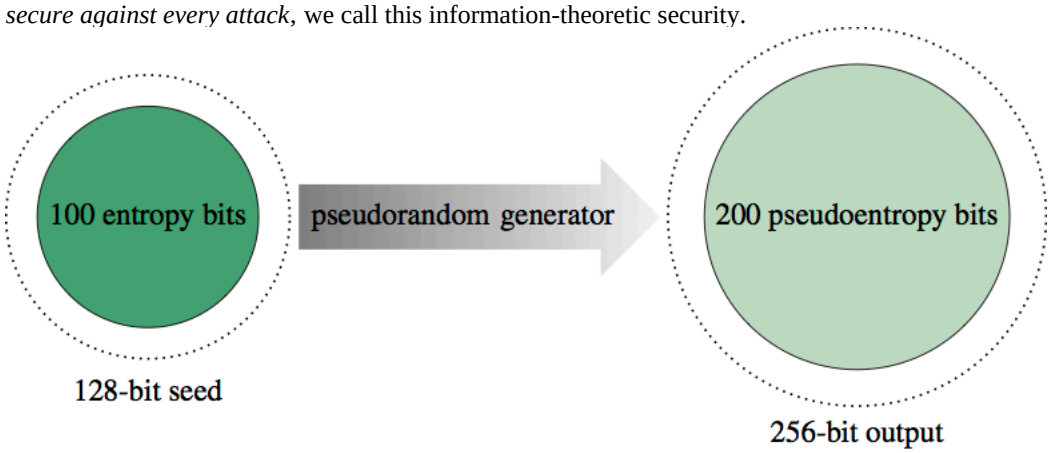
1. **Research Goals**
   The aim of this project is to contribute to the \emph{theory of pseudoentropy}, a young subfield of theoretical computer science with many exciting connections to information theory, cryptography and complexity theory.
2. **Resarch Tasks**
   1. **Choice of topics.**
      The project is a basic research project, focused on extending our knowledge in these pseudoentropy topics, which are currently less understood but offer potentially high research impact. These topics have been carefully selected based on author's previous research experience, opportunities for scientific collaboration, and already obtained preliminary results. The project will continue the research originated in author's master thesis.

   2. **What is pseudoentropy**

      ***Meta-definition and motivations.*** Pseudoentropy notions are relaxations of classical entropy notions. Their purpose is to help quantifying *computational security*, that is security against adversaries of bounded computational power.

      ***Entropy and information-theoretic security***. For cryptographic purposes one choses mostly min-entropy (not to be confused with Shannon entropy), which \emph{quantifies randmomness in terms of unpredictability}. A typical application is a password which should be sampled and kept secret. With some extra knowledge about the sampling strategy, we can make sure (for example) that guessing password is not more likely than $1:2^{80}$ no matter what the strategy is, which is considered secure enough nowadays, and refer to as security of $80$ bits. Since we are *secure against every attack*, we call this information-theoretic security.

      More entropy at the price of quality. From a $128$-bit seed having $100$ bits of best quality entropy (dark green) we obtain 200 pseudorandom bits of high quality (light green) within the $256$-bit output. Despite its simplicity, it is a deep fact called the *dense model theorem*.

      ***Pseudoentropy.*** As opposed to information theory, cryptography takes into account computational aspects. That is, we don't want to be secure against \emph{every} attack. We just want security against \emph{computationally efficient}, that is more realistic, attacks. The gain from this is *saving randomness.* For example, information-theoretic encryption, that is perfect security, requires a huge secret key. Whereas every day we use ciphers with much less randomness, secure against computationally bounded adversaries (*computational security*), which covers almost all practical attacks. To summarize:

      *Pseudoentropy is an ammount-quality tradeoff: we convert entropy of best quality into more entropy of good quality.*

      This tradeoff is illustrated in the figure above.

      ***Pseudoentropy in crypto***. Except a trivial application to encrypt larga data using less randomness, pseuduentroy has recently found important applications in the ``hot'' research area are called *leakage-resilient cryptography*. This line of research focuses on making computations secure even in the presence of some leakage, and uses pseudoentropyproperties as auxiliary technical tools. Thus, better understanding of pseudoentropy translates to better understanding of leakage-resilient cryptography.

   3. **What are the tasks?**

      ***Understand the quality loss issue.*** Having said that we trade the amount for the quality, we did not ask a quite natural question

      **Question:** When manipulating pseudoentropy, wow much do we lose in quality?

      In fact, in all the estimates we know we lose a lot in quality and that is the main issue concerning manipulating pseudoentropy notions. To date, we don't know if these big loses are necessarily or not, which is a serious and frustrating concern in proving security of leakage-resilient crypto primitives. The gap between what could be proven

and what seems reasonable to conjecture (given our intuitions) is really big. The purpose of this project is to answer this question and make it clear whether we were unhappy with proof techniques or simply manipulating pseudoentropy must be so expensive.

***Cleaning the state of the art***. Recently some progress has been made towards positive results in pseudoentropy, however all the results are scattered across the literature. The second-priority goal of this project is to prepare a good metaanalysis (*literature-based discovery*) on what is known and what are possible directions and applications to other problems (including combining existing results). It is very likely that such a review will expose some interesting connections and opportunities to apply pseudoentropy. A special emphasize will be put on leakage-resilient cryptography and key-derivation research areas, which are perhaps first to benefit from progress in pseudoentropy.