TROPICAL CRYPTOGRAPHY II: EXTENSIONS BY HOMOMORPHISMS

DIMA GRIGORIEV AND VLADIMIR SHPILRAIN

Abstract. We use extensions of tropical algebras as platforms for very efficient public key exchange protocols.

Keywords: tropical algebra, public key exchange

Mathematics subject classification: 15A80, 94A60.

1. Introduction

In our earlier paper [3], we employed *tropical algebras* as platforms for two cryptographic schemes by mimicking some well-known "classical" schemes in the "tropical" setting. What it means is that we replaced the usual operations of addition and multiplication by the operations $\min(x, y)$ and $x + y$, respectively. An obvious advantage of using tropical algebras as platforms is unparalleled efficiency because in tropical schemes, one does not have to perform any multiplications of numbers since tropical multiplication is the usual addition, see Section 2. On the other hand, "tropical powers" of an element exhibit some patterns, even if such an element is a matrix over a tropical algebra. This weakness was exploited in [6] to arrange a fairly successful attack on one of the schemes in [3].

In this paper, we use extensions of tropical matrix algebras by homomorphisms as platforms in an attempt to destroy patterns in powers of elements of a platform algebra. We call these extensions *semidirect products* since they are similar to a well-known operation (with the same name) in (semi)group theory. Semidirect products of (semi)groups as platforms for public key exchange similar to (yet different from) the standard Diffie-Hellman key exchange were introduced in [4] (see also [5]).

We emphasize once again an obvious advantage of using tropical algebras as platforms: unparalleled efficiency due to the fact that there is no "actual" multiplication involved since tropical multiplication is the same as "usual" addition.

2. Preliminaries

We start by giving some necessary information on tropical algebras here; for more details, we refer the reader to the monograph [1].

Research of the first author was partially supported by the RSF (Russian Science Foundation) grant 16-11-10075. Research of the second author was partially supported by the ONR (Office of Naval Research) grant N000141512164.

Consider a tropical semiring S (also known as the min-plus algebra due to the following definition). This semiring is defined as a subset of reals that contains 0 and is closed under addition, with two operations as follows:

$x \oplus y = \min(x, y)$

$x \otimes y = x + y.$

It is straightforward to see that these operations satisfy the following properties:

associativity:
$x \oplus (y \oplus z) = (x \oplus y) \oplus z$
$x \otimes (y \otimes z) = (x \otimes y) \otimes z.$

commutativity:
$x \oplus y = y \oplus x$
$x \otimes y = y \otimes x.$

distributivity:
$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z).$

There are some "counterintuitive" properties as well:
$x \oplus x = x$

$x \otimes 0 = x$

$x \oplus 0$ could be either 0 or x.

There is also a special "ϵ-element" $\epsilon = \infty$ such that, for any $x \in S$,

$\epsilon \oplus x = x$

$\epsilon \otimes x = \epsilon.$

A (tropical) monomial in S looks like a usual linear function, and a tropical polynomial is the minimum of a finite number of such functions, and therefore a concave, piecewise linear function. The rules for the order in which tropical operations are performed are the same as in the classical case, see the example below.

Example 1. *Here is an example of a tropical monomial:* $x \otimes x \otimes y \otimes z \otimes z$. *The (tropical) degree of this monomial is 5. We note that sometimes, people use the alternative notation* $x^{\otimes 2}$ *for* $x \otimes x$, *etc.*

An example of a tropical polynomial is: $p(x, y, z) = 5 \otimes x \otimes y \otimes z \oplus x \otimes x \oplus 2 \otimes z \oplus 17 = (5 \otimes x \otimes y \otimes z) \oplus (x \otimes x) \oplus (2 \otimes z) \oplus 17$. *This polynomial has (tropical) degree 3, by the highest degree of its monomials.*

We note that, just as in the classical case, a tropical polynomial is canonically represented by an ordered set of tropical monomials (together with non-zero coefficients), where the order that we use here is deglex.

2.1. **Tropical matrix algebra.** A tropical algebra can be used for matrix operations as well. To perform the $A \oplus B$ operation, the elements m_{ij} of the resulting matrix M are set to be equal to $a_{ij} \oplus b_{ij}$. The $\otimes$ operation is similar to the usual matrix multiplication, however, every "+" calculation has to be substituted by a $\oplus$ operation, and every "$\cdot$" calculation by a $\otimes$ operation.

Example 2. $\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 3 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & -1 \end{pmatrix}$.

Example 3. $\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 1 & 7 \end{pmatrix}$.

The role of the identity matrix I is played by the matrix that has "0"s on the diagonal and ∞ elsewhere. Similarly, a scalar matrix would be a matrix with an element $\lambda \in S$ on the diagonal and ∞ elsewhere. Such a matrix commutes with any other square matrix (of the same size). Multiplying a square matrix by a scalar amounts to multiplying it by the corresponding scalar matrix.

Example 4. $2 \otimes \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} = \begin{pmatrix} 2 & \infty \\ \infty & 2 \end{pmatrix} \otimes \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 7 & 1 \end{pmatrix}$.

Then, tropical *diagonal matrices* have something (but not ∞) on the diagonal and ∞ elsewhere.

We also note that, in contrast with the "classical" situation, it is rather rare that a "tropical" matrix is invertible. More specifically (see [1, p.5]), the only invertible tropical matrices are those that are obtained from a diagonal matrix by permuting rows and/or columns.

Example 5. $\begin{pmatrix} a & \infty \\ \infty & b \end{pmatrix}^{-1} = \begin{pmatrix} -a & \infty \\ \infty & -b \end{pmatrix}$.

Example 6. *Conjugation:*
$\begin{pmatrix} a & \infty \\ \infty & b \end{pmatrix}^{-1} \otimes \begin{pmatrix} x & y \\ z & t \end{pmatrix} \otimes \begin{pmatrix} a & \infty \\ \infty & b \end{pmatrix} = \begin{pmatrix} x & y + (b-a) \\ z + (a-b) & t \end{pmatrix}$.

2.2. **Semidirect product.**

Definition 1. *Let G be a semigroup acting on a tropical algebra T. That is, for any $x \in T$ and $g \in G$, there is a well-defined element $x^g \in T$ and $(x \otimes y)^g = x^g \otimes y^g$, $x^{gh} = (x^g)^h$ for any $x, y \in T$ and $g, h \in G$. Then the set of pairs*

$$\Gamma = T \rtimes G = \{(x, g) : x \in T,\ g \in G\}$$

is a semigroup under the following operation:

$$(x, g)(y, h) = (x^h \otimes y,\ g \otimes h).$$

We call this Γ a *semidirect product* of T and G. The general operation in this case becomes

$$(x, g)(y, h) = (h^{-1} \otimes x \otimes h \otimes y,\ g \otimes h).$$

We also note that the action of G on T can be an additive homomorphism rather than multiplicative. In that case, the operation $\otimes$ on elements of T in the above definitions should be replaced by $\oplus$. Actually, it is better to have *both* operations (addition and multiplication) employed, to have a better "diffusion", i.e., scrambling elements that are operated on. This is provided by the *adjoint multiplication* operation, see Section 3. We use a relevant instantiation of the semidirect product in our Section 4 as the platform for a Diffie-Hellman-like key exchange protocol.

3. Adjoint multiplication

There is a well-known "adjoint multiplication" operation on $\mathbf{R}$:

$$a \circ b = a + b + ab$$

It is associative but not distributive with respect to addition. Interestingly, with respect to the min-plus operations, the adjoint multiplication is both associative and distributive, whereas in the "classical" case the adjoint multiplication is associative but not distributive. Here is why:

$(a + b) \circ c = a + b + c + (a + b)c = a + b + c + ac + bc$

$(a \circ c) + (b \circ c) = (a + c + ac) + (b + c + bc) = a + b + c + c + ac + bc.$

Thus, the difference between these two expressions is that the first one has just one c whereas the second one has $c + c$. However, in the tropical case, $c \oplus c = c$ and therefore we have

$$(a \oplus b) \circ c = (a \circ c) \oplus (b \circ c).$$

In other words, we have an action by homomorphisms of the semigroup of $\mathbf{Z}$ (with respect to the $\circ$ operation) on the additive (in the tropical sense) semigroup of $\mathbf{Z}$. This action can be used to build an extension of the additive (in the tropical sense) semigroup of $\mathbf{Z}$, and this extension will be a semigroup with respect to the following operation:

$$(x, g)(y, h) = ((x \circ h) \oplus y,\ g \circ h).$$

As before, one can use the tropical algebra T of matrices over $\mathbf{Z}$ instead of $\mathbf{Z}$ itself as the platform, and this is what we suggest in the following public key exchange protocol. We note that in the tropical algebra of matrices, the adjoint multiplication is not commutative. We also point out that the adjoint multiplication has an advantage of employing not one but two operations: (tropical) addition and multiplication, which is good for diffusing information and destroying patterns in the matrix entries.

4. Public key exchange protocol

Let U be the tropical algebra of $k \times k$ matrices over $\mathbf{Z}$. In what follows, H^n means $H \circ H \circ \ldots \circ H$ (n times). Note that, just as in the "classical" case, H^n can be computed with at most $2 \log_2 n$ (adjoint tropical) multiplications by using the "square-and-multiply" method. This also applies to computing $(M, H)^n$ in the semidirect product.

(1) Alice and Bob agree on public matrices $M, H \in U$. Alice selects a private positive integer m, and Bob selects a private positive integer n.

(2) Alice computes $(M,H)^m = (A,\ H^m)$. The matrix A here does not have a simple expression in terms of the matrices M and H, which can be considered an advantage because this makes it more difficult to find any pattern.
Alice sends to Bob only the matrix A.

(3) Bob computes $(M,H)^n = (B,\ H^n)$.
Bob sends to Alice only the matrix B.

(4) Alice computes $K_{Alice} = (B \circ H^m) \oplus A = B \oplus H^m \oplus (B \otimes H^m) \oplus A$.

(5) Bob computes $K_{Bob} = (A \circ H^n) \oplus B = A \oplus H^n \oplus (A \otimes H^n) \oplus B$.

(6) Since both K_{Alice} and K_{Bob} are equal to the first component of $(M,H)^{m+n}$, we should have $K_{Alice} = K_{Bob} = K$, the shared secret key.

Now we give a sample of how the matrices A, B are expressed in terms of M and H, for small exponents.

Example 7. $(M,H)^2 = ((M \circ H) \oplus M,\ H^2) = (M \oplus H \oplus (M \otimes H) \oplus M,\ H^2) = ((M \oplus H \oplus (M \otimes H),\ H^2)$. *(Recall that $M \oplus M = M$.)*
$(M,H)^3 = (M,H)^2(M,H) = ((M \oplus H \oplus (M \otimes H) \circ H) \oplus M,\ H^3) = (M \oplus H \oplus M^2 \oplus (M \otimes H) \oplus (H \otimes M) \oplus (M \otimes H \otimes M),\ H^3)$.

We see that the first component includes (tropical) products of the matrices M and H of different length and in different order, which makes it hard to find any pattern in the entries of the resulting matrix.

4.1. **Parameters.** We suggest the following parameters.

- The size k of matrices: 30.
- The entries of public matrices M, H are selected uniformly at random from integers in the range $[-1000, 1000]$.
- Private exponents m, n are on the order of 2^{200}.

With these parameters, the total bit size of matrices during execution of the protocol in Section 4 can go up to almost 20,000 bits, which is larger than in most known public key exchange protocols, but on the other hand, computations in our protocol are much more efficient since there are no multiplications or reductions modulo an integer involved.

5. Yet another action and public key exchange protocol

In this section, we consider the following action of the multiplicative (in the tropical sense) semigroup of $n \times n$ matrices over $\mathbf{Z}$ on the additive (again, in the tropical sense) semigroup of these matrices:

$$M^H = (H \otimes M^T) \oplus (M^T \otimes H),$$

where M^T is the transpose of a matrix M. The semidirect product associated with this action is a semigroup with the following operation:

$$(M,G)(S,H) = ((H \otimes M^T) \oplus (M^T \otimes H) \oplus S,\ G \otimes H).$$

The relevant public key exchange protocol is similar to that in Section 4 and is presented below. We note that the above action, just as the action by adjoint multiplication (see

Section 3) employs not one but two operations: (tropical) addition and multiplication, which is good for diffusing information and destroying patterns in the matrix entries.

Let U be the tropical algebra of $k \times k$ matrices over $\mathbf{Z}$. In what follows, H^n means $H \otimes H \otimes \ldots \otimes H$ (n times). Just as in the "classical" case, H^n can be computed with at most $2 \log_2 n$ (tropical) multiplications by using the "square-and-multiply" method. This also applies to computing $(M, H)^n$ in the semidirect product.

(1) Alice and Bob agree on public matrices $M, H \in U$. Alice selects a private positive integer m, and Bob selects a private positive integer n.

(2) Alice computes $(M, H)^m = (A,\ H^m)$. The matrix A here does not have a simple expression in terms of the matrices M and H, which makes it difficult to find any pattern.
Alice sends to Bob only the matrix A.

(3) Bob computes $(M, H)^n = (B,\ H^n)$.
Bob sends to Alice only the matrix B.

(4) Alice computes $K_{Alice} = (B \otimes H^m) \oplus A$.

(5) Bob computes $K_{Bob} = (A \otimes H^n) \oplus B$.

(6) Since both K_{Alice} and K_{Bob} are equal to the first component of $(M, H)^{m+n}$, we should have $K_{Alice} = K_{Bob} = K$, the shared secret key.

Parameters recommended for this protocol are the same as before, see Section 4.1.

Now we give a sample of how the matrices A, B are expressed in terms of M and H, for small exponents.

Example 8. $(M, H)^2 = ((H \otimes M^T) \oplus (M^T \otimes H) \oplus M, H^2)$.
$(M, H)^3 = (M, H)^2 (M, H) = ((H \otimes (H \otimes M^T \oplus M^T \otimes H \oplus M)^T) \oplus (H \otimes M^T \oplus M^T \otimes H \oplus M)^T \otimes H \oplus M, H^3) = ((H \otimes M \otimes H^T) \oplus (H \otimes H^T \otimes M) \oplus (H \otimes M^T) \oplus (M \otimes H^T \otimes H) \oplus (H^T \otimes M \otimes H) \oplus (M^T \otimes H) \oplus M, H^3)$.

We see that there are 4 matrices involved in expression of the first component: M, M^T, H, and H^T. The first component includes (tropical) products of these matrices of different length and in different order, which makes it hard to find any pattern in the entries of the resulting matrix.

Acknowledgement. Both authors are grateful to the Hausdorff Research Institute for Mathematics, Bonn for its hospitality during the final stage of this work. The first author is also grateful to MCCME for inspiring atmosphere.

References

[1] P. Butkovic, *Max-linear systems: theory and algorithms*, Springer-Verlag London, 2010.
[2] D. Grigoriev, I. Ponomarenko, *Constructions in public-key cryptography over matrix groups*, Contemp. Math., Amer. Math. Soc. **418** (2006), 103–119.
[3] D. Grigoriev, V. Shpilrain, *Tropical cryptography*, Comm. Algebra. **42** (2014), 2624–2632.

[4] M. Habeeb, D. Kahrobaei, C. Koupparis, V. Shpilrain, *Public key exchange using semidirect product of (semi)groups*, in: ACNS 2013, Lecture Notes Comp. Sc. **7954** (2013), 475–486.
[5] D. Kahrobaei, V. Shpilrain, *Using semidirect product of (semi)groups in public key cryptography*, in: CiE 2016, Lecture Notes Comp. Sc. **9709** (2016), 132–141.
[6] M. Kotov, A. Ushakov, *Analysis of a key exchange protocol based on tropical matrix algebra*, J. Math. Cryptology **12** (2018).
[7] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC-Press 1996.
[8] V. Roman'kov, *Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups*, preprint. *http://arxiv.org/abs/1501.01152*
[9] T. Theobald, *On the frontiers of polynomial computations in tropical geometry*, J. Symbolic Comput. **41** (2006), 1360–1375.

CNRS, Mathématiques, Université de Lille, 59655, Villeneuve d'Ascq, France
Email address: Dmitry.Grigoryev@univ-lille.fr

Department of Mathematics, The City College of New York, New York, NY 10031
Email address: shpil@groups.sci.ccny.cuny.edu