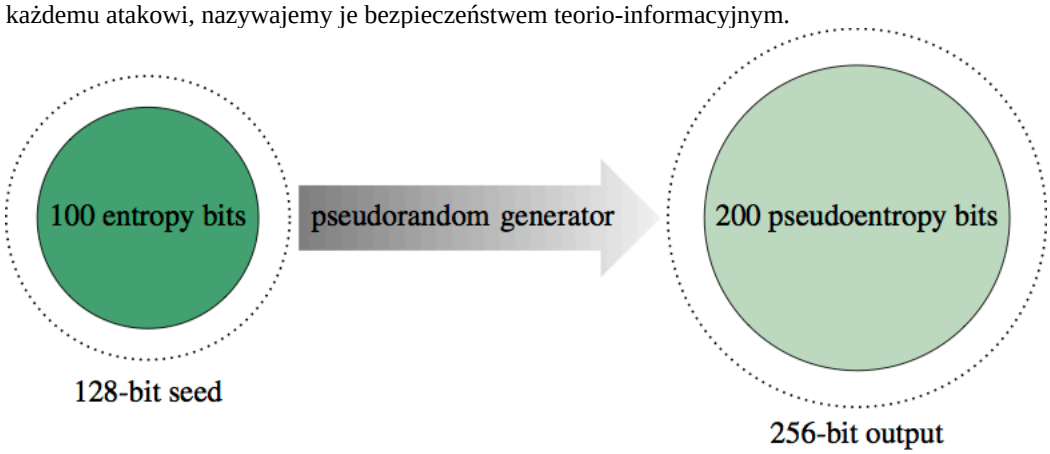
1. **Cele Projektu**
   Celem projektu jest wkład do \emph{teorii pseudoentropii}, młodej dziedziny badań w informatyce teoretycznej która ma wiele pasjonujących powiązań z teorią informacji, kryptografią i teorią złożoności.

2. **Zadania badawcze**
   1. **Wybór tematu**
      Projekt dotyczy badań podstawowych, skoncentrowany jest na poszerzeniu wiedzy o pseudoentropii w tych obszarach, które obecnie rozumiemy najmniej a które oferują duży potencjał rozwojowy. Tematy te zostały wyselekcjonowane na podstawie doświadczenia autora, okazji do współpracy z innymi badaczami i już otrzymanych wyników. Projekt jest kontynuacją badań zapoczątkowanych w pracy magisterskiej.

   2. **Co to jest pseudoentropia**

      Meta-definicja i motywacje. Pojęcia pseudoentropii są uogólnieniami klasycznych pojęć entropii.
      Ich celem jest pomóc ilościowo oceniać \emph{obliczeniowe bezpieczeństwo}, tzn. bezpieczeństwo względem przeciwników o ograniczonej mocy obliczeniowej.

      Entropia i bezpieczeństwo teorio-informacyjne. Dla potrzeb kryptografii najczęściej używa się min-entropii (nie należy mylić z entropią Shannona), która \emph{mierzy losowość w terminach nieprzewidywalności}. Typowe zastosowanie to hasło które powinno być wylosowane i bezpiecznie przechowywane. Z dodatkową wiedzą o procesie generowania hasła, możemy się upewnić (na przykład) że nie można odgadnąć hasła z prawdopodobieństwem większym niż $1:2^{80}$ (niezależnie od strategii), co uchodzi za bezpieczną granicę, i określić jako bezpieczeństwo na poziomie 80 bitów. Ponieważ bezpieczeństwo gwarantowane jest przeciwko każdemu atakowi, nazywajemy je bezpieczeństwem teorio-informacyjnym.

      Więcej entropii za cenę jakości. Ze 128-bitowego ziarna mającego 100 bitów entropii najlepszej jakości (ciemny zielony) otrzymujemy 200 pseudolosowych bitów o wysokiej jakości (jasny zielony) wśród 256-bitowego ciągu wyjścia. Pomimo swojej prostoty, to głęboki rezultat nazywany *twierdzeniem o gęstym modelu.*

      Pseudoentropia. W przeciwieństwie do teorii informacji, kryptografia bierze pod uwagę aspekty obliczeniowe. To znaczy, nie chcemy bezpieczeństwa wgzlędem \emph{każdego} ataku. Chcemy bezpieczeństwa względem *wydajnych obliczeniowo*, tzn. bardziej realistycznych, ataków. Zysk z tego podejścia to \emph{oszczędzanie losowości}. Na przykład, teorio-informacyjne szyfrowanie, tzn. perfekcyjne bezpieczeństwo, wymaga użycia olbrzymiego tajnego klucza. Tymczasem na co dzień używamy szyfrów ze znacznie mniejszą ilością losowości, bezpiecznych względem \emph{ograniczonych obliczeniowo} przeciwników (*bezpieczeństwo obliczeniowe*) co pokrywa wszystkie praktyczne ataki. Podsumowując

      Pseudoentropia handluje jakość za ilość: zamieniamy entropię doskonałej jakości w więcej entropii dobrej jakości.

      Ta zależność jest ilustrowana na ilustracji powyżej.

      Pseudoentropia w kryotografii. Poza trywialnym zastosowaniem do szyfrowania danych z użyciem mniejszej ilości losowości, pseudoentropia znalazła niedawno ważne zastosowania w ``gorącej" dziedzinie badań nazywanej \emph{kryptografią odporną na wycieki}. Te badania koncentrują się na zabezpieczaniu obliczeń nawet w obecności wycieków informacji. W ten sposób, lepsze zrozumiemie pseudoentropii przekłada się na lepsze zrozumienie kryptografii odporną na wycieki.

   3. **Jakie są zadania?**

      Zrozumieć problem straty jakości. Odnotowawszy fakt strat na jakości, nie postawiliśmy całkiem naturalnego pytania

      Pytanie: Przy posługiwaniu się pseudoentropią, jak dużo tracimy na jakości?

W istocie, wszystkie znane oszacowania tracą bardzo dużo i to jest główny problem przy posługiwaniu się pseudoentropią. Na dzień dzisiejszy, nie wiemy czy te duże straty są konieczne czy nie, co jest frapującym i poważnym problemem w dowodzeniu bezpieczństwa aplikacji odpornych na wycieki, takich jak szyfry strumieniowe. Luka pomiędzy tym co potrafimy udowodnić a tym co wydaje się być rozsądną hipotezą (bazującą na najlepszych intuicjach) jest naprawdę duża. Celem projektu jest odpowiedziec na to pytanie, i wyjaśnić czy nie mieliśmy szczęścia z technikami dowodowymi czy może posługiwanie się pseudoentropią musi być tak drogie.

Uporządkowanie stanu wiedzy. Niedawno poczynione zostały duże postępy w zakresie pozytywnych wyników o pseudoentropii, jednakże są one rozrzucone po całej literaturze. Drugo-rzędowym celem projektu jest przygotować dobrą metaanalizę (ang. *literature-based discovery*) o tym co jest znane ja jakie są możliwe kierunki rozwoju i zastosowań w innych problemach (włączając otrzmywanie nowych wyników na bazie połączenia już znanych). Jest prawdopodne że taki przegląd ujawni pewne interesujące relacje i nowe okazje do zastosowań pseudoentropii. Sepcjalny nacisk położny będzie na dziedziny: kryptografię odporną na wycieki i pozyskiwanie klucza, które są jak się zdaje pierwszymi beneficjentami postępu w teorii pseudoentropii.