Equivalence of Uniform Key Agreement and Composition Insecurity

Chongwon Cho Chen-Kuei Lee Rafail Ostrovsky

UCLA

Plan

- Main Question:
  - hardness amplification via composition
- Previous Works
- Our main result
- Conclusions

Types of Compositions

- Parallel Composition
  Let F and G be functions with the same domain and range. Parallel composition of F and G is defined as P(·):

  $$P(\cdot) = F(\cdot) \text{ XOR } G(\cdot)$$

Types of Compositions

- Parallel Composition
  Let F and G be functions with the same domain and range. Parallel composition of F and G is defined as P(·):

  $$P(\cdot) = F(\cdot) \text{ XOR } G(\cdot)$$

- Instead of Z_2 can define over other groups.

Types of Compositions

- Parallel Composition
  Let F and G be functions with the same domain and range. Parallel composition of F and G is defined as P(·):

  $$P(\cdot) = F(\cdot) \text{ XOR } G(\cdot)$$

- Instead of Z_2 can define over other groups.

- Sequential Composition
  Let F and G be functions with the same domain and range. Sequential composition of F and G is defined as S(·):

  $$S(\cdot) = G(F(\cdot))$$

Security Amplification via Composition

- Does **composition** of Non-adaptively secure PRF (unconditionally) implies adaptive security?
  - - In an information-theoretic setting?
  - - In a computational setting?
    - If not, under what assumptions?

Security Amplification via Composition

- Does **composition** of Non-adaptively secure PRF (unconditionally) implies adaptive security?
  - - In an information-theoretic setting?
  - - In a computational setting?
    - If not, under what assumptions?

- A lot is known already, lets review…
  [LR86], [Vaud03], [MP 04], [Piet05], [Piet06]

Previous Works

- Information Theoretic Setting
  - **Vaudenay [Vaud 03]** showed the sequential composition of k non-adaptively ε-secure Permutation implies $2^{k-1}\varepsilon^{k}$ adaptive security.

Previous Works

- Information Theoretic Setting
  - **Vaudenay [Vaud 03]** showed the sequential composition of k non-adaptively ε-secure Permutation implies $2^{k-1}\varepsilon^k$ adaptive security.
  - **Luby and Rackoff [LR86]** showed the parallel composition of k ε-secure functions implies $2^{k-1}\varepsilon^k$ adaptive security.

Previous Works (Cont)

- Information Theoretic Setting
- **Maurer and Pietrzak [MP 04]** showed for permutations that composition of 2 ε-secure non-adaptive permutations implies $2\varepsilon(1+\ln(\varepsilon^{-1}))$ secure adaptive permutation.

Previous Works (Cont)

- Information Theoretic Setting
- **Maurer and Pietrzak [MP 04]** showed for permutations that composition of 2 ε-secure non-adaptive permutations implies $2\varepsilon(1+\ln(\varepsilon^{-1}))$ secure adaptive permutation.

- Computational Setting

  Pietrzak [Piet05] showed:

  - DDH ➔ composition does not help, i.e.:
  - If ***DDH*** assumption holds, then the composition of non-adaptively secure functions is **not** adaptively secure (i.e. 3 adaptive-query breakable)!

Previous Works (Cont.)

- **Pietrzak [Piet06]**:
  - *If* sequential composition does not help (for PRF) ➔ there exists Key-agreement
  - If the *sequential* composition of k-adaptively secure functions is not k+1 adaptively secure, then there exists a (2k-1)-pass key agreement.
  - In fact, the above construction of key agreement implies uniform transcript key agreement.
  - If sequential composition does not help ➔ uniform-transcript Key-agreement

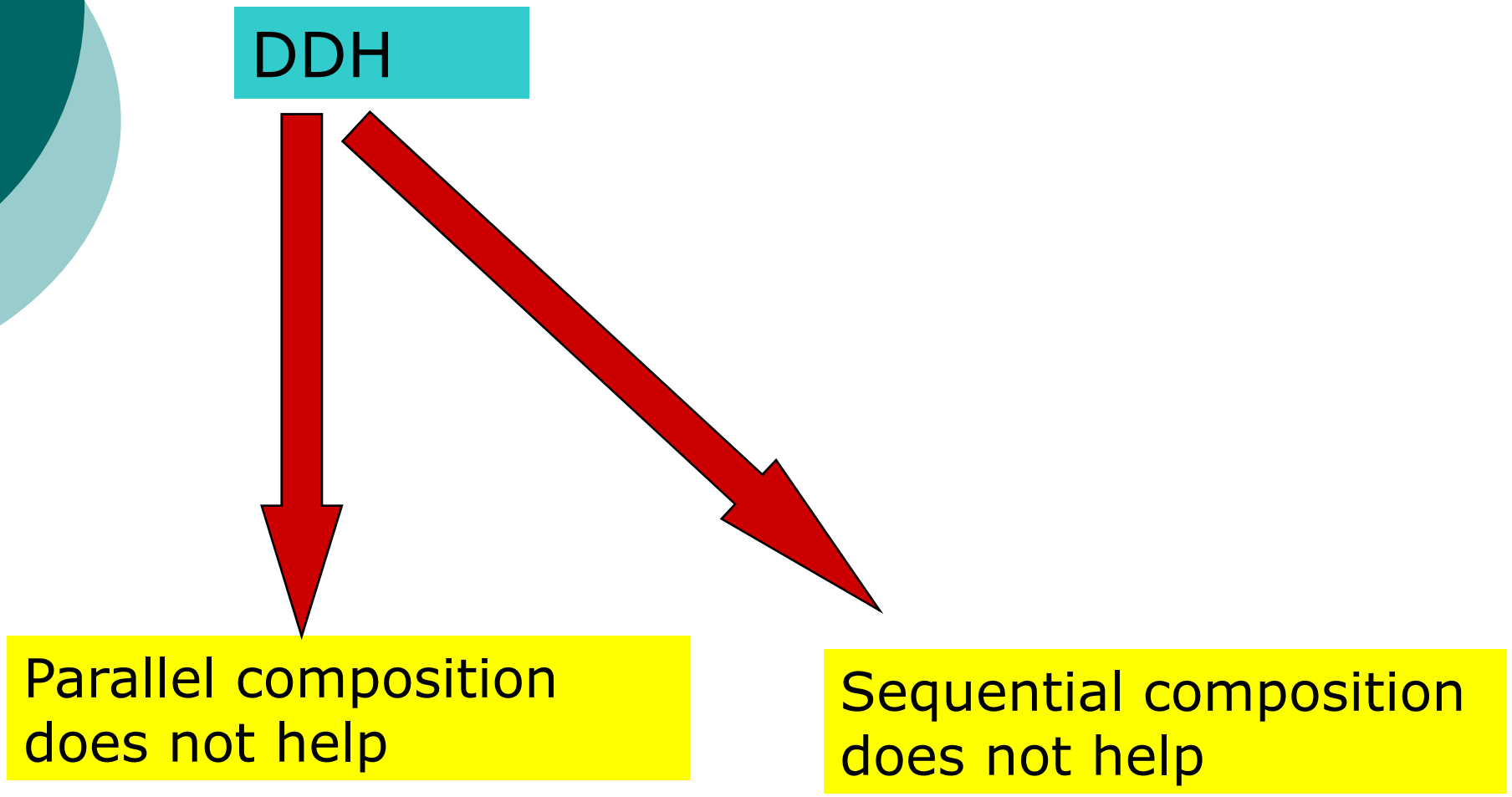
Summary of [Piet05] and [Piet06]:

DDH

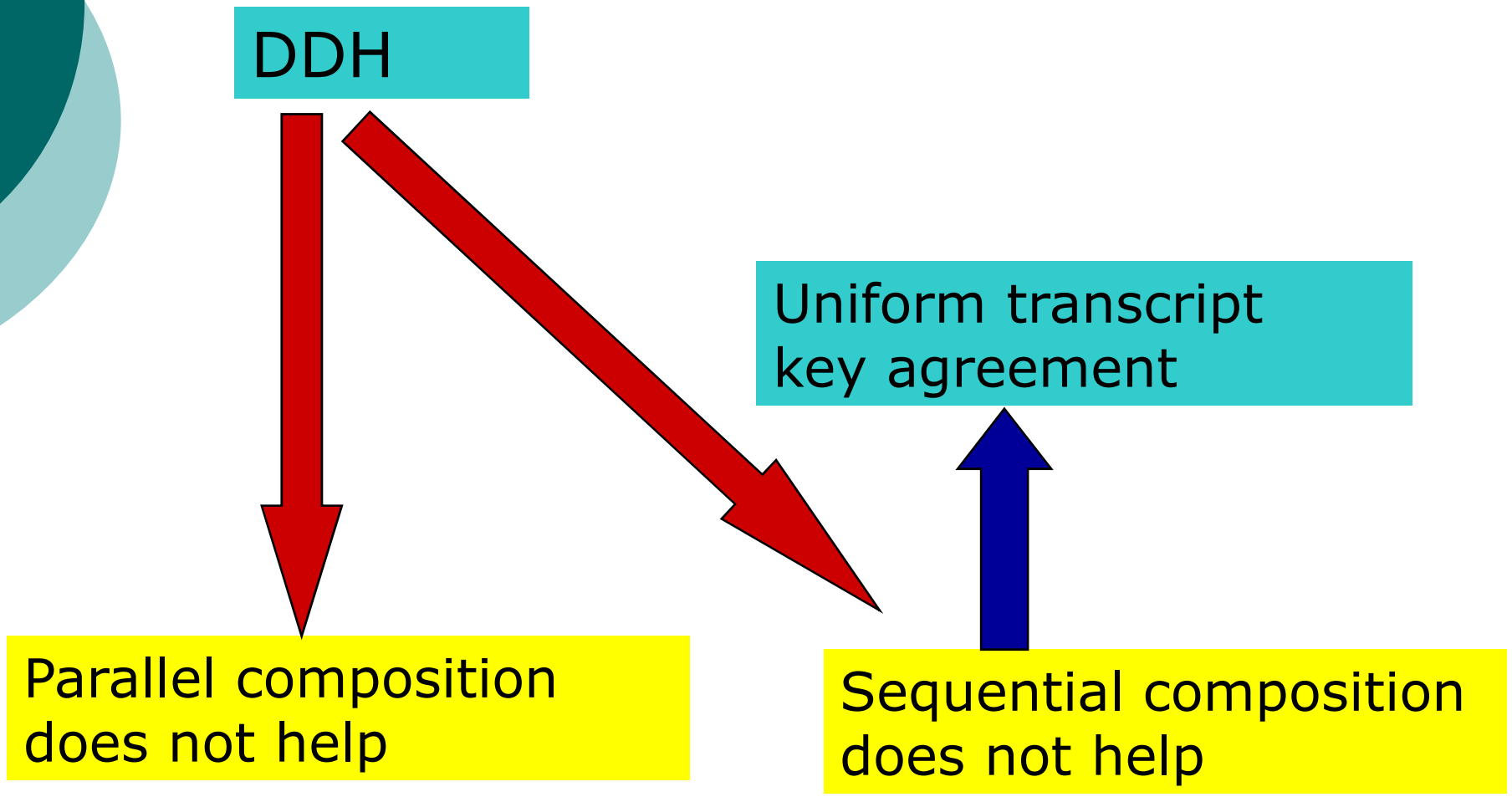
Parallel composition does not help

Sequential composition does not help

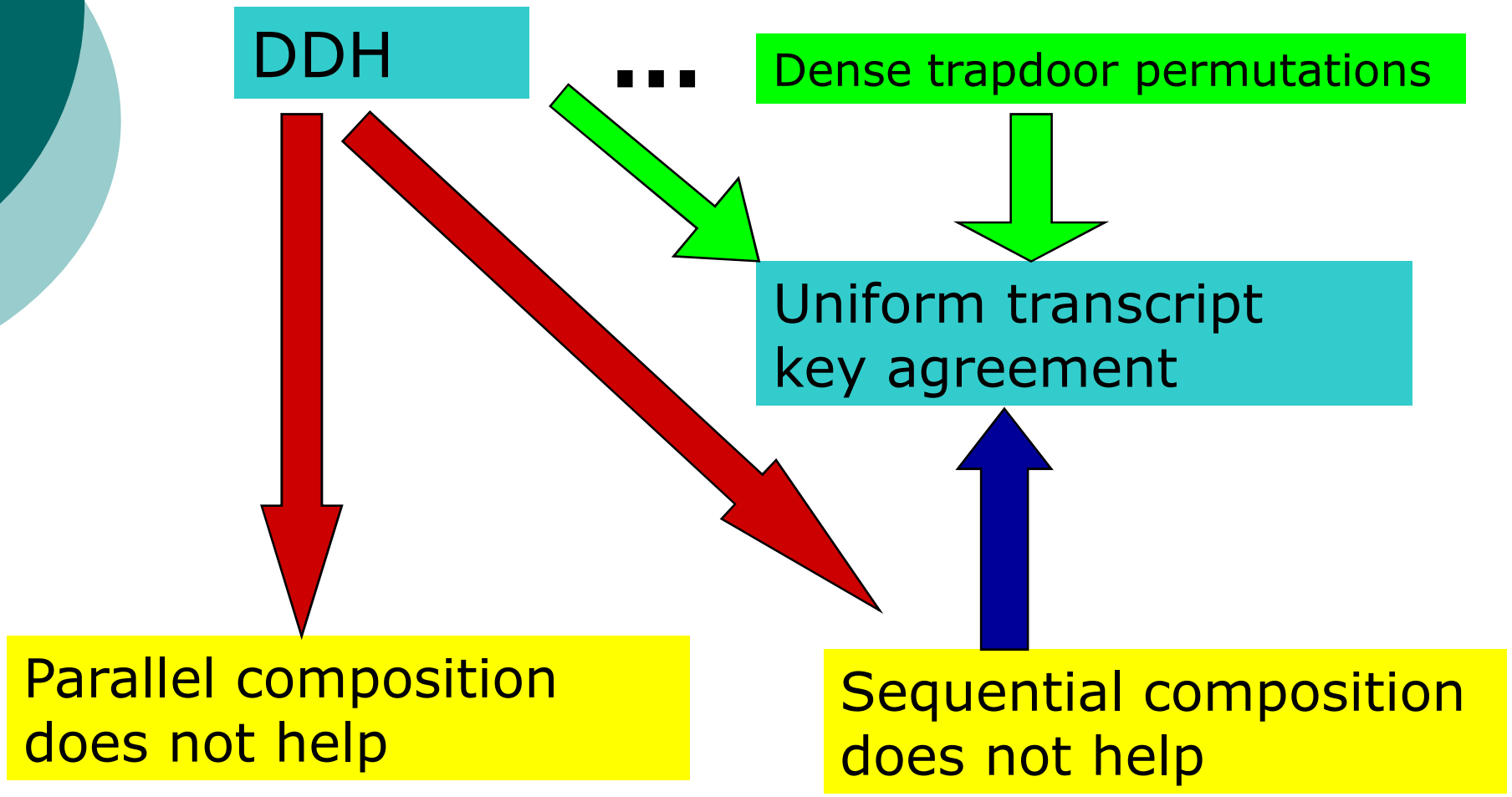
Summary of [Piet05] and [Piet06]:



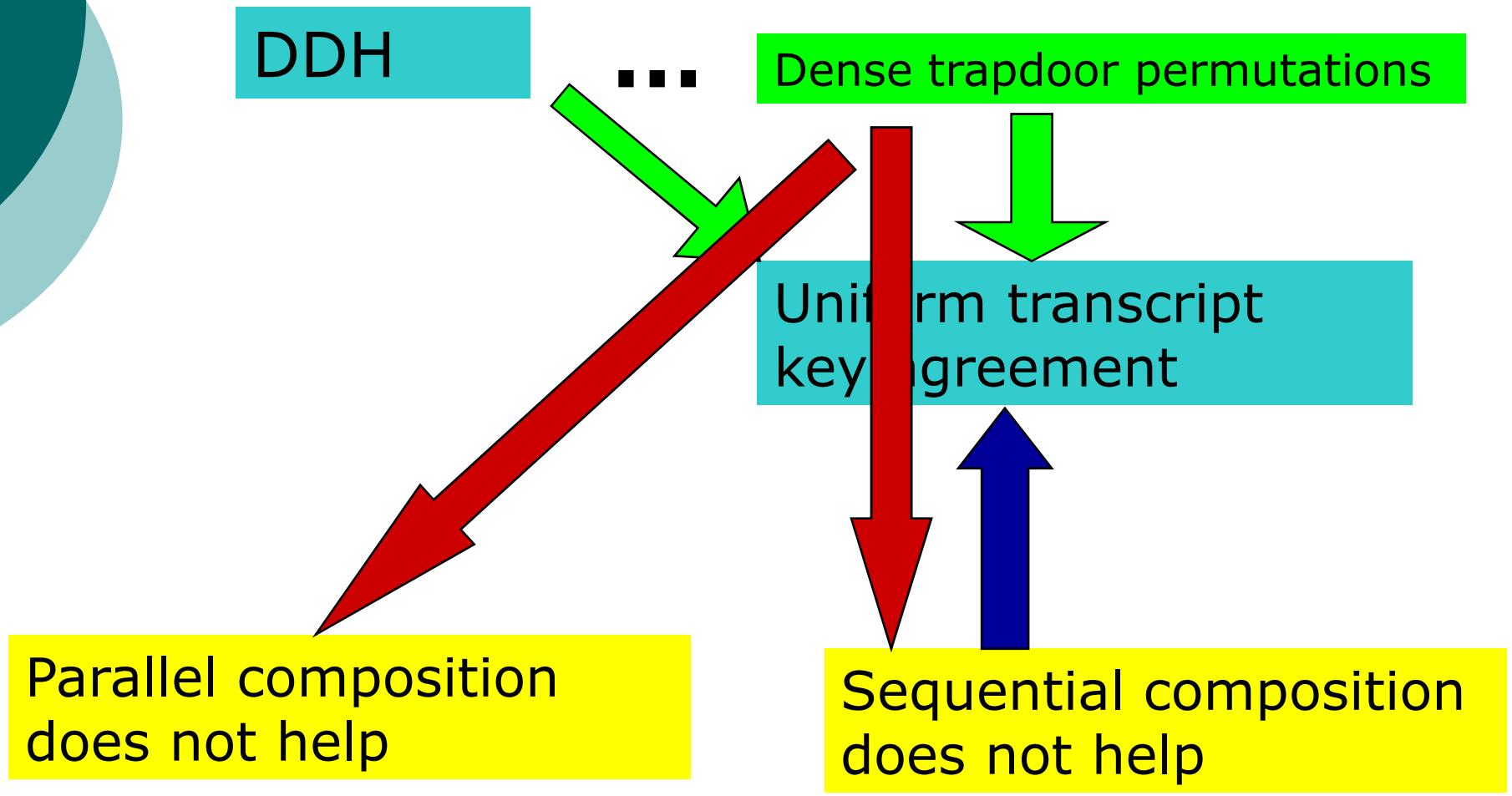
Summary of [Piet05] and [Piet06]:



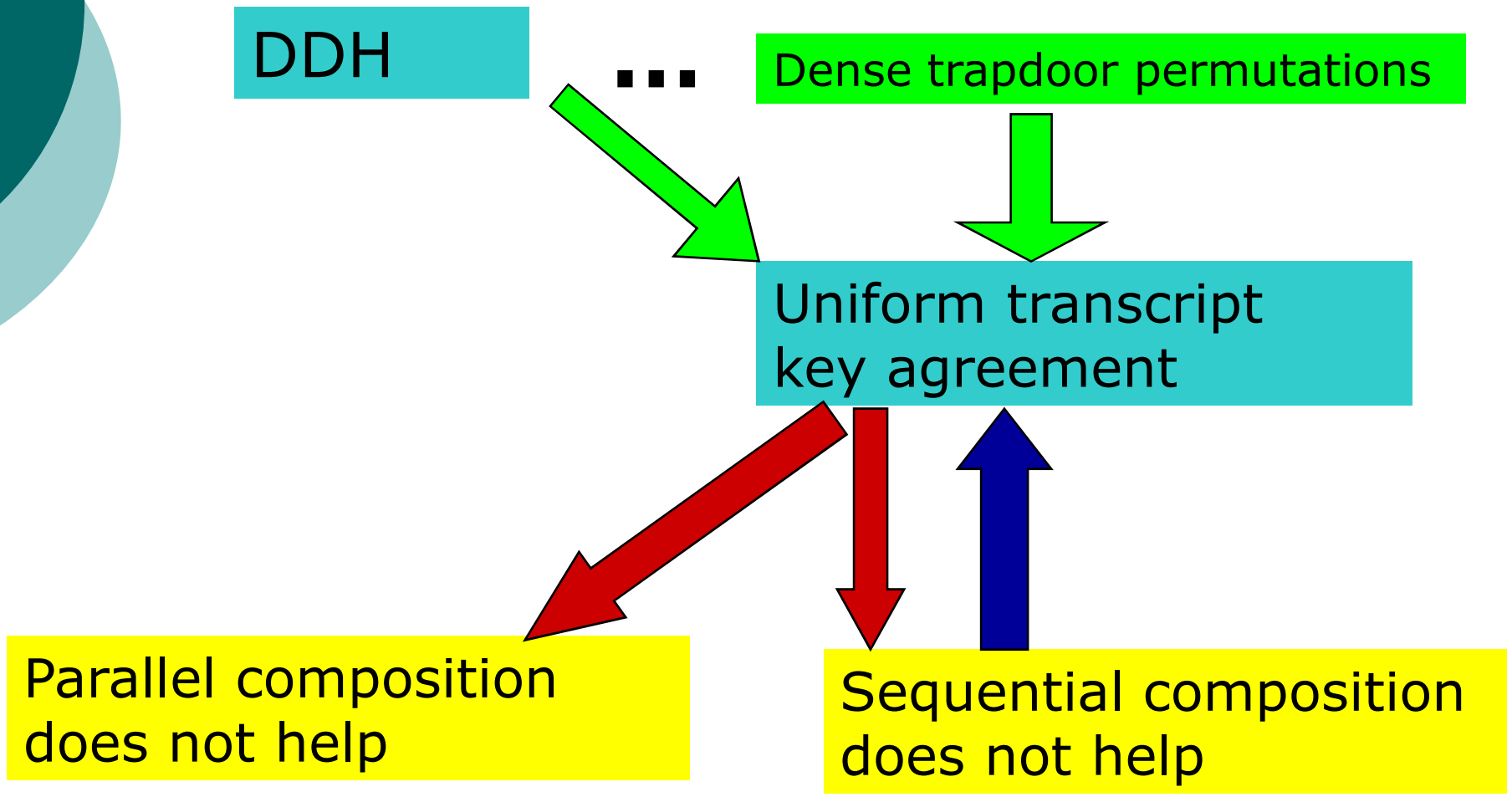
What else do we know?



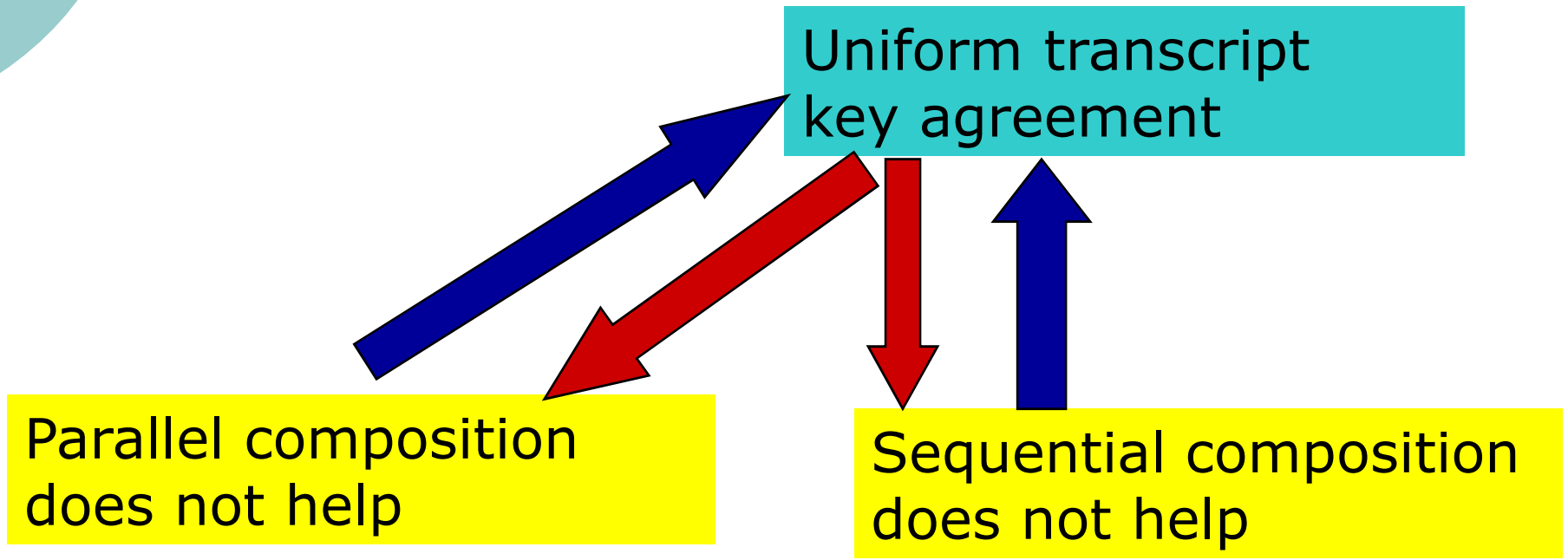
Wishful thinking…



Wishful thinking…



THIS IS EXACTLY WHAT WE DO



THIS IS EXACTLY WHAT WE DO

Uniform transcript key agreement

Parallel composition does not help

Sequential composition does not help

THIS IS EXACTLY WHAT WE DO

Public Key World

Uniform transcript
key agreement

Parallel composition
does not help

Sequential composition
does not help

Private Key World

THIS IS EXACTLY WHAT WE DO

Uniform transcript
key agreement

Parallel comp
does not help

composition
elp

Private Key World

Our Result

- **Main Thm:** **Both sequential and parallel composition of two pseudo-random functions does not imply adaptive-security**

  if and only if

  a uniform-transcript key agreement exists.

Conclusion and Open Questions

- Composition Insecurity ←→ Uniform Transcript Key Agreement
- Round Complexity of UTKA is Linearly Proportional to the Adaptive Security of Compositions.
- Open: Tighter Relation between the security of component functions and the security of their compositions.