Cryptanalysis of a Cryptosystem based on Drinfeld modules

Simon R. Blackburn and Steven D. Galbraith

Information Security Group
Mathematics Department
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom
S.Blackburn@rhul.ac.uk, Steven.Galbraith@rhul.ac.uk

Abstract. A public key cryptosystem based on Drinfeld modules has been proposed by Gillard, Leprevost, Panchishkin and Roblot. The paper shows how an adversary can directly recover a private key using only the public key, and so the cryptosystem is insecure.

1 Introduction

Gillard, Leprevost, Panchishkin and Roblot [1] have recently proposed a cryptosystem based on Drinfeld modules. We refer to this cryptosystem as the GLPR cryptosystem. We aim to show that this cryptosystem is insecure, by showing how an adversary with access to just the public key may recover a corresponding private key. Thus the title of a paper by Scanlon [3] remains correct.

The paper is divided into three sections. Section 2 describes the encryption function of the GLPR cryptosystem, avoiding the use of Drinfeld module terminology. This description makes use of two linear maps λ_1 and λ_2 that Gillard *et al* [1] define using Drinfeld modules. Section 3 explores the definition of λ_1 and λ_2 in more detail, and shows that these linear maps have a property claimed in Section 2 which we use in our cryptanalysis. Section 3 is the only section that uses Drinfeld modules explicitly. Finally, Section 4 describes our attack on the GLPR scheme.

2 The Cryptosystem

We describe the encryption function of GLPR cryptosystem. Let p be a prime and let d and e be integers. Typical values according to [1] are $p \approx 2^{32}$, $d = 5$ or $d = 6$ and $e = 5$ or $e = 7$.

The GLPR cryptosystem is a trapdoor one-way function $\psi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ specified by selecting two bijective $\mathbb{F}_p$-linear maps λ_1, λ_2 on the vector space $\mathbb{F}_{p^d}$ and an element $\delta \in \mathbb{F}_{p^d}$. The function is then defined by

$$\psi(z) = \lambda_1((\lambda_2\, z)^e + \delta) \tag{1}$$

In fact, the linear maps λ_1 and λ_2 are chosen to be of the form

$$b_0 + b_1 F + \cdots b_{d-1} F^{d-1} \tag{2}$$

where F is the p-power Frobenius map on $\mathbb{F}_{p^d}$ and where the coefficients b_i lie in $\mathbb{F}_{p^d}$.

The **public key** of the system will be the prime p, the integer d and certain information about how to compute ψ. The **private key** or **trapdoor** consists of the transformations λ_1, λ_2 and the values e and δ. Note that if λ_1, λ_2, e and δ are all known, it is easy to compute the inverse of ψ.

The particular structure of the maps λ_i means that, if e is small, it is possible to give a compact description of how to compute the function $\psi(z)$, without explicitly describing λ_1, λ_2, e or δ. We refer to the original paper [1] for details; for our purposes it is sufficient to know the fact (obvious, since the GLPR proposal is a public key cryptosystem) that the image of any element in $\mathbb{F}_{p^d}$ under ψ can easily be computed from the public key.

We note that the public key does not determine the private key uniquely: for any $b \in \mathbb{F}_{p^d}$ the private key $(\lambda_1 b^{-e}, b\lambda_2, e, b^e\delta)$ gives the same function ψ as the private key $(\lambda_1, \lambda_2, e, \delta)$. Any of these solutions can be used as a trapdoor for the function ψ.

3 Drinfeld modules

The mappings λ_1 and λ_2 of the previous section were originally defined using Drinfeld modules [1]. This section recaps this definition, so that it can be seen that λ_1 and λ_2 really do have the form (2).

Let p be a prime number. We denote by $\mathcal{A}$ the ring $\mathbb{F}_p[T]$ of polynomials in a variable T with coefficients in $\mathbb{F}_p$. We write $\mathcal{A}\{\tau\}$ for the ring defined as follows. The set of elements of $\mathcal{A}\{\tau\}$ is the set of polynomials in τ with coefficients in $\mathcal{A}$. Addition in $\mathcal{A}\{\tau\}$ is the usual addition for polynomials. However, multiplication in $\mathcal{A}\{\tau\}$ is 'twisted' by using the rule $\tau^k \times a = a^{p^k}\tau^k$ for all $a \in \mathcal{A}$ and all positive integers k. Thus $\mathcal{A}$ is naturally has the structure of a (left) $\mathcal{A}\{\tau\}$-module, where for $x = \sum_{i=0}^m a_i\tau^i \in \mathcal{A}\{\tau\}$ and $z \in \mathcal{A}$ we define

$$xz = \sum_{i=0}^{m} a_i z^{p^i}.$$

(So the elements of $\mathcal{A} \subseteq \mathcal{A}\{\tau\}$ act by left multiplication, and τ acts as the Frobenius map.)

A *Drinfeld module* is simply an $\mathbb{F}_p$-algebra morphism $\varphi : \mathcal{A} \to \mathcal{A}\{\tau\}$, with the property that $\varphi(T)$ is a polynomial in τ of degree at least 1 whose constant term is T.

Let d be an integer such that $d > 1$, and let $f(T) \in \mathcal{A}$ be an irreducible polynomial of degree d. We write $\mathcal{B}$ for the quotient $\mathcal{A}/(f(T))$ of $\mathcal{A}$ by the principal ideal generated by $f(T)$, so $\mathcal{B} \cong \mathbb{F}_{p^d}$. For $z \in \mathcal{A}$, we write $\overline{z}$ for the corresponding element $z + (f(T)) \in \mathcal{B}$. The ideal $(f(T))$ is an $\mathcal{A}\{\tau\}$-submodule of $\mathcal{A}$, and so the quotient $\mathcal{B} = \mathcal{A}/(f(T))$ may be regarded as an $\mathcal{A}\{\tau\}$-module in a natural way by defining

$$x\overline{z} = \overline{xz}$$

for any $\overline{z} \in \mathcal{B}$. When $x = \sum_{i=0}^m a_i\tau^i \in \mathcal{A}\{\tau\}$, we have that

$$x\overline{z} = \overline{\sum_{i=0}^{m} a_i z^{p^i}} = \sum_{i=0}^{m} \overline{a_i}\,\overline{z}^{p^i},$$

and so the map from $\mathcal{B}$ to itself defined by $\overline{z} \mapsto x\overline{z}$ is $\mathbb{F}_p$-linear. For $i \in \{1, 2, \ldots, d\}$, define $b_i \in \mathcal{B}$ by $b_i = \sum_{j \equiv i \bmod d} \overline{a_j}$. Since the Frobenius map F on $\mathcal{B}$ has order d, the map $\overline{z} \mapsto x\overline{z}$ is of the form (2).

Let $\varphi : \mathcal{A} \to \mathcal{A}\{\tau\}$ be a Drinfeld module, and let $a \in \mathcal{A}$. Define $x \in \mathcal{A}\{\tau\}$ by $x = \varphi(a)$. We write $\overline{\varphi_a}$ for the map from $\mathcal{B}$ to itself given by $\overline{z} \mapsto x\overline{z}$ discussed above. Note that for any Drinfeld module φ and any $a \in \mathcal{A}$ we have that $\overline{\varphi_a}$ is of the form (2). The mappings λ_1 and λ_2 in the GLPR encryption function are defined by setting $\lambda_1 = \overline{\varphi_{c_1}}$ and $\lambda_2 = \overline{\varphi_{c_2}}$ where $c_1, c_2 \in \mathcal{A}$ are secret, and are chosen so that λ_1 and λ_2 are bijective. So λ_1 and λ_2 are of the form (2), as required.

4 An attack on the scheme

We show how to recover the private key from the public key. The first step of the attack is to guess e. The original paper suggests either $e = 5$ or $e = 7$, and in any case e must be small, so we can simply run the attack on each possible value of e in turn.

Now, using the public key we can generate many pairs

$$(z, w) \text{ where } w = \psi(z) \tag{3}$$

for random values of $z \in \mathbb{F}_{p^d}$. We will need a large number of these pairs.

The main point of the attack is to recover the two linear maps λ_1^{-1} and λ_2. This is done by expressing the coefficients of the transformations as variables, generating sufficiently many equations, and then solving these equations over a finite field. A generic attack would be to represent λ_1^{-1} and λ_2 as matrices over $\mathbb{F}_p$, each having d^2 variables, and to solve the equations over $\mathbb{F}_p$. Since ψ is a bijection it follows that λ_1 is invertible. It is also clear that λ_1^{-1} can be written in the form of equation (2).

Instead, we will use d unknowns in $\mathbb{F}_{p^d}$. Write

$$\lambda_1^{-1} = x_0 + x_1 F + \cdots x_{d-1} F^{d-1} \tag{4}$$

$$\lambda_2 = y_0 + y_1 F + \cdots y_{d-1} F^{d-1} \tag{5}$$

where the x_i and y_j are treated as unknowns in $\mathbb{F}_{p^d}$. To be precise, for any given element $z \in \mathbb{F}_{p^d}$, the value of $\lambda_2(z)$ is the linear equation

$$\lambda_2(z) = y_0 + y_1 z^p + y_2 z^{p^2} + \cdots + y_{d-1} z^{p^{d-1}}$$

and similarly for $\lambda_1^{-1}(w)$. We also introduce a variable δ, which will replace the private value of δ. Now, each pair (z, w) gives rise to a relation

$$\lambda_1^{-1}(w) = \lambda_2(z)^e + \delta. \tag{6}$$

Since z and w are exact field elements, each of these relations gives rise to a large multivariate polynomial relation in the $2d + 1$ variables x_i, y_j and δ. Note that these polynomials are linear in the x_i and δ but of degree e in the y_j.

So we have obtained a number of degree e multivariate polynomial relations between the $2d+1$ variables. It remains to find an $\mathbb{F}_{p^d}$-solution to this polynomial system. It is probably possible to apply Gröbner basis techniques, but we suggest using the linearisation methods (see, for example, [2, 4]) and which have proved to be effective against multivariate schemes. The key to these methods is to replace each non-linear monomial $\prod_j y_j^{e_j}$ by a new term u_k and thus obtain a linear equation in a larger number of variables. In this case the number of monomials is less than d^e (typically $5^5 = 3125$).

As mentioned above, we know there is not a unique solution to the system, but once the system is sufficiently reduced it will be easy to select a solution. If enough independent linear equations can be generated then the system can easily be solved in practice. We do not expect there to be any difficulties to the above construction producing sufficiently many independent equations.

Finally, once one obtains λ_1^{-1} and λ_2 it is trivial to recover λ_1 and the private key is completely known to the adversary.

References

1. R. Gillard, F. Leprevost, A. Panchishkin and X.-F. Roblot, Utilisation des modules de Drinfeld an cryptologie, *C. R. Acad. Sci. Paris, Ser. I* 336 (2003), 879-882.
2. A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in M. Wiener (ed.) CRYPTO 1999, Springer LNCS 1666 (1999) 19–30.
3. T. Scanlon, Public key cryptosystems based on Drinfeld modules are insecure, *J. Cryptology* 14 (2001), 225-230.
4. A. Shamir, J. Patarin, N. Courtois and A. Klimov, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, Eurocrypt 2000, Springer LNCS 1807 (2000), 392–407.