Cryptographic Group and Semigroup Actions

Oliver W. Gnilke[1] and Jens Zumbrägel[2]

[1] Deparment of Mathematical Sciences
Aalborg University, Denmark
owg@math.aau.dk
[2] Faculty of Computer Science and Mathematics
University of Passau, Germany
jens.zumbraegel@uni-passau.de

Abstract. We consider actions of a group or a semigroup on a set, which generalise the setup of discrete logarithm based cryptosystems. Such cryptographic group actions have gained increasing attention recently in the context of isogeny-based cryptography. We introduce generic algorithms for the semigroup action problem and discuss lower and upper bounds. Also, we investigate Pohlig-Hellman type attacks in a general sense. In particular, we consider reductions provided by non-invertible elements in a semigroup, and we deal with subgroups in the case of group actions.

Keywords: Discrete logarithm problem, cryptographic group action, semigroup action problem

1 Introduction

The discrete logarithm problem has a long and profound history (see [GJ21] for a recent survey). In cryptography it has been playing a key role ever since Diffie and Hellman have based the security of their famous protocol [DH76] on the hardness of computing discrete logarithms modulo a large prime p. The underlying group $\mathbb{F}_p^*$ has then been generalized, most notably to the $\mathbb{F}_q$-rational points on an elliptic curve, due to Miller [Mil86] and Koblitz [Kob87]. In fact, while the discrete logarithm problem in the unit group $\mathbb{F}_q^*$ of a finite field can be solved in subexponential time by index calculus algorithms (for an overview, see [GKZ18]), the fastest known algorithm in a general elliptic curve is basically a generic one that requires exponential time.

However, Shor's quantum algorithm [Sho97] constitutes a polynomial time attack on the discrete logarithm problem in any group (as well as on the integer factorisation problem). These observations, and reports on the progress in building quantum computers now achieving a "quantum supremacy" [Aru+19], underline the need for new concepts to build cryptosystems resistant to quantum attacks. One of the most interesting approaches is based on isogenies of supersingular elliptic curves (SIDH, [DJP14]), leading to the candidate SIKE in the NIST post-quantum standardisation competition [Ala+20].

More recently, a commutative supersingular isogeny-based Diffie-Hellman scheme (CSIDH, [Cas+18]) has been proposed as a more efficient variant, which is based on the action of the class group of an endomorphism ring on isomorphism classes of elliptic curves. This is an example for an action of an abelian group on a set, which as a framework suffices to build a Diffie-Hellman protocol, as has been observed by Couveignes [Cou06] and independently by Rostovtsev and Stolbunov [RS06,Sto10].

With a somewhat different background, Maze, Monico and Rosenthal have introduced actions of commutative semigroups on sets [Mon02,MMR07] in order to generalise the discrete logarithm problem, one motivation being to find examples that do not allow even an (exponential) square-root attack. The setup was further investigated by the theses of the present authors, in which Zumbrägel [Zum08] considered a generalisation to non-commutative semigroups and Gnilke [Gni14] showed how a Pohlig-Hellman like reduction applies to semigroups with non-invertible elements, thus leaving group actions as a main object of study.

In this work, we revisit the concept of semigroup actions for discrete logarithm based cryptosystems and connect it to recent proposals of isogeny-based cryptography. In the case of abelian group actions, with a view towards isogenies, this has been considered by Couveignes [Cou06] and, more recently, by Smith [Smi18] and Alamati et al [ADMP20]. Here we aim to take a slightly more abstract viewpoint and introduce generic algorithms for the semigroup action problem. We also investigate Pohlig-Hellman type reductions and consider those provided by non-invertible elements in a semigroup and by subgroups in the context of a group action.

2 Cryptographic semigroup actions

In this section we briefly recall the notion of a semigroup action and its application to cryptography [Mon02,MMR07].

By a *semigroup* we mean a set S with an associative binary operation (written multiplicatively). A *semigroup action* with respect to a semigroup S and a set X is given by a map

$$S \times X \to X\,, \quad (s,x) \mapsto s.x$$

such that $st.x = s.(t.x)$ for all $s,t \in S$ and $x \in X$. Considering for $s \in S$ the transformation $\Phi_s \colon X \to X$, $x \mapsto s.x$, this means that $\Phi_{st} = \Phi_s \circ \Phi_t$ for $s,t \in S$. When there is such a semigroup action, then X is also called *S-set*.

Definition 1. *Consider a semigroup S acting on a set X. The* semigroup action problem *is the problem, for given $x, y \in X$ to find some $s \in S$ such that $y = s.x$.*

So the semigroup action problem asks to find preimages of the "orbit map"

$$\Psi_x \colon S \to X\,, \quad s \mapsto s.x\,.$$

Suppose that S is a group and let $S_x = \{s \in S \mid s.x = x\}$ be the *stabiliser subgroup* of $x \in X$. Then the orbit map induces a bijection $S/_\ell S_x \xrightarrow{\sim} S.x$ of the

left cosets and the orbit. Thus solutions to the semigroup action problem in a group are unique up to left congruence modulo the stabiliser.

Since we deal with cryptographic applications, we assume all structures to be finite and that the semigroup action is efficiently computable. This means that elements of the semigroup S and the set X are encoded by bit strings, and both the semigroup operation and the action are computable in polynomial time.

Example 2. Consider a finite cyclic group $(G, \cdot)$ of order n, which may be seen as a $\mathbb{Z}_n$-module. If we "forget" its additive structure, we have the action

$$(\mathbb{Z}_n, \cdot) \times G \to G\,, \quad (s, g) \mapsto g^s\,,$$

and the semigroup action problem is just the discrete logarithm problem in the group G. Note that the action is efficiently computable by a square-and-multiply method, provided the group operation is efficient.

In order to set up a Diffie-Hellman like key agreement, we need some way to generate commuting elements of the semigroup S. For simplicity we assume then that the semigroup is commutative, in which case we have to following key agreement scheme:

Alice		*public*		Bob
		$x \in X$		
$a \in S$	$\to$	$a.x \in X$		
		$b.x \in X$	$\leftarrow$	$b \in S$
$k_A = a.(b.x)$				$k_B = b.(a.x)$

Observe that both parties compute the same key $ab.x = ba.x$. Also notice that in the case of Example 2 the scheme amounts to classical Diffie-Hellman.

Definition 3. *Consider a commutative semigroup S acting on a set X. The* semigroup Diffie-Hellman problem *is the problem, for given $x, y, z \in X$ to find some $k \in X$ such that $y = a.x$, $z = b.x$ and $k = ab.x = ba.x$ for some $a, b \in S$.*

It is clear that if one can solve the semigroup action problem, then one can break the Diffie-Hellman protocol, while the converse direction is not obvious. There have been results on subexponential reductions in the classical case of group exponentiation [Mau94,MW99], and recently on polynomial quantum reduction for abelian group actions [GPSV21].

Example 4. In isogeny-based cryptography and CSIDH, a particular case of interest is the action of an abelian group on a set X (cf. [Cou06,Cas+18,Smi18]). In Couveignes' work the group action is also assumed to be simply transitive, and the semigroup action problem and the semigroup Diffie-Hellman problem are called *vectorisation problem* and *parallelisation problem*, respectively; if those are intractable, the set X is referred to as a *hard homogeneous space*.

It would be interesting to view SIDH also in the framework of a group action, but this seems not to be obvious, cf. [Smi18, Sec. 15].

3 Generic algorithms

We use Maurer's abstract model of computation [Mau05] to describe generic algorithms for a semigroup action. Recall that in this model one specifies

- a ground set X,
- a set Π of certain operations $f\colon X^t \to X$ of arity $t \in \{0, 1, 2, \dots\}$,
- a set Σ of certain relations $\rho \subseteq X^t$ of arity $t \in \{1, 2, \dots\}$.

There are internal state variables $V_1, V_2, \dots$ storing elements in X. Computation operations and queries can then be made for $f \in \Pi$ and $\rho \in \Sigma$, using the internal state variables as input (and operation output). We denote by $\mathcal{C}$ the set of all *constants*, i.e., nullary operations $X^0 \to X$.

Example 5. Generic algorithms in a cyclic group of order n can be modeled using $X = \mathbb{Z}_n$, $\Pi = \mathcal{C} \cup \{+\}$ and $\Sigma = \{=\}$, and the discrete logarithm problem can be described as the *extraction problem* to obtain the initial value $x \in V_1$.

Now let $S \times X \to X$ be a semigroup action described by transformations $\Phi_s\colon X \to X$, which we view as unary operations. In the case of group actions we then have the following result, which provides a generic lower bound of $\Omega(\sqrt{n})$ for the semigroup action problem in a set X of size n. Notice here that in light of the bijection $S/_\ell S_x \xrightarrow{\sim} S.x$ induced by the orbit map, the semigroup action problem can be modeled as an extraction problem.

Theorem 6. *Let $S \times X \to X$ be a free group action, let $\Pi = \mathcal{C} \cup \{\Phi_s \mid s \in S\}$ and $\Sigma = \{=\}$. Then the success probability of any k-step extraction algorithm is upper bounded by $\frac{1}{4}k^2/|X|$.*

Proof (sketch). Following the proof of [Mau05, Thm. 1] it suffices to upper bound the probability that a collision in the state variables occurs. These entries are either of the form $s.x$ for known $s \in S$, or chosen constants $y \in X$. Since the action is free, we have $s.x = t.x$ only if $s = t$, so the only way to provoke a collision is if $s.x$ equals some constant y. Since for a group action the maps Φ_s are permutations of X, this probability is $1/|X|$.

If the algorithm computes u constants and v values of the form $s.x$, the probability for a collision is thus at most $uv/|X|$. But since $u+v \le k$ we have $uv \le \frac{1}{4}k^2$, from which the result follows. □

In contrast, for proper semigroup actions the difficulty of the generic semigroup action problem very much depends on the structure of the semigroup, and ranges from efficient algorithms in $O(\log n)$ to lower bounds of $\Omega(n)$, see the examples below. From a cryptography perspective there are however issues with applying those actions, as discussed in the next section.

Example 7. Let S be a semigroup, X a set and $\varphi\colon S \to X$ a bijection. Then we can make X an S-set by letting

$$s.\varphi(t) = \varphi(st)$$

for $s, t \in S$. We assume this action to be efficiently computable and think of the inverse map φ^{-1} as "hidden". For example, if G is a cyclic group with a generator g of order n, we use the bijection $\varphi\colon (\mathbb{Z}_n, \cdot) \to G$, $s \mapsto g^s$. Let us look at two further cases.

1. Suppose that $(S, \cdot) = (\{1, \dots, n\}, \min)$ and we are given a semigroup action problem instance $x, y \in X$ where $y = s.x$. Let $a = \varphi^{-1}(x)$ which we suppose is known, e.g., $a = n$ if $x = \varphi(n)$. Since $y = s.x = s.\varphi(a) = \varphi(sa) = \varphi(saa) = sa.\varphi(a) = sa.x$, we may assume that $s = sa$, i.e., $s \le a$. Then for any $t \in S$, $t \le a$, there holds

$$\begin{aligned} t \le s \quad &\Leftrightarrow \quad t = ts \quad \Leftrightarrow \quad ta = tsa \quad \Leftrightarrow \quad \varphi(ta) = \varphi(tsa) \\ &\Leftrightarrow \quad t.\varphi(a) = t.(s.\varphi(a)) \quad \Leftrightarrow \quad t.x = t.y\,. \end{aligned}$$

   Hence, we can find s using binary search in $O(\log n)$.

2. On the other hand, define $(S, \cdot) = (\{0, s_1, \dots, s_m, 1\}, \wedge)$, where $\wedge$ is a semilattice operation such that

$$0 \wedge s_i = 0\,, \quad 1 \wedge s_i = s_i\,, \quad \text{and} \quad s_i \wedge s_j = 0 \text{ whenever } i \ne j\,,$$

   and let $o = \varphi(0)$ and $e = \varphi(1)$ in X. Consider a semigroup action problem instance $e, y \in X$ where $y = s.e$. As $s.e = s.\varphi(1) = \varphi(s1) = \varphi(s)$ and φ is bijective, there is a unique solution s. When using a generic algorithm we may for $t \in S$ compute $t.e = \varphi(t)$ and $t.y = t.(s.e) = ts.e = \varphi(ts)$, where a collision occurs only if $t = ts$, which if $s = s_i$ means that $t \in \{0, s_i\}$. Thus it requires $\Omega(n)$ steps to find any collision and thus information about s.
   Note that this example is not interesting for a Diffie-Hellman type key agreement, because the key $k = a.(b.e) = b.(a.e)$ will usually be o.

Regarding upper bounds, Monico [Mon02] and Maze [Maz03] both mention variants of time-memory trade-offs for special cases of the semigroup action problem. Monico describes an attack based on Brent's cyclic finding algorithm for the case of group actions, which achieves an expected running time of $O(\sqrt{n})$. Maze argues that semigroups with large subgroup can be attacked similarly by excluding all non-units first and then employing Monico's idea on the unit subgroup. An alternative attack adopting Shank's baby-step giant-step algorithm has been proposed by Gnilke [Gni14].

4 Pohlig-Hellman type reductions

Here we recollect the framework of Pohlig-Hellman type reductions from [Gni14, Sec. 4.3] and discuss a few special cases for cryptographic group actions.

Recall that the classical Pohlig-Hellman algorithm [PH78] essentially reduces the difficulty of the discrete logarithm problem in a group G of order n to that in a group of order the largest prime factor of n. The algorithm can be viewed as applying multiplication-by-m maps

$$\lambda_m\colon \mathbb{Z}_n \to \mathbb{Z}_n\,, \quad s \mapsto ms$$

in order to reduce the problem to the action of the (smaller) ideal $m\mathbb{Z}_n$. The following general concept captures this scenario and many others.

Definition 8. *Let S and T be semigroups, let X be an S-set and Y be a T-set. A* reduction (f, F, G) *consists of maps $f\colon S \to T$ and $F, G\colon X \to Y$ such that*

$$f(s).G(x) = F(s.x)$$

for all $s \in S$ and $x \in X$.

For example, in classical Pohlig-Hellman as above one has for $m \mid n$ the reduction $(\lambda_m, \Phi_m, \Phi_m)$, where $\Phi_m\colon G \to G$, $g \mapsto g^m$. Indeed, there holds $g^{ms} = (g^s)^m$ for $s \in \mathbb{Z}_n$ and $g \in G$.

Given any reduction (f, F, G), an adversary who can solve the semigroup action problem in T can restrict the search in S to preimages of the solutions in T under the map f. Indeed, given a semigroup action problem instance $x, y \in X$ where $y = s.x$, one reduces it to the instance $G(x), F(y) \in Y$ where $F(y) = f(s).G(x)$. (However, it is not clear that if $F(y) = t.G(x)$ for some $t \in T$, there always exists $s \in f^{-1}(t)$ such that $y = s.x$, and the practicality of the reduction is to be further discussed.)

We call a reduction *effective* if the maps f, F, G can be efficiently computed and there holds $1 < |T| < |S|$. The next result describes a very general class of reductions on semigroups.

Proposition 9. *Let S be a semigroup, X an S-set and $m \in S$. Then the triple $(\lambda_m, \Phi_m, \mathrm{id})$ forms a reduction. If S is a monoid, this reduction is effective iff m is a non-unit and the semigroup operation and action are efficient.*

Proof. For all $x \in X$ and $s \in S$ there holds that

$$\lambda_m(s).x = ms.x = m.(s.x) = \Phi_m(s.x)\,.$$

The reduction maps the semigroup S onto its right ideal mS, which is a proper ideal iff λ_m is not surjective. □

Given any semigroup action we may apply these reductions recursively, until we essentially arrive at semigroup ideals which are either groups or have a trivial operation. These reductions constitute a threat to the security of a cryptosystem based on proper semigroup actions.

Now we consider a second family of reductions, which also applies to group actions. Let X be an S-set. Its automorphisms are the bijective maps $\varphi\colon X \to X$ such that $\varphi(s.x) = s.\varphi(x)$ for all $s \in S$, $x \in X$. Suppose then that a group H acts on X by automorphisms, i.e., we have

$$H \times X \to X\,, \quad (h, x) \mapsto h.x$$

satisfying $h.s.x = s.h.x$ for $h \in H$, $s \in S$, $x \in X$. Let $X/\!\sim$ be the set of its orbits $[x] = \{h.x \mid h \in H\}$. Then we have an action

$$S \times X/\!\sim \to X/\!\sim\,, \quad (s, [x]) \mapsto [s.x]\,.$$

In the sense of Definition 8 we deal here with reductions where $S = T$ and where $F = G$ is a homomorphism of S-sets, in fact, $F\colon X \to X/\!\sim$, $x \mapsto [x]$ is the canonical map.

Example 10. As in Example 2 consider the discrete logarithm setup of an abelian group X of order n, i.e., we have the action of $(\mathbb{Z}_n, \cdot)$ on X by exponentiation. Every group automorphism is also an automorphism of X as an $\mathbb{Z}_n$-set, thus any subgroup H of the automorphism group of X gives rise to a "reduced" action

$$(\mathbb{Z}_n, \cdot) \times X/\!\sim \to X/\!\sim, \quad (s, [x]) \mapsto [x^s]\,.$$

In the special case of $H = \{\pm 1\}$ we have the orbits $[x] = \{x, x^{-1}\}$, reflecting the practice in elliptic curve cryptography to identify the points $\pm P$ and thus use only the x-coordinate [Mil86].

Does such a reduction weaken the security of the discrete logarithm problem in groups for which the automorphism group has several subgroups, e.g., in cyclic groups of order n where $\varphi(n) = |\mathbb{Z}_n^*|$ is smooth? Not necessarily. We should mention here that the reduction is in general not effective, because the equality of orbits may not be easy to check.

Finally, we note the case of abelian group actions as in CSIDH, cf. Example 4. In this case, subgroups also provide a reduction as above, but there are difficulties to exploit them, cf. [Smi18, Sec. 12].

Acknowledgements

We would like to thank the reviewers for their valuable feedback and suggestions.

References

[Ala+20] G. Alagic, et al, "Status report on the second round of the NIST post-quantum cryptography standardization process," *NIST Internal Report*, no. 8309 (2002), 39 pages

[ADMP20] N. Alamati, L. De Feo, H. Montgomery, S. Patranabis, "Cryptographic group actions and applications," in: Advances in Cryptology—ASIACRYPT 2020, pp. 411–439, LNCS 12492, Springer, 2020

[Aru+19] F. Arute, et al, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779 (2019), pp. 505–510

[Cas+18] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, "CSIDH: an efficient post-quantum commutative group action," in: Advances in Cryptology—ASIACRYPT 2018, pp. 395–427, LNCS 11274, Springer, 2018

[Cou06] J. M. Couveignes, "Hard homogenous spaces," 15 pages, IACR eprint 2006/291 (1997, published 2006)

[DH76] W. Diffie, M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, no. 6 (1976), pp. 644–654

[Gni14] O. W. Gnilke, "The semigroup action problem in cryptography," Ph. D. dissertation, University College Dublin (2014)

[GJ21] R. Granger, A. Joux, "Computing discrete logarithms," in: Computational Cryptography—Algorithmic Aspects of Cryptology (to appear), 32 pages, IACR eprint 2021/1140 (2021)

[GKZ18] R. Granger, T. Kleinjung, J. Zumbrägel, "Indiscreet logarithms in finite fields of small characteristic," *Adv. Math. Commun.*, vol. 12, no. 2 (2018), pp. 263–286

[DJP14] L. De Feo, D. Jao, J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," *J. Math. Cryptol.*, vol. 8, no. 3 (2014), pp. 209–247

[GPSV21] S. Galbraith, L. Panny, B. Smith, F. Vercauteren, "Quantum equivalence of the DLP and CDHP for group actions," *Math. Cryptol.*, vol. 1, no. 1 (2021), pp. 40–44

[Kob87] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comp.*, vol. 48, no. 177 (1987), pp. 203–209

[Mau94] U. M. Maurer, "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms," in: Advances in Cryptology—CRYPTO '94, pp. 271–281, LNCS 839, Springer, 1994

[Mau05] U. M. Maurer, "Abstract models of computation in cryptography," in: Cryptography and Coding 2005, pp. 1–12, LNCS 3796, Springer, 2005

[MW99] U. M. Maurer, S. Wolf, "The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms," *SIAM J. Comput.*, vol. 28 (1999), no. 5, pp. 1689–1721

[Maz03] G. Maze, "Algebraic methods for constructing one-way trapdoor functions," Ph. D. dissertation, University of Notre Dame (2003)

[MMR07] G. Maze, C. Monico, J. Rosenthal, "Public-key cryptography based on semigroup actions," *Adv. Math. Commun.*, vol. 1, no. 4 (2007), 489–507

[Mil86] V. .S. Miller, "Use of elliptic curves in cryptography," in: Advances in Cryptology—CRYPTO '85, pp. 417–426, LNCS 218, Springer, 1986

[Mon02] C. Monico, "Semirings and semigroup actions in public-key cryptography," Ph. D. dissertation, University of Notre Dame (2002)

[PH78] S. C. Pohlig, M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Trans. Inform. Theory*, vol. 24, no. 1 (1978), pp. 106–110

[RS06] A. Rostovtsev, A. Stolbunov, "Public-key cryptosystem based on isogenies," 19 pages, IACR eprint 2006/145

[Sho97] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Computing*, vol. 26, no. 5 (1997), pp. 1484–1509

[Smi18] B. Smith, "Pre- and post-quantum Diffie-Hellman from groups, actions, and isogenies," in: Workshop on the Arithmetic of Finite Fields WAIFI 2018, pp. 3–40, LNCS 11321, Springer, 2018

[Sto10] A. Stolbunov, "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves," *Adv. Math. Commun.*, vol. 4, no. 2 (2010), pp. 215–235

[Zum08] J. Zumbrägel, "Public-key cryptography based on simple semirings," Ph. D. dissertation, University of Zurich (2008)