Cryptanalysis of Cryptosystems Based on Noncommutative Skew Polynomials

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

[1] DGA-MI, Bruz, France
[2] Institut de recherche mathématique de Rennes, Université de Rennes 1
Rennes, France
vivien.dubois (at) m4x.org
jean-gabriel.kammerer (at) m4x.org

Abstract. We describe an attack on the family of Diffie-Hellman and El-Gamal like cryptosystems recently presented at PQ Crypto 2010. We show that the reference hard problem is not hard.

1 Description of the Cryptosystems

Skew polynomials are polynomials with a particular noncommutative 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 still a left and right Euclidean domain, that is, there are both a left and a right Euclidean division algorithm. Using the Euclidean algorithms we can thus compute left and right greatest common divisors. However, due to the noncommutativity 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.

Based on this property, the authors of [1] designed public key cryptosystems where the trapdoor information is knowing one particular factorization of a skew polynomial. However, for the purpose of the cryptosystem, both the public skew polynomial and its secret factorization must be of particular nature. At this point, it is not useful to describe the proposed cryptosystems. Instead, we simply show that the instance of the factoring problem arising in their cryptosystems is easy.

This problem is the following. Let $\mathcal{S}$ be a randomly generated subset of skew polynomials whose elements commute with each others. This set is public information. Let Q be a randomly chosen polynomial with

many factors of small degree which do not commute with the elements of $\mathcal{S}$. This polynomial is also public information. In the Diffie-Hellman like protocol of [1], any participant randomly chooses two polynomials L and R which are generated from elements of $\mathcal{S}$, and outputs $P = L \star Q \star R$. The cryptosystem relies on the intractability of extracting L and R from P. The rationale of the cryptosystem is that this particular factorization is lost among the exponentially numerous other ones.

2 Our Attack

A particular property of the polynomial P is that it is 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 construct a Diffie-Hellman like cryptosystem. Here we use it to attack the scheme. Let indeed Λ be an arbitrary element of $\mathcal{S}$. Then:

$$P \star \Lambda = L \star (Q \star \Lambda) \star R,$$

because Λ and R are both in $\mathcal{S}$ and therefore commute. As one can see, R is therefore a right factor of both P and $P \star \Lambda$. This is true for any Λ in $\mathcal{S}$. As a consequence, the right GCD of P and $P \star \Lambda$ is a multiple of R. Hopefully, relying on the noncommutativity of Q with elements of $\mathcal{S}$, it might be R itself. If it is, which we can detect from the degree of the GCD matching the degree of R, then we simply right divide P by it, next by Q and get L. If it is not, then the computed GCD (denote it by G) is a left multiple of R and let A such that $G = A \star R$. Again we can right divide P by G and find a polynomial M. From

$$P = M \star A \star R = L \star Q \star R,$$

we deduce that

$$M \star A = L \star Q.$$

In the above equation, M and Q are known and L and A are unknown. To render this distinction, we write known polynomials in bold characters:

$$\boldsymbol{M} \star A = L \star \boldsymbol{Q}. \tag{1}$$

Finding L or A is equivalent to finding L and A altogether. Hence, we consider solving the above equation in (L, A).

With the usual polynomial product, one could commute say $\boldsymbol{Q}$ and L and the problem would resemble computing the least common multiple

of $\boldsymbol{M}$ and $\boldsymbol{Q}$. More precisely, since both multiples have prescribed degree $\delta = \deg(P) - \deg(R)$, the problem is finding a common multiple of $\boldsymbol{M}$ and $\boldsymbol{Q}$ with degree at most δ. This is a simple linear algebra problem since the coefficients of both handsides are linear in the coefficients of the searched polynomials L and A. With obvious notation, one would have for any $k = 0, \ldots, \delta$,

$$\sum_{i+j=k} \boldsymbol{m}_i \; a_j = \sum_{i+j=k} l_i \; \boldsymbol{q}_j.$$

Here, with the skew inner product, the equations are slightly more complicated. For any $k = 0, \ldots, \delta$, we get

$$\sum_{i+j=k} \boldsymbol{m}_i \; \theta^i(a_j) = \sum_{i+j=k} l_i \; \theta^i(\boldsymbol{q}_j).$$

These equations are not linear in the variables a_j's because θ is not linear over $\mathbb{F}_q$. However, we can write all elements of $\mathbb{F}_q$ over the prime field $\mathbb{F}_p$ of $\mathbb{F}_q$ and, since θ is linear over $\mathbb{F}_p$, solve the associated linear equations over $\mathbb{F}_p$. Let $e_1, \ldots, e_n$ denote a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ ($n = \log_p(q)$). Then the above identity rewrites into n linear equations over $\mathbb{F}_p$ in the $\mathbb{F}_p$ coefficients $a_i^1, \ldots, a_i^n$ of the a_i's and the $\mathbb{F}_p$ coefficients $l_i^1, \ldots, l_i^n$ of the l_i's. The total number of linear equations is therefore $(\delta + 1)n$, and the number of unknown coefficients is $n(\deg(A) + \deg(L) + 2)$. We know that Equation 1 has at least one solution (together with the $\mathbb{F}_p$-line it spans), and we expect no other solution as soon as

$$n(\delta + 1) \geq n(\deg(A) + \deg(L) + 2).$$

Substituting with the value of δ, this condition rewrites

$$\deg(\boldsymbol{M}) > \deg(L).$$

It means that in both handsides the number of known coefficients must exceed the number of unknown values. It seems a marginal case that the above inequality may not be satisfied because it implies that the right GCD of P and $P \star \Lambda$ has degree more than the degree of Q plus the degree of R. Should this however happen, one may consider another choice of Λ. Should this happen for any Λ in the generator basis of $\mathcal{S}$, we can still artificially increase the number of known coefficients in both handsides by using the following trick.

Let G be the smallest of the right GCDs of P and $P \star \Lambda$ when Λ runs over a generator basis of $\mathcal{S}$. Let Λ' be an arbitrary element of $\mathcal{S}$.

We know that G is a right divisor of $P \star \Lambda'$ and we let M' be such that $P \star \Lambda' = M' \star G$. Also, as before, $P = M \star G$. Since $G = A \star R$, we get $P \star \Lambda' = M \star A \star \Lambda' \star R$ and also $P \star \Lambda' = M' \star A \star R$, and therefore

$$M \star A \star \Lambda' = M' \star A.$$

Again we write in bold characters known polynomials:

$$\boldsymbol{M} \star A \star \boldsymbol{\Lambda'} = \boldsymbol{M'} \star A.$$

And again, this gives a set of linear equations over $\mathbb{F}_p$ in the $\mathbb{F}_p$ coordinates of the coefficients of A. When increasing the degree of Λ', one increases the number of linear equations while A remains the same. As a consequence, we expect that by taking Λ' large enough one can successfully determine A. From A, one finally gets L by using our initial equation.

3 Future Work

The attack is being implemented and we expect to provide experimental details of the attack in the very near future.

Acknowledgement. We wish to thank Pierre Loidreau for helpful discussion on the subject of skew polynomials at the early stage of this work.

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.