Cryptanalysis of Cryptosystems Based on Non-commutative Skew Polynomials

Vivien Dubois[1] and Jean-Gabriel Kammerer[1,2]

[1] DGA/MI, Rennes, France
vivien.dubois@m4x.org
[2] IRMAR, Université de Rennes 1, France
jean-gabriel.kammerer@m4x.org

Abstract. Ten years ago, Ko *et al.* described a Diffie-Hellman like protocol based on decomposition with respect to a non-commutative semigroup law. Instantiation with braid groups had first been considered, however intense research on braid groups revealed vulnerabilities of the group structure and of the braid based DH problem itself.
Recently, Boucher *et al.* proposed a similar scheme based on a particular non-commutative multiplication of polynomials over a finite field. These so called skew polynomials have a well-studied theory and have many applications in mathematics and coding theory, however they are quite unknown in a cryptographic application.
In this paper, we show that the Diffie-Hellman problem based on skew polynomials is susceptible to a very efficient attack. This attack is in fact general in nature, it uses the availability of a one-sided notion of gcd and exact division. Given such tools, one can shift the Diffie-Hellman problem to a linear algebra type problem.

Keywords. Diffie-Hellman key exchange, skew polynomials.

1 Introduction

Since the proposal of the original Diffie-Hellman key exchange [5], many variations around the same principle have been proposed. The core structure of a Diffie-Hellman-like key exchange is as follows. Let $\mathcal{K}$ and $\mathcal{D}$ denote fixed domains and let F be a function from $\mathcal{D} \times \mathcal{K}$ to $\mathcal{D}$ such that

1. for any z in $\mathcal{D}$, $F(z, \cdot)$ is a one-way function,
2. the set of functions $F_a = F(\cdot, a)$, a in $\mathcal{K}$ is commutative for the composition of maps, that is, for any a, b in $\mathcal{K}$, $F_a \circ F_b = F_b \circ F_a$.

In a Diffie-Hellman like protocol the function F and a particular element z of $\mathcal{D}$ are public information. In a first pass, each party chooses a random element on his own in the set $\mathcal{K}$ (a for Alice's and b for Bob's), encrypts z with it and sends the result to the other party. Then each party encrypts again the received data with his element of $\mathcal{K}$. In the end, they both hold

$$F_a(F_b(z)) = F_b(F_a(z)).$$

The security of the protocol assumes that given $F_a(z)$ and $F_b(z)$ it is infeasible to compute this common data (computational DH assumption). Of course, the assumption cannot be true if $F(\cdot, z)$ is not a one-way function since one can (for instance) recover a from $F_a(z)$ and stand in the same position as Alice.

The original proposal by Diffie and Hellman was to set F to the exponentiation of z by a in a multiplicative group [5]. When z is a fixed group element, its powers describe a cyclic (hence commutative) subgroup. The one-wayness of $F(z, \cdot)$ means the infeasability of identifying the power (discrete logarithm) of z corresponding with an arbitrary element of $\langle z \rangle$. This proposal seems to find satisfactory instantations and is by far the most widely used. On the other hand, there has been several attempts at building functions F for a Diffie-Hellman protocol from non-commutative algebraic structures. In general, these schemes rely on a particular factorization problem rather than on discrete logarithms. Furthermore, they all appear as variations of the following construction [6].

Generic Diffie-Hellman protocol based on a non-commutative semigroup. Let $(\mathcal{D}, \diamond)$ be a non-commutative semigroup (that is, it needs not have either a neutral element nor all elements to have an inverse). Elements of $\mathcal{D}$ may decompose in a large number of ways in general. Therefore it is assumed that given elements z, z' of $\mathcal{D}$ such that z' admits a factorization of the shape $u \diamond z \diamond v$, it is intractable to find such left and right factors u, v. Hence, one defines the set $\mathcal{K}$ to be ordered pairs $[u, v]$ and one defines $F : (z, [u, v]) \mapsto u \diamond z \diamond v$. When the aforementioned decomposition problem is intractable, F has Property 1. For Property 2 to be fulfilled too, we need functions $F(\cdot, [u, v])$ to commute. This is ensured by choosing elements u, v in a *commutative* sub-semigroup $\mathcal{S}$. Hence, $\mathcal{K} = \mathcal{S} \times \mathcal{S}$. Note that this specialization modifies the one-wayness property of F. It becomes: given an element z of $\mathcal{D}$ and an element z' in $\mathcal{S} \diamond z \diamond \mathcal{S}$ where $\mathcal{S}$ is a commutative sub-semigroup, find u and v in $\mathcal{S}$ such that $z' = u \diamond z \diamond v$.

At this point, it is not clear whether picking left and right factors in a commutative sub-semigroup weakens the decomposition problem. Either way, the cryptosystem can hardly save such a property. Encountered variations of the above description are choosing u and v in distinct subsets $\mathcal{L}, \mathcal{R}$ that are either both commutative or commute the one with the other (in this case, one party of the Diffie-Hellman protocol uses $\mathcal{L} \times \mathcal{R}$ while the other one uses $\mathcal{R} \times \mathcal{L}$). A more general setting may not require the commutative semigroup $\mathcal{S}$ to be a subset of $\mathcal{D}$: it simply needs to act in a different way on the left and on the right of $\mathcal{D}$. This is even more analogous to a general discrete log scheme where $\mathcal{D}$ may be an arbitrary cyclic group while $\mathcal{S}$ is a set of modular integers.

Instantiations. A well-known example of such a scheme based on a full group structure is the one on braid groups [6]. In this setting, pairs of the shape $[u, u^{-1}]$ are considered and the associated decomposition problem is called conjugacy problem. There had already been partial (still exponential) attacks on the general conjugacy problem in braid groups (see for instance [7] for a survey). It turned out a specific polynomial time algorithm exists to attack the Diffie-Hellman assumption in braid groups [3]. The attack uses the property that braid group

elements can be represented by invertible matrices over some (complicated) ring. For any element z of the braid group, we denote by Z the associated matrix. Then, the conjugacy problem arising in the DH-like protocol rewrites to finding U in the representation of the particular commutative set $\mathcal{S}$ such that $Z' = UZU^{-1}$ where Z, Z' are public matrices such that at least one such solution U exists. Candidate solutions can be found by solving the linear algebraic problem: find a matrix U such that $Z'U - UZ = 0$ and $S_iU - US_i = 0$ for any generator s_i of $\mathcal{S}$. The above system in general has many solutions that are not representatives of elements of the braid groups. When it is not possible to sieve them, it does not solve the conjugacy problem. However, the authors further observed that any invertible solution of the above linear system (a random solution is invertible with high probability) has the property of commuting with the elements of $\mathcal{S}$, and as a consequence is equally useful to uncover the shared output of the Diffie-Hellman protocol. Albeit polynomial, this attack did not yield a practical break as is. Yet, instantiation of the Diffie-Hellman protocol with braid groups does not seem to be still investigated.

Recently, Boucher *et al.* proposed a Diffie-Hellman scheme (and a companion ElGamal scheme) based on so called skew polynomials [1]. Skew polynomials are polynomials over a finite field with a particular non-commutative multiplication which uses the Frobenius field automorphism. They were introduced by Ore in 1933 [8] and have found many applications in applied mathematics and coding theory. The proposed Diffie-Hellman scheme follows the previous description with multiplication of skew polynomials as the non-commutative law. Hence, it is an instantiation of the non-commutative Diffie-Hellman protocol which is not based on a full group law.

Our contribution. In this paper, we show that the scheme of Boucher *et al.* is susceptible to a very efficient attack. The attack in fact only remotely uses the structure of skew polynomials, it only uses the availability of a notion of left (or right) gcd and of a related exact division procedure in the underlying domain. In any such setting, one can shift solving the relevant decomposition problem to a linear algebra type problem.

Similarly to the attack on the braid DH scheme, not all solutions of the linear type problem are solutions of the initial decomposition problem. *Real solutions* satisfy one additional condition (such as invertibility in the case of the braid DH scheme). Particular heuristics must be used, then, to find real solutions among the solutions of the linear problem. Based on an assumption which is satisfied in practice for skew polynomials, one can very easily get a real solution by means of gcds, and the attack is completely polynomial time.

We first describe the precise setting and working of the attack without reference to skew polynomials and then describe application to this particular case. Then we consider a possible variation of the scheme based on modular skew polynomials. While our attack seems unfit to this case, we show that density of invertible elements makes it completely weak. Finally we point out that examples based on matrix multiplication can be reduced to modular skew polynomials.

Hence, although the attack looks general in nature, we could not produce another case of application of this attack, and we must leave it as an open problem.

2 General Strategy of the Attack

2.1 The Invertible Case

As a preliminary, let us consider the case when the commutative subsemigroup $\mathcal{S}$ is a group, that is, all its elements are invertible. In this case, a pair $[u, v]$ in $\mathcal{S} \times \mathcal{S}$ is a solution to the Diffie-Hellman decomposition problem for given z in $\mathcal{D}$ and z' in $\mathcal{S} \diamond z \diamond \mathcal{S}$ if and only if $z' = u \diamond z \diamond v$, that is $u' \diamond z' = z \diamond v$ where $u' = u^{-1}$. (Let us denote public variables in bold letters.) As a consequence, when $\mathcal{S}$ is a group, the quadratic looking equation $\boldsymbol{z'} = u \diamond \boldsymbol{z} \diamond v$ with unknown (u, v) can be directly turned into a linear looking equation $u' \diamond \boldsymbol{z'} = \boldsymbol{z} \diamond v$ with unknown $(u' = u^{-1}, v)$. Of course it is the case in braid groups, where one additionally has $u' = v$. Then, representing braid groups elements by matrices (see [3]), the linear looking equation is turned into a linear relation on matrices (over a ring), which can be solved as shown in [3]. Note that the attack may not solve the DH conjugacy problem. The same approach can also be used to find a linear invertible change of variables mapping two sets of quadratic multivariate equations over a field (which is a particular instance of the problem of 'isomorphism of polynomials' [9]). Quadratic multivariate polynomials can be represented by upper triangular matrices (with the same number of non-zero coefficients), and whenever a linear invertible change of coordinates U maps a quadratic polynomial $\boldsymbol{p}$ to a polynomial $\boldsymbol{p'}$, it translates into the matrix identity $\boldsymbol{P'} = U^t \boldsymbol{P} U$ (where superscript t denotes transposition). Since U is invertible, one can attack this problem by solving the linear equation $V\boldsymbol{P'} - \boldsymbol{P}U = 0$ with unknown $(V = (U^t)^{-1}, U)$. It can easily be seen that roughly 3 independent pairs $(\boldsymbol{p}, \boldsymbol{p'})$ with the same U only are heuristically needed to directly solve this problem (*i.e.* find a one-dimensional space of solutions). Higher degree cases can be attacked as well from the identity between degree 2 homogeneous parts. A less immediate attack to this problem was also developed in [10]. A similar attack was independently developed in [2].

2.2 The Setting of our Attack

In this paper, we consider cases where the elements of $\mathcal{S}$ are not invertible, but breaking the Diffie-Hellman problem can also be shifted to solving a commutator-type (linear looking) equation. The basic structure of $\mathcal{D}$ that we need is that of *a domain with a computable notion of left (or right) gcd and computable left (right) exact division* (and $\mathcal{S}$ is a multiplicative commutative sub-semigroup). Here, domain means that it has no divisors of zero: $u \diamond v = 0 \Rightarrow u$ or $v = 0$. Note that it needs not be a form of Euclidean ring.

Before we describe the attack, let us recall the problem hierarchy on which the protocol relies. The Diffie-Hellman problem is: given $\boldsymbol{z}_A = u_A \diamond \boldsymbol{z} \diamond v_A$ and

$\boldsymbol{z}_B = u_B \diamond \boldsymbol{z} \diamond v_B$, compute

$$z_{AB} = u_A \diamond \boldsymbol{z}_B \diamond v_A = u_B \diamond \boldsymbol{z}_A \diamond v_B.$$

A sufficient way of breaking the DH problem is the one of solving the decompositional problem arising in the Diffie-Hellman protocol: given $\boldsymbol{z}$ in $\mathcal{D}$ and $\boldsymbol{z}'$ in $\mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$, compute u, v in $\mathcal{S}$ such that $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$. However, it was noted in [3,12] that breaking a relaxed variant of this problem is enough to break the DH problem: given $\boldsymbol{z}$ in $\mathcal{D}$ and $\boldsymbol{z}'$ in $\mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$, compute u, v *commuting with the elements of* $\mathcal{S}$ such that $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$. Indeed, if an attacker can recover u'_A, v'_A commuting with the elements of $\mathcal{S}$ and such that $\boldsymbol{z}_A = u'_A \diamond \boldsymbol{z} \diamond v'_A$, she can compute

$$u'_A \diamond \boldsymbol{z}_B \diamond v'_A = u_B \diamond u'_A \diamond \boldsymbol{z} \diamond v'_A \diamond v_B = u_B \diamond \boldsymbol{z}_A \diamond v_B = z_{AB}.$$

Hence, with obvious notation, the problem hierarchy is

$$\text{DH} \quad \leq \quad \text{RelaxedDecomposition-DH} \quad \leq \quad \text{Decomposition-DH}.$$

2.3 The Attack

Now we describe the attack. Assume that $\mathcal{D}$ is a domain such that the left (or right) greatest common divisor of two elements always exists and can be computed efficiently and left (or right) exact division can performed efficiently. The attack originates from the following observation. Elements in the set $\mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$ are changed in a particular way when multiplying on the left (or on the right) by an element of $\mathcal{S}$. This property is used to create the Diffie-Hellman protocol. Here we use it to attack the scheme. Let indeed $\boldsymbol{\lambda}$ be an arbitrary element of $\mathcal{S}$. Then,

$$\boldsymbol{\lambda} \diamond (u \diamond \boldsymbol{z} \diamond v) = u \diamond \boldsymbol{\lambda} \diamond \boldsymbol{z} \diamond v.$$

Hence, we obtain another element which too has u as a left divisor. As a consequence, taking the left gcd of $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$ and $\boldsymbol{\lambda} \diamond \boldsymbol{z}'$, one obtains a (non-zero) multiple of u. The same can be done for any element $\boldsymbol{\lambda}$ of $\mathcal{S}$. Let $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_s$ be generators of $\mathcal{S}$. For $\mathcal{S}$ to be transmittable data, these generators must be in very practical number (which we do not consider). Let $\boldsymbol{g}$ be the left gcd of $\{\boldsymbol{z}', \boldsymbol{\lambda}_1 \diamond \boldsymbol{z}', \ldots, \boldsymbol{\lambda}_s \diamond \boldsymbol{z}'\}$, obtained iteratively from pairwise left gcds. Hopefully, relying on the non-commutativity of $\boldsymbol{z}$ with the elements of $\mathcal{S}$, $\boldsymbol{g}$ might be u itself. It can happen that we actually have a way to distinguish between u and its non-trivial multiples. In this case and if $\boldsymbol{g}$ actually equals u, then we use the left exact division algorithm and get v, and the decomposition problem is already broken. Otherwise, let anyway a be such that $\boldsymbol{g} = u \diamond a$. By using the exact division algorithm, we obtain $\boldsymbol{m}$ and $\boldsymbol{m}_i$, $i = 1, \ldots, s$ such that

$$\begin{cases} \boldsymbol{z}' = \boldsymbol{g} \diamond \boldsymbol{m} \\ \boldsymbol{\lambda}_i \diamond \boldsymbol{z}' = \boldsymbol{g} \diamond \boldsymbol{m}_i. \end{cases} \tag{1}$$

Since there are no divisors of zero in $\mathcal{D}$, this system of equations rewrites

$$\begin{cases} \boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} = 0 \\ \boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v - a \diamond \boldsymbol{m}_i = 0. \end{cases} \tag{2}$$

Hence we obtain a set of linear looking equations in the unknown (v, a). Since relevant solutions v commute with $\mathcal{S}$, one has the additional linear looking equations $\boldsymbol{\lambda}_i \diamond v - v \diamond \boldsymbol{\lambda}_i$ for any $i = 1, \ldots, s$.

Not all solutions to these linear conditions, however, are solutions of the initial decomposition problem. This is because when shifting from the initial system (1) to the linear system (2), one loses the information that $\boldsymbol{z} \diamond v$ is a right divisor of $\boldsymbol{z}'$. For instance, any linear combination of such solutions satisfies the linear conditions while not necessarily satisfying the divisibility condition.

Let divisor solutions refer to the linear solutions (v, a) such that $\boldsymbol{z} \diamond v$ is a right divisor of $\boldsymbol{z}'$. We first show that any divisor solution is enough to break the relaxed decomposition problem. Assume indeed that the linear-looking system can be solved, and let (v', a') be an arbitrary divisor solution. By using the exact division algorithm, we get u' such that $\boldsymbol{z}' = u' \diamond \boldsymbol{z} \diamond v'$. From $\boldsymbol{z} \diamond v' = a' \diamond \boldsymbol{m}$, we find $\boldsymbol{z}' = u' \diamond a' \diamond \boldsymbol{m}$, and therefore we also have $\boldsymbol{g} = u' \diamond a'$. Furthermore, u' commutes with all generators of $\mathcal{S}$: from $\boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v' = a' \diamond \boldsymbol{m}_i$, we get

$$u' \diamond \boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v' = \boldsymbol{g} \diamond \boldsymbol{m}_i = \boldsymbol{\lambda}_i \diamond \boldsymbol{z}' = \boldsymbol{\lambda}_i \diamond u' \diamond \boldsymbol{z} \diamond v',$$

and therefore $u' \diamond \boldsymbol{\lambda}_i = \boldsymbol{\lambda}_i \diamond u'$. As a consequence, (u', v') is a pair of elements that both commute with $\mathcal{S}$ and satisfy $\boldsymbol{z}' = u' \diamond \boldsymbol{z} \diamond v'$. Hence the relaxed decomposition problem is broken.

The only unproven step in the attack is the one of finding a divisor solution among the solution linear space. This part may only be heuristically approached. We first need to understand the structure of the solution linear space itself. Observe the following property.

Property 1. Let $\tilde{\mathcal{C}}(\boldsymbol{z})$ denote the set of pairs (c, c') such that $\boldsymbol{z} \diamond c = c' \diamond \boldsymbol{z}$. For any solution (v, a) of the linear looking equation $\boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} = 0$ and any (c, c') in $\tilde{\mathcal{C}}(\boldsymbol{z})$, the pair $(c \diamond v, c' \diamond a)$ is also a solution. As a consequence, the solutions of the equation $\boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} = 0$ are closed under left (coordinate-wise) multiplication by $\tilde{\mathcal{C}}(\boldsymbol{z})$. Of course, they are also closed under addition.

One easily sees that the property generalizes to solutions (v, a) of the complete linear system and left multiplication by $I = \tilde{\mathcal{C}}(\boldsymbol{z}) \cap_i \tilde{\mathcal{C}}(\boldsymbol{\lambda}_i \diamond \boldsymbol{z}) \cap (\cdot, \bar{S})$ where $\bar{\mathcal{S}}$ is the elements that commute with $\mathcal{S}$. One easily checks that $I = \tilde{\mathcal{C}}(\boldsymbol{z}) \cap (\bar{S}, \bar{S})$. Also note that I is a ring for coordinate-wise addition and multiplication.

Additivity and left multiplication by I are degeneracies that are independent of the existential solution. Save these degeneracies, we expect the system of equations to be characteristic of the existential solution. Hence, we expect:

Claim. the solutions of the linear system are all spanned by a single generator through addition and left multiplication by I. Let (v_g, a_g) denote this generator.

Then, since I is a ring, the linear solutions write simply $I \diamond (v_g, a_g)$. For the existential solution $(\hat{v}, \hat{a})$ in particular, there exists $(\hat{c}, \hat{c}')$ in I such that $(\hat{v}, \hat{a}) = (\hat{c}, \hat{c}') \diamond (v_g, a_g)$. This means that (v_g, a_g) is $(\hat{v}, \hat{a})$ purged out of its factors in I. This shows that (v_g, a_g), just like $(\hat{v}, \hat{a})$, is a divisor solution. The other ones are spanned by factors (c, c') related to left factors c of v or right factors c' of u. Finally note that (v_g, a_g) is a common right factor of all linear solutions and since it includes itself, it is in fact the right gcd of the linear solutions.

3 Application to Skew Polynomials Cryptosystems

Diffie-Hellman and ElGamal-like schemes based on skew polynomials were recently presented at PQCrypto 2010 [1]. The Diffie-Hellman protocol follows the general construction described in the introduction and developed by the earlier group-based proposals. We first recall the particularities of skew polynomials and review the setting up of the cryptosystem. Then, we describe unrolling the attack in this particular case. Since the ElGamal scheme relies on the DH problem, we only consider the DH protocol.

3.1 Skew Polynomials

Skew polynomials are polynomials over a finite field with a particular non-commutative inner product. Let $\mathbb{F}_q$ denote the finite field with q elements, and p be the characteristic of the field. Automorphisms of $\mathbb{F}_q$ are the so-called Frobenius maps which are powering to a power of p. Let θ be such an automorphism. We denote by $\star$ the inner product of skew polynomials. It is defined inductively for all $a \in \mathbb{F}_q$ by $X \star a = \theta(a)X$. The ring of skew polynomials is sometimes denoted $\mathbb{F}_q[X, \theta]$.

The ring of skew polynomials is a left and right Euclidean domain, that is, there are both a left and a right Euclidean division algorithm. Using the Euclidean algorithms one can thus compute left and right greatest common divisors, and also perform exact division.

As priorly addressed, due to the non-commutativity of the inner product, skew polynomials admit many factorizations instead of a single one. The cardinality of the number of possible factorizations is expected to be exponential in the degree of the polynomial.

3.2 Generation of the Scheme

For the sake of completeness, we recall part of the specification given in [1]. However the attack is not tied to any particular key generation.

A brute-force approach is suggested to construct the commutative subset $\mathcal{S}$. One iteratively constructs a set of generators $G_0, \ldots, G_s$ of small degree δ. At each step, a polynomial of degree δ is picked at random and tested for commuting with the current set of generators. If it does, it increments the set of

generators, otherwise repeat. The set $\mathcal{S}$ is the commutative algebra spanned by these generators.

Let d be the security parameter of the protocol. A public polynomial $\boldsymbol{Z}$ of degree d is generated. At the execution of the Diffie-Hellman protocol, each participant selects two elements U and V in $\mathcal{S}$ with degree d through combination of the generators of $\mathcal{S}$. More precisely, any picked element is a product of sums of products of the generators.

All tasks performed during the protocol can clearly be made practical, however the cost of generating a set of generators for $\mathcal{S}$ is quoted as a long computation without further detail. The proposed instantiation is with skew polynomials over $\mathbb{F}_4$, generators of $\mathcal{S}$ have degree $\delta = 8$ or 9, and the protocol uses polynomials of degree $d = 600$. For these parameters, they give two examples of $\mathcal{S}$ through generator sets with ≥ 90 polynomials.

3.3 Commutativity Among Skew Polynomials

Before we go on with the attack, it is useful to investigate commutation properties of skew polynomials.

There are particular skew polynomials that commute with any other. This subset is called the center and we denote it by $\mathcal{C}$. A characterization of these elements can be found in [1]. Let m be the order of θ (say the degree of $\mathbb{F}_q$ over $\mathbb{F}_p$ to simplify). Then, the center polynomials are the polynomials over $\mathbb{F}_p$ and in the only powers of X^m.

$$\mathcal{C} = \mathbb{F}_p[X^m].$$

Also, for any polynomial P, let $\mathcal{C}_P$ denote the set of polynomials that commute with P. Of course, P commutes with itself and the elements of the center. As a consequence, $\mathcal{C}_P$ contains the algebra generated by P and $\mathcal{C}$, that is, the set of sums and multiples of elements of $\mathcal{C}$ and P. This algebra is a vector space over $\mathbb{F}_p$. On the other hand, if P has all its coefficients in $\mathbb{F}_p$, it commutes with any polynomial with coefficients in $\mathbb{F}_p$, not only itself and $\mathcal{C}$. Hence,

$$\begin{cases} \text{if } P \in \mathbb{F}_p[X], & \mathcal{C}_P \supseteq \mathbb{F}_p[X] \\ \text{otherwise,} & \mathcal{C}_P \supseteq \langle \mathcal{C}, P \rangle = \mathcal{C}[P]. \end{cases}$$

On the other hand, for any degree bound r, one can easily compute the elements of $\mathcal{C}_P$ with degree $\leq r$. Indeed, the equation $P \star Q = Q \star P$ in the degree $\leq r$ indeterminate Q is a linear system over $\mathbb{F}_p$, and one can find its solutions through linear algebra. We ran experiments for many random choices of P (not with all coefficients in $\mathbb{F}_p$) of degree $\simeq \delta = 8$ and we found that at least up to degree $r = 30$ the elements of $\mathcal{C}_P$ in fact all were in $\mathcal{C}[P]$. It suggests that when one picks generators for $\mathcal{S}$ during the key generation, one actually obtains polynomials in $\mathcal{C}[P_0]$, where P_0 is any smallest degree polynomial in $\mathcal{S}$ modulo $\mathcal{C}$ (modulo is well defined for central polynomials). Hence it is pointless to generate this set by brute force. This is confirmed for the proposals of $\mathcal{S}$ in [1]: we respectively found $P_0 = X^5 + X^3 + \alpha$ and $P_0 = X^3 + X + \alpha$.

3.4 Unrolling the Attack

Let $\boldsymbol{Z}' = U \star \boldsymbol{Z} \star V$ be the data transmitted by one of the participants of the protocol. Our first step is to take the gcd of $\boldsymbol{Z}'$ and $\boldsymbol{\Lambda}_i \star \boldsymbol{Z}'$ over all generators $\boldsymbol{\Lambda}_i$ of $\mathcal{S}$. Due to our previous comment on these generators having a common generator P_0, we actually take the gcd of $\boldsymbol{Z}'$ and $P_0 \star \boldsymbol{Z}'$. We find a polynomial $\boldsymbol{G}$ which is a right multiple of U: there exists a polynomial A such that $\boldsymbol{G} = U \star A$. Also we compute $\boldsymbol{M}, \boldsymbol{M}_0$ such that

$$\begin{cases} \boldsymbol{Z}' = \boldsymbol{G} \star \boldsymbol{M} \\ P_0 \star \boldsymbol{Z}' = \boldsymbol{G} \star \boldsymbol{M}_0. \end{cases}$$

Since the ring is a domain, one deduces from these equations,

$$\begin{cases} \boldsymbol{Z} \star V = A \star \boldsymbol{M} \\ P_0 \star \boldsymbol{Z} \star V = A \star \boldsymbol{M}_0. \end{cases}$$

In addition, one has $P_0 \star V = V \star P_0$ since V commutes with $\mathcal{S}$. These three equations are not linear over $\mathbb{F}_q$, as it would be with the usual product of polynomials, however they are linear alright over $\mathbb{F}_p$. Expanding these equations over $\mathbb{F}_p$, and degree bounding the search space according to the expected degree of the existential (V, A), we can solve the system through linear algebra.

The output of the previous phase is a degree bounded restriction of the entire solution subspace of the linear system. Recall from Section 2.3 that the entire solution space is closed under left multiplication by $I = \tilde{\mathcal{C}}(\boldsymbol{Z}) \cap (\tilde{\mathcal{S}}, \bar{\mathcal{S}})$. If the entire solution space indeed is monogeneous under linearity and left multiplication by I, then this generator is the lowest degree solution (V, A). Then, it can also be found as the right gcd of a linear basis of the bounded degree solution subspace.

We checked the previous expectations in practice with the recommended parameters and beyond. In any tested case, the bounded degree solution admitted only one lowest degree solution (up to $\mathbb{F}_p$ multiples) and any other solution was a multiple of it by a central factor. It incidentally shows that $I = \mathcal{C} \star (1, 1)$ up to the fixed degree bound. Let (V_g, A_g) denote the found generator. We verified that it is a divisor solution and also that it is the right gcd of a linear basis of the bounded degree solutions. We also checked that (V_g, A_g) is the greatest central factor of the original solution $(\hat{V}, \hat{A})$. This greatest central factor can be extracted by taking the left gcd of $(\hat{V}, \hat{A})$ and arbitrary left multiples of it.

The attack has theoretical complexity in $(md)^3$. It takes about a minute with the recommended parameters and with a straightforward implementation in `C++` using the NTL library [11].

4 The Case of Modular Skew Polynomials

We consider a possible variation of the Diffie-Hellman protocol based on modular skew polynomials.

4.1 Constructing Modular Skew Polynomial Rings

Let $\mathcal{R}$ denote a skew polynomial ring $\mathbb{F}_q[X, \theta]$ and let N be an arbitrary element of $\mathcal{R}$. Let $\star N$ denote the set of left multiples of N. Congruence modulo $\star N$ is an equivalence relation over $\mathcal{R}$ and the associated partition elements are called left classes modulo N. Obviously right classes can be defined all the same from $N\star$. Reduction modulo $\star N$ (resp. $N\star$) can be performed by using the left (resp. the right) Euclidean division algorithm.

One awkward property of left classes is that they cannot be multiplied the ones with the others unless N commutes with their elements in a certain sense. Indeed, let $U + \Lambda \star N$ and $V + \Lambda' \star N$ be arbitrary reprensentatives of two classes. Their product

$$(U + \Lambda \star N) \star (V + \Lambda' \star N) = U \star V + \Lambda \star N \star V + (U \star \Lambda' + \Lambda \star N \star \Lambda') \star N$$

does not equal $U \star V$ modulo $\star N$ unless $\Lambda \star N \star V$ is right divisible by N. Since Λ may be chosen arbitrarily, it means $N \star V$ is right divisible by N, or again that there exists W such that $N \star V = W \star N$. When such a W exists, we say that N quasi-commutes with V.

When we want the set of classes to itself be a (non-commutative) ring, we need N to quasi-commute with all elements of $\mathcal{R}$. Let $\mathcal{N}$ denote the set of such N's; we call it the quasi-center of $\mathcal{R}$. Observe that the elements with which N quasi-commutes is closed under the ring operations. Therefore, N quasi-commutes with all elements of $\mathcal{R}$ if and only it quasi-commutes with X and all the constants. This yields an easy characterization of such polynomials N. If a constant a quasi-commutes with N, because of the degree, its dual element is also a constant b. For any a,

$$N \star a = \textstyle\sum_i n_i \theta^i(a) X^i = b \star N = \sum_i n_i b X^i$$

implies that there is k such that all non-zero terms are at $i \equiv k \bmod m$ (where m is the order of θ, assumed equal to the degree of $\mathbb{F}_q$ over $\mathbb{F}_p$). Next, we do the same with X: there are constants a, c such that

$$N \star X = \textstyle\sum_i n_i X^{i+1} = (aX + c) \star N = \sum_i (a\theta(n_i) + c n_{i+1}) X^{i+1} + c n_0 \,.$$

Let j be the smallest i such that $n_i \neq 0$. Then, $c.n_j = 0$ implies $c = 0$, and for any i such that $n_i \neq 0$, $a = n_i/\theta(n_i)$. Let $\bar{a}$ satisfy $\bar{a}/\theta(\bar{a}) = a$. Finally the quasi-center $\mathcal{N}$ is the union of the sets $\mathcal{N}_{k,a} = \bar{a} X^k \mathcal{C}$, $k \in \{0, \ldots, m-1\}$, $a \in \mathbb{F}_q$, where $\mathcal{C} = \mathbb{F}_p[X^m]$ is the center of $\mathcal{R}$. More concisely, this is $\cup_{k=0}^{m-1} \mathbb{F}_q X^k \mathcal{C}$.

For any polynomial N of the quasi-center, left and right multiples of N are just the same sets and classes modulo these sets are simply said classes modulo N. These classes form a ring, which we denote by $\mathcal{R}_N$.

4.2 The Modified Scheme

Modular skew polynomial rings might be considered at the basis of a non-commutative Diffie-Hellman protocol following exactly the same construction

as proposed in [1]. Let d denote the degree of N. Any class admits a unique representative with degree $< d$. Multiplication of classes is realized through multiplication of canonical representatives and subsequent reduction mod N. We denote this operation by $\circ$.

A commutative set $\mathcal{S}$ may again be constructed by selecting commuting classes with canonical representatives of small degree δ. Since δ is a small constant while d is the security parameter, one can assume $2\delta < d$. In this case, the picked canonical representatives in fact commute without modulo. Then, following 3.3, these representatives are spanned over the center by a single polynomial P_0. Elements of $\mathcal{S}$ are arbitrary combinations of P_0 over $\mathcal{C}$ reduced mod N.

4.3 First Remarks

It is immediate that $\mathcal{R}_N$ is not a domain: for any pairwise factorization $U \star V$ of N, we get $U \star V = 0 \bmod N$ while neither U or V is divisible by N.

Now, by definition a class $\bar{U}$ is a left factor of a class $\bar{P}$ if $\bar{P}$ lies in the image space of the map

$$\begin{aligned} \mu(\bar{U}) : \mathcal{R}_N &\longrightarrow \mathcal{R}_N \\ \bar{V} &\longmapsto \bar{U} \circ \bar{V}. \end{aligned}$$

Recall the product $\bar{U} \circ \bar{V}$ equals $U \star V \bmod N$ where U and V are arbitrary elements of $\bar{U}$ and $\bar{V}$. Observe that the set $U \star + N\star$ is independent of the particular U in $\bar{U}$. As a consequence, the left gcd G of U and N is independent of U in $\bar{U}$. Now, from $U\star + N\star = G\star$, we get that right multiples of U and G are the same mod N. As a consequence, the image of $\mu(\bar{U})$ is the set $\bar{G}\circ$. Finally,

Property 2. the set of left factors of a class $\bar{P}$ is the set of classes $\bar{U}$ whose left gcd G with N is a left factor of the canonical representative $\hat{P}$ of $\bar{P}$.

In particular, classes that are left coprime with N are left factors of any class (they are the units of the ring). As one can see, the relationship between divisors and multiples is very loose in $\mathcal{R}_N$. Then, the fact that a class $\bar{\boldsymbol{Z}}'$ is computed as $\bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$ hardly carries information on the particular $\bar{U}$ and $\bar{V}$. Therefore, there is not much information to be obtained in using gcds on $\bar{\boldsymbol{Z}}'$ and $\bar{P}_0 \circ \bar{\boldsymbol{Z}}'$. Instead, since $\bar{P}$ is loosely related to the initial $(\bar{U}, \bar{V})$, one may take advantage of the many equivalent pairs $(\bar{U}, \bar{V})$.

4.4 Attacking the Modular Decomposition

Given a class $\bar{\boldsymbol{Z}}'$, we search for a decomposition $\bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$ where $\bar{U}$ and $\bar{V}$ are in $\bar{\mathcal{S}}$ (that is, commute with P_0 mod N). At least one exists by construction of $\bar{\boldsymbol{Z}}'$ and we expect many others.

We target pairs $(\bar{U}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ such that (e.g.) $\bar{U}$ is left coprime with N. Before going on, observe that being left or right coprime with N is the same when N is in the quasi-center. From $\bar{U}$ being left coprime with N, we get $\bar{W}$ such that $\bar{U} \circ \bar{W} = \bar{1}$. Then right multiplication by $\bar{U}$ is clearly injective (right

multiply by $\bar{W}$), and therefore bijective, and $\bar{U}$ is right coprime with N. Using associativity, one also gets that the left and right inverses are the same.

Now, for any $(\bar{U}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ where $\bar{U}$ is coprime with N,

$$\bar{\boldsymbol{Z}}' = \bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V} \qquad \Longleftrightarrow \qquad \bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}.$$

Also, $\bar{U}$ commutes with $\bar{P}_0$ iff $\bar{W}$ commutes with $\bar{P}_0$. Therefore, the decompositional pairs $(\bar{U}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ with $\bar{U}$ invertible are in bijection with the solutions $(\bar{W}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ of the linear equation $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$ with $\bar{W}$ invertible.

For the attack to be successful, we simply need to extract a pair $(\bar{W}, \bar{V})$ with an invertible $\bar{W}$ from the solutions of the linear system. For this, we rely on the density of such pairs. First observe that restricting elements of pairs in $\bar{\mathcal{S}}$ can only negligibly impact the density of invertible elements. Indeed, the modular condition is exact for all classes whose canonical representative has degree under $\deg(N) - \deg(P_0)$. Since $\deg(P_0)$ asymptotically remains a small constant, the fraction of classes for which the condition involves N is negligible. Besides, we see no reason why the density of $\bar{W}$ among solution pairs $(\bar{W}, \bar{V})$ (not restricted to $\bar{\mathcal{S}}$) of the equation $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$ should differ from the global density.

Claim. The density of invertible $\bar{W}$ among solutions $(\bar{W}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ of $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$ is the same as the density of invertible classes in $\mathcal{R}_N$.

Although N can have many distinct irreducible left factors, these are a subcollection of all possible irreducible left factors of degree $\deg(N)$ polynomials. As a consequence, we expect the fraction of classes left coprime with N to be asymptotically a constant close to 1. For the sake of intuition, for any $u < d$, the fraction of right multiples of degree u monic polynomial L among degree $< d$ polynomials is q^{-u}. Then, the probability that two degree $< d$ polynomials be both right multiples of L is q^{-2u}. Then, the probability that they not share a common left multiple of degree u is $1 - q^u q^{-2u} = 1 - q^{-u}$. We estimate the probability of they be coprime by the probability not to share degree 1 left factors: $1 - 1/q$. This is our expectation of the density of invertible elements.

We checked the above properties in practice. We checked (through sampling) the density of invertible classes both among the left coordinates $\bar{W}$ of the solution space and among all classes. We found densities of the same order in both cases: equal in large characteristic and indeed close to $1 - 1/q$, but slightly different in small characteristic. Hence, we could in any case extract a decompositional solution almost at once.

Interestingly, the attack can be slightly generalized. We may more generally target decompositional solutions $(\bar{U}, \bar{V})$ such that $\bar{U}$ has a right gcd with N not necessarily 1 but a target right factor G of N which commutes with P_0 (for instance a central polynomial). Then, for any such $\bar{U}$, there exist $\bar{W}$ such that $\bar{W} \circ \bar{U} = \bar{G}$. Since both $\bar{U}$ and $\bar{G}$ commute with P_0, the same holds for $\bar{W}$. Then, we simply compute solutions $(\bar{W}, \bar{V})$ in $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ of $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{G} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$, and extract $\bar{W}$ such that the left gcd of $\bar{W}$ and N is G.

5 Beyond the Case of Skew Polynomials?

Another usual example of a non-commutative algebra are square matrices over a finite field. Then, the question arises as to whether this algebra can be used to build a non-commutative Diffie-Hellman protocol. We answer this question negatively by simply describing a well-known connection between square matrices over a finite field and modular skew polynomials (see for instance [4]): square matrices are modular skew polynomials with particular moduli.

Let $\mathbb{F}_p$ be an arbitrary finite field and let $\mathbb{F}_q = \mathbb{F}_{p^n}$ be the degree m extension field of $\mathbb{F}_p$. It is well-known that $\mathbb{F}_q$ is an m-dimensional vector space over $\mathbb{F}_p$. Hence, fixing arbitrary basis elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, one can encode any element of $\mathbb{F}_q$ into an n-dimensional vector. This correspondence also induces a one-to-one correspondence between $\mathbb{F}_p$-linear maps on $\mathbb{F}_q$ and $\mathbb{F}_p$-linear maps on $(\mathbb{F}_p)^m$. The latter simply are represented by $m \times m$ matrices over $\mathbb{F}_p$. Hence, composition of $\mathbb{F}_p$-linear maps on $\mathbb{F}_q$ is the same as matrix multiplication. We can now regard the ring of $m \times m$ matrices over $\mathbb{F}_p$ as the ring of $\mathbb{F}_p$-linear maps on $\mathbb{F}_q$ for $+$ and the composition of maps, which we denote by $L_p(\mathbb{F}_q)$.

We now describe a generator basis for $L_p(\mathbb{F}_q)$. It is well-known that powerings to the power of p are $\mathbb{F}_p$-linear bijections on $\mathbb{F}_q$ called the Frobenius maps. We let θ be the first Frobenius map. Multiplication by an element of $\mathbb{F}_q$ is also $\mathbb{F}_p$-linear. Therefore, linear combinations over $\mathbb{F}_q$ of Frobenius maps (powers of θ) also are $\mathbb{F}_p$-linear. It can be seen that this representation is injective and finally, by a simple cardinality argument, one-to-one. As a consequence, $L_p(\mathbb{F}_q)$ is the set of linear combinations over $\mathbb{F}_q$ of the Frobenius maps, $\sum_{i=0}^{m-1} a_i \circ \theta^i$. These maps can be identified with polynomials $\sum_{i=0}^{m-1} a_i X^i$. Mapping the ring structure of $L_p(\mathbb{F}_q)$ to these polynomials, one obtains the usual $+$ law but multiplication following the identities $X \circ a = \theta(a)X$ and $X^n = 1$. This is exactly the identities defining skew polynomials $\mathbb{F}_q[X, \theta]$ modulo the center polynomial $X^m - 1$.

$$\{m \times m \text{ matrices over } \mathbb{F}_p\} = L_p(\mathbb{F}_q) = \mathbb{F}_q[X, \theta]/(X^m - 1).$$

Acknowledgements

We wish to thank Pierre Loidreau for helpful discussion on the subject of skew polynomials at the early stage of this work. We also wish to thank the anonymous referees of PKC 2011 for their detailed and helpful comments.

References

1. Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. In Nicolas Sendrier, editor, *PQCrypto*, volume 6061 of *Lecture Notes in Computer Science*, pages 126–141. Springer, 2010.
2. Charles Bouillaguet, Jean-Charles Faugère, Pierre-Alain Fouque, and Ludovic Perret. Differential-algebraic algorithms for the isomorphism of polynomials problem. Cryptology ePrint Archive, Report 2009/583, 2009. http://eprint.iacr.org/.

3. Jung Hee Cheon and Byungheup Jun. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 212–225. Springer, 2003.
4. R.S. Coulter, G. Havas, and M. Henderson. Giesbrecht's algorithm, the HFE cryptosystem, and Ore's ps-polynomials. In *Computer Mathematics: Proceedings of the Fifth Asian Symposium (ASCM 2001) (K. Shirayanagi and K. Yokoyama, eds.), Lecture Notes Series on Computing, vol. 9, World Scientific*, pages 36–45, 2001.
5. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT–22(6):644–654, November 1976.
6. Ki Hyoung Ko, Sangjin Lee, Jung Hee Cheon, Jae Woo Han, Ju-Sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Mihir Bellare, editor, *CRYPTO*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2000.
7. Karl Mahlburg. An overview of braid group cryptography, 2004.
8. O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.
9. Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *EUROCRYPT*, pages 33–48, 1996.
10. Ludovic Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370. Springer, 2005.
11. Victor Shoup. NTL: A library for doing number theory. Available at http://www.shoup.net/ntl.
12. Vladimir Shpilrain and Alexander Ushakov. The conjugacy search problem in public key cryptography: unnecessary and insufficient. Cryptology ePrint Archive, Report 2004/321, 2004. http://eprint.iacr.org/.