# Article information:

What is the difference between PRF and a Random Oracle? - Cryptography Stack Exchange  
<https://crypto.stackexchange.com/questions/15372/what-is-the-difference-between-prf-and-a-random-oracle>

# Article summary:

1. Random oracle and pseudo-random function (PRF) are two different concepts in cryptography.

2. A random oracle is a function sampled uniformly at random from a set of all possible functions, while a PRF is a family of explicit, efficiently-computable keyed functions that appear random to computationally bounded machines.

3. The advantage of using PRFs over random oracles is that PRFs have a succinct representation and can be constructed from the assumption that one-way functions exist, while the construction of PRFs from random oracles is not explicitly known.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

这篇文章探讨了伪随机函数（PRF）和随机预言机（Random Oracle）之间的区别。然而，文章存在一些潜在的偏见和不完整的报道。

首先，文章将PRF描述为计算模拟信息理论中的一次性密码本，而将随机预言机描述为从Fn中均匀随机选择的函数。然而，作者没有提供关于为什么PRF是计算模拟信息理论中的一次性密码本的证据或解释。这种断言可能是基于作者个人观点或经验，并没有提供充分的依据。

其次，文章声称使用PRF而不是随机预言机的优势在于其简洁表示。然而，作者没有提供关于为什么PRF具有简洁表示的证据或解释。这种主张可能是基于作者对PRF构造方法的了解，但缺乏详细说明。

此外，文章还声称在实践中使用基于PRF的协议比使用基于随机预言机的协议更可取，因为我们不知道如何实例化随机预言机。然而，作者没有提供关于为什么我们不知道如何实例化随机预言机以及替代方案（如使用具体哈希函数）存在哪些风险和局限性的证据或解释。这种主张可能是基于作者对密码学领域的了解，但缺乏详细说明和支持。

总体而言，这篇文章在解释PRF和随机预言机之间的区别时存在一些偏见和不完整的报道。作者提出了一些主张，但没有提供充分的证据或解释来支持这些主张。读者应该对这些主张保持怀疑，并寻找更多的信息来全面了解PRF和随机预言机的区别及其在密码学中的应用。

# Topics for further research:

* PRF的定义和特性
* 随机预言机的定义和特性
* PRF作为一次性密码本的证据或解释
* PRF具有简洁表示的证据或解释
* 随机预言机的实例化问题和替代方案的风险和局限性
* PRF和随机预言机在密码学中的应用和优势

# Report location:

<https://www.fullpicture.app/item/ce799c7dbe4ca861d2c20234ce4b7315>