Analysis of pseudorandom sequences

Viktória Tóth, Viktória Fonyó, Levente Kovács
Eötvös Loránd University, Budapest, Hungary
Department of Computer Algebra

Summer School on Real-world Crypto and Privacy
June 17–21, 2019
Sibenik, Croatia

Pseudorandomness:
- defined in different ways
- standard approach: next bit predictibility is $\approx \frac{1}{2}$ which has certain limitations
- application: keystream in One Time Pad:

$$m \oplus k = c$$

Problems:
- new sequence for every usage
- $|k| \geq |m|$
- aposteriori testing: filter sequences with weak statistics

New, constructive approach: real-valued measures of randomness instead of computational complexity
Mauduit and Sárközy, 1996

Advantages:

1. More constructive
2. No use unproved hypothesis
3. Describe the single sequences
4. Apriori testing: proved bounded measures
5. Characterizing with real-valued function

   $\Rightarrow$ comparableness

The following 2 constructions have good pseudorandom properties from this point of view:
They have "small" measures.

1st construction: Legendre symbol

A good candidate for testing the measures of pseudorandomness is the **Legendre symbol**:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ +1, & \text{if } a \text{ quadratic residue mod } p \\ -1, & \text{if } a \text{ nonquadratic residue mod } p \end{cases}$$

- its random behaviour is known for long (Jacobstahl, Davenport, Bach, Peralta, Damgard, Sárközy)

Mauduit and Sárközy, 1997 :

$$e_n = \left(\frac{n}{p}\right) \quad (n = 1, 2, ..., p-1)$$

Goubin, Mauduit and Sárközy, 2004 :

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{if } (f(n), p) = 1 \\ +1, & \text{if } p | f(n). \end{cases} \tag{1}$$

2nd construction: based on additive character

Mauduit, Rivat and Sárközy introduced the following construction in 2004:

let p be an odd prime number, $f(X) \in \mathbb{F}_p[X]$, and define $E_p = (e_1, ..., e_p)$ by

$$e_n = \begin{cases} +1, & \text{if } 0 \leq r_p(f(n)) < p/2 \\ -1, & \text{if } p/2 \leq r_p(f(n)) < p, \end{cases} \tag{2}$$

where $r_p(n)$ denotes the unique $r \in \{0, ..., p-1\}$ such that $n \equiv r \pmod{p}$.

Properties of Legendre Symbol Construction

Theorem 1 (VTóth)

The family of binary sequences constructed by Legendre symbols construction is collision free.

Theorem 2 (VTóth)

The family of binary sequences constructed by Legendre symbols construction possesses the strong avalanche property.

Properties of Additive Character Construction

Theorem 3 (VTóth)

If $f(x) \in \mathcal{P}_d$, then the family of binary sequences constructed by (2) is collision free and possesses the strict avalanche property.

Where

$$\mathcal{P}_d = \{f(x) \in \mathbb{F}_p[x] : f(x) = \sum_{i=0}^{d} a_i x^i \text{ ,where } a_0 = 0, a_d = 1\}$$

Other results

- We tested the constructions in real life applications:
  - generation of the sequences: fast
  - calculation of the measures: comparing with other constructions
  - measures can be applied to any PR Generator, e.g.: ChaCha, RC4
  - using the sequences in OTP
- Result: they can be used easily and in a fast way in applications as well

Future work

- construction based on additive character can be improved by filtering primes, because for some primes the measures are outstandingly high

- estimate the magnitude of colleration measure, because its computational time is exponential