Laconic Zero Knowledge to Public Key Cryptography

Itay Berman Akshay Degwekar Ron Rothlum Prashant Nalini Vasudevan

Which general complexity-theoretic assumptions imply public-key cryptography?

Possible Answers

NP hardness

- Nice try
- Some impossibility results [Brassard79, GoldreichGoldwasser98,…]

One-Way Functions

- Some barriers [ImpagliazzoRudich89, Dachman-Soled16]
- Some possibilities if exponentially strong [BihamGorenIshai08]

SZK hardness

- Implies OWFs [Ostrovsky91]
- Many problems in SZK give PKE, many don’t

PKE from Laconic SZK hardness

$L \in$ NP has HVSZK argument:

- with **efficient prover**
- that is **laconic**

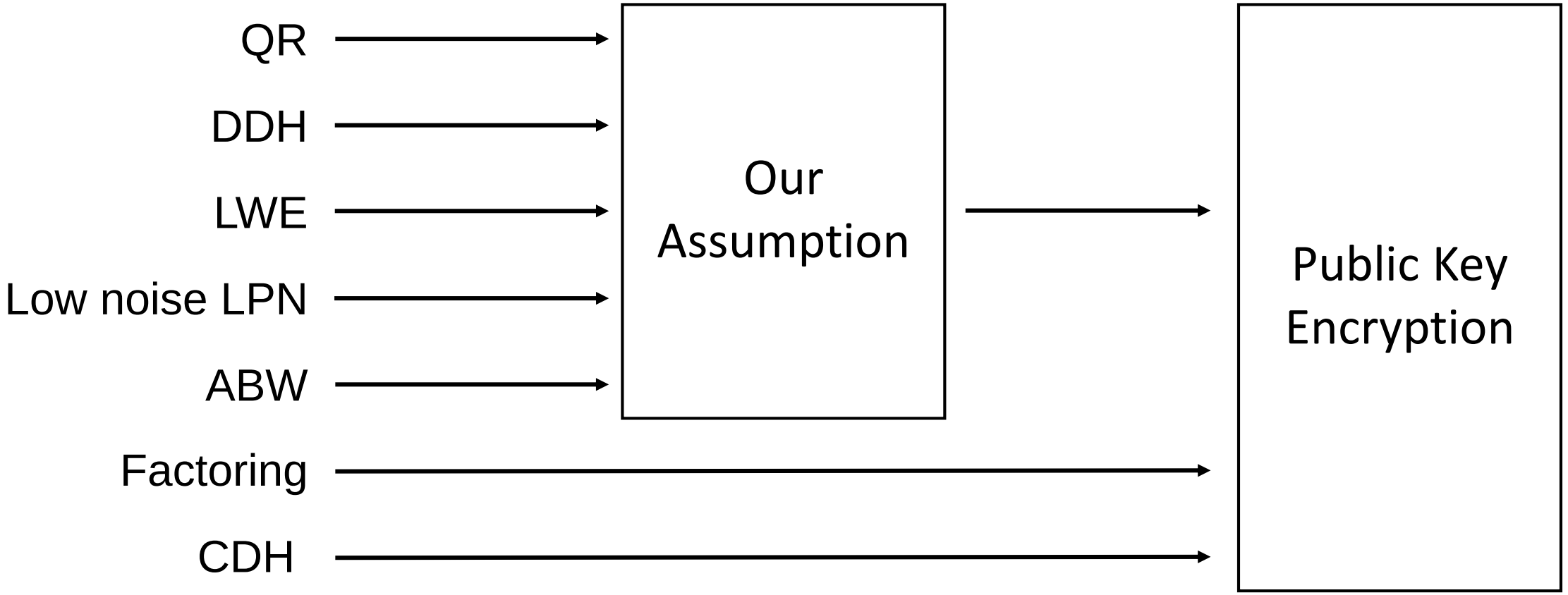
+

L is cryptographically-hard:

- has indist. YES and NO distributions
- can sample YES instances with NP witness

Public Key Encryption

Other Assumptions



PKE from Laconic SZK hardness

$L \in$ NP has HVSZK argument:

- ~~with **efficient prover**~~
- ~~that is **laconic**~~

[SahaiVadhan03] → SZK hardness ⇒ PKE

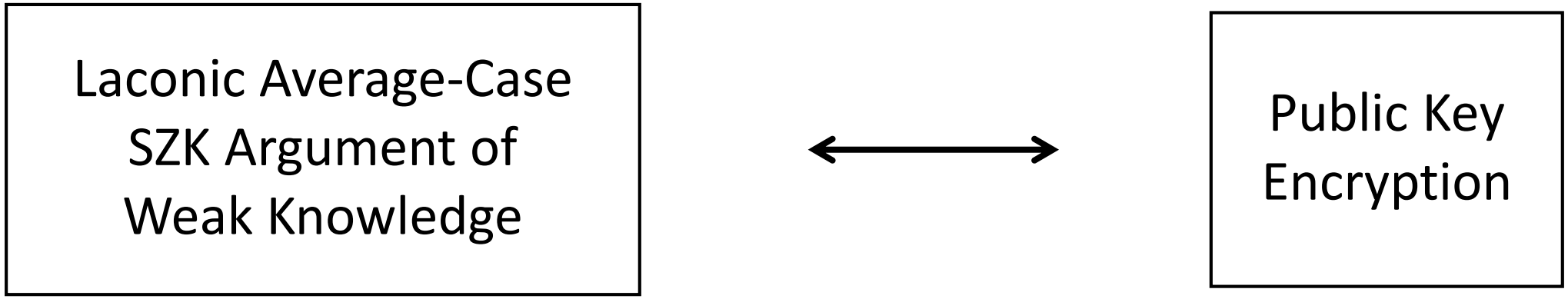
[HaitnerNguyenOngReingoldVadhan03] → OWF ⇒ PKE

+

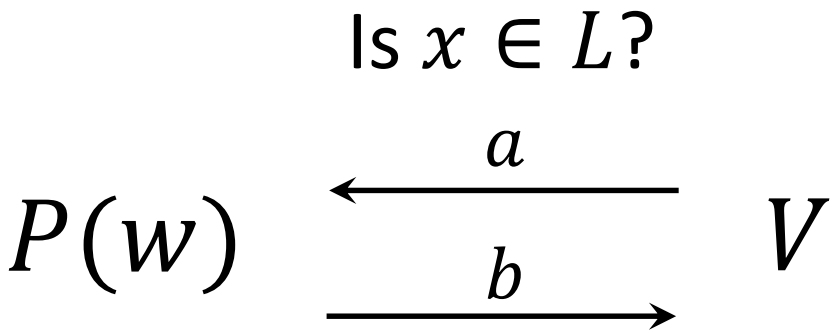
L is cryptographically-hard:

- has indist. YES and NO distributions
- can sample YES instances with NP witness

Characterisation



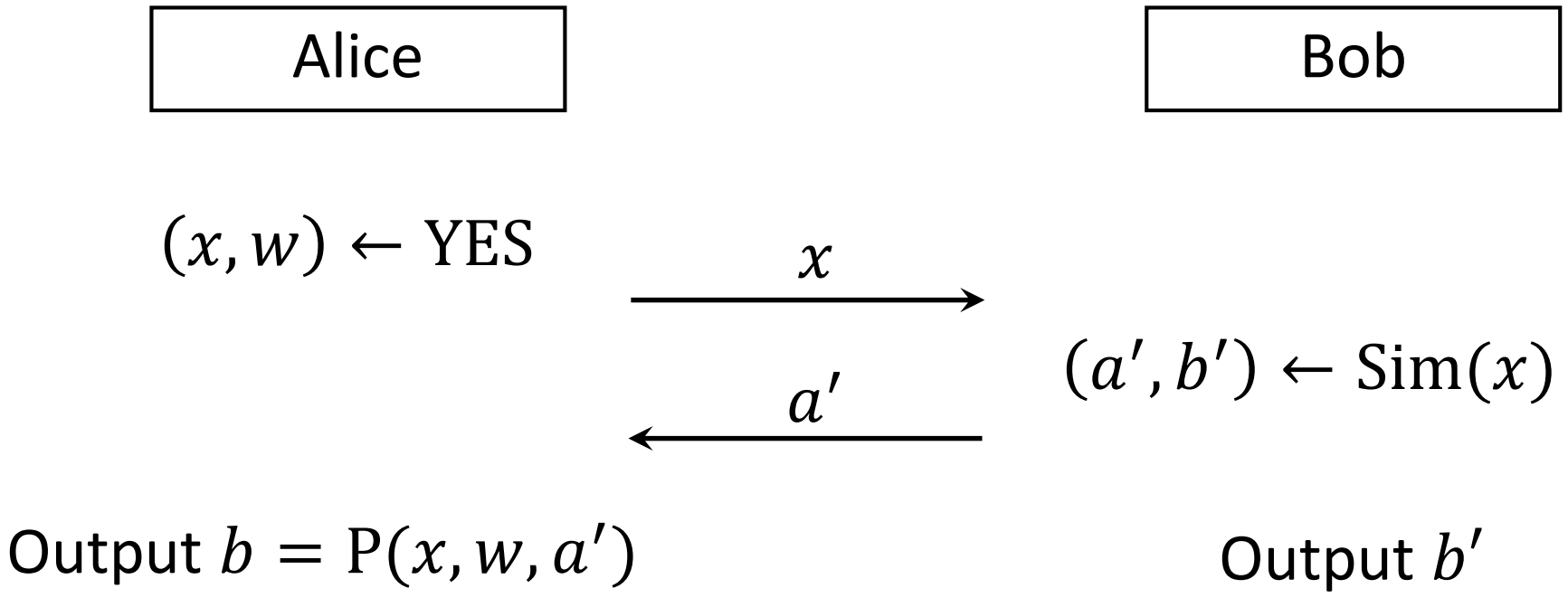
How



- $Sim(x)$ outputs (a', b')
- Constant Soundness error
- Perfect Completeness, Zero Knowledge

L is hard $\Rightarrow$ b is unpredictable given (x, a)

How



L is hard $\Rightarrow$ b is unpredictable given (x, a)

Randomised P: Repeat, Hash, Brute-force