Test attack on SSAG codes

In the tables below, we present some results of our attack both in the case of a Kummer and Artin-Schreir cover of the projective line. Computations are made using *Magma* with an Intel(R) Core(TM) i5-10210U @ 1.60GHz. We take the following notations:

- q^m is the cardinality of the field $\mathbb{F}_{q^m}$;
- ℓ is the order of quasi-cyclicity (equals to p in the Artin-Schreier case);
- d is the degree of the polynomial f (actually it doesn't impact the complexity of the attack);
- n, k are respectively the lenght and dimension of the public code, while n_0, k_0 are those of the invariant subcode;
- **Time** is the average running time of the algorithm.

q	m	ℓ	d	n	k	n_0	k_0	**Time**
2	10	3	5	750	537	250	181	$20,59$ secs
2	10	3	5	900	627	300	211	$34,67$ secs
2	12	5	4	1250	870	250	176	$42,67$ secs
3	6	7	5	630	479	90	71	$4,31$ secs
3	8	5	4	1150	720	230	145	$115,9$ secs
5	5	11	5	1100	806	100	76	$11,43$ secs

Table 1: Kummer over $\mathbb{P}^1$

q	m	ℓ	d	n	k	n_0	k_0	**Time**
3	8	3	4	600	358	200	121	$12,82$ secs
3	8	3	4	1200	718	400	241	$168,59$ secs
5	5	5	3	750	447	150	91	$21,74$ secs
5	5	5	3	1250	697	250	141	$112,06$ secs
7	4	7	3	560	345	80	51	$2,85$ secs
7	4	7	3	1120	765	160	111	$52,57$ secs

Table 2: Artin-Schreier over $\mathbb{P}^1$