1):186–208.

References (cont'd)

- [Kilian-Petrank] Kilian, J. and Petrank, E. (2001). Concurrent zero-knowledge in poly-logarithmic rounds. In *Proceedings of the thirty third annual ACM Symposium on Theory of Computing*. ACM Press.
- [Richardson-Kilian] Richardson, R. and Kilian, J. (1999). On the concurrent composition of zero-knowledge proofs. *Lecture Notes in Computer Science*, 1592:415–431.