An information rate improvement for a polynomial variant of the Naccache–Stern knapsack cryptosystem

Giacomo Micheli, Joachim Rosenthal, Reto Schnyder
University of Zurich
giacomo.micheli@math.uzh.ch, rosenthal@math.uzh.ch, reto.schnyder@math.uzh.ch

I. Recalling the NSK protocol

In 1997 Naccache and Stern [1] proposed a new public key cryptosystem often referred to nowadays as the "NSK protocol". This system was based on modular arithmetic in the integers and had a number theoretic flavor.

More than a decade after the NSK protocol was invented Micheli and Schiavina presented a generalized monoid based version of the NSK Protocol [1]. Both the NSK and its generalization are based on the following problem:

Problem 1. *Let L be a positive integer, M be a monoid and $c, v_1, \dots, v_L$ elements of M. Find (if one exists) a vector $m = (m_1, \dots m_L) \in \{0,1\}^L$ for which*

$$c = \prod_{i=1}^{L} v_i^{m_i}.$$

In the what follows we show some instances of the problem above and recall a cryptographic protocol arising from them. Let $\mathbb{F}_q$ be the finite field of order q.

Problem 2. *Fix a positive integer L, $M = (\mathbb{F}_q[x], \cdot)$, irreducible polynomials $p_1, \dots, p_L \in M$ and*

$$c = \prod_{i=1}^{L} p_i^{m_i}.$$

for some $(m_1, \dots m_L) \in \{0,1\}^L$. Find the vector m.

As it is immediate to observe, Problem 2 can be solved easily by reducing c modulo p_i for each i: we have in fact $m_i = 1$ if and only if $c \equiv 0 \mod p_i$.

Problem 3. *Let g be an irreducible polynomial of degree N, L a positive integer and $M = (\mathbb{F}_q[x]/(g(x)), \cdot) \cong (\mathbb{F}_{q^N}, \cdot)$. Let $v_1, \dots, v_L \in M$ and*

$$c = \prod_{i=1}^{L} v_i^{m_i}.$$

for some $(m_1, \dots m_L) \in \{0,1\}^L$. Find the vector m.

The generic instance of Problem 3 is now difficult compared to Problem 2. This gap is exploited in [2]. In what follow we recall their protocol.

Alice set up the public key as follows:

- Alice chooses a finite field $\mathbb{F}_q$, L irreducible polynomials $p_i \in \mathbb{F}_q[x]$, an irreducible polynomial g for which $\sum_{i=1}^{L} \deg p_i < \deg g$ and a pair (e, s) for which $es \equiv 1 \mod q^N - 1$.
- Alice set up the public key as $(p_1^e, \dots, p_L^e, \mathbb{F}_q[x]/(g(x)))$.

Research was supported in part by Swiss National Science Foundation under grant no. 149716 and a grant by Armasuisse.

- Alice set up the private key as $(p_1, \ldots, p_L, s)$.

The encryption of a message $m \in \{0,1\}^L$ is performed as

$$m \mapsto \prod_i p_i^{em_i} = c \in \mathbb{F}_q[x]/(g(x))).$$

Alice can then decrypt by computing $c^s \in \mathbb{F}_q[x]/(g(x))$ and then reducing the result modulo p_i for each i, since $c^s \mod g(x)$ (together with its factorization in terms of the p_i's) suitably lifts to the natural numbers using the property $\sum_{i=1}^{L} \deg p_i < \deg g$.

II. Tuning the information rate

In what follows our goal is to show that a direct adaptation of the NSK packing presented in [3] is also possible in the case of the MSK protocol. We pack the irreducible polynomials up to degree d as follows: Let $b, s \in \mathbb{N}$ be positive integers for which $bs \leq \overline{\pi}(d)$, where $\overline{\pi}(d)$ is the number of irreducible polynomials up to degree d. Partition the first (according to the partial ordering related to the degree) bs polynomials in t sets $\{S_i\}$ each of size b satisfying that for all $i, j \in \{1, \ldots, t\}$, if $f \in S_i$ and $h \in S_j$ we have

$$i \leq j \Rightarrow \deg(f) \leq \deg(h).$$

More informally, we pack the polynomials up to degree d into t packs, each of them containing the b polynomials of the lowest possible degree. Let us denote by $p_i^{(j)}$ the i-th polynomial living in the j-th box S_j. The protocol will then be modified as follows. The space of messages becomes $\{0, \ldots, b-1\}^t$, we require now only $\sum_{i=1}^{L} \deg p_b^{(j)} < \deg g = N$. Again, let $es \equiv 1 \mod q^N - 1$.

The public key is set up as $\big(\{(p_i^{(j)})^e\}_{i,j}, \mathbb{F}_q[x]/(g(x))\big)$. The secret key is analogously $\big(\{(p_i^{(j)})\}_{i,j}, s\big)$. The encryption of a message $m = (m_1, \ldots, m_t) \in \{0, \ldots, b-1\}^t$ is performed as

$$m \mapsto \prod_{j=1}^{t} (p_{m_j}^{(j)})^e = c \in \mathbb{F}_q[x]/(g(x)).$$

Alice can then decrypt by computing $c^s \in \mathbb{F}_q[x]/(g(x)))$ and reducing the result modulo $p_i^{(j)}$ for each i, j, as before.

III. Example

As an example, consider the binary case $q = 2$. In [2], the information rate of the MSK scheme was computed for ciphertext sizes 1024, 2048 and 4096. We compare the information rate and public key size of our scheme in the case $\deg h = 1024$ for various values of the box size b in Table I. The first row corresponds to the original MSK (which is not quite the same as setting $b = 1$).

b	t	information rate	public key size
MSK	131	12.8%	134 kbit
2	116	11.3%	237 kbit
6	97	24.5%	595 kbit
10	91	29.5%	931 kbit
50	75	41.3%	3840 kbit
72	72	43.4%	5308 kbit
100	70	45.4%	7168 kbit

Table I

Information rate and public key size for $\deg h = 1024$ and various box sizes.

Evidently, the information rate can be greatly improved at the cost of a much larger public key size. This cost can be somewhat reduced by applying the "Power of Primes" technique of [3].

References

[1] D. Naccache and J. Stern, "A new public key cryptosystem," in *Advances in Cryptology*. EUROCRYPT, 1997, pp. 27–36.

[2] G. Micheli and M. Schiavina, "A general construction for monoid-based knapsack protocols," *Advances in Mathematics of Communications*, vol. 8, no. 3, 2014.

[3] B. Chevallier-Mames, D. Naccache, and J. Stern, "Linear bandwidth naccache-stern encryption," in *Security and Cryptography for Networks*. Springer, 2008, pp. 327–339.