UNIVERSITÄT
DES
SAARLANDES

Polynomially-hard Crypto

Michael Backes, Markus Dürmuth,
Dominique Unruh

Crypto 2008: Rump Session

Poly-hard one-way functions

Do one-way functions and
key-exchange protocols exist?

- Hard to prove (without assumptions)

- In practice: adversary running in time $n^{100000000}$ not “efficient”
- Alternative: n^{δ}-hard one-way functions

“Traditional” one-way functions

$$\begin{tikzcd} x \arrow[r, bend left, "n"] & f(x) \arrow[l, bend left, "> \mathrm{poly}(n)"] \end{tikzcd}$$

n^{δ}-hard one-way functions

$\delta>1$

$$\begin{tikzcd} x \arrow[r, bend left, "n"] & f(x) \arrow[l, bend left, "> n^{\delta}"] \end{tikzcd}$$

- Does not imply P≠NP, does not contradict [Razborov et al 97],…
- See [Merkle 78], [Biham et al 08], [Barak et al 08]

Existence of poly-hard crypto

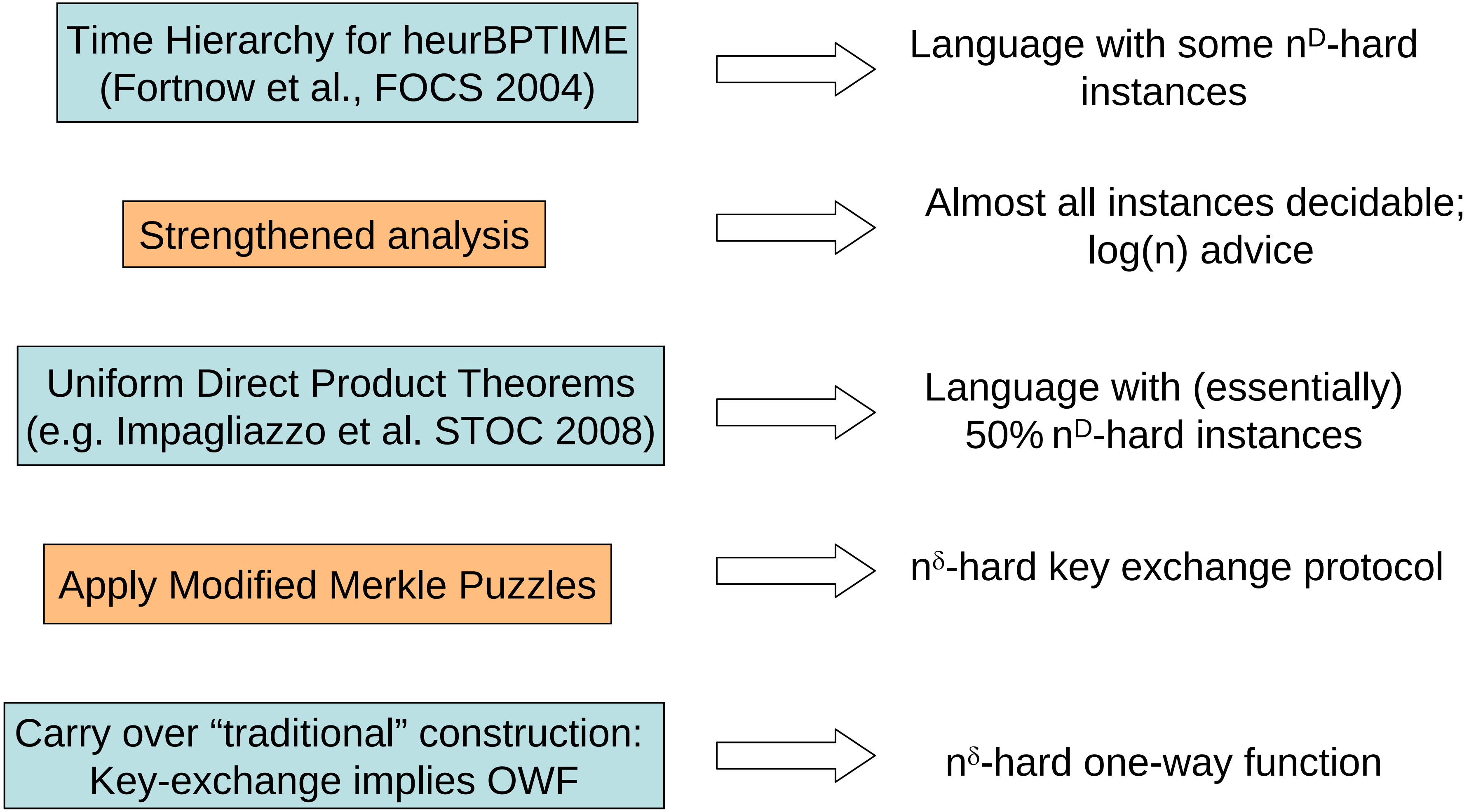
Goal: Prove that n^{δ}-hard OWF exist **unconditionally**

There exist an n^{δ}-hard one-way function and an n^{δ}-hard key-exchange protocol for some $\delta > 1$.

Current state: 20 pages proof sketch

Additionally:
Ideas how to strengthen this to $\delta \approx 3/2$.

Overall proof structure



Time Hierarchy for heurBPTIME (Fortnow et al., FOCS 2004) → Language with some n^D-hard instances

Strengthened analysis → Almost all instances decidable; log(n) advice

Uniform Direct Product Theorems (e.g. Impagliazzo et al. STOC 2008) → Language with (essentially) 50% n^D-hard instances

Apply Modified Merkle Puzzles → n^δ-hard key exchange protocol

Carry over “traditional” construction: Key-exchange implies OWF → n^δ-hard one-way function

THANK YOU