# Definition of Bachelor Thesis Project

## True Random

| | |
|---|---|
| ID | IKNR1-2-15 |
| Students | Matteo Alain Morandi<br>Tobias Rothen |
| Advisor | Reto Koenig |
| Experts | |
| Assignment | True random generators which are in use today, are not verifiable by nature, as they claim to gather entropy from uncontrollable context (on quantum level). Hence they present us with data which results from a black box process.<br>For cryptographic tasks such as randomized encryption, it is important for the sender to know that the randomization used during encryption is truly high entropy for any other party. This way it is important be able to trust the randomization gathering machinery. This is only possible if this machine can be challenged ---verified.<br><br>The goal of this bachelor thesis is to create such a verifiable randomization gathering machine and to prove its maximum entropy.<br>A special challenge is the question on how to provide such a random stream to a computer in a possibly infected computer environment, without cheaply loosing too much entropy. |
| Industry Partner | |