A Public Key Cryptosystem Based on Actions by Semigroups

Gérard Maze, Chris Monico, and Joachim Rosenthal
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana, 46556, USA
{gmaze, cmonico, Rosenthal.1}@nd.edu

I. Introduction

A generalization of the original Diffie-Hellman key exchange in $\mathbb{F}_p^*$ found a new depth when Miller [4] and Koblitz [2] suggested that such a protocol could be used with the group over an elliptic curve. In the present article, we extend such a generalization to the setting of a semigroup action (G-action) on a finite set. We define this extended protocol, show how it is related to the general Diffie-Hellman key exchange and give some examples. The interesting thing is that every 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 this in detail.

II. Diffie-Hellman protocol 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:

$$\begin{array}{rcl} G \times S & \longrightarrow & S \\ (g, s) & \longmapsto & gs. \end{array}$$

By the definition of a group action we require that $(g \cdot h)s = g(hs)$ for all $g, h \in G$ and $s \in S$.

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

Protocol 1 (Extended Diffie-Hellman key exchange) Let S be a finite set and G an abelian semigroup acting on S. 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 private key is a, her public key is as.
3. Bob chooses $b \in G$ and computes bs. Bob's private 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 exponentiation in cyclic groups, it is possible to construct an ElGamal one-way trapdoor function which is based on semigroup actions if one assumes that the set S has a group structure. See [3] for details.

[1]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.

III. A matrix action on abelian groups

In this example consider an abelian group H. The group H is a $\mathbb{Z}$ module and $(Mat_{n\times n}(\mathbb{Z}), \cdot)$ acts on $S := H^n = H \times \ldots \times H$ via the formal multiplication:

$$(A \cdot g)_i = \prod_{j=1}^{n} g_j^{a_{ij}}, \text{ with } (A)_{ij} = a_{ij} \in \mathbb{Z}.$$

The semigroup operation in $Mat_{n\times n}(R)$ is not commutative, but we can easily define a commutative subsemigroup as follows:

Fix a matrix $A \in Mat_{n\times n}(\mathbb{Z})$ and define

$$G := R[A] := \{p(A) \mid p(t) \in R[t]\}.$$

With respect to matrix multiplication G has the structure of an abelian semigroup. The protocol then simply requires that Alice and Bob agree on a vector $s \in H^n$. Then Alice chooses a matrix $X \in Z[A]$ and sends to Bob the vector Xs, an element of the module H^n. Bob chooses a matrix $Y \in Z[A]$ and sends to Alice the vector Ys. The common key is then the vector XYs which both can compute since X and Y commute.

IV. An Action from the endomorphism ring of an abelian group

Let H be an abelian group, and $\operatorname{End} H$ the ring of endomorphisms of H. Consider the natural action of $\operatorname{End} H$ on H. For a given $\varphi \in \operatorname{End} H$, the subring $\mathbb{Z}[\varphi]$ is commutative and yields to a Diffie-Hellman protocol. Note that in the case of a cyclic group or when $\varphi = Id_H$, we are dealing with the traditional Diffie-Hellman protocol. A concrete example is the case of an elliptic curve E over a finite field $\mathbb{F}_p$. If this curve is ordinary with complex multiplication, then the action of the Frobenius endomorphism φ on $E(\mathbb{F}_{p^2})$ gives rise to a new situation that extends the usual DLP over such a group [1]. Details about this group action will be provided in [3].

References

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

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

[3] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on group actions. In preparation.

[4] 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.