J. Cryptology (2001) 14: 225–230
DOI: 10.1007/s00145-001-0004-9

Journal of
CRYPTOLOGY

Public Key Cryptosystems Based on Drinfeld Modules Are Insecure*

Thomas Scanlon
Department of Mathematics, University of California,
Evans Hall, Berkeley, CA 94720, U.S.A.
scanlon@math.berkeley.edu

Communicated by Tom Berson

Received August 1999 and revised October 2000
Online publication 9 April 2001

Abstract. We show that analogues of popular public key cryptosystems based on Drinfeld modules are insecure by providing polynomial time algorithms to solve the Drinfeld module versions of the inversion and discrete logarithm problems.

Key words. Drinfeld module, Public key cryptography, Discrete logarithm.

1. Introduction

Koblitz [3] and Miller [5] substituted computations on elliptic curves for multiplication in some public key cryptosystems obtaining (presumably) more secure systems. Since they made the leap from ordinary multiplication to elliptic curve addition, other authors have suggested other analogous cryptosystems based on other finite mathematical structures.

Drinfeld christened the structures that bear his name as "elliptic modules" to emphasize the tight connection between the theories of elliptic curves and of Drinfeld modules. In the ensuing years, work on the arithmetic of Drinfeld modules has borne out Drinfeld's insight into the the correspondence between elliptic curves and Drinfeld modules [2]. With these analogies in mind one might reasonably hope (as did the author of the current note) that cryptosystems based on Drinfeld modules should, at least, share the properties of their elliptic curve based cousins. Unfortunately, we dash this hope by showing that Drinfeld module based cryptosystems are insecure.

We define precisely what we mean by "Drinfeld module" and the various "Drinfeld module versions" of cryptosystems and problems in the next section. Roughly, a Drinfeld module is a nonlinear, commutative subring of the ring of regular endomorphisms of the additive group of a field. For example, if k is a field of characteristic $p > 0$, then

* This research was partially supported by an NSF MSPRF.

the ring generated under addition and composition by the function $f\colon k \to k$ given by $f(x) = x^p - x$ is a Drinfeld module. Usually, the Drinfeld module version of a group based cryptosystem is given by replacing the underlying group by the additive group of a finite field and multiplication by integers (or exponentiation) by the action of the Drinfeld module. Since every Drinfeld module contains nonlinear elements, such cryptosystems may very well be secure. Because the underlying group is an additive group, these cryptosystems should be relatively easy to implement. However, the latter property points to the fundamental flaw in the heuristics behind the former property: while a Drinfeld module is generically nonlinear, when considered on a fixed finite field it may be regarded as a linear object. In this note we translate this observation into a proof that any cryptosystem based on the supposed infeasibility of solving the Drinfeld module versions of the discrete logarithm or inversion problems is insecure.

The proofs of the main results of this note are not difficult at all. It would surprise me to learn that similar ideas have not flashed through the heads of other people acquainted with Drinfeld modules and elliptic curve public key cryptosystems. In fact, I have been told that the idea of cryptosystems based on Drinfeld modules has been proposed before, but I was unable to locate a published reference. I hope that if anyone else is smitten with the notion that Drinfeld modules have anything to do with encryption, this note will serve to help them avoid wasted effort in this direction.

2. Definitions and Notation

In this section we fix our notation and define our terms precisely.

Denote by p a fixed prime number and q a fixed power of p. We denote by $\mathbb{F}_p$ the field of p elements and $\mathbb{F}_q$ the field of q elements. Let k be a field of characteristic p. The Frobenius endomorphism of k is the function $F\colon k \to k$ defined by $F(x) := x^p$. The ring of twisted polynomials in F over k is $k\{F\} := \{\sum_{i=0}^n a_i F^i\colon n \in \mathbb{N}, a_i \in k\}$ where addition is defined coordinatewise and multiplication is defined by the usual convolution formula with the commutation rule $Fa = a^p F$. We may regard an element $\Lambda = \sum_{i=0}^n \lambda_i F^i$ of $k\{F\}$ as an additive homomorphism of k by the formula $x \mapsto \sum_{i=0}^n \lambda_i x^{p^i}$. We denote this homomorphism assigning to a polynomial in F its corresponding additive map by $\iota\colon k\{F\} \to \mathrm{Hom}(k, +)$. If $\Lambda = \sum_{i=0}^n \lambda_i F^i$ is a nonzero element of $k\{F\}$, then we define the degree of Λ to be $\deg(\Lambda) := \max\{i\colon \lambda_i \neq 0\}$.

Definition. A Drinfeld module (for the ring $\mathbb{F}_p[t]$) is a ring homomorphism $\varphi\colon \mathbb{F}_p[t] \to k\{F\}$ for which $\deg(\varphi(t)) > 0$.

In the literature, Drinfeld modules for slightly more complicated rings are considered on occasion. Since we aim to dismiss all Drinfeld modules as candidates as bases for cryptosystems, we include the definition of the more general Drinfeld modules, but the reader would lose very little by ignoring this generalization. Let C be an absolutely irreducible, smooth, projective curve over $\mathbb{F}_q$ and let $\infty \in C$ be a closed point. Let A be the ring of regular functions on $C\backslash\{\infty\}$. The field $\mathbb{F}_q$ is called the field of constants of A.

Definition. A Drinfeld module for A is a ring homomorphism $\varphi\colon A \to k\{F\}$ for which there is some $a \in A$ with $\deg(\varphi(a)) > 0$.

Take $q = p$, $C = \mathbb{P}^1$, and $\infty = [0\colon 1]$ to recover the definition of a Drinfeld module for $\mathbb{F}_p[t]$. As mentioned in the Introduction, a Drinfeld module is just the choice of a nonlinear commutative (normal) subring of $k\{F\}$ given together with a presentation.

It is always possible to find two elements $s, t \in A$ so that A is generated as a ring by s, t, and the field of constants of A, $\mathbb{F}_q$. Moreover, if $q = p^r$, A has field of constants $\mathbb{F}_q$, and $\varphi\colon A \to k\{F\}$ is a Drinfeld module, then the image of φ lies in the subring $k\{F^r\}$.

Definition. By the discrete logarithm problem for a Drinfeld module we mean: given a finite field k of characteristic p, Drinfeld module $\varphi\colon A \to k\{F\}$, and elements $x, y \in k$, find $a \in A$ (if it exists) so that $\varphi(a)(x) = y$.

Definition. By the inversion problem for a Drinfeld module we mean: given a finite field k of characteristic p, Drinfeld module $\varphi\colon A \to k\{F\}$, and $a \in A$ for which $\varphi(a)\colon k \to k$ is a bijection, find $b \in A$ so that $\varphi(b)\colon k \to k$ is the inverse of $\varphi(a)$.

Public key cryptosystems based on the supposed intractibility of the discrete logarithm problem for certain groups (e.g., Diffie–Hellman, Massey–Omura, ElGamal) have natural Drinfeld module analogues. Likewise, cryptosystems based on the difficulty of inverting certain group automorphisms (e.g., RSA) have Drinfeld module versions. Since none of these systems is secure, we do not describe them in detail, but to fix ideas we sketch the Drinfeld module version of the Diffie–Hellman cryptosystem.

Cryptosystem (Drinfeld Module Version of Diffie–Hellman). Fix p a prime and q a power of p. Set $k := \mathbb{F}_q$. Fix also a Drinfeld module $\varphi\colon A \to k\{F\}$ and an element $\zeta \in k$. All these data are assumed to be public knowledge. I and II choose a_I (respectively, a_{II}) in A. I transmits $\varphi(a_{\mathrm{I}})(\zeta)$ to II while II transmits $\varphi(a_{\mathrm{II}})(\zeta)$ to I. The common private key is $\varphi(a_{\mathrm{II}})(\varphi(a_{\mathrm{I}})(\zeta)) = \varphi(a_{\mathrm{II}}a_{\mathrm{I}})(\zeta) = \varphi(a_{\mathrm{I}}a_{\mathrm{II}})(\zeta) = \varphi(a_{\mathrm{I}})(\varphi(a_{\mathrm{II}})(\zeta))$.

3. Attacks

We attack the cryptosystems introduced in the last section by observing that the ring of functions induced by a Drinfeld module on a finite field is equal to a ring of linear functions, properly interpreted. Linear algebra provides our picks.

The proofs of the propositions below involve regarding the finite field k as a vector space over a smaller finite field and then performing certain matrix computations. In order to perform these matrix computations we need to fix a basis for k and a method for expressing elements of k with respect to this basis. In most practical implementations of the encryption schemes described in the previous section, k is already expressed thus. If one perversely chose to work with a coordinate-free k, we could put k in the required form very quickly (see Proposition 1), anyhow. So, in all the statements following Proposition 1 we regard the choice of a basis for k as being cost-free.

Proposition 1. *There is a probabilistic polynomial time algorithm which given a finite field k of characteristic p produces a basis of k over $\mathbb{F}_p$ and a polynomial time procedure to express any element of k in terms of that basis.*

Proof. Let $d := [k\colon \mathbb{F}_p] = \log_p|k|$. Randomly choose $(e_1, \ldots, e_d) \in k^d$. Set $B := \{e_1, \ldots, e_d\}$. With probability $\prod_{i=0}^{d-1}(1 - p^{-i})$ it is a basis. Repeating this step roughly $-\log_p \varepsilon$ times we can guarantee that we have found at least one basis with probability $1 - \varepsilon$.

We now define by recursion some elements $b_i \in k$ and additive operators $\psi_i\colon k \to k$ for $1 \leq i \leq d$. Set $b_1 := e_1$ and $\psi_1 := \mathrm{id}_k$. For $i + 1$, set $\psi_{i+1} := b_i^p(F - 1)b_i^{-1}\psi_i$ and $b_{i+1} := \psi_{i+1}(e_{i+1})$.

B is a basis if and only if all of the b_i's are nonzero. If this choice of B fails to be a basis, then repeat the above steps.

Given $a \in k$ written as $a = \sum_{i=1}^{d} a_i \cdot e_i$ with $a_i \in \mathbb{F}_p$ we have the following recursive (starting with $i = d$ and working backwards) formula for a_i:

$$a_i = b_i^{-1}\psi_i\left(a - \sum_{j>i} a_j e_j\right).$$

If one counts the taking of multiplicative inverses and the application of F as no more costly than multiplication, then the above formula requires $O(d^2)$ operations to implement. If one insists upon counting only addition and multiplication as basic operations, then the cost estimate rises to $O(d^3)$ as one may compute $b^{-1} = b^{p^d-1}$ for $b \in k$. If one wishes to make the estimate uniform in p, then the right bound is $O(\log(p)d^3)$. □

In what follows, the real number ω is a constant for which the problem of multiplying two $m \times m$ matrices over the field K may be solved with $O(m^\omega)$ ring operations in K. The standard approach to matrix multiplication gives $\omega \leq 3$, but there are algorithms to achieve $\omega < 2.376$ [1].

Proposition 2. *There are real numbers C_1 and r_1 and an algorithm to find, for any prime p, finite field k of characteristic p, Drinfeld module $\varphi\colon A \to k\{F\}$, and $a \in A$ with $\varphi(a)$ inducing a bijection of k, an inverse to $\varphi(a)$ using at most $C_1(\log_p|k|)^{r_1}$ field operations in $\mathbb{F}_p$.*

Proof. Let $\mathcal{A} := \iota \circ \varphi(A) \subseteq \mathrm{Hom}(k, +)$. The elements of $\mathcal{A}$ are additive homomorphisms, but they are most likely not k-linear maps. However, they are $\mathbb{F}_p$-linear maps. After fixing a basis Γ for k over $\mathbb{F}_p$ (as given by Proposition 1) we may identify $\mathrm{Hom}(k, +)$ with the matrix ring $M_m(\mathbb{F}_p)$ where $m = \dim_{\mathbb{F}_p}(k) = \log_p(|k|)$. Under this identification, $\mathcal{A}$ is a ring of $m \times m$ matrices over $\mathbb{F}_p$. Given $a \in A$ for which $\iota \circ \varphi(a)$ is a unit, we can find the inverse to $\iota \circ \varphi(a)$ simply by inverting the corresponding matrix to obtain $\beta \in \mathcal{A}$. Even without taking into account extra information about a, this inversion requires at the worst $O(m^\omega)$ field operations. □

Thus, cryptosystems based on the supposed intractibility of inverting the action of a Drinfeld module (for example, the Drinfeld module version of RSA) are insecure.

One might imagine that in some systems knowing the inverse to $\iota \circ \varphi(a)$ is not enough. However, without much additional effort we can recover some $b \in A$ for which $\iota \circ \varphi(b) = (\iota \circ \varphi(a))^{-1}$.

Proposition 3. *There is a polynomial time algorithm for solving the inversion problem for Drinfeld modules.*

More precisely, there are real numbers C_2 and r_2 and an algorithm which, given a prime p, finite field k of characteristic p, Drinfeld module $\varphi\colon A \to k\{F\}$, and $a \in A$ for which $\varphi(a)$ induces a bijection of k, finds $b \in A$ for which $\varphi(b)$ is the inverse to $\varphi(a)$ on k requiring fewer than $C_2(\log_p|k|)^{r_2}$ field operations in $\mathbb{F}_p$.

Proof. Let $s, t \in A$ generate A over its field of constants, $\mathbb{F}_{p^r}$. As above, let $\mathcal{A} := \iota \circ \varphi(A)$. For now, let Γ be a basis for k over $\mathbb{F}_{p^r}$ as given by Proposition 1. Let $m := \dim_{\mathbb{F}_{p^r}}(k)$. As $\mathcal{A}$ is a commutative subalgebra of $M_m(\mathbb{F}_{p^r})$, $\dim_{\mathbb{F}_{p^r}}(\mathcal{A}) \le m$. Compute the vectors $S := \{\iota \circ \varphi(s^i t^j)\colon 0 \le i, j < m\}$. Assuming that we have already computed $\iota \circ \varphi(s)$ and $\iota \circ \varphi(t)$ as matrices relative to Γ, this requires m^2 matrix multiplications and can be accomplished with $O(m^{2+\omega})$ field operations in $\mathbb{F}_{p^r}$. We can extract a basis B for $\mathcal{A}$ from S with $O(m^{\omega+1})$ field operations in $\mathbb{F}_{p^r}$ using the algorithm of Problem 2.2.10a of [1]. So, we have a set $I \subseteq \{(i, j)\colon 0 \le i, j < m\}$ so that $\{\varphi(s^i t^j)\colon (i, j) \in I\}$ is a basis of $\mathcal{A}$ over $\mathbb{F}_{p^r}$.

Let $\beta = (\iota \circ \varphi(a))^{-1}$ be the inverse to $\iota \circ \varphi(a)$ computed in the previous proposition. From the basis Γ of k, we obtain a standard basis Γ' for $\mathrm{Hom}(k, +)$. We know that $\beta \in \mathcal{A}$. We are given the vectors β and b for $b \in B$ in terms of the basis Γ' of $\mathrm{Hom}(k, +)$. Say, $C\Gamma' = (\beta, \varphi(1), \varphi(a), \ldots, \varphi(a^{t-1}))$ for appropriate $C \in M_{(|B|+1)\times m^2}(\mathbb{F}_p)$. To find the expression for β as a linear combination of the elements of B, we find the kernel of C (which we can accomplish in time $O(m^{1+\omega})$ [1, Problem 2.2.3b]) and then scale. So, we have an expression $\beta = \sum_{(i,j)\in I} \mu_{(i,j)}\varphi(s^i t^j)$ for appropriate $\mu_{(i,j)} \in \mathbb{F}_{p^r}$. We take $b = \sum_{(i,j)\in I} \mu_{(i,j)} s^i t^j$.

Converting the field operations in $\mathbb{F}_{p^r}$ into operations in $\mathbb{F}_p$ costs a factor of $O(r \log r)$, but we should replace m by $\dim_{\mathbb{F}_p}(k) = rm$. Thus, the estimate of $O(\log_p(|k|)^{1+\omega})$ for the number of field operations used in $\mathbb{F}_p$ remains valid. □

The techniques of the last proposition extend to the discrete logarithm problem for Drinfeld modules.

Proposition 4. *There is a polynomial time algorithm to solve the discrete logarithm problem for Drinfeld modules.*

That is, there are real numbers C_3 and r_3 and an algorithm which, given a prime p, finite field k of characteristic p, Drinfeld module $\varphi\colon A \to k\{F\}$, and elements ζ and y of k, computes an $a \in A$ with $\varphi(a)(\zeta) = y$ (if such an a exists) using fewer than $C_3(\log_p|k|)^{r_3}$ field operations in $\mathbb{F}_p$.

Proof. Let $M := \varphi(A) \cdot \zeta$ be the A-module generated by ζ. Let $\mathcal{A} := \iota \circ \varphi(A) \subseteq \mathrm{Hom}(k, +)$. Let $\mathbb{F}_{p^r}$ be the field of constants of A. Let $m := \dim_{\mathbb{F}_{p^r}}(k)$. As above, thin the set of $\{\varphi(s^i t^j)(\zeta)\colon 0 \le i, j < m\}$ to a basis B for M where A is generated by s and t

over $\mathbb{F}_{p^r}$. The method described in the proof of the previous proposition requires at most $O(m^{1+\omega})$ field operations in $\mathbb{F}_{p^r}$.

If $y \in M$, that is $y = \varphi(a)(\zeta)$ for some $a \in A$, then as in the previous paragraph we need only express y in terms B. Following the algorithm already outlined in the previous proposition, we carry out this computation in time $O(m^{1+\omega})$. □

Thus, no public key cryptosystem based on the apparent infeasibility of solving the discrete logarithm problem for Drinfeld modules (such as the Drinfeld module versions of Diffie–Hellman, Massey–Osmura, and ElGamal) is secure.

Acknowledgments

I thank Bernd Sturmfels for directing me to the algorithms in [1] and the anonymous referees for suggesting improvements to this paper.

References

[1] D. Bini and V. Pan, *Polynomial and Matrix Computations*: *Fundamental Algorithms*, Birhäuser, Boston, 1994.

[2] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebniße der Mathmatik und ihrer Grenzgebiete, vol. 35, Springer-Verlag, Berlin, 1996.

[3] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* 48 (1987), 203–209.

[4] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1987.

[5] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology—CRYPTO* '85 (Santa Barbara, CA, 1985), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, Berlin.