Public Key Cryptography Based on Simple Modules over Simple Rings [*]

Gérard Maze Chris Monico Joachim Rosenthal
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556, USA

Joan-Josep Climent
Departament de Ciència de la Computació
i Intelligència Artificial
Universitat d'Alacant
Campus de Sant Vicent
E-03071 Alacant, SPAIN

June 26, 2002

Abstract

The Diffie Hellman key exchange and the ElGamal oneway trapdoor function are the basic ingredients of public key cryptography. Both these protocols are based on the hardness of the discrete logarithm problem in a finite ring. In this paper we show how the action of a ring on a module gives rise to a generalized Diffie-Hellman and ElGamal protocol. This leads naturally to a cryptographic protocol whose difficulty is based on the hardness of a particular control problem, namely the problem of steering the state of some dynamical system from an initial vector to some final location.

1 Introduction

The discrete logarithm problem is the basic ingredient of many cryptographic protocols. It asks the following question:

Problem 1.1. *Let G be a fixed group and let $g, h \in G$ be arbitrary elements. Find an integer $n \in \mathbb{N}$ such that $g^n = h$.*

Problem 1.1 has a solution if and only if $h \in \langle g \rangle$, the cyclic group generated by g. If $h \in \langle g \rangle$ then there is a unique integer n satisfying $1 \leq n \leq ord(g)$ such that $g^n = h$. We call this unique integer the discrete logarithm of h with base g and we denote it by $\log_g h$.

[*] The authors were supported in part by NSF grant DMS-00-72383. The second author was also supported by a fellowship from the Center of Applied Mathematics at the University of Notre Dame.

The Diffie-Hellman protocol [4] allows two parties, say Alice and Bob, to exchange a secret key over some insecure channel. In order to achieve this goal Alice and Bob agree on a group G and a common base $g \in G$. Alice chooses a random integer $a \in \mathbb{N}$ and Bob chooses a random integer $b \in \mathbb{N}$. Alice transmits to Bob g^a and Bob transmits to Alice g^b. Their common secret key is $k := g^{ab}$.

The ElGamal public key cryptosystem [5] works in the following way: Alice chooses $n \in \mathbb{N}$, $h, g \in G$, where $h = g^n$. The private key of Alice consists of (g, h, n), the public key consists of (g, h). Bob chooses a random integer $r \in \mathbb{N}$ and with this he applies the encryption function

$$\begin{array}{cccc} \varepsilon : & G & \longrightarrow & G \times G \\ & m & \longrightarrow & (c_1, c_2) := (g^r, mh^r) \end{array}$$

Alice, who knows $n = \log_g h$ readily computes m from the ciphertext (c_1, c_2): $m = c_2(c_1{}^n)^{-1}$. In order for the protocol to work it is required that multiplication and inversion inside the group G can be efficiently done and it should be computationally infeasible to compute a discrete logarithm with base $g \in G$.

In the literature many groups have been proposed as candidates for studying the discrete logarithm problem. Groups which have been implemented in practice are the multiplicative group $(\mathbb{Z}_n)^*$ of integers modulo n, the multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ of nonzero elements inside a finite field $\mathbb{F}$ and subgroups of these groups. In recent time there has been intense study of the discrete logarithm problem in the group over an elliptic curve [2, 7, 10]. In [3, 12] the discrete logarithm problem in finite matrix rings have been studied and it has been shown that this necessitates good examples of finite simple semirings.

In [8, 9] we have shown how the discrete logarithm problem over a group can be seen as a special instance of an action by a semigroup. The interesting thing is that every group action by an abelian semigroup gives rise to a Diffie-Hellman key exchange. With an additional assumption it is also possible to extend the ElGamal protocol. In the next section we explain the results of [8, 9] in more detail.

In Section 3 we show how to build semigroup actions from actions by semirings on semimodules. In Subsection 3.3 we describe an interesting semigroup action which in our opinion holds a lot of promise for implementation as a practical system.

2 The generalized Diffie-Hellman and ElGamal protocols in the context of group actions

Consider a semigroup G, i.e. a set that comes with an associative multiplication '$\cdot$'. In particular we do not require that G has either an identity element or that each element has an inverse. We say that the semigroup is abelian if the multiplication $\cdot$ is commutative.

Let S be a finite set and consider an action of G on S:

$$\begin{array}{cccc} \varphi : & G \times S & \longrightarrow & S \\ & (g, s) & \longmapsto & gs \end{array}$$

We will refer to this action as a G-action on the set S. By the definition of a group action we require that $(g \cdot h)s = g(hs)$ for all $g, h \in G$ and $s \in S$. We also assume throughout that arithmetic in G and computation of the G-action can be done in polynomial time.

If the semigroup G is abelian then every G-action gives rise to a generalized Diffie-Hellman Key Exchange:

Protocol 2.1. (Extended Diffie-Hellman Key Exchange) Let S be a finite set, G an abelian semigroup and an action of G on S as defined above. The Extended Diffie-Hellman key exchange is the following protocol:

1. Alice and Bob agree on an element $s \in S$.

2. Alice chooses $a \in G$ and computes as. Alice's secret key is a, her public key is as.

3. Bob chooses $b \in G$ and computes bs. Bob's secret key is b, his public key is bs.

4. Their common secret key is then $a(bs) = (a \cdot b)s = (b \cdot a)s = b(as)$

As in the situation of the discrete logarithm problem it is possible to construct an ElGamal one-way trapdoor function which is based on group actions: assume that the set S has in addition some group structure with respect to some binary operation $\circ$. We would like to stress that the group structure of S is unrelated with the binary operation on the semigroup G.

Protocol 2.2. (Extended ElGamal Public Key System) If S is a group with respect to some operation $\circ$, then the Extended ElGamal public key system is the following protocol:

1. Alice's public key is (s, as).

2. Bob chooses a random element $b \in G$ and encrypts a message m using the encryption function

$$(m, b) \longmapsto (bs, (b(as)) \circ m) = (c_1, c_2).$$

3. Alice can decrypt the message using $m = (b(as))^{-1} \circ c_2 = (ac_1)^{-1} \circ c_2$.

One would build a cryptosystem on such a G-action only if the following problem is hard:

Problem 2.1. *Semigroup action problem (SAP): Let G be an abelian semigroup acting on a set S. Given $x, y \in S$ find $g \in G$ such that $gx = y$.*

For if an attacker, Eve, can find an $\alpha \in G$ such that $\alpha s = as$, then Eve may find the shared secret by computing $\alpha(bs) = (\alpha \cdot b)s = b(\alpha s) = b(as)$. Although the semigroup G need not be finite, the finiteness of S is sufficient in order to provide a bound for the size of the data during the communication. Nevertheless, if the action preserves the "size" of s with respect to some fixed representation, finiteness of S is not necessary. The traditional Diffie-Hellman key exchange and ElGamal protocol are special instances of Protocol 2.1 and Protocol 2.2. Note that in the special case where G is actually a group, the SAP can be solved in a straightforward way with $O(\sqrt{|\mathcal{O}_x|})$ operations, where $\mathcal{O}_x$ is the orbit of x. At present, we do not know of any such algorithm for the general SAP, though prudence suggests we assume that one exists.

3 Semirings acting on semimodules

In this section we show a way on how to construct semigroup actions on finite sets in a practical algebraic way. The trapdoor function we obtain will rely on a finite version of a difficult control problem, namely the problem of steering the state of some dynamical system from an initial vector to some final location. The setup is general enough that it includes the Diffie-Hellmann protocol over a general finite group as a special case. It provides on the other hand the flexibility to construct new protocols where some of the known attacks against the discrete logarithm problem in a finite group do not work anymore.

Let R be an additively commutative semiring, not necessarily finite. This means that R is a semigroup with respect to both addition and multiplication and the distributive laws hold. It is understood that the semiring is commutative with respect to addition but not necessrily with respect of multiplication. Some authors assume that a semiring has a neutral element with respect to addition. We will not assume that R has either a zero or a one.

Let M be a finite semimodule over R. With this we mean that M has the structure of a finite semigroup and there is an action $R \times M \longrightarrow M$ such that

$$r(sm) = (rs)m, \;\; (r+s)m = rm + sm \text{ and } r(m+n) = rm + rn$$

for all $r, s \in R$ and $m, n \in M$.

Let $Mat_{n\times n}(R)$ be the set of all $n \times n$ matrices with entries in R. The semiring structure on R induces a semiring structure on $Mat_{n\times n}(R)$. Moreover the semimodule structure on M lifts to a semimodule structure on M^n via the matrix multiplication:

$$\begin{array}{rcl} Mat_{n\times n}(R) \times M^n & \longrightarrow & M^n \\ (A, x) & \longmapsto & Ax. \end{array} \tag{3.1}$$

The action 3.1 forms a group-action of the multiplicative group of $Mat_{n\times n}(R)$ on the set M^n. In general $Mat_{n\times n}(R)$ is not commutative with respect to matrix multiplication. However we can easily define a commutative subgroup as follows:

Let $C \subset R$ be the center of R. This is the subset of elements which commutes with respect of multiplication with every element of R. Let $C[t]$ be the polynomial ring in the indeterminant t and let $A \in Mat_{n\times n}(R)$ be a fixed matrix. If

$$p(t) = r_0 + r_1 t + \cdots + r_k t^k \in C[t]$$

then we define in the usual way $p(A) = r_0 I_n + r_1 A + \cdots + r_k A^k$, where $r_0 I_n$ is the $n \times n$ diagonal matrix with entry r_0 in each diagonal element.

Consider the semigroup

$$G := C[A] := \{p(A) \mid p(t) \in C[t], A \in Mat_{n\times n}(R)\}.$$

Clearly $C[A]$ has the structure of an abelian semigroup. Protocol 2.1 then simply requires that Alice and Bob agree on a vector $s \in M^n$. Then Alice chooses a matrix $X \in \; C[A]$ and sends to Bob the vector Xs, an element of the module M^n. Bob chooses a matrix $Y \in C[A]$ and sends to Alice the vector Ys. The common key is then the vector XYs which both can compute since X and Y commute.

3.1 Systems Theoretic Interpretation

It is possible to give the key exchange a systems theoretic interpretation. For this note that in order to choose $X \in C[A]$ Alice has to choose $r_0, \ldots, r_k \in C$ and with this she can compute

$$Xs = (r_0 I_n + r_1 A + \cdots + r_k A^k)s = r_0 s + r_1 As + \cdots + r_k A^k s.$$

Consider now the linear time invariant system:

$$x_{t+1} = Ax_t + u_t s, \ \ s, x_t \in M^n, u_t \in R. \tag{3.2}$$

Assume further that $x_0 = 0$. (If M has no zero we can simply assume that the system is initialized through $x_1 = u_0 s, \ x_{t+1} = Ax_t + u_t s$ for $t \geq 1$.) If Alice chooses the input sequence $u_0 = r_k$, $u_1 = r_{k-1} \ldots, u_k = r_0$ then x_{k+1}, the state vector at time $k+1$ is exactly Xs, the public vector to be computed by Alice.

Once Alice receives from Bob his public key Ys, then she defines $b := Ys$ and by choosing her input sequence $u_0, \ldots, u_k$ in the system

$$x_{t+1} = Ax_t + u_t b, \tag{3.3}$$

she will be able to compute the common secret key XYs.

Eve who wants to find an element $\tilde{X} \in C[A]$ such that $\tilde{X}s = Xs$ faces the task of finding a control sequence $u_0, \ldots, u_\kappa$ which steers the initial state vector x_0 into the state vector Xs. This problem is in general very hard and we will see that it contains some of the hardest known discrete logarithm problems as a special case. In the special case when $R = M = \mathbb{F}$, a finite field then the problem is however simply solved by methods of linear algebra. Indeed in the field case the Cayley Hamilton theorem implies that

$$\mathbb{F}[A] = \{p(A) \mid p(t) \in \mathbb{F}[t] \text{ and } \deg p \leq n-1\}.$$

Eve therefore knows that the vector Xs is in the column space of $\left[s, As, \ldots, A^{n-1}s\right]$ and she simply has to solve the system of linear equations:

$$Xs = \left[s, As, \ldots, A^{n-1}s\right] \begin{bmatrix} r_0 \\ \vdots \\ r_{n-1} \end{bmatrix}. \tag{3.4}$$

The system has always a solution and Eve finds a matrix $\tilde{X} \in \mathbb{F}[A]$ with $\tilde{X}s = Xs$. But this is enough to compute the common key $XYs = YXs = Y\tilde{X}s = \tilde{X}Ys$ as explained in Section 2.

In the Section 3.3 we show that this simple linear algebra procedure breaks down if we deal with more general rings and modules:

3.2 Some considerations

At present, we lack a convincing example of a system based on the previous sections. All of the examples presently known to the authors have proved to be either insecure or already well-known. The insecure examples have arisen by generating random finite semirings for base-objects. However, if the base-objects are not simple they admit smaller homomorphic images which can often be used to reduce the problem with a Pohlig-Hellman type algorithm. One may wish to explicitly allow the security of the system to rest on the difficulty of finding such homomorphisms (via congruence relations), but we would certainly prefer not to.

Finite simple commutative semirings have been classified in [1] and none lead to a new secure system. Such semirings without the assumption of commutative multiplication have been 'almost' classified in [11], and again seem to yield nothing interesting for our purposes.

Finally, there are some strong results in [6] on simple semimodules over commutative semirings that might suggest using semimodules over non-commutative (i.e., with commutative addition only) semirings. More work is needed to determine if there exists such objects that will suit our needs.

3.3 A matrix action on abelian groups

In this subsection take as a ring $R = \mathbb{Z}$, the integers and as a module any finite abelian group $M = H$. The group H is a $\mathbb{Z}$ module and $Mat_{n\times n}(\mathbb{Z})$ operates on $S := H^n = H \times \ldots \times H$ via the formal multiplication:

$$\begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} \longmapsto \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix}. \tag{3.5}$$

If $l = \operatorname{lcm}\{|g_1|, \ldots, |g_n|\}$, and $C \in Mat_{n\times n}(\mathbb{Z})$ is a matrix with all entries congruent to zero modulo l, then $(A + C)g = Ag$ for all $A \in Mat_{n\times n}(\mathbb{Z})$. Whence, we may simply consider the action of $Mat_{n\times n}(\mathbb{Z}_l)$ on S.

Remark 3.1. *If one writes the group operation in a multiplicative way then the jth component in H^n is given as $(A \cdot g)_j = \prod_{i=1}^{n} g_i^{a_{ji}}$. If $n = 1$ then the action reduces to the action $g \longmapsto g^a$, i.e. we deal with the usual discrete logarithm problem in the cyclic subgroup of H generated by the element $g = g_1$. In particular when $n = 1$ Protocols 2.1 and 2.2 reduce to the usual Diffie-Hellman and ElGamal protocol. If $n > 1$ we do not know however if a reduction of the general case to a small number of discrete logarithm problems can be achieved with reasonable complexity.*

As before, since $Mat_{n\times n}(\mathbb{Z}_l)$ is not commutative and based on the Cayley Hamilton theorem we will restrict ourself to the abelian sub-semigroup $\mathbb{Z}_l[A]$ consisting of all sums of the form $\sum_{i=0}^{n-1} a_i A^i$.

The question now arises of how one can attack this system.

The problem: Given $g, Ag \in H^n$, find $\tilde{X} \in \mathbb{Z}_l[A]$ with $\tilde{X}g = Xg$ is the instance of Problem 2.1 that this system presents. We therefore could try to see if there is once more a linear system of equation which can solve similar to the situation when $R = M = \mathbb{F}$ a finite field.

For this assume once more that $X = \sum_{i=0}^{n-1} a_i A^i$. Again we have a system of linear equations, as in equation (1):

$$\begin{bmatrix} h_1 \\ \vdots \\ h_n \end{bmatrix} := Xg = \left[g, Ag, \ldots, A^{n-1}g\right] \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix}. \tag{3.6}$$

In this system of equations the unknowns are $a_0, \ldots, a_{n-1} \in \mathbb{Z}_l$. The coefficient matrix $\left[g, Ag, \ldots, A^{n-1}g\right]$ as well as the entries h_i of the vector Xg are elements of the abelian group.

The question now arises if there is a chance to reduce this system of equations to solving a discrete logarithm problem in a finite group. There are two special case attacks that must be avoided:

Lemma 3.1. *Let $A \in Mat_{n\times n}(\mathbb{Z}_l)$ and $g, h \in H^n$ and suppose that $X \in \mathbb{Z}_l[A]$ is unknown. If one can construct, in polynomial time, an invertible matrix $S \in Mat_{n\times n}(\mathbb{Z}_l)$ such that SAS^{-1} is diagonal then solving the equation $Xg = h$ polynomial time reduces to solving n discrete logarithm problems.*

We would like to stress that a diagonalization of A over some extension ring $\mathbb{Z}_l[\zeta] \supset \mathbb{Z}_l$ will help little. Indeed it is not clear how one should interpret the multiplication of an element in H with an element in $\mathbb{Z}_l[\zeta]$ in general. The above reduction is therefore easily avoided if one chooses a matrix A whose characteristic polynomial does not factor over $\mathbb{Z}_l$. There is another situation where one can show that the problem reduces to a discrete logarithm problem in a cyclic group. This can happen when all elements g_i are elements of a cyclic group:

Lemma 3.2. *If there exists $\gamma \in H$ with $g_i \in \langle\gamma\rangle$ for all i then solving the equation $Xg = h$ polynomial time reduces to solving $2n$ discrete logarithm problems.*

Having described the special cases to be avoided, we should also remark that if we define $l = \operatorname{lcm}\{|g_1|, \ldots, |g_n|\}$, there exists an obvious Pollard-Rho type birthday attack to solve the problem with $\mathcal{O}(l^{\frac{n+1}{2}})$ operations. Furthermore, if $l = p_1^{e_1} \cdots p_m^{e_m}$, there is an obvious Pollig-Hellman type reduction of the problem to m problems with $l_1 = p_1^{e_1}, \ldots, l_m = p_m^{e_m}$. Thus, if p^e is the largest prime power dividing l, the problem can be solved with $\mathcal{O}(p^{\frac{en+n}{2}})$ operations.

Thus, to maximize the difficulty of the problem to be solved relative to the input size, one should choose the g_i so that $l = \operatorname{lcm}\{|g_1|, \ldots, |g_n|\} = p^k$ for some prime p.

4 Conclusion

In this article we showed how the discrete logarithm problem over a finite group can be viewed as an instance of an action by a semigroup. It was shown how the well known Diffie-Hellman key exchange and the ElGamal protocol do generalize to this framework. Some examples of actions by semigroups have been given and it was shown that there are some situations that should be avoided. It remains to find concrete instances of such actions that have high (believed) security relative to their key sizes.

References

[1] R. El Bashir, J. Hurt, A. Jančařék, and T. Kepka. Simple commutative semirings. *Journal of Algebra*, 236:277–306, 2001.

[2] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* Lecture Note Series 265. London Mathematical Society, 1999.

[3] J. J. Climent, C. Monico, and J. Rosenthal. The DLP in finite semirings. In preparation.

[4] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6):644–654, 1976.

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[6] J. Ježek and T. Kepka Simple semimodules over commutative semirings.. *Acta Sci. Math. (Szeged)*, 46:17–27, 1983.

[7] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[8] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on group actions. Preprint, October 2001.

[9] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on actions by semigroups. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 484, Lausanne, Switzerland, 2002.

[10] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, pages 417–426. Springer, Berlin, 1986.

[11] C. Monico. On finite congruence-simple semirings. E-print math.RA/0205083, May 2002.

[12] C. Monico. *Semirings and Semigroup Actions in Public-Key Cryptography.* PhD thesis, University of Notre Dame, May 2002. Available at http://www.nd.edu/˜rosen/preprints.html.