

# How to sample (securely) from any distribution?

*Dennis Hofheinz, Tibor Jager, Dakshita Khurana,  
Amit Sahai, Brent Waters and Mark Zhandry*

How to generate and use Universal Parameters?

<https://eprint.iacr.org/2014/507>

# Universal Samplers

# Universal Samplers

- Function  $u$

# Universal Samplers

- Function  $u$
- Input: Distribution  $d$

# Universal Samplers

- Function  $u$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$

# Universal Samplers

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

# Universal Samplers

- Samples from several distributions
- Several samples from same distribution

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

# Universal Samplers

- Samples from several distributions
- Several samples from same distribution

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

ADAPTIVE



# Universal Samplers

- Samples from several distributions
- Several samples from same distribution

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

ADAPTIVE

UNBOUNDED

# Universal Samplers

- Samples from several distributions
- Several samples from same distribution

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

SELECTIVE

UNBOUNDED

# Universal Samplers

- Samples from several distributions
- Several samples from same distribution

- Function  $\mathcal{U}$
- Input: Distribution  $d$
- Output: Sample  $s_d$  from distribution  $d$
- Security:  $r_d \leftarrow d; (\mathcal{U}, s_d) \approx (\mathcal{U}, r_d)$

SELECTIVE

BOUNDED

# Assuming iO

# Assuming iO

$$\mathcal{U} = \text{iO}(\mathcal{P})$$

# Assuming iO

$$\mathcal{U} = \text{iO}(\mathcal{P})$$

$\mathcal{P}$

Input:  $d$

Constant: PRF key  $K$

Output:  $d(\text{PRF}(K,d))$

Assuming  $iO + RO$

Assuming  $iO + RO$



# Assuming iO + RO

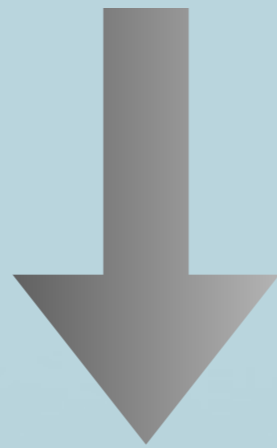
SELECTIVE

BOUNDED

# Assuming iO + RO

SELECTIVE

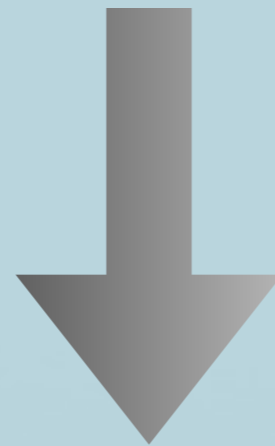
BOUNDED



# Assuming iO + RO

SELECTIVE

BOUNDED



ADAPTIVE

UNBOUNDED

# Applications

# Applications

- **RSA** modulus without knowing primes

# Applications

- **RSA** modulus without knowing primes
- **CRS** for different protocols with single initial setup

# Applications

- **RSA** modulus without knowing primes
- **CRS** for different protocols with single initial setup
- PKE + Universal Samplers  $\Rightarrow$  **IBE**  
(fresh  $\langle pk, sk \rangle$  samples for every ID)

# Applications

- **RSA** modulus without knowing primes
- **CRS** for different protocols with single initial setup
- PKE + Universal Samplers  $\Rightarrow$  **IBE**  
(fresh  $\langle pk, sk \rangle$  samples for every ID)
- PKE + Universal Samplers  $\Rightarrow$  Multiparty **NIKE**



# Follow-up Applications

# Follow-up Applications

- Use universal parameters as core technique

# Follow-up Applications

- Use universal parameters as core technique
- Adaptively secure **constrained PRFs** [HKKW14- eprint]

# Follow-up Applications

- Use universal parameters as core technique
- Adaptively secure **constrained PRFs** [HKKW14- eprint]
- **Universal Signature Aggregators** [HKW14- eprint]

**Thank you!**