[[1]](#footnote-1)

Significantly improving the homomorphic secret sharing scheme in the voter model

Ben Jones, Ethan Mines, Philip Speegle

*Abstract*—This paper describes a recent alternative to Fully Homomorphic Encryption, called Homomorphic Secret Sharing. Recent developments in homomorphic secret sharing have led to more secure and efficient schemes. These recent developments are simulated in the context of secure voting.

# INTRODUCTION

I

n this paper, we implement improvements to Homomorphic Secret Sharing (HSS) schemes to secure voting. HSS Schemes were first introduced in 2016 by [1]. We begin with a high-level comparison of HSS schemes with their predecessors, Fully Homomorphic Encryption (FHE) and Function Secret Sharing (FSS). This comparison provides clarity and context that highlight the benefits that HSS provides in relation to the others. In particular, we consider the improvements that [2] make to existing HSS schemes, and apply them to voting. We construct an implementation of the ElGamal cryptosystem, which will be used as a major basis element in the implementation of the HSS algorithms.

## Homomorphic Encryption

Homomorphic encryption allows a user to perform operations on encrypted data without decrypting it [3]. An example use case of this is secure cloud computation. With homomorphic encryption, Alice could encrypt her financial data and upload it to a remote server, owned by Bob. Bob could then sum the numbers in the financial data, without knowledge of what the numbers are. Bob then sends back the encrypted result, which is finally decrypted by Alice. In this case, Alice is the only entity that knows the plaintext, but Alice was able to outsource her computation to Bob.

In [3], Gentry categorizes homomorphic encryption schemes into several classes. Two examples of these are the partially homomorphic and fully homomorphic. In a partially homomorphic cryptosystem, the user is able to perform precisely one operation on the encrypted data, such as addition or multiplication. In contrast, fully homomorphic encryption (FHE) allows the user to do arbitrary computation. In 2009 and after being an open problem since 1978, Craig Gentry proposed the first viable FHE scheme in [3].

One way to formalize the concept of FHE is to create a scheme ℰ with an algorithm Eval that can evaluate an arbitrary logical circuit C, with algorithms Encrypt and Decrypt for encrypting data and decrypting it, respectively. Gentry accomplished this with a concept called “bootstrapping.” A scheme ℰ is bootstrappable whenever the evaluation algorithm can compute the decryption algorithm Decrypt and an augmented NAND gate. From this, Gentry proves that you can create a complete set of circuits [3]. Finally, he constructs a bootstrappable scheme.

## Function Secret Sharing

This subsection summarizes the seminal paper on function secret sharing in a format that will be used to compare FSS to HSS. The full details can be found in [4].

A function secret sharing scheme splits a function into secure "shares" such that certain subsets of the shares cannot be recombined to give an advantage in computing the original function.

More precisely, an FSS scheme has 6 components. The first is a set of p parties, denoted [p] who will receive the shares. The second is a subset T of [p] that are adversaries. The third is a class of functions, ℱ, containing our eventually secret function. The fourth is an output decoder algorithm, Dec, that takes the shares as inputs and decodes it as a single output. This is usually a sum function. The fifth is a key generation algorithm Gen that generates the p “keys” or “shares” for the input function, according to a security parameter constraint. The sixth and final component is an evaluation function, Eval, that evaluates each function share.

The FSS is also subject to a correctness and security constraint. The correctness constraint rigorously states that with probability 1, the decoder algorithm operating on the shares generated from a function, f, will return the same value as f. The security constraint for

## Overview of Homomorphic Secret Sharing

Homomorphic secret sharing was originally conceived as a dual to function secret sharing, which splits the *program* rather than the inputs into shares [1], [4]. Of the variants of homomorphic secret sharing described in [1], we use *Distributed Evaluation Homomorphic Encryption*, which allows multiple clients to send shares of inputs to two servers [1], [2].

Our Distributed-Evaluation Homomorphic Encryption scheme consists of 5 parts,

1. An algorithm Gen(1λ) that generates the public and secret keys, pk and (ek0,ek1) respectively, with securityparameter1λ∈{0,1}λ.
2. An algorithm Share that outputs encrypted, additives hares of a ciphertext, using the keys from Gen.
3. An algorithm Eval that each server uses to run a program on the encrypted data. In this case, the programs will be voting programs, although it applies to a much broader class of programs.
4. In algorithm Dec that each client, in this case voters, are able to use to decrypt the result from Eval. In our implementation, this is simply a sum of the additive shares.

They describe three different ``levels'' of encoding [2]. The first is ElGamal encryptions of the inputs [2]. The second is additive shares in which, given a variable where . The third are multiplicative shares in which, given a variable where . These notions can of course be generalized to cases with servers where each share vector has components [5].

Restricting ourselves to the current case of , each clients splits its input into additive shares and sends one share to each server [2]. Each server must then perform an evaluation of its share such that given evaluations is equivalent to the computation desired by the clients.

For these “subprograms” executed by the servers, [2] permit only four types of instructions:

* Load input:
* Add variables:
* Multiply variable by input:
* Output result:

The circumflex mark denotes that for each input and variable , an individual server does not have the actual value of this variable, but rather an additive share of it [1]. Note that additive shares are homomorphic over addition [2]; that is, given with and a similar :

This formalism is known as Restricted Multiplication Straight-Line Programs (RMS) [1]. Do note that since we cannot multiply two memory locations , this formalism does not cover arbitrary boolean circuits.

Now, the multiplication instruction temporarily creates multiplicative shares, but these are then converted back to additive ones with some probability of error [1]. During computations by the servers, multiplicative shares of a program variable must sometimes by converted to additive ones [2]. This is done via a probabilistic procedure known as DistributedDLog that relies on a pseudorandom function. If each of the two servers call the procedure on their multiplicative share , they each receive a new additive share such that . Since this is a probabilistic procedure, the outputs fail to be correct additive shares with probability at most , where is a parameter that can tweaked such that lower values of result in longer runtimes of the procedure. This is the primary limiting factor of the size of programs executed by the servers: error may accumulate by repeated calls to DistributedDLogn [1].

Because these instructions maintain the invariant that every variable is represented as an additive share [1], it is easy to reconstruct the actual result from the servers' individual outputs: given sharing , we have

# Gen: Simple ElGamal Cryptosystem

The ElGamal cryptosystem is an asymmetric cryptosystem making use of a public key and a single-use private or `ephemeral key.'

One of its variants is homomorphic with respect to addition, making it a suitable candidate for Homomorphic Secret Sharing.

## Key Generation and Encryption

Consider a voting system where there are questions and two options for each question, {0,1}. Let denote the set of all possible permutations of options chosen given that all the questions were answered. Then, we define the bijective map which maps each coefficient of to the chosen option for question . Note that this bijection implies that there are possible outcomes for a vote. For a quick example, let . Then, the eight possible outcomes are . It will be advantageous to utilize the fact that all elements of can be written in binary by only using their coefficients. As such, we seek a group order such that .

## The Group G

The hypotheses in [1] require that the group G be cyclic of prime order. In this subsection, we compare the usage of different groups G, not necessarily of prime order, and how they may impact the HSS scheme. We consider groups of order pq,p−1,s= 2pq+ 1,and p, where p,q, and s are primes. We note that [2], [6] establish several groups of prime order that are usable in the context of HSS. After investigating these other groups, we intend to move forward with the groups of order p, because [2] gives some examples that are computationally efficient to implement. These will also be discussed in this subsection. In the current work, we use groups of order p−1. We will see that this is moderately successful. Given that there are known attacks on groups with this construction, we plan to adapt to efficient, large groups of prime order. In spite of this, our groups of orderp−1are able to successfully handle many computations.

### The case for Group Order pq:

Let be a cyclic group of order , where and are primes. Recall that , and the amount of generators of is , where each element in is all for which . Then, the proposed generation algorithm is as follows. First, we randomly generate two distinct prime numbers and , preferably making the product large. Using the Miller-Rabin primality test, large values of primes can be found easily. Without loss of generality, assume . Compute and let . Randomly choose an integer until is sufficient such that . The following results show that, for sufficiently large and , the time this takes is essentially negligible.

**Proposition II.1.** Let .Then,

where is Euler’s Totient function.

*Proof.* It is well-known that is a multiplicative homomorphism, so we have . The primality of both and implies and , and the result trivially follows.□

**Remark:** Indeed, is quite close to itself. This notion is rigorized in the following theorem:

**Theorem II.1.** Let where for two distinct primes . Then, with probability.

*Proof.* Consider . Since and are both prime, . For all integers . So the amount of possible generators for is surely since we require We sample a total of elements, so the probability of choosing a generator is , as desired.□

We claim that this probability is sufficiently large to guarantee a generator very quickly. The probability that the algorithm fails times in succession is

, (1)

since each trial is independent. Indeed, even if is minimized (), the probability of failing to generate 3 times is less than . After this, we randomly choose and let . Since is cyclic, the possible values for is (we remove the identity). We denote as our public key, and the value is the private key. It is important to note, however, that keeping close to will achieve more desirable probablistic results than fixing and making large. The reason for this is due to the fact that and vice versa.

After the key generation, a second party will encrypt a message using the public key generated by the above algorithm. We choose an integer and compute the *shared secret* denoted by . The cyphertext is computed by and . The ciphertext is then sent back to the first party. Finally, it is important to note that this method of encryption is fully reliant on the Diffie-Hellman problem being NP-hard, as if this were not the case, an attacker could quickly compute given and [6].

### Drawbacks to Group Order pq:

### The case for Group Order p-1:

Here we discuss using the group , the multiplicative group modulo a prime p. This group has order p−1, since p is prime and gcd(p,g) = 1for all nonzero g∈. We now discuss how to find a candidate generator.

The number of generators in this group is φ(φ(p)) =φ(p−1) [8]. This means that there is always a generator for this group. A randomized approach to searching for generators has a probability of succeeding of φ(p−1)/p−1. It has been shown that

and hence that in infinitely many cases φ(n)is arbitrarily close to n. This suggests that the desired probability is quite large, and a randomized approach may be successful.

However, an iterative solution may be similarly efficient and is deterministic. It is shown in [9] that an upper bound on the smallest generator modulo p Is O(log6(p)), which is very fast asymptotically.

First, we factor φ(p) =p−1. While factoring large numbers is difficult, we are guaranteed that 2|p−1, since p is odd. This allows us to more rapidly find the prime factors of φ(p).Then, given the prime factors p1,...,pk, we consider . If g generates the group, then |g|=p−1, and so since (p−1)/pi < p−1, we have that

Now if g does not generate the group, it must have some finite order k dividing (p−1), by Lagrange’s Theorem. Then there exist pj, c such that p−1 =k·pj·c, and so(p−1)/pj=k·c. This implies that for some j, . Then since k=|g|, we have . Therefore, if g is not a generator, then will be equivalent to 1 mod p for some prime pj dividing (p-1). This gives us a test for if any given element $g$ is a generator of .

### Drawbacks to Group Order p-1

Unfortunately, this relies on the ease of factoring p−1. However, if p−1 is factored easily, then [10] shows that we have violated the primary cryptographic assumptions of HSS, called Decision Diffie Hellman (DDH)[2], and hence we have lost all security of the protocol.

### The case for

The case where, for some prime s= 2pq+ 1 and p,q are prime is similar to the above case where we take . This approach, however, seeks to combat the issues raised with DDH. Since we start with primes p,q, we know that the only small factor of (s−1) is 2, and so it will be much more computationally difficult to factor s−1.

### Drawbacks to

Unfortunately, while we can guarantee that it is more difficult to factor than the general group , we cannot guarantee that it is asymptotically more difficult. In particular, we still violate Decision Diffie Hellman. This case falls into Boneh’s case 1.1.2 [10], where we have p=aq+ 1, p,q prime and a arbitrary, and . In our case, we have a primes= 2pq+ 1, and hence we require both and . This would imply ,which is false for s as small as 5. Hence, we still do not have security.

### The case for Group Order p

It is explained in [6] and [10] that there are multiplicative groups of prime order that do not necessarily violate DDH, but they must be chosen very carefully. The suggested case is p= 2q+ 1, where p and q are both special primes, and in particular p is a pseudo-Mersenne prime such that p≡±1 mod 8, where a pseudo-Mersenne prime takes the form p= −γ [6]. Such primes arecalled “conversion friendly” in [2] and [6], since they make it computationally easy to compute the convert shares procedure. Then by Sylow’s theorems from Group Theory, we know that there exists a subgroup Q of order q in. In this group,every non-identity element is of order q, and hence generates the group.

By Lagrange’s Theorem, we can see that the order of 2∈ is 2, q, or 2q. It cannot be 2, so it must be q or 2q. If it were 2q, then 2 would generate . However, it is impossible for 2j≡1mod n whenever n is even and j >1, so it is not possible for |2|= 2q. Hence,|2|=q. Sylow’s theorems also guarantee that all Sylow q−subgroups are conjugate to each other, orthat for some h. However, since ||= 2q,we can have at most two such Sylow q−subgroups, simply by counting elements. Then 2 must be in one of them, and furthermore 2 must generate it. Therefore, we have a G such that |G| is prime and a generator, namely 2.

### Drawbacks to Group Order p:

In general, it may be difficult to find a pseudo-Mersenne prime p and also verify that p= 2q+ 1for some prime q. To this end, [2], [2] give explicit conversion-friendly primes and groups that work for HSS, including and . A smaller case, yields p= 7,q= 3, which is useful for verifying correctness.

There are also other multiplicative groups of prime order, namely some groups over elliptic curves. It is noted in [6] that these are not subject to as many optimizations as there are with conversion-friendly primes, and hence that you lose multiple orders of magnitude of efficiency. They did, however ,leave open the problem of optimizing the elliptic curve implementation, which could prove useful under further research. Given the slow speed and difficult implementation, we will not be using elliptic curves.

## Decryption

Decryption is done in the multiplicative group with order . This means that for any element in this group, . This will be useful in the decryption algorithm.

**Proposition II.2.** The shared secret .

*Proof.* Routine. and the result follows. □

As such, with the private key , the first party can find the shared secret. Next, we compute with the main result of this section:

**Theorem II.2.** The inverse **.**

*Proof.* By Proposition II.1, . This implies that . By extension, . As such, . Since , . Finally, since , quick substitution gives . □

With , one can compute the original message by computing , which can be mapped back to the original plaintext.

TABLE I

Simulation Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p | q | Votes | Result | Duration (s) |
| 1433 | 1553 | 0101101111 | 7 | 52.17 |
| 1439 | 2039 | 1000110010 | 4 | 123.89 |
| 1103 | 1801 | 1101111110 | 8 | 76.47 |
| 1447 | 1573 | 0001000011 | 3 | 71.35 |
| 1471 | 1571 | 0111100100 | 5 | 87.18 |
| 1847 | 1879 | 1010101010 | 5 | 228.65 |
| 1033 | 1867 | 0110101011 | 6 | 58.74 |
| 1327 | 1721 | 0100000100 | 2 | 77.43 |
| 1193 | 1553 | 0110011000 | 4 | 76.00 |
| 1187 | 1619 | 1111010100 | 6 | 61.62 |

## Additive Homomorphism

The key aspect that makes this variant of ElGamal useful is that multiplication in the ciphertext space is equivalent to addition in the plaintext space [7]. Given encryptions of messages and , we have

which is a valid ElGamal encryption of input .

# Simple ElGamal Results

Before implementing a full homomorphic secret sharing scheme, we pilot a simple voting application using an ElGamal cryptosystem, reminiscent of that of [7]. We implement the simulation in Python3, with all keys and primes being generated by the “secrets” module. We have clients each cast a binary vote . We perform ten iterations of this, noting the correctness of the output and the runtime in Table I.

# Share

## AdditiveShare

This routine generates a tuple denoted< x >= (x0,x1)such that in Zq, x0= x1+x. This is done by choosing a cryptographically random 0≤x0< x and setting x1=x−x0.

# Evaluation Algorithm eval

In this section, we describe in more detail the procedures in Eval as presented in [1]. We will assume for this section that we have access to a multiplicative cyclic group G of prime order q and generator g∈G. The Homomorphic Secret Sharing scheme also requires a security parameter, λ, which we will use liberally. There are 3 primary functions, additiveShare, multShares, and convertShares.The additive share Theseprimary functions make frequent use of a subroutine calledthe Distributed Discrete Logarithm, or DistributedDLog and aPseudo-Random Function (PRF)

# Next Steps

Mimicking most of the examples given in [2],[1], we let the number of servers be with indices . As in an ElGamal cryptosystem, we find a cyclic group generated by [1]. We choose a secret key of bits and let the public key be

,

where is used for encryption and the latter components are the ElGamal encryptions of the individual bits of the secret key (still using the entire as the key)[1]. Likewise, each of the two servers received an evaluation key

where the additive share indicates the index of the server and is the server's additive share of the secret key.

We first intend to do a simple tally of binary votes of clients, with representing “yes” and representing “no.” Consequently, if one client votes “no,” his additive share would be , since [2]. Likewise, if another client votes “yes,” his additive share would be or [2]. As with our earlier test of the ElGamal cryptosystem, we take advantage of the fact that multiplication in the ciphertext space is equivalent to addition in the plaintext space [7]. This time, however, each of the two servers performs a separate product.

Each server receives inputs , each of which corresponds to one of the n clients. We first load each input into memory:

In this precise variant of HSS, rather than load input directly into memory, we multiply it by a symbolic constant . This constant is shared between the servers in the same way that any other input or variable is [1].

Following this, we perform a cumulative sum over the variables:

Finally, each server outputs its personal product:

Thus, the program is exactly instructions according to the RMS formalism.

References

1. E. Boyle, N. Gilboa, and Y. Ishai, “Breaking the circuit size barrier for secure computation under ddh,” *Advances in Cryptology – CRYPTO 2016 Lecture Notes in Computer Science*, p. 509–539, 2016.
2. E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, and M. Orr`u, “Homomorphic secret sharing: optimizations and applications,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*,2017, pp. 2105–2122.
3. C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing,* ser. STOC ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 169–178.
4. E. Boyle, N. Gilboa, and Y. Ishai, “Function secret sharing,” in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2015, pp. 337–367.
5. E. Boyle, N. Gilboa, Y. Ishai, H. Lin, and S. Tessaro, “Foundations of homomorphic secret sharing,” *Innovations in Theoretical Computer Science,* 2018.
6. D. R. L. Brown and R. P. Gallant, “The static diffie-hellman problem,” 2004.
7. R. Cramer, R. Gennaro, and B. Schoenmakers, “A secure and optimally efficient multi-authority election scheme,” *European Transactions on Telecommunications*, vol. 8, 10 2000.

1. [↑](#footnote-ref-1)