7-29-2011

# The Square Discrete Exponentiation Map

A Wood
*DePaul University*

# The Square Discrete Exponentiation Map

A. Wood

Adviser: Joshua Holden

Mathematical Sciences Technical Report Series
MSTR 11-05

July 29, 2011

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 Phone (812)-877-8193

# THE SQUARE DISCRETE EXPONENTIATION MAP

A. WOOD
DEPAUL UNIVERSITY

*Produced at the Rose-Hulman Institute of Technology Mathematics REU*
*Sponsored by NSF grant DMS-1003924*

Abstract. We will examine the square discrete exponentiation map

$$x \to g^{x^2} \pmod p$$

and its properties. The square discrete exponentiation map is a variation on a commonly seen problem in crytographic algorithms. This paper focuses on understanding the underlying structure of the functional graphs generated by this map. Specifically, this paper focuses on explaining the in-degree of graphs of safe primes, which are primes of the form $p = 2q + 1$, where $q$ is also prime.

## 1. Background and Motivation

Much of modern society is built around keeping information private. Whether it is access to online bank accounts or credit card information while paying for online shopping, most of us have information that we trust to be kept safe online. Various cryptographic algorithms have been developed in an attempt to keep our information secure. So far, they have been generally successful.

Cryptographic algorithms, more specifically public-key cryptography, generally work like this: a person, say Alice, has some information that she would like to get to her friend Bob and only to Bob. However, a common acquaintance of theirs, Eve, is trying to intercept this information. Alice will have a public key and a private key, where the private key is known only to her. It is important for the private key to be kept secret because it is the important information needed for decryption. For instance, in ElGamal encryption, Bob uses Alice's public key information to generate an encrypted message and Alice uses her private key information to decrypt it. Without the private key, the message is supposed to be indecipherable. The security of messages depends upon Alice being the only one to know her private key.

Various maps are used to keep this information private. A map involves taking elements from one set and relating them onto elements of another set. For instance, in the square discrete exponentiation map $x \to g^{x^2} \pmod p$, the element $x \in$

*Date*: July 29, 2011.

Faculty Advisor Joshua Holden, Rose-Hulman Institute of Technology.

$\{1, \cdots, p-1\}$ is mapped on to $g^{x^2} \pmod p$. These maps should be easy to compute when you have the private key, but difficult to compute the inverse of when you do not have the private key.

However, the troubling truth is that these maps have not been proven to be secure. For instance, the most widely used map, the discrete exponentiation map $x \to g^x \pmod p$, has not been proven to be secure. It is relatively straightforward to encrypt information using algorithms based upon this map, but we are unsure how difficult it is for an outsider to read this information. The discrete logarithim problem, $x \leftarrow g^x \pmod p$, is presumed to be computationally hard but has not been proven as such. If computing the inverse of the map takes a vast amount of effort, time, and resources, then the algorithm using the map is probably secure. We do know that, at this point in time, it takes a significant amount of time and resources to decrypt information that was encrypted with algorithms that use the discrete exponentiation map. We do not know for certain that this always will be the case. With this in mind, various attempts have been made at discovering how secure this map really is [2, 4, 5].

Several variations on the discrete exponentiation map exist and have yet to be studied in detail. Whether or not these maps are more or less secure than the discrete exponentiation map has yet to be determined. However, if it could be shown that one of these variations is more secure than the discrete map then we know cryptographic algorithms based upon these maps would be more secure.

One such algorithm that uses the square discrete exponentiation map is a group signature scheme outlined by Camenisch and Stadler [1]. In a group signature scheme, members of a larger group are able to authenticate information individually without revealing their individual identities. Their individual identities are able to be determined only by a group manager, and authentication is unable to be forged. The algorithm outlined by Camenisch and Stadler uses the map $x \to g^{x^e} \pmod p$ for an integer $e$; the square discrete exponentiation map corresponds to the case of $e = 2$.

With this in mind, in this paper I discuss the square discrete exponentiation map, $x \to g^{x^2} \pmod p$. If this map truly is computationally difficult, then it could be useful in cryptographic algorithms. One clear example of its usefulness is in the group signature structure discussed above. Previous group signature schemes had several undesirable properties: for instance, the length of the group's public key is determined by the size of the group, and every time a new group member is added the public key has to be modified. Camenisch and Stadler's group signature scheme is the first prosed scheme that avoids these problems, due largely to the fact that they use the map $x \to g^{x^e} \pmod p$ [1].

## 2. Prior Work

The difficulty now lies in determining if a map is computationally intractable, or at least computationally extremely difficult. One method of doing this is by comparing the functional graphs generated by the square discrete map to random graphs.

**Definition 2.1.** *A functional graph is a directed graph from a set onto itself. It represents each $x$ as a node and draws an arrow, called an edge, from that $x$ to its corresponding output. We say that we have an edge from a tail to a head.*

For instance, in the functional graph for $x \to 3^{x^2} \pmod 5$ seen in Figure 1, we have an edge from 4 to 1, an edge from 2 to 1, an edge from 1 to 3, and an edge from 3 to 3.

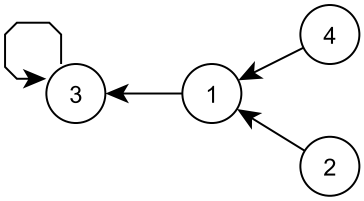


Figure 1. $x \to 3^{x^2} \pmod 5$

If the graph appears sufficiently random, then computing the inverse of the map is probably a difficult feat. In order to determine if the graphs generated by a map appear random, we have to understand the underlying structure. Underlying structure could mean number of image nodes and terminal nodes, in-degree, connected components, cycle length, et cetera. In-degree is the number of edges that each node is the head of. In Figure 1, 1 has in-degree two, 3 has in-degree one, and 2 and 4 both have in-degree zero. An image node is a node that has in-degree greater that zero, such as the nodes 1 and 3 in Figure 1, and a terminal node is a node with in-degree zero, such as nodes 2 and 4. Connected components refers to the number of subgraphs connected by edges on a functional graph. For instance, Figure 1 has only one connected component. Cycle length refers to the number of nodes in a cycle, a cycle being a set of nodes that map to each other with the last node mapping to the first node. For instance, in Figure 1, the cycle length is 1, the cycle being from the node 3 to itself. A tree is a section of a graph that contains no cycles—for instance, in Figure 1, the section of the graph containing the nodes 1, 2, and 4 is a tree.

These are just a few examples of properties of directed graphs that you can study. In this paper, I will focus only on in-degree. Cloutier used this method of comparision to random graphs to study the discrete map $x \to g^x \pmod p$ and had success in characterizing in-degree [2]. In his work, he discovered that the in-degree of the functional graphs for the map $x \to g^x \pmod{p}$ is dependent upon the value of $g$ and $p$—namely, he found that all graphs are $m$-ary [2].

**Definition 2.2.** *We say that a functional graph is $m$-ary when each node has in-degree 0 or $m$.*

The reason that in-degree had such strong structure on this graph is the relationship between $g$ and $p-1$. Cloutier found this relationship via a property of what is called a primitive root. Specifically,

**Definition 2.3.** *We say that $g$ is a primitive root modulo $p$ if $x = p-1$ is the smallest positive integer such that $g^x \equiv 1 \pmod{p}$.*

His main theorem states as follows:

**Theorem 2.1.** [2] *Let $p$ be fixed and let $m$ be any positive integer that divides $p-1$. Then as $g$ ranges over the integers, there are $\phi\left(\frac{p-1}{m}\right)$ different functional graphs which are $m$-ary produced by maps of the form $f\colon x \mapsto g^x \pmod{p}$. Furthermore, if $h$ is any primitive root modulo $p$, and $g \equiv h^a \pmod{p}$, then the values of $g$ that produce an $m$-ary graph are precisely those for which $\gcd(a, p-1) = m$.*

As you can see from his theorem, the structure of the functional graphs produced by the discrete exponentiation map depend entirely on the relationship between $g$ and $p-1$.

Useful in our understanding of this relationship is the idea that, in modular arithmetic, we know that for a primitive root $r$, if $r^x \equiv r^y \pmod{p}$, then $x \equiv y \pmod{p-1}$. This fact is what much of the structure of the discrete exponentiation map is based upon. Unsurprisingly due to the similarity between the ways in wich the two maps are formulated, the structure of the in-degree on the square discrete exponentiation map is found modulo $p-1$ as well.

Another important indicator of the relationship between $g$ and $p-1$ is what power residue $g$ is modulo $p$. Specifically,

**Definition 2.4.** *We say that $g$ is an $n^{th}$ power residue modulo $p$ if there exists an $h$ such that $h^n \equiv g \pmod{p}$.*

For instance, 11 is a quadratic residue modulo 19 because $7^2 \equiv 11 \pmod{19}$.

## 3. Methods

The method for determining the computational intractability of the square discrete exponentiation map involves: determining the underlying structure of the functional graphs generated by a the map, using exponential generating functions to determine the behavior of random graphs of the same structure, and performing statistical analysis to observe the behavior of the actual graphs for comparison to the random graphs. In this paper, the underlying structure is explored and exponential generating functions for this structure are outlined.

3.1. **The Underlying Structure.** The underlying structure of the functional graphs must be determined before it is possible to analyze random graph behavior with exponential generating functions. Without an understanding of the structure of the map, it would not be possible to analyze the behavior of random maps of a similar form.

In this paper, I focus on characterizing in-degree due to the success Cloutier had with finding structure in the in-degree on the discrete exponentiation map [2]. Furthermore, when studying the graphs generated by lower primes, no clear pattern seemed to emerge in terms of cycle length or connected components. However, the in-degree of the graphs clearly had some structure. Therefore, in order to determine the structure of the functional graphs, I focus on in-degree.

My main result concerns the in-degree of functional graphs modulo a safe prime. Safe primes are primes of the form $2q+1$, where $q$ is a prime. Safe primes are of interest in cryptography because they fulfill one criterion of strong primes. To be a strong prime, $p$ must be large, $p-1 = aq+1$ where $q$ is prime must have a large prime factor, $q-1$ must have a large prime factor, and $p+1$ must have a large prime factor. Safe primes fit the criterion of $p-1$ having a large prime factor.

Safe primes are useful because $p-1$ has only four divisors: 1, 2, $q$, and $2q$. As we will see, the relationship between $g$ and $p-1$ determines the in-degree of the functional graphs for the square discrete exponentiation map, thus it makes sense that safe primes, with their small number of divisors, will prove key in our understanding of in-degree.

To determine in-degree, we will go over various patterns found in the maps and generalize them to find the exact in-degree for maps modulo a safe prime. To prove these patters, we will use the fact that if $g^a \equiv g^b \pmod{p}$ for some integers $a, b$ and a primitive root $g$, then $a \equiv b \pmod{p-1}$.

3.2. **Exponential Generating Functions.** A random map is a map that has been drawn randomly, without any specific pattern. However, on average random maps will have certain properties, such as average cycle length, average number of terminal nodes, et cetera.

An exponential generating function is just another way of counting combinatorial objects. They can be a useful tool for analyzing random maps [3].

**Definition 3.1.** *The function*

$$f(x) = a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + \cdots = \sum_{i=0}^{\infty} a_i \frac{x^i}{i!}$$

*is called the exponential generating function for the sequence* $a_0, a_1, a_2, a_3, \ldots$.

For instance, the sequence $1, 1, 1, 1, \ldots$ can be represented as the exponential generating function

$$1 + 1 \cdot x + 1 \cdot \frac{x^2}{2!} + 1 \cdot \frac{x^3}{3!} + \cdots = e^x.$$

Once some part of the structure of a map is thoroughly understood, it is possible to derive exponential generating functions that model random graphs of the same general structure.

Using generating functions we can determine the average expected structure of a randomly generated graph with the same in-degree structure as seen on the square discrete exponentiation map using the method was developed by Flajolet and Odlyzko [3].

3.3. **Statistics.** After the struture of the maps has been determined and random graphs sufficiently described, it will be useful to gather statistics on the behavior of the square discrete exponentiation map. Previous work has been done on writing code that will generate these results [2, 4, 5].

Once all of the statistical data has been gathered, the information can be used to compare the square discrete exponentiation map to random maps. We will look at data such as cycle length, number of terminal nodes, et cetera. If the square discrete exponentiation map's data is close enough to that of random maps, then we say that the graphs seem random. The more random a graph appears, the more difficult the inverse of the map will be to compute. Therefore, if the functional graphs appear random, it is reasonable to conclude that cryptographic algorithms using the square discrete exponentiation map are probably secure.

## 4. Theoretical Results: In-Degree

Now we will look at some of the properties of the square discrete exponentiation map. In order to discover the underlying structure of in-degrees, we will first look at the in-degree of the image node 1.

The next theorems describe certain $x$ values that, for all $g$, give us a specific output.

**Theorem 4.1.** *Let $p - 1 = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$. For all $g$, $g^{x^2} \equiv 1 \pmod{p}$ for*

$$x = k\left(\prod_{i=1}^{n} p_i^{\lceil \frac{a_i}{2} \rceil}\right) = k\left(p_1^{\lceil \frac{a_1}{2} \rceil} p_2^{\lceil \frac{a_2}{2} \rceil} \cdots p_n^{\lceil \frac{a_n}{2} \rceil}\right) = k\left(2^{\lceil \frac{a_1}{2} \rceil} p_2^{\lceil \frac{a_2}{2} \rceil} \cdots p_n^{\lceil \frac{a_n}{2} \rceil}\right)$$

*where $k \in \mathbb{N}$. We will call these values $\bar{x}_k$.*

*Proof.* First consider $\bar{x}_1 = \prod_{i=1}^{n} p_i^{\lceil \frac{a_i}{2} \rceil}$. Then, for any $g$,

$$g^{\bar{x}_1^2} \equiv g^{\left(p_1^{\lceil \frac{a_1}{2} \rceil} \cdots p_n^{\lceil \frac{a_n}{2} \rceil}\right)^2} \equiv g^{p_1^{2\lceil \frac{a_1}{2} \rceil} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil}} \equiv \left(g^{p_1^{2\lceil \frac{a_1}{2} \rceil - x_1} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil - x_n}}\right)^{p_1^{x_1} \cdots p_n^{x_n}} \pmod{p}$$

where $x_i = 2\lceil \frac{a_i}{2} \rceil - a_i$. Note that $x_i = 0$ if $a_i$ is even, and $x_i = 1$ if $a_i$ is odd. Then,

$$\left( g^{p_1^{2\lceil \frac{a_1}{2} \rceil - x_1} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil - x_n}} \right)^{p_1^{x_1} \cdots p_n^{x_n}} \equiv \left( g^{p-1} \right)^{p_1^{x_1} \cdots p_n^{x_n}} \equiv 1^{p_1^{x_1} \cdots p_n^{x_n}} \equiv 1 \pmod{p}$$

Finally, note that $g^{x^2} \equiv g^{(k\bar{x}_1)^2} \equiv (g^{\bar{x}_1^2})^{k^2} \equiv 1^{k^2} \equiv 1 \pmod{p}$. □

For instance, observe the chart for $p = 13$ in Figure 2 [1]. The areas shaded brown are the $x$ values that, for all $g$, give us 1 as an output.

The next theorem tells for what $x$ we will get ±1 as an output for all $g$.

**Theorem 4.2.** *Let $p - 1 = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$. For all $g$, $g^{x^2} \equiv \pm 1 \pmod{p}$ for*

$$x = l \left( 2^{\lfloor \frac{a_1}{2} \rfloor} \prod_{i=2}^{n} p_i^{\lceil \frac{a_i}{2} \rceil} \right) = l \left( 2^{\lfloor \frac{a_1}{2} \rfloor} p_2^{\lceil \frac{a_2}{2} \rceil} \cdots p_n^{\lceil \frac{a_n}{2} \rceil} \right)$$

*where $l \in \mathbb{N}$. We will call these values $\bar{\bar{x}}_l$.*

*Proof.* First consider $\bar{\bar{x}}_1 = 2^{\lfloor \frac{a_1}{2} \rfloor} \prod_{i=2}^{n} p_i^{\lceil \frac{a_i}{2} \rceil}$. Then, for any $g$,

$$g^{\bar{\bar{x}}_1^2} \equiv g^{\left( 2^{\lfloor \frac{a_1}{2} \rfloor} p_2^{\lceil \frac{a_2}{2} \rceil} \cdots p_n^{\lceil \frac{a_n}{2} \rceil} \right)^2} \equiv g^{2^{2\lfloor \frac{a_1}{2} \rfloor} p_2^{2\lceil \frac{a_2}{2} \rceil} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil}}$$

$$\equiv \left( g^{2^{2\lfloor \frac{a_1}{2} \rfloor - x_1} p_2^{2\lceil \frac{a_2}{2} \rceil - x_2} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil - x_n}} \right)^{p_1^{x_1} \cdots p_n^{x_n}} \pmod{p}$$

where $x_i = 2\lceil \frac{a_i}{2} \rceil - a_i$. Note that for $2 \leq x_i \leq n$, $x_i = 0$ if $a_i$ is even, and $x_i = 1$ if $a_i$ is odd. In the case of $i = 1$, note that $x_1$ is 0 if $a_1$ is even and is $-1$ if $a_1$ is odd. Then,

$$\left( g^{2^{2\lfloor \frac{a_1}{2} \rfloor - x_1} p_2^{2\lceil \frac{a_2}{2} \rceil - x_2} \cdots p_n^{2\lceil \frac{a_n}{2} \rceil - x_n}} \right)^{p_1^{x_1} \cdots p_n^{x_n}} \equiv \left( g^{p-1} \right)^{2^{x_1} p_2^{x_2} \cdots p_n^{x_n}} \equiv 1^{2^{x_1} p_2^{x_2} \cdots p_n^{x_n}} \equiv 1^{2^{x_1}} \pmod{p}$$

If $x_1 = 0$, then $1^{2^{x_1}} \equiv 1 \pmod{p}$. If $x_1 = -1$, then $1^{2^{x_1}} \equiv 1^{1/2} \equiv \pm 1 \pmod{p}$. Finally, note that $g^{x^2} \equiv g^{(l\bar{\bar{x}}_1)^2} \equiv (g^{\bar{\bar{x}}_1^2})^{l^2} \equiv (\pm 1)^{l^2} \equiv \pm 1 \pmod{p}$. □

However, also note sometimes the solutions for $\bar{x}_k$ and $\bar{\bar{x}}_l$ will be exactly the same, as seen in Figure 4.

Now we will take things a step further and attempt to generally characterize the output for a specific $g$ and $p$. Let $q_i = \{q_1, \cdots, q_s\}$ be all divisors of $p - 1$, in ascending order. If $g$ is a ${q_i}^{th}$ power residue modulo $p$, then the map for $g^{x^2}$ has $q_i$ repetitions. For example, consider $g = 8$, a $3^{rd}$ power residue modulo 19, as seen in Figure 5. Notice that the outputs have three repetitions, as expected.

In terms of a formula,

[1] All remaining figures can be found at the end of the document.

**Theorem 4.3.** *Let $q_1, \cdots, q_j$ be all divisors of $p-1$. Assume $g$ is a ${q_i}^{th}$ root modulo $p$. Then, for $1 \leq \xi \leq q_i, 0 \leq z \leq \left\lceil \frac{\left(\frac{p-1}{q_i}\right)}{2} \right\rceil$,*

$$g^{z^2} \equiv g^{\left(\xi\left(\frac{p-1}{q_i}\right) \pm z\right)^2} \pmod{p}. \tag{1}$$

*Proof.* Consider $g^{\left(\xi\left(\frac{p-1}{q_i}\right) \pm z\right)^2} \equiv g^{\xi^2\left(\frac{p-1}{2}\right)^2 \pm 2\xi z\left(\frac{p-1}{2}\right) + z^2} \pmod{p}$.

Since $g$ is a $q_i$th residue modulo $p$, $g \equiv r^{q_i} \pmod{p}$ for some $r$.

Observe that

$$g^{\xi^2\left(\frac{p-1}{q_i}\right)^2} \equiv \left(g^{\frac{1}{q_i}}\right)^{\xi^2\frac{(p-1)^2}{q_i}} \equiv r^{\frac{\xi^2(p-1)^2}{q_i}} \equiv \left(r^{(p-1)}\right)^{\xi^2\left(\frac{p-1}{q_i}\right)} \pmod{p}$$

Fermat's Little Theorem tells us that $r^{p-1} \equiv 1 \pmod{p}$, thus

$$\left(r^{(p-1)}\right)^{\xi^2\left(\frac{p-1}{q_i}\right)} \equiv 1^{\xi^2\left(\frac{p-1}{q_i}\right)} \equiv 1 \pmod{p}$$

and

$$g^{\pm 2\xi z\frac{p-1}{q_i}} \equiv \left(g^{\frac{1}{q_i}}\right)^{\pm 2\xi z(p-1)} \equiv r^{\pm 2\xi z(p-1)} \equiv 1^{\pm 2\xi z} \equiv 1 \pmod{p}.$$

Thus

$$g^{\left(\xi\left(\frac{p-1}{q_i}\right) \pm z\right)^2} \equiv g^{z^2} \pmod{p}.$$

Notice that although this is true for all $z, \xi$, considering only $0 \leq \xi \leq q_i$ and $0 \leq z \leq \left\lceil \frac{\left(\frac{p-1}{q_i}\right)}{2} \right\rceil$ helps get rid of redundant cases. □

In Figure 6, the $g$=2, 3, 10, 13, 14, and 15 are primitive roots modulo 19, therefore we see that the outputs of $x \mapsto g^{x^2} \pmod{p}$ for these $g$ cycle through once. In other words, $q_i = 1$ and $\xi = 1$. Note that $g$=4, 5, 6, 16, and 17 are quadratic residues modulo 19 and their outputs run through two cycles, where $q_i = 2$ and $\xi = 2$. Meanwhile, $g$=8 and $g$=12 are cubic residues modulo 19 and their outputs run through 3 cycles, where $q_i = 3$ and thus $\xi = 3$. Also note that $g$=18 is a $9^{th}$ power residue modulo 19 and its outputs run through 9 cycles ($q_i = 9$, $\xi = 9$), while $g$=1 is an $18^{th}$ power residue modulo 19 and its outputs run through 18 cycles ($q_i = 18$, $\xi = 18$).

This corollary follows quite easily, but is important in determining the in-degree of 1:

**Corollary 4.1.** *Let $q_1, \cdots, q_j$ be all divisors of $p-1$. Assume $g$ is a $q_i$th power residue modulo $p$. Then, for all $\xi$,*

$$g^{\left(\xi\left(\frac{p-1}{q_i}\right)\right)^2} \equiv 1 \pmod{p}.$$

*Proof.* Note that this equation is a case of (1), when $z = 0$. Thus, $g^{0^2} \equiv g^{\left(\xi\left(\frac{p-1}{q_i}\right) \pm 0\right)^2} \equiv 1 \pmod{p}$. □

With the previous theorems, it is possible to draw conclusions about the in-degree of the functional graphs, because we know that the in-degree is strongly related to what power residue $g$ is modulo $p$.

**Theorem 4.4.** *Let $q_1, \cdots, q_j$ be all divisors of $p-1$. Let $g$ be a $q_i$th power residue modulo p. Then, the in-degree for image nodes on the directed graph for $x \to g^{x^2} \pmod{p}$ will have three cases. Let*

$$a^* \equiv g^{\left(\frac{\left(\frac{p-1}{q_i}\right)}{2}\right)^2} \pmod{p}$$

*where $a^*$ exists only when $\frac{p-1}{q_i}$ is even.*

1. *If $a^* \equiv 1 \pmod{p}$ then the in-degree on the node $1$ is $2q_i + 2q_i s_1$, for some $s_1 \in \mathbb{N}^{\geq 0}$.*
2. *If $a^* \not\equiv 1 \pmod{p}$ or $a^*$ does not exist, then the in-degree on the node $1$ is $q_i + 2q_i s_2$, for some $s_2 \in \mathbb{N}^{\geq 0}$, and when $a^*$ exists it has in-degree $q_i + 2q_i s_3$, for some $s_3 \in \mathbb{N}^{\geq 0}$.*
3. *All other non-terminal nodes have in-degree $2q_i s_4$ for some $s_4 \in \mathbb{N}^{\geq 0}$*

*Proof.* First, note that by Corollary 4.1, if $x$ is a multiple of $\frac{p-1}{q_i}$, then $g^{x^2} \equiv 1 \pmod{p}$. Therefore, the node for 1 has in-degree of at least $q_i$.

If $a^*$ exists, note that $a^*$ is the image of at least $q_i$ numbers as well. This is because $a^*$ occurs when $x = \frac{\left(\frac{p-1}{q_i}\right)}{2}$. For every $\xi$ we know that $g^{\left(\xi\left(\frac{p-1}{q_i}\right)\right)^2} \equiv 1 \pmod{p}$, and it is straightforward to see that

$$g^{\left(\xi\left(\frac{p-1}{q_i}\right)-\frac{\frac{p-1}{q_i}}{2}\right)^2} \equiv a^* \pmod{p}.$$

With this and by observing that $\xi\left(\frac{p-1}{q_i}\right) - \frac{\left(\frac{p-1}{q_i}\right)}{2} = (\xi - 1)\left(\frac{p-1}{q_i}\right) + \frac{\left(\frac{p-1}{q_i}\right)}{2}$, we see that $a^*$ occurs halfway in between each occurence of 1 that is gotten by $x = \xi\left(\frac{p-1}{q_i}\right)$. Thus for every time $x = \xi\left(\frac{p-1}{q_i}\right)$ gives us 1 as an output, we will have $x = \xi\left(\frac{p-1}{q_i}\right) - \frac{\left(\frac{p-1}{q_i}\right)}{2}$ giving us $a^*$ as an output.

We know by Theorem 4.3 that the images for $g^{x^2} \pmod{p}$ repeat themselves $q_i$ times, and that inside of each repetition each output is repeated twice, except for the the following two cases: where $x$ is a multiple of $\frac{p-1}{q_i}$, because then $z = 0$ and $+0 = -0$; or, when $x$ is a multiple of $\frac{\frac{p-1}{q_i}}{2}$ when $\frac{p-1}{q_i}$ is even, because it corresponds to the case in Theorem 4.3 where $z$ is such that $(\xi - 1)(\frac{p-1}{q_i}) + z = \xi(\frac{p-1}{q_i}) - z$. The second case happens under the same conditions that give us $a^*$.

Because the outputs are repeated a certain number of times as seen in Theorem 4.3, the in-degree on the nodes for those outputs will correspond to the number of times the outputs are repeated. Thus, if $a^* \equiv 1 \pmod{p}$, then the node for 1 has in-degree $q_i + q_i + 2q_i s_1 = 2q_i + 2q_i s_1$ for some $s_1 \in \mathbb{N}^{\geq 0}$. If $a^*$ does not exist or $a^* \not\equiv 1 \pmod{p}$ then the node 1 has in-degree $q_i + 2q_i s_2$ for some $s_2 \in \mathbb{N}^{\geq 0}$, while $a^*$ has in-degree $q_i + 2q_i s_3$ for some $s_3 \in \mathbb{N}^{\geq 0}$. All other non-terminal nodes in all cases have in-degree $2q_i s_4$ for some $s_4 \in \mathbb{N}^{\geq 0}$. □

With this theorem, we have some general knowledge about the in-degree of the square discrete exponentiation map. The structure of the map is fairly complicated, but by examining specific cases we can gain a deeper understanding of it.

We will consider the case where $p-1$ is a product of two distinct primes. Notice that one of these primes must always be two, because otherwise $p$ would be even and thus not prime. Therefore, $p-1 = 2r$ for some odd prime $r$. This is the same as letting $p$ be a safe prime, excluding the case of $p = 5 = 2 \cdot 2 + 1$. However, before we can prove the in-degree, there is one more property we must discuss.

**Lemma 1.** *Let $g$ be a primitive root modulo $p$. Then $x = p-1$ is the smallest positive integer such that $g^{x^2} \equiv 1 \pmod{p}$ if and only if $p-1 = p_1 p_2 \cdots p_n$ for distinct $p_i$.*

*Proof.* "⇒" Let $g$ be a primitive root mod $p$. Then, $g^{p-1} \equiv 1 \pmod{p}$. Also, note that $g^{(p-1)^2} \equiv 1 \pmod{p}$. Assume to the contrary that $p-1$ is not a product of distinct primes.

Then, $p-1 = p_1^{a_1} p_2^{a_2} \cdots p_i^{a_i} \cdots p_n^{a_n}$ such that $a_i \neq 1$ for some integer $i$. Then,

$$g^{(p_1^{a_1} \cdots p_i^{a_i} \cdots p_n^{a_n})^2} \equiv 1 \pmod{p}.$$

However, note also that when $a_i$ is even,

$$g^{(p_1^{a_1} \cdots p_i^{\frac{a_i}{2}} \cdots p_n^{a_n})^2} \equiv \left(g^{p_1^{a_1} \cdots p_i^{a_i} \cdots p_n^{a_n}}\right)^{p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}} \equiv 1^{p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}} \equiv 1 \pmod{p}.$$

And when $a_i$ is an odd number greater than one,

$$g^{(p_1^{a_1} \cdots p_i^{\frac{a_i+1}{2}} \cdots p_n^{a_n})^2} \equiv \left(g^{p_1^{a_1} \cdots p_i^{a_i} \cdots p_n^{a_n}}\right)^{p_1^{a_1} \cdots p_i \cdots p_n^{a_n}} \equiv 1^{p_1^{a_1} \cdots p_i \cdots p_n^{a_n}} \equiv 1 \pmod{p}.$$

where

$$p_1^{a_1} \cdots p_i^{\frac{a_i}{2}} \cdots p_n^{a_n} < p_1^{a_1} \cdots p_i^{a_i} \cdots p_n^{a_n}$$

and

$$p_1^{a_1} \cdots p_i^{\frac{a_i+1}{2}} \cdots p_n^{a_n} < p_1^{a_1} \cdots p_i^{a_i} \cdots p_n^{a_n}$$

implying $x = p-1$ is not the smallest positive integer such that $g^{x^2} \equiv 1 \pmod{p}$.

"⇐" To prove "if," let $g$ be a primitive root and assume $p-1 = p_1 p_2 \cdots p_n$. Then, $g^{p-1} \equiv 1 \pmod{p}$. Note that $g^{(p-1)^2} \equiv 1 \pmod{p}$, thus there exists $x \in \mathbb{N}$ such that $g^{x^2} \equiv 1 \pmod{p}$. Together this implies that $g^{p-1} \equiv g^{x^2} \pmod{p}$, thus $x^2 \equiv p-1 \pmod{p-1}$, thus $x^2 \equiv 0 \pmod{p-1}$.

Then, $x^2 = (p-1)m = (p_1p_2\cdots p_n)m$ for some $m \in \mathbb{N}$. Note $m$ must be of the form $m = (p_1p_2\cdots p_n)l^2$ for some $l \in \mathbb{N}$, because otherwise $x \notin \mathbb{N}$. Thus, $x^2 = (p_1p_2\cdots p_n)^2l^2$, therefore $x = (p_1p_2\cdots p_n)l = (p-1)l$ for some $l$.

Thus, $x = p-1$ is the smallest positive integer such that $g^{x^2} \equiv 1 \pmod{p}$. □

Now we can describe the structure of in-degree on maps modulo a prime $p$, where $p-1 = 2r$ for an odd prime $r$.

**Theorem 4.5.** *Let $p = 2r+1$, where $r$ is an odd prime. Note that $1$, $2$, $r$, and $2r$ are all divisors of $p-1$, thus let $q_i = 1, 2, r,$ or $2r$ and let $g$ be a $q_i$th power residue modulo $p$, such that if $g$ is also a $q_j$th power residue then $q_j < q_i$.*

1. *The in-degree on the node corresponding to $1$ is $q_i$.*
2. *If $q_i$ is odd, then the node corresponding to $p-1$ has in-degree $q_i$.*
3. *All other non-terminal nodes have in-degree $2q_i$.*

*Proof.* We will prove each condition separately.

1. First, we will prove that the in-degree on the node corresponding to 1 is $q_i$. To do this, we will show that $g^{x^2} \equiv 1 \pmod{p}$ if and only if $x = \xi\left(\frac{p-1}{q_i}\right)$. Note that the "if" was proven in Corollary 4.1, so all that remains to be proven is "only if."

   Assume $g$ is a $q_i$th power residue modulo $p = 2r+1$, where $r$ is an odd prime. We want to find all solutions to the equation $g^{x^2} \equiv 1 \pmod{p}$.

   Since $g$ is a $q_i$th power residue modulo $p$, there is a primitive root $h$ such that $h^{q_i} \equiv g \pmod{p}$. Thus,
$$g^{x^2} \equiv 1 \pmod{p}$$
   can be written as
$$h^{q_ix^2} \equiv h^0 \pmod{2r+1}.$$
   Since $h$ is a primitive root, we know that
$$q_ix^2 \equiv 0 \pmod{2r}.$$
   Furthermore, $q_i$ is a factor of $2r$, thus
$$x^2 \equiv 0 \quad \left(\operatorname{mod} \frac{2r}{q_i}\right).$$
   Therefore, $x^2 = \frac{2r}{q_i}k$ for some integer $k$. Thus, $x$ is a multiple of $\frac{2r}{q_i}$.
2. Next, we will prove that if $q_i$ is odd, then the node corresponding to $p-1$ has in-degree $q_i$. The only cases where $q_i$ is odd are $q_i = 1$ or $q_i = r$.

   Theorem 4.2 tells us that if $x = r$ then $g^{x^2} \equiv \pm 1 \pmod{p}$. If $g$ is a primitive root, in other words if $q_i = 1$, then we know by Lemma 1 that $g^{r^2} \not\equiv 1 \pmod{p}$. Therefore, $g^{r^2} \equiv -1 \equiv p-1 \pmod{p}$. Now, we want to prove that $x = r$ is the only $x$ for which $g^{x^2} \equiv -1 \pmod{p}$.

Consider $g^{x^2} \equiv -1 \pmod{2r+1}$, where $g$ is a primitive root. We know $g^r \equiv -1 \pmod{p}$, because $g^{p-1} \equiv 1 \pmod{p}$ implies that $g^r \equiv g^{\frac{p-1}{2}} \equiv 1^{\frac{1}{2}} \equiv \pm 1 \pmod{p}$, and since $g$ is primitive we know $g^r \not\equiv 1 \pmod{p}$. This implies that $x^2 \equiv r \pmod{2r}$. Then, $g^{x^2} \equiv g^r \pmod{2r+1}$. Then, $x^2 - r^2 = 2rk$ for some integer $k$. Then, $x = \sqrt{r(2k+1)}$. Since $x$ is an integer and $r$ is prime, we know that $2k+1 = rl^2$ for some integer $l$, implying that $x = rl$, or that $x$ is a multiple of $r$. We know that $x \neq 2r$ because $x^{2r} \equiv 1 \pmod{2r+1}$.

Therefore, we know that when $g$ is a primitive root, $g^{x^2} \equiv -1 \pmod{2r+1}$ if and only if $x = r$.

Now we need to prove that if $g$ is an $r$th power residue then the in-degree is $r$ on the node corresponding to $p-1$. Note that, as seen above in the equation $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, the only $r$th power residues modulo $p$ are 1 and $p-1$. However, $g = 1$ is also a $2r$th power residue, thus the only $r$th power residue modulo $p$ we consider is $g = p-1$.

Note that $(p-1)^{x^2} \equiv (-1)^{x^2} \pmod{p}$. Thus, for all even $x$, $(p-1)^{x^2} \equiv 1 \pmod{p}$ and for all odd $x$, $(p-1)^{x^2} \equiv -1 \pmod{p}$. Therefore the node for $p-1$ has in-degree $r$.

(3) By Theorem 4.3, We know that $g^{z^2} \equiv g^{\left(\xi\left(\frac{2r}{q_i}\right)\pm z\right)^2} \pmod{2r+1}$. Here, we see that the values for $z$ are unique only for $0 \leq z \leq \left\lceil \frac{\frac{2r}{q_i}}{2} \right\rceil$. Therefore, to prove part (3), it is sufficient to prove that $g^{z_1^2} \equiv g^{z_2^2} \pmod{2r+1}$ if and only if $z_1 = z_2$, where $0 \leq z_1, z_2 \leq \left\lceil \frac{\frac{2r}{q_i}}{2} \right\rceil$. We know that if $z_1 = z_2$ then $z_1^2 \equiv z_2^2 \pmod{2r}$, thus $g^{z_1^2} \equiv g^{z_2^2} \pmod{2r+1}$.

All that we must show now is that if $g^{z_1^2} \equiv g^{z_2^2} \pmod{2r+1}$ then $z_1 = z_2$, where $0 \leq z_1, z_2 \leq \left\lceil \frac{\frac{2r}{q_i}}{2} \right\rceil$.

If $g$ is a $q_i$th power residue modulo $p$, then there exists a primitive root $h$ such that $h^{q_i} \equiv g \pmod{2r+1}$. This is clearly true when $g$ is a primitive root, or when $q_i = 1$. This also is fairly obvious for the case of $g = 1$, a $2r$th power residue, due to Fermat's Little Theorem. Furthermore, we saw in (2) that the only $r$th power residue to consider is $g = p-1$ and that for all primitive roots $h$, $h^{\left(\frac{p-1}{2}\right)^2} \equiv h^{\left(\frac{2r}{2}\right)^2} \equiv h^{r^2} \equiv -1 \pmod{p}$. The only case left is when $q_i = 2$. Consider quadratic residue $g$ and a primitive root $k$. We know that $g \equiv x^2 \pmod{p}$ for some $x$. Then,

$$\log_k g \equiv \log_k x^2 \pmod{p-1}$$

which implies that

$$\log_k g \equiv 2\log_k x \pmod{p-1}.$$

We now want to find the $\gcd(\log_k x, p-1)$. Because $p-1 = 2r$, possible choices are $\gcd(\log_k x, p-1) = 1, 2, r$ or $2r$. If $2r|\log_k x$, then $log_kx \equiv 0 \pmod{p-1}$, implying that $x \equiv 1 \pmod{p}$, so $g \equiv 1 \pmod{p}$, a contradiction. Similarly, if $r|\log_k x$, then $\log_k x \equiv 0 \pmod{\frac{p-1}{2}}$, implying that $x \equiv \pm 1 \pmod{p}$, so $g \equiv 1 \pmod{p}$, a contradiction. If $2|\log_k x$ then note that $2 \not|(r+\log_k x)$, so $\gcd(r+\log_k x, p-1) = 1$. Therefore, $k^{(r+\log_k x)} = -x$ is a primitive root modulo $p$. Therefore, we know that if $g$ is a $q_i$th power residue modulo $p$, then there exists a primitive root $h$ such that $h^{q_i} \equiv g \pmod{2r+1}$.

Therefore, if $g^{z_1^2} \equiv g^{z_2^2} \pmod{2r+1}$ then $h^{q_i(z_1{}^2)} \equiv h^{q_i(z_2{}^2)} \pmod{2r+1}$ for a primitive root $h$. Therefore, $q_i {z_1}^2 \equiv q_i {z_2}^2 \pmod{2r}$, implying that ${z_1}^2 \equiv {z_2}^2 \left(\bmod \frac{2r}{q_i}\right)$. Therefore,

$${z_1}^2 - {z_2}^2 \equiv 0 \quad \left(\bmod \frac{2r}{q_i}\right)$$

thus

$$(z_1 + z_2)(z_1 - z_2) \equiv 0 \quad \left(\bmod \frac{2r}{q_i}\right).$$

Thus, when $\frac{2r}{q_i}$ is prime, either $z_1 + z_2 \equiv 0 \left(\bmod \frac{2r}{q_i}\right)$ or $z_1 - z_2 \equiv 0 \left(\bmod \frac{2r}{q_i}\right)$. Therefore, either $z_1 \equiv -z_2 \left(\bmod \frac{2r}{q_i}\right)$ or $z_1 \equiv z_2 \left(\bmod \frac{2r}{q_i}\right)$. Since $0 \leq z_1, z_2 < \left\lceil \frac{\frac{2r}{q_i}}{2} \right\rceil$, $z_1 = -z_2$ or $z_1 = z_2$. However, $z_1, z_2 \geq 0$, thus $z_1 = z_2$.

The only case where $\frac{2r}{q_i}$ is not prime is when $q_i = 1$, or when $g$ is a primitive root. In this case, ${z_1}^2 - {z_2}^2 \equiv 0 \left(\bmod \frac{2r}{q_i}\right)$ when $q_i = 1$ implies that

$${z_1}^2 - {z_2}^2 \equiv 0 \pmod{2r}$$

thus

$$(z_1 - z_2)(z_1 + z_2) \equiv 0 \pmod{2r}$$

Since $2r$ is composite, $z_1 + z_2 \equiv 0 \left(\bmod \frac{2r}{q_i}\right)$ and $z_1 - z_2 \equiv 0 \left(\bmod \frac{2r}{q_i}\right)$ are not the only two cases. We also have the case where $(z_1 - z_2)$ is a multiple of 2 while $(z_1 + z_2)$ is a multiple of $r$, or vice versa, but neither is a multiple of $2r$. Also, $0 \leq z_1, z_2 \leq \left\lceil \frac{\frac{2r}{q_i}}{2} \right\rceil = r$. Furthermore, we know that if $z_1 - z_2$ is even then $z_1 + z_2$ is also even. However, we know $z_1 + z_2$ cannot exceed $2r$ because $z_1, z_2 \leq r$. Thus $z_1 + z_2$ is even, thus not a multiple of $r$. Also note that if $z_1 - z_2 = r$ then $z_1 > r$, a contradiction.

Therefore, either $z_1 \equiv -z_2 \pmod{\frac{2r}{q_i}}$ or $z_1 \equiv z_2 \pmod{\frac{2r}{q_i}}$. Since $0 \leq z_1, z_2 < \frac{2r}{q_i}$, $z_1 = z_2$.

□

## 5. Theoretical Results: Generating Functions

In this section, we will outline the exponential generating functions for the funtional graphs generated by the square discrete exponention map over a safe prime modulus $p$ and a primitive root $g$.

To do this, we will begin with the description of a functional graph given by Flajolet and Odlyzko [3]. It defined functional graphs in a computer science-minded way as follows:

$$\begin{cases} FunctionalGraph = set(Components) \\ Components = cycle(Tree) \\ Tree = node \cdot set(Tree) \end{cases} \tag{2}$$

Here, we have a recursive formula for the trees of a functional graph, while the rest of the graph is built out of the trees. A random graph with no specific in-degree structure would be represented as the following exponential generating functions, with $z$ representing a node [3]:

$$\begin{cases} f(z) = e^{c(z)} \\ c(z) = \log \frac{1}{1-t(z)} \\ t(z) = ze^{t(z)} \end{cases} \tag{3}$$

The square discrete exponentiation map has known in-degree structure, so the above equations will need to be modified to take that structure into account.

Consider first the equation for the trees. Because trees on the discrete exponentiation map have to have a specific structure, the exponential generating function for trees must reflect that structure. To review, maps for the square discrete exponentiation map over a safe prime modulus $p$ and a primitive root $g$ have in-degree 1 on the nodes for 1 and $p-1$, and in-degree 2 on all other image nodes. We will consider a model that does not keep track of which nodes have in-degree one and which have in-degree two. All that matters is that, since there will always be an edge from $p-1$ to 1, the two nodes with in-degree 1 are connected by an edge.

The tree function is built as follows: we have a node, or we have a node with two trees, or we have two nodes with one tree. This is represented as $t(z) = z + z\frac{t(z)^2}{2} + z^2 t(z)$, where the middle term is divided by two to remove redundancies. A similar method of constructing a tree function was also used by Cloutier, who constructed a generating functions for binary trees, trees with in-degree 0 or 2, as $b(z) = z + z\frac{b^2(z)}{2}$ [2].

From this function we are able to build the rest of our functions. We know that part of a cycle on our graphs will either be one node and a tree, or three nodes with one tree. We represent this as $c(z) = \log\left(\frac{1}{1-(zt(z)+z^3t(z))}\right)$.

The functions are as follows:

$$\begin{cases} f(z) = e^{c(z)} \\ c(z) = \log\left(\frac{1}{1-(zt(z)+z^3t(z))}\right) \\ t(z) = z + z\frac{t(z)^2}{2} + z^2t(z) \end{cases} \tag{4}$$

However, while these models count all graphs with in-degrees as we have modelled, they do not keep track of the two nodes with in-degree one. Therefore, we will stick a counting variable, $u$, into each equation. The revised equations read as follows:

$$\begin{cases} f(z,u) = e^{c(z,u)} \\ c(z,u) = \log\left(\frac{1}{1-(zt(z,u)+uz^3t(z,u))}\right) \\ t(z,u) = z + z\frac{t(z,u)^2}{2} + uz^2t(z,u) \end{cases} \tag{5}$$

To really count the graphs with only two nodes of in-degree one, after expanding them as generating functions, we must differentiate with respect to $u$ and solve for $u = 0$. By doing this, we get an exponential generating function that counts graphs with only two nodes of in-degree one. We will call this function $g(z)$. Using Maple, we see that

$$g(z) = \frac{2z^4}{(1-2z^2)^{3/2}}.$$

Basic testing on Maple to see if the graphs are counting the graphs correctly make the above characterization seem successful.

## 6. Conclusion and Future Work

This paper has focused on determining the general structure of the in-degree on maps for the square discrete exponentiation map. It has fully characterized the in-degree for safe primes. Safe primes are a useful case to have characterized because of how widely they are used in cryptographic algorithms.

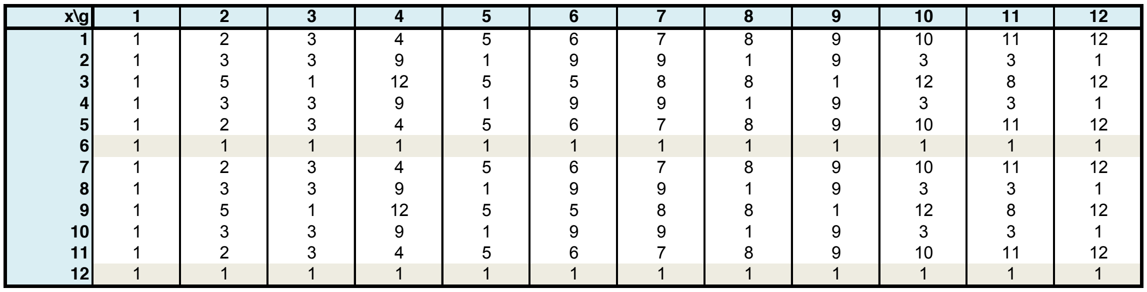
This paper has also focused on maps with a prime modulus. This is seen in the group signature scheme created by Camenisch and Stadler [1]. Future work could include exploring the non-prime modulus case.

If the square discrete exponentiation map were to fall into a predictable pattern, it would not be useful for cryptographic algorithms. With this in mind, in the future it will be important to run statistical analysis on the structure of the graph and to continue work with exponential generating functions. Further work analyzing the generating functions will give us information pertaining to the behavior of random graphs of the same in-degree structure. Statistical analysis will give us the actual structure of things like cycle length and connected components, while the generating functions give us the structure of the same things on random graphs. Comparing the two to see how far the actual values differ from random values will give us an idea of the predictability of the behavior of the square discrete exponentiation map.

## 7. Acknowledgements

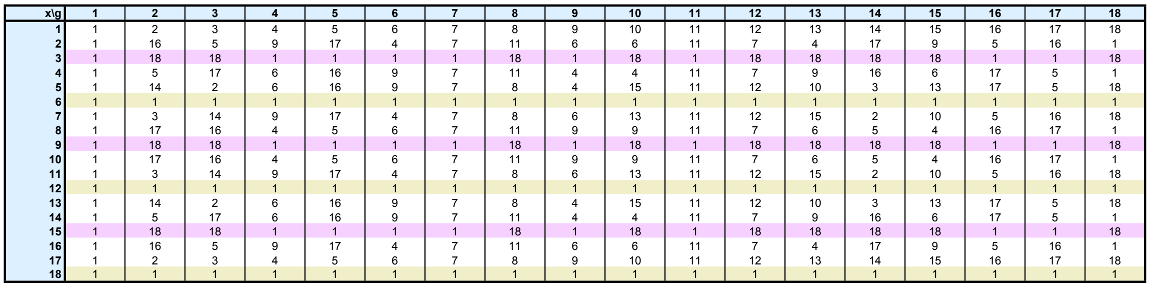
Many thanks to my advisor, Joshua Holden of Rose-Hulman Institute of Technology, for his guidance, to Rose-Hulman Institute of Technology for hosting the REU, and to the NSF for funding the research.

## 8. Figures



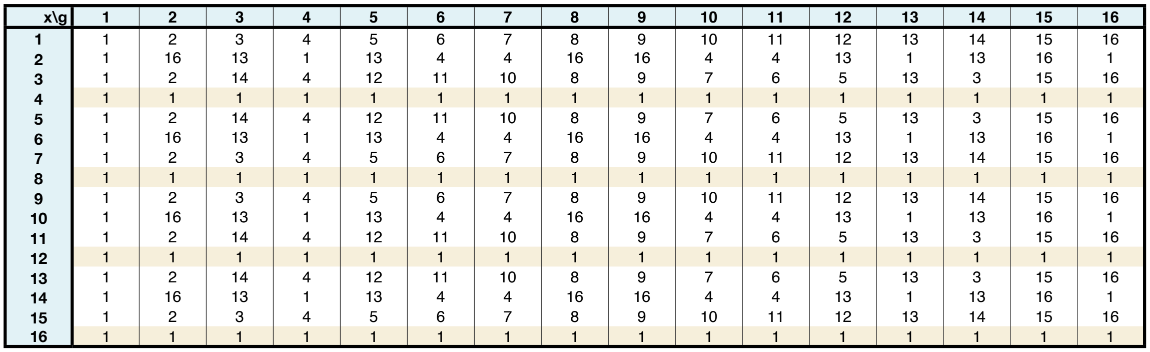
| x\g | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2 | 1 | 3 | 3 | 9 | 1 | 9 | 9 | 1 | 9 | 3 | 3 | 1 |
| 3 | 1 | 5 | 1 | 12 | 5 | 5 | 8 | 8 | 1 | 12 | 8 | 12 |
| 4 | 1 | 3 | 3 | 9 | 1 | 9 | 9 | 1 | 9 | 3 | 3 | 1 |
| 5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 8 | 1 | 3 | 3 | 9 | 1 | 9 | 9 | 1 | 9 | 3 | 3 | 1 |
| 9 | 1 | 5 | 1 | 12 | 5 | 5 | 8 | 8 | 1 | 12 | 8 | 12 |
| 10 | 1 | 3 | 3 | 9 | 1 | 9 | 9 | 1 | 9 | 3 | 3 | 1 |
| 11 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 2. $x \to g^{x^2} \pmod{13}$, $\bar{x}_k = 6, 12$



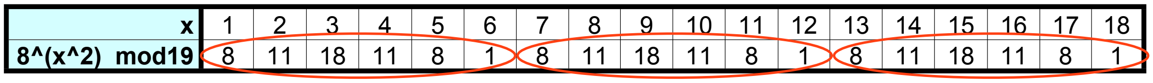
| x\g | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 2 | 1 | 16 | 5 | 9 | 17 | 4 | 7 | 11 | 6 | 6 | 11 | 7 | 4 | 17 | 9 | 5 | 16 | 1 |
| 3 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 4 | 1 | 5 | 17 | 6 | 16 | 9 | 7 | 11 | 4 | 4 | 11 | 7 | 9 | 16 | 6 | 17 | 5 | 1 |
| 5 | 1 | 14 | 2 | 6 | 16 | 9 | 7 | 8 | 4 | 15 | 11 | 12 | 10 | 3 | 13 | 17 | 5 | 18 |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 7 | 1 | 3 | 14 | 9 | 17 | 4 | 7 | 8 | 6 | 13 | 11 | 12 | 15 | 2 | 10 | 5 | 16 | 18 |
| 8 | 1 | 17 | 16 | 4 | 5 | 6 | 7 | 11 | 9 | 9 | 11 | 7 | 6 | 5 | 4 | 16 | 17 | 1 |
| 9 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 10 | 1 | 17 | 16 | 4 | 5 | 6 | 7 | 11 | 9 | 9 | 11 | 7 | 6 | 5 | 4 | 16 | 17 | 1 |
| 11 | 1 | 3 | 14 | 9 | 17 | 4 | 7 | 8 | 6 | 13 | 11 | 12 | 15 | 2 | 10 | 5 | 16 | 18 |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 13 | 1 | 14 | 2 | 6 | 16 | 9 | 7 | 8 | 4 | 15 | 11 | 12 | 10 | 3 | 13 | 17 | 5 | 18 |
| 14 | 1 | 5 | 17 | 6 | 16 | 9 | 7 | 11 | 4 | 4 | 11 | 7 | 9 | 16 | 6 | 17 | 5 | 1 |
| 15 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 16 | 1 | 16 | 5 | 9 | 17 | 4 | 7 | 11 | 6 | 6 | 11 | 7 | 4 | 17 | 9 | 5 | 16 | 1 |
| 17 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 18 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 3. $x \to g^{x^2} \pmod{19}$, $\bar{x}_k = 6, 12, 18$, $\bar{\bar{x}}_l = 3, 6, 9, 12, 15, 18$



| x\g | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 1 | 16 | 13 | 1 | 13 | 4 | 4 | 16 | 16 | 4 | 4 | 13 | 1 | 13 | 16 | 1 |
| 3 | 1 | 2 | 14 | 4 | 12 | 11 | 10 | 8 | 9 | 7 | 6 | 5 | 13 | 3 | 15 | 16 |
| 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 5 | 1 | 2 | 14 | 4 | 12 | 11 | 10 | 8 | 9 | 7 | 6 | 5 | 13 | 3 | 15 | 16 |
| 6 | 1 | 16 | 13 | 1 | 13 | 4 | 4 | 16 | 16 | 4 | 4 | 13 | 1 | 13 | 16 | 1 |
| 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 8 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 9 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 10 | 1 | 16 | 13 | 1 | 13 | 4 | 4 | 16 | 16 | 4 | 4 | 13 | 1 | 13 | 16 | 1 |
| 11 | 1 | 2 | 14 | 4 | 12 | 11 | 10 | 8 | 9 | 7 | 6 | 5 | 13 | 3 | 15 | 16 |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 13 | 1 | 2 | 14 | 4 | 12 | 11 | 10 | 8 | 9 | 7 | 6 | 5 | 13 | 3 | 15 | 16 |
| 14 | 1 | 16 | 13 | 1 | 13 | 4 | 4 | 16 | 16 | 4 | 4 | 13 | 1 | 13 | 16 | 1 |
| 15 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 16 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4. $x \to g^{x^2} \pmod{19}$, $\bar{x}_k = 6, 12, 18$, $\bar{\bar{x}}_l = 3, 6, 9, 12, 15, 18$



| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8^(x^2) mod19 | 8 | 11 | 18 | 11 | 8 | 1 | 8 | 11 | 18 | 11 | 8 | 1 | 8 | 11 | 18 | 11 | 8 | 1 |

Figure 5. $x \to 8^{x^2} \pmod{19}$

| x\g | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 2 | 1 | 16 | 5 | 9 | 17 | 4 | 7 | 11 | 6 | 6 | 11 | 7 | 4 | 17 | 9 | 5 | 16 | 1 |
| 3 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 4 | 1 | 5 | 17 | 6 | 16 | 9 | 7 | 11 | 4 | 4 | 11 | 7 | 9 | 16 | 6 | 17 | 5 | 1 |
| 5 | 1 | 14 | 2 | 6 | 16 | 9 | 7 | 8 | 4 | 15 | 11 | 12 | 10 | 3 | 13 | 17 | 5 | 18 |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 7 | 1 | 3 | 14 | 9 | 17 | 4 | 7 | 8 | 6 | 13 | 11 | 12 | 15 | 2 | 10 | 5 | 16 | 18 |
| 8 | 1 | 17 | 16 | 4 | 5 | 6 | 7 | 11 | 9 | 9 | 11 | 7 | 6 | 5 | 4 | 16 | 17 | 1 |
| 9 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 10 | 1 | 17 | 16 | 4 | 5 | 6 | 7 | 11 | 9 | 9 | 11 | 7 | 6 | 5 | 4 | 16 | 17 | 1 |
| 11 | 1 | 3 | 14 | 9 | 17 | 4 | 7 | 8 | 6 | 13 | 11 | 12 | 15 | 2 | 10 | 5 | 16 | 18 |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 13 | 1 | 14 | 2 | 6 | 16 | 9 | 7 | 8 | 4 | 15 | 11 | 12 | 10 | 3 | 13 | 17 | 5 | 18 |
| 14 | 1 | 5 | 17 | 6 | 16 | 9 | 7 | 11 | 4 | 4 | 11 | 7 | 9 | 16 | 6 | 17 | 5 | 1 |
| 15 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 18 | 1 | 1 | 18 |
| 16 | 1 | 16 | 5 | 9 | 17 | 4 | 7 | 11 | 6 | 6 | 11 | 7 | 4 | 17 | 9 | 5 | 16 | 1 |
| 17 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 18 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 6. $x \to g^{x^2} \pmod{19}$

## References

[1] Jan Camenisch and Markus Stadler. Efficient Group Signiture Schemes for Large Groups. *Lecture Notes in Computer Science*, 1997, Volume 1294/1997, 410-424, DOI: 10.1007/BFb0052252

[2] Daniel R. Cloutier. Mapping the discrete logarithm. Senior thesis, Rose-Hulman Institute of Technology, 2005.

[3] Philippe Flajolet and Andrew Odlyzko. Random Mapping Statistics. *Advances in Cryptology, Proc. Eurocrypt'89*, J-J. Quisquater Ed., *Lect. Notes in Comp. Sc.* vol 434, 1990, pp. 329-354.

[4] Andrew Hoffman. Statistical Investigation of Structure in the Discrete Logarithm, Rose-Hulman Undergraduate Mathematics Journal, Vol. 10, Issue 2, 2009.

[5] Nathan W. Lindle. A Statistical Look at Maps of the Discrete Logarithm. Senior thesis, Rose-Hulman Institute of Technology, 2008.