A one million ~~dollars~~problems idea?

Laurent Lyaudet[*]

July 15, 2025

Initial version: 2025/07/15 Current version: 2025/07/15
Keywords: one-way function, random noise XD

- Stop it with your catchy titles!
- If I want to! XD

In this note, I will talk about a funny idea I had during my thesis (I must have talked about it in our PhD students office): What if there are “one-way functions” that can only secure random noise ? If RSA was one of them ? Indeed, human messages are very far from random noise. They have weak entropy. Hence, it would be funny that some one-way functions are easily breakable if they are used to transmit low entropy informations. It would be one-way functions that are good only for random noise: some“random noise one-way functions”. But, you will say “Compress your message, it will have high entropy, and success.”. And I will reply that my coding/information theory teacher in computer science master explained to us that there are compression algorithms that are quasi-optimal according to information theory ; quasi because there is the correspondence table that adds an annoying overhead. Hence, even compressed, there is this table, and this is still not “random noise”. Moreover, in a hardened public key cryptography protocol, you must know where is the table in the original message... Maybe this is a silly idea, and maybe not.

Even stronger and less intuitive: What if there is a one-way function that is not random noise, like RSA for example, but is vulnerable to quantum computers; when there is also a random noise one-way function that cannot be broken by quantum computers, if this is indeed random-noise. It would be counter-intuitive; but the world of mathematics is sometimes surprising, like my result of complexity inversion in Lyaudet(2010) (there are many more counter-intuitive results).

And if, a contrario, a plain-text message with high entropy increased the winning odds of another type of attack, singularizing radio signals of the key of the algorithm of the background of the message, because it becomes the only repetitive signal.

RSA will be 50 years old in 2 years, and it’s still used. During my thesis between 2004 and 2007, I was certain that it would be replaced during the following 10 years (at least by unbreakable quantum cryptography for state communications). Nice longevity for such a simple algorithm.

L. Lyaudet. NP-hard and linear variants of hypergraph partitioning. *Theor. Comput. Sci.*, 411(1):10–21, 2010. doi: 10.1016/J.TCS.2009.08.035. URL https://doi.org/10.1016/j.tcs.2009.08.035.

[*] https://lyaudet.eu/laurent/, laurent.lyaudet@gmail.com