A Public Key Cryptosystem based on Actions by Semi-Groups

Gérard Maze, Chris Monico, and Joachim Rosenthal
Deptartment 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 $\mathbb{Z}_p^*$ found a new depth when Miller [3] 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 semi-group 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 group action by an abelian semi-group 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 semi-group 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 semi-group is abelian if the multiplication $\cdot$ is commutative.

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

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

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

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

Protocol II.1 (Extended Diffie-Hellman Key Exchange) Let S be a finite set, G an abelian semi-group 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 $a(bs) = (a \cdot b)s = (b \cdot a)s = b(as)$

[1]This work was 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.

As in the situation of exponentiation in cyclic groups, it is possible to construct an ElGamal one-way trapdoor function which is based on group actions if one assumes that the set S has in addition some group structure.

III. A matrix action on abelian groups

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

$$(A \cdot g)_j = \prod_{i=1}^{n} g_i^{a_{ji}}, \quad \text{with } (A)_{ij} = a_{ij} \in \mathbb{Z}$$

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

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

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

Clearly G has the structure of an abelian semi-group. 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 ellitpic 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 extend the usual DLP over such a group [1].

References

[1] I. Blake, G. Seroussi and N. Smart. Elliptic curve in cryptography. London Math. Soc., Lecture Notes Series 265. Cambridge University Press 2000.

[2] N Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48,203-209, 1987.

[3] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology, CRYPTO 85*, 417-426, Springer-Verlag, 1986.