MATH 474 - Tropical Cryptopgraphy

Brian Ha

May 27, 2021

---

1 Introduction

This paper covers the tropical key-exchange protocol that is described in Grigoriev et al.'s paper [1]. A standard cryptography scheme at a top-level contains three components: a key generating function Gen, an encryption function Enc_k with respect to a key k, and a decryption key function Dec_k. For the purposes of this paper, we will only handle the generation of the key and how two parties would exchange it publicly while maintaining secrecy of the key. An implementation of the tropical key-exchange protocol is also attached with this document.

2 Tropical Key-Exchange Protocol

Now, we describe the tropical key-exchange protocol, which we will consider over our usual tropical algebra $\overline{\mathbb{R}}$.

Definition 2.1 (Grigoriev et al., [1])**.** Let $A, B \in \overline{\mathbb{R}}^{n\times n}$ be two public matrices such that $A \odot B \neq B \odot A$. Then, the tropical key-exchange protocol is as follows.

1. Alice picks two tropical polynomials $p_1(x), p_2(x) \in \overline{\mathbb{R}}[x]$ with integer coefficients and sends $p_1(A) \odot p_2(B)$ to Bob.
2. Similarly, Bob picks two tropical polynomials $q_1(x), q_2(x) \in \overline{\mathbb{R}}[x]$ with integer coefficients and sends $q_1(A) \odot q_2(B)$ to Alice.
3. Next, Alice computes $K_A = p_1(A) \odot (q_1(A) \odot q_2(B)) \odot p_2(B)$.
4. Likewise, Bob computes $K_B = q_1(A) \odot (p_1(A) \odot p_2(B)) \odot q_2(B)$

Since $p_1(A) \odot q_1(A) = q_1(A) \odot p_1(A)$ and $p_2(A) \odot q_2(A) = q_2(A) \odot p_2(A)$, we have $K = K_A = K_B$ as the public shared key between Alice and Bob.

Note that for our tropical polynomials to be well-defined when x is a tropical matrix, we require that the constant term in the polynomial be multiplied by the tropical identity matrix.

Example 2.1. Let's consider two people Alice and Bob. For simplicity, assume that we already have a given encryption and decryption function, Enc and Dec. According to the key-exchange protocol, we first require that both individuals have a public tropical polynomial that both people can exchange with each other (and with possible adversaries). Let

$p_{A_1}(x) = 3 \odot x^2 \oplus 5 \odot x \oplus 2 \odot I$ and $p_{A_2}(x) = 5 \odot x^4 \oplus 2 \odot x^3 \oplus x^2 \oplus 9 \odot x \oplus I$ be the two private tropical polynomials associated with Alice.

Similarly, let $q_1(x) = 3 \odot x^2 \oplus 8 \odot x \oplus -2 \odot I$ and $q_2(x) = x^2 \oplus x \oplus I$ be Bob's two private polynomials.

For the public matrices A, B assigned to Alice and Bob respectively, we define them as follows

$$A = \begin{bmatrix} 3 & 2 \\ 1 & -2 \end{bmatrix}$$
$$B = \begin{bmatrix} 7 & 1 \\ 2 & -3 \end{bmatrix}$$

Next, we calculate $p_1(A)$ and $p_2(B)$:

$$p_1(A) = \begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix}$$
$$p_2(B) = \begin{bmatrix} 0 & 1 \\ 2 & -3 \end{bmatrix}$$

Similarly, we calculate $q_1(A)$ and $q_2(B)$:

$$q_1(A) = \begin{bmatrix} 0 & 0 \\ -1 & -4 \end{bmatrix}$$
$$q_2(B) = \begin{bmatrix} 0 & 1 \\ 2 & -3 \end{bmatrix}$$

Next, we verify that $A \odot B \neq B \odot A$,

$$A \odot B = \begin{bmatrix} 4 & -1 \\ 0 & -5 \end{bmatrix}$$
$$B \odot A = \begin{bmatrix} 2 & -1 \\ -2 & -5 \end{bmatrix}$$

Now, we can generate the key:

$$\begin{aligned} q_1(A) \odot (p_1(A) \odot p_2(B)) \odot q_2(B) &= \begin{bmatrix} 4 & 0 \\ 1 & -4 \end{bmatrix} \\ &= K \end{aligned}$$

Then, if Alice and Bob wanted to communicate a message M to each other, then one of them would send the ciphertext $\text{Enc}_k(M)$ to the other, and they would have to decrypt it to get $\text{Dec}_k(\text{Enc}_k(M)) = M$, the message. Note that in cryptography, methods of encryption and decryption are considered to be public. Thus, it is crucial that the method of exchanging keys is also secure, as otherwise any adversary is able to decrypt these encrypted messages.

Next, we discuss the advantages of the tropical key-exchange protocol. The protocol was based on a classical implementation (i.e. over the usual operations of $\mathbb{R}$ and the matrix ring $\mathcal{M}_n(\mathbb{R})$) of a key-exchange protocol that had a flaw: it was vulnerable to a linear algebra attack. This linear algebra attack is reduced to solving a system of linear equations, which can be efficiently solved and typically have a unique solution. However, this is not the case over a tropical algebra.

First, unlike matrices in $\mathcal{M}_n(\mathbb{R})$, invertible matrices over a tropical algebra are exceptionally rare if we consider them to be randomly generated. As we recall, a tropical matrix is invertible if and only if each row and column contains exactly one non-infinite element. Thus, attacking the tropical key-exchange protocol generally cannot be attacked through the same linear algebra approach of solving a system of linear equations.

If one takes a different approach towards attacking the tropical key-exchange protocol (i.e. an attack involving not necessarily invertible matrices), then it can be reduced to solving a certain class of system of equations. However, it's been shown that solving this class of system of equations is computationally difficult. Furthermore, there does exist a method of finding a single solution to the system, however, there's no way to find all solutions to the system.

References

[1] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography, 2013.