On Pseudorandom Encodings

Thomas Agrikola
Karlsruhe Institute of Technology

Geoffroy Couteau
IRIF, Paris-Diderot University, CNRS

Yuval Ishai
Technion

Stanisław Jarecki
UC Irvine

Amit Sahai
UCLA

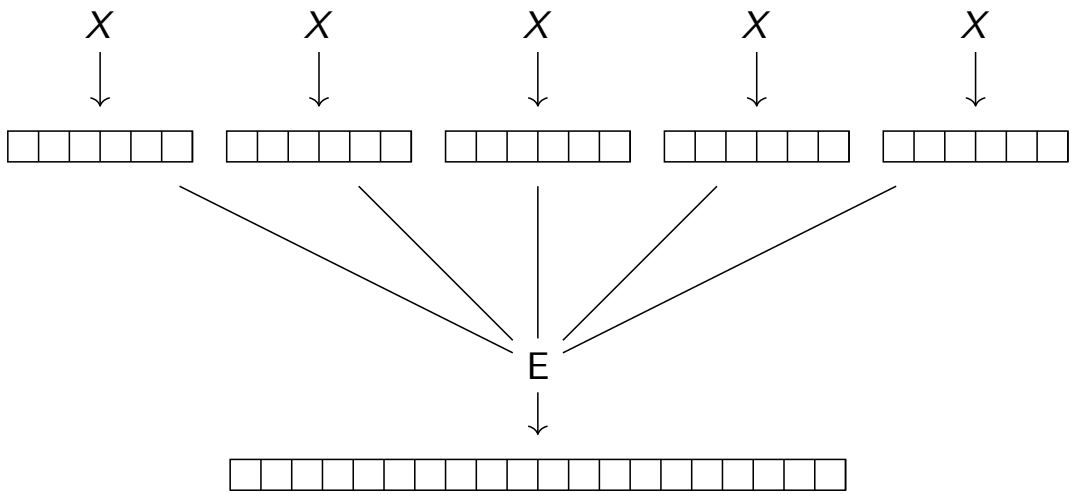
November 11, 2020

Compression in Information Theory

- encoding information using fewer bits than its original representation

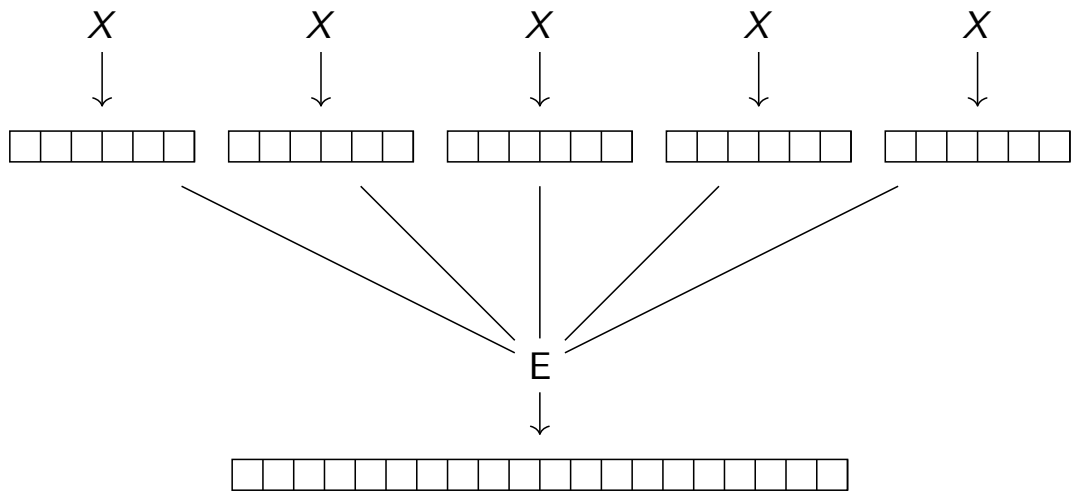
Compression in Information Theory

- encoding information using fewer bits than its original representation
  - an information source X is modeled as a distribution
  - map a sequence of samples from X to a short representation



Compression in Information Theory

- encoding information using fewer bits than its original representation
  - an information source X is modeled as a distribution
  - map a sequence of samples from X to a short representation



- [Sha48; Huf52; GM59; Flo64; Sch72; Ris76; Pas77; ZL77; ZL78; RJ79]

Compression in Complexity Theory

- compression has received considerable attention [GS85; Wee04; TVZ05; HLR07]

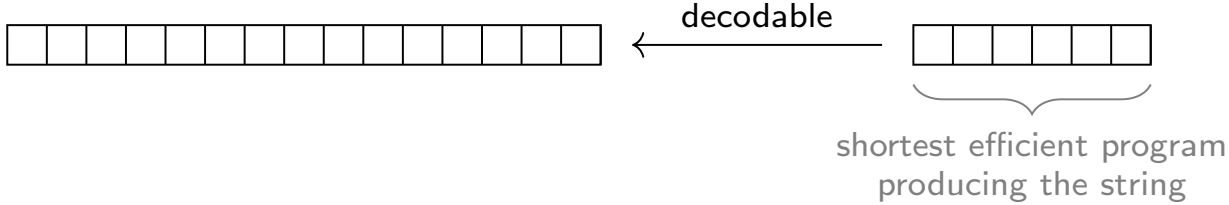
Compression in Complexity Theory

- compression has received considerable attention [GS85; Wee04; TVZ05; HLR07]
- general case:
  - $\Pr\left[\mathsf{D}(\mathsf{E}(X)) = X\right]$ is overwhelming
  - $\mathbb{E}\left[|\mathsf{E}(X)|\right]$ is small

Compression in Complexity Theory

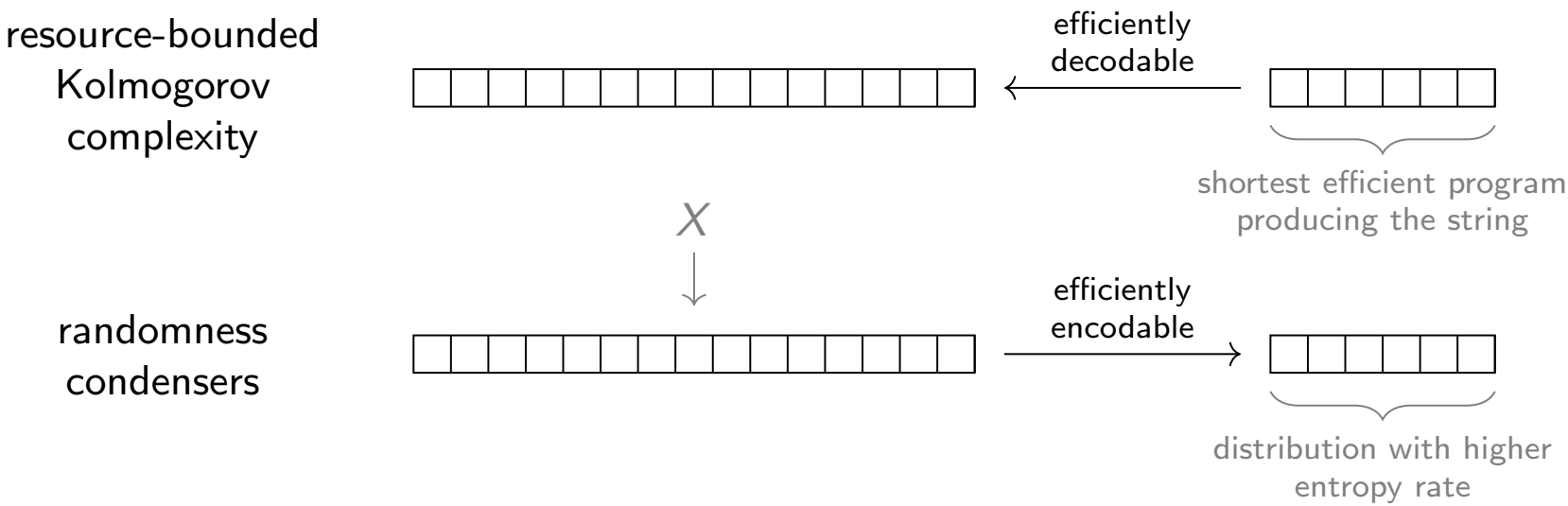
- compression has received considerable attention [GS85; Wee04; TVZ05; HLR07]
- general case:
  - $\Pr\left[\mathsf{D}(\mathsf{E}(X)) = X\right]$ is overwhelming
  - $\mathbb{E}\left[|\mathsf{E}(X)|\right]$ is small

resource-bounded Kolmogorov complexity



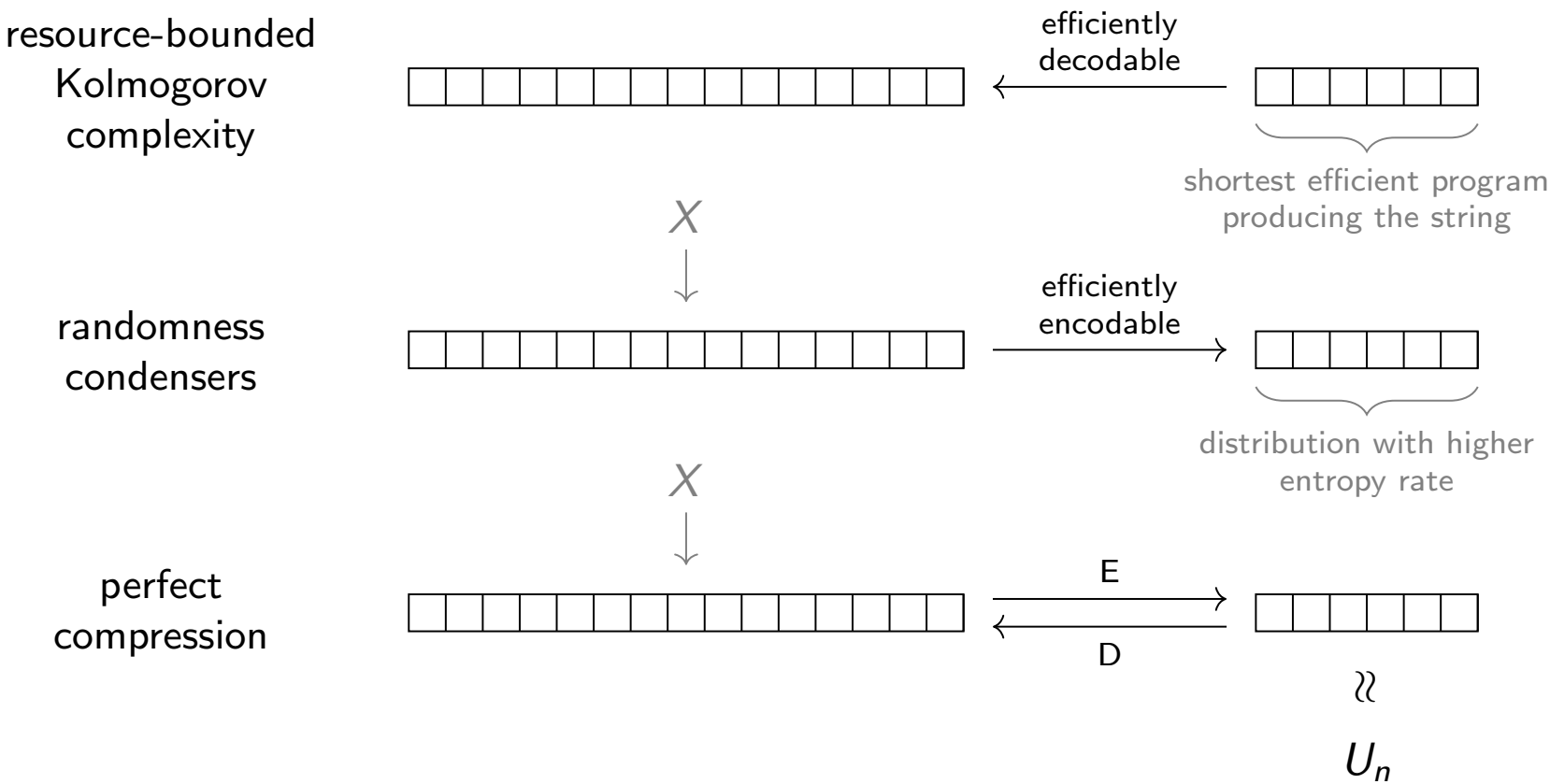
Compression in Complexity Theory

- compression has received considerable attention [GS85; Wee04; TVZ05; HLR07]
- general case:
  - $\Pr\left[\mathsf{D}(\mathsf{E}(X)) = X\right]$ is overwhelming
  - $\mathbb{E}\left[|\mathsf{E}(X)|\right]$ is small



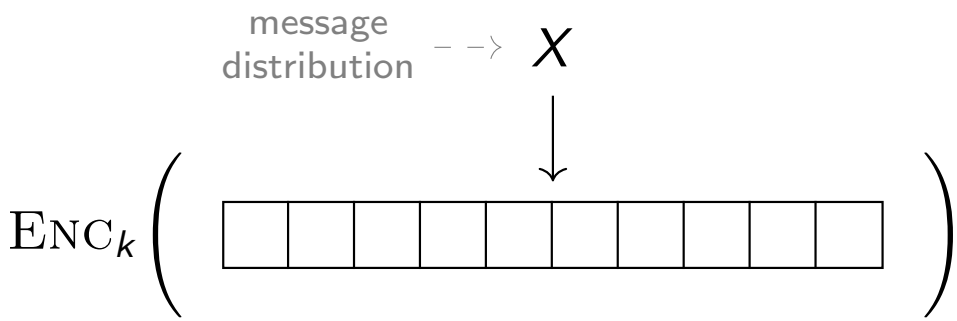
Compression in Complexity Theory

- compression has received considerable attention [GS85; Wee04; TVZ05; HLR07]
- general case:
  - $\Pr\left[\mathsf{D}(\mathsf{E}(X)) = X\right]$ is overwhelming
  - $\mathbb{E}\left[|\mathsf{E}(X)|\right]$ is small



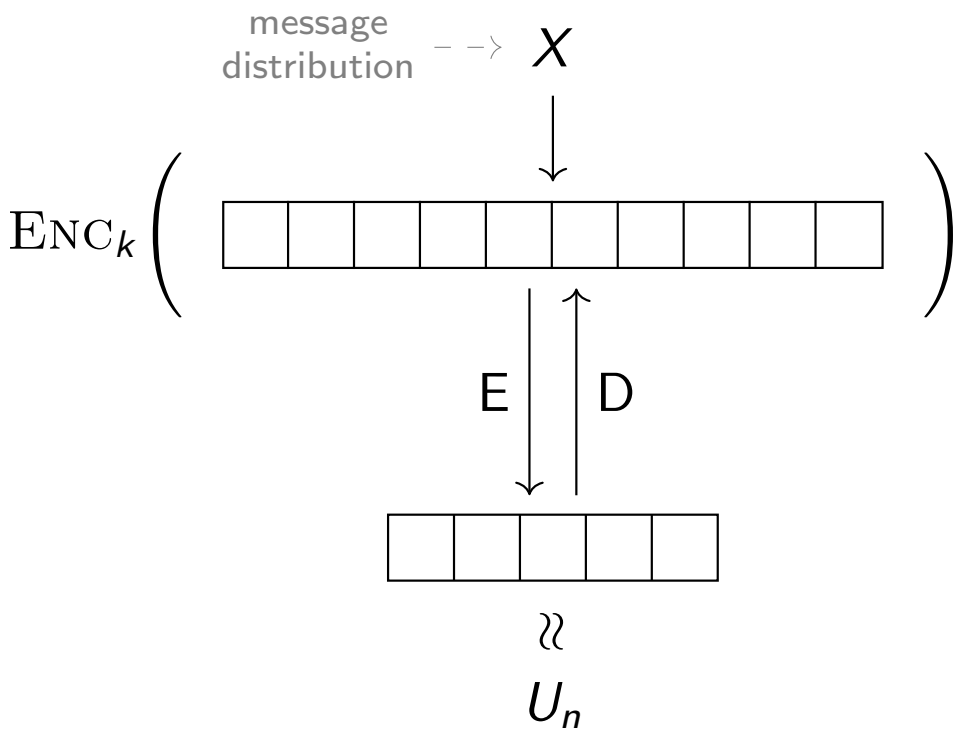
Compression in Cryptography

- **problem:** low-entropy encryption keys (e.g. passwords)
  - brute-force attack:
    try most likely keys k' until $\mathrm{DEC}_{k'}(c)$ looks like, e.g., natural speech



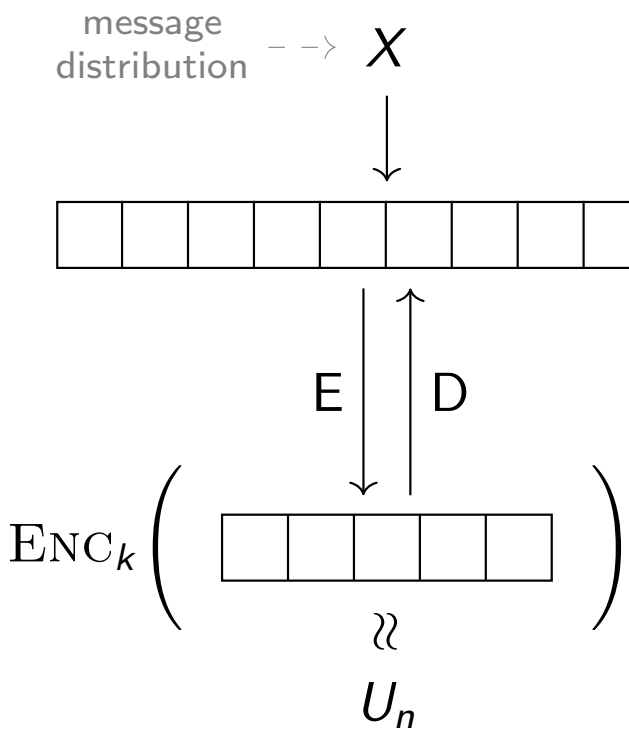
Compression in Cryptography

- **problem:** low-entropy encryption keys (e.g. passwords)
  - brute-force attack:
    try most likely keys k' until $\mathrm{DEC}_{k'}(c)$ looks like, e.g., natural speech
- **solution:** perfect compression [BM92; BMN01]



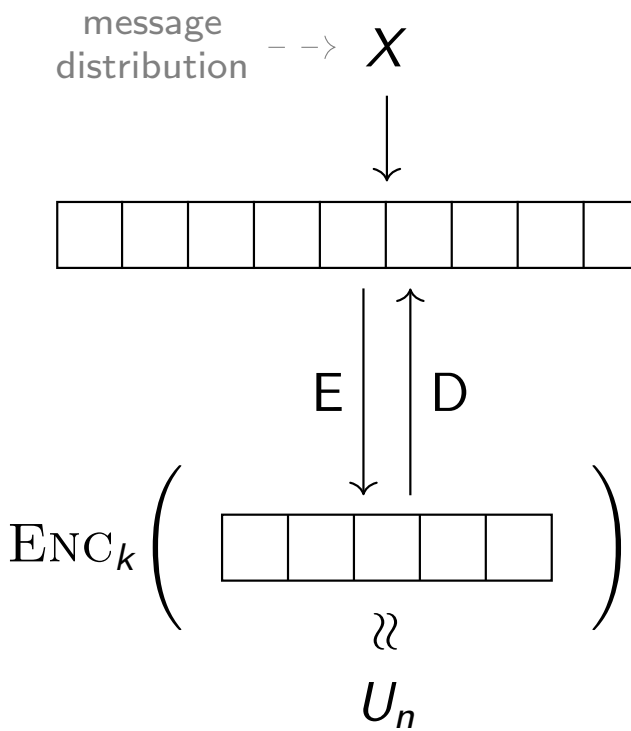
Compression in Cryptography

- **problem:** low-entropy encryption keys (e.g. passwords)
  - brute-force attack:
    try most likely keys k' until $\mathrm{DEC}_{k'}(c)$ looks like, e.g., natural speech
- **solution:** perfect compression [BM92; BMN01]



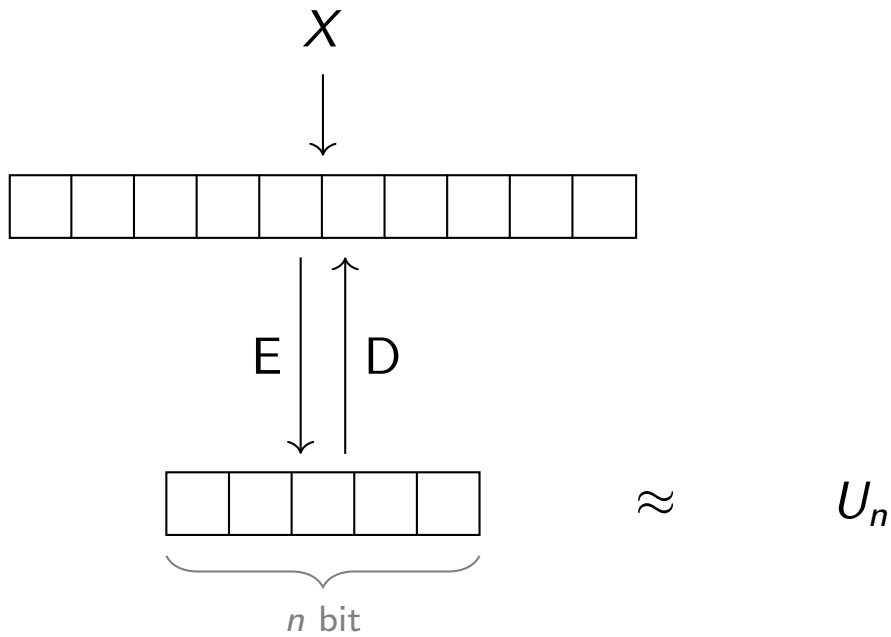
Compression in Cryptography

- **problem:** low-entropy encryption keys (e.g. passwords)
  - brute-force attack:
    try most likely keys k' until $\mathrm{DEC}_{k'}(c)$ looks like, e.g., natural speech
- **solution:** perfect compression [BM92; BMN01]



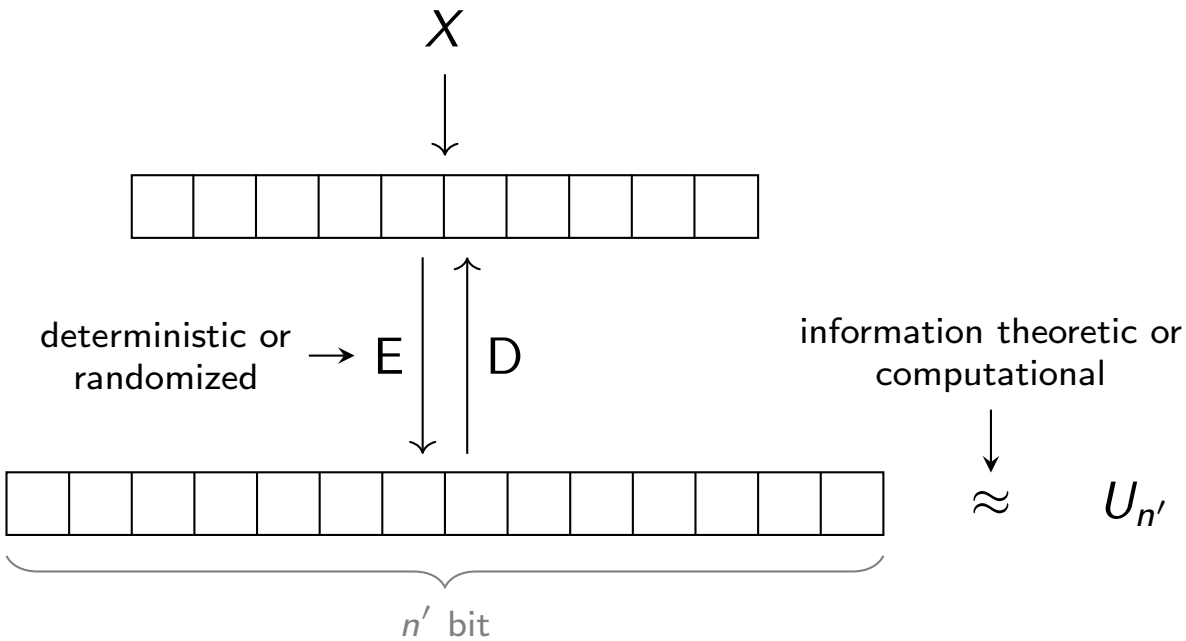
- **but:** perfect compression only exists for very few distributions

Relaxing Compression – Pseudorandom Encodings



- relaxing compression:

Relaxing Compression – Pseudorandom Encodings



- relaxing compression:
  - drop "shorter outputs" requirement
  - consider *deterministic* and *randomized* E

  } similar to "honey encryption" [JR14]
  - consider *information theoretic* and *computational* guarantees
  - consider notion with and without *trusted setup assumption*

Our Contributions in Short

- negative results for most stronger variants of PRE
- positive result from `iO`

Our Contributions in Short

- negative results for most stronger variants of PRE
- positive result from `iO`
- establish equivalence between PRE and invertible sampling

Our Contributions in Short

- negative results for most stronger variants of PRE
- positive result from `iO`
- establish equivalence between PRE and invertible sampling
- many applications from seemingly unrelated areas in cryptography
  - adaptive MPC
  - covert MPC
  - honey encryption
  - variant of steganography

Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

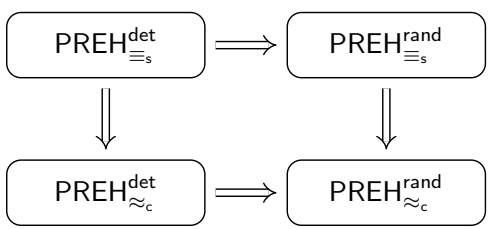
may depend on input m

Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

may depend on input m

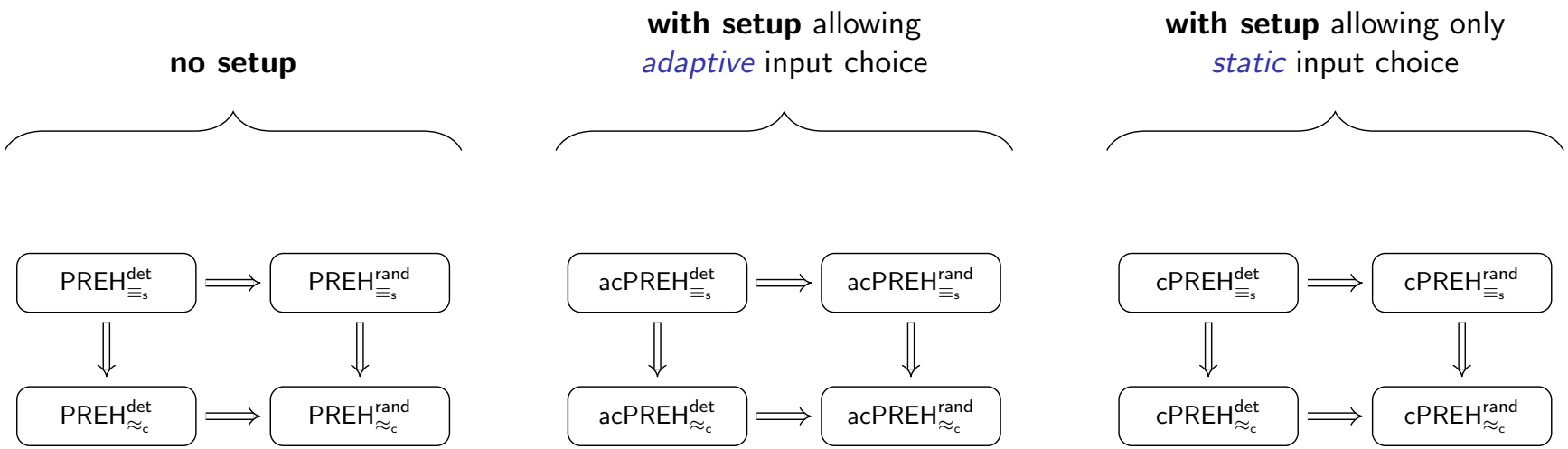
no setup



Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

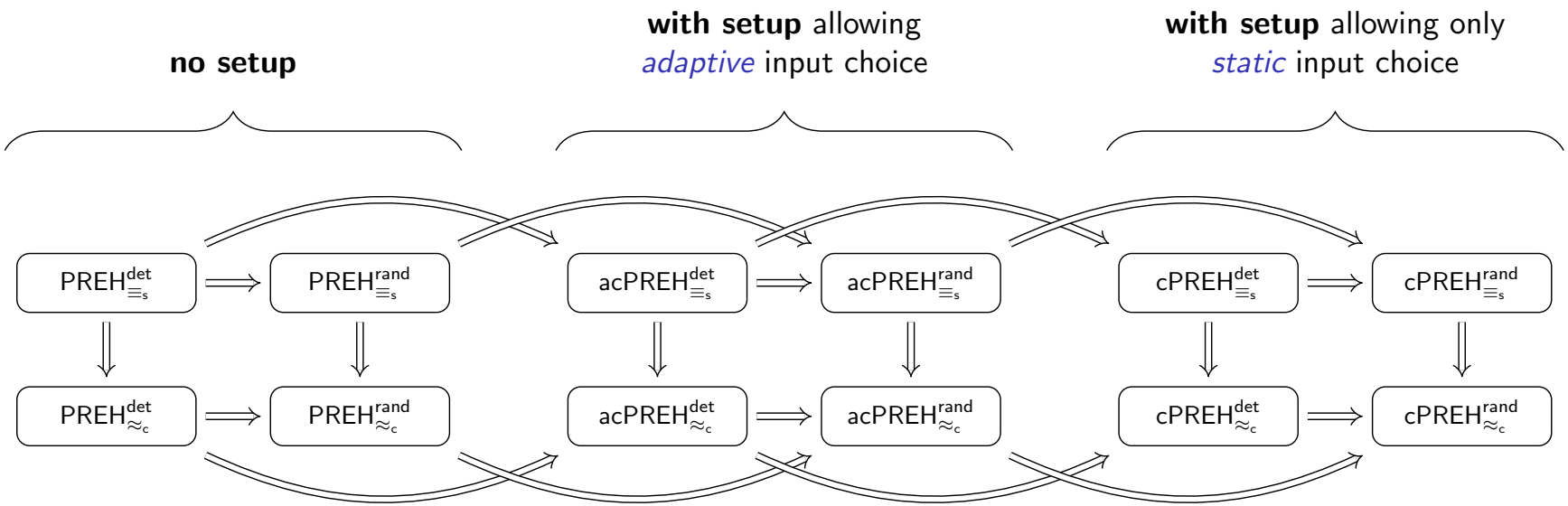
may depend on input m



Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

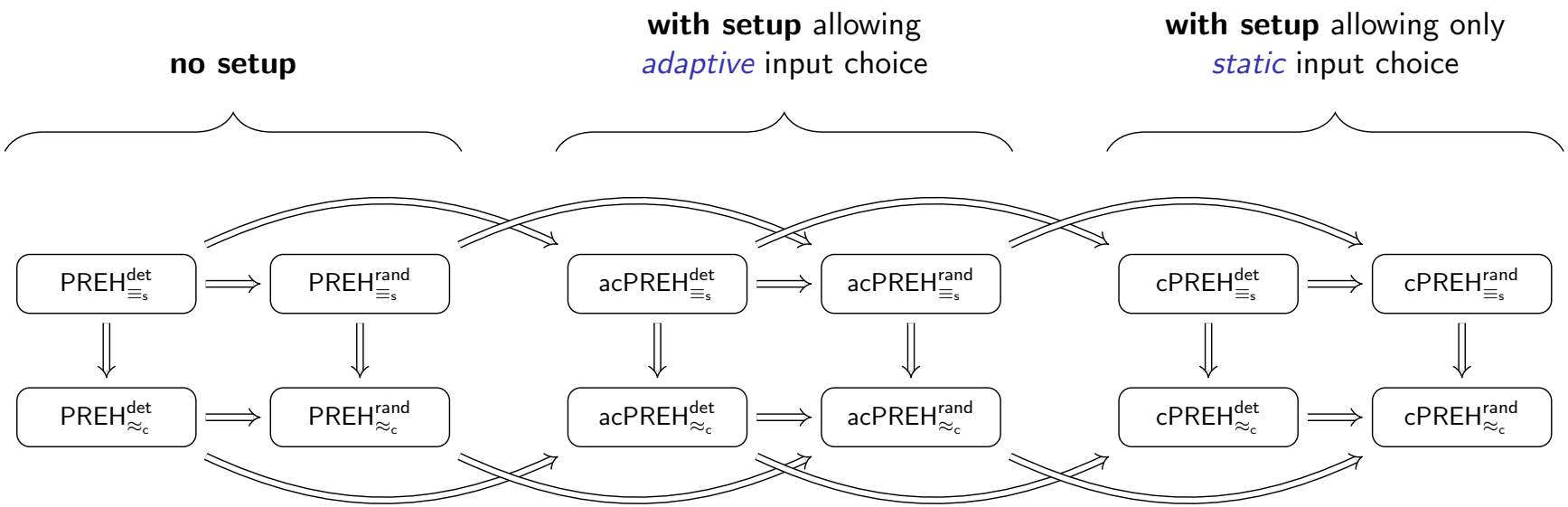
may depend on input m



Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

may depend on input m

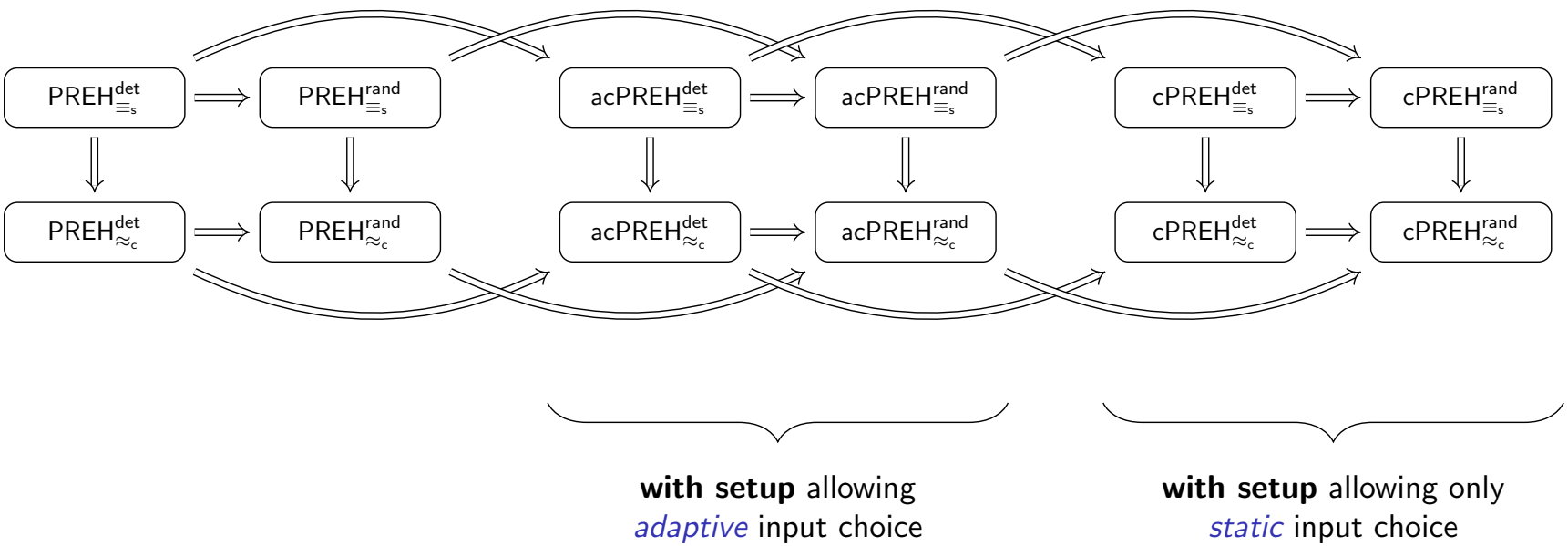


- **goal:** understand landscape of pseudorandom encodings

Landscape of Pseudorandom Encodings

Deterministic Encoding

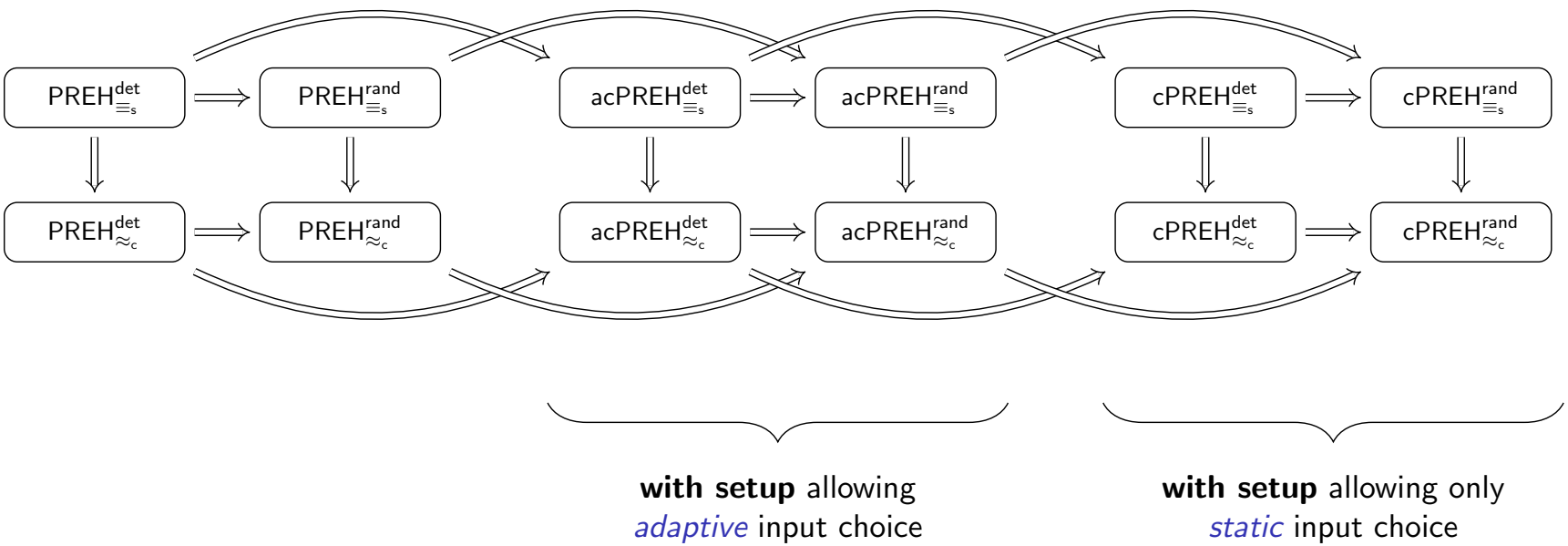
- deterministic PREH unconditionally false



Landscape of Pseudorandom Encodings

Deterministic Encoding

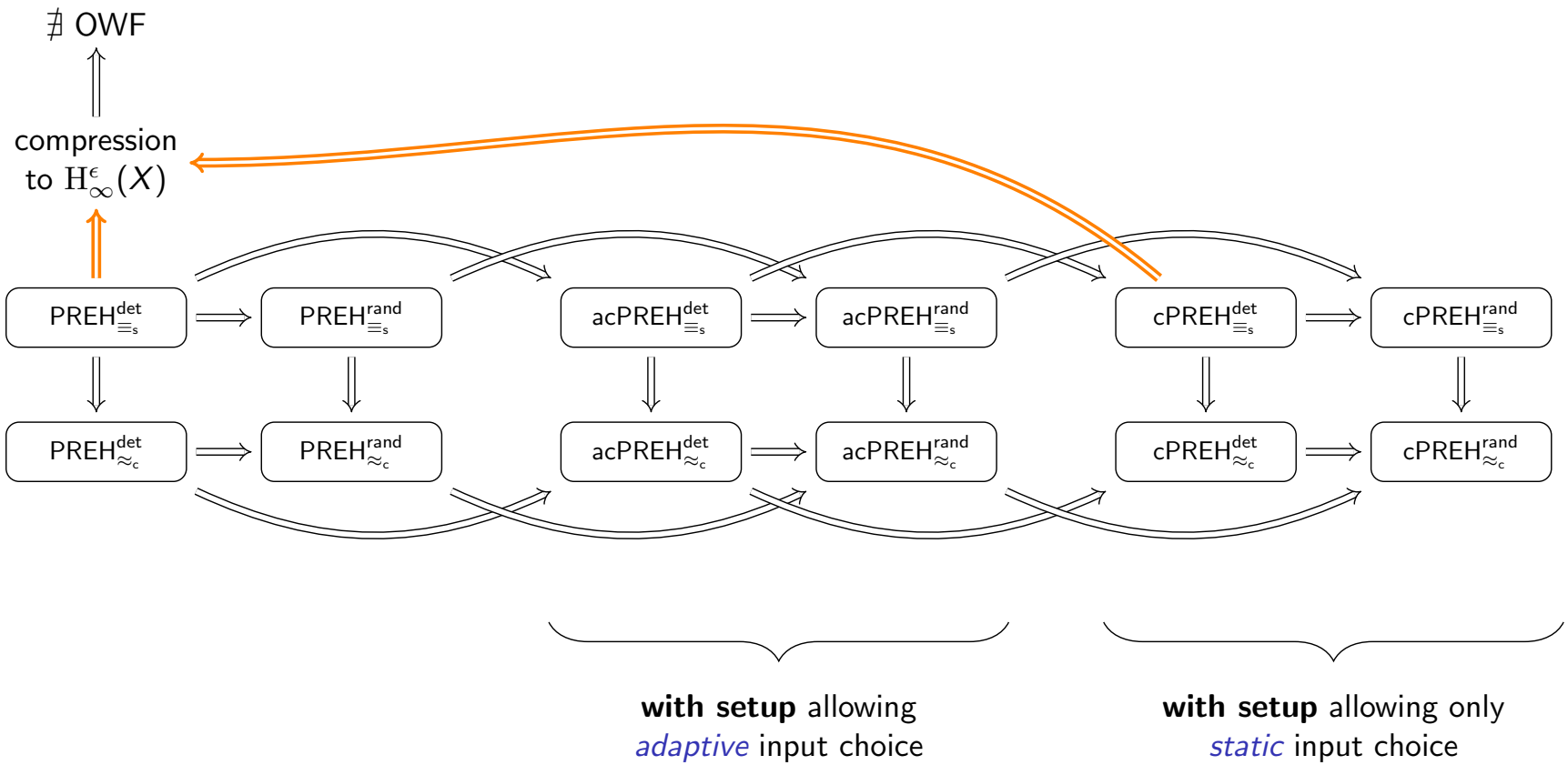
- deterministic PREH unconditionally false
- restriction to "compatible" distributions still interesting



Landscape of Pseudorandom Encodings

Deterministic Encoding

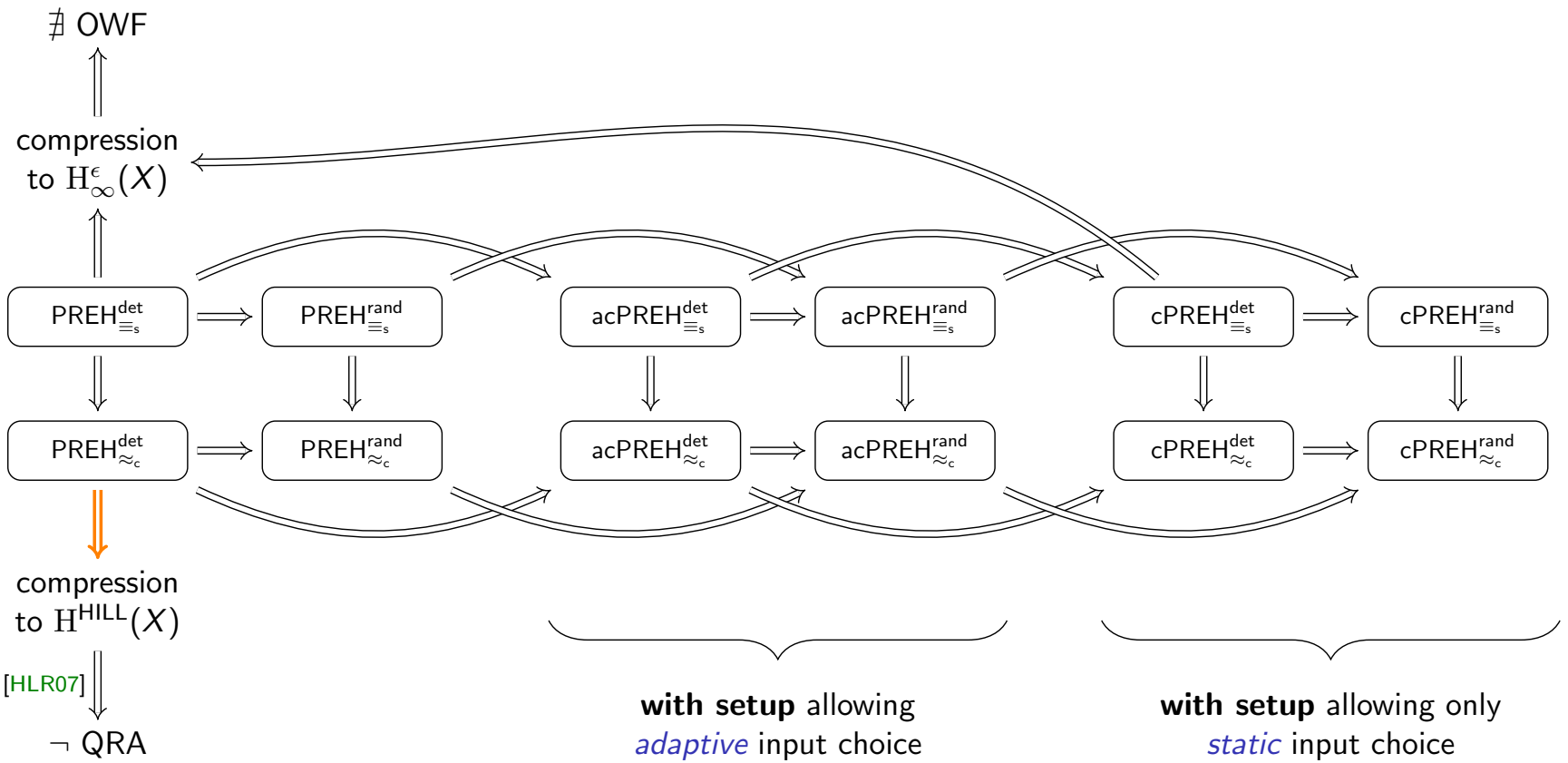
- deterministic PREH unconditionally false
- restriction to "compatible" distributions still interesting



Landscape of Pseudorandom Encodings

Deterministic Encoding

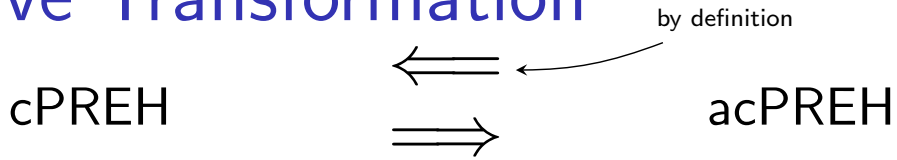
- deterministic PREH unconditionally false
- restriction to "compatible" distributions still interesting



Static-to-Adaptive Transformation

cPREH ⟸ acPREH

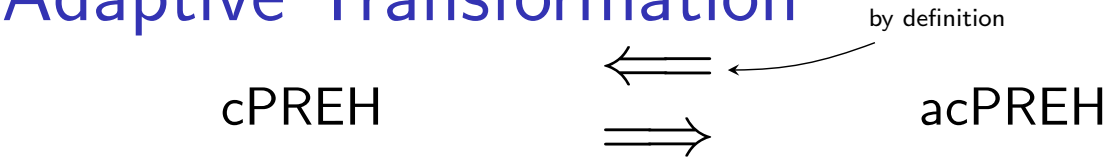
Static-to-Adaptive Transformation



build adaptive PRE from 2 static PRE instances

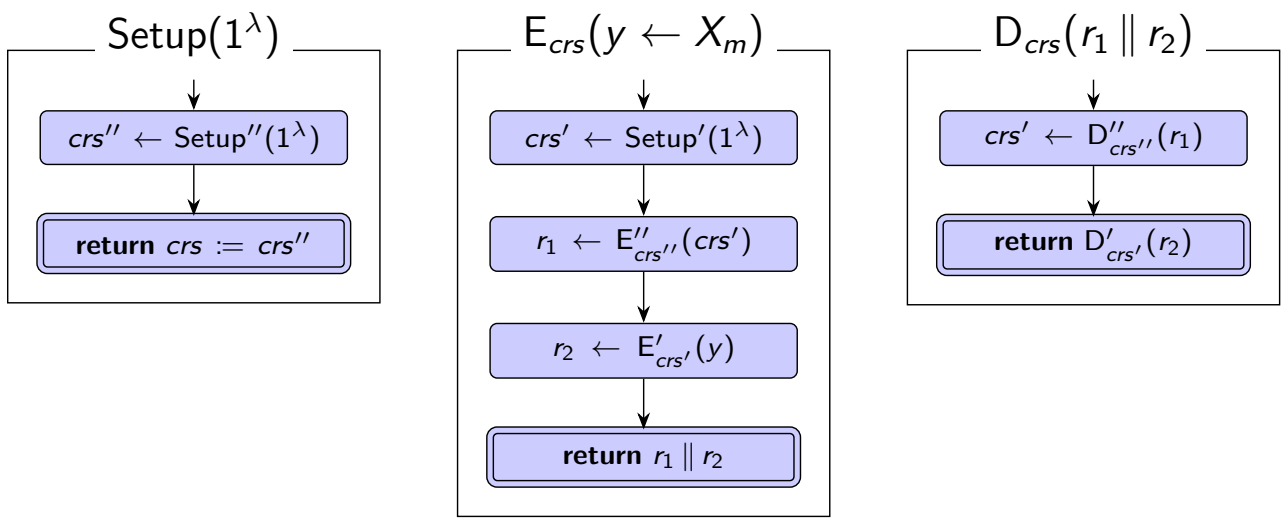
- for X: $(\mathsf{Setup}', \mathsf{E}', \mathsf{D}')$
- for Setup': $(\mathsf{Setup}'', \mathsf{E}'', \mathsf{D}'')$

Static-to-Adaptive Transformation

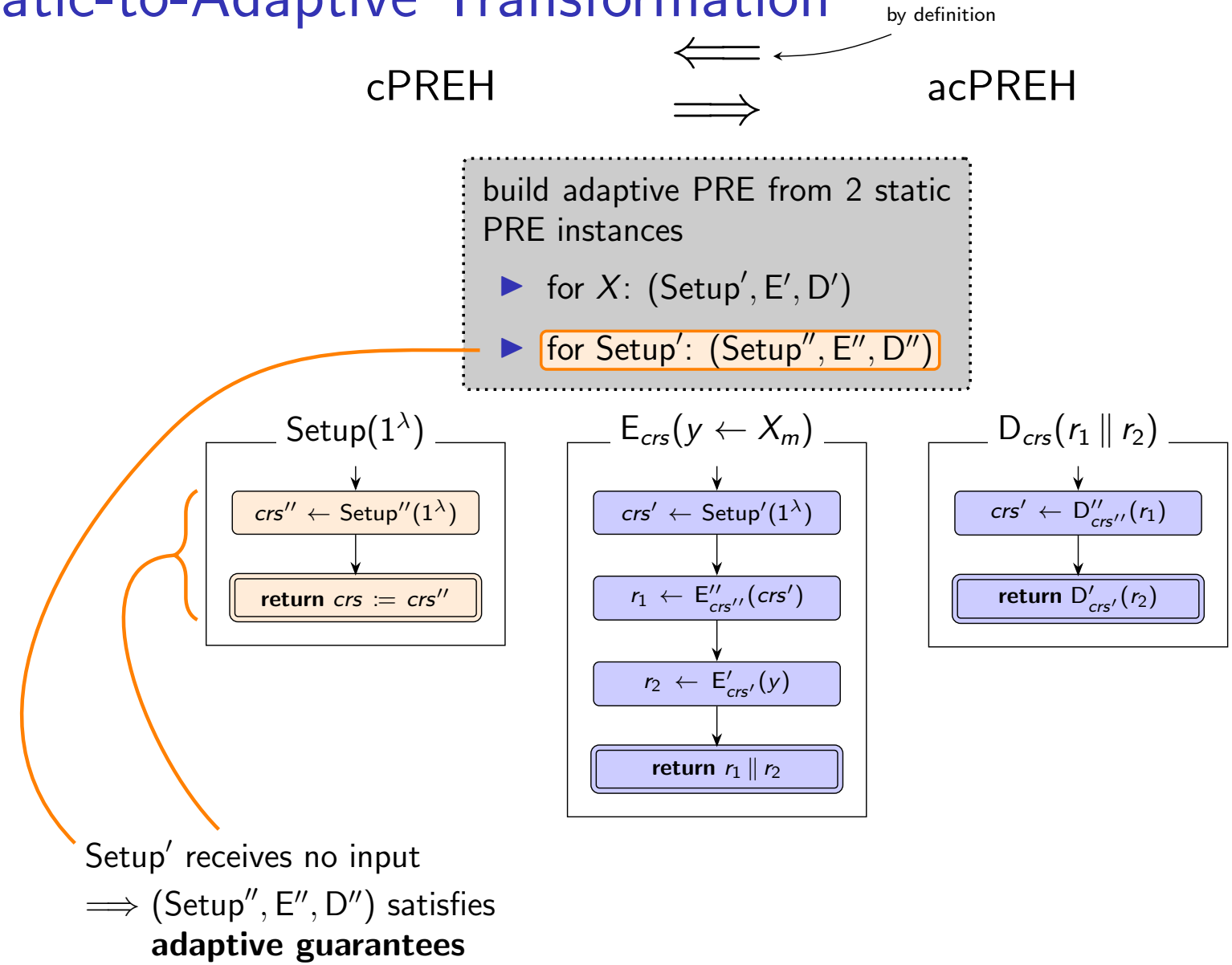


build adaptive PRE from 2 static PRE instances

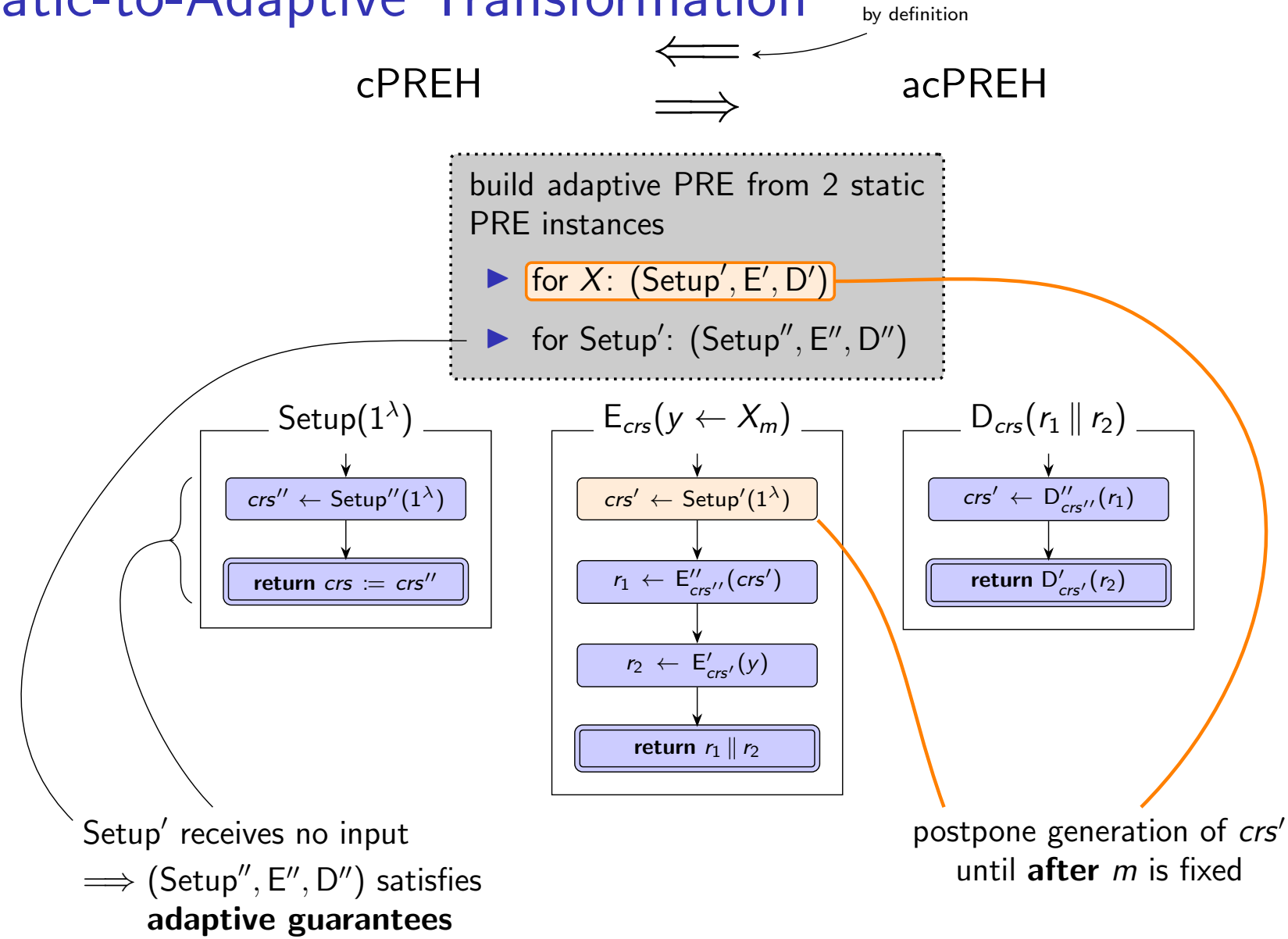
- for X: $(\mathsf{Setup}', \mathsf{E}', \mathsf{D}')$
- for Setup': $(\mathsf{Setup}'', \mathsf{E}'', \mathsf{D}'')$



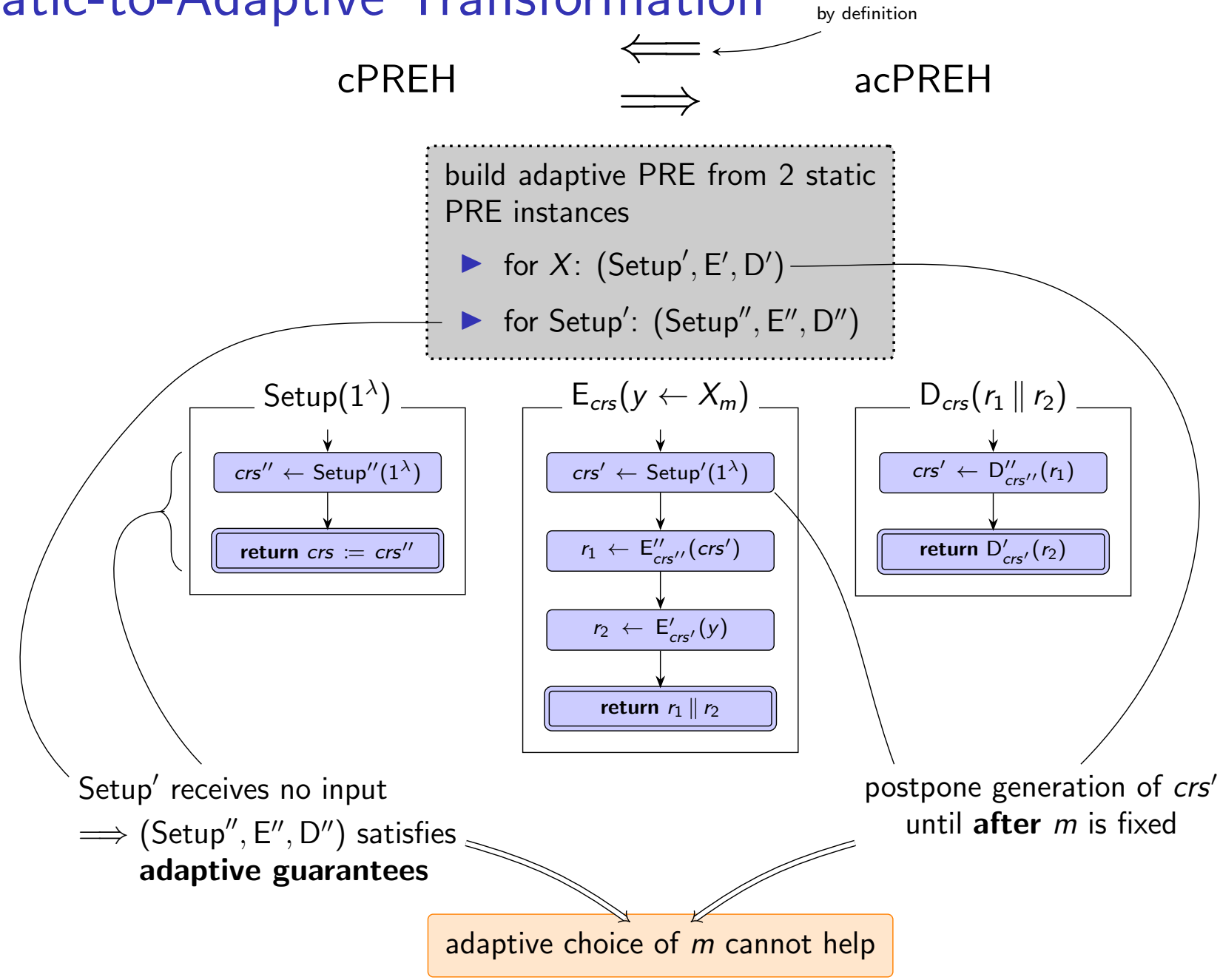
Static-to-Adaptive Transformation



Static-to-Adaptive Transformation



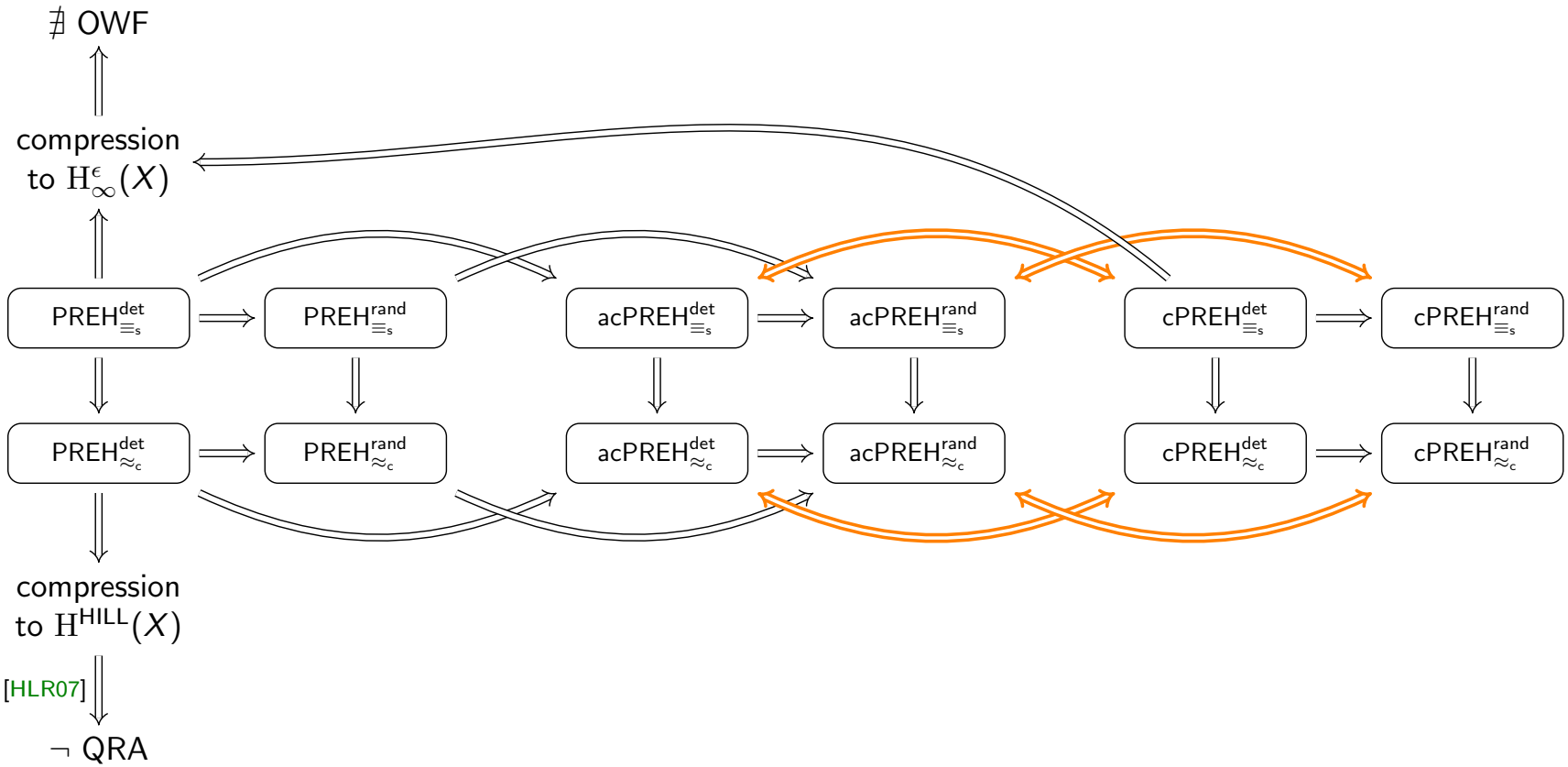
Static-to-Adaptive Transformation



Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

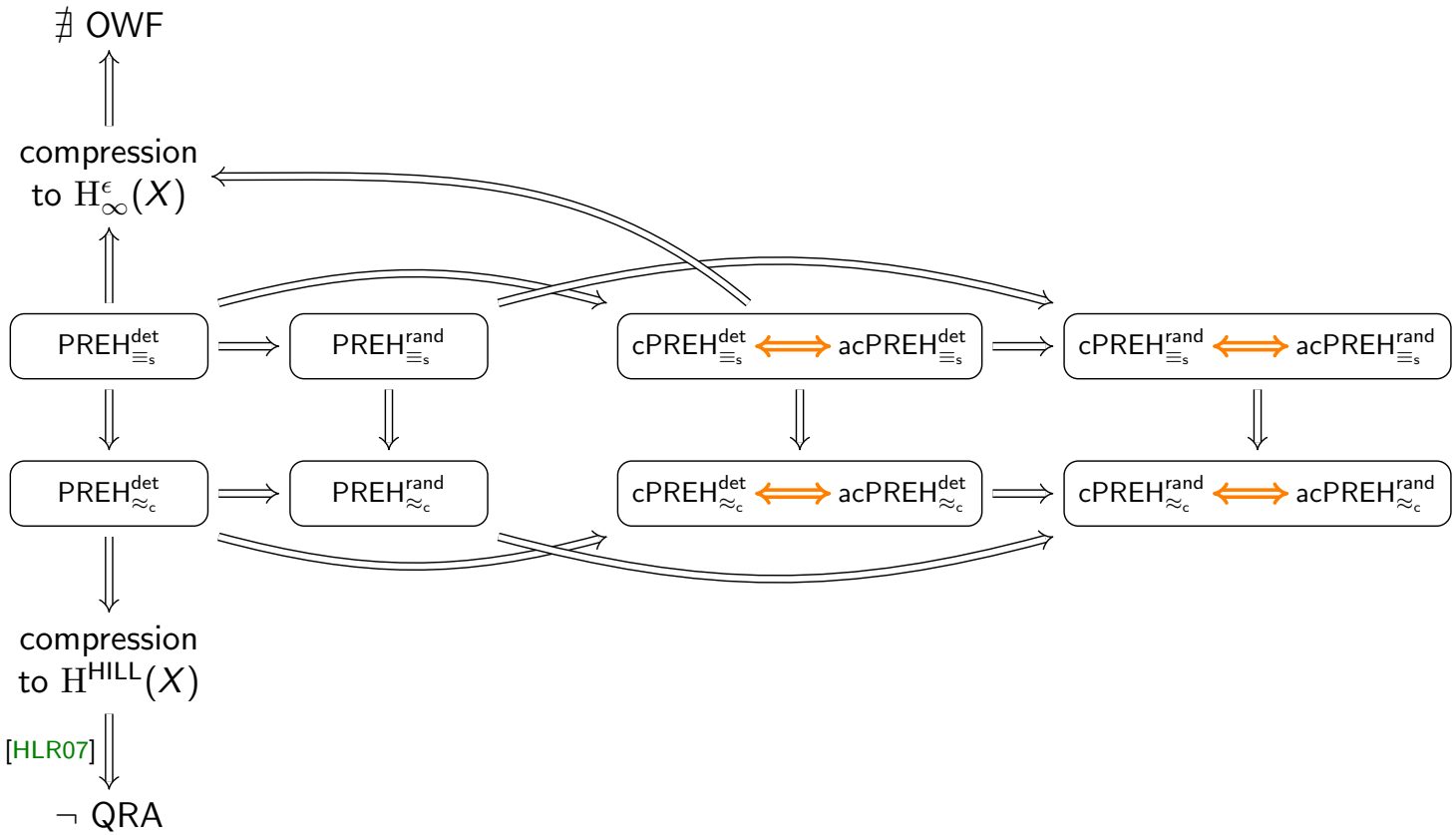
may depend on input m



Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

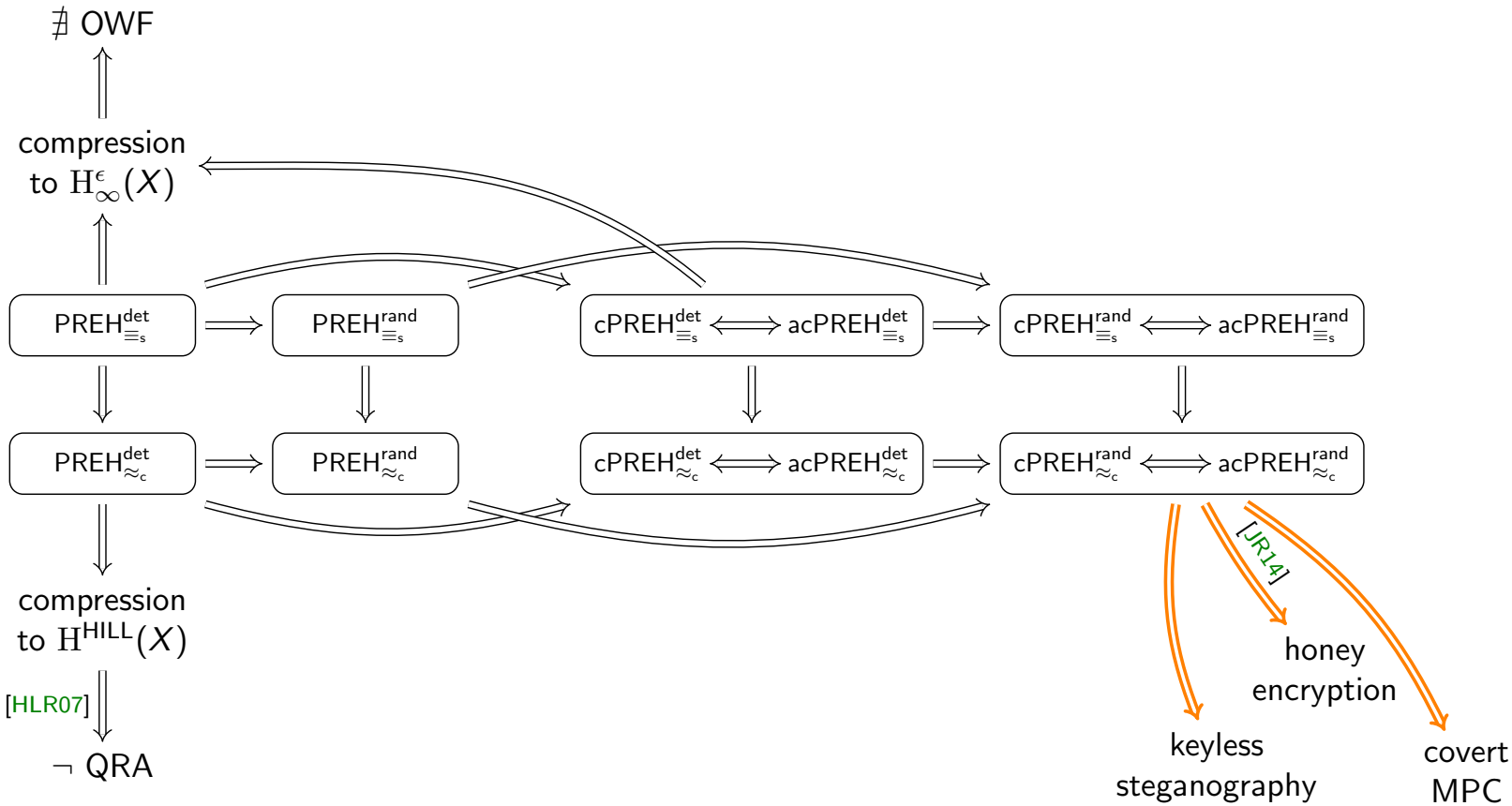
may depend on input m



Landscape of Pseudorandom Encodings

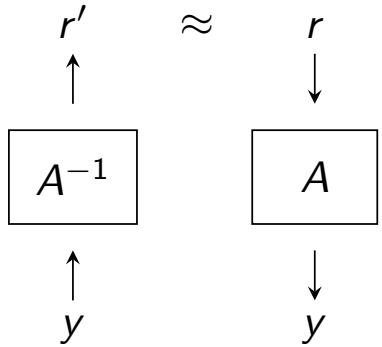
- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

may depend on input m



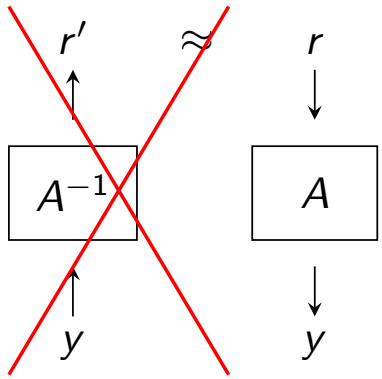
Invertible Sampling

- **problem:** is it efficiently possible to recover a random tape for some PPT algorithm?



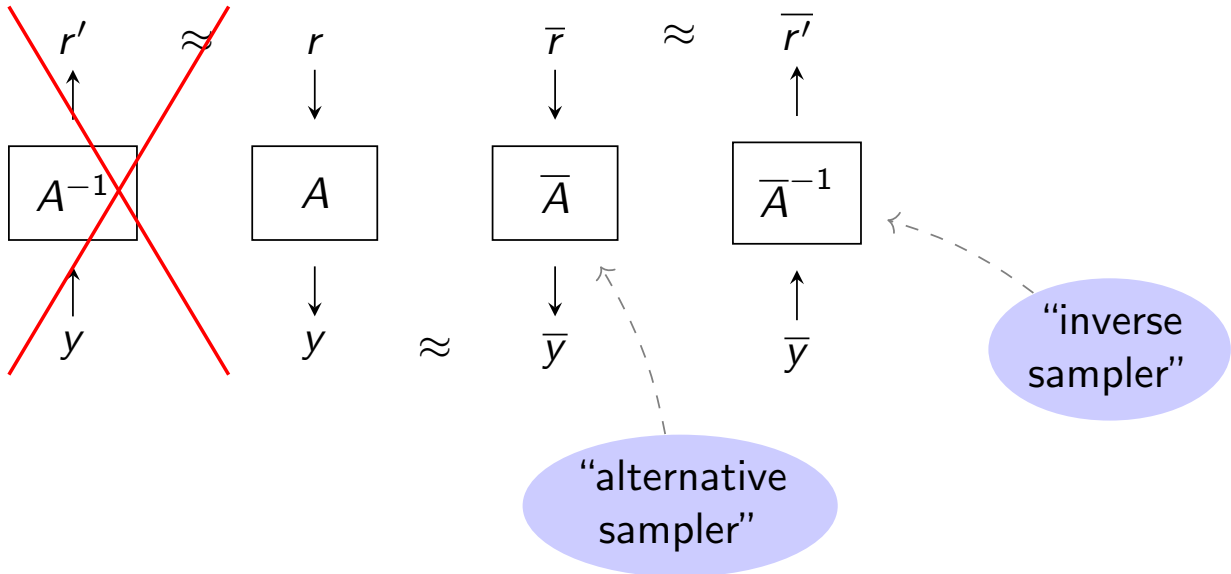
Invertible Sampling

- **problem:** is it efficiently possible to recover a random tape for some PPT algorithm?
- if yes, there are no *hard-on-average* problems



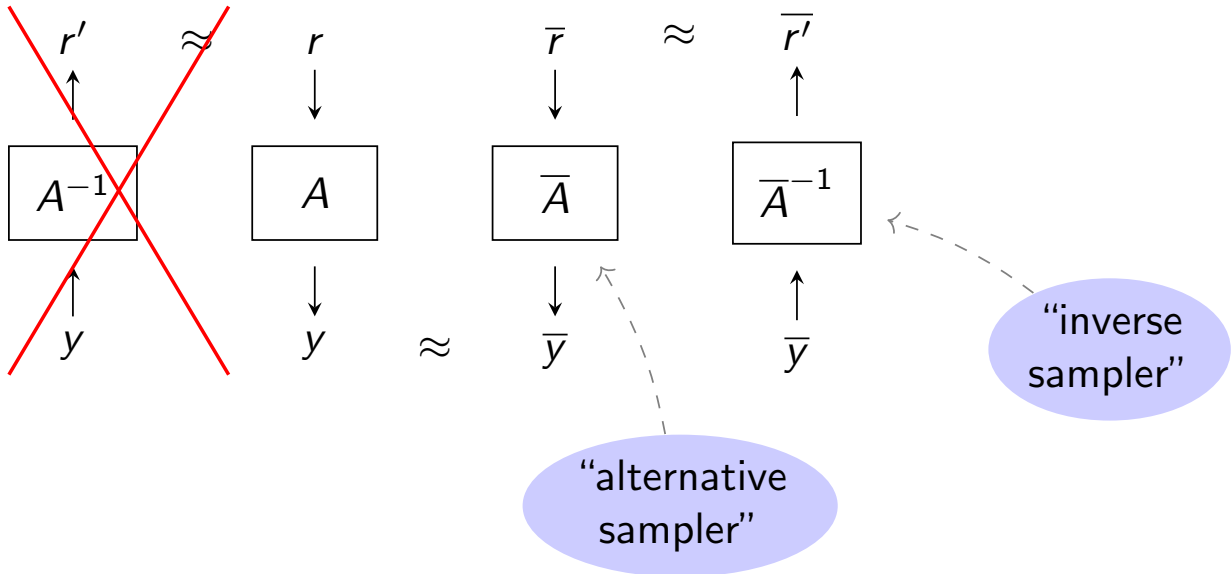
Invertible Sampling

- **problem:** is it efficiently possible to recover a random tape for some PPT algorithm?
- if yes, there are no *hard-on-average* problems



Invertible Sampling

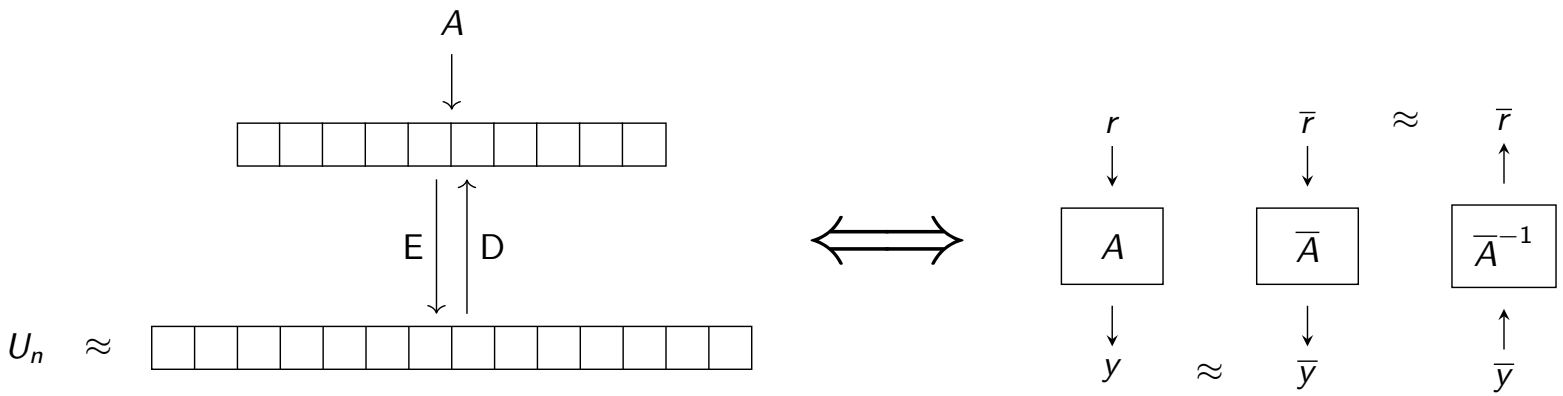
- **problem:** is it efficiently possible to recover a random tape for some PPT algorithm?
- if yes, there are no *hard-on-average* problems



- invertible sampling is an intriguing problem studied in [CFGN96; DN00; GKM+00; IKOS10]
- allows for oblivious sampling
- [IKOS10] establish an equivalence between fully adaptively secure MPC and invertible sampling for all PPT algorithms

Pseudorandom Encodings and Invertible Sampling

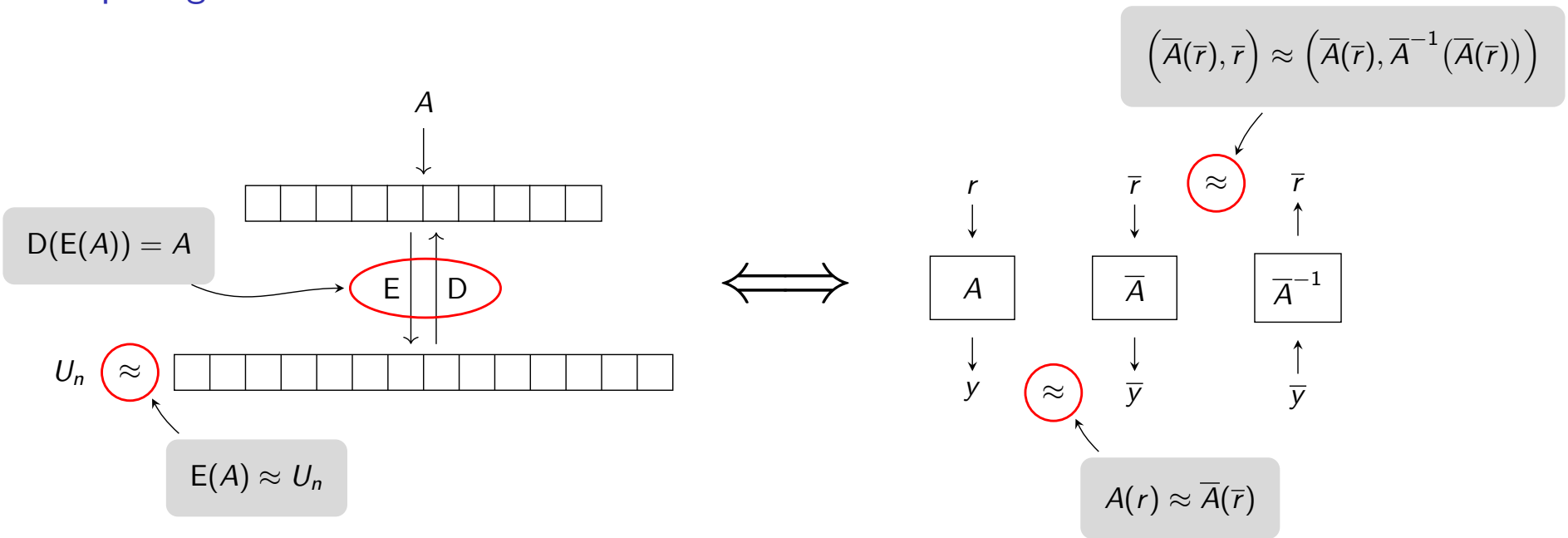
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

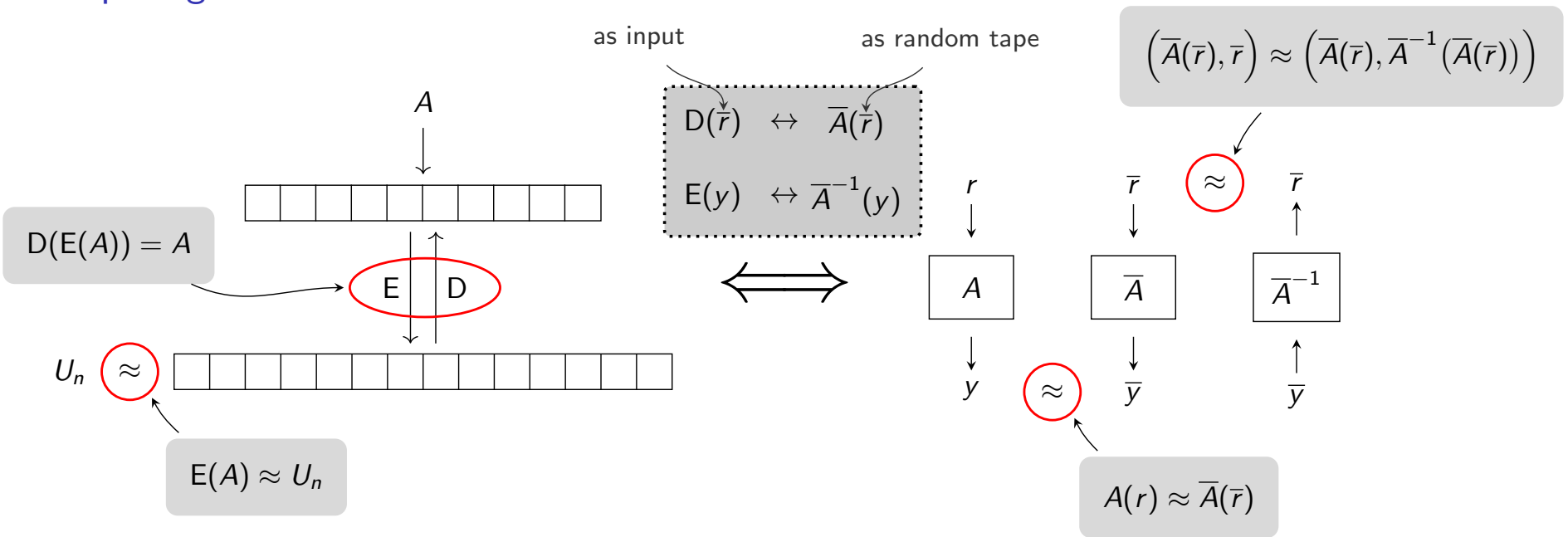
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

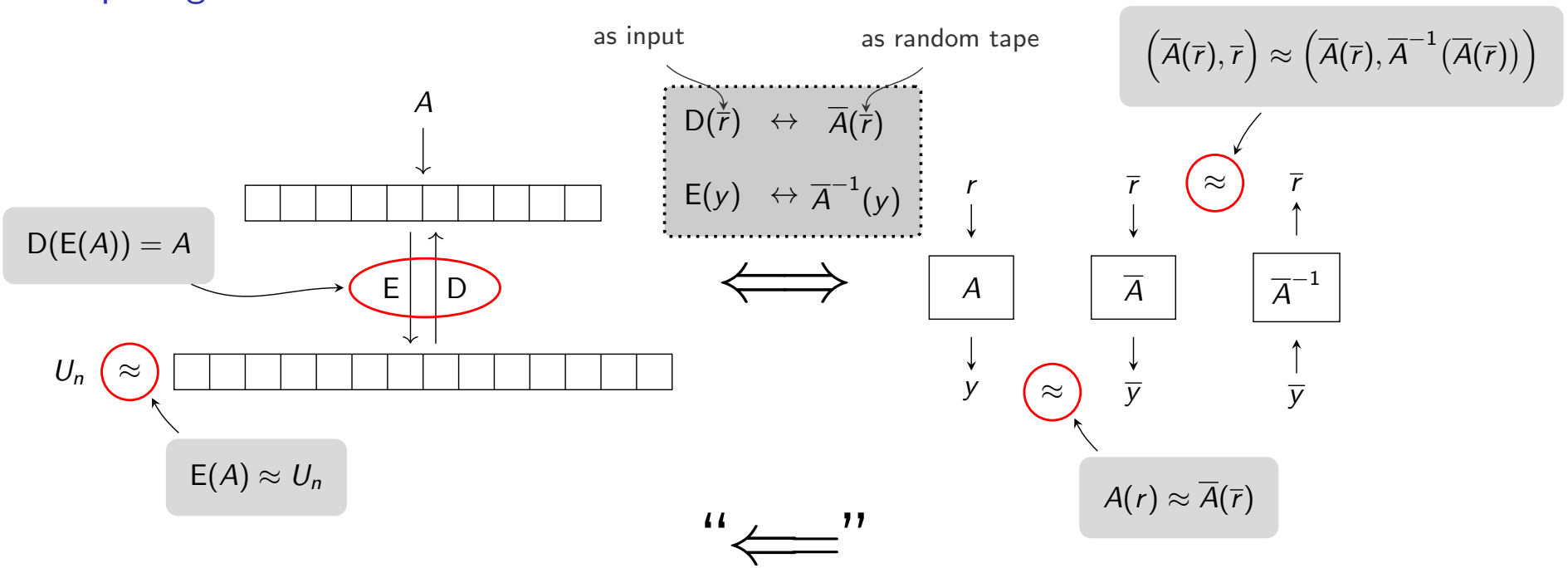
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

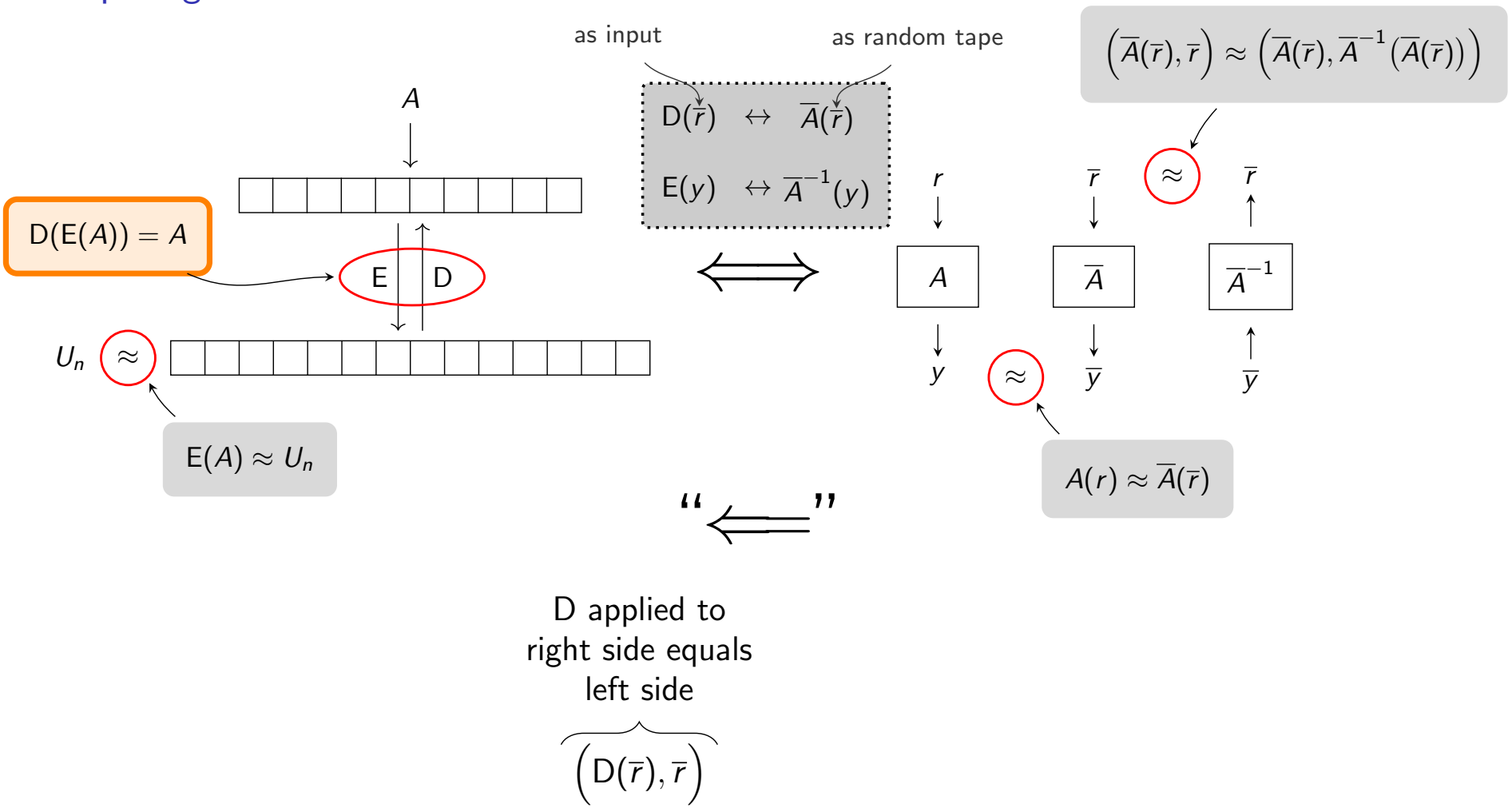
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

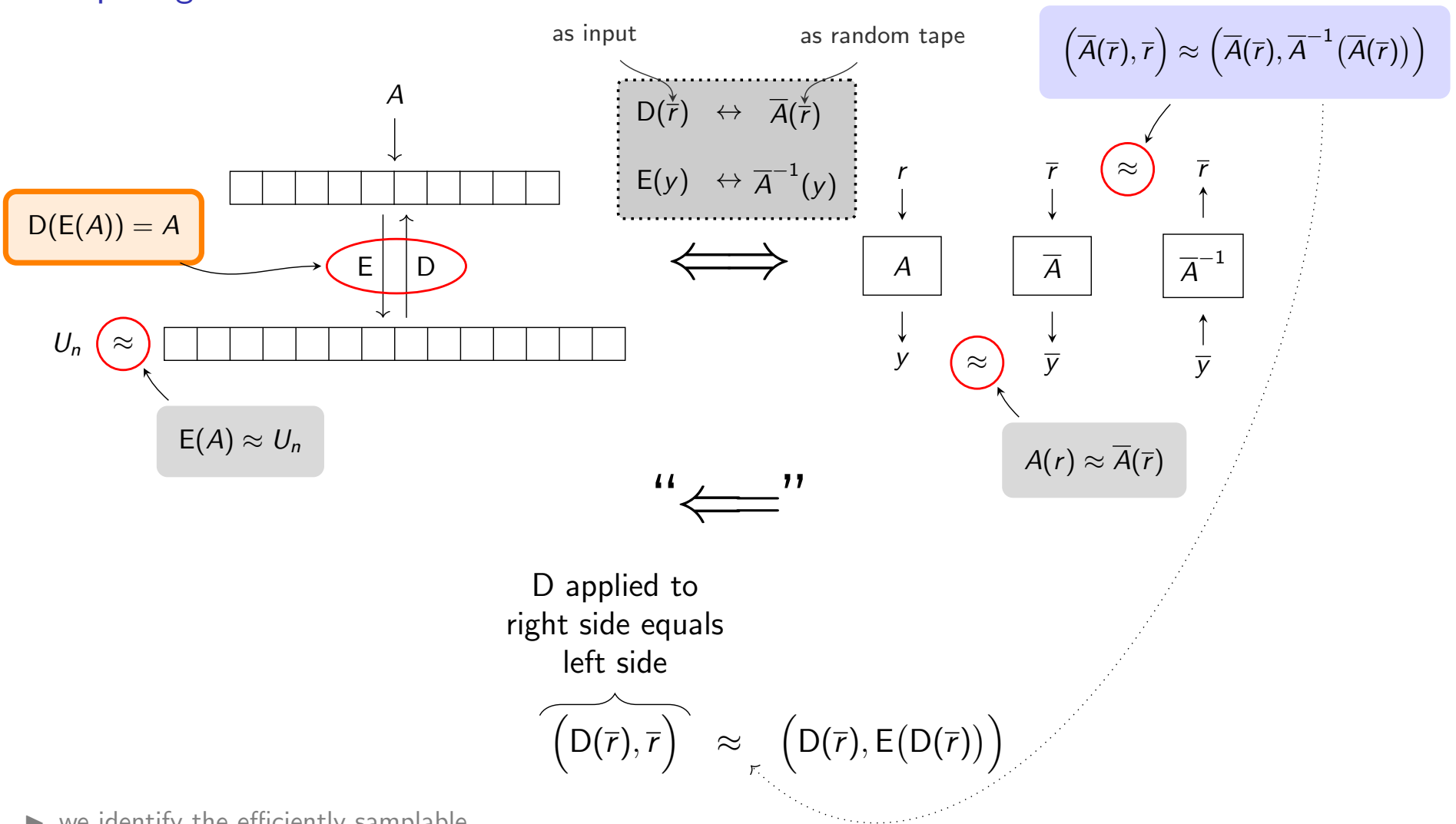
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

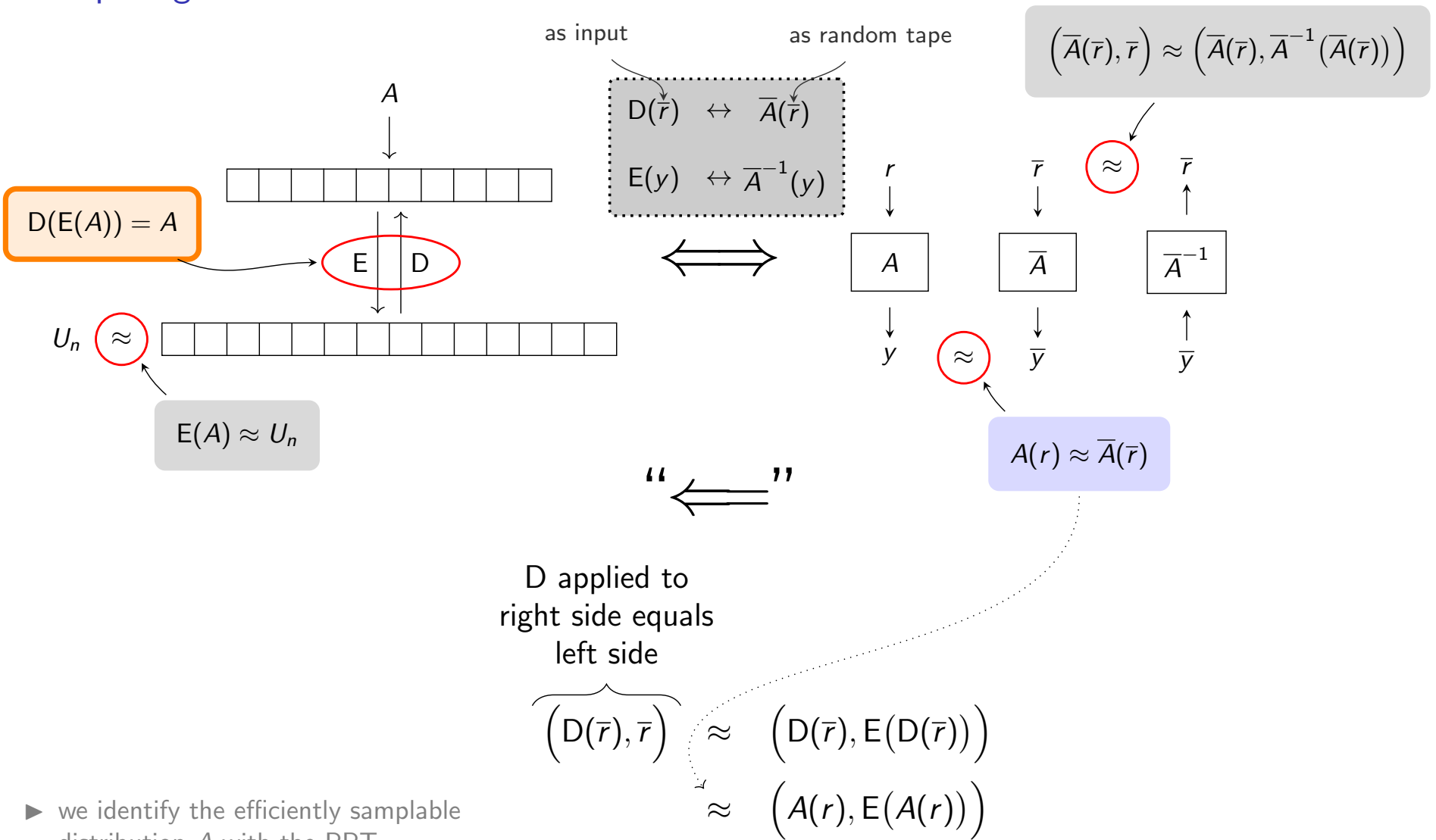
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

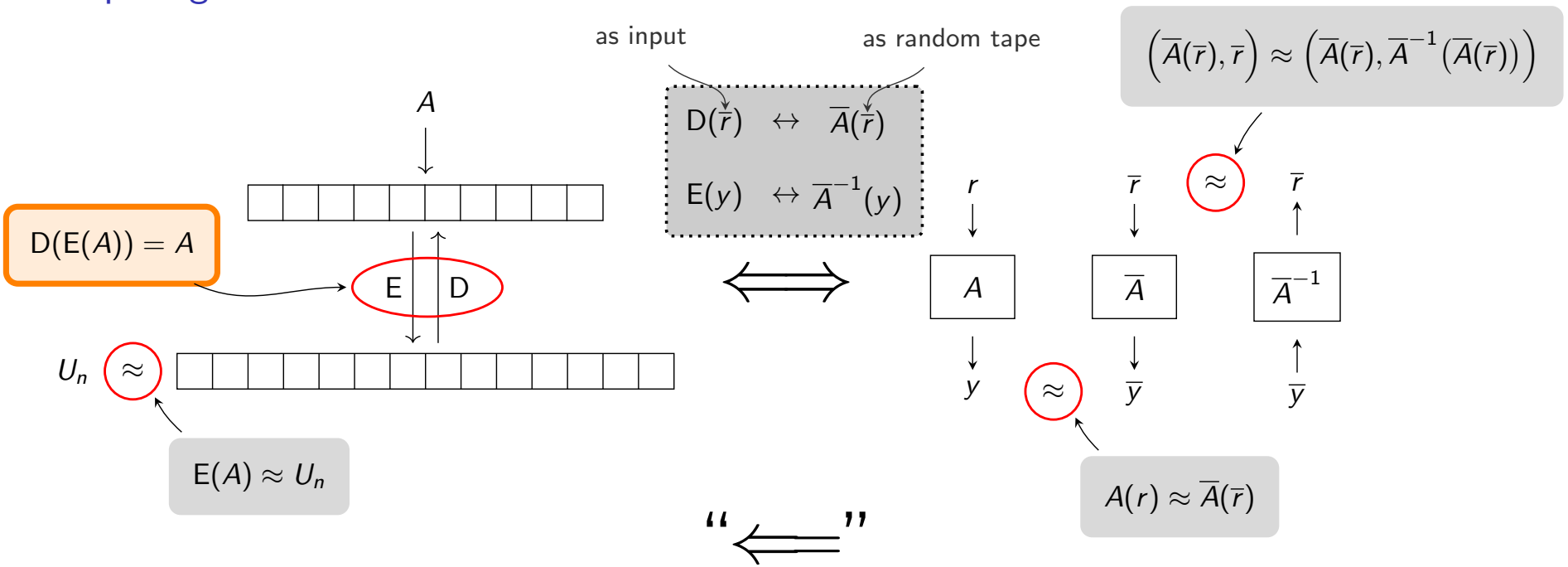
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection



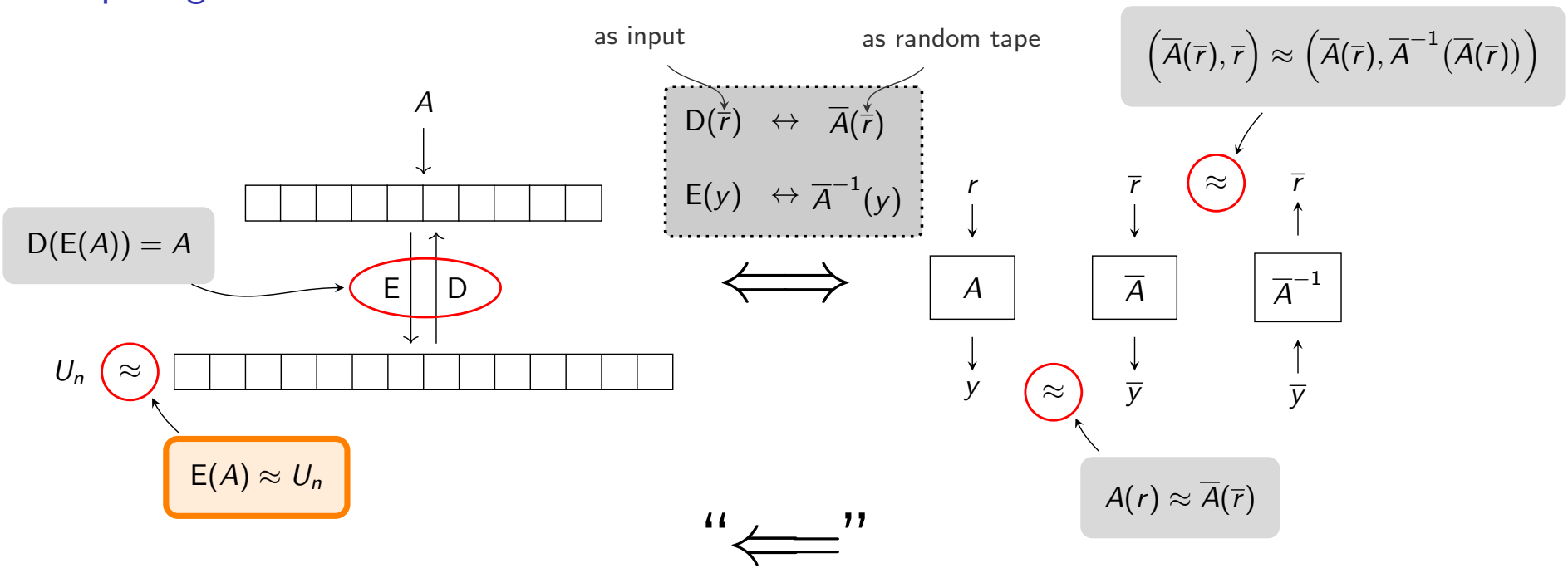
D applied to right side equals left side

$$\overbrace{\left(\mathrm{D}(\overline{r}), \overline{r}\right)} \approx \left(\mathrm{D}(\overline{r}), \mathrm{E}(\mathrm{D}(\overline{r}))\right)$$
$$\approx \left(A(r), \mathrm{E}(A(r))\right)$$
$$\Longrightarrow \mathrm{D}\left(\mathrm{E}(A(r))\right) = A(r)$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection

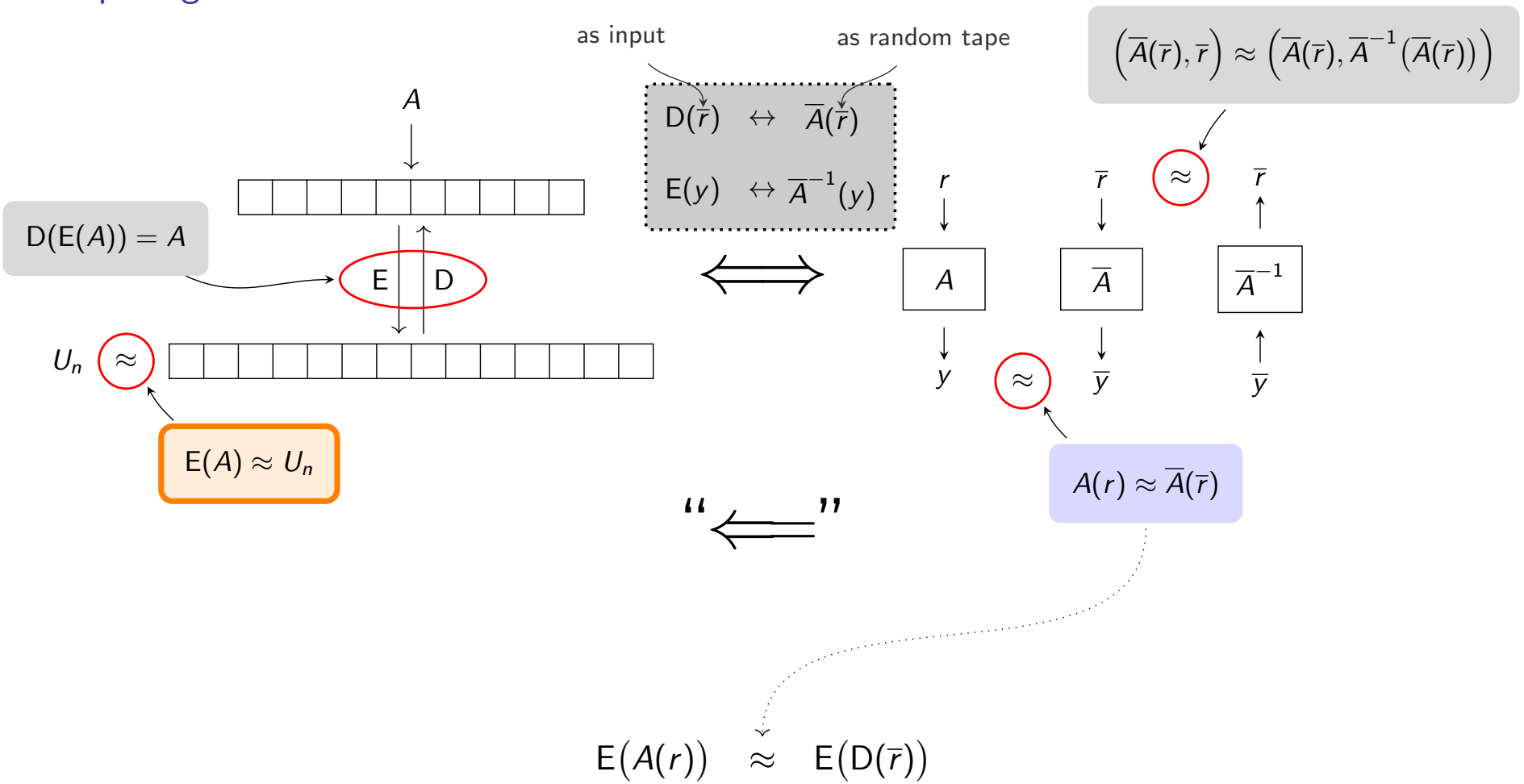


$$\mathsf{E}\big(A(r)\big)$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

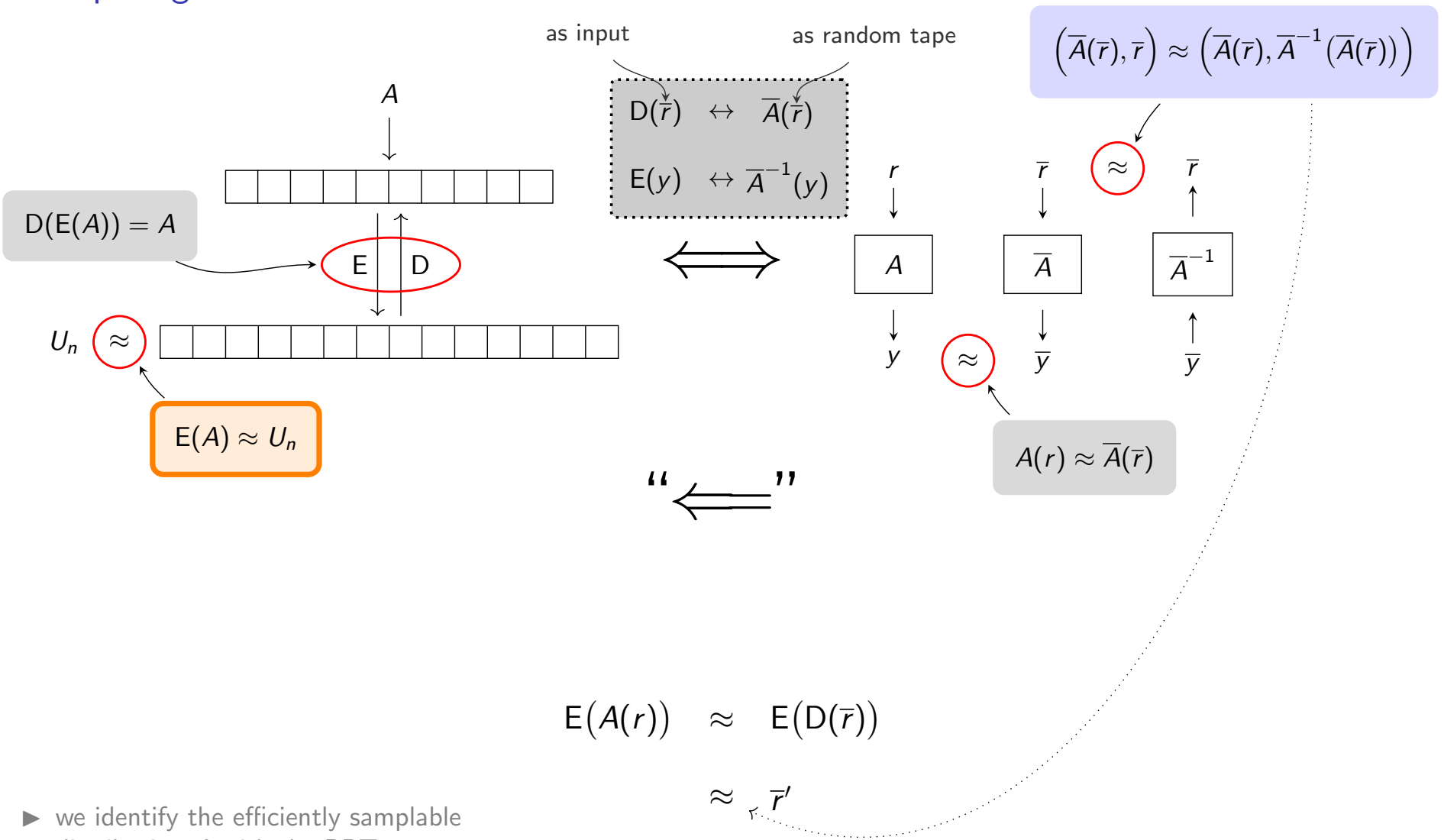
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

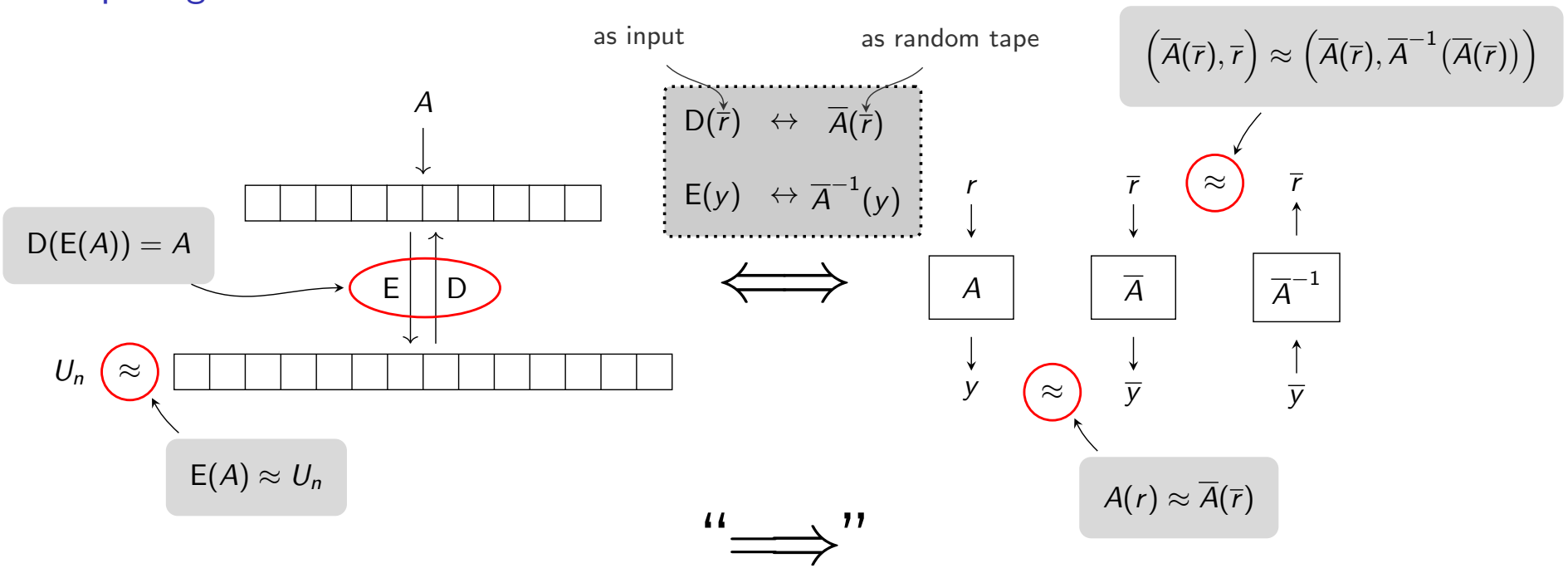
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

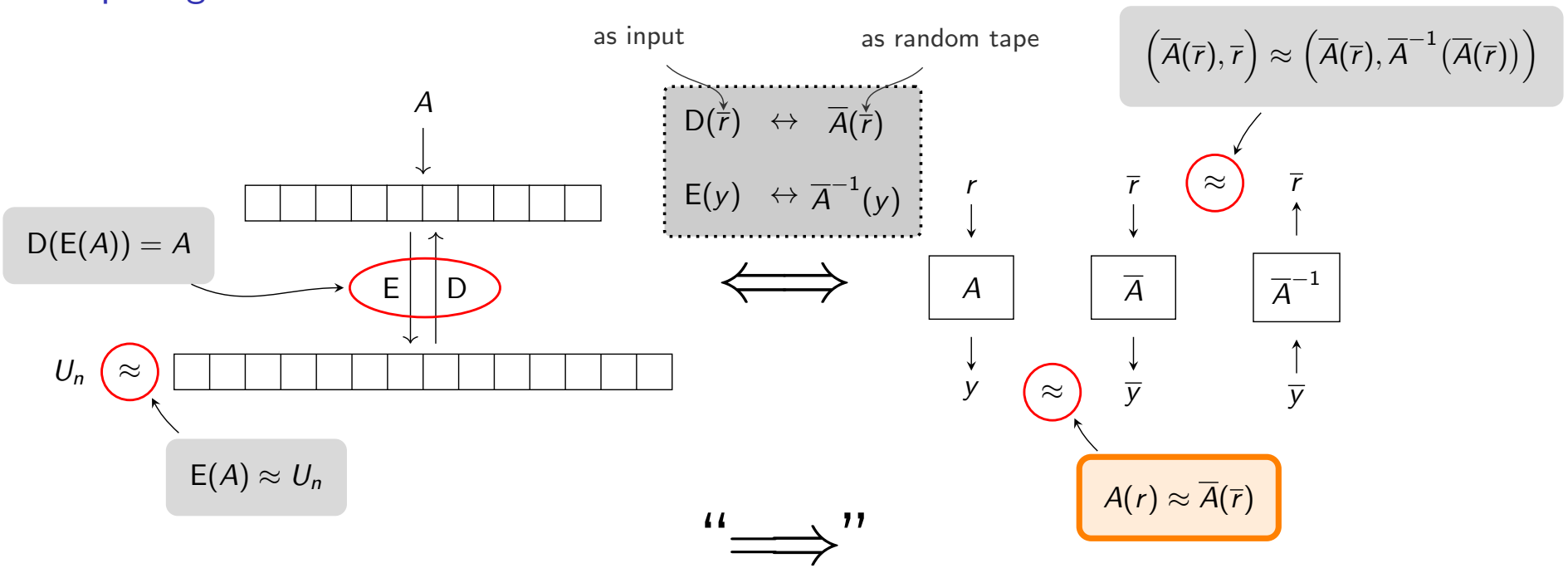
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

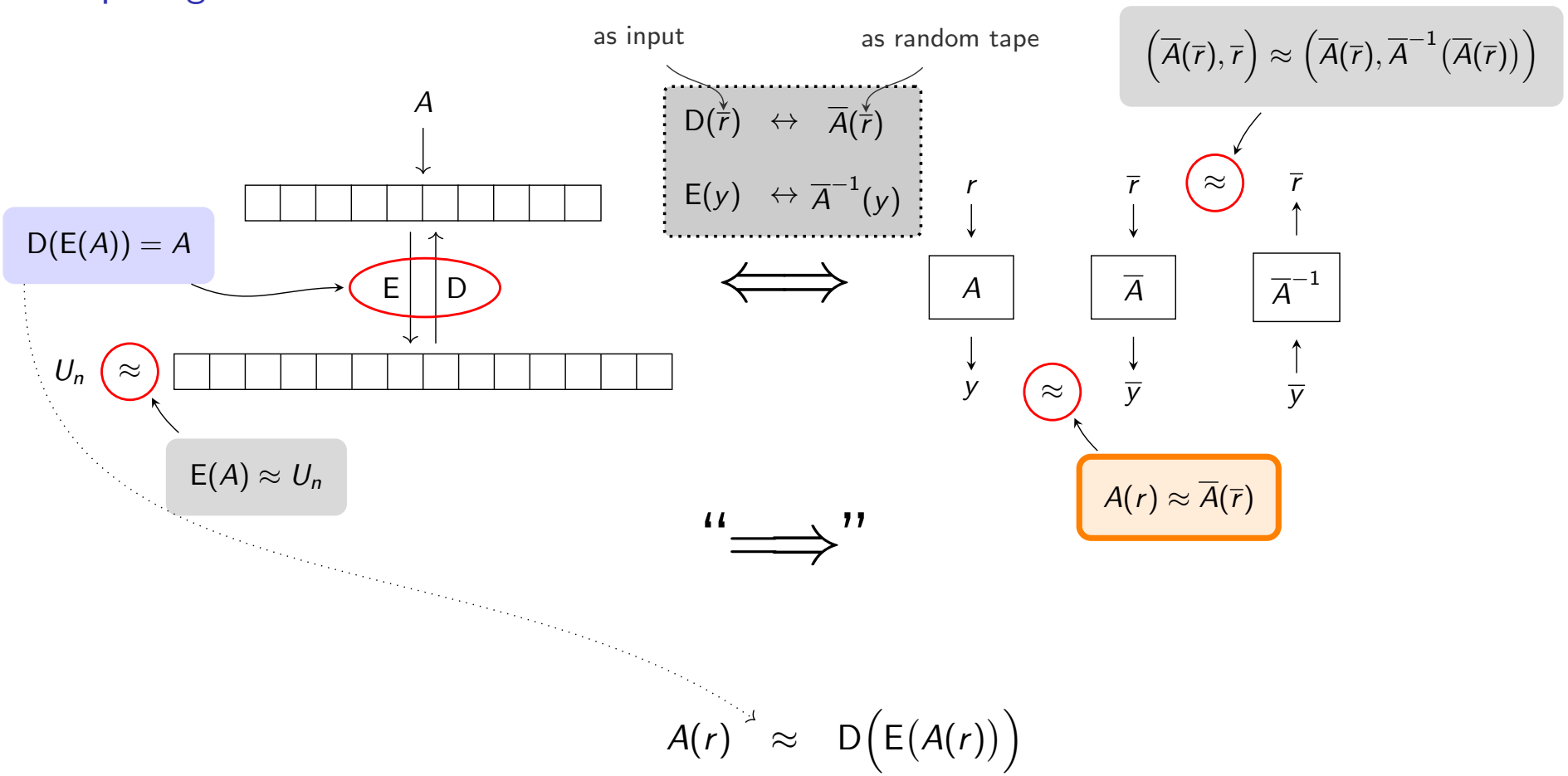
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

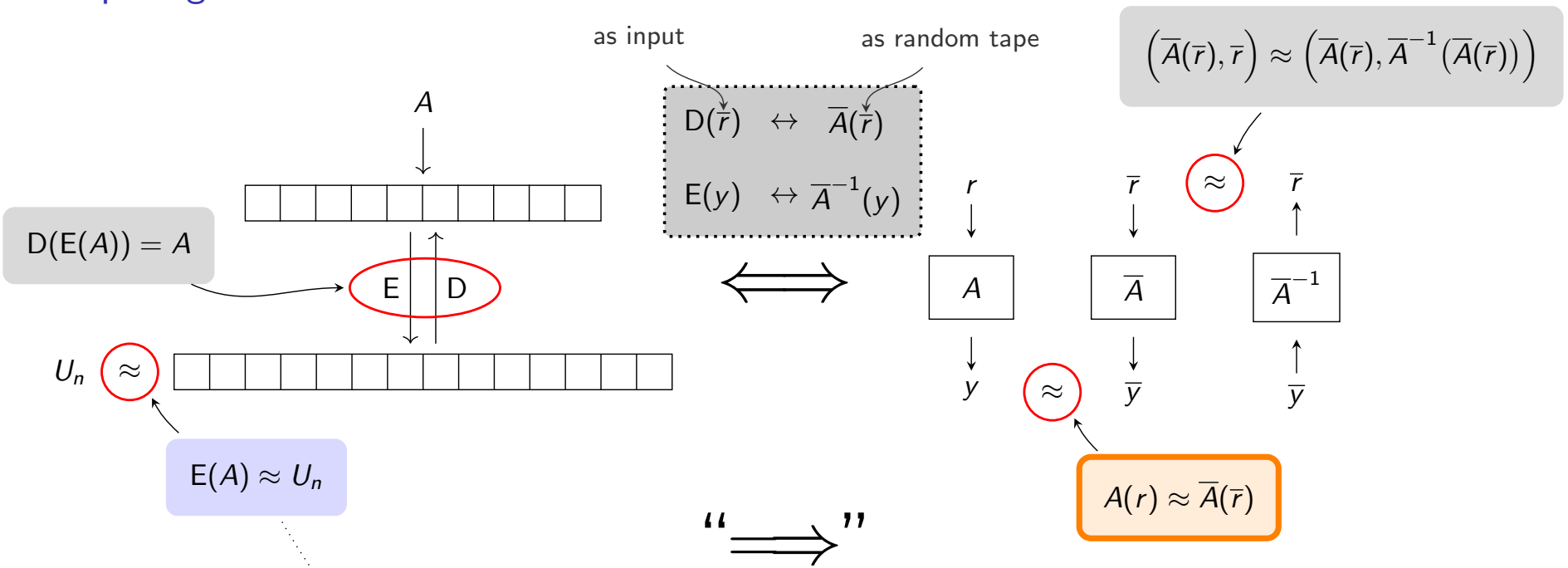
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection

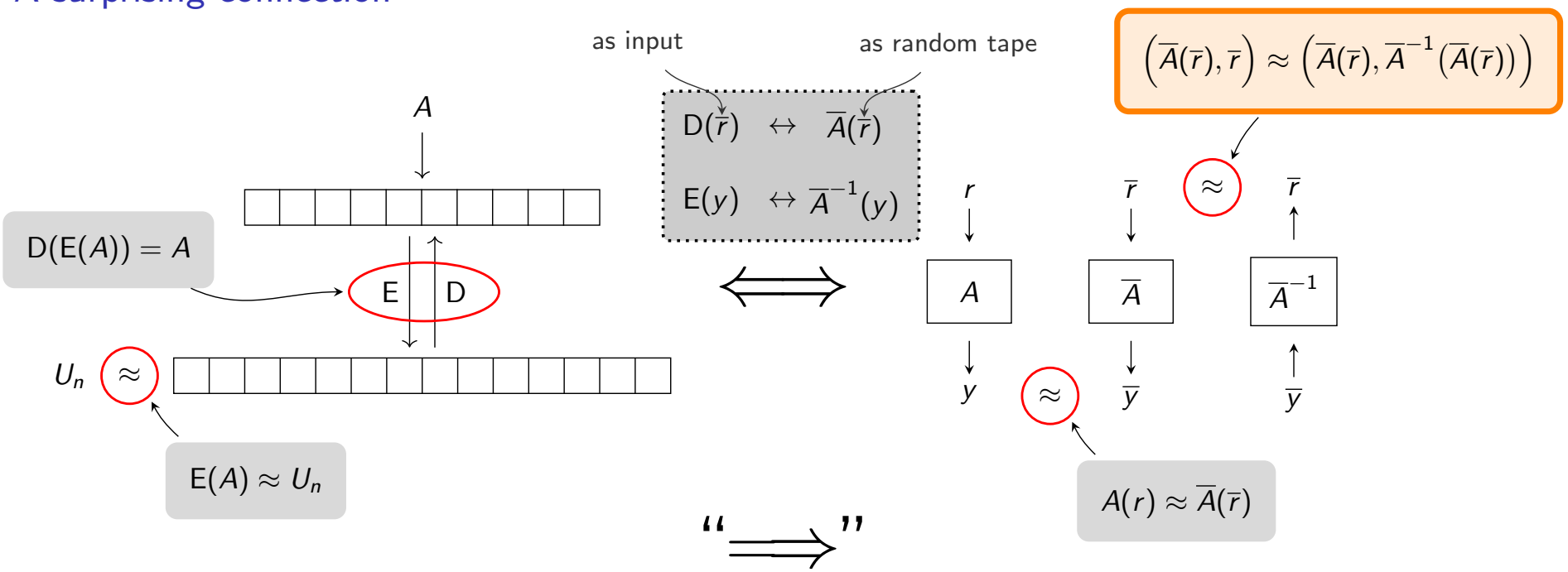


$$A(r) \approx \mathsf{D}\left(\mathsf{E}\left(A(r)\right)\right)$$
$$\approx \mathsf{D}\left(\overline{r}\right)$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection

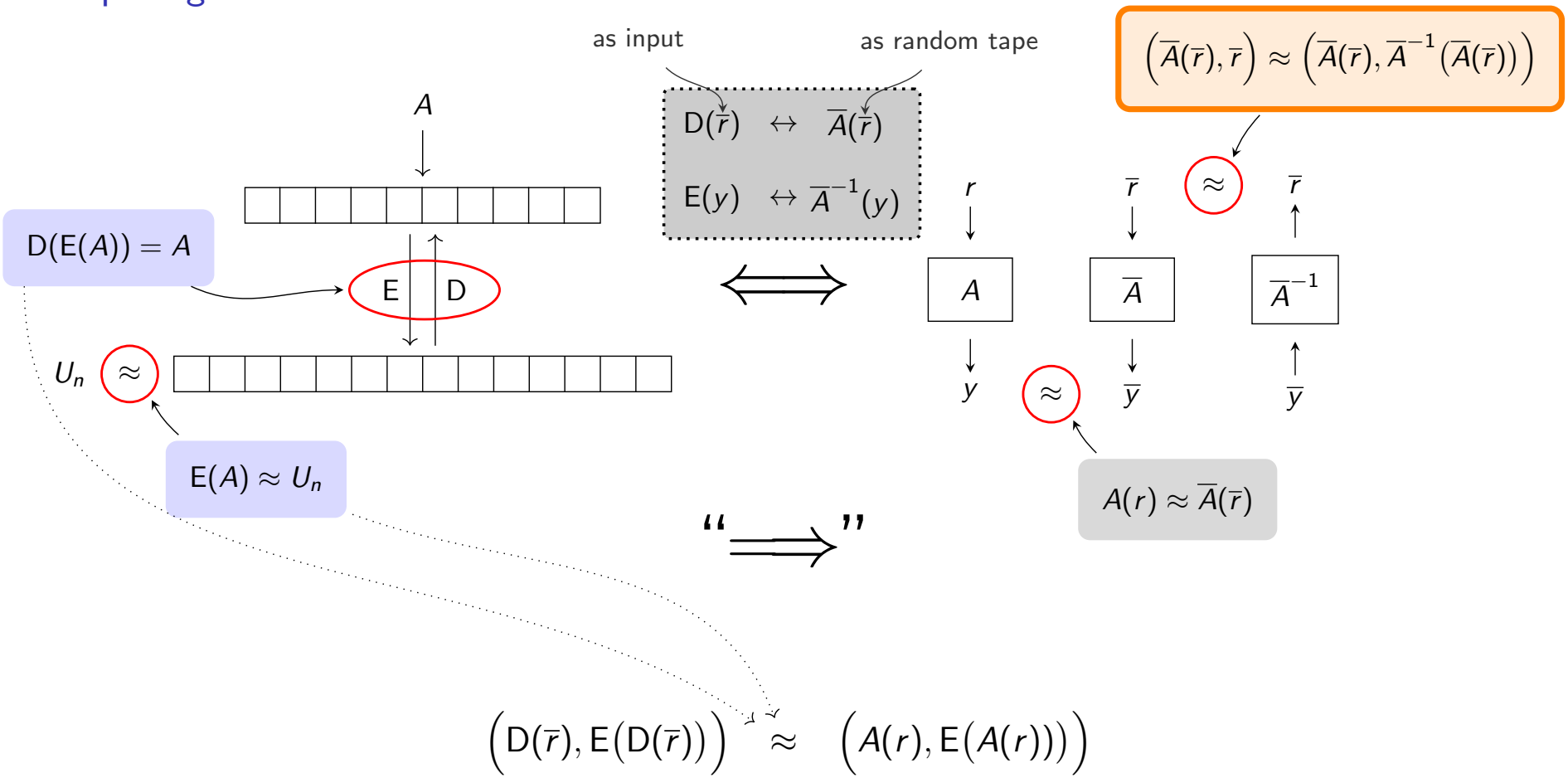


$$\left(\mathsf{D}(\overline{r}), \mathsf{E}\left(\mathsf{D}(\overline{r})\right)\right)$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

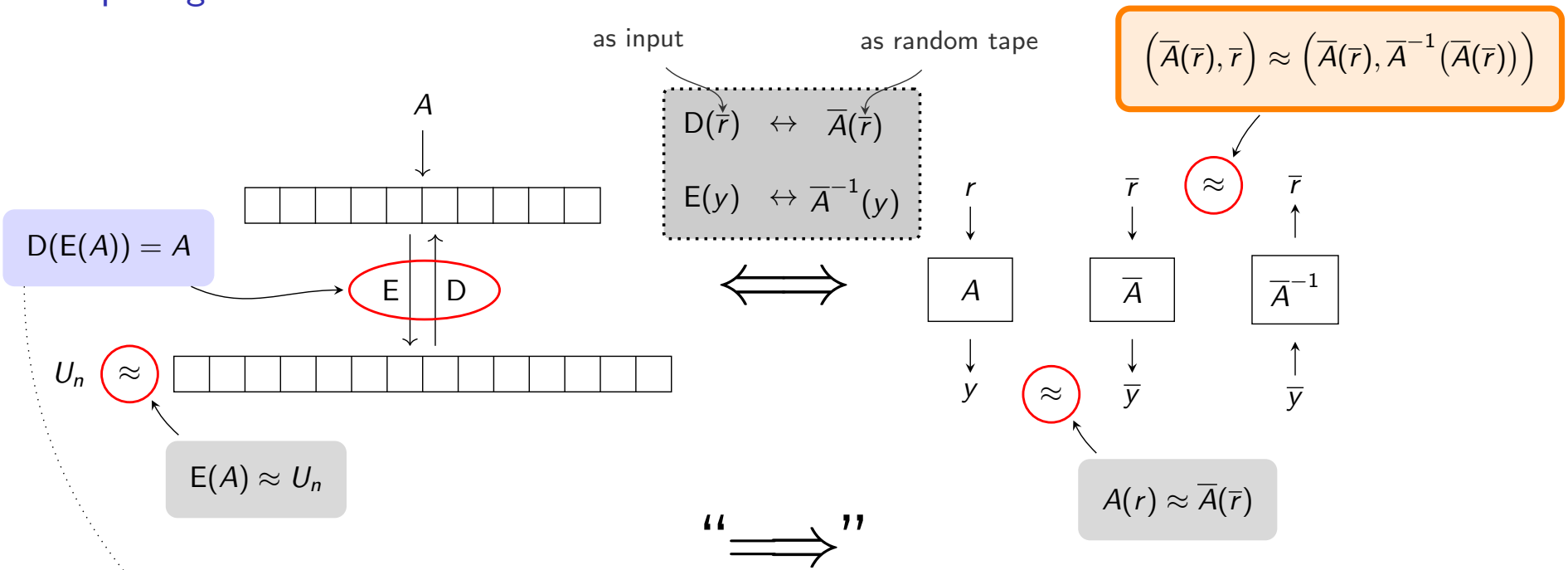
A surprising connection



- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection

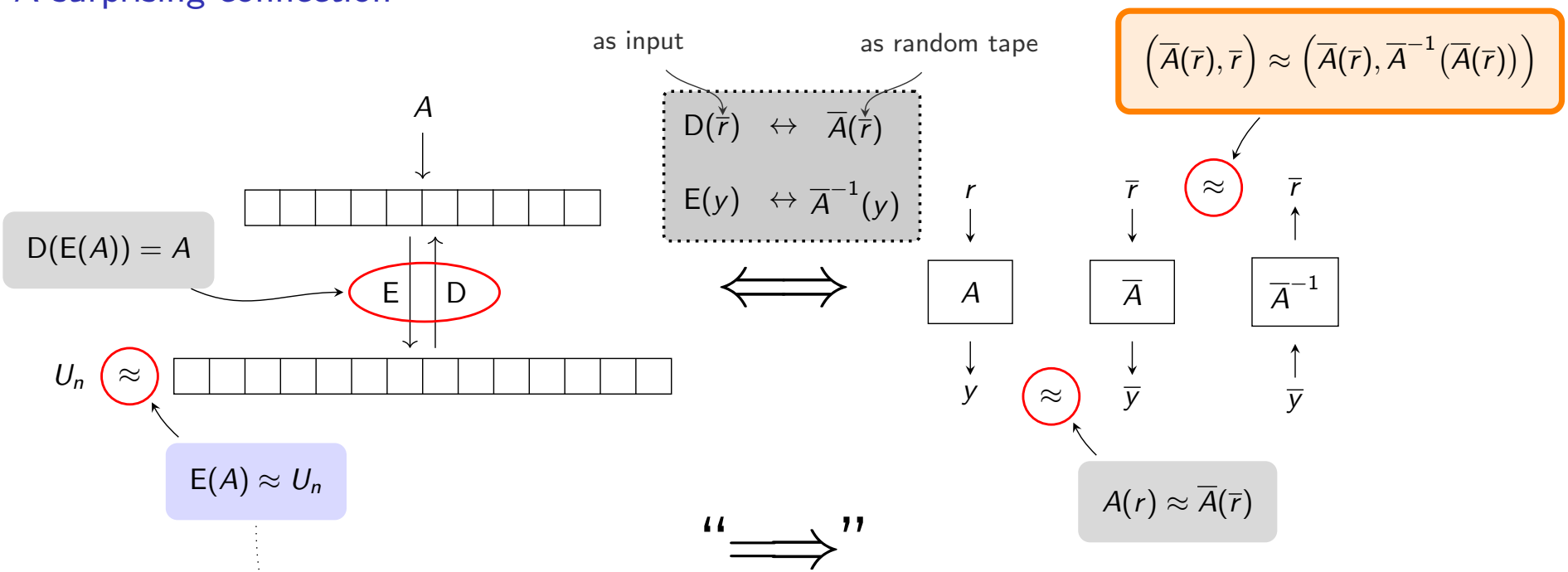


$$\left(\mathsf{D}(\overline{r}), \mathsf{E}(\mathsf{D}(\overline{r}))\right) \approx \left(A(r), \mathsf{E}(A(r))\right)$$
$$\approx \left(\mathsf{D}(\mathsf{E}(A(r))), \mathsf{E}(A(r))\right)$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Pseudorandom Encodings and Invertible Sampling

A surprising connection



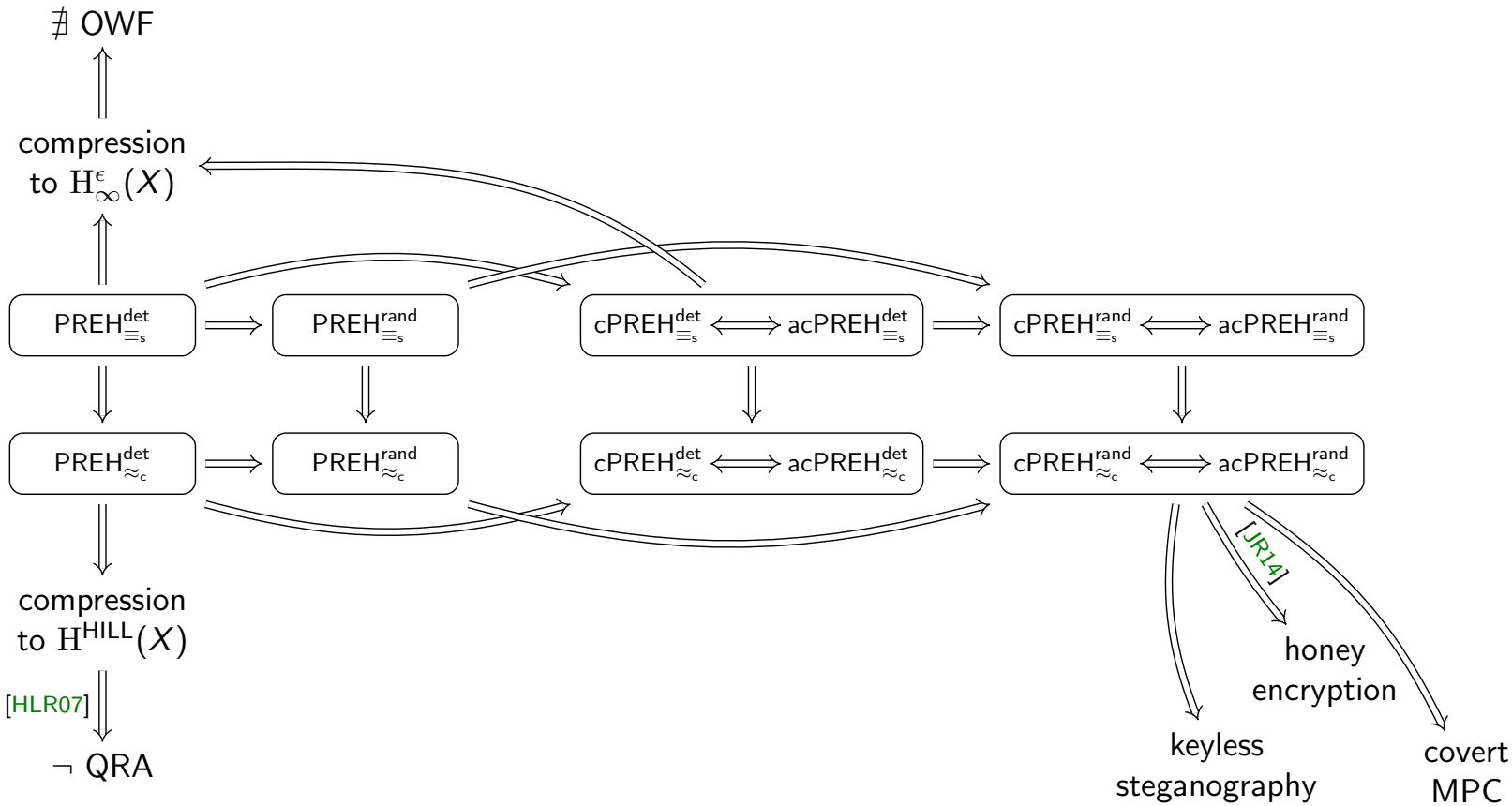
$$\begin{aligned}
\left(\mathsf{D}(\overline{r}), \mathsf{E}(\mathsf{D}(\overline{r}))\right) &\approx \left(A(r), \mathsf{E}(A(r))\right) \\
&\approx \left(\mathsf{D}(\mathsf{E}(A(r))), \mathsf{E}(A(r))\right) \\
&\approx \left(\mathsf{D}(\overline{r}), \overline{r}\right)
\end{aligned}$$

- we identify the efficiently samplable distribution A with the PPT algorithm A using a random tape r
- we omit the input m here

Landscape of Pseudorandom Encodings

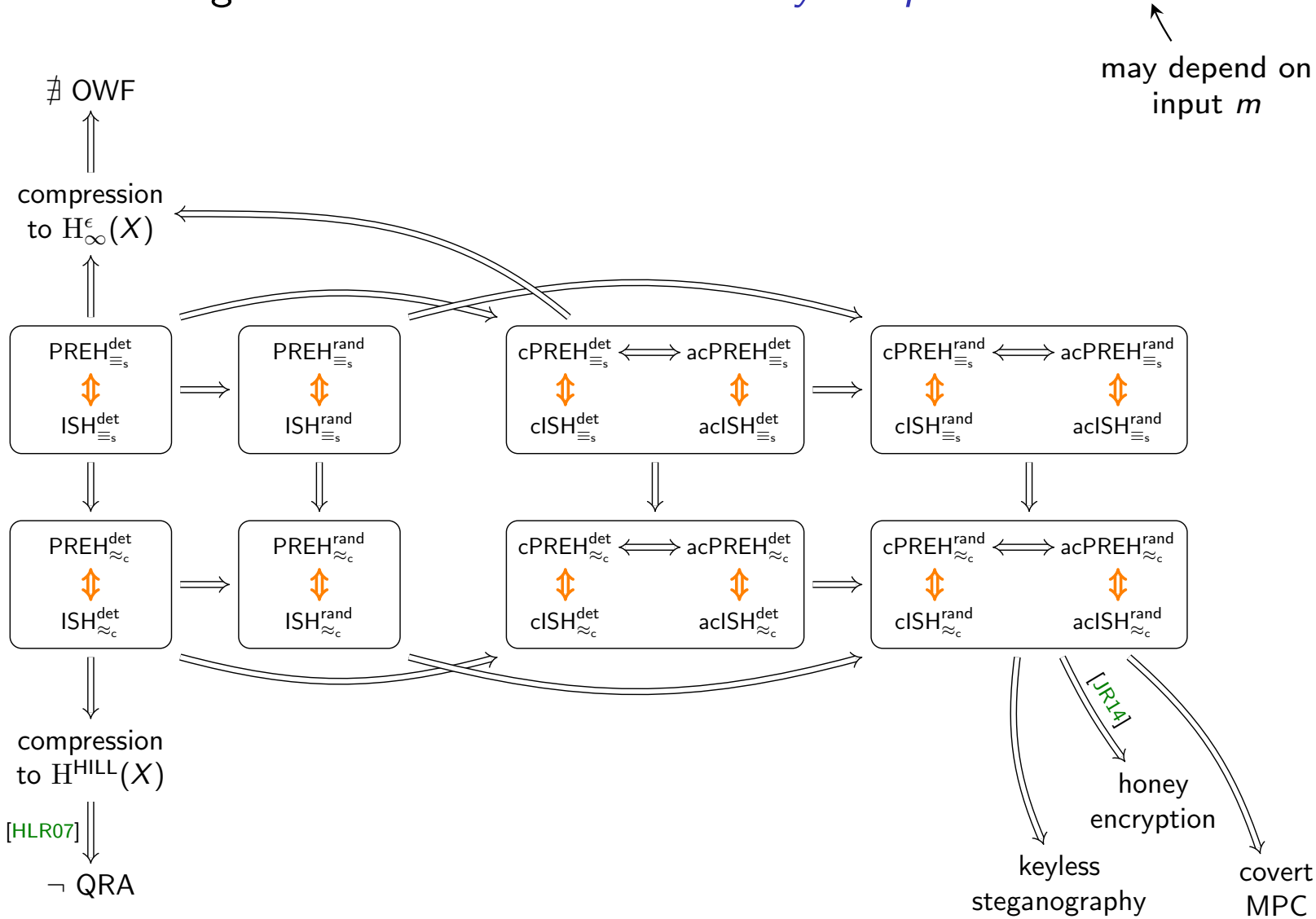
- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*

may depend on input m



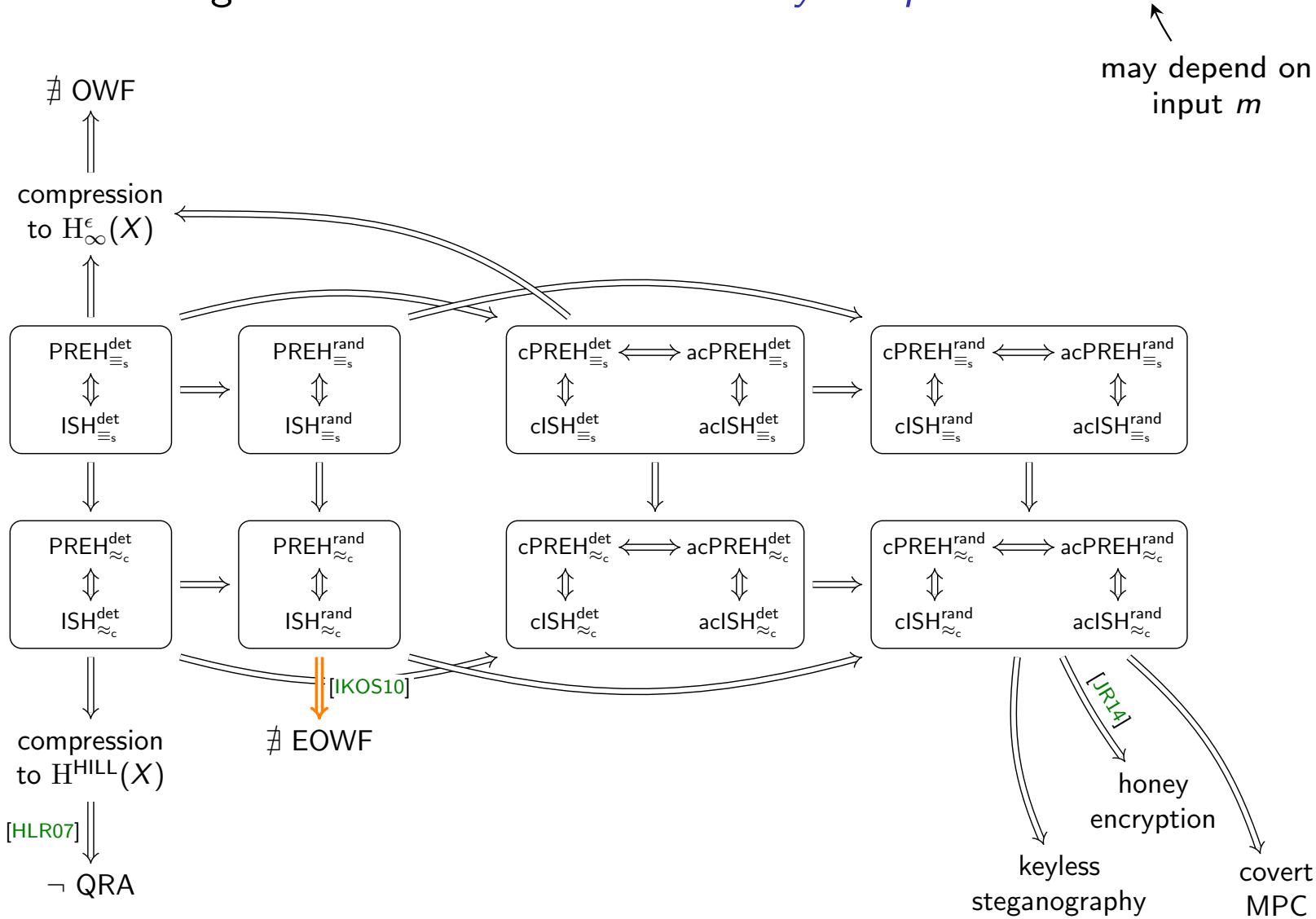
Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



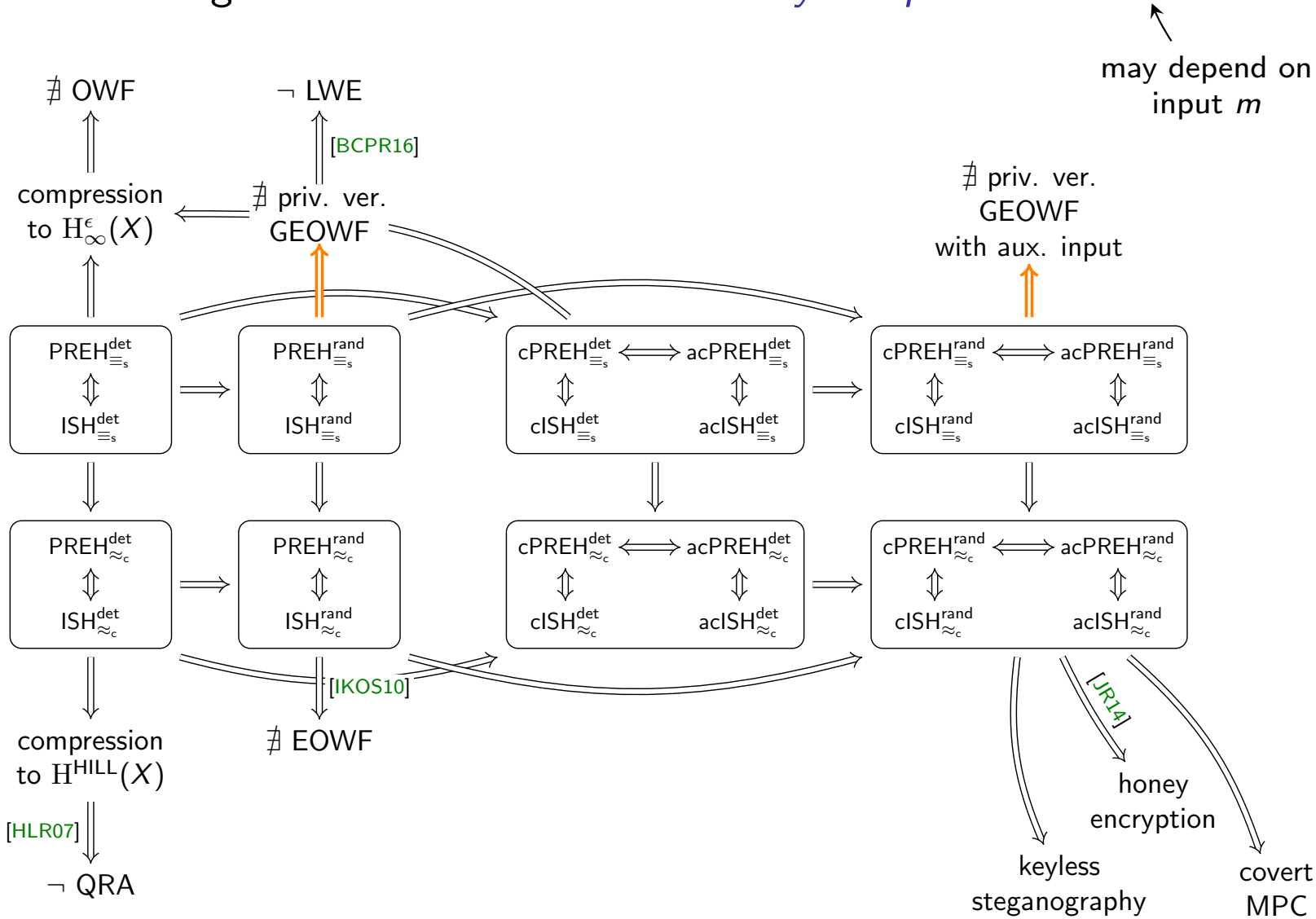
Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



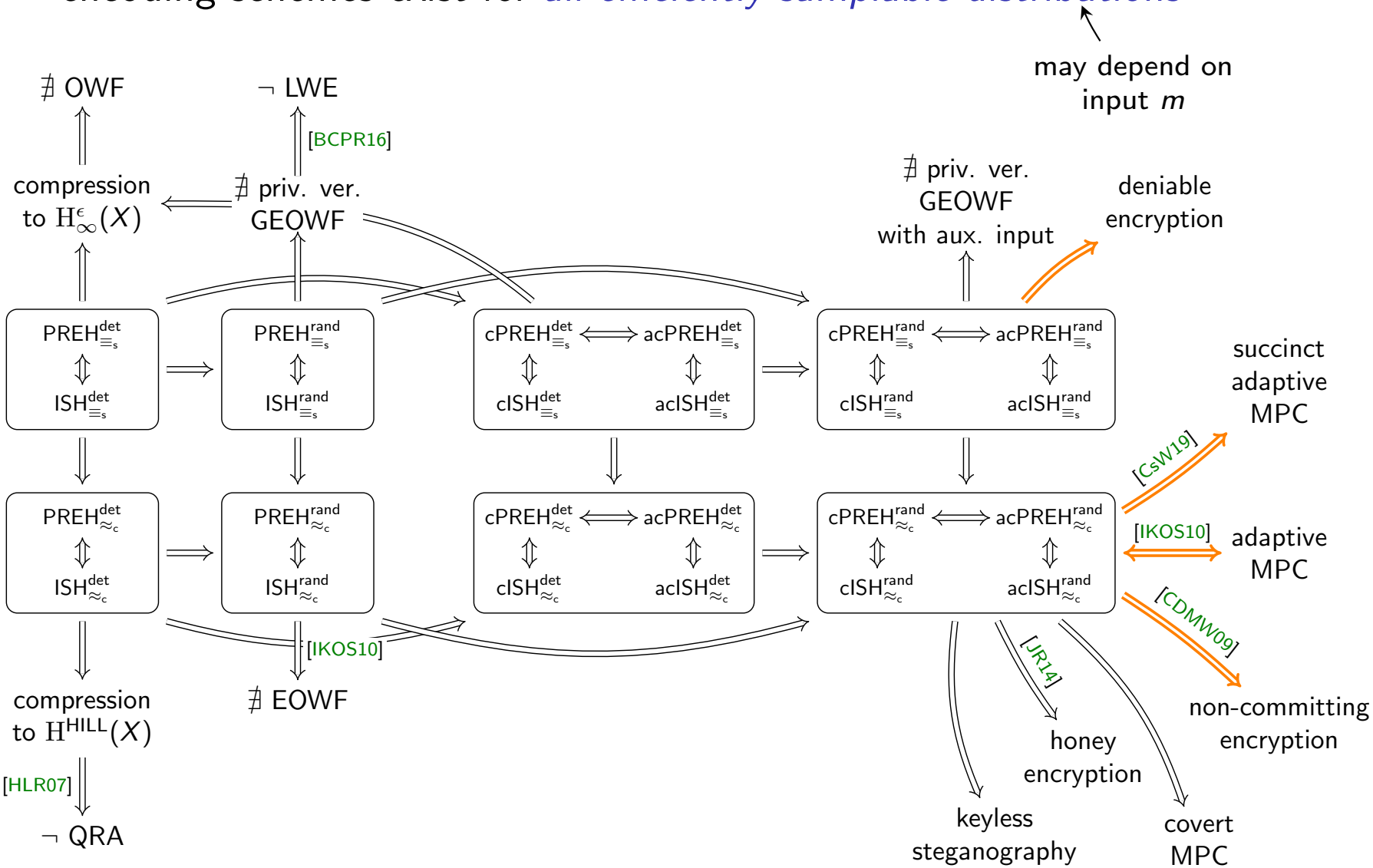
Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



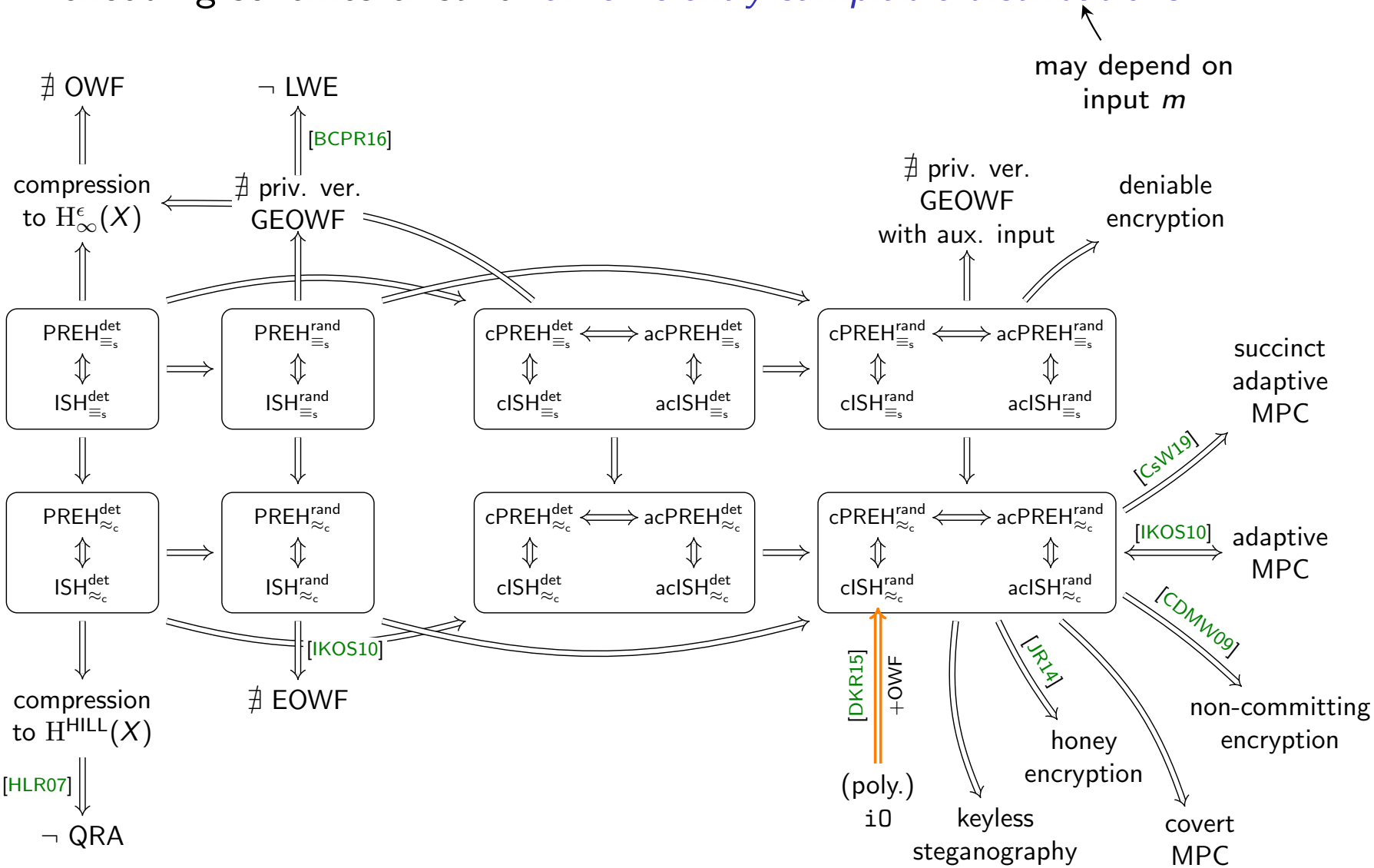
Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



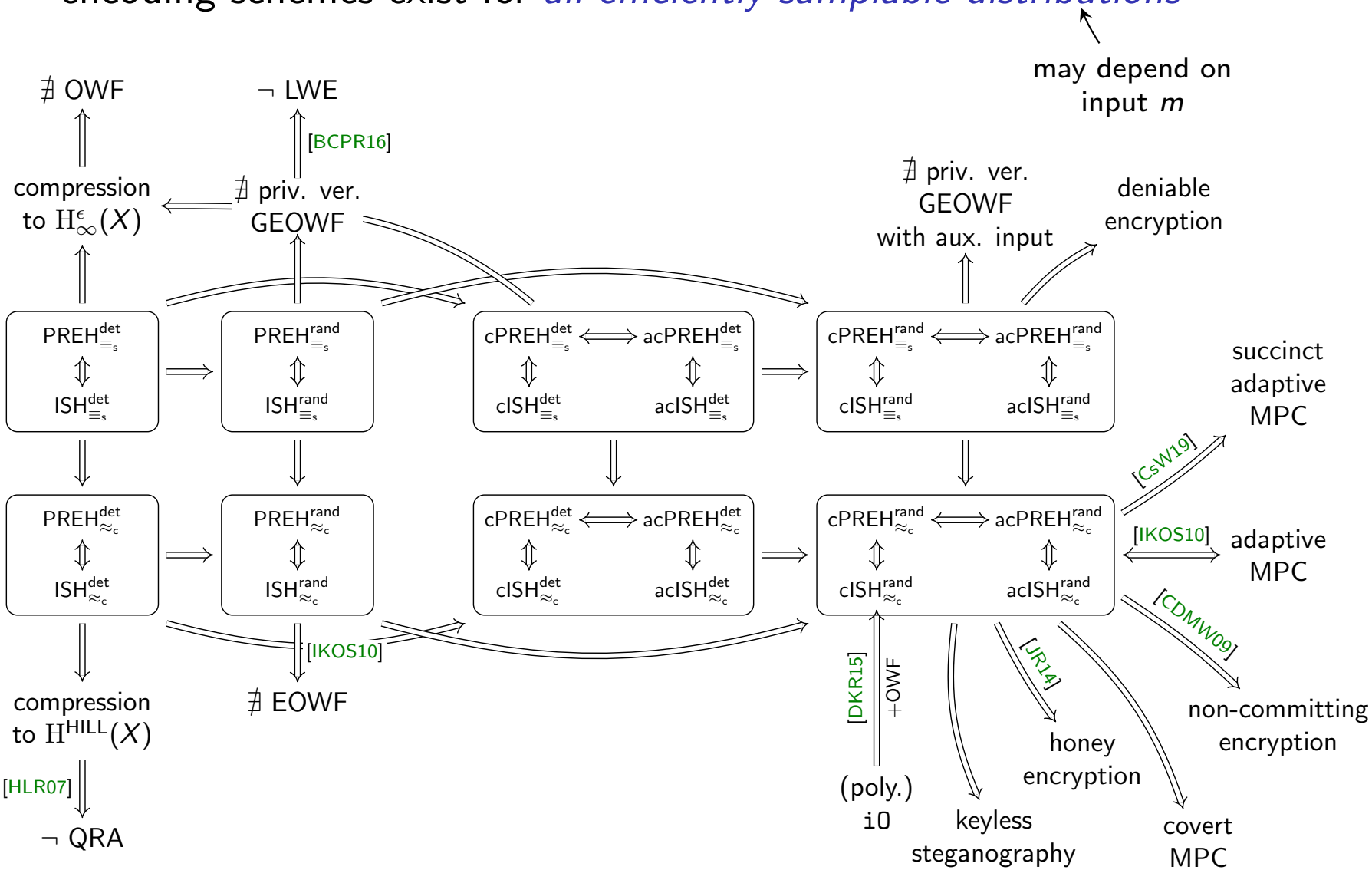
Landscape of Pseudorandom Encodings

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



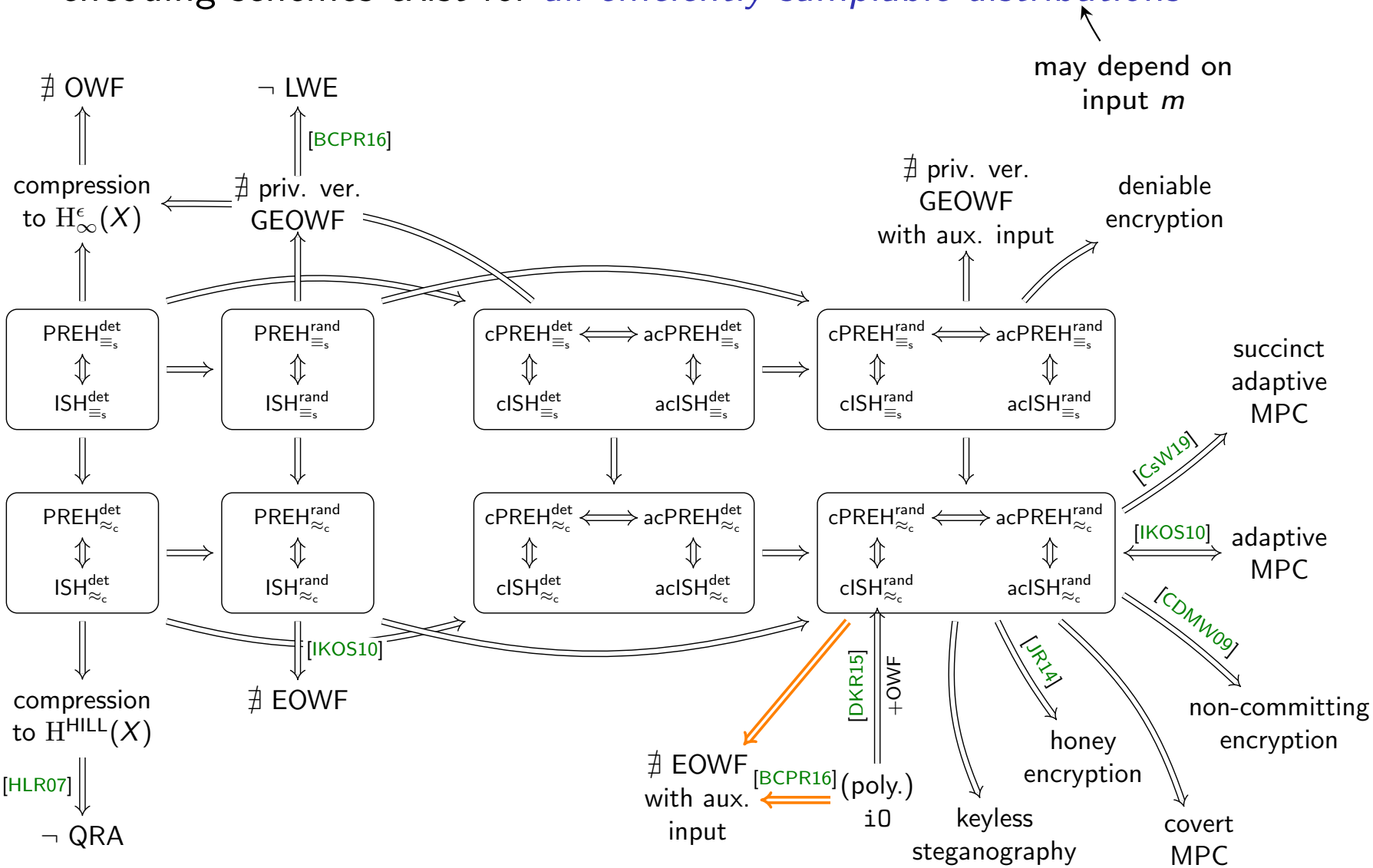
Subsequent Work

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



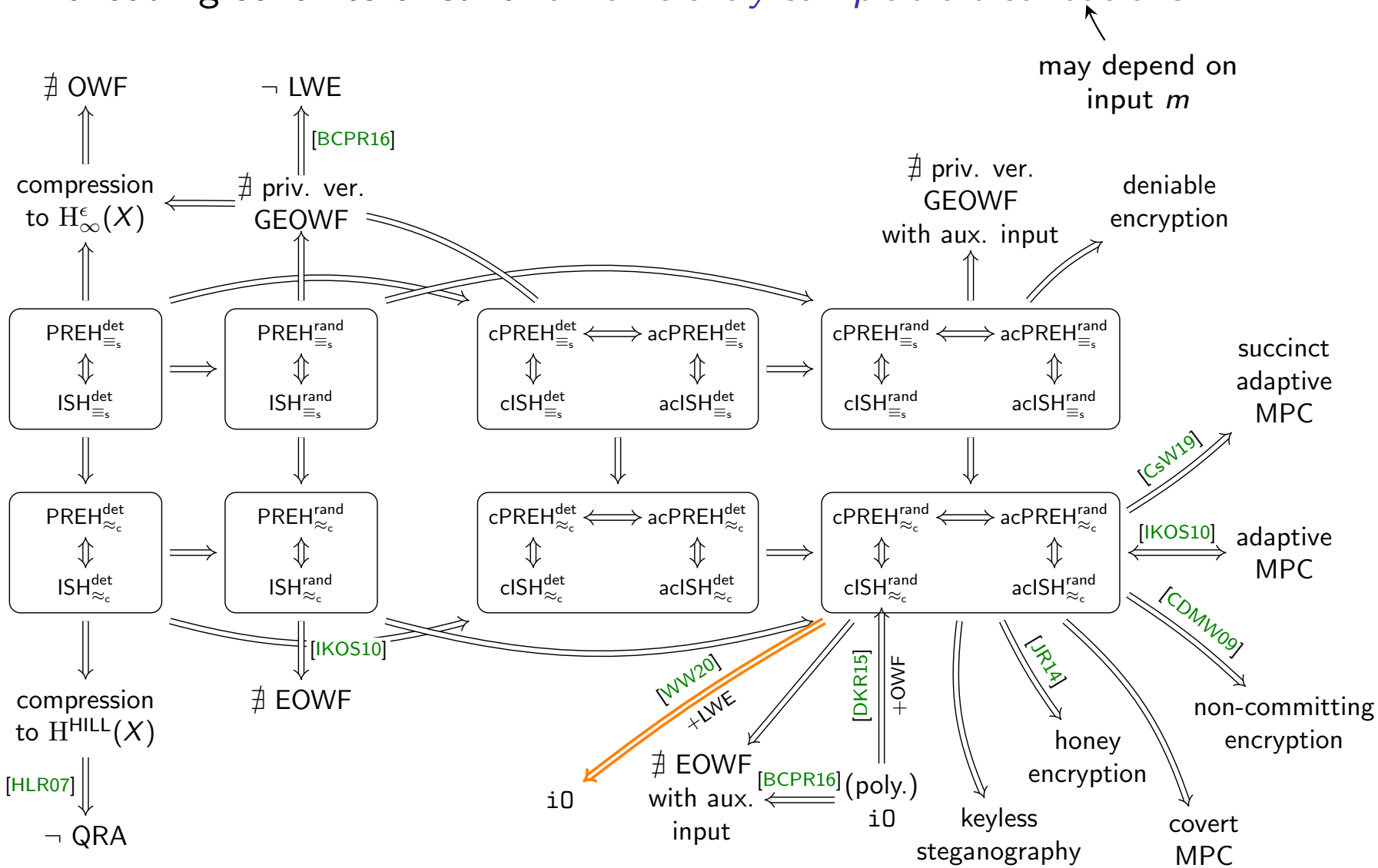
Subsequent Work

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



Subsequent Work

- **Pseudorandom encoding hypothesis (PREH):** pseudorandom encoding schemes exist for *all efficiently samplable distributions*



Conclusion

- study of different flavors of PRE
  - identify PRE in the CRS model as a useful and achievable notion

Conclusion

- study of different flavors of PRE
  - identify PRE in the CRS model as a useful and achievable notion
- equivalence between PRE and invertible sampling [IKOS10] reveals unexpected connections

Conclusion

- study of different flavors of PRE
  - identify PRE in the CRS model as a useful and achievable notion
- equivalence between PRE and invertible sampling [IKOS10] reveals unexpected connections
- relation to covert MPC and adaptive MPC reveals unexpected connection between different security notions for MPC

Conclusion

- study of different flavors of PRE
  - identify PRE in the CRS model as a useful and achievable notion
- equivalence between PRE and invertible sampling [IKOS10] reveals unexpected connections
- relation to covert MPC and adaptive MPC reveals unexpected connection between different security notions for MPC

$\Longrightarrow$ PRE offers a new way to look at things and may find application elsewhere

References I

[BCPR16] Nir Bitansky, Ran Canetti, Omer Paneth, and Alon Rosen. "On the Existence of Extractable One-Way Functions". In: *SIAM J. Comput.* 45.5 (2016), pp. 1910–1952. DOI: 10.1137/140975048. URL: https://doi.org/10.1137/140975048 (cit. on pp. 60–68).

[BM92] Steven M. Bellovin and Michael Merritt. "Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks". In: *1992 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 1992, pp. 72–84. DOI: 10.1109/RISP.1992.213269 (cit. on pp. 10–13).

[BMN01] Colin Boyd, Paul Montague, and Khanh Quoc Nguyen. "Elliptic Curve Based Password Authenticated Key Exchange Protocols". In: *Information Security and Privacy, 6th Australasian Conference, ACISP 2001, Sydney, Australia, July 11-13, 2001, Proceedings*. Ed. by Vijay Varadharajan and Yi Mu. Vol. 2119. Lecture Notes in Computer Science. Springer, 2001, pp. 487–501. DOI: 10.1007/3-540-47719-5_38 (cit. on pp. 10–13).

[CDMW09] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. "Improved Non-committing Encryption with Applications to Adaptively Secure Protocols". In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Vol. 5912. Lecture Notes in Computer Science. Tokyo, Japan: Springer, Heidelberg, Germany, 2009, pp. 287–302. DOI: 10.1007/978-3-642-10366-7_17 (cit. on pp. 60–68).

[CFGN96] Ran Canetti, Uriel Feige, Oded Goldreich, and Moni Naor. "Adaptively Secure Multi-Party Computation". In: *28th Annual ACM Symposium on Theory of Computing*. Philadephia, PA, USA: ACM Press, 1996, pp. 639–648. DOI: 10.1145/237814.238015 (cit. on pp. 37–40).

References II

[CsW19] Ran Cohen, abhi shelat, and Daniel Wichs. "Adaptively Secure MPC with Sublinear Communication Complexity". In: *Advances in Cryptology – CRYPTO 2019, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2019, pp. 30–60. DOI: 10.1007/978-3-030-26951-7_2 (cit. on pp. 60–68).

[DKR15] Dana Dachman-Soled, Jonathan Katz, and Vanishree Rao. "Adaptively Secure, Universally Composable, Multiparty Computation in Constant Rounds". In: *TCC 2015: 12th Theory of Cryptography Conference, Part II*. Ed. by Yevgeniy Dodis and Jesper Buus Nielsen. Vol. 9015. Lecture Notes in Computer Science. Warsaw, Poland: Springer, Heidelberg, Germany, 2015, pp. 586–613. DOI: 10.1007/978-3-662-46497-7_23 (cit. on pp. 60–68).

[DN00] Ivan Damgård and Jesper Buus Nielsen. "Improved Non-committing Encryption Schemes Based on a General Complexity Assumption". In: *Advances in Cryptology – CRYPTO 2000*. Ed. by Mihir Bellare. Vol. 1880. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2000, pp. 432–450. DOI: 10.1007/3-540-44598-6_27 (cit. on pp. 37–40).

[Flo64] William B. Floyd. "Review of 'Information Theory and Coding' (Abramson, N.; 1963)". In: *IEEE Trans. Inf. Theory* 10.4 (1964), p. 392. DOI: 10.1109/TIT.1964.1053709. URL: https://doi.org/10.1109/TIT.1964.1053709 (cit. on pp. 2–4).

[GKM+00] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. "The Relationship between Public Key Encryption and Oblivious Transfer". In: *41st Annual Symposium on Foundations of Computer Science*. Redondo Beach, CA, USA: IEEE Computer Society Press, 2000, pp. 325–335. DOI: 10.1109/SFCS.2000.892121 (cit. on pp. 37–40).

References III

[GM59] E. N. Gilbert and E. F. Moore. "Variable-length binary encodings". In: *The Bell System Technical Journal* 38.4 (1959), pp. 933–967. DOI: 10.1002/j.1538-7305.1959.tb01583.x (cit. on pp. 2–4).

[GS85] Andrew V. Goldberg and Michael Sipser. "Compression and Ranking". In: *17th Annual ACM Symposium on Theory of Computing*. Providence, RI, USA: ACM Press, 1985, pp. 440–448. DOI: 10.1145/22145.22194 (cit. on pp. 5–9).

[HLR07] Chun-Yuan Hsiao, Chi-Jen Lu, and Leonid Reyzin. "Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by Moni Naor. Vol. 4515. Lecture Notes in Computer Science. Barcelona, Spain: Springer, Heidelberg, Germany, 2007, pp. 169–186. DOI: 10.1007/978-3-540-72540-4_10 (cit. on pp. 5–9, 24–27, 34–36, 60–68).

[Huf52] David A Huffman. "A method for the construction of minimum-redundancy codes". In: *Proceedings of the IRE* 40.9 (1952), pp. 1098–1101 (cit. on pp. 2–4).

[IKOS10] Yuval Ishai, Abishek Kumarasubramanian, Claudio Orlandi, and Amit Sahai. "On Invertible Sampling and Adaptive Security". In: *Advances in Cryptology – ASIACRYPT 2010*. Ed. by Masayuki Abe. Vol. 6477. Lecture Notes in Computer Science. Singapore: Springer, Heidelberg, Germany, 2010, pp. 466–482. DOI: 10.1007/978-3-642-17373-8_27 (cit. on pp. 37–40, 60–72).

[JR14] Ari Juels and Thomas Ristenpart. "Honey Encryption: Security Beyond the Brute-Force Bound". In: *Advances in Cryptology – EUROCRYPT 2014*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Copenhagen, Denmark: Springer, Heidelberg, Germany, 2014, pp. 293–310. DOI: 10.1007/978-3-642-55220-5_17 (cit. on pp. 14, 15, 34–36, 60–68).

References IV

[Pas77] Richard C. Pasco. "Source coding algorithms for fast data compression (Ph.D. Thesis abstr.)". In: *IEEE Trans. Inf. Theory* 23.4 (1977), p. 548. DOI: 10.1109/TIT.1977.1055739. URL: https://doi.org/10.1109/TIT.1977.1055739 (cit. on pp. 2–4).

[Ris76] Jorma Rissanen. "Generalized Kraft Inequality and Arithmetic Coding". In: *IBM J. Res. Dev.* 20.3 (1976), pp. 198–203. DOI: 10.1147/rd.203.0198. URL: https://doi.org/10.1147/rd.203.0198 (cit. on pp. 2–4).

[RJ79] Jorma Rissanen and Glen G. Langdon Jr. "Arithmetic Coding". In: *IBM J. Res. Dev.* 23.2 (1979), pp. 149–162. DOI: 10.1147/rd.232.0149. URL: https://doi.org/10.1147/rd.232.0149 (cit. on pp. 2–4).

[Sch72] J. Pieter M. Schalkwijk. "An algorithm for source coding". In: *IEEE Trans. Inf. Theory* 18.3 (1972), pp. 395–399. DOI: 10.1109/TIT.1972.1054832. URL: https://doi.org/10.1109/TIT.1972.1054832 (cit. on pp. 2–4).

[Sha48] Claude E. Shannon. "A mathematical theory of communication". In: *Bell Syst. Tech. J.* 27.3 (1948), pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x. URL: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x (cit. on pp. 2–4).

[TVZ05] Luca Trevisan, Salil P. Vadhan, and David Zuckerman. "Compression of Samplable Sources". In: *Computational Complexity* 14.3 (2005), pp. 186–227. DOI: 10.1007/s00037-005-0198-6. URL: https://doi.org/10.1007/s00037-005-0198-6 (cit. on pp. 5–9).

[Wee04] Hoeteck Wee. "On Pseudoentropy versus Compressibility". In: *19th Annual IEEE Conference on Computational Complexity (CCC 2004), 21-24 June 2004, Amherst, MA, USA*. IEEE Computer Society, 2004, pp. 29–41. DOI: 10.1109/CCC.2004.1313782. URL: https://doi.org/10.1109/CCC.2004.1313782 (cit. on pp. 5–9).

References V

[WW20] Hoeteck Wee and Daniel Wichs. *Candidate Obfuscation via Oblivious LWE Sampling*. Cryptology ePrint Archive, Report 2020/1042. https://eprint.iacr.org/2020/1042. 2020 (cit. on pp. 66–68).

[ZL77] Jacob Ziv and Abraham Lempel. "A universal algorithm for sequential data compression". In: *IEEE Trans. Inf. Theory* 23.3 (1977), pp. 337–343. DOI: 10.1109/TIT.1977.1055714. URL: https://doi.org/10.1109/TIT.1977.1055714 (cit. on pp. 2–4).

[ZL78] Jacob Ziv and Abraham Lempel. "Compression of individual sequences via variable-rate coding". In: *IEEE Trans. Inf. Theory* 24.5 (1978), pp. 530–536. DOI: 10.1109/TIT.1978.1055934. URL: https://doi.org/10.1109/TIT.1978.1055934 (cit. on pp. 2–4).