Weak Zero-Knowledge via the Goldreich-Levin Theorem

Dakshita Khurana (UIUC)
Giulio Malavolta (Bocconi University & MPI-SP)
Kabir Tomer (UIUC)

Open Problem: Round Optimal Zero Knowledge

- ZK with negligible soundness error (in the standard model)
  - Known in four rounds [FS90]
  - Impossible (outside BPP) in two rounds [GO94]
- What about three rounds?

Open Problem: Round Optimal Zero Knowledge

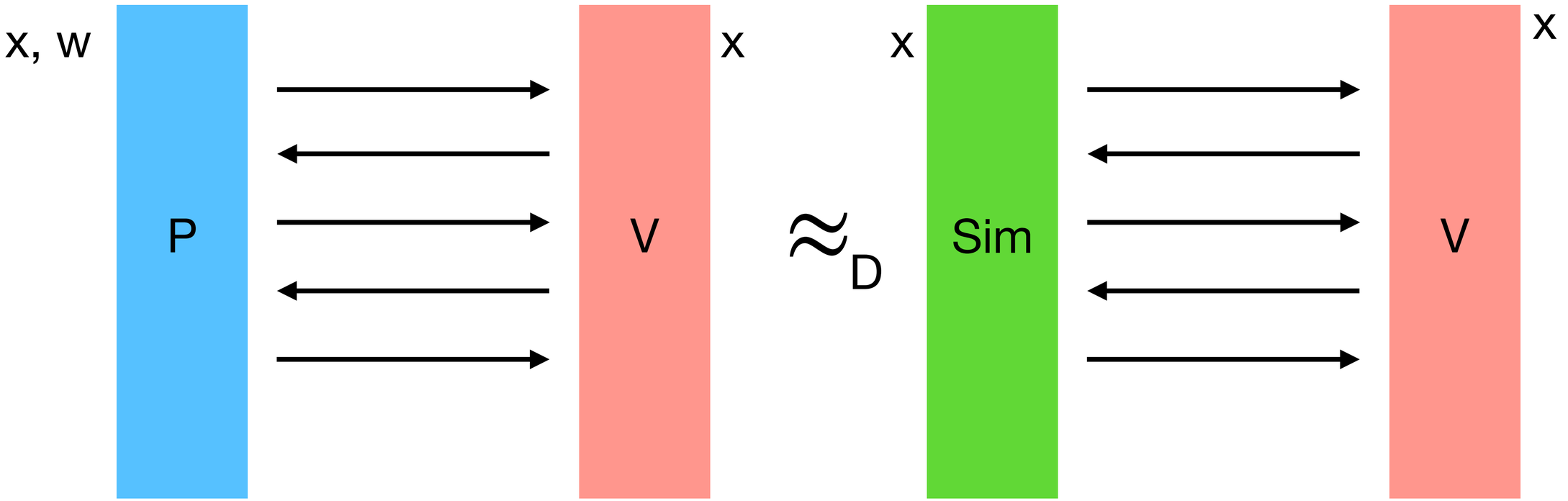
- ZK with negligible soundness error (in the standard model)
  - Known in four rounds [FS90]
  - Impossible (outside BPP) in two rounds [GO94]
- What about three rounds?
- Black-Box Barrier: Three round ZK with black-box simulation impossible outside BPP [GK96]

Bypassing the Barrier

- Known non black-box simulation techniques either:
  - Require four rounds
  - Achieve three rounds from non-standard assumptions
- Weaker notions of ZK?

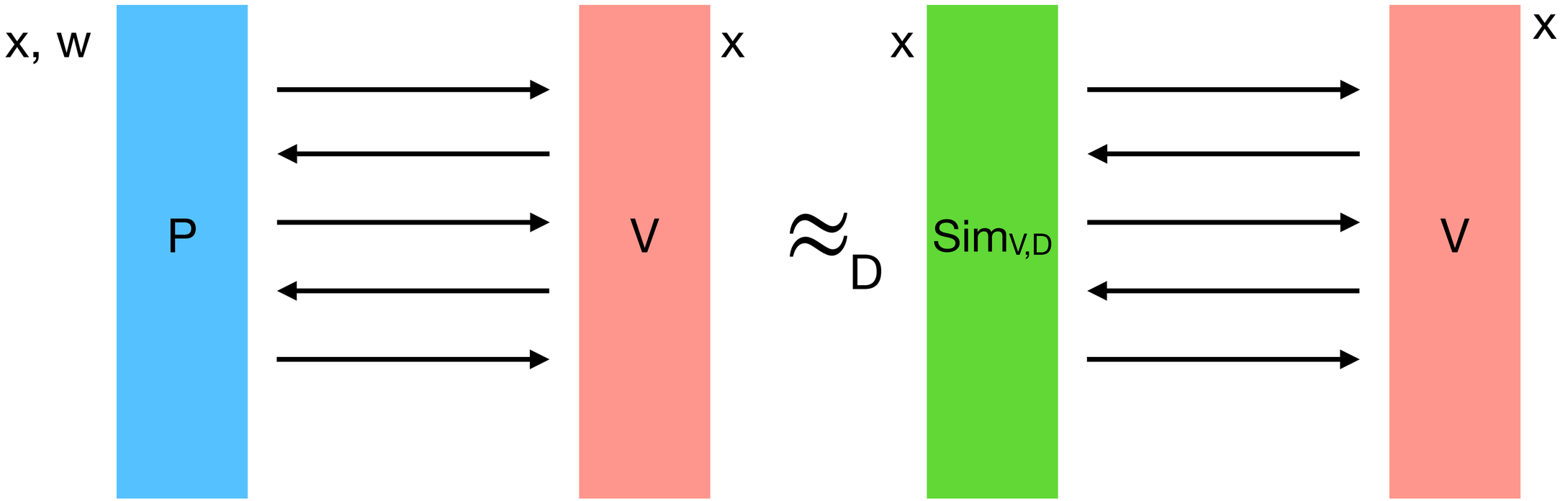
Standard Zero Knowledge

$\exists Sim$ s.t. $\forall V, D$:



Weak Zero Knowledge [DNRS03]

$\forall V, D, \exists Sim_{V,D}$:



Weak ZK is not really that weak

- ZK is typically used to enforce honest behavior
- Example: Commit to x and prove that x satisfies some property.
  - Commit to a vote and prove that it is to a valid candidate.
  - Commit to a bit several times in parallel and prove consistency.
- ZK Simulation is used to achieve indistinguishability based security
- Weak ZK also implies indistinguishability based security!

Weak ZK is not really that weak

- Weak Zero-Knowledge implies extremely useful notions such as:
  - Witness Hiding
  - Strong Witness Indistinguishability
  - Witness Indistinguishability
- In fact, WZK is the only known way to get strong WI and witness hiding.

Previous Constructions of 3-Round WZK

- Non Black-Box Techniques:
  - From Unleveled FHE [BKP22]

- Non-Adaptive Setting (V's challenge does not depend on x):
  - From Random Self-Reducible PKE [implicit in BKP22]
  - From Statistically Sender-Private OT [JKKR17]
  - From Factoring [Den20]

Previous Constructions of 3-Round WZK

- Non Black-Box Techniques:
  - From Unleveled FHE [BKP22]
- Non-Adaptive Setting (V's challenge does not depend on x):
  - From Random Self-Reducible PKE [implicit in BKP22]
  - From Statistically Sender-Private OT [JKKR17]
  - From Factoring [Den20]

All require encryption with some homomorphic structure!

Our Goal:

Understand which generic assumptions imply Weak Zero-Knowledge

Our Results:

Three-Round WZK from Trapdoor Permutations

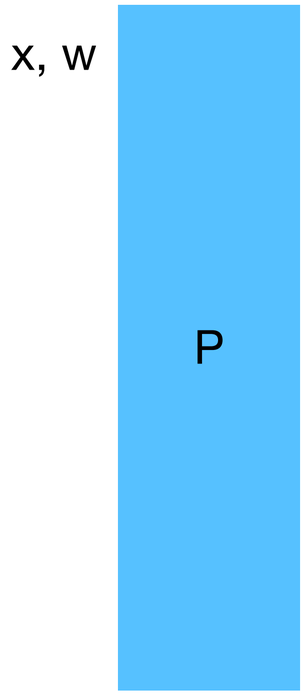
Our Results (Precisely):

Non-Adaptive Distributional Three-Round WZK from Doubly-Enhanced Injective TDFs

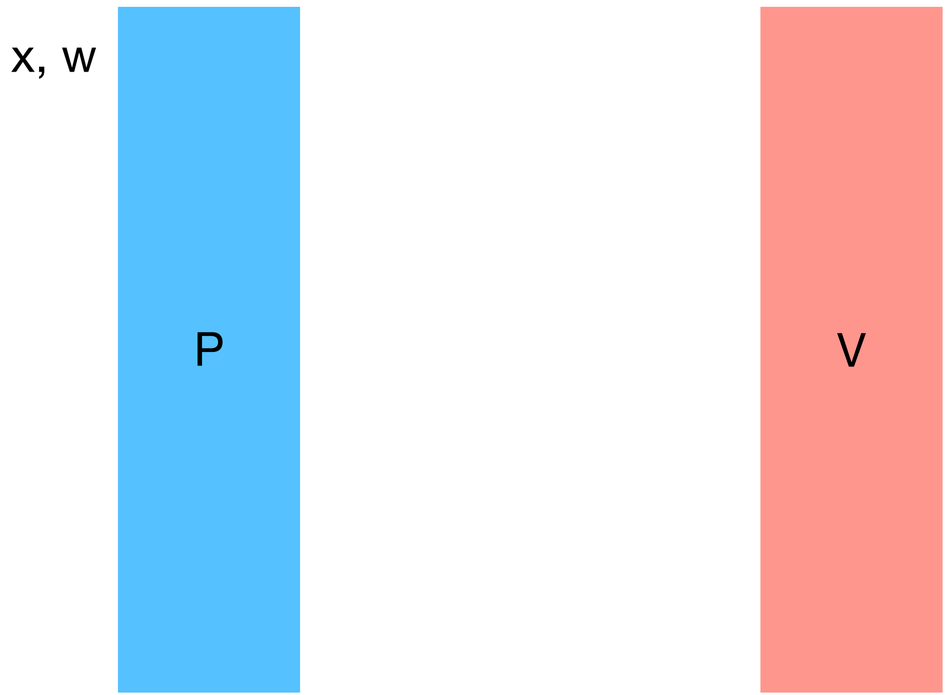
Key Idea

- Proof system for $x \in L$ such that verification requires a trapdoor.
- Without the trapdoor, real and fake proofs look the same!
- If the adversary does not check proofs, it can be fooled using fake proofs.
- If the adversary checks proofs, simulator extracts the trapdoor.

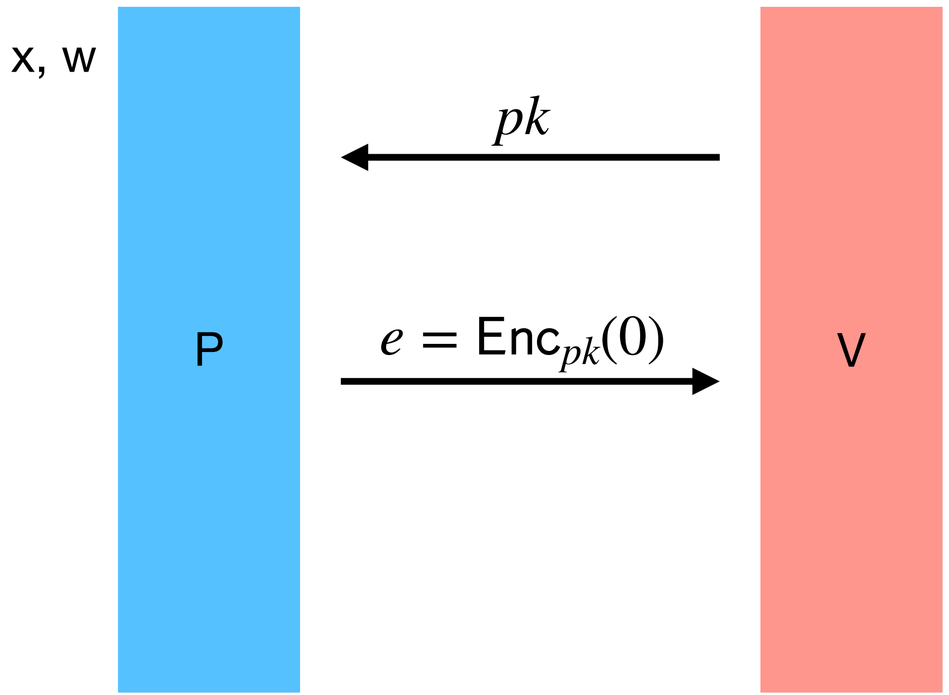
Verification that requires a trapdoor



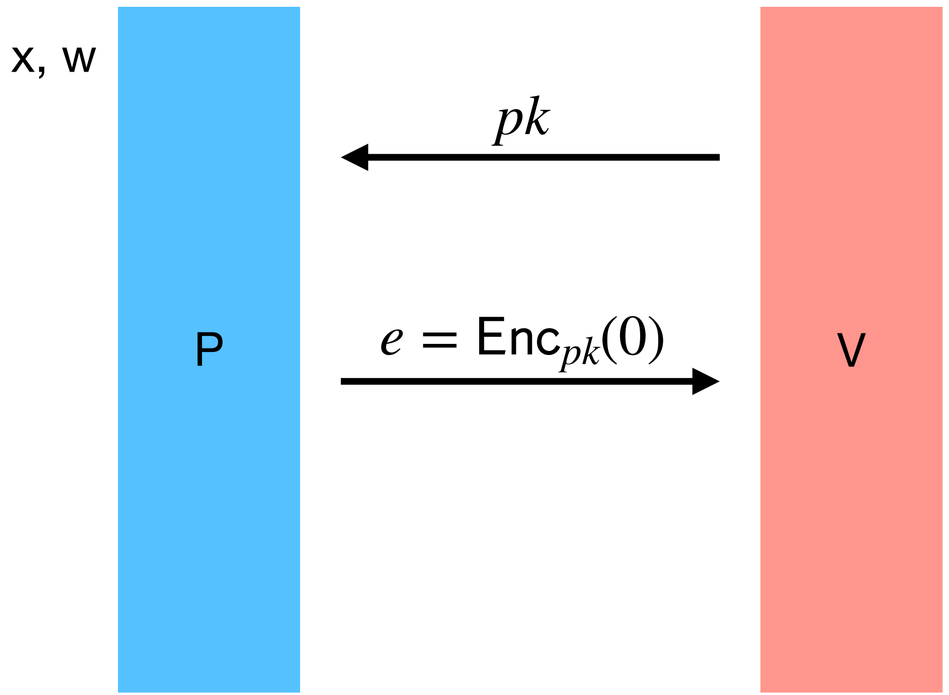
Verification that requires a trapdoor



Verification that requires a trapdoor

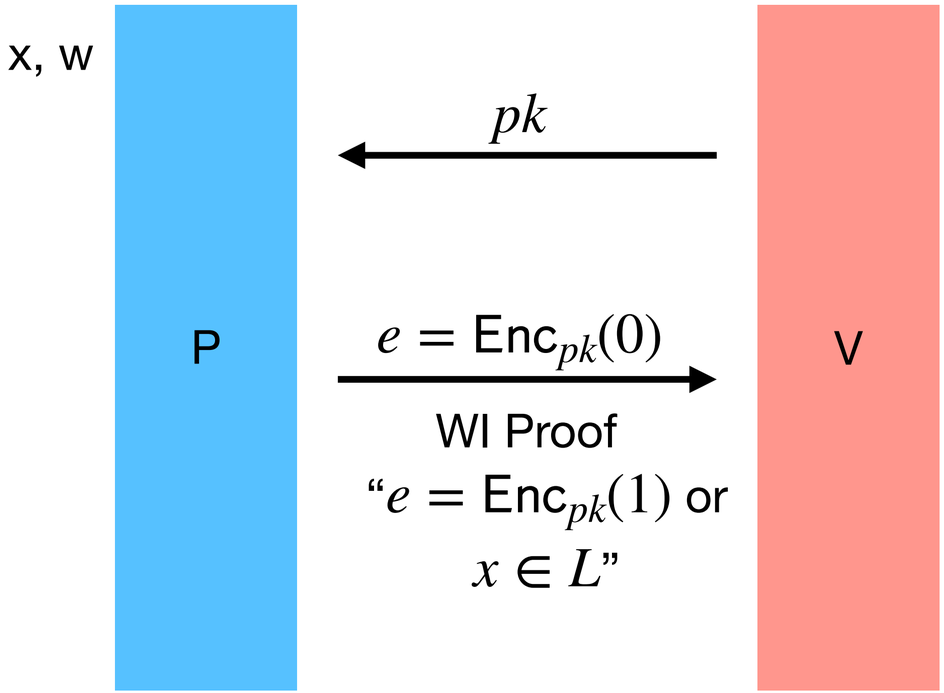


Verification that requires a trapdoor



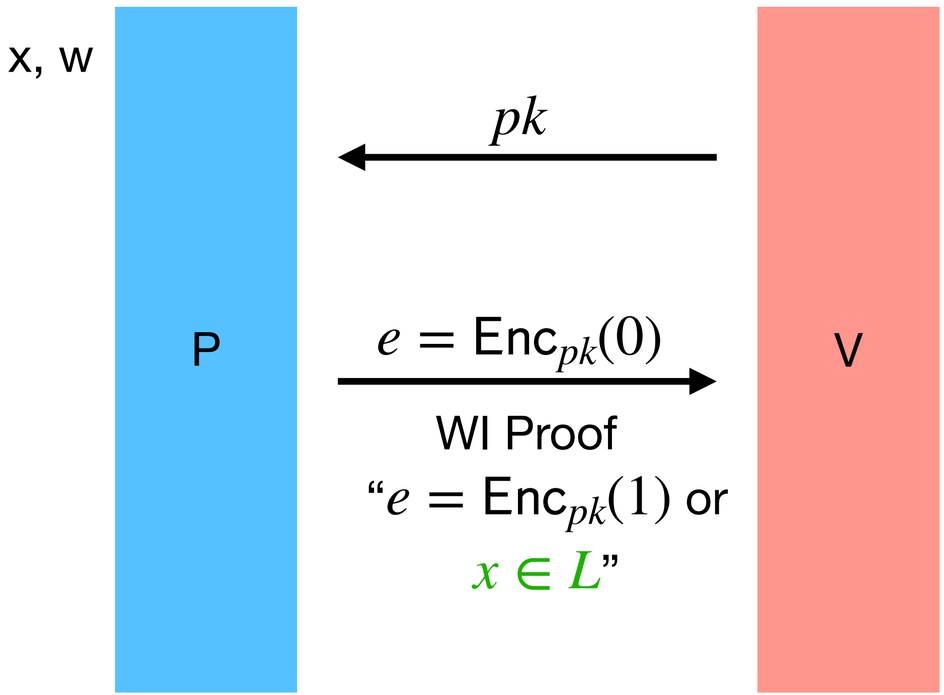
Decryption requires the secret trapdoor known by the verifier

Verification that requires a trapdoor



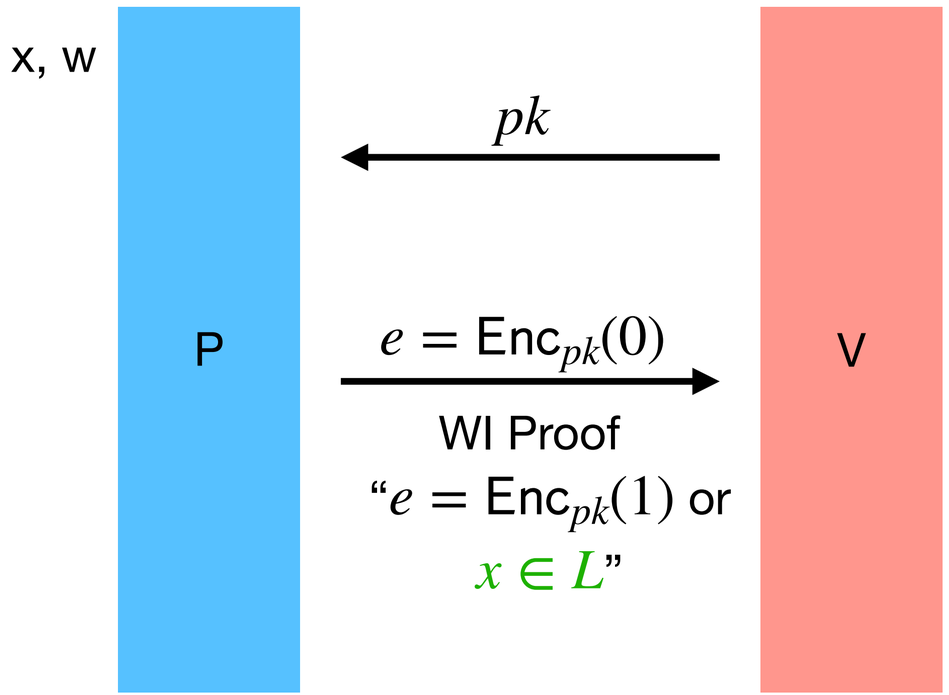
Decryption requires the secret trapdoor known by the verifier

Verification that requires a trapdoor

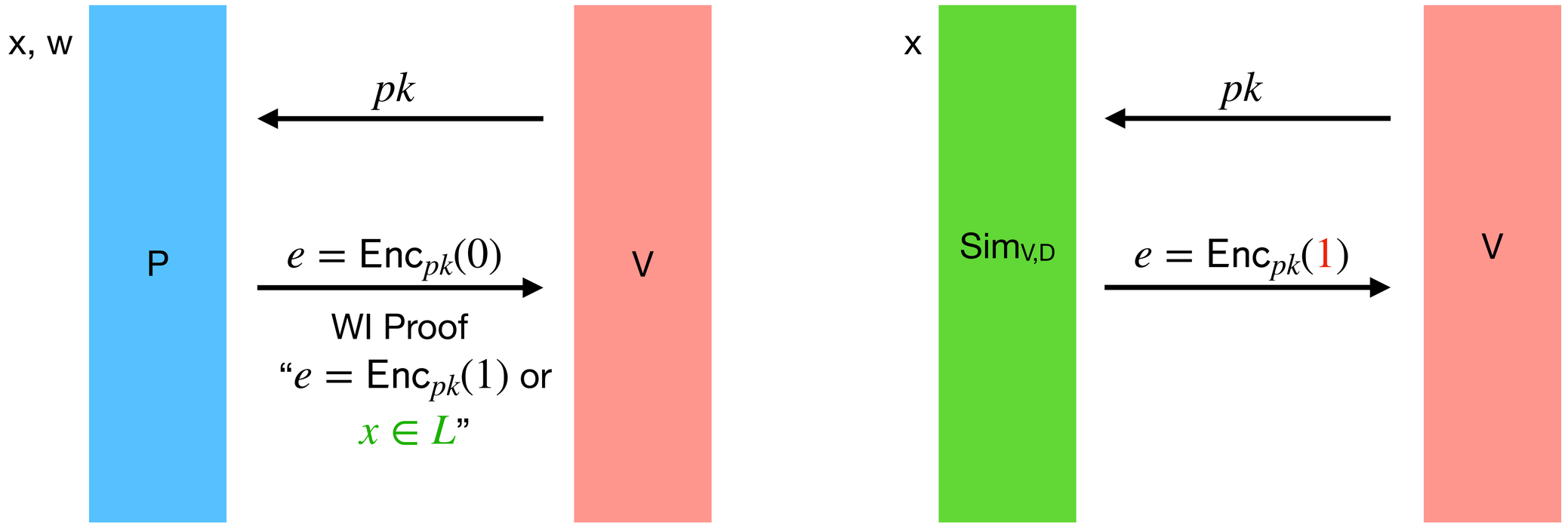


Decryption requires the secret trapdoor known by the verifier

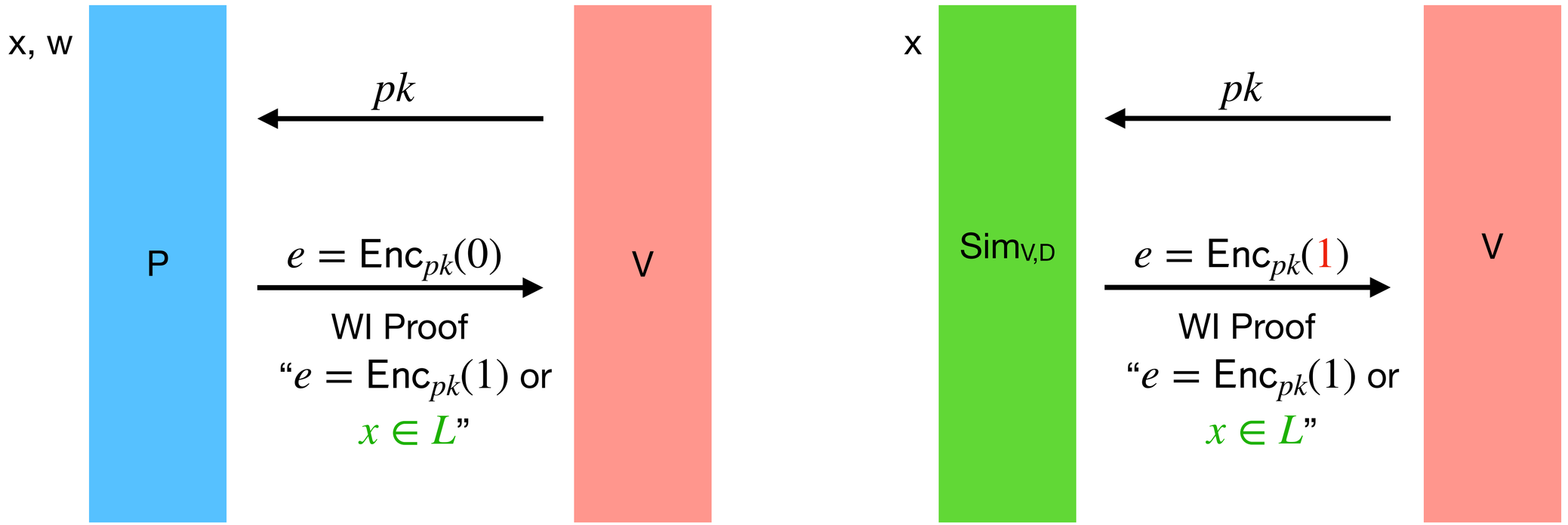
Suppose D does not check the encryption



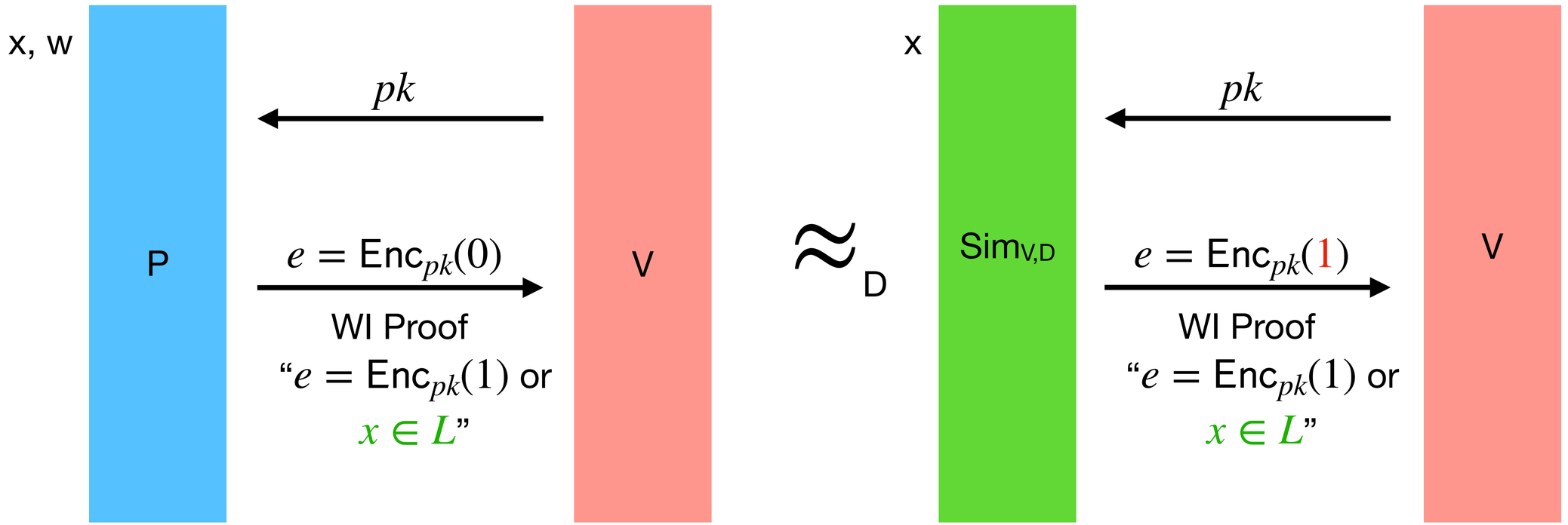
Suppose D does not check the encryption



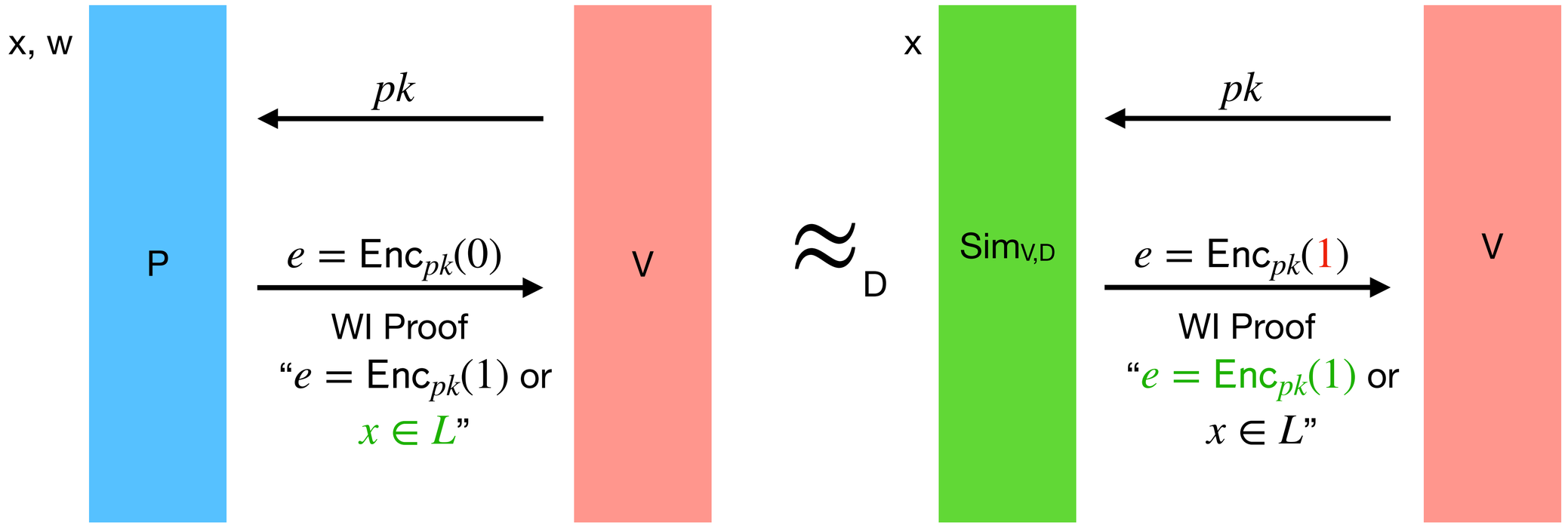
Suppose D does not check the encryption



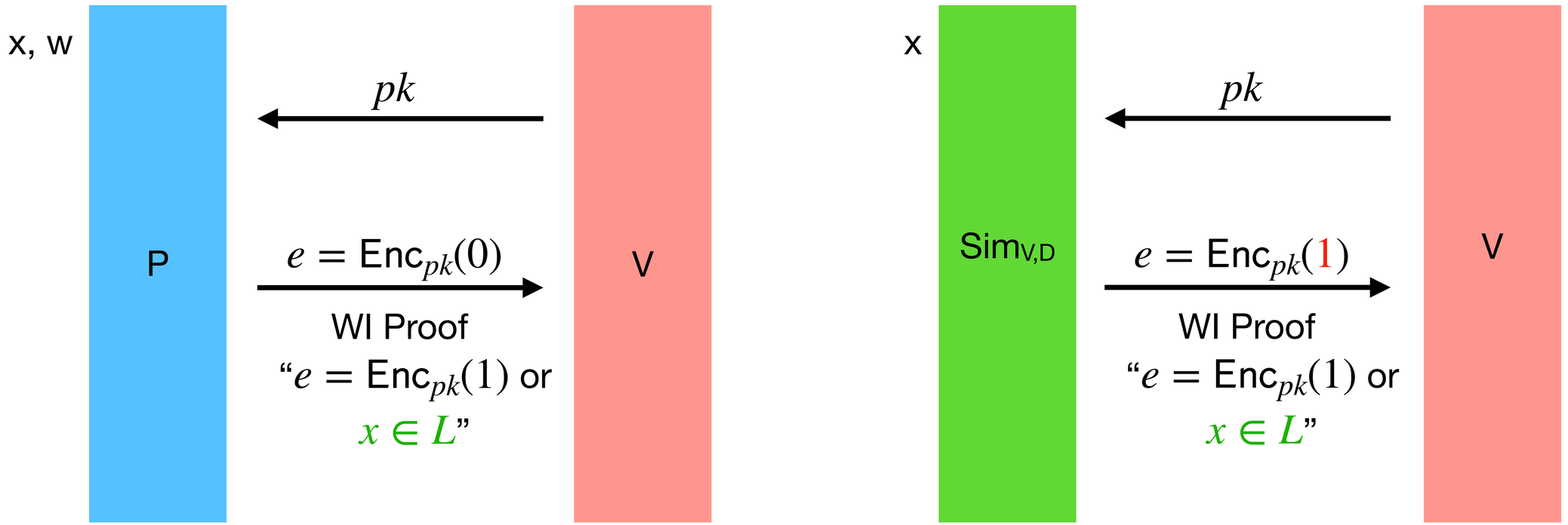
Suppose D does not check the encryption



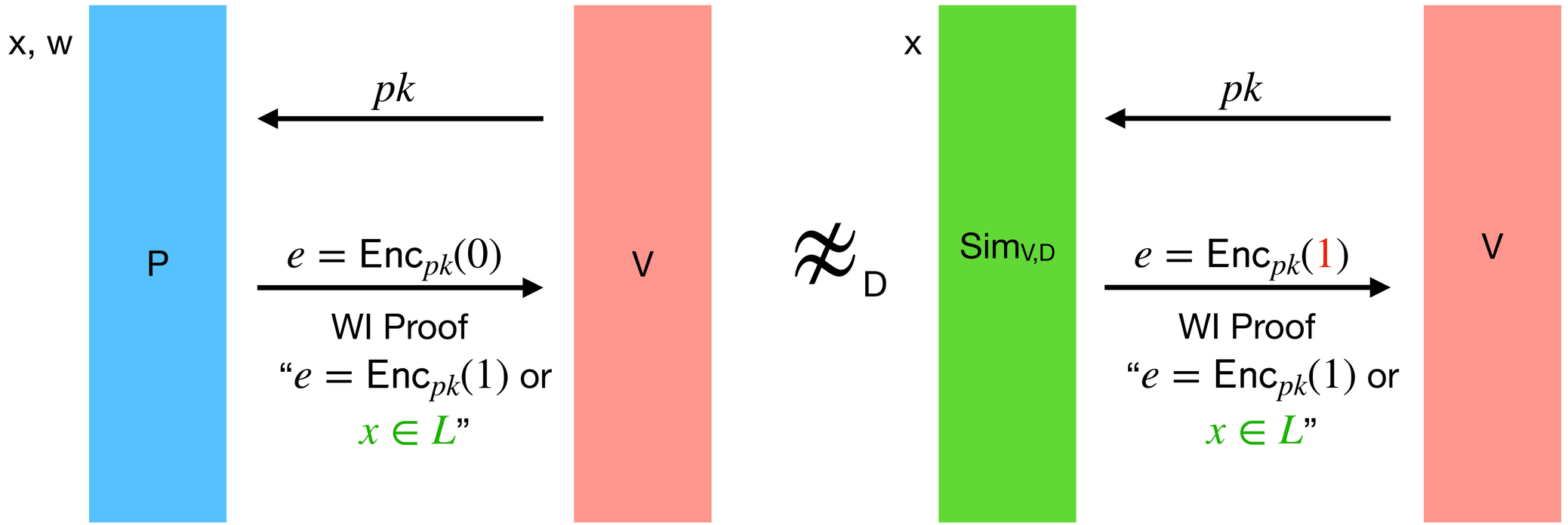
Suppose D does not check the encryption



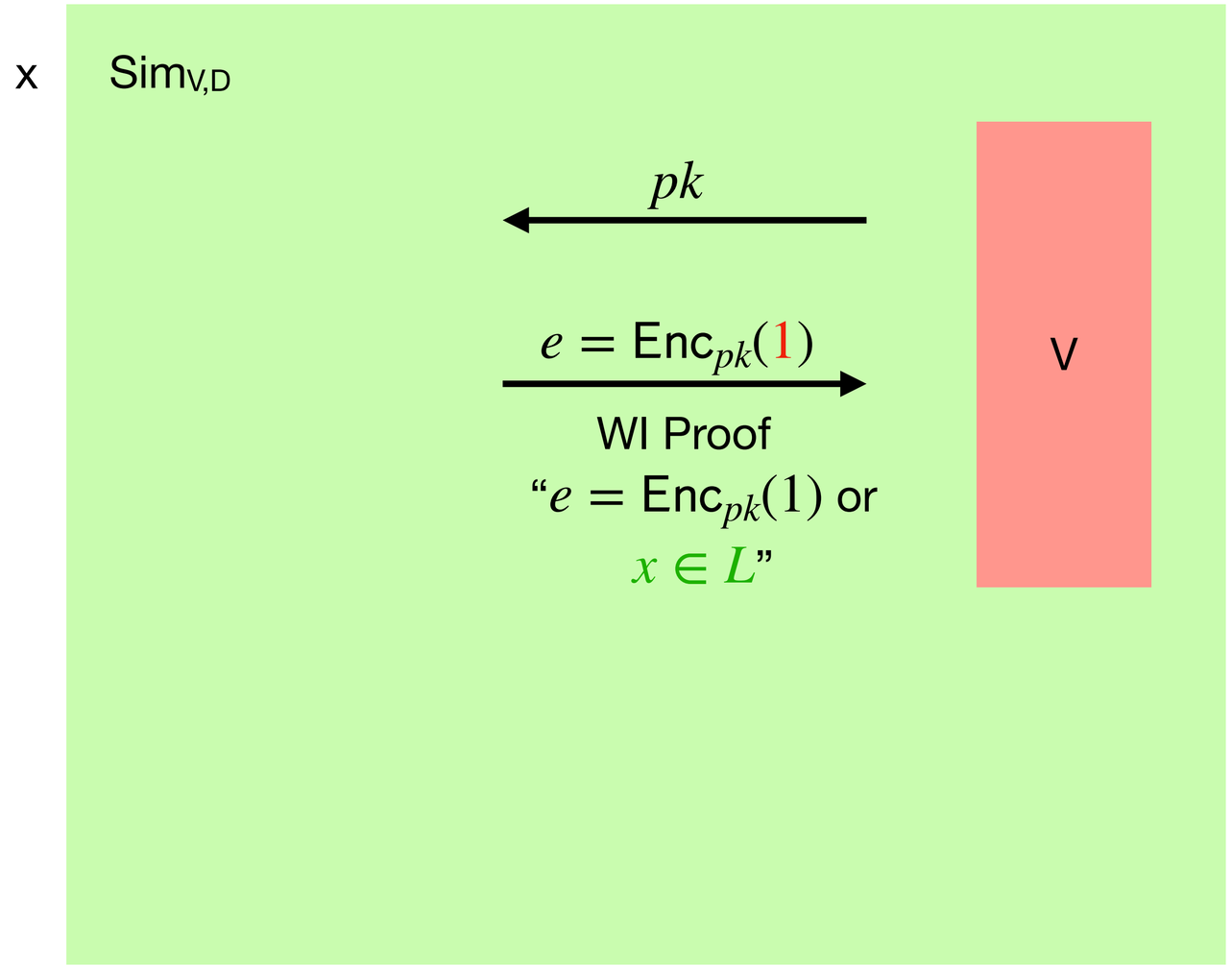
What if D uses the trapdoor to decrypt?



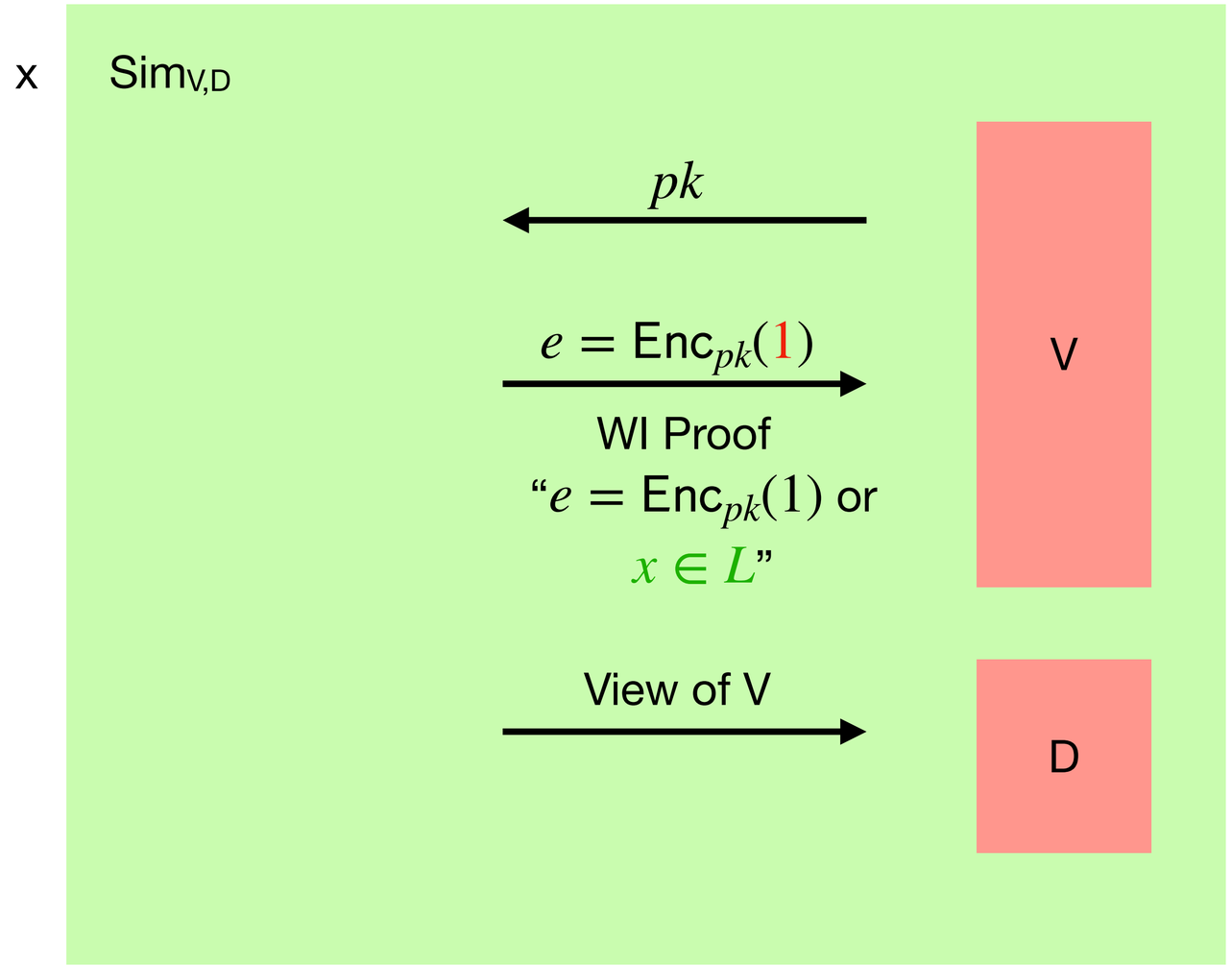
What if D uses the trapdoor to decrypt?



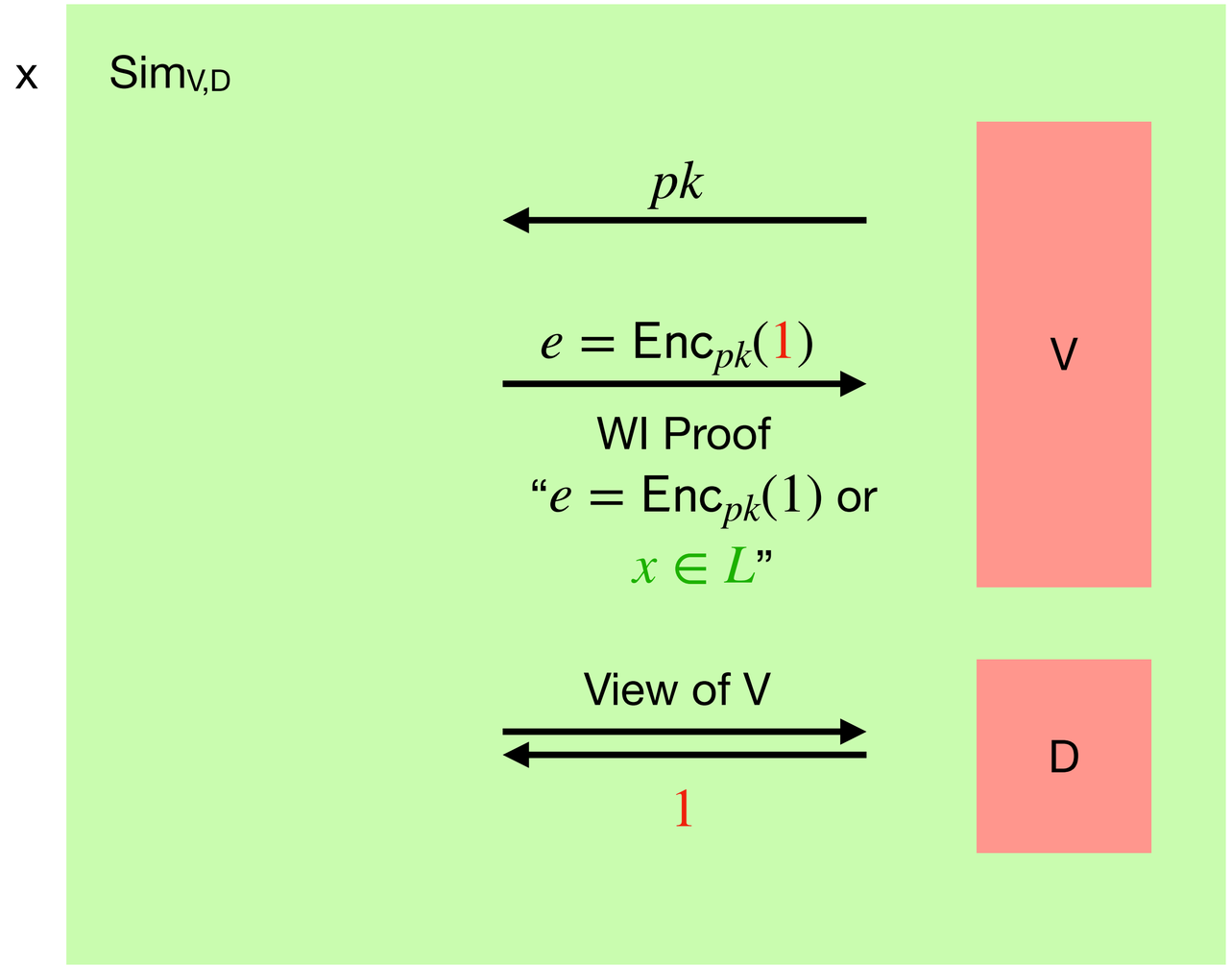
Using D to our advantage



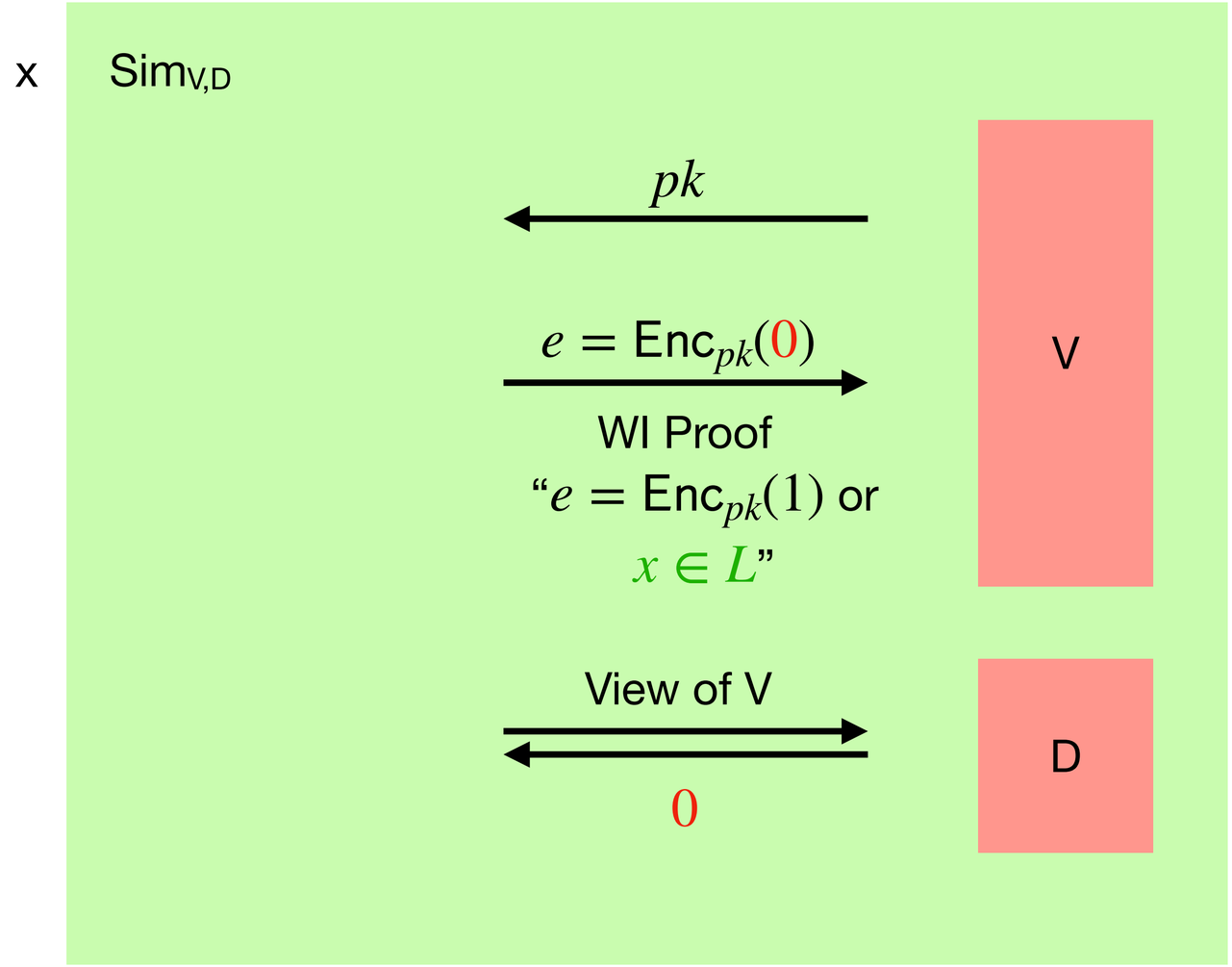
Using D to our advantage



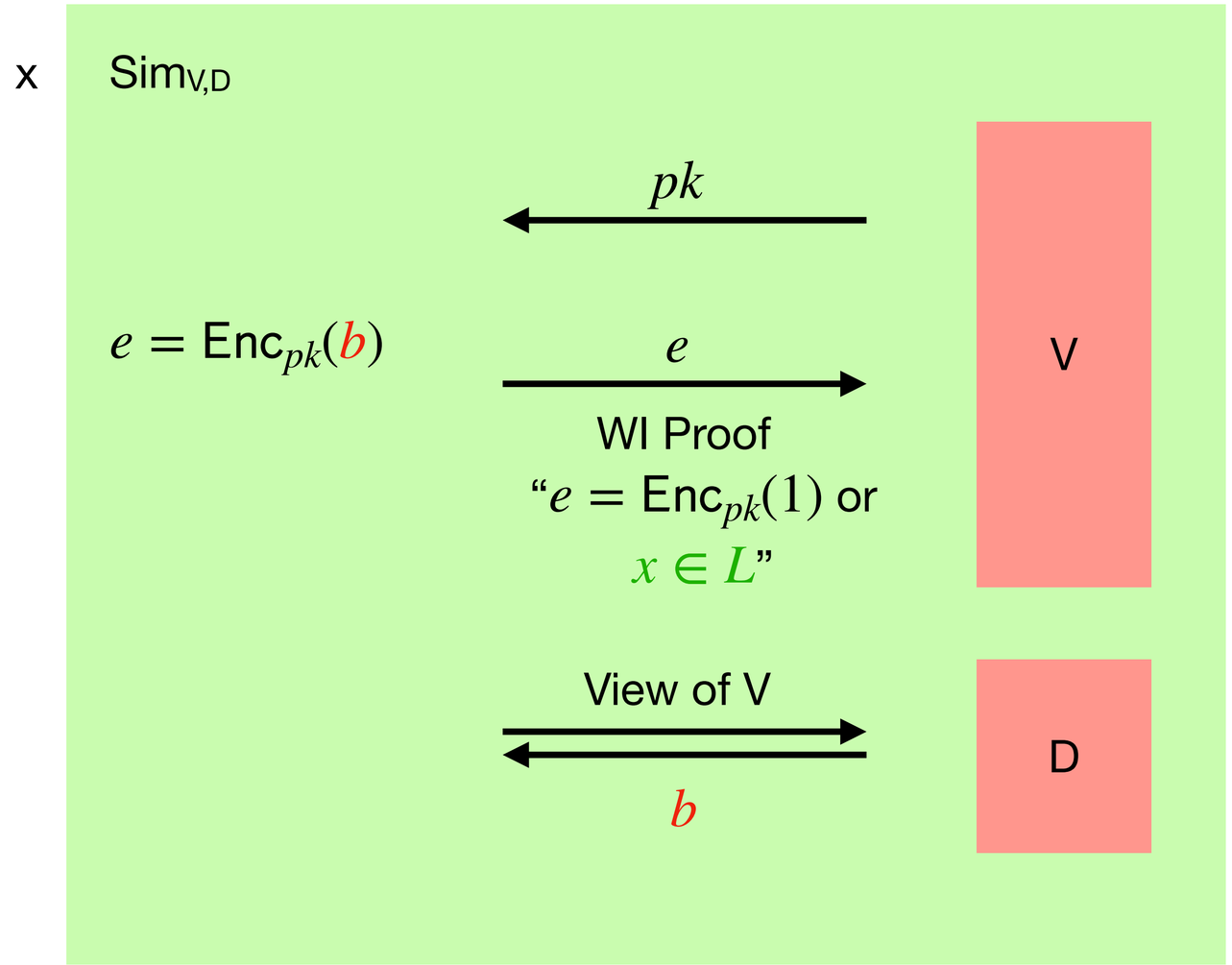
Using D to our advantage



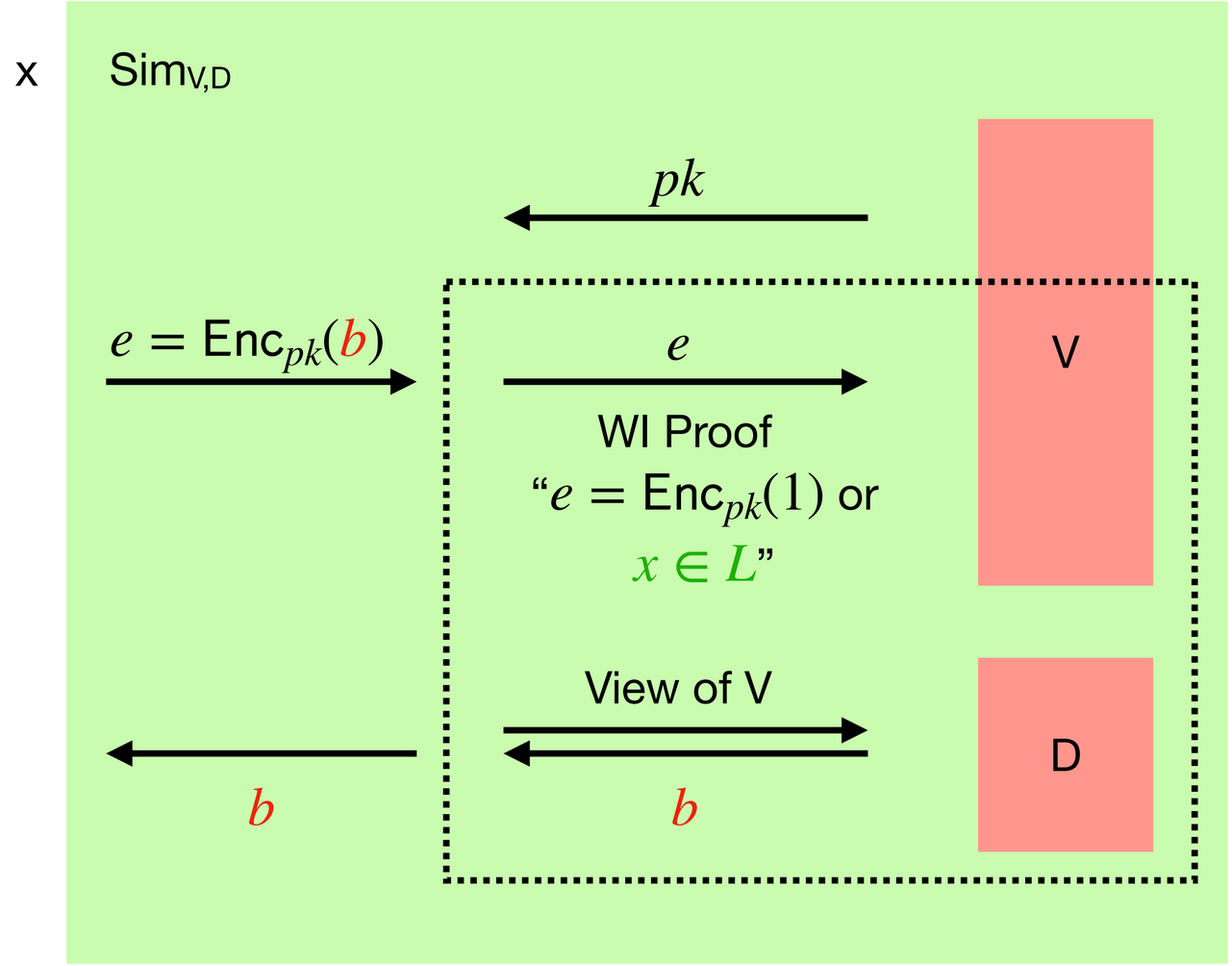
Using D to our advantage



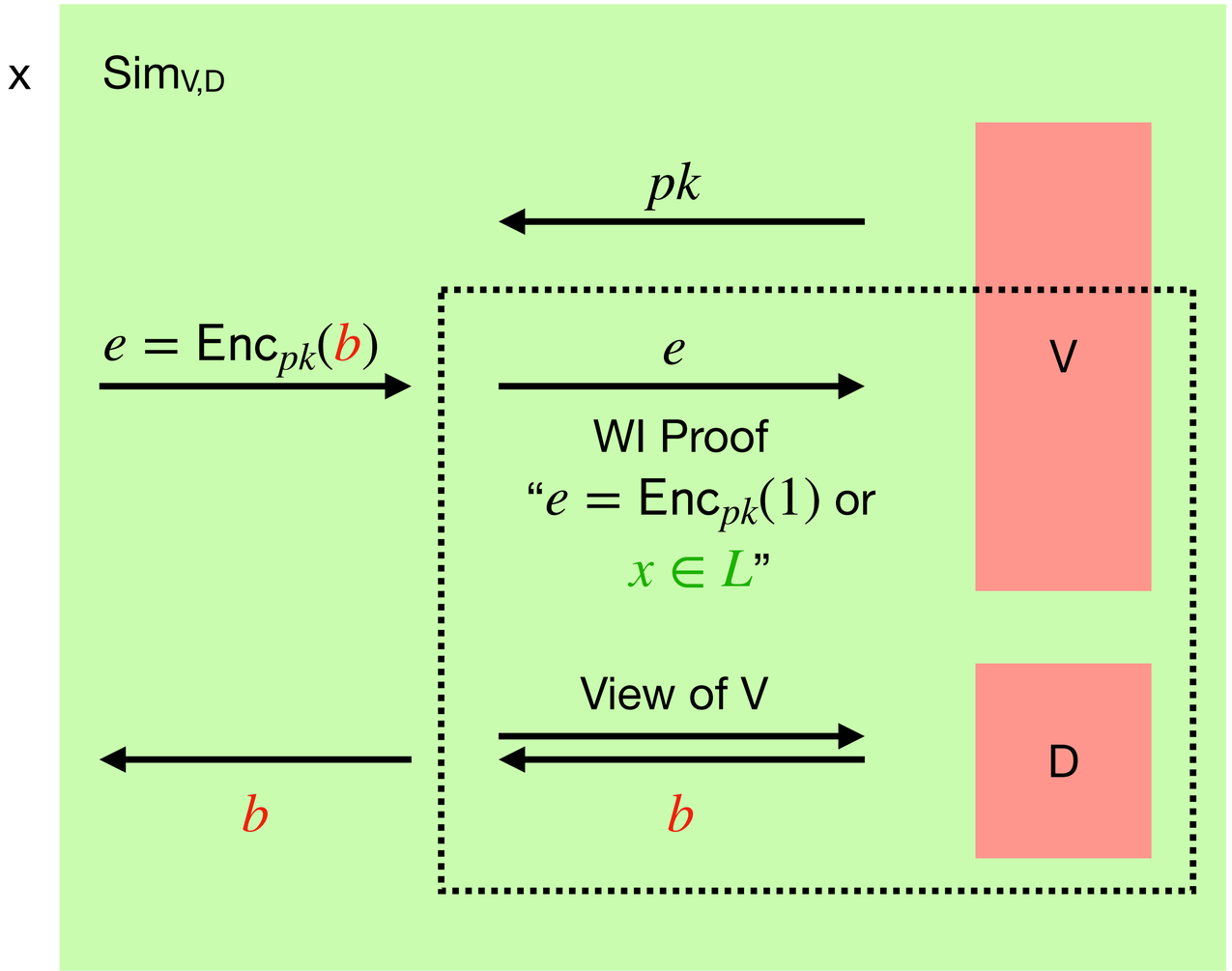
Using D to our advantage



Using D to our advantage



Using D to our advantage



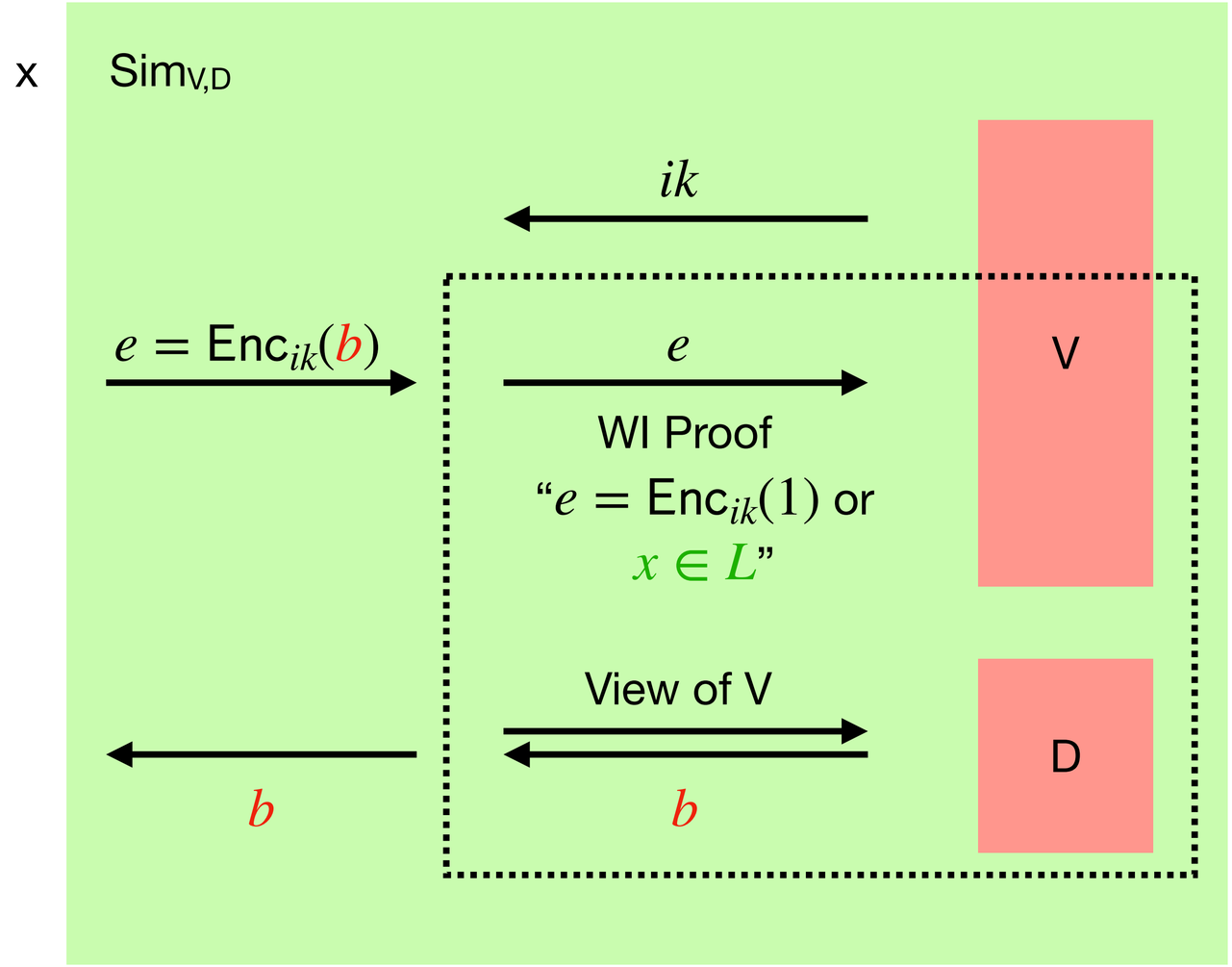
Sim can decrypt with probability better than 1/2

P cannot!

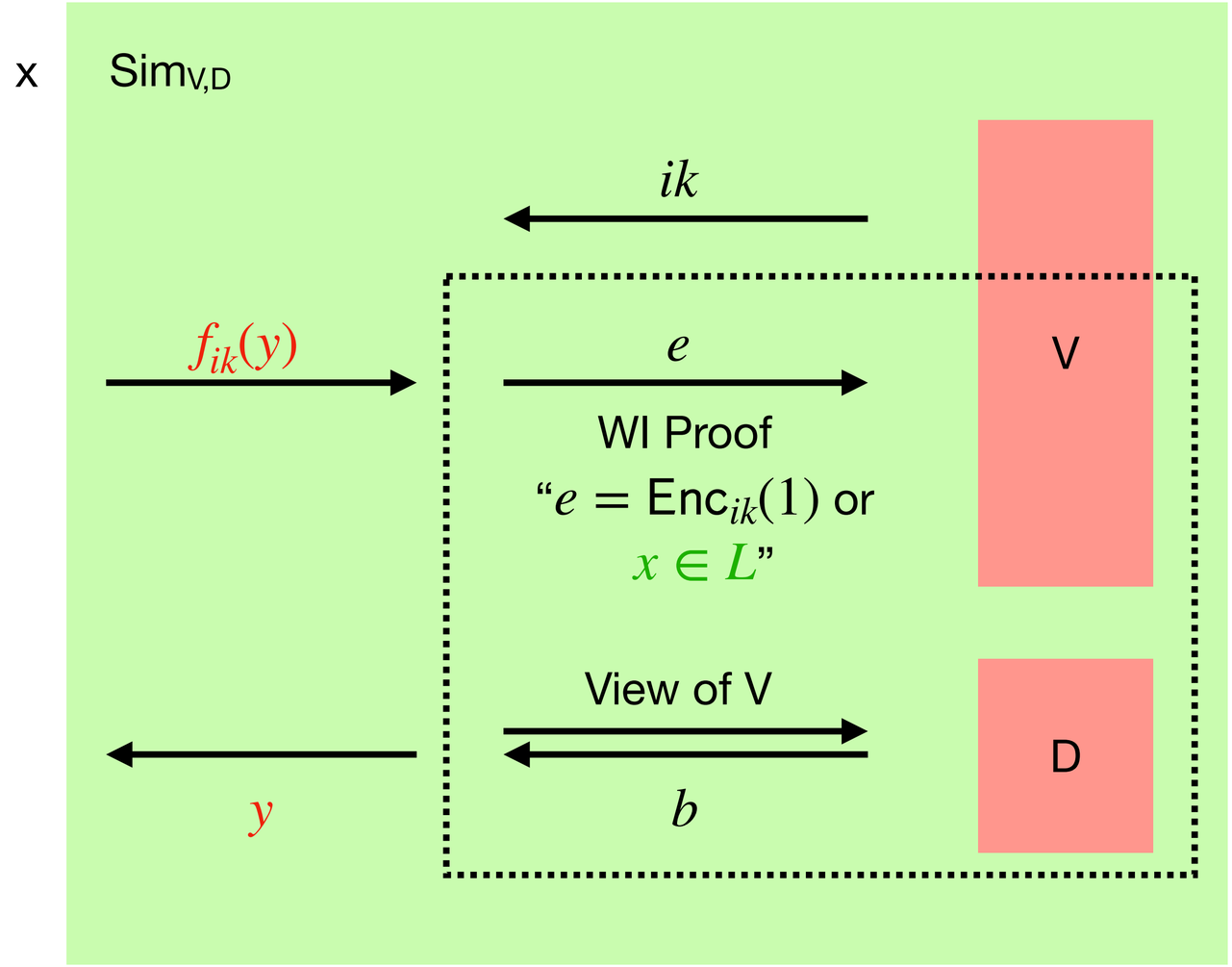
Instantiating the Encryption with Trapdoor Permutations

- Let ik be an index key and let τ be the corresponding trapdoor for a TDP f.
- $\mathsf{Enc}_{ik}(b; y, r) := f_{ik}(y), r, \langle y, r \rangle \oplus b$
- By Goldreich-Levin List Decoding, inverting $f_{ik}(y)$ reduces to distinguishing $\mathsf{Enc}_{ik}(0; y, r)$ from $\mathsf{Enc}_{ik}(1; y, r)$

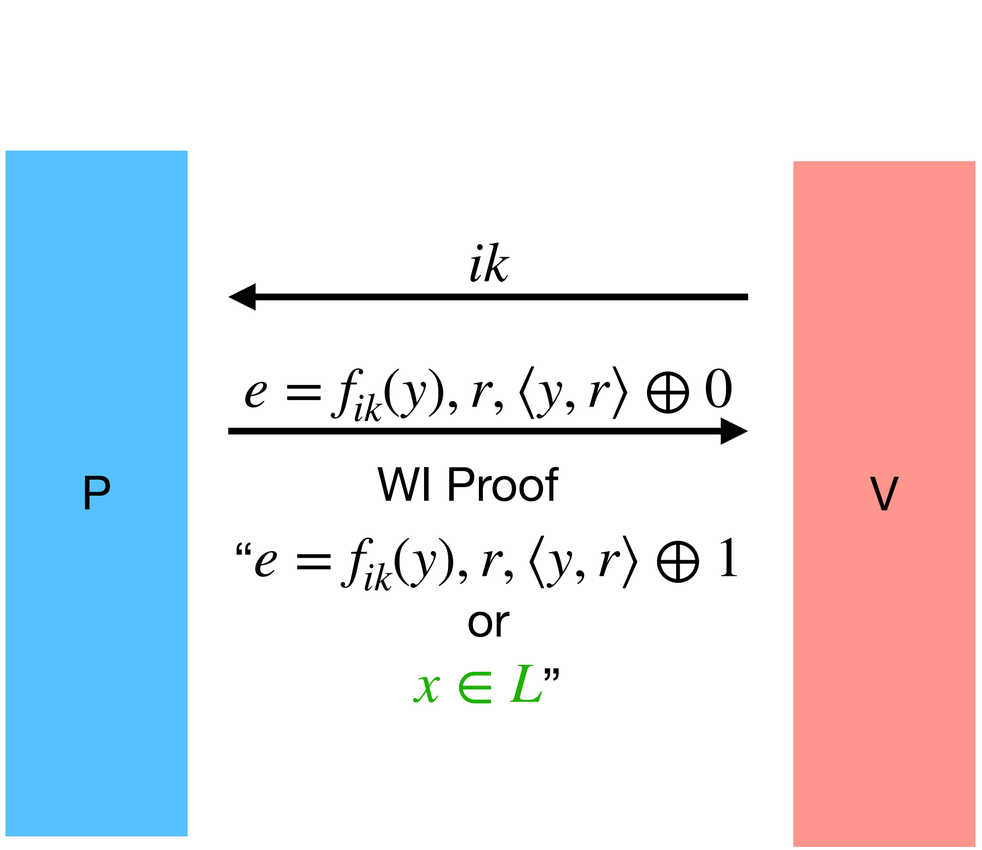
Goldreich-Levin allows us to invert

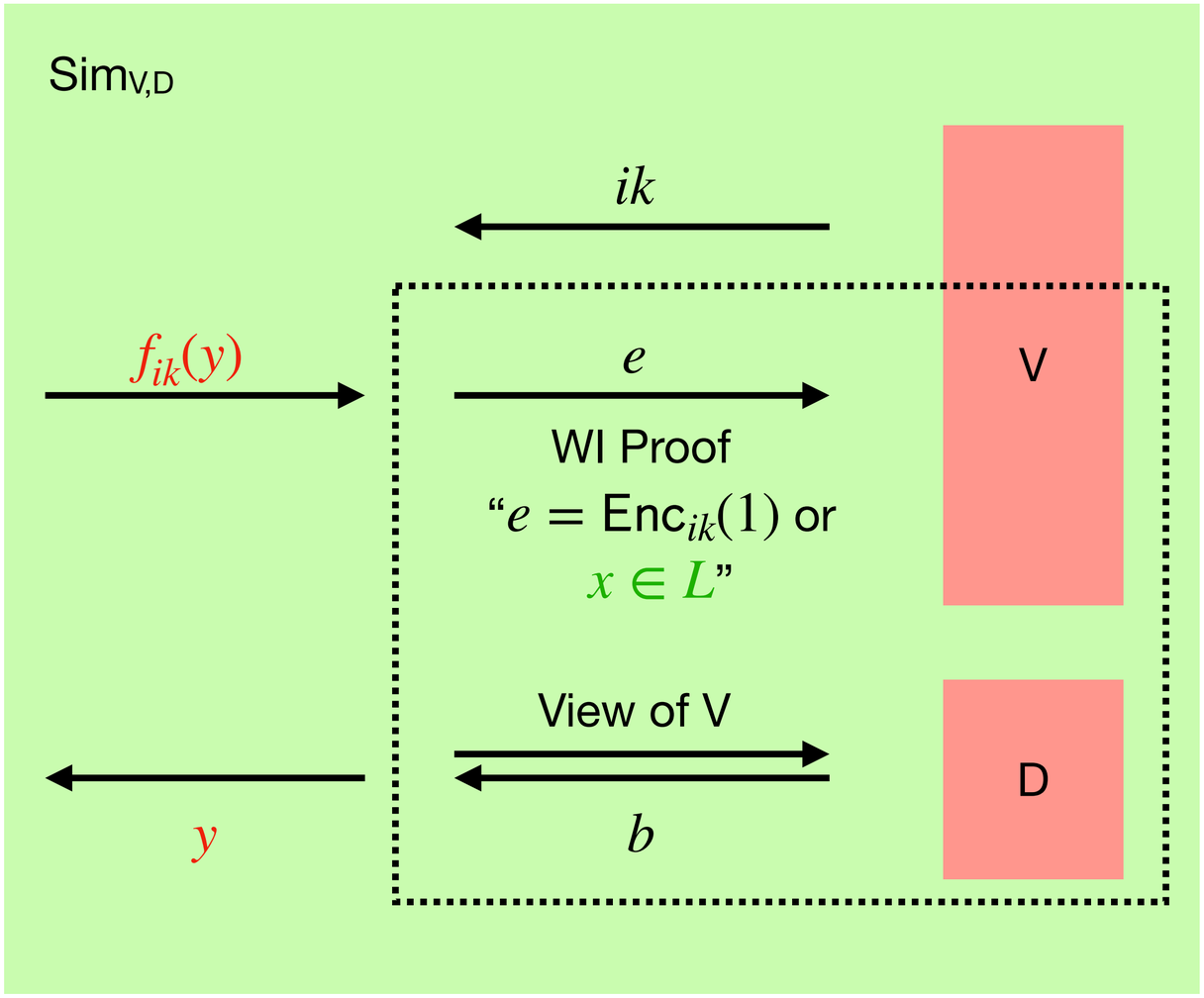


Goldreich-Levin allows us to invert

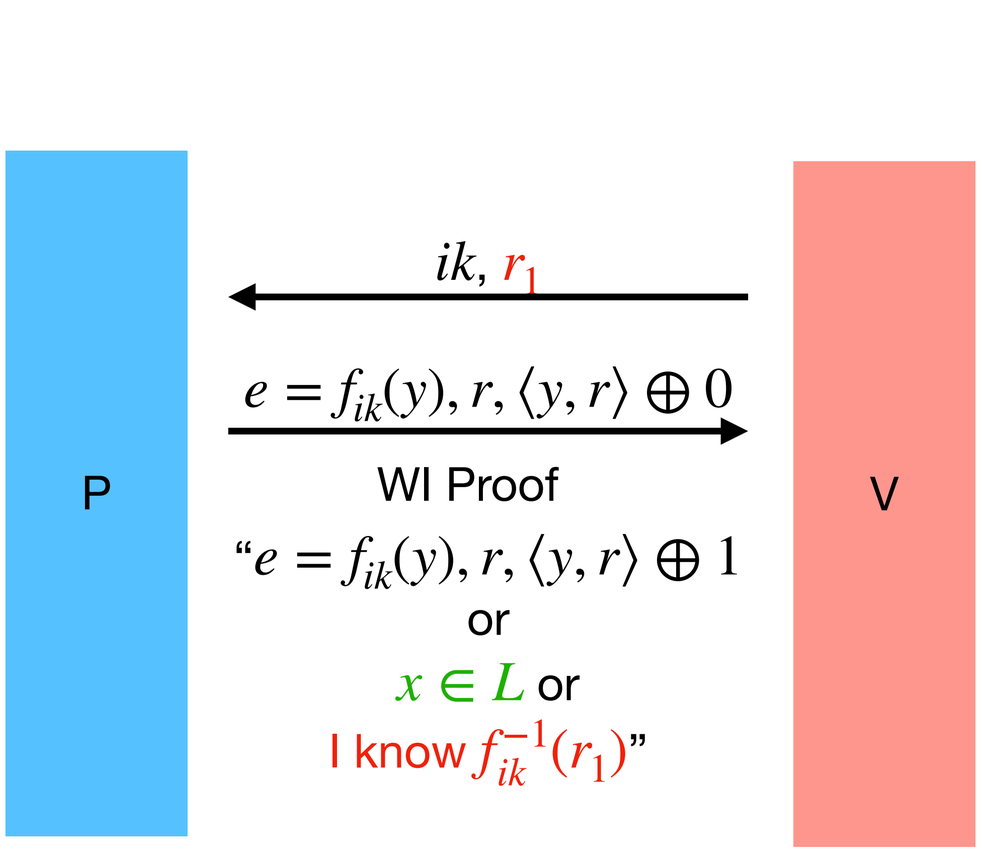


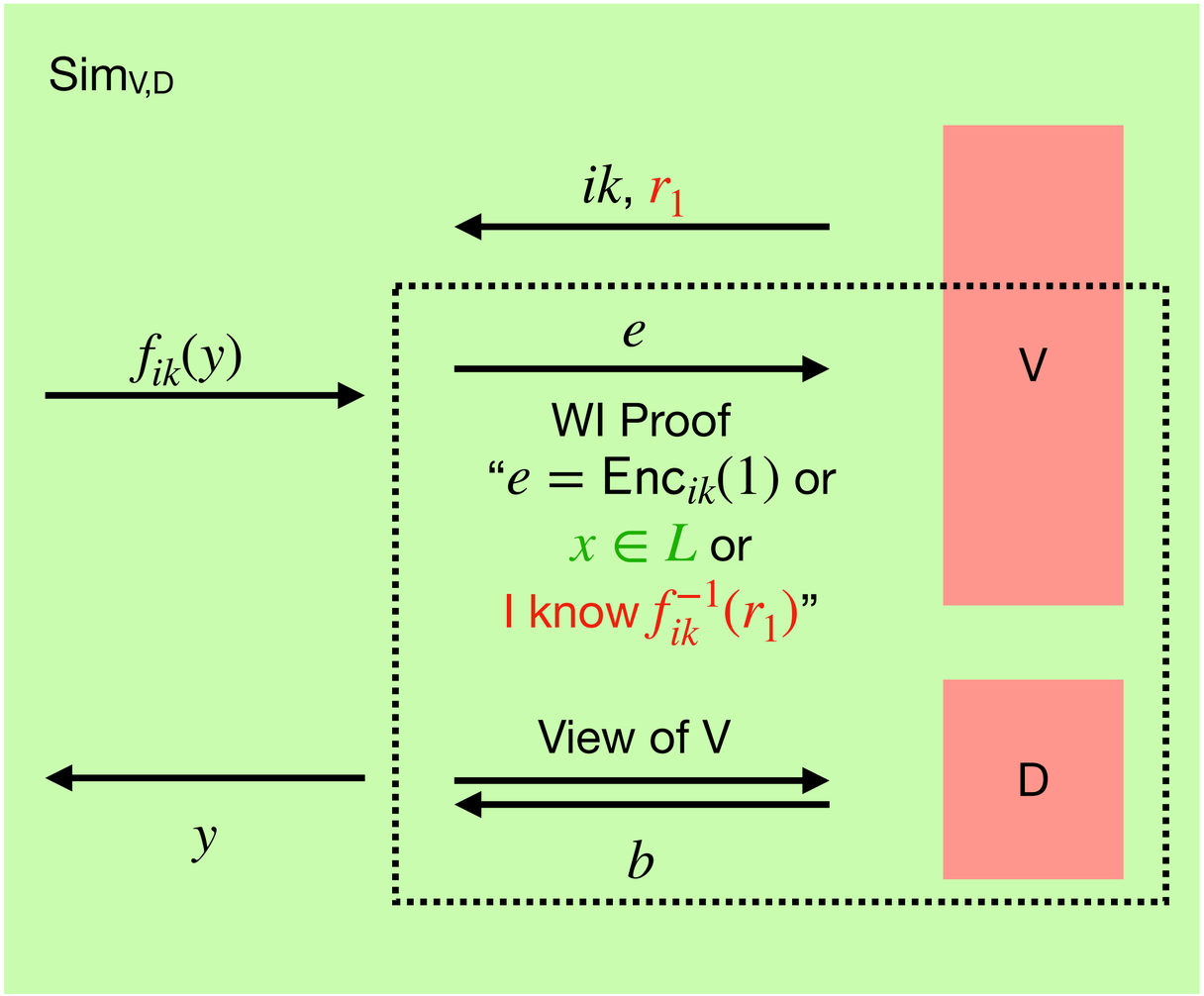
Adding a new branch to the WI proof



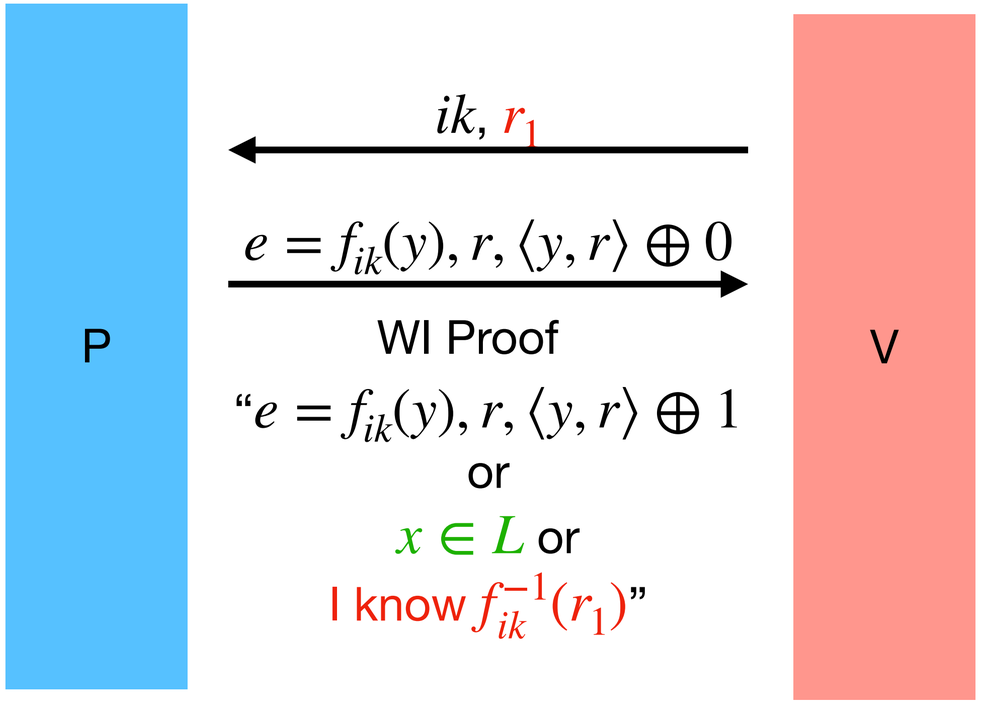


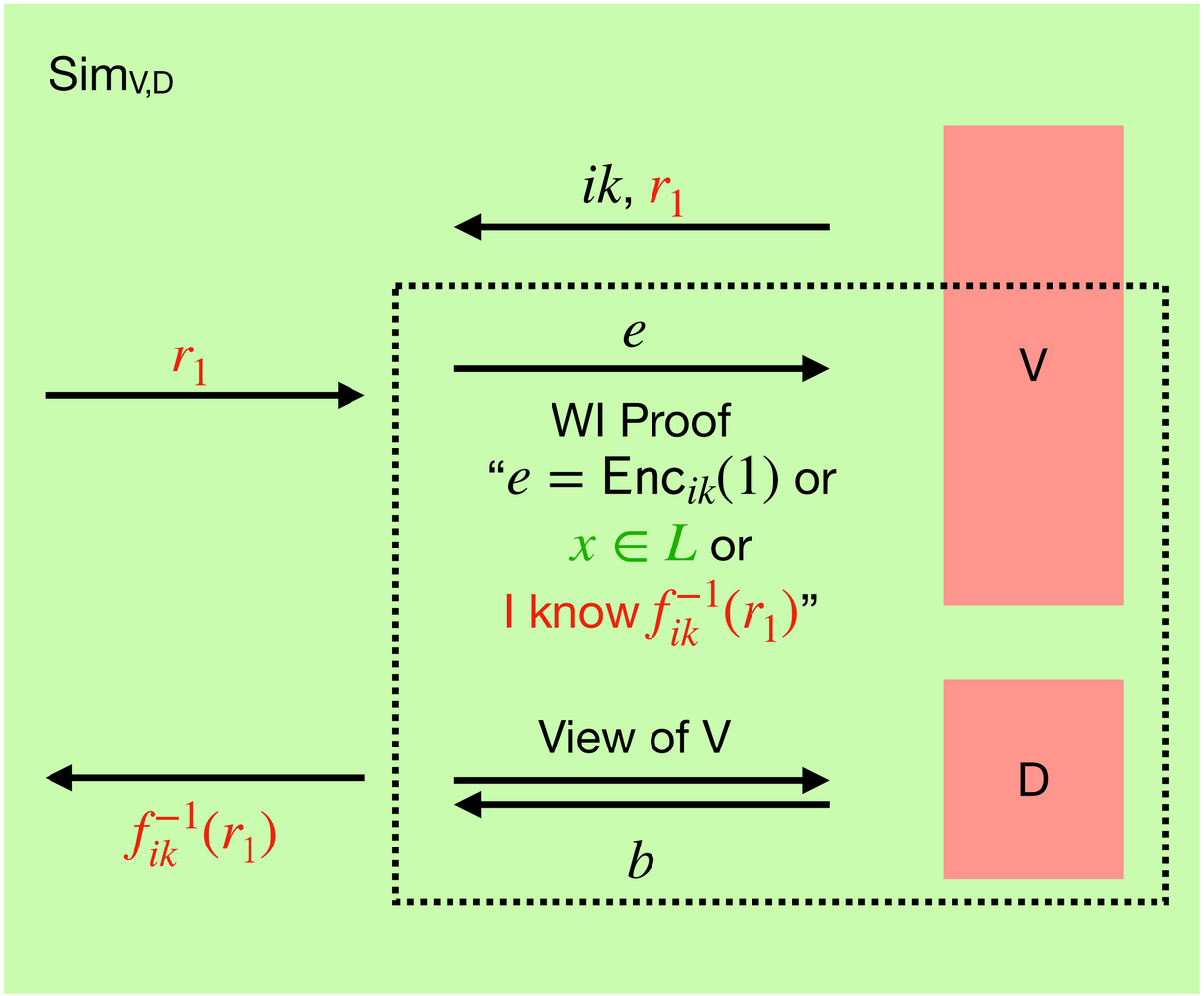
Adding a new branch to the WI proof



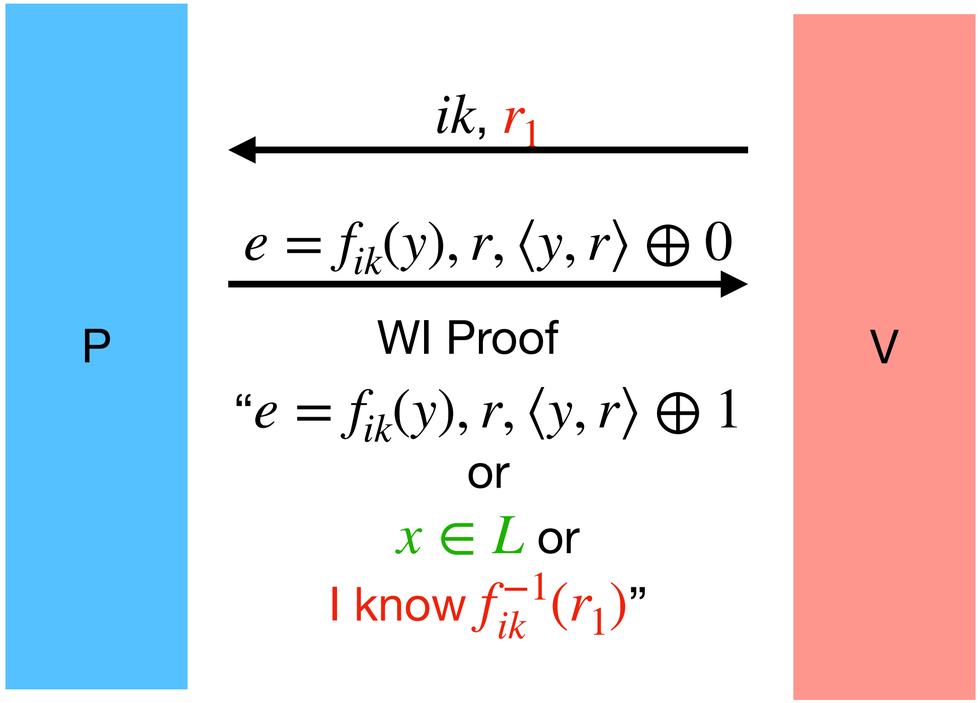


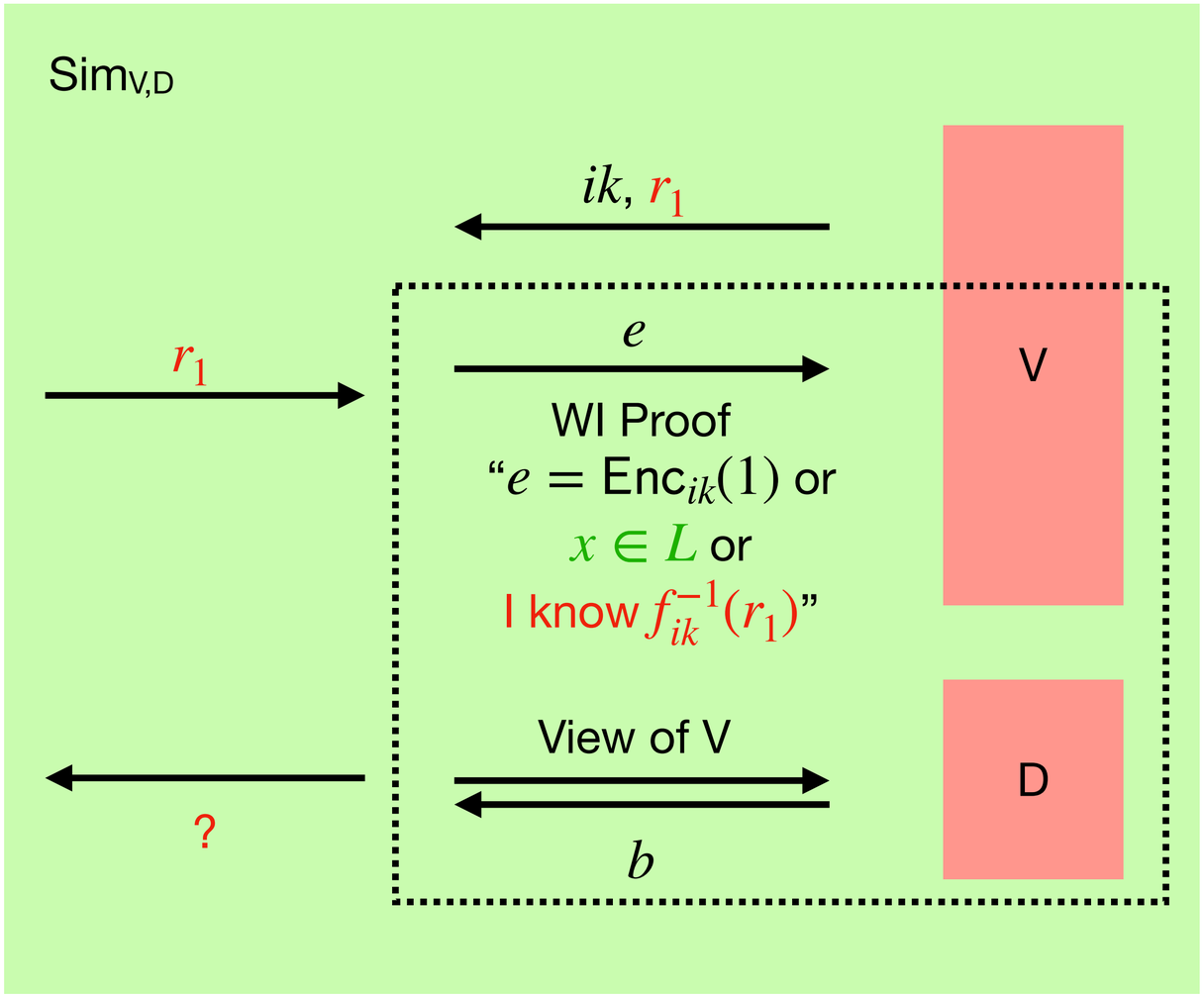
Simulator inverts r_1?



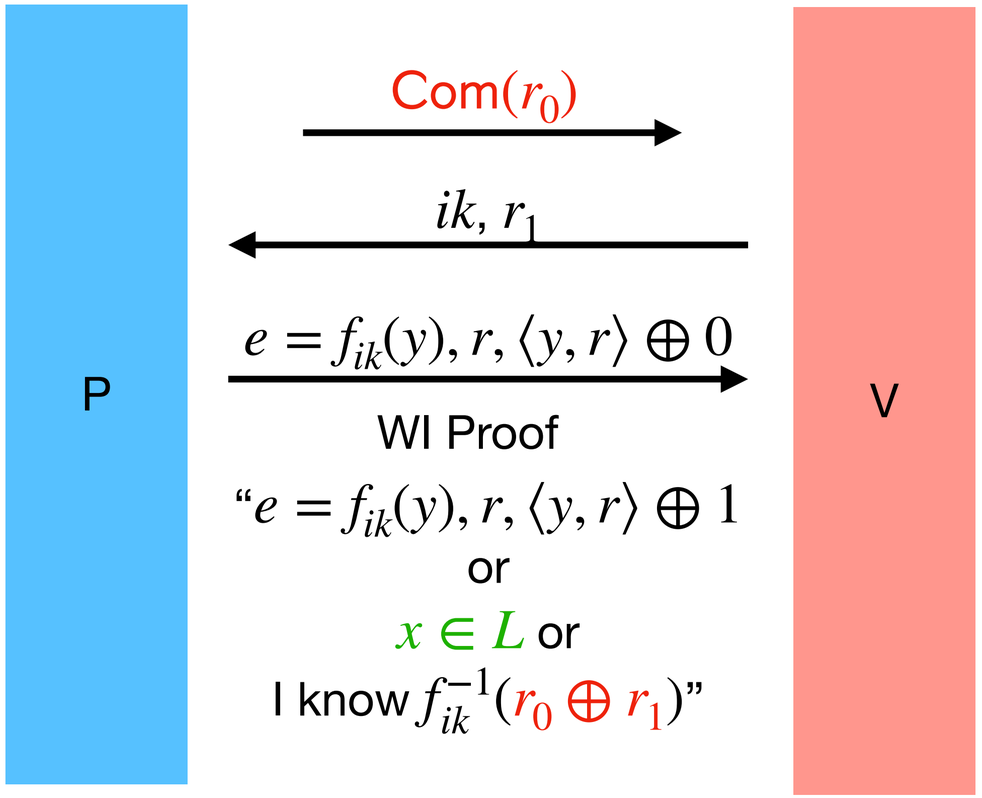


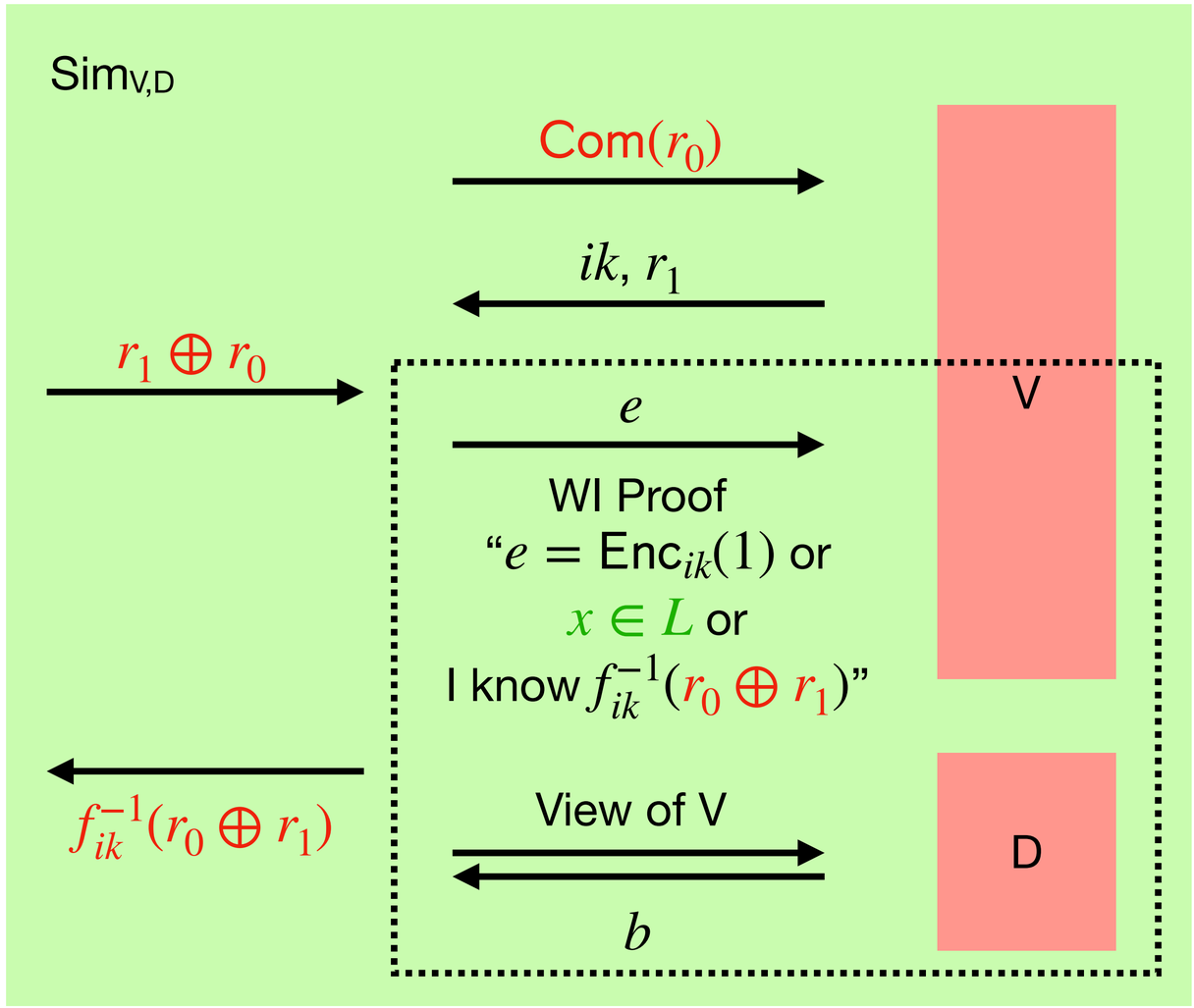
Problem: r_1 is not necessarily uniform





Fix via Coin Flipping





Conclusion: Three Round WZK from TDPs

Open Problems

- Can we obtain three-round WZK from Injective Trapdoor Functions? PKE?
- Can we obtain three-round WZK from OWFs? All previous works require extracting trapdoors.
- Can three-round WZK be separated from OWFs?

- Can three-round ZK be based on standard assumptions?

Thank You!