Common Randomness Amplification: A Constructive View

Grégory Demay and Ueli Maurer

ETH Zürich, Switzerland

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

3-7 September 2012 IEEE Information Theory Workshop (ITW) 2012 Lausanne, Switzerland

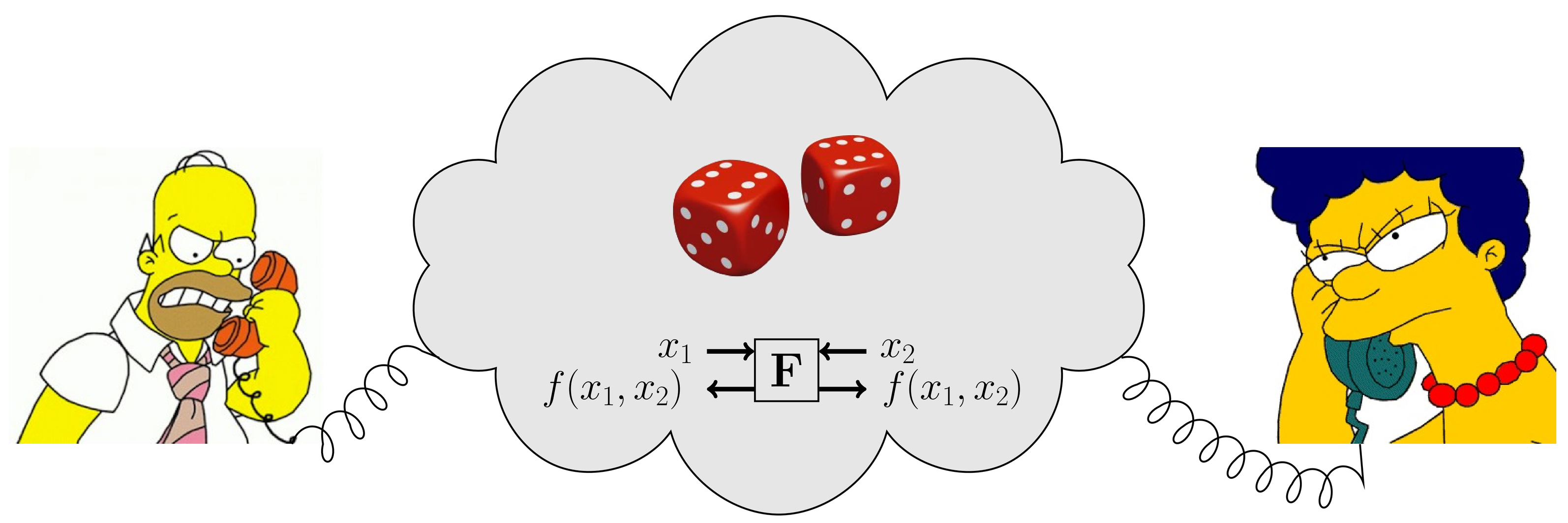
Abstract

Two distrustful parties wish to agree on a common value distributed according to a target distribution by using their initial amount of common randomness and exchanging messages. Our results show that no protocol which is secure in a composable sense can significantly amplify the entropy initially shared by the parties.

Randomness as a Resource

Common randomness is useful for two *distrustful* parties

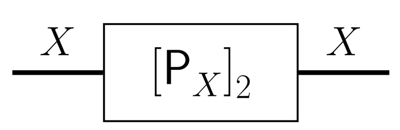
- playing a probabilistic game (over a communication channel) in order to emulate what could have had happened if the players were physically present, e.g., to throw a dice;
- in cryptography, e.g., to securely compute a function of their input.



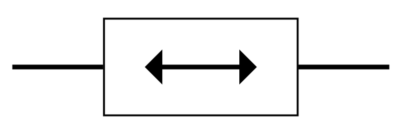
We see common randomness as a *resource*, which we model as a system with an interface to every party in consideration.

2-Interface Resources Considered

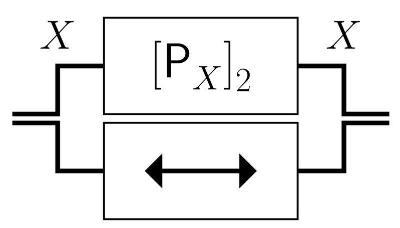
- Symmetric source of randomness $[\mathsf{P}_X]_2$



- Perfect bi-directional communication channel $\longleftrightarrow$



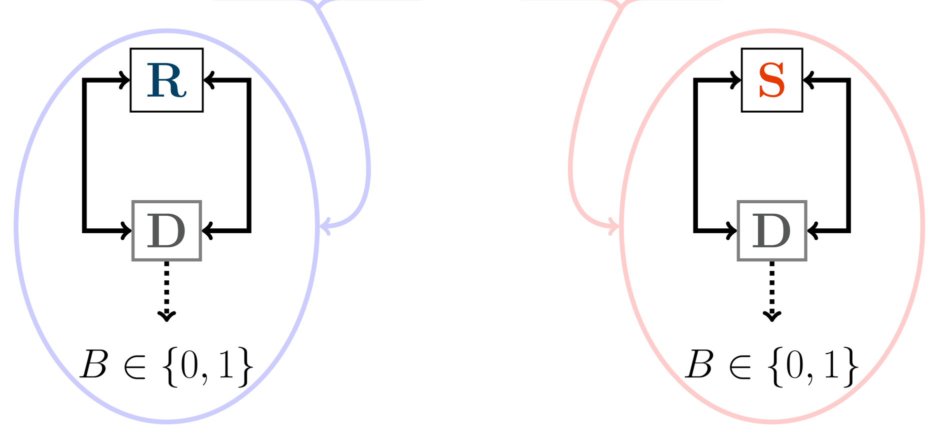
- Both in parallel ($[\mathsf{P}_X]_2 \parallel \longleftrightarrow$)



Comparing Resources

- Distinguishing advantage of a distinguisher D

$$\Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) := \left| \mathsf{P}^{\mathbf{DR}}(B=1) - \mathsf{P}^{\mathbf{DS}}(B=1) \right|$$

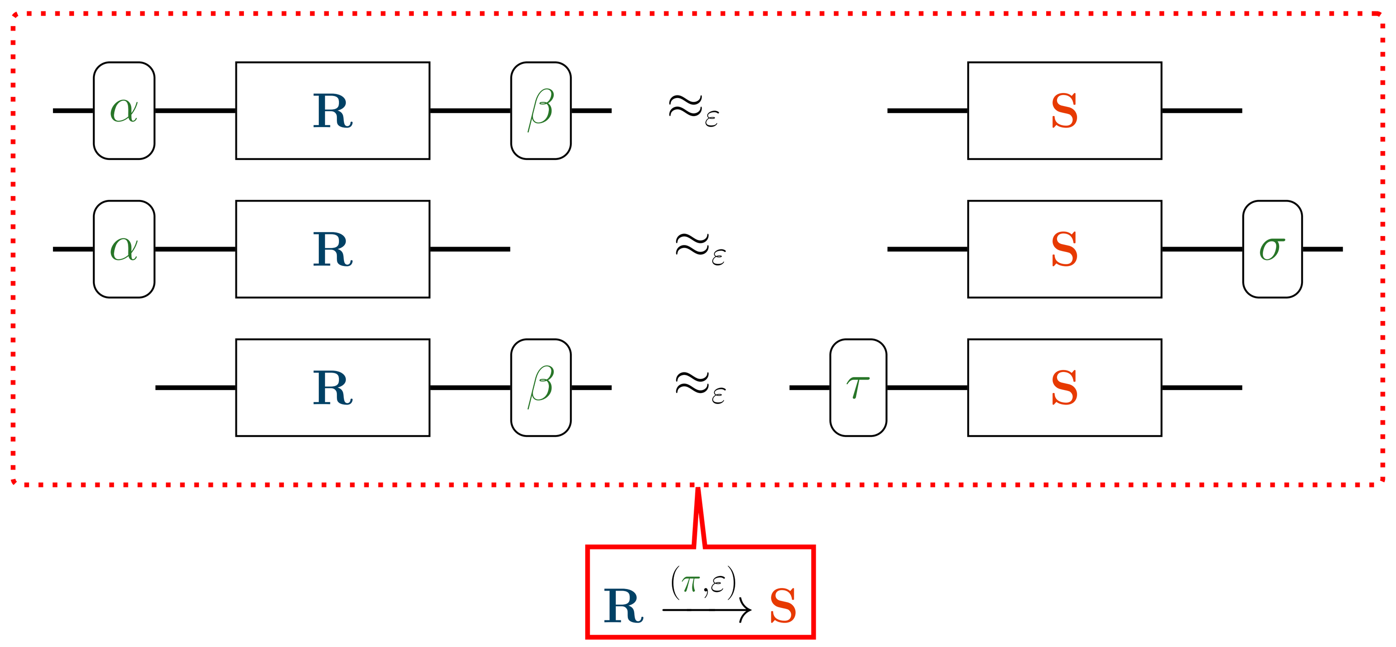


- Pseudo-metric induced

$$\mathbf{R} \approx_\varepsilon \mathbf{S} \quad :\Leftrightarrow \quad \forall \mathbf{D} \in \mathcal{D}: \ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \le \varepsilon.$$

Secure Construction [1]

A two-party protocol $\pi = (\alpha, \beta)$, where one party could be dishonest, securely constructs a resource $\mathbf{S}$ from a resource $\mathbf{R}$ within ε, if and only if, there exists a pair of simulators (τ, σ) s.t.:



[1] U. Maurer and R. Renner, "Abstract Cryptography," in *The Second Symposium in Innovations in Computer Science, ICS 2011*, B. Chazelle, Ed. Tsinghua University Press, Jan. 2011, pp. 1–21.

Secure Amplification of Common Randomness

A two-party protocol $\pi = (\alpha, \beta)$ is said to securely amplify common randomness within ε if

$$([\mathsf{P}_X]_2 \parallel \longleftrightarrow) \xrightarrow{(\pi,\varepsilon)} [\mathsf{P}_W]_2 \text{ and } H(W) > H(X).$$

Theorem - Impossibility Result

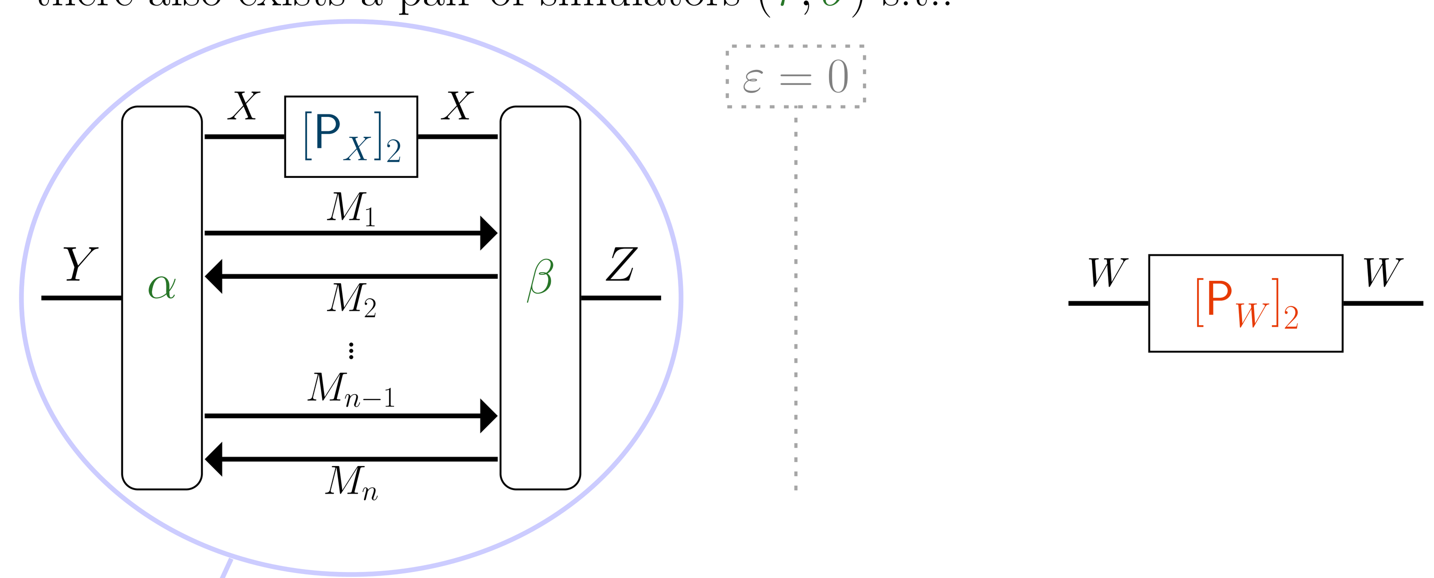
There is no statistically secure protocol with n messages which significantly amplifies common randomness. For any $\varepsilon \in \left[0, \frac{1}{4(n+1)}\right]$,

$$([\mathsf{P}_X]_2 \parallel \longleftrightarrow) \xrightarrow{(\pi,\varepsilon)} [\mathsf{P}_W]_2 \implies H(W) \le H(X) + f_n(\varepsilon).$$

If π is efficient (n is polynomially bounded) and secure (ε is negligible), then $f_n(\varepsilon)$ is negligible.

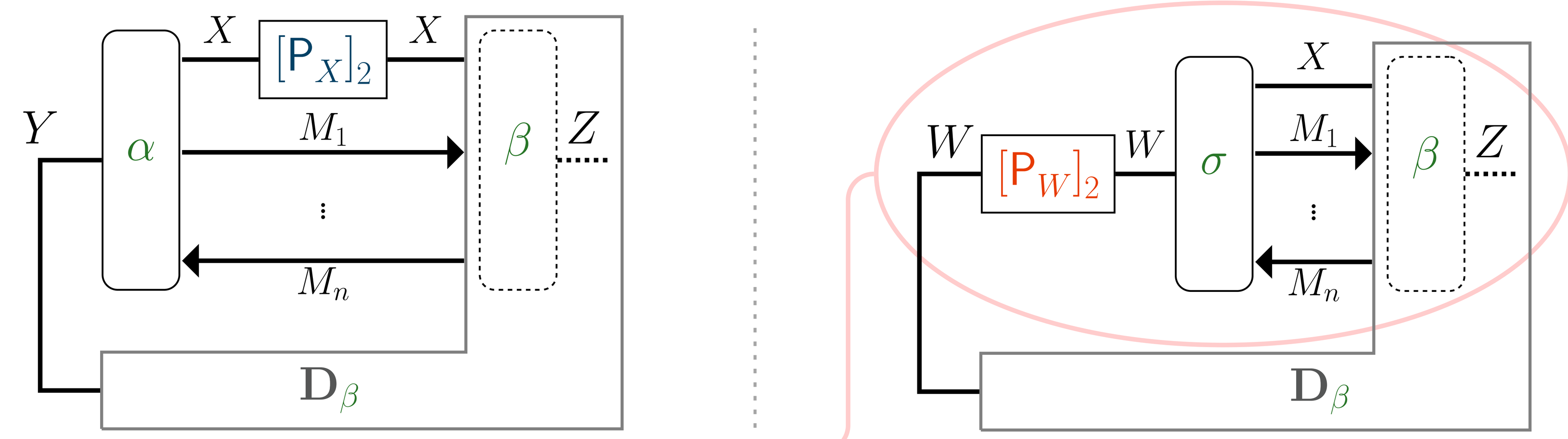
Proof Ideas for $\varepsilon = 0$

Assume there exists $\pi = (\alpha, \beta)$ such that $([\mathsf{P}_X]_2 \parallel \longleftrightarrow) \xrightarrow{(\pi,0)} [\mathsf{P}_W]_2$. Then, there also exists a pair of simulators (τ, σ) s.t.:



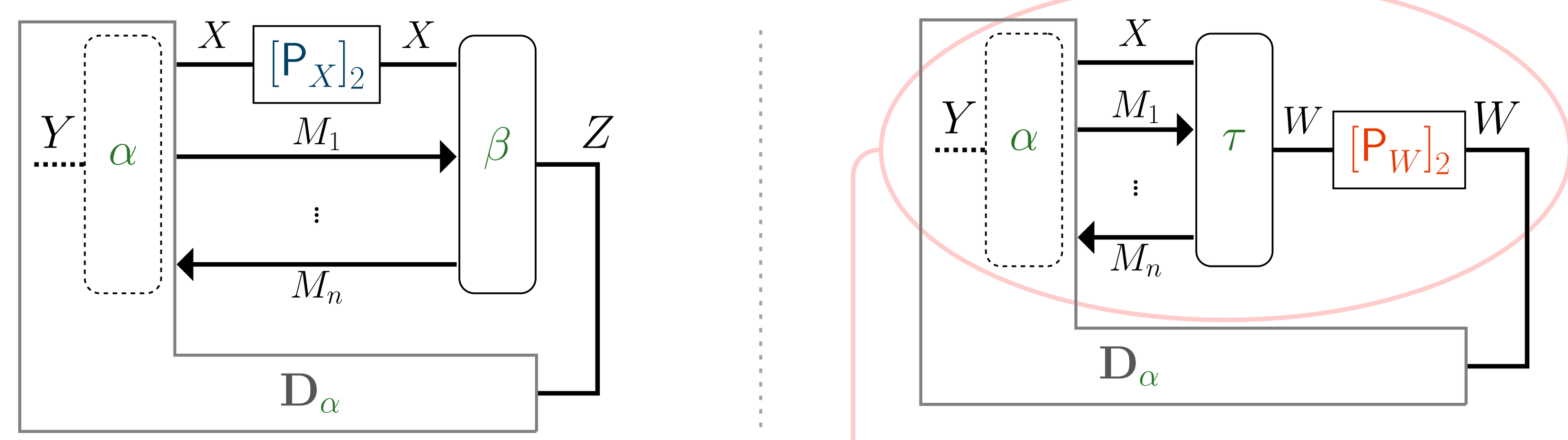
$$\mathsf{R}_{XM^nYZ} \text{ is such that } \begin{cases} Y - (X, M^n) - Z \\ \mathsf{R}_{YZ} = \mathsf{P}_{WW} \end{cases} \implies H^{\mathsf{R}}(Y \mid XM^n) = 0$$

- For a specific distinguisher $\mathbf{D}_\beta$ which emulates β



$$\mathsf{S}_{XM^nWZ} \text{ is such that } \begin{cases} W - (X, M^{i-1}) - M_i \text{ for even } i \\ \mathsf{R}_{XM^nYZ} = \mathsf{S}_{XM^nWZ} \end{cases}$$

- For a specific distinguisher $\mathbf{D}_\alpha$ which emulates α



$$\mathsf{T}_{XM^nYW} \text{ is such that } \begin{cases} W - (X, M^{i-1}) - M_i \text{ for odd } i \\ \mathsf{R}_{XM^nYZ} = \mathsf{T}_{XM^nYW} \end{cases}$$

- Overall

$$H^{\mathsf{R}}(Y \mid X) = I^{\mathsf{R}}(Y; M^n \mid X) = \sum_{i \in [n]} I^{\mathsf{R}}(Y; M_i \mid XM^{i-1}) = 0.$$