A general construction for monoid-based knapsack protocols

Micheli, Giacomo ; Schiavina, Michele

DOI: https://doi.org/10.3934/amc.2014.8.343

Advances in Mathematics of Communications
Volume 8, No. 3, 2014, 343–358
doi:10.3934/amc.2014.8.343

A GENERAL CONSTRUCTION FOR MONOID-BASED KNAPSACK PROTOCOLS

Giacomo Micheli and Michele Schiavina
Institut für Mathematik
Winterthurerstrasse 190
Zürich, CH8057, Switzerland

(Communicated by Joan-Josep Climent)

Abstract. We present a generalized version of the knapsack protocol proposed by D. Naccache and J. Stern at the Proceedings of Eurocrypt (1997). Our new framework will allow the construction of other knapsack protocols having similar security features. We will outline a very concrete example of a new protocol using extension fields of a finite field of small characteristic instead of the prime field $\mathbb{Z}/p\mathbb{Z}$, but more efficient in terms of computational costs for asymptotically equal information rate and similar key size.

1. Introduction

Building new asymmetric encryption schemes has always been one of the main goals of cryptographers. After the idea of public key cryptography was presented in [2], only few more public key encryption schemes were developed such as the RSA [15], the El Gamal [3], the McEliece cryptosystem [10], the NTRU [6] or the HFE [14] (for an overview [5, 17]). Some new ideas for building new cryptographic schemes based on semigroup actions can also be found in [9], while in the context of knapsack quantum cryptographic schemes we refer for instance to [13]. What D. Naccache and J. Stern built in [12] was a proposal for an asymmetric protocol (NSK) following the earlier ideas of Morii and Kasahara in [11], further developed by Kasahara et al. in [7, 8]. The NSK protocol consists of a shuffling modulo p of an easy problem over the integers, i.e. the factorization of a composite integer where the prime factors are chosen among a fixed set of small size. Given p a prime and $\mathbb{Z}/p\mathbb{Z}$ the finite field of remainder classes, the NSK protocol is based on the unique factorization property of $\mathbb{Z}$, which guarantees the uniqueness of the encryption.

This approach can be generalized to the case of multiplicative monoids (Section 2), and the NSK protocol is just a particular instance for the monoid $(\mathbb{Z}, \cdot)$ of the general framework (subsection 2.1). Using this new general setting we are able to construct an analogous of the NSK protocol relying on the unique factorization properties of $\mathbb{F}_q[x]$, instead of $\mathbb{Z}$, where $\mathbb{F}_q$ is the finite field of order q (Section 3). The security of our particular proposal will rely on the arithmetic structure of the finite field $\mathbb{F}_q[x]/(h(x))$ for some $h(x) \in \mathbb{F}_q[x]$, irreducible of suitable degree (instead of the finite field of remainder classes $\mathbb{Z}/p\mathbb{Z}$). One of the main advantages of this kind of setting is that the security is based on an exponentiation over a finite field in such a way that it will be unfeasible for an attacker even to set up a

2010 *Mathematics Subject Classification:* Primary: 94A60; Secondary: 11T71.
Key words and phrases: Public key encryption, knapsack protocols, polynomials over finite fields, monoids, Naccache-Stern protocol.

discrete logarithm problem (DLP). Indeed, as we will show in the following, since the optimal version of the NSK protocol requires that the chosen prime be next to $\prod_i p_i$, the factorization of $p-j$ for some small j could allow for a reduction to a DLP. In our case, instead, we choose a set of irreducible polynomials and fix the degree of the reducing polynomial. By doing so there is no information leakage. Our new structural conditions will be related only to the degree of the carrier polynomials used for the encryption, avoiding any kind of DLP reduction.

In subsection 3.2.3 some issues concerning the security of the protocol will be addressed, in particular to avoid *subgroup attacks*, that could possibly lead to information.

This new setting will lead to some advantages in terms of computational costs of encryption and decryption. In fact, arithmetics over finite fields $\mathbb{F}_{q^m}$ is considered to be preferrable than arithmetics over $\mathbb{Z}_p$ when $p \simeq q^m$ and $q \ll p$ in terms of computations. We will analyse the key features of our protocol, such as the number of parameters involved for the setting up of the public key, and this will allow us to show a greater deal of flexibility, in comparison with the NSK protocol.

In subsection 3.2.2 we will analise the asymptotics of the information rate of our protocol, showing that it is equal to that of [12]. An exact formula for the information rate will also be provided.

As a subproduct, we present in Section 3.3 a variation of the polynomial protocol where the irreducibility of $h(x)$ is dropped. The encryption is performed over a suitable direct sum of fields, and a decryption is available thanks to the Chinese Remainder Theorem.

2. The new class

In this section we will present a generalized version of the protocol presented in [12].

Let S be a monoid and $\sim$ a finite index congruence on S. We will denote the class of an element $s \in S$ with respect to $\sim$ as $[s]$.

Definition 1. A morphism ψ will be said to be $\sim$proper, if

- $\psi\colon S \longrightarrow S$ is injective;
- ψ is compatible with $\sim$ (i.e. $\psi(x) \sim \psi(y)$ iff $x \sim y$);
- the induced application $\widetilde{\psi}\colon S/\!\sim \longrightarrow S/\!\sim$ is invertible.

Definition 2. Given $L \in \mathbb{N}$ we will say that S is *L-cryptable* under $\sim$ if there exists a $\sim$proper morphism ψ and elements $s_1, \dots, s_L \in S$ such that

$$\alpha_{\sim}^{\psi} : \mathbb{Z}_2^L \longrightarrow S/\!\sim$$
$$m = (m_1, \dots, m_L) \mapsto \left[\prod_{i=1}^{L} \psi(s_i)^{m_i}\right]$$

is an injective application.

The following proposition will be useful later on

Proposition 1. *Given a monoid S that is L-cryptable under $\sim$, the following maps are also injective:*

$$\alpha^{\psi} : \mathbb{Z}_2^L \longrightarrow S$$
$$(m_1, \dots, m_L) \mapsto \prod_{i=1}^{L} \psi(s_i)^{m_i}$$

$$\begin{aligned}\alpha_\sim : \mathbb{Z}_2^L &\longrightarrow S/\sim \\ (m_1,\dots,m_L) &\mapsto \left[\prod_{i=1}^{L} s_i^{m_i}\right] \\ \alpha : \mathbb{Z}_2^L &\longrightarrow S \\ (m_1,\dots,m_L) &\mapsto \prod_{i=1}^{L} s_i^{m_i}.\end{aligned}$$

Proof. The proof follows by observing that, since ψ is $\sim$proper morphism, then also $\alpha_\sim$ is injective. Also $\alpha_\sim^\psi$ injective implies that α^ψ is injective. Again, since ψ is an injection, also α is injective. □

As we have already pointed out, this properties are necessary to keep the encryption meaningful. In the following we will see how it is possible to find non trivial examples of this construction.

Now, denote the image of any map f between sets by $\Im(f)$, and consider the following problems:

Problem 1. *Given $c \in \Im(\alpha_\sim^\psi)$ find m such that $\alpha_\sim^\psi(m) = c$.*

Problem 2. *Given $c' \in \Im(\alpha_\sim)$ find m such that $\alpha_\sim(m) = c'$.*

Let now S, be an L-cryptable monoid under a congruence $\sim$. Whenever a given triple $(S, \sim, \psi)$ is such that Problem 1 is difficult, Problem 2 is easy we define a cryptosystem as follows. Let

$$(S, \sim, L, \widetilde{\psi}([s_1]), \dots, \widetilde{\psi}([s_L]))$$

be the public key and

$$(\widetilde{\psi}^{-1}, s_1, \dots, s_L)$$

be the secret key, the main operations are given by

- *Encryption*: $E(m) := \alpha_\sim^\psi(m) = \prod_{i=1}^{L} \widetilde{\psi}([s_i])^{m_i} =: c$;
- *Decryption*: $D(c)$ is given by solving Problem 2 for $c' = \widetilde{\psi}^{-1}(c)$.

Remark 1. The reader should observe that in the definition of the protocol we did not use the injectivity of ψ nor the fact that $S/\sim$ is a quotient of a monoid S. This is nevertheless the case in all the examples of this protocol we could find, where Problem 2 is easy since a *suitable* lift to S is given. Indeed, in practical situations the problem will be solved computing $(\alpha^{-1} \circ \Gamma)(c')$ where Γ is a lift $S/\sim \longrightarrow S$ such that the following diagram

(1)
$$\begin{array}{ccc} \mathbb{Z}_2^L & \xrightarrow{\alpha} & \Im(\alpha) \\ & \searrow^{\alpha_\sim} & \uparrow{\scriptstyle \widehat{\Gamma}} \\ & & \Im(\alpha_\sim) \end{array}$$

commutes when $\widehat{\Gamma} := \Gamma|_{\Im(\alpha_\sim)}$

Remark 2. Notice that the information rate is given by L/b where b is the number of bits that are needed to represent an element of $S/\sim$

In what follows we will show how the NSK protocol fits in this rather general framework, as well as brand new protocols involving polynomials over finite fields.

2.1. NSK AS A PARTICULAR INSTANCE. In this section we will show how the Naccache-Stern (NSK) protocol fits in our general framework, in the case $S = (\mathbb{Z}, \cdot)$.

Consider the prime ideal $P = \langle p \rangle$ generated by a prime number $p \in \mathbb{Z}$. Let us denote by $\sim$ the congruence induced by the ideal P. Such a congruence is obviously of finite index. Let v be a positive integer with $u = v^{-1} \mod p-1$, and let

$$\begin{aligned} \psi \colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto a^v. \end{aligned}$$

It can be easily checked that ψ is a $\sim$proper morphism of $\mathbb{Z}$.

Now choose L distinct prime numbers p_i such that $\prod_{i=1}^{L} p_i < p$.

Proposition 2. *The map*

$$\begin{aligned} \alpha_{\sim}^{\psi} \colon \mathbb{Z}_2^L &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ (m_1, \dots, m_L) &\longmapsto \left[\prod_{i=1}^{L} p_i^{m_i v} \right] \end{aligned} \tag{2}$$

is an injection and $(\mathbb{Z}, \cdot)$ is therefore L-cryptable under the relation induced by the ideal generated by p.

Proof. Assume that there exist two L-tuples $(m_1, \dots, m_L), (n_1, \dots, n_L)$ such that $\alpha_{\sim}^{\psi}(m_1, \dots, m_L) = \alpha_{\sim}^{\psi}(n_1, \dots, n_L)$, then

$$\left[\prod_{i=1}^{L} p_i^{m_i v} \right] = \left[\prod_{i=1}^{L} p_i^{n_i v} \right] \Rightarrow \left[\prod_{i=1}^{L} p_i^{m_i v} \right]^u = \left[\prod_{i=1}^{L} p_i^{n_i v} \right]^u \Leftrightarrow \left[\prod_{i=1}^{L} p_i^{m_i} \right] = \left[\prod_{i=1}^{L} p_i^{n_i} \right]$$

in $\mathbb{Z}/p\mathbb{Z}$. Since $\prod_{i=1}^{L} p_i^{m_i}$ and $\prod_{i=1}^{L} p_i^{n_i}$ are smaller than p we also have

$$\prod_{i=1}^{L} p_i^{m_i} = \prod_{i=1}^{L} p_i^{n_i} \tag{3}$$

in the unique factorization domain $\mathbb{Z}$, which implies $m_i = n_i \ \forall i$. □

Remark 3. Notice that we are able to express equation (3) because we can always consider the canonical representative $x \in \{0, \dots, p-1\}$ in the remainder class modulo p. This representative is also the only representative in $\Im(\alpha)$ by construction, and therefore we have a canonical lift satisfying (1).

Remark 4. The reader should observe that when $p = t + \prod_i p_i$ for t small, than the information rate is maximal. Unfortunately in this case factoring $p - t$ is easy because $p - t$ is p_L-smooth and $p_L \ll p$, and this gives informations about the bare carriers p_i's. Indeed in this case breaking the NSK protocol is not harder than solving the DLP for the p_i's. Nevertheless the protocol remains interesting for additional features like [12, Section 3].

3. A POLYNOMIAL VERSION

In this section we give a version of the protocol that works over $\mathbb{F}_{q^d}$ instead of $\mathbb{Z}/p\mathbb{Z}$ in such a way that q^d will be of the same order of magnitude than the size p of the field $\mathbb{Z}/p\mathbb{Z}$ in the NSK but $q \ll p$. In this case the specific difficult problem we want to rely on is the following

Problem 3. *Let $\mathbb{F}$ be a finite field and $L \in \mathbb{N}$. Given $y_1, \dots, y_L \in \mathbb{F}$,*

$$\alpha : \mathbb{Z}_2^L \longrightarrow \mathbb{F}$$
$$\alpha(m) = \prod_i y_i^{m_i}$$

and $c \in \Im(\alpha)$, find m such that $\alpha(m) = c$.

Let now $k = \mathbb{F}_q$ and $k[x]$ the polynomial ring in one variable over k. Let $h(x)$ be an irreducible element in $k[x]$ of degree d. Set $\sim$ to be the congruence associated to the ideal $H = \langle h(x) \rangle$ generated by the irreducible polynomial $h(x)$. An efficient algorithm to find irreducible polynomials of fixed degree is given, for instance in [18]. Set

$$S = (k[x], \cdot)$$

and

$$S' := S/\sim = ((k[x]/H)^*, \cdot)$$

where $(k[x]/H)^* = (k[x]/H) \setminus \{0\}$. Fix $v, u \in \mathbb{N}$ such that $\gcd(v, |S'|) = \gcd(v, q^d - 1) = 1$ and $uv \equiv 1 \mod |S'|$. Set

$$\widetilde{\psi} \colon S' \longrightarrow S'$$
$$[s] \longmapsto [s^v].$$

Remark 5.

- $\widetilde{\psi}^{-1} \colon [z] \longmapsto [z]^u$;
- $k[x]/H \cong \mathbb{F}_{q^d}$ is again a finite field.

Let now $L \in \mathbb{N}$ such that there exist L distinct irreducible monic polynomials $p_1, \dots, p_L \in \mathbb{F}_q[x]$ with the property

$$\sum_{i=1}^{L} \deg p_i < d. \tag{4}$$

Notice that in the present description of the protocol there are several different strategies to choose the polynomials; we will analyse the properties of some interesting choices in the following sections.

Again, we have the encryption map.

Proposition 3. *$(k[x], \cdot)$ is an L cryptable monoid with the map*

$$\alpha_\sim^\psi : \mathbb{Z}_2^L \longrightarrow S'$$
$$m = (m_1, \dots, m_L) \longmapsto \left[\prod_{i=1}^{L} p_i^{vm_i} \right]. \tag{5}$$

Proof. Definition 2 requires that the map $\alpha_\sim^\psi$ be an injection. Assume

$$\alpha_\sim^\psi(m_1, \dots, m_L) = \alpha_\sim^\psi(n_1, \dots, n_L)$$
$$\left[\prod_{i=1}^{L} p_i^{vm_i} \right] = \left[\prod_{i=1}^{L} p_i^{vn_i} \right].$$

It follows

$$\left[\prod_{i=1}^{L} p_i^{vm_i} \right]^u = \left[\prod_{i=1}^{L} p_i^{vn_i} \right]^u$$

$$\left[\prod_{i=1}^{L} p_i^{m_i}\right] = \left[\prod_{i=1}^{L} p_i^{n_i}\right]$$

where, in the last equation, we can assume no reduction has happened, since property (4) holds. Indeed

$$\prod_{i=1}^{L} p_i^{m_i} = \prod_{i=1}^{L} p_i^{n_i}. \tag{6}$$

Recalling that $k[x]$ is a unique factorization domain we have $m_i = n_i \ \forall i$. □

So our cyphered text is given by $c(x) = \alpha^{\psi}_{\sim}(m_1, \dots, m_L)$. The explicit decryption for this protocol is simply given by the polynomial division of the decyphered code $(c(x))^u$, that is to say

$$m_i = 1 \iff (c(x))^u = 0 \mod p_i(x). \tag{7}$$

Remark 6. We stress once again the fact that in obtaining equation (6) we used the canonical lift

$$\begin{aligned} \Gamma\colon S/\sim &\longrightarrow S \\ [f(x)] &\longmapsto g(x) \end{aligned}$$

where, for any representative $l(x) \in [f(x)]$, $g(x)$ is the remainder of the division of $l(x)$ by $h(x)$ in $k[x]$, and it is obviously independent of the choice of $l(x)$. The decryption is effectively performed in $\Im(\alpha)$ and the solution to Problem 2 is then given by $(\alpha^{-1} \circ \Gamma)(c(x)^u)$.

The information rate $\mathcal{I} = L/\deg(h)\log_2(q)$ depends on the choice of the carrier polynomials. We will explain later how to maximise this value.

Remark 7. Once the p_i's are fixed the top information rate for this protocol is obtained when we choose $h(x)$ such that

$$\sum_{i=1}^{L} \deg p_i = \deg h - 1. \tag{8}$$

Indeed the information rate can always be maximised since it is always possible to choose $h(x)$ in $k[x]$ such that (8) is satisfied (cf. Remark 4) without allowing for a straightforward reduction to a DLP. This case will be analysed in detail in 3.2.1.

3.1. A SIMPLE EXAMPLE. We now give an example in which $k[x] = \mathbb{F}_2[x]$ and the space of messages has size 2^9. In order to reach a message size of 9 bits, we need exactly 9 keys, that is to say monic irreducible polynomials in $\mathbb{F}_2[x]$. From finite field theory, we know that there are exactly q monic polinomials of degree 1, and

$$\frac{q^d - q}{d}$$

irreducible monic polynomials of prime degree d. So, for $q = 2$ we have two polynomials of degree 1, one polynomial of degree 2, two polynomials of degree 3 and six polynomials of degree 5. For the sake of simplicity, even if the example is non optimal as we will explain, let us choose all the irreducible monic polynomials of

degree 1,2 and 5, summing up to exactly 9 keys, namely:

$$p_1 = x \tag{9}$$

$$p_2 = 1 + x \tag{10}$$

$$p_3 = 1 + x + x^2 \tag{11}$$

$$p_4 = 1 + x^2 + x^5 \tag{12}$$

$$p_5 = 1 + x^3 + x^5 \tag{13}$$

$$p_6 = 1 + x + x^2 + x^3 + x^5 \tag{14}$$

$$p_7 = 1 + x + x^2 + x^4 + x^5 \tag{15}$$

$$p_8 = 1 + x + x^3 + x^4 + x^5 \tag{16}$$

$$p_9 = 1 + x^2 + x^3 + x^4 + x^5. \tag{17}$$

Then, the public key $h(x)$ must be of degree

$$d = \deg(h(x)) = \sum_{i=1}^{9} \deg(p_i(x)) + 1 = 35$$

and irreducible. For instance we may take

$$h(x) = 1 + x^2 + x^{35} \tag{18}$$

and set our protocol onto $\mathbb{F}_{2^{35}} \cong (\mathbb{F}_2[x]/H)^*$, whose order is $2^{35} - 1$ when $H = \langle h(x) \rangle$. We choose the secret key and the decryption exponent, accordingly, to be $v = 3821$ and $u = 25169564954$, so that $uv = 1 \bmod (2^{35} - 1)$. Then we may publish the 9 carrier keys $p_i^v \mod (h(x), 2)$:

$$\begin{aligned} p_1^v =& 1 + x^2 + x^4 + x^{10} + x^{12} + x^{18} + x^{22} \\ &+ x^{23} + x^{24} + x^{26} + x^{27} + x^{29} + x^{32} \end{aligned} \tag{19}$$

$$\begin{aligned} p_2^v =& x + x^3 + x^5 + x^6 + x^7 + x^{10} + x^{12} + x^{13} \\ &+ x^{17} + x^{20} + x^{21} + x^{22} + x^{24} + x^{28} + x^{30} + x^{32} \end{aligned} \tag{20}$$

$$\begin{aligned} p_3^v =& x + x^4 + x^5 + x^7 + x^{13} + x^{20} + x^{22} \\ &+ x^{28} + x^{29} + x^{30} + x^{31} + x^{32} + x^{33} + x^{34} \end{aligned} \tag{21}$$

$$\begin{aligned} p_4^v =& 1 + x^2 + x^3 + x^4 + x^{11} + x^{14} + x^{15} + x^{17} + x^{18} \\ &+ x^{19} + x^{20} + x^{21} + x^{24} + x^{28} + x^{30} + x^{34} \end{aligned} \tag{22}$$

$$\begin{aligned} p_5^v =& 1 + x + x^2 + x^3 + x^4 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15} \\ &+ x^{18} + x^{20} + x^{21} + x^{22} + x^{24} + x^{26} + x^{29} + x^{32} + x^{33} \end{aligned} \tag{23}$$

$$\begin{aligned} p_6^v =& 1 + x + x^2 + x^4 + x^7 + x^{12} + x^{13} + x^{15} + x^{16} + \\ & x^{18} + x^{21} + x^{22} + x^{23} + x^{24} + x^{30} + x^{34} \end{aligned} \tag{24}$$

$$p_7^v = 1 + x^4 + x^8 + x^9 + x^{10} + x^{15} + x^{19} + x^{28} + x^{30} + x^{32} + x^{33} \tag{25}$$

$$\begin{aligned} p_8^v =& x + x^3 + x^4 + x^5 + x^8 + x^{10} + x^{12} + x^{13} + x^{15} + x^{16} \\ &+ x^{17} + x^{25} + x^{26} + x^{27} + x^{28} + x^{30} \end{aligned} \tag{26}$$

$$\begin{aligned} p_9^v =& x + x^4 + x^6 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} \\ &+ x^{17} + x^{18} + x^{20} + x^{23} + x^{24} + x^{30} + x^{31} + x^{32} + x^{33}. \end{aligned} \tag{27}$$

Suppose we want to send the message $m = 111000111 \in \mathbb{Z}_2^9$, we encode it into

$$\begin{aligned} c &= \prod_{i=1}^{9} p_i^{vm_i} \mod (h(x), 2) \\ &= x^2 + x^3 + x^6 + x^{10} + x^{15} + x^{16} + x^{17} + x^{18} \\ &\quad + x^{20} + x^{21} + x^{23} + x^{26} + x^{27} + x^{30} + x^{31} + x^{33} + x^{34}. \end{aligned} \tag{28}$$

Once the message has been received, it is sufficient to take the u-th power, and the result is as follows:

$$\begin{aligned} c^u &= \prod_{i=1}^{9} p_i^{vum_i} \mod (h(x), 2) = \prod_{i=1}^{9} p_i^{m_i} \\ &= x + x^3 + x^4 + x^6 + x^{11} + x^{12} + x^{14} + x^{15} + x^{16} + x^{19} \end{aligned} \tag{29}$$

whose factorization yields:

$$\begin{aligned} \mathsf{Factor}_2(c^u) = &x(1+x)(1+x+x^2)(1+x+x^2+x^3+x^5) \\ &(1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5). \end{aligned} \tag{30}$$

We used the factorization algorithm in this simple example because we are working with small messages. The decryption algorithm presented in (7) is to be considered preferential.

The information rate associated to this encryption protocol is

$$\mathcal{I} = \frac{L}{\deg(h)} = \frac{9}{35} \cong 25,7\% \tag{31}$$

with the size of the space of messages being 2^9.

Remark 8. A similar example is presented in [12], with 2^8 messages. In the cited example the information rate is slightly higher than ours, yet comparable, but the space of messages is smaller.

If we wanted to match the size of space of messages it would be sufficient to remove one polynomial of degree 5, obtaining an information rate of $\mathcal{I} = 8/30 \sim 26,7\%$.

Remarkably enough, as in the NSK-protocol there is apparently no key leakage, our protocol preserves the security of the carrier keys. As a matter of fact, factoring the cyphertext c, one gets no information whatsoever on the cleartext, as it can be seen in the given example:

$$\begin{aligned} \mathsf{Factor}_2(c) = x^2 \left(x^4 + x^3 + 1\right) &\left(x^{28} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + \right. \\ &\left. x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1\right) \end{aligned}$$

Remark 9. More generally, let $g(x)$ be the public modulus and

$$p_1^{vm_1} p_2^{vm_2} \cdots p_L^{vm_L} \equiv c(x) \mod g(x)$$

a cyphetext. Observe that over $\mathbb{F}_q[x]$ we have

$$P(x) = p_1^{vm_1} p_2^{vm_2} \ldots p_L^{vm_L} = t(x)g(x) + c(x)$$

for some $t(x) \in \mathbb{F}_q[x]$. Now notice that infering on the factorization of $P(x)$ from the data of $c(x)$ in terms of the factor basis

$$\{p_1^{vm_1}, \ldots, p_L^{vm_L}\}$$

is the difficult problem on which the protocol relies, since the factorization of polynomials behaves badly with respect to reductions modulo irreducible polynomials. As a matter of fact, we base the security of our protocol on the randomness of the factorization of elements in the image of the map

$$\Gamma_{g,c} : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]$$
$$\Gamma_{g,c}(t(x)) = t(x)g(x) + c(x).$$

In general, the usual security one expects using prime numbers as carriers (NSK) can be extended to monic irreducible polynomials.

As we already pointed out, we are using here a non-optimal setting for our example, in that we skipped the polynomials of degree 3 and 4, and used all those of degree 5 instead. If we decided to optimize the information rate, we could take the two polynomials of degree 1, the single polynomial of degree 2, two of degree 3 and three of degree 4, for an overall encoding power of 2^8 messages. Notice that the space of messages is again equal to the example given in [12].

Choosing polynomials of degree 3 and 4 instead of 5 allows us to reduce the degree of $h(x)$, that is to say the number of bits that are needed to encrypt a message. So, if we compute the information rate in this case we obtain a much better result:

$$\mathcal{I} = \frac{\log_2 m}{\log_2 c} = \frac{8}{23} \cong 34,78\% \tag{32}$$

which is slightly higher than the information rate presented in [12] for the same message size.

The procedure works exactly the same when we change the ground field from $p = 2$ to $p = 3$. This time we may choose three polynomials of degree 1, three of degree 2 and two of degree 3, all monic and irreducible, allowing us to reduce the overall degree of $h(x)$ to $\deg(h(x)) = 16$. In this case, for the same message size, we get an information rate of

$$\mathcal{I} = \frac{8}{16 \log_2 3} \cong 31,55\% \tag{33}$$

which is not better than the information rate in [12], for a space of messages of the same size, yet comparable.

3.2. Flexibility of the protocol. We have already pointed out in the previous sections that the important condition (4) can be fulfilled in several different ways according to the strategy we use in choosing the carrier polynomials p_i's. In what follows we will present a strategy that optimises the information rate and one that, to our analysys, improves security.

We will give a detailed analysis of the asymptotics of the information rate of our protocol and of NSK, showing that they have the same behaviour. In what follows our finite field k will be $\mathbb{F}_q$ for some prime power q.

3.2.1. *Optimization of the information rate.* The optimization of the information rate is ensured by the following:

Proposition 4. *There exists a strategy that maximises the information rate $\mathcal{I}$ for any choice of q and L. Moreover, in this strategy the information rate is determined*

by the closed formula

$$\mathcal{I}(q,N) = \frac{\sum_{n=1}^{N} \frac{1}{n} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k}{\left(\sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k + 1\right) \log_2 q} \tag{34}$$

where $\mu(x)$ is the Möbius function.

Proof. We defined the information rate to be $\mathcal{I} = L/(\deg h \log_2 q)$ and we know that the degree of h depends on the particular choice of carrier polynomials. The strategy we will consider is simply given by choosing *all* irreducible polynomials of all degrees up to a given degree N. Denote the number of degree-n irreducible polynomials in $\mathbb{F}_q[x]$ by D_n^q, we have the formula

$$D_n^q = \frac{1}{n} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k$$

where $\mu(x)$ is the Möbius function. The overall number of chosen polynomials, that is the number of bits that the plain text is composed by, as well as the sum of the degrees of the p_i's are given by a closed formula, namely:

$$L = \sum_{n=1}^{N} D_n^q = \sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) \frac{q^k}{n} \tag{35}$$

$$\deg(h(x)) = \sum_{n=1}^{N} n D_n^q + 1 = \sum_{n=1}^{N} \sum_{k|n} \mu\left(\frac{n}{k}\right) q^k + 1 \tag{36}$$

for some maximal degree N (which is dependent on L if we consider L to be the fundamental parameter). Then, the information rate $\mathcal{I}$ as a function of the prime power q and (implicitly) the parameter L has the desired closed expression.

It is easy to gather that such a choice of the polynomials guarantees maximal information rate, in that we are lowering as much as possible the degree of $h(x)$ and as a result the number of bits of the encrypted message. □

Remark 10. The obvious disadvantage of the strategy above is that one can always assume that the bare carrier polynomials are known, for we take all of them progressively up to degree N. As a matter of fact, the strategy above gives us a clear upper bound for the information rate, for all different combinations of L and q. Notice, however, by comparison with the tables of [12], that this is the same strategy adopted by Naccache and Stern, where the chosen prime p has the same size of $\mathsf{NextPrime}(\prod p_i)$.

Within this strategy it is important to notice that all the variations proposed in [12, Section 2.3] are importable in the present context. For example, it is possible to express the message m in a basis different from 2, and this would lead to some modification to the suitable degrees for our carriers. Moreover, it is possible to restrict the space of messages to constant-weight strings. This last choice increases the information rate since it allows to lower the degree of $h(x)$. In fact, if w is the constant weight, the bound on the degree of h is:

$$\deg h > wN$$

where N is the highest degree of the chosen carriers.

L (bits)	$\deg h$ (bits)	$\mathcal{I}$
131	1024	12,8 %
233	2048	11,4%
418	4096	11,2%

TABLE 1. Information rate matching with [12, Section 2.2]

L (bits)	$\mathcal{M}$ (bits)	Size of p & $\deg h$ (bits)	$\mathcal{I}$
759	758	8192	11,4%

TABLE 2. Extension to next block and matching of the information rate

Apart from these extensions, the standard NSK protocol is summarized in the table presented in [12, Section 2.2], where the information rate for 512, 1024 and 2048 bits-sized p's is given. The strategy we have just outlined to reach the maximal information rate, allows us to obtain the exact values presented in [12] matching the degree of our polynomial h with the size of their prime p and L with the size $\mathcal{M}$ of the message. So we are able to obtain the same information rate.

The matching procedure works as follows: compute the degree of h obtained by choosing all polynomials up to a given degree, say 9 to obtain $\deg h = 977$. Then, top it to the next block, in this case 1024 bits, choosing *some* polynomials of one degree higher, in this case 11. This leads to an increase in the number L of carrier polynomials from 127 to 131, and the information rate is then given by the ratio $L/\deg h$.

In Table 1 we show how to match the examples presented in [12], and the last row is obtained by extending their calculations to 4096 bits. If we go further and compute the relevant figures in the case of 8192 bits we find almost perfect agreement also in this case (cf. Table 2). It will be clear in what follows why this happens.

3.2.2. *Asymptotics comparison with previous works.* We will prove in this section that our protocol has the same asymptotic information rate of [12]. A naive explanation of this fact is given by arguing that the number of primes below a certain number of bits has the same behaviour as the number of irreducible polynomials in $\mathbb{F}_q[x]$ below a certain degree.

Let us fix the notation

$$a_N \sim b_N \iff \lim_{N\to\infty} \frac{a_N}{b_N} = 1.$$

We will make use of the following

Lemma 5.

$$\sum_{n=1}^{N} D_n^q \sim \frac{q}{q-1} D_N^q \tag{37}$$

Proof. First recall that [16, Theorem 2.2] $D_n^q \sim \frac{q^n}{n}$ and therefore the sums behave asymptotically as $\sum_{n=1}^{N} D_n^q \sim \sum_{n=1}^{N} \frac{q^n}{n}$. Then we have (37) if and only if

$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} \frac{q^n}{n}}{\frac{q^N}{N}} = \frac{q}{q-1}. \tag{38}$$

Now, denote by $S_N := \sum_{n=1}^{N} \frac{N}{n} q^{n-N}$ and observe that it might be expressed in terms of the recursive sequence

$$S_{N+1} = \frac{1}{q}\frac{N+1}{N} S_N + 1. \tag{39}$$

for the initial value $S_1 = 1$. Consider $S_- = \liminf_{N\to\infty} S_N$ and $S_+ = \limsup_{N\to\infty} S_N$. Passing to the lim sup and lim inf in (39) we get the same equation for $S_\pm$:

$$S_\pm = \frac{S_\pm}{q} + 1$$

provided that they are both finite. Assuming that they are, we conclude that

$$\lim_{N\to\infty} S_N = S_\pm = \frac{q}{q-1} \tag{40}$$

This assumption is legitimate since $S_N \geq 0$ for all $N \in \mathbb{N}$, thus $S_- \geq 0$, and for S_+ we observe that

- When $x \in \mathbb{R}^+$ we have that $\frac{q^x}{x}$ is increasing for $x \geq \frac{1}{\log q} \geq 2$, since $q \geq 2$, and in particular this is true for $x \in \mathbb{N}^*$;
- $\limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=1}^{N} \frac{q^n}{n} = \limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=2}^{N} \frac{q^n}{n}$.

It follows that

$$\limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=1}^{N} \frac{q^n}{n} = \limsup_{N\to\infty} \frac{N}{q^N} \sum_{n=2}^{N} \frac{q^n}{n} \leq \limsup_{N\to\infty} \frac{N}{q^N} \int_2^{N+1} \frac{q^x}{x} dx$$

where the last inequality comes from the fact that $\sum_{n=2}^{N} \frac{q^n}{n}$ are the lower sums of $\int_2^{N+1} \frac{q^x}{x} dx$, since $\frac{q^x}{x}$ is increasing for $x \geq 2$. Moreover

$$\lim_{N\to\infty} \frac{\int_2^{N+1} \frac{q^x}{x} dx}{\frac{q^N}{N}} = \lim_{t\to\infty} \frac{\int_2^{t+1} \frac{q^x}{x} dx}{\frac{q^t}{t}} = \lim_{t\to\infty} \frac{\frac{q^{t+1}}{t+1}}{\frac{q^t}{t}(\log q - \frac{1}{t})} = \frac{q}{\log q}$$

where the second equality follows from the De L'Hôpital rule. This proves that

$$0 \leq \liminf_{N\to\infty} S_N \leq \limsup_{N\to\infty} S_N \leq \frac{q}{\log q}$$

and yields the claim. □

We are now ready to prove

Proposition 6.

$$\mathcal{I}(q, N) \sim \frac{1}{\log_2 q} \frac{1}{N} \tag{41}$$

Proof. Observe that $n D_n^q \sim q^n$ and therefore, from (34)

$$\mathcal{I}(q, N) \sim \left(\sum_{n=1}^{N} \frac{q^n}{n} \right) \Big/ \left(\log_2 q \sum_{n=1}^{N} q^n \right)$$

Now, it is easy to gather that

$$\sum_{n=1}^{N} q^n \sim \frac{q}{q-1} q^N \tag{42}$$

then, plugging the results of (42) and of Lemma 5 into (34), we obtain

$$\mathcal{I}(q,N) \sim \frac{1}{\log_2 q} \frac{\frac{q}{q-1}\frac{q^N}{N}}{\frac{q}{q-1}q^N} = \frac{1}{\log_2 q}\frac{1}{N}. \tag{43}$$ □

We would like to compare this result with the information rate of the NSK protocol. Notice that in order to make a consistent comparison we must understand the role of our parameter N in the NSK.

Once q is fixed, bounding the degree of the carrier polynomials by N is the same as bounding the number of bits required to represent any of them by the quantity $M = \lfloor N \log_2(q) \rfloor$.

The analogous bound for the NSK is then given by bounding the number of bits of the prime carriers by M. This is the same as bounding the prime carriers themselves by $2^M \simeq q^N$. In the following proposition the comparison is made explicit.

Proposition 7. *Let N be the bound on the degree of the carrier polynomials and $M = \lfloor N \log_2(q) \rfloor$ the analogous bound for the bits of the prime carriers in the NSK. The information rate for the NSK protocol is asymptotically given by*

$$I_{NSK} \sim \frac{1}{\log_2 q}\frac{1}{N}. \tag{44}$$

Proof. It is known [4, Equation 2] that for large $m \in \mathbb{N}$

$$\prod_{p<m} p \sim e^m.$$

Let us consider $m = 2^M \simeq q^N$, then $\prod_{p<q^N} p \sim \exp q^N$. Now, the number of prime numbers up to q^N asymptotically goes, by the prime number theorem, as

$$\pi(q^N) \sim \frac{q^N}{N \ln q}.$$

In our case this will be the number of carrier prime numbers up to q^N. On the other hand $\exp q^N$, which is the size of the prime modulus of [12], has $\lfloor q^N \log_2 e \rfloor$ digits, and therefore the information rate is computed as

$$I_{NSK} \sim \frac{\frac{q^N}{N \ln q}}{q^N \log_2 e} = \frac{1}{\log_2 q}\frac{1}{N}. \tag{45}$$ □

By comparing Propositions 6 and 7 it is now clear that the two information rates have the same behaviour. This explains that the matching procedure we perform at the end of the previous section will attain the information rate of NSK also in the asymptotic limit. Moreover it justifies the claim on the large-N behaviour of irreducible polynomials with respect to prime numbers.

3.2.3. *Some precautions to avoid subgroup-like attacks.* The security of this protocol is strictly related to the size of the degree of h and, as a consequence, to the range of degrees that the carriers can have. Indeed, when the carriers are chosen within a large set, the attacker will not have chances (in terms of a brute force attack) to find the p_i's to set up a discrete logarithm problem for the pair (p_i, p_i^s) for any i.

As a matter of fact, the knowledge of h will only lead to the following information on the degrees:

$$\deg(h) = \sum_i \deg(p_i) + 1.$$

This is not the case when working with integers and primes in $\mathbb{Z}/p\mathbb{Z}$, where we can always assume that the prime factors are known when $p \simeq \prod_i p_i$.

We first sketch a subgroup like attack in the most *unsafe* case. Let G be an abelian group and $p_1^v, \dots, p_L^v$ be carriers, as in Section 3. Let the order of p_i^v in G be n_i and suppose $\gcd(n_i, n_j) = 1$ for $i \neq j$. Let now

$$M_j = n_1 \cdots n_{j-1} \cdot n_{j+1} \cdots n_L.$$

It is easy to observe that, for a generic cyphertext c, $m_j = 1$ if and only if $c^{M_j} \neq 1$. As it is elementary to observe, this leads to decryption in L steps. Moreover, it can also be adapted to work when the condition $\gcd(n_i, n_j) = 1$ is just partially fulfilled. In this case, indeed, only partial information on the text can be extracted.

Consider now the decomposition in cyclic subgroups of the multiplicative group of the finite field $(\mathbb{F}_{q^d})^*$. In order to avoid subgroup-like attacks on the cyphertext we will require all the p_i's to be generators of the same subgroup of large order. This will lead to certain requirements on $q^d - 1$.

The most natural choice to solve this problem is asking that the degree d of the reducing polynomial $h(x)$ be constrained by the following:

$$r := \frac{q^d - 1}{q - 1} \text{ is prime.} \tag{46}$$

Now one could choose the p_i's such that

$$p_i(x)^r \neq 1 \mod h(x) \quad \forall i \in \{1, \dots, L\}. \tag{47}$$

3.3. "CHINESE REMAINDER" VERSION. In what follows we will present another example of a protocol that fits the general picture, which stems on the well known chinese remainder theorem. To do this, let us introduce a large prime power q and a natural number $L \in \mathbb{N}$. Consider now the monoid $S = (\mathbb{F}_q^{L+1})^*$, with the multiplication defined componentwise, and the set $R = \{r_1, \dots, r_{L+1}\} \subseteq \mathbb{F}_q$.

Let $\alpha_i \in \mathbb{F}_q \backslash R \quad \forall i \in \{1, \dots, L\}$ and choose two large integers u, v such that $uv = 1 \mod (q-1)$. Compute the following list of vectors $p_i \in (\mathbb{F}_q^{L+1})^*$ as

$$(g_i)_j := (r_j - \alpha_i)$$
$$(p_i)_j := (g_i)^v.$$

Let

$$((\mathbb{F}_q^{L+1})^*, \{p_1, \dots, p_L\})$$

be the public key and

$$(\{g_1, \dots, g_L\}, \{r_1 \dots r_L\})$$

be the secret key. Let

$$\begin{aligned} F: \quad \mathbb{Z}_2^L &\longrightarrow S \\ (m_1, \dots, m_L) &\mapsto \prod_{i=1}^{L} p_i^{m_i} \end{aligned}$$

be the encryption map.

Remark 11. Observe that the information rate is

$$\frac{L}{(L+1)\log_2(q)}.$$

Proposition 8. *F is an injection.*

Proof. We define a polynomial on $\mathbb{F}_q[x]$ by

$$h_R(x) := \prod_{i=1}^{L+1}(x - r_i)$$

whose set of zeros coincide with R. We will prove the proposition by showing how to compute the inverse over the image of F using $h(x)$, i.e. we will show how to uniquely decrypt any cyphertext $c \in \Im(F)$ using the secret key. Let

$$\begin{aligned} \psi : S &\longrightarrow S \\ x &\mapsto x^v, \end{aligned}$$

$$\begin{aligned} G : \mathbb{F}_q[x]/h_R(x) &\xrightarrow{\text{CRT}} \mathbb{F}_q^L \\ k(x) &\mapsto (k(r_1), \ldots, k(r_L)), \end{aligned}$$

and

$$\Gamma : \mathbb{F}_q[x]/h_R(x) \longrightarrow \mathbb{F}_q[x]$$

be the canonical lift. The decryption map D is given by checking $\Gamma(G^{-1}(\psi^{-1}(x)))$ modulo $g_i(x) = (x - \alpha_i)$: whenever it is zero it means $m_i = 1$, where $\psi^{-1}(x) = x^u$. Observe that the decryption is well defined: the map

$$\alpha_\sim^\psi : \mathbb{Z}_2^L \longrightarrow \mathbb{F}_q[x]/(h_R(x))$$

is clearly injective (and then $\alpha_\sim$ is, by Proposition 1) since the product of all the $g_i(x)$ has degree $L < L + 1$. Observe that $\sim$ is as usual the relation induced by the ideal of $h_R(x)$. □

4. Outlook and further research

In the present communication we have given a new setting to produce many examples of knapsack encryption schemes, showing also how a remarkable example such as [12] perfectly fits our framework. We have proposed a next-to-simplest example when the monoid is chosen to be $(k[x], \cdot)$, one realization of which is given by $\mathbb{F}_q[x]$ reduced by the ideal of an irreducible polynomial of suitable degree.

This brand new application of the knapsack idea reproduces the key results presented in [12] in terms of information rate, but allows us to improve some important features such as

- the information rate is shown to be deterministic by providing an exact formula for it (cf. [12, Section 2.2]).
- it reduces the computations over $\mathbb{F}_{q^d}$ with $p \sim q^d$ but $q \ll p$, where $\mathbb{F}_q$ is a field of small characteristic.

A non trivial variation of this scheme has been found, by taking into account a polynomial which splits over the base field and applying the chinese remainder theorem, allowing the computations to be performed over a direct sum of fields.

In [12] Naccache and Stern conjectured that it might be possible to elliptic curve their scheme, and the new general framework we have presented might be of some help to address this problem.

Moreover, it would be interesting to see how the recent improvements to the NSK protocol presented in [1] may apply to our polynomial instance. This will be matter of further studies.

ACKNOWLEDGEMENTS

The authors would like to thank Patrick Kühn, Gérard Maze, Joachim Rosenthal and Davide Schipani for helpful discussions and suggestions. G.M. was supported in part by Swiss National Science Foundation grant number 149716, M.S. acknowledges partial support from SNF grant 200020_149150/1.

REFERENCES

[1] B. Chevallier-Mames, D. Naccache and J. Stern, Linear bandwidth Naccache-Stern encryption, in *Security and Cryptography for Networks*, 2008, 337–339.
[2] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory*, **22** (1976), 644–654.
[3] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory*, **31** (1985), 469–472.
[4] P. Erdös, Ramanujan and I, *Resonance*, **3** (1998), 81–92.
[5] M. E. Hellman, An overview of public key cryptography, *IEEE Commun. Soc. M.*, **16** (1978), 24–32.
[6] J. Hoffstein, J. Pipher and J. H. Silverman, A ring based public key cryptosystem, in *Algorithmic Number Theory (ANTS III)*, (ed. J.P. Buhler), Springer-Verlag, Berlin, 1998, 267–288.
[7] S. Kiuchi, Y. Murakami and M. Kasahara, High rate mulitiplicative knapsack cryptosystem (in Japanese), *IEICE Tech. Report*, **ISEC98-26** (1998), 43–50.
[8] S. Kiuchi, Y. Murakami and M. Kasahara, New mulitiplicative knapsack-type public key cryptosystems, *IEICE Trans.*, **E84-A** (2001), 188–196.
[9] G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, *Adv. Math. Commun.*, **1** (2007), 489–507.
[10] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report*, **114** (1978), 42–44.
[11] M. Morii and M. Kasahara, New public key cryptosystem using discrete logarithms over GF(P) (in Japanese), *IEICE Trans.*, **J71-D** (1988), 448–453.
[12] D. Naccache and J. Stern, New public key cryptosystem, in *Proceedings of Eurocrypt 97*, Springer-Verlag, 1997, 27–36.
[13] T. Okamoto, K. Tamaka and S. Uchiyama, Quantum public key cryptosystem, in *Advances in cryptology – CRYPTO 2000*, Springer, 2000, 147–165.
[14] J. Patarin, Hidden field equations HFE and isomorphisms of polynomials IP: two new families of asymmetric algorithms, in *Advances in Cryptology – EUROCRYPT '96*, 1996, 33–48.
[15] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, **21** (1978), 120–126.
[16] M. Rosen, *Number Theory in Function Fields*, Springer, 2002.
[17] A. Salomaa, *Public Key Cryptography*, Springer-Verlag, 1990
[18] V. Shoup, New algorithms for finding irreducible polynomials over finite fields, *Math. Comput.*, **54** (1990), 435–447.

Received November 2013; revised February 2014.

E-mail address: giacomo.micheli@math.uzh.ch
E-mail address: michele.schiavina@math.uzh.ch