Statistically Secure One Multiplication and Additions of Secret Shares

by

Daniel Berend, Dor Bitan, Shlomi Dolev

Technical Report #17-01

January 25, 2017

The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel.

Statistically Secure One Multiplication and Additions of Secret Shares

(Preliminary version)

Daniel Berend[1,2], Dor Bitan[1], Shlomi Dolev[2]

[1]Department of Mathematics, Ben-Gurion University
[2]Department of Computer Science, Ben-Gurion University

Abstract

One of the most interesting research topics in cryptography is finding schemes for an efficient fully-homomorphic encryption (FHE), preferably information-theoretically secure schemes, which are not based on unproven computational hardness assumptions. The greatest breakthrough in the field of FHE schemes was made by Gentry [7] in 2009, and since then there were some interesting developments, e.g. Boneh et al. [13] and Barkevski and Perlman [16]. All currently known FHE schemes have computational security and are time-wise inefficient.

We suggest here an information-theoretically secure secret sharing scheme of restricted values that supports one homomorphic multiplication of secrets and homomorphic additions of, practically, any number of such multiplied secrets. In particular, our scheme enables sharing secrets amongst $n+1$ participants, using polynomials of degree n, in such a way that no information is revealed to any single participant, both before and after the above series of operations. Moreover, for the case $n = 3$ we prove that any coalition of two participants will be able to reveal only limited information concerning the secrets: when the secrets are elements of $\mathbb{F}_p$, then every value for $(s_1, s_2) \in \mathbb{F}_p^2$ is possible with probability $\approx \frac{1}{p^2}$, except for a small portion of values that are possible with probability $\approx \frac{2}{p^2}$.[1] One possible application of our scheme is a secure homomorphic evaluation of multi-variant quadratic functions and 2-CNF circuits.

1 Introduction

Cryptographic schemes can be divided into two types, according to the security of the system. The first type is *information-theoretical security*. In information-theoretically secure schemes the security of the system does not depend on the computing power of the adversary, is not based on any computational hardness assumption, and is derived purely from information theory. It is possible that in such schemes some information about the plaintext will be revealed to an adversary by the ciphertext, but that leakage of information can be accurately measured by statistical tools. That is why information-theoretically secure schemes, on which there is some leakage of information, are often called *statistically information theoretic secure*, or simply *statistically secure*. Information-theoretically secure systems on which there is absolutely no leakage of information are called *perfectly secure* schemes. Those schemes constitute a very important class of cryptographic schemes, on which, not only will any adversary be unable to decrypt an encrypted message, but it will gain *absolutely no information* about the plaintext from the ciphertext. The second type of security is *computational security*, and it refers to cryptographic schemes that are based on computational hardness assumptions. Specifically, a certain function f is assumed to be easy to compute but hard to invert, then used to build a cryptographic system, such that, breaking the system is strongly related to inverting f. The security of those schemes is based on two unproven assumptions: (a) there is no efficient algorithm that inverts f, (b) the adversary does not have enough computing power to break the system in reasonable time. Therefore, if an information theoretically secure scheme provides certain performances, it will be preferred over a computationally secure scheme that provides similar performances. Even though, computationally secure cryptographic schemes are considered reliable for many uses, often providing great performances, and are in very common use.

Secret sharing is a fundamental cryptographic primitive on which shares of a secret value are distributed to a set of participants in such way that only authorized sets of participants can reconstruct the secret, while unauthorized sets can neither find the secret nor gain information about it. The set of all authorized subsets of participants is called *the access structure* of the scheme. An access structure is of course closed under containment (a set containing authorized set is also authorized) and can be defined by its minimal authorized subsets. Since secret sharing was first introduced by Shamir and Blakley (independently) in 1979, it is a very active field of research in cryptography. In Shamir's secret sharing scheme [9] the secret s is an element of the finite field $\mathbb{F}_p$ (where $p > n+1$) and is shared by a *dealer* amongst a set of $n+1$ participants in the following way. Each participant P_i, $1 \le i \le n+1$, is assigned by the dealer with an element α_i of $\mathbb{F}_p^\times$, where the α_i's are pairwise distinct. Random elements a_j of $\mathbb{F}_p$, $1 \le j \le t$ are picked by the dealer and the following polynomial is defined: $f(x) = s + \sum_{j=1}^{t} a_j x^j$, then the value $f(\alpha_i)$ is distributed to participant P_i. It was proved by Shamir [9] that, in this way, any group of $t+1$ participants will be able to reconstruct s, but no group of t participants gains any information about s. These properties are derived directly from the fact that a polynomial of degree t is uniquely determined by its values at $t+1$ points. Shamir's secret sharing scheme is one of the most influential schemes [1,2,3,4,5,6], as it is perfect information-theoretically secure. As we have mentioned, secret sharing is a very active field of research for almost the last four decades. Some of the research topics of it are: finding schemes for general access structures, finding verifiable schemes, reducing the size of the shares, constructing secret-sharing-based cryptographic primitives, and finding schemes with homomorphic properties. Our research focuses on the last topic. We now describe the main ideas concerning homomorphic secret sharing. Assume $s_1, \ldots, s_d$ are secrets that were shared amongst a set of par-

[1]That is when the secrets are chosen randomly. When the secrets are chosen according to any other distribution Γ, the statistical difference between: (a) the distribution induced by any pair of secrets over the information held by the coalition, and (b) the uniform distribution over that information, is no more than $\frac{1}{p}$.

* This research was partially supported by the Rita Altura Trust Chair in Computer Sciences; the Lynne and William Frankel Center for Computer Sciences; grant of the Ministry of Science, Technology and Space, Israel, and the National Science Council (NSC) of Taiwan; the Ministry of Foreign Affairs, Italy; the Ministry of Science, Technology and Space, Infrastructure Research in the Field of Advanced Computing and Cyber Security and the Israel National Cyber Bureau.

ticipants $P_1, \ldots P_{n+1}$. Each participant, P_j, is holding a share of each of the secrets, denoted: $s_{1_j}, \ldots, s_{d_j}$. If P_j can use the shares it is holding to construct a value denoted $(s_{add})_j$, such that it is a share of $s_{add} = \sum_{i=1}^{d} s_i$, and such that s_{add} can be reconstructed by an authorized set, then the scheme is *additively homomorphic*. Similarly, the scheme is *multiplicatively homomorphic* if $s_{1_j}, \ldots, s_{d_j}$ can be used by P_j to construct a share of $s_{mult} = \Pi_{i=1}^{d} s_i$, denoted $(s_{mult})_j$. If a scheme is both additively homomorphic and multiplicatively homomorphic, it is *fully homomorphic*. If a scheme supports arbitrary homomorphic additions and a bounded number of homomorphic multiplications [2] then it is *somewhat homomorphic*. Such homomorphic properties of cryptographic systems are very important attributes. One important property of Shamir's scheme is that it is additively homomorphic. This property is based on the fact that the sum of polynomials of degree $\leq t$ is again such a polynomial of degree $\leq t$. Unfortunately, Shamir's scheme is not multiplicatively homomorphic due to the fact that the product of two polynomials of degree $\leq t$ is in general of a higher degree. As the degree of the polynomial gets larger, more participants are required in order to extract the secret.

Homomorphic properties are important attributes not only of secret sharing schemes but also of general cryptographic schemes. In particular, assume π is a cryptographic system, m is a message and c is its encryption, denoted $Enc_\pi(m)$. And assume f is a function defined over the message space of π. How, if anyhow, can c be publicly converted into an encryption of $f(m)$? This interesting question is a main subject of research in cryptography almost for the last four decades. If we assume that the messages and the ciphertexts are elements of a field or a ring (and so it is in many cases), then a more specific form of that question will be as follows. Let $m_1, \ldots, m_d$ be two messages, and let $c_1, \ldots, c_d$ be their encryptions (for now, d can be arbitrarily large). How, if anyhow, can $c_1, \ldots, c_d$ be used to publicly create c, such that $c = Enc_\pi\big(\sum_{i=1}^{d} m_i\big)$ or $c = Enc_\pi\big(\Pi_{i=1}^{d} m_i\big)$? If it is possible to use $c_1, \ldots, c_d$ to publicly create $c_{add} = Enc_\pi\big(\sum_{i=1}^{d} m_i\big)$, respectively, $c_{mult} = Enc_\pi\big(\Pi_{i=1}^{d} m_i\big)$, then we say that π is *additively homomorphic*, respectively, *multiplicatively homomorphic*. If both tasks can be carried out then we say π is a *fully homomorphic encryption* (FHE) system. There are several single-operation homomorphic schemes, such as the RSA cryptosystem, which is multiplicatively homomorphic (but cannot support homomorphic additions at all[3]), and Shamir's secret sharing scheme, which is additively homomorphic (but cannot support homomorphic multiplications at all).

A mid-step between single-operation homomorphic encryption systems and FHE systems are *somewhat homomorphic encryption systems*. These systems are additively homomorphic systems that can also support one homomorphic multiplication (or multiplicatively homomorphic systems that can also support one homomorphic addition). To make this concept clear we can modify the above definitions. Instead of taking d to be arbitrarily large, define a cryptographic system to be d_1-*additively homomorphic* if its additively homomorphic for $d \leq d_1$, and d_2-*multiplicatively homomorphic* if its multiplicatively homomorphic for $d \leq d_2$. Then, additively homomorphic systems are ∞-additively homomorphic and multiplicatively homomorphic systems are ∞-multiplicatively homomorphic.

Finding FHE schemes was called the holy grail of cryptography. The first to propose a computationally secure FHE method was Gentry [7]. Unfortunately, the time complexity of the current implementations of it is too high to make the scheme practical. Sander et al. [14] proposed a system to evaluate NC^1 circuits on encrypted values, considering the following case: Alice holds an input x and Bob is holding a circuit C. Alice should get $C(x)$, while keeping her input x private, and Bob keeping his circuit C private as well. A main drawback of the system is that the ciphertext length grows exponentially in the depth of the circuit [13]. Their system is based on random self-reducible probabilistic encryption, which might be either computationally or information theoretically secure. Either way, under the suggested protocol, Alice's input is computationally private, while Bob's circuit remains information theoretically private. Rabin and Ben-Or [15] suggested a verifiable secret sharing scheme, on which a secret is shared amongst a group of participants in a way that the secret can be extracted by a sufficiently large set of participants, even if some of them are malicious, as long as the majority of them are honest. The results are information theoretically secure, with exponentially small error probability. A protocol for multi-party computation is also suggested in [15], but it requires ongoing communication between the participants. Carmer, Damgard and Maurer [1] suggested a way to construct a multi-party computation protocol based on any linear secret sharing scheme. Some of their results are information theoretically secure, while others assume the existence of trapdoor one-way permutation, or the computation hardness of a certain function, based on the Diffie-Hellman encryption system. Either way, their protocols require ongoing communication between the participants proportionally to the depth of the arithmetic circuit. Specifically, when regarding Shamir's secret sharing scheme, a multiplication of secrets is possible only if the encrypting polynomials are taken to be of smaller degree to begin with. Dolev et al. [6] used the standard Shamir's scheme for information theoretically secure multi-party evaluation of RAM programs, where the parties obliviously run a given RAM program over given input. Their solution is based on secure multi-party computation and requires ongoing communication between parties and an external entity called *reducer*, and hence implies high overhead. Boneh et al. [13] proposed a computationally secure public key encryption scheme and showed how it can be used to evaluate 2-DNF circuits over ciphertexts. Their scheme is somewhat homomorphic as it is additively homomorphic and 2-multiplicatively homomorphic. Barkevski and Perlman [16] achieved a computationally secure FHE scheme that can be carried out by an unbounded number of participants. They used the multi-key approach and achieved a scheme with fully dynamic properties, O(N) ciphertext expansion, and O(N) space complexity for an atomic homomorphic operation, where N is the number of parties whose ciphertexts have been introduced into the computation so far, and inputs from more participants can join the computation later. Unfortunately, their results are only theoretical and their scheme is not practical.

This is the place to make an important distinction regarding FHE properties of different types of cryptographic systems. Above we defined a cryptographic system π to be a FHE system if a ciphertext $c = Enc_\pi(m)$ can be used to publicly create an encryption of $f(m)$ for given f. This definition is similar to the one we gave regarding fully homomorphic secret sharing systems. The main difference between the two definitions is that, while in a private/public key encryption systems the ciphertext c is being held by a single entity, in a secret sharing scheme the encryption of m is distributed amongst a set of participants.

[2] Or arbitrary homomorphic multiplications and a bounded number of homomorphic additions.

[3] and is computationally secure

Moreover, we do not really think of the set of all shares as an encryption of m, since when being held together, they contain all the information needed to extract m. The shares of m can be regarded as an encryption of it only if being held by different entities, or by sets that are not in the access structure of the scheme.

Regarding this last distinction, and to conclude, given a cryptographic scheme, four questions can be asked:

1. Is the encryption of a message can be held by a single entity, or is it distributed to several machines?
2. Is the scheme fully homomorphic, somewhat homomorphic, single-operation homomorphic or not supporting any homomorphic operations?
3. Is the scheme information theoretically secure or computationally secure?
4. Is the scheme practical?

No system is known that satisfies all the above requirements. Fully homomorphic systems with a single ciphertext holder, such as Gentry's and Barkevski and Perlman's, are neither information theoretically secure, nor practical. No information theoretically secure scheme is fully homomorphic, and no practical scheme is fully homomorphic. The scheme suggested by Boneh et al. is a single-entity, somewhat homomorphic, computationally secure and practical scheme.

1.1 Our contribution

The main result we obtain on our research is a novel procedure we found which we call *function sieving*. That procedure yields pairs of 1-*homomorphic multiplicative polynomials*, which enable us to adjust Shamir's secret sharing scheme to support one homomorphic multiplication of shares, keeping it perfectly secure against an attack of a single curious participant. For the case $n = 3$ we also prove our scheme to be statistically secure against an attack of a coalition of two curious participants, with statistical difference of no more than $\frac{1}{p}$. Of course, one can use Shamir's original scheme to share two secrets amongst four participants using linear polynomials, enabling one multiplication, but in this way, any group of two participants can easily determine the exact value of the secrets. In our scheme any subgroup of two participants cannot find the secrets, and all options for $(s_1, s_2) \in \mathbb{F}_p^2$ are possible in almost the same probability. Our novel scheme is based on a sophisticated way of choosing the polynomials in a correlated way. On account of the four questions we have stated above, the scheme we suggest is:

1. A secret sharing scheme, such where, an encryption of a message is distributed to several machines.
2. Somewhat homomorphic, as we support one (restricted) multiplication and consecutive additions.
3. Information theoretically secure, with perfect security against a single curious participant attack, and statistical security against an attack of a coalition of two curious participants (for $n = 3$).
4. A practical scheme.

Organization. In section 2 we introduce the function sieving method and our scheme for secret sharing and multiplication of two secrets amongst $n + 1$ participants using polynomials of degree n. In section 3 we prove the correctness of the scheme and discuss the security of it against an attack of one curious participant and, for the case n=3, against an attack of a coalition of two curious participants. In section 4 we discuss possible applications of the scheme. Section 5 is conclusions. Detailed proofs for some of the propositions appear in appendix.

2 Homomorphic Multiplication of Secret Shares

In this section we introduce our secret sharing scheme, based on Shamir's scheme, that will enable us to share two secrets amongst $n + 1$ participants using polynomials of degree n, perform one homomorphic multiplication of the secrets and consecutive homomorphic additions with further secrets, without increasing the number of participants required to extract the result. As we will show here, our scheme has perfect security against an attack of a single participant, and is not based on any computational hardness assumption. For the case $n = 3$ we also prove that our scheme has statistical security.

We begin with a brief overview of our methods and constructions. Assume s_1 and s_2 are two secrets that were secret shared by Shamir's scheme amongst $n + 1$ participants, P_j, $1 \le j \le n + 1$, using two polynomials of degree n, f_1 and f_2, respectively. Each participant is holding a share of each of the secrets: $\big(\alpha_j, f_1(\alpha_j)\big)$ and $\big(\alpha_j, f_2(\alpha_j)\big)$. As Shamir's scheme is additively homomorphic, the points $\big(\alpha_j, f_1(\alpha_j) + f_2(\alpha_j)\big)$ are shares of $s_1 + s_2$. Interpolation of them will yield the unique polynomial of degree $\le n$ going through them, which is $f_1 + f_2$, whose value at 0 is $s_1 + s_2$. Now, as Shamir's scheme is not multiplicatively homomorphic, in general, the points $\big(\alpha_j, f_1(\alpha_j) \cdot f_2(\alpha_j)\big)$ are not shares of $s_1 \cdot s_2$. The polynomial $f_1 \cdot f_2$ is of degree $\le 2n$, hence, $2n + 1$ points are required to determine it, and obviously the $n+1$ we have will not suffice. If one insists on interpolating the points $\big(\alpha_j, f_1(\alpha_j) \cdot f_2(\alpha_j)\big)$, that interpolation will yield some polynomial g of degree $\le n$. It might be the case, though, that $g(0) = s_1 \cdot s_2$. When does it happen? We seek for a set of pairs of polynomials to be used with Shamir's scheme that yield $g(0) = s_1 \cdot s_2$. We call this procedure *function sieving*, and it yields pairs of 1-*homomorphic multiplicative polynomials*, which are pairs of polynomials that meet the required condition. We will show that, given the α_j's, these pairs are independent of the secrets and can be determined according to the other coefficients of the polynomials (i.e., all coefficients except for the free terms, which are the secrets).

2.1 Function Sieving

Assume one has two secrets $s_1, s_2 \in \mathbb{F}_p$, where $p \equiv 1 \pmod{n+1}$. In that case, $\mathbb{F}_p$ contains a primitive root of unity of order $n + 1$. Let α be that element. For $1 \le j \le n + 1$ denote $\alpha_j := \alpha^j$. Let P_j, $1 \le j \le n + 1$, be a set of participants for a secret sharing scheme, and assign the value α_j to participants P_j. For $i \in \mathbb{N}$ let ε_i be the sum of all products of i distinct α_j's. Namely, for a $A \subseteq \mathbb{F}_p$ denote $\varepsilon_A := \prod_{\alpha \in A} \alpha$, then $\varepsilon_i = \sum_{|A|=i} \varepsilon_A$, where $A \subset \{\alpha_1, \ldots, \alpha_{n+1}\}$. Since the α_j's are roots of unity we have $\sum_{j=1}^{n+1} \alpha_j^k = 0$ for $1 \le k \le n$. It implies that $\varepsilon_1 = \cdots = \varepsilon_n = 0$. Denote $\psi(x) = \Pi_{j=1}^{n+1}(x - \alpha_j)$. Opening the brackets one has $\psi(x) = \sum_{i=0}^{n+1} (-1)^i \varepsilon_i x^{n+1-i}$, where we denote $\varepsilon_0 = 1$. Since the ε_j's are zeros (for $1 \le j \le n$) one simply has $\psi(x) = x^{n+1} + (-1)^{n+1} \varepsilon_{n+1}$.

Now, let $f_1(x) = s_1 + \sum_{i=1}^{n} a_i x^i$, $f_2(x) = s_2 + \sum_{i=1}^{n} b_i x^i$, two polynomials in $\mathbb{F}_p[x]$. Share the secrets s_1, s_2 amongst the set of participants P_j using f_1, f_2. Namely, distribute to participant P_j the values $f_1(\alpha_j), f_2(\alpha_j)$. Let $y_j = f_1(\alpha_j) \cdot f_2(\alpha_j)$. The pairs $(\alpha_j, y_j) \in \mathbb{F}_p^2$ are $n + 1$ distinct points such that the polynomial $(f_1 \cdot f_2)(x)$ is going through them. As mentioned

above, the polynomial $f := f_1 \cdot f_2$ is of degree $\leq 2n$, hence, $2n+1$ points are required to determine it. However, let $g(x)$ be the polynomial obtained by interpolation of the $n+1$ points we have, (α_j, y_j). Obviously g is of degree $\leq n$. Since f and g agree on the roots of ψ we see that $g(x) \equiv f(x) \pmod{\psi(x)}$. Observe that since $\psi(x) = x^{n+1} + (-1)^{n+1}\varepsilon_{n+1}$, $g(x)$ is easy to compute. Denote $f(x) = s_1 s_2 + \sum_{i=1}^{2n} c_i x^i$. Modulo ψ we have $x^{n+1} = (-1)^n \varepsilon_{n+1}$, then $g(x) \equiv f(x) \pmod{\psi(x)} = s_1 s_2 + c_{n+1}(-1)^n \varepsilon_{n+1} + \sum_{i=1}^{n} d_i x_i$, for $d_i = c_i + c_{n+1+i}(-1)^n \varepsilon n + 1$. That in turn implies that $g(0) = s_1 s_2 + c_{n+1}(-1)^n \varepsilon_{n+1}$. So now we see that if we take f_1 and f_2 such that $c_{n+1} = 0$ we get $g(0) = f(0)$. c_{n+1} is easy to compute, as it is the sum products $a_j b_{n+1-j}$. So instead of picking the coefficients for f_1 and f_2 uniformly we can pick them in such a way that $c_{n+1} = 0$. That is, in essence, the function sieving process. Instead of using Shamir's secret sharing scheme with random polynomials from the ring $\mathbb{F}_p[x]$, we sieve $\mathbb{F}_p[x]$ and use specific polynomials of it that make $g(0) = f(0)$. We call such (f_1, f_2) a pair of 1-homomorphic-multiplicative-polynomials. We define the set of coefficients for such pairs

$$\mathcal{V}_p := \left\{ (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbb{F}_p^{2n} \;\middle|\; \sum_{i=1}^{n} a_i b_{n+1-i} = 0, \right.$$
$$\left. (a_1, \ldots a_n) \neq \overline{0} \neq (b_1, \ldots b_n) \right\} \cup \left\{ \overline{0} \in \mathbb{F}_p^{2n} \right\}.$$

In this point, the reader might rightfully ask where did the further conditions came from. Meaning, why we omit $2n$-tuples with $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, and why is $\overline{0} \in \mathbb{F}_p^{2n}$ allowed? As we will show, these are necessary requirements to achieve perfect security against a single participant attack.

Next, since elements should be picked from $\mathbb{V}_p$ we must define probability over it. First we compute its cardinality.

Proposition 1: $|\mathcal{V}_p| = (p^n - 1)(p^{n-1} - 1) + 1$.

Proof: The element $\overline{0} \in \mathbb{F}_p^{2n}$ contributes 1 to $|\mathcal{V}_p|$. The n-tuple $(a_1, \ldots, a_n)$ may be chosen in $p^n - 1$ different ways. The n-tuple $(b_1, \ldots, b_n)$ satisfies

$$\sum_{i=1}^{n} a_i b_{n+1-i} = 0.$$

Since $(a_1, \ldots, a_n) \neq \overline{0}$, the equation has p^{n-1} solutions. The trivial solution is irrelevant, but each of the other $p^{n-1} - 1$ solutions gives one element for $\mathcal{V}_p$. All in all we get a total of $(p^n - 1)(p^{n-1} - 1) + 1$ elements in $\mathcal{V}_p$. $\square$

We now define a probability Q over $\mathcal{V}_p$. Let

$$Q(v) = \begin{cases} \frac{1}{p^n}, & v = \overline{0} \in \mathbb{F}_p^{2n} \\ \frac{1}{p^n(p^{n-1}-1)}, & \text{otherwise.} \end{cases}$$

One verifies readily, using Proposition 1, that Q is indeed a probability.

2.2 The Scheme

We now present our secret sharing scheme, based on Shamir's scheme. A single homomorphic multiplication between two secrets is supported, to which further secrets can be added homomorphically. In particular, we use a polynomial of degree n to represent each of the secrets, and yet, we are able to reconstruct their product with only $n+1$ participants (versus $2n+1$ that would be needed originally).

Assume a dealer D has two secrets $s_1, s_2 \in \mathbb{F}_p$ and private connection channels with $n+1$ participants P_i, $1 \leq j \leq n+1$. As a preliminary phase, the dealer D assigns to each participant P_j an $\alpha_j \in \mathbb{F}_p^{\times}$ in such a way that $\varepsilon_1 = \cdots = \varepsilon_n = 0$, as we explained above (we can achieve that by taking the α_js to be powers of a suitable root of unity of order $n+1$).

The scheme stages are as follows:

Algorithm 1: Sharing secrets and computing product

1. The Dealer D picks an element $(a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$ according to the distribution Q.
2. D sets $f_1(x) = s_1 + \sum_{i=1}^{n} a_i x^i$ and distributes the value $f_1(\alpha_j)$ to each participant P_j.
3. D sets $f_2(x) = s_2 + \sum_{i=1}^{n} b_i x^i$ and distributes the value $f_2(\alpha_j)$ to each participant P_j.
4. Each participant P_j computes $y_j = f_1(\alpha_j) \cdot f_2(\alpha_j)$ in $\mathbb{F}_p$ and sends y_j to back to D.
5. D finds the unique polynomial $g(x)$ over $\mathbb{F}_p$ that goes through (α_j, y_j), using Lagrange interpolation.
6. D calculates $s = g(0)$.

Regarding stage 1 of the protocol, one simple way to Q-pick suitable element is to create an array with the elements of the set $\mathcal{V}_p$ and insert the element $\overline{0} \in \mathbb{F}_p^{2n}$ into the array $p^{n-1} - 2$ more times. Then, uniformly-picking an element from that array is equivalent to Q-picking an element of $\mathcal{V}_p$. [4] In stage 5, since $1 \leq i \leq n+1$, the polynomial g is of degree $\leq n$.

3 Results

3.1 Correctness

We now prove the correctness of the scheme. Namely, we prove the following proposition:

Proposition 2: *The value s, found at stage 6 of the scheme, is equal to $s_1 \cdot s_2$.*

Proof of proposition 2: The proof follows directly from the function sieving process described above in section 2. The coefficients of the polynomials f_1, f_2 were picked from $\mathcal{V}_p$, hence, $\sum_{i=1}^{n} a_i b_{n+1-i} = 0$. The α_js were picked so that $\varepsilon_1 = \cdots = \varepsilon_n = 0$, hence, $\psi(x) = x^{n+1} + (-1)^{n+1}\varepsilon_{n+1}$. In stage 5 of the scheme the dealer finds a polynomial $g(x)$ of degree $\leq n$ such that $g(\alpha_j) = y_j$ for $1 \leq j \leq n+1$. That implies that $g(x) \equiv (f_1 \cdot f_2)(x) = s_1 s_2 + \sum_{i=1}^{2n} c_i x^i \equiv s_1 s_2 + c_{n+1}(-1)^n \varepsilon_{n+1} + \sum_{i=1}^{n} (c_i + c_{n+1+i}(-1)^n \varepsilon n + 1) x_i \pmod{\psi(x)}$. Hence $g(0) = s_1 s_2 + c_{n+1}(-1)^n \varepsilon_{n+1} \equiv s_1 s_2 \pmod{\psi(x)}$. $\square$

Now, $g(x)$ can be treated as it was originally used to secret share $s_1 s_2$ amongst $n+1$ participants, as each of them is now holding y_j, and further secret shares can be distributed and added now as in the standard scheme of Shamir.

3.2 The Scheme Security

We now analyze the scheme security against curious participants attacks. We will show that our scheme has perfect security against one participant attack. For the case $n = 3$ we will show that our scheme has statistical security against an attack of a coalition of two participants, and compute the statistical difference. To conclude such arguments, first we must make our assumptions clear. We assume the following:

1. The prime p is public.
2. The pair of secrets $(s_1, s_2) \in \mathbb{F}_p^2$ is arbitrary. To be precise, we assume they are picked according to any distribution Γ, on which we have no assumptions. Moreover, the distribution Γ is public. Thus, for each pair $(s_1, s_2) \in \mathbb{F}_p^2$, the probability $P[(S_1, S_2) = (s_1, s_2)]$ is known.

[4] This is a straightforward naive way to Q-pick an element from $\mathcal{V}_p$, because this way we actually run over all p^{2n} elements of $\mathbb{F}_p^{2n}$ and check for each element whether it meets the requirements of the set $\mathcal{V}_p$, and save it in memory. This way is very inefficient, time-wise and memory-wise. We note that there are much efficient ways that we omit for the sake of simplicity.

3. We define the $\mathbb{F}_p$-valued random variables S_1 and S_2 as the values of s_1 and s_2 that the dealer D picks according to Γ.
4. The set $\mathcal{V}_p$ and the distribution Q over it are public.
5. The element $(a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$, that is Q-picked during stage 1 of the scheme, is kept secret.
6. The values $f_1(\alpha_j)$ and $f_2(\alpha_j)$, $1 \leq i \leq n+1$, that D sends to participant P_j at stages 2 and 3 of the scheme, are kept secret by the participants in the single participant attack scenario. Namely, P_j does not know $f_1(\alpha_i)$ and $f_2(\alpha_i)$ for $i \neq j$. In the two participant coalition attack scenario we assume, with no loss of generality, that P_1 and P_2 are curious participants that join their shares in an attempt to find the secrets, but they do not know the shares of the other participants.

3.2.1 Perfect security against single participant attack ($n \geq 2$)

In order to show that our scheme has perfect security against one curious participant attack, we need to show that, when P_j receives information from D during stages 2 and 3 of the scheme, P_j gains absolutely no information about the values of s_1 and s_2. We can summarize the information that P_j receives during stages 2 and 3 of the scheme by the following equations:

$$\begin{aligned} s_1 + \sum_{i=1}^{n} a_i \alpha^i &= y_{1,j}, \\ s_2 + \sum_{i=1}^{n} b_i \alpha^i &= y_{2,j}. \end{aligned} \tag{3.2.1}$$

The unknowns in these equations are s_1, s_2, a_i and b_i, $1 \leq i \leq n$, while all other parameters are known to P_j. We start with the following lemma.

Lemma 1: For $\alpha \in \mathbb{F}_p^\times$ denote $u = \begin{pmatrix} \sum_{i=1}^n a_i \alpha^i \\ \sum_{i=1}^n b_i \alpha^i \end{pmatrix}$. Under the above assumptions, $P[u = \binom{x}{y}] = \frac{1}{p^2}$ for each $\binom{x}{y} \in \mathbb{F}_p^2$.

A detailed proof of Lemma 1 can be found in appendix. We use Lemma 1 to prove the perfect security of our scheme in this scenario. We show now

Proposition 3: $P[(S_1, S_2) = (s_1, s_2) \mid (3.2.1)] = P[(S_1, S_2) = (s_1, s_2)]$.

Proof of Proposition 3: Denote:

$$\theta = P[(S_1, S_2) = (s_1, s_2) \mid (3.2.1)].$$

Explicitly,

$$\theta = P\left[(S_1, S_2) = (s_1, s_2) \middle| \begin{smallmatrix} s_1 + \sum_{i=1}^n a_i \alpha^i = y_1 \\ s_2 + \sum_{i=1}^n b_i \alpha^i = y_2 \end{smallmatrix}\right]$$

We may write

$$\theta = P\Big[(S_1, S_2) = (s_1, s_2) \Big| u = \begin{pmatrix} y_1 - s_1 \\ y_2 - s_2 \end{pmatrix}\Big].$$

Equivalently

$$\theta = \frac{P\Big[(S_1, S_2) = (s_1, s_2) \cap u = \begin{pmatrix} y_1 - s_1 \\ y_2 - s_2 \end{pmatrix}\Big]}{P\Big[u = \begin{pmatrix} y_1 - s_1 \\ y_2 - s_2 \end{pmatrix}\Big]}$$

According to Lemma 1, $P\big[u = \binom{x}{y}\big] = \frac{1}{p^2}$. Hence, the values of u are independent of (S_1, S_2), so we have

$$\theta = \frac{P[(S_1, S_2) = (s_1, s_2)] \cdot \frac{1}{p^2}}{\frac{1}{p^2}} = P[(S_1, S_2) = (s_1, s_2)]$$

□

3.3 Security against coalition of two curious participants for $n = 3$

We now turn to analyze the scheme's security against a coalition of two participants for the case $n = 3$. Without loss of generality, we assume P_1 and P_2 are two curious participants which received shares of the secrets s_1, s_2 from the dealer during stages 2 and 3 of the scheme, and join their shares in order to obtain information about the secrets. We will refer to the coalition of P_1 and P_2 from now on as *the adversary*. As in the preceding scenario, we can summarize the information the adversary is holding by a set of equations:

$$\begin{aligned} a_3\alpha_1^3 + a_2\alpha_1^2 + a_1\alpha_1 + s_1 &= y_{11}, \\ a_3\alpha_2^3 + a_2\alpha_2^2 + a_1\alpha_2 + s_1 &= y_{12}, \\ b_3\alpha_1^3 + b_2\alpha_1^2 + b_1\alpha_1 + s_2 &= y_{21}, \\ b_3\alpha_2^3 + b_2\alpha_2^2 + b_1\alpha_2 + s_2 &= y_{22}. \end{aligned} \tag{3.3.1}$$

As before, the unknowns in these equations are a_i, b_i, s_1, s_2, while all other parameters are known to the adversary. We will now show two significant results concerning this scenario. First, given (3.3.1), all p^2 options for $(s_1, s_2) \in \mathbb{F}_p^2$ are possible. Second, they occur with almost the same probability. We will soon make it mathematically clear by analyzing how the matrix $\begin{pmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{pmatrix}$ is distributed over $M_2(\mathbb{F}_p)$ given a pair of secrets (s_1, s_2), and show that this distribution is statistically close to the uniform distribution over this space.

Let (s_1, s_2) and (s_1', s_2') be two pairs of secrets, and let $Y_{(s_1,s_2)}$ and $Y_{(s_1',s_2')}$ be the $M_2(\mathbb{F}_p)$-random variables indicating the matrices $\begin{pmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{pmatrix}$ induced by (s_1, s_2) and (s_1', s_2'), respectively. We will show that the statistical difference between the distributions $Y_{(s_1,s_2)}$ and $Y_{(s_1',s_2')}$ is at most $\frac{2}{p}$. In order to show that we use the following lemma.

Lemma 3:
Denote $U = \begin{pmatrix} a_3\alpha_1^3 + a_2\alpha_1^2 + a_1\alpha_1 & a_3\alpha_2^3 + a_2\alpha_2^2 + a_1\alpha_2 \\ b_3\alpha_1^3 + b_2\alpha_1^2 + b_1\alpha_1 & b_3\alpha_2^3 + b_2\alpha_2^2 + b_1\alpha_2 \end{pmatrix}$.

We call U *the result matrix.*

$$P\big[U = \begin{pmatrix} x & z \\ y & w \end{pmatrix}\big] = \begin{cases} \frac{1}{p^3}, & \begin{pmatrix} x & z \\ y & w \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \\ \frac{2p-1}{p^3(p^2-1)}, & \begin{pmatrix} x & z \\ y & w \end{pmatrix} \in \Omega, \\ \frac{p-1}{p^3(p^2-1)}, & \text{otherwise}, \end{cases}$$

where Ω is a proper subset of $M_2(\mathbb{F}_p)$, with cardinality of $\leq 2p(p-1)^2$.

Detailed proof of Lemma 3 can be found in appendix. The immediate result rising from Lemma 3 is that, given (3.3.1), all p^2 options for $(s_1, s_2) \in \mathbb{F}_p^2$ are possible: If the adversary is holding $\begin{pmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{pmatrix} \in M_2(\mathbb{F}_p)$, then for each of the p^2 possible pairs of secrets $(s_1, s_2) \in \mathbb{F}_p^2$, there is a single suitable element $\begin{pmatrix} x & z \\ y & w \end{pmatrix} \in M_2(\mathbb{F}_p)$. Namely, this element is:

$$\begin{pmatrix} x & z \\ y & w \end{pmatrix} = \begin{pmatrix} y_{11} - s_1 & y_{21} - s_2 \\ y_{12} - s_1 & y_{22} - s_2 \end{pmatrix}.$$

Since all elements $\begin{pmatrix} x & z \\ y & w \end{pmatrix} \in M_2(\mathbb{F}_p)$ occur with positive probability, the adversary simply does not have enough information in order to determine the secrets.

Now, not all elements $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$ have the same probability. According to Lemma 3, about $\approx p^3$ out of the p^4 elements of $M_2(\mathbb{F}_p)$ have a slightly larger probability. Specifically, $|\Omega| \leq 2p(p-1)^2$. We use the statistical difference function [12] to measure the leakage of information: If (s_1, s_2) and (s_1', s_2') are two pairs of secrets, we denote by $Y_{(s_1,s_2)}$ and $Y_{(s_1',s_2')}$ the $M_2(\mathbb{F}_p)$-random variables indicating the matrices $\left(\begin{smallmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{smallmatrix}\right)$ induced by (s_1, s_2) and (s_1', s_2'), respectively, over the Q-picking of v from V_p.

We compute the statistical difference SD between the distributions:

$$SD(Y_{(s_1,s_2)}, Y_{(s_1',s_2')}) =$$

$$\frac{1}{2} \cdot \sum_{Y \in M_2(\mathbb{F}_p)} \left| P\big[Y_{(s_1,s_2)} = Y\big] - P\big[Y_{(s_1',s_2')} = Y\big] \right| =$$

$$\frac{1}{2} \cdot \sum_{\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)} \left| P\left[\left(\begin{smallmatrix} a_3\alpha_1^3+a_2\alpha_1^2+a_1\alpha_1+s_1 & a_3\alpha_2^3+a_2\alpha_2^2+a_1\alpha_2+s_1 \\ b_3\alpha_1^3+b_2\alpha_1^2+b_1\alpha_1+s_2 & b_3\alpha_2^3+b_2\alpha_2^2+b_1\alpha_2+s_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\right]\right.$$

$$\left. -P\left[\left(\begin{smallmatrix} a_3\alpha_1^3+a_2\alpha_1^2+a_1\alpha_1+s_1' & a_3\alpha_2^3+a_2\alpha_2^2+a_1\alpha_2+s_1' \\ b_3\alpha_1^3+b_2\alpha_1^2+b_1\alpha_1+s_2' & b_3\alpha_2^3+b_2\alpha_2^2+b_1\alpha_2+s_2' \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\right]\right| =$$

$$\frac{1}{2} \cdot \sum_{\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)} \left| P\left[\left(\begin{smallmatrix} a_3\alpha_1^3+a_2\alpha_1^2+a_1\alpha_1 & a_3\alpha_2^3+a_2\alpha_2^2+a_1\alpha_2 \\ b_3\alpha_1^3+b_2\alpha_1^2+b_1\alpha_1 & b_3\alpha_2^3+b_2\alpha_2^2+b_1\alpha_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x-s_1 & z-s_1 \\ y-s_2 & w-s_2 \end{smallmatrix}\right)\right]\right.$$

$$\left. -P\left[\left(\begin{smallmatrix} a_3\alpha_1^3+a_2\alpha_1^2+a_1\alpha_1 & a_3\alpha_2^3+a_2\alpha_2^2+a_1\alpha_2 \\ b_3\alpha_1^3+b_2\alpha_1^2+b_1\alpha_1 & b_3\alpha_2^3+b_2\alpha_2^2+b_1\alpha_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x-s_1' & z-s_1' \\ y-s_2' & w-s_2' \end{smallmatrix}\right)\right]\right|$$

Now, assume $Y_{(s_1,s_2)}$ and $Y_{(s_1',s_2')}$ are as statistically far as they can be. I.e., (s_1, s_2) and (s_1', s_2') are such pairs that for each $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in M_2(\mathbb{F}_p)$, if $P\Big[U = \left(\begin{smallmatrix} x-s_1 & z-s_1 \\ y-s_2 & w-s_2 \end{smallmatrix}\right)\Big] > \frac{p-1}{p^3(p^2-1)}$ then, $P\Big[U = \left(\begin{smallmatrix} x-s_1' & z-s_1' \\ y-s_2' & w-s_2' \end{smallmatrix}\right)\Big] = \frac{p-1}{p^3(p^2-1)}$, and vice versa. Then:

$$SD(Y_{(s_1,s_2)}, Y_{(s_1',s_2')}) \leq \frac{1}{2} \cdot \left(2 \cdot \left(\frac{1}{p^3} - \frac{p-1}{p^3(p^2-1)}\right)\right.$$

$$\left. +2 \cdot 2p(p-1)^2 \cdot \left(\frac{2p-1}{p^3(p^2-1)} - \frac{p-1}{p^3(p^2-1)}\right)\right).$$

Rearrange and get: $SD(Y_{(s_1,s_2)}, Y_{(s_1',s_2')}) \leq \frac{2p^2-2p+1}{p^2(p+1)} < \frac{2}{p}$. Similar computations show that the statistical difference between $Y_{(s_1,s_2)}$ and the uniform distribution over $M_2(\mathbb{F}_p)$ is no more than $\frac{1}{p}$.

4 Applications

One drawback of our scheme is that the secrets are restricted. Meaning, if s_1 and s_2 are two secrets that were shared as we suggest, then they only can be multiplied with each other. E.g., if s_3 and s_4 were also shared in the same way, then we cannot perform homomorphic cross-multiplication of s_1 with s_3 and guarantee the correctness of the multiplication. This drawback makes our scheme unsuitable for some applications. We overcome that drawback by generating a pool of shares of the secrets $s_1, \ldots, s_m$ that is distributed to each participant and makes any pair of secrets possible to cross-multiply homomorphically and correctly with each other. We explain how such pool is generated, and how it can be used to perform homomorphic evaluation of any quadratic expression over variables $s_1, \ldots, s_m$, and arbitrarily long 2-CNF circuits. A quadratic function over variables $s_1, \ldots s_m$ is of the form $F(s_1, \ldots, s_m) = \sum_{1 \leq i,j, \leq m} r_{ij} s_i s_j + \sum_{k=1}^{m} t_k s_k$, where the indices $r_{ij}, t_k \in \mathbb{F}_p$. There are $p^{\frac{1}{2}m(m+3)}$ such functions. We can use our scheme to homomorphically evaluate F. For each of the m^2 pairs of variables s_i, s_j, use our scheme to generate two polynomials f_{ij}, f_{ji} and distribute the secret shares of s_i, s_j to the participants. This pre-processing requires $O(m^2)$ communication, but now F can be homomorphically evaluated in a straightforward way. Each participant P_i simply evaluates F over its shares of the secrets and sends the result y_i to the dealer. The dealer in turn calculates the polynomial g going through the points (α_i, y_i) and has $g(0) = F(s_1, \ldots, s_m)$. A 2-CNF expression over literals $s_1, \ldots, s_m$ is an expression of the form $(s_{i_1} \vee s_{i_2}) \wedge \cdots \wedge (s_{i_{2t-1}} \vee s_{i_{2t}})$. As we work in $\mathbb{F}_p$, we consider a True-valued literal to be $1 \in \mathbb{F}_p$ and a False-valued literal to be $0 \in \mathbb{F}_p$ (other elements of $\mathbb{F}_p$ are not logically defined). A $\vee$ operation between literals s_1, s_2 is implemented using $\mathbb{F}_p$ operations by: $s_1 + s_2 - s_1 s_2$, and a "not" operation over s_1 is $1 - s_1$. The $\wedge$ operation will be considered as addition in $\mathbb{F}_p$. Then a 2-CNF expression of length $2t$ is a multi-variant quadratic function, and is assigned *True* if the function is evaluated to $t \in \mathbb{F}_p$, and *False* otherwise. There are 2^{2m^2+m} such expressions that can be homomorphically evaluated using our scheme.

5 Conclusions

We have proposed a scheme to perform a multiplication over secret shares without increasing the number of participants required to extract the product. In our scheme we have used $n+1$ participants and polynomials of degree n. Of course, one can avoid increasing the number of participants by just taking the polynomials to be of lower degree to begin with, but under that naive solution the security would be compromised. E.g., if one runs the standard Shamir secret sharing scheme with four participants and would like to be able to extract a product of two secrets, he/she would be obligated to work with linear polynomials. In that case, if an adversary manages to discover two of the shares of a certain secret then the secret is revealed. If one tried to work with quadratic polynomials in the standard scheme, then the product polynomial would be of degree 4, and it require 5 participants to extract the product. In our scheme, even if an adversary manages to put his/her hands on two out of four shares of a certain secret, the secret is information-theoretically kept. We proved that each of the participants holding two correlated secret shares gains absolutely no information about the secrets[5]. We also proved that a coalition of two curious participants still cannot reveal the exact value of (s_1, s_2). Furthermore, (s_1, s_2) distributes almost uniformly over $\mathbb{F}_p^2$ given the information the two participants are holding, and all options for (s_1, s_2) are possible under that attack. Our scheme can be used to reduce the communication complexity of cryptographic systems as Shamir secret shared database [11], secure multiparty computation [4], secret shared random access machine [6] and in outsourcing of computations, such as in cloud computing, when statistical security may suffice. The scheme we suggest here is somewhat surprising. We multiply two shares of degree n-

[5] Even if knowing the α_i that was assigned to him/her by the Dealer.

polynomial-shared secrets and manage to extract the product using no more than the $n+1$ participants we began with, proving it to be information-theoretically secure. The innovation is in the function sieving process and in the way we built the set $\mathcal{V}_p$ and defined the probability Q over it.

Acknowledgments: With pleasure, we thank Amos Beimel on useful inputs.

References

[1] Cramer, R., Damgård, I. and Maurer, U. (2000). General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology-EUROCRYPT* 2000 (pp. 316−334). Springer-Berlin-Heidelberg.

[2] Dawson, E. and Donovan, D. (1994). The breadth of Shamir's secret-sharing scheme. *Computers and Security*, 13(1), 69−78.

[3] Dolev, S., Garay, J., Gilboa, N. and Kolesnikov, V. (2009). Swarming secrets. In *47th Annual Allerton Conference on Communication, Control, and Computing* (pp. 1438−1445). IEEE.

[4] Dolev, S., Gilboa, N. and Li, X. (2015). Accumulating automata and cascaded equations automata for communicationless information theoretically secure multi-party computation. In *Proceedings of the 3rd International Workshop on Security in Cloud Computing* (pp. 21−29). ACM.

[5] Dolev, S., Lahiani, L. and Yung, M. (2007). Secret swarm unit reactive k-Secret sharing. In *Progress in Cryptology-INDOCRYPT* 2007 (pp. 123−137). Springer Berlin-Heidelberg.

[6] Dolev, S., & Li, Y. (2016). Secret Shared Random Access Machine. In *Algorithmic Aspects of Cloud Computing* (pp. 19-34). Springer International Publishing.

[7] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *STOC* (Vol. 9, pp. 169−178).

[8] Micciancio, D. (2010). A first glimpse of cryptography's Holy Grail. *Communications of the ACM*, 53(3), 95−96.

[9] Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612−613.

[10] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, 28(4), 656-715.

[11] Avni, H., Dolev, S., Gilboa, N., & Li, X. (2016). SSSDB: Database with Private Information Search. In *Algorithmic Aspects of Cloud Computing* (pp. 49-61). Springer International Publishing.

[12] Goldreich, O. (2009). Foundations of cryptography: volume 2, basic applications. Cambridge university press.

[13] Boneh, D., Goh, E. J., & Nissim, K. (2005, February). Evaluating 2-DNF formulas on ciphertexts. In *Theory of Cryptography Conference* (pp. 325-341). Springer Berlin Heidelberg.

[14] âĂŘ Sander, T., Young, A., & Yung, M. (1999). Non-interactive cryptocomputing for NC 1. In *Foundations of Computer Science*, 1999. 40th Annual Symposium on (pp. 554-566). IEEE.

[15] Rabin, T., & Ben-Or, M. (1989, February). *Verifiable secret sharing and multiparty protocols with honest majority.* In Proceedings of the twenty-first annual ACM symposium on Theory of computing (pp. 73-85). ACM.

[16] Brakerski, Z., & Perlman, R. (2016). *Lattice-based fully dynamic multi-key FHE with short ciphertexts.* CRYPTO.

6 Appendix

6.1 Proof of Lemma 1

Lemma 1: For $\alpha \in \mathbb{F}_p^\times$ denote $u = \begin{pmatrix} \sum_{i=1}^n a_i\alpha^i \\ \sum_{i=1}^n b_i\alpha^i \end{pmatrix}$. Under the above assumptions, $P[u = \binom{x}{y}] = \frac{1}{p^2}$ for each $\binom{x}{y} \in \mathbb{F}_p^2$.

Proof of Lemma 1: We call u *the result vector*. Since p and α are set, the result vector u depends only on the Q-choice of $v \in \mathcal{V}_p$. For $v = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$, denote:

$$M_v = \begin{pmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix} \in M_{2\times n}(\mathbb{F}_p).$$

Together with the following notations we are able to state the connection between u and v clearly. We define a mapping $\mu_\alpha : \mathcal{V}_p \to \mathbb{F}_p^2$ by

$$\mu_\alpha(v) = M_v \begin{pmatrix} \alpha \\ \vdots \\ \alpha^n \end{pmatrix}.$$

For convenience we denote $\mu = \mu_\alpha$. The map μ provides the connection between the Q-choice of $v \in \mathcal{V}_p$ and the result vector u in a way that $P[u = \binom{x}{y}] = P[\mu(v) = \binom{x}{y}]$.

To compute $P[u = \binom{x}{y}]$, we first partition $\mathbb{F}_p^2$ into four subsets U_j , $1 \le j \le 4$:

- $U_1 = \{\binom{0}{0}\} \subset \mathbb{F}_p^2$.
- $U_2 = \{\binom{x}{0} \in \mathbb{F}_p^2 \mid x \neq 0\}$.
- $U_3 = \{\binom{0}{y} \in \mathbb{F}_p^2 \mid y \neq 0\}$.
- $U_4 = \{\binom{x}{y} \in \mathbb{F}_p^2 \mid x \neq 0, y \neq 0\}$.

In the course of the proof, each time we set a j between 1 and 4 and compute $P[u = \binom{x}{y}]$ for $\binom{x}{y} \in U_j$.

We begin with $j = 1$. We look for elements $v \in \mathcal{V}_p$ such that:

$$\mu(v) = \binom{0}{0}. \tag{6.1.1}$$

Of course, $v = \overline{0} \in \mathbb{F}_p^{2n}$ is a solution of (6.1.1). Assume $v = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$ is such that $v \neq \overline{0}$ and M_v is a solution of (6.1.1). It follows that:

$$\begin{aligned} &\text{I} && \sum_{i=1}^n a_i\alpha^i = 0, \\ &\text{II} && \sum_{i=1}^n b_i\alpha^i = 0 \\ &\text{III} && \sum_{i=1}^n a_i b_{n+1-i} = 0 \end{aligned} \tag{6.1.2}$$

where $(a_1, \ldots, a_n) \neq \overline{0} \neq (b_1, \ldots, b_n)$. Each solution for (6.1.2) gives a suitable element of $\mathcal{V}_p$. Now, (6.1.2)I is a linear equation of n variables a_i. Since the trivial solution is not acceptable we have $p^{n-1} - 1$ possible solutions $(a_1, \ldots, a_n)$ for (6.1.2)I. For each of those solutions (6.1.2)II, III is a system of linear equations of n variables b_i. If they are independent, it has $p^{n-2} - 1$ solutions $(b_1 \ldots, b_n)$, when we omit the trivial solution. Can they be dependent? If they are, there is $c \in \mathbb{F}_p$ such that $c \cdot \alpha^i = a_{n+1-i}$ for $1 \le i \le n$. By (6.1.2)I we get then $\sum_{i=1}^n c \cdot \alpha^{n+1-i} \cdot \alpha^i = 0$. Then $n \cdot c \cdot \alpha^{n+1} = 0$. Each of the factors is $\neq 0$, hence (6.1.2)II, III are independent. All in all we get $(p^{n-1} - 1)(p^{n-2} - 1)$ solutions $(a_1, \ldots, a_n, b_1, \ldots, b_n) \neq \overline{0}$.

We conclude that:

$$P[u = \binom{0}{0}] = 1 \cdot Q(\overline{0}) + (p^{n-1} - 1)(p^{n-2} - 1) \cdot Q(v)$$

while $v \neq \overline{0}$. That is

$$P[u = \binom{0}{0}] = 1 \cdot \frac{1}{p^n} + \frac{(p^{n-1}-1)(p^{n-2}-1)}{p^n(p^{n-1}-1)} = \frac{1}{p^2}.$$

To compute $P[u = \binom{x}{y}]$ for $\binom{x}{y} \in U_j$ when $j \neq 1$, we define a family of transformations $T_{k,l}$ over $\mathcal{V}_p$. For arbitrary fixed $k, l \in \mathbb{F}_p^\times$, let $T_{k,l} : \mathcal{V}_p \to \mathcal{V}_p$ be defined by:

$$T_{k,l}(a_1, \ldots, a_n, b_1, \ldots, b_n) = (ka_1, \ldots, ka_n, lb_1, \ldots, lb_n).$$

The map $T_{k,l}$ is clearly bijective. In fact, the number and positions of zeroes in v (if any) are the same as in $T_{k,l}(v)$.

The set $\mathcal{V}_p$ and some of its subsets have important properties regarding $T_{k,l}$:

- $\mathcal{V}_p$ **is** $T_{k,l}$**-invariant** : If $v = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$, then $\sum_{i=1}^n a_i b_{n+1-i} = 0$. It immediately follows that $T_{k,l}(v) = kl \sum_{i=1}^n a_i b_{n+1-i} = 0$. Hence $T_{k,l}(v)$ is indeed in $\mathcal{V}_p$.
- **The sets** $\mu^{-1}(U_j)$ **are** $T_{k,l}$**-invariant:** If $v = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathcal{V}_p$, and $\mu(v) \in U_j$ for a certain j, then:

  $$\mu(v) = \begin{pmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix} \begin{pmatrix} \alpha \\ \vdots \\ \alpha^n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_1 \alpha^i \\ \sum_{i=1}^n b_1 \alpha^i \end{pmatrix} \in U_j.$$

  We have:

  $$\mu\big(T_{k,l}(v)\big) = \begin{pmatrix} ka_1 & \cdots & ka_n \\ lb_1 & \cdots & lb_n \end{pmatrix} \begin{pmatrix} \alpha \\ \vdots \\ \alpha^n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n ka_1 \alpha^i \\ \sum_{i=1}^n lb_1 \alpha^i \end{pmatrix}.$$

  Then

  $$\mu\big(T_{k,l}(v)\big) = \begin{pmatrix} k \sum_{i=1}^n a_1 \alpha^i \\ l \sum_{i=1}^n b_1 \alpha^i \end{pmatrix}.$$

  Since $k, l \neq 0$, we can see that a certain entry of $\mu(v)$ is 0 if and only if the corresponding entry of $\mu\big(T_{k,l}(v)\big)$ is such. Meaning, if $\mu(v) \in U_j$, then $\mu\big(T_{k,l}(v)\big) \in U_j$. We conclude that the sets $\mu^{-1}(U_j) \subseteq \mathcal{V}_p$ are invariant under $T_{k,l}$.

We now make an important observation regarding $\mathcal{V}_p$, μ and $T_{k,l}$: Let $\binom{x}{y}, \binom{x'}{y'} \in U_j$ for some $1 \leq j \leq 4$. Take $v = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mu^{-1}\big(\binom{x}{y}\big)$. We have, $\mu(v) = \begin{pmatrix} \sum_{i=1}^n a_1 \alpha^i \\ \sum_{i=1}^n b_1 \alpha^i \end{pmatrix} = \binom{x}{y}$. Put

$$k = \begin{cases} \frac{x'}{x}, & x \neq 0, \\ 1, & x = 0, \end{cases} \quad , \quad l = \begin{cases} \frac{y'}{y}, & y \neq 0, \\ 1, & y = 0. \end{cases}$$

We get $\mu\big(T_{k,l}(v)\big) = \begin{pmatrix} k \sum_{i=1}^n a_1 \alpha^i \\ l \sum_{i=1}^n b_1 \alpha^i \end{pmatrix} = \begin{pmatrix} \frac{x'}{x} x \\ \frac{y'}{y} y \end{pmatrix} = \binom{x'}{y'}$. So for every $v \in \mu^{-1}\big(\binom{x}{y}\big)$ we have $T_{k,l}(v) \in \mu^{-1}\big(\binom{x'}{y'}\big)$ by taking the appropriate k, l. This implies that: $\big|\mu^{-1}\big(\binom{x}{y}\big)\big| = \big|\mu^{-1}\big(\binom{x'}{y'}\big)\big|$ for $\binom{x}{y}, \binom{x'}{y'} \in U_j$.

We use the last observation to show that, for a given $j \neq 1$, all elements of U_j have the same probability. Specifically, we show that if $\binom{x}{y}, \binom{x'}{y'} \in U_j$, $j \neq 1$, then $P[u = \binom{x}{y}] = P[u = \binom{x'}{y'}]$. We will use the properties of the transformations $T_{k,l}$ that we have just shown, and the fact that all elements $v \in \mathcal{V}_p$, such that $v \neq \overline{0}$, have the same probability $Q(v)$. Observe that:

$$P[u = \binom{x}{y}] = P[\mu(v) = \binom{x}{y}] = P[v \in \mu^{-1}\big(\binom{x}{y}\big)].$$

Since $j \neq 1$

$$P[u = \binom{x}{y}] = P[v \in \mu^{-1}\big(\binom{x}{y}\big) \big| \mu(v) \notin U_1] \cdot P[\mu(v) \notin U_1]$$

$$= \frac{\big|\mu^{-1}\big(\binom{x}{y}\big)\big|}{|\mathcal{V}_p| - |\mu^{-1}(U_1)|} \cdot \Big(1 - \frac{1}{p^2}\Big)$$

$$= \frac{\big|\mu^{-1}\big(\binom{x}{y}\big)\big|}{(p^{n-1}-1)(p^n-1) + 1 - (p^{n-1}-1)(p^{n-2}-1) - 1} \cdot \frac{p^2-1}{p^2}$$

$$= \frac{\big|\mu^{-1}\big(\binom{x}{y}\big)\big|}{p^{n-2}(p^{n-1}-1)(p^2-1)} \cdot \frac{p^2-1}{p^2} = \frac{\big|\mu^{-1}\big(\binom{x}{y}\big)\big|}{p^{n-2}(p^{n-1}-1)} \cdot \frac{1}{p^2}.$$

By the same token:

$$P[u = \binom{x'}{y'}] = \frac{\big|\mu^{-1}\big(\binom{x'}{y'}\big)\big|}{p^{n-2}(p^{n-1}-1)} \cdot \frac{1}{p^2}.$$

Since $\big|\mu^{-1}\big(\binom{x}{y}\big)\big| = \big|\mu^{-1}\big(\binom{x'}{y'}\big)\big|$ for $\binom{x}{y}, \binom{x'}{y'} \in U_j$, by the above computations we have $P[u = \binom{x}{y}] = P[u = \binom{x'}{y'}]$. Moreover, we see that all we need to do to complete the proof is to show that $\big|\mu^{-1}\big(\binom{x}{y}\big)\big| = p^{n-2}(p^{n-1}-1)$. Since $|U_2| = |U_3| = p-1$, it will be enough to show that $|\mu^{-1}(U_2)| = |\mu^{-1}(U_3)| = (p-1)p^{n-2}(p^{n-1}-1)$. It will imply that, if $\binom{x}{y}$ is in U_2 or U_3, then $P[u = \binom{x}{y}] = \frac{1}{p^2}$. Knowing $|\mathcal{V}_p|$, we just subtract to get $|\mu^{-1}(U_4)| = p^{n-2}(p^{n+1}-1)(p-1)^2$. As $|U_4| = (p-1)^2$, it will imply the desired result for $j = 4$ as well.

Thus, all there is left to show is

$$|\mu^{-1}(U_2)| = (p-1)p^{n-2}(p^{n-1}-1).$$

As we mentioned above, regarding the properties of $T_{k,l}$, all elements of U_j have the same amount of pre-images under μ. So it suffice to show

$$\Big|\mu^{-1}\Big(\binom{1}{0}\Big)\Big| = p^{n-2}(p^{n-1}-1).$$

We look for $v \in \mathcal{V}_p$ such that $\mu(v) = \binom{1}{0}$. Assuming $v = (a_1, \ldots, a_n, b_1, \ldots, b_n)$ and similarly to the computation of $\Big|\mu^{-1}\Big(\binom{0}{0}\Big)\Big|$,we get the following set of equations

$$\begin{aligned} &\text{I} && \sum_{i=1}^n a_i \alpha^i = 1, \\ &\text{II} && \sum_{i=1}^n b_i \alpha^i = 0 \\ &\text{III} && \sum_{i=1}^n a_i b_{n+1-i} = 0, \end{aligned} \tag{6.1.3}$$

where $(a_1, \ldots, a_n) \neq \overline{0} \neq (b_1, \ldots, b_n)$, and each solution for (6.1.3) gives a suitable element of $\mathcal{V}_p$.

(6.1.3)I is a linear equation of n variables a_i, hence it has p^{n-1} solutions. For each of those solutions (6.1.3)II, III is a system of linear equations of n variables b_i. If they are independent, it has $p^{n-2}-1$ solutions for b_i, when we omit the trivial solution. When are they dependent? Assume they are, there is $c \in \mathbb{F}_p$ such that $c \cdot \alpha^{n+1-i} = a_i$ for $1 \leq i \leq n$. By (6.1.3)I we get then $\sum_{i=1}^n c \cdot \alpha^{n+1-i} \cdot \alpha^i = 1$. Then $n \cdot c \cdot \alpha^{n+1} = 1$, implying $c = n^{-1}\alpha^{-1-n}$. Hence, there is exactly one solution in a_i for (6.1.3)I that yields dependent equations (6.1.3)II, III. Namely, for $a_i = c \cdot \alpha^{n+1-i} = n^{-i}\alpha^{-i}$ the system (6.1.3)II, III is a dependent system of linear equations of n variables b_i, hence its has $p^{n-1}-1$ solutions (when again, we omit the trivial solution). All in all we get

$$(p^{n-1}-1) \cdot (p^{n-2}-1) + 1 \cdot (p^{n-1}-1) = p^{n-2}(p^{n-1}-1)$$

solutions for $(a_1, \ldots, a_n, b_1, \ldots, b_n)$.

□

6.2 Proof of Lemma 3

Lemma 3: Denote $U = \begin{pmatrix} a_3\alpha_1^3+a_2\alpha_1^2+a_1\alpha_1 & a_3\alpha_2^3+a_2\alpha_2^2+a_1\alpha_2 \\ b_3\alpha_1^3+b_2\alpha_1^2+b_1\alpha_1 & b_3\alpha_2^3+b_2\alpha_2^2+b_1\alpha_2 \end{pmatrix}$. We call U *the result matrix.*

$$P\big[U = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\big] = \begin{cases} \frac{1}{p^3}, & \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \\ \frac{2p-1}{p^3(p^2-1)}, & \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in \Omega, \\ \frac{p-1}{p^3(p^2-1)}, & \text{otherwise}, \end{cases}$$

where Ω is a proper subset of $M_2(\mathbb{F}_p)$, further detail on which will be given in the course of the proof.

Proof of Lemma 3: Since p and α_1, α_2 are set, the result matrix U depends only on the Q-choice of $v \in \mathcal{V}_p$. Using the same notation for M_v as in the proof of Lemma 1, we state the connection between U and v. For $\alpha_1, \alpha_2 \in \mathbb{F}_p^\times$ we define a mapping $\rho_{\alpha_1,\alpha_2} : \mathcal{V}_p \to M_2(\mathbb{F}_p)$ by

$$\rho_{\alpha_1,\alpha_2}(v) = M_v \begin{pmatrix} \alpha_1^3 & \alpha_2^3 \\ \alpha_1^2 & \alpha_2^2 \\ \alpha_1 & \alpha_2 \end{pmatrix}.$$

For convenience we denote $\rho = \rho_{\alpha_1,\alpha_2}$. As in Lemma 1, the map ρ provides the connection between the Q-choice of $v \in \mathcal{V}_p$ and the result matrix U, in a way that $P[U = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)] = P[\rho(v) = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)]$.

Let $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in M_2(\mathbb{F}_p)$. We compute $P[U = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)]$ by finding the elements $v \in V_p$ that make $\rho(v) = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$, and use the probability Q that was defined over V_p above. These are exactly the elements $(a_1, a_2, a_3, b_1, b_2, b_3) \in V_p$ that solve the following set of equations.

$$\begin{aligned} &\text{I} && a_3\alpha_1^3 + a_2\alpha_1^2 + a_1\alpha_1 = x, \\ &\text{II} && b_3\alpha_1^3 + b_2\alpha_1^2 + b_1\alpha_1 = y, \\ &\text{III} && a_3\alpha_2^3 + a_2\alpha_2^2 + a_1\alpha_2 = z, \\ &\text{IV} && b_3\alpha_2^3 + b_2\alpha_2^2 + b_1\alpha_2 = w, \\ &\text{V} && a_3b_1 + b_2b_2 + a_1b_3 = 0, \end{aligned} \tag{6.2.1}$$

with $(a_1, a_2, a_3) \neq (0, 0, 0) \neq (b_1, b_2, b_3)$.

We solve (6.2.1) and analyze the number of solutions for given x, y, z, w. Some of the algebraic steps are quite routine and exhausting, so we occasionally omit them.

Since $\alpha_1 \neq 0$ we may write (6.2.1)I and (6.2.1)II in the form:

$$\begin{aligned} a_1 &= \frac{x}{\alpha_1} - a_2\alpha_1 - a_3\alpha_1^2, \\ b_1 &= \frac{y}{\alpha_1} - b_2\alpha_1 - b_3\alpha_1^2. \end{aligned} \tag{6.2.2}$$

Replace c_1,c_2 in (6.2.1)III and (6.2.1)IV with those of (6.2.2). Using the fact that $\alpha_1, \alpha_2 \neq 0$ and $\alpha_1 \neq \alpha_2$, we can rearrange and get

$$\begin{aligned} a_2 &= \frac{\alpha_1 z - \alpha_2 x}{\alpha_1\alpha_2(\alpha_2 - \alpha_1)} - a_3(\alpha_1 + \alpha_2), \\ b_2 &= \frac{\alpha_1 w - \alpha_2 y}{\alpha_1\alpha_2(\alpha_2 - \alpha_1)} - b_3(\alpha_1 + \alpha_2). \end{aligned} \tag{6.2.3}$$

Denote $\lambda(\alpha_1, \alpha_2) = \alpha_1\alpha_2(\alpha_2 - \alpha_1)(\alpha_1^2 + 4\alpha_1\alpha_2 + \alpha_2^2)$. Recall that we have picked the α_i's in such a way that $\lambda(\alpha_1, \alpha_2) \neq 0$. Replace a_2, b_2, a_1, b_1 in (6.2.1)V by the right-hand side of (6.2.2) and (6.2.3). Rearrange (6.2.1)V and get

$$\begin{aligned} &a_3[y \cdot \alpha_2(2\alpha_2 + \alpha_1) - w \cdot \alpha_1(2\alpha_1 + \alpha_2)] \\ &+b_3[x \cdot \alpha_2(2\alpha_2 + \alpha_1) - z \cdot \alpha_1(2\alpha_1 + \alpha_2)] \\ &+a_3b_3 \cdot \lambda(\alpha_1, \alpha_2) = \frac{(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{\alpha_1\alpha_2(\alpha_2 - \alpha_1)}. \end{aligned} \tag{6.2.4}$$

It remains only to find the number of solutions (a_1, a_2) of the bilinear equation (6.2.4). For each of those solutions, v is determined by (6.2.2) and (6.2.3), and we only need to verify the condition $(a_1, a_2, a_3) \neq (0, 0, 0) \neq (b_1, b_2, b_3)$. Since α_1, α_2 are set, the number of solutions only depends on x, y, z, w.

Observe that when $x = z \cdot \frac{\alpha_1}{\alpha_2}$ or $y = w \cdot \frac{\alpha_1}{\alpha_2}$, the right-hand side of (6.2.4) is zero. We divide the problem into four cases and discuss each of them separately:

1. $x = z \cdot \frac{\alpha_1}{\alpha_2}$, $y = w \cdot \frac{\alpha_1}{\alpha_2}$
2. $x \neq z \cdot \frac{\alpha_1}{\alpha_2}$, $y \neq w \cdot \frac{\alpha_1}{\alpha_2}$
3. $x = z \cdot \frac{\alpha_1}{\alpha_2}$, $y \neq w \cdot \frac{\alpha_1}{\alpha_2}$
4. $x \neq z \cdot \frac{\alpha_1}{\alpha_2}$, $y = w \cdot \frac{\alpha_1}{\alpha_2}$

Case 1: $x = z \cdot \frac{\alpha_1}{\alpha_2}$, $y = w \cdot \frac{\alpha_1}{\alpha_2}$.

Rewrite (6.2.4) as

$$a_3 \cdot w + b_3 \cdot z + a_3b_3 \cdot \frac{\lambda(\alpha_1, \alpha_2)}{\alpha_1(\alpha_2 - \alpha_1)} = 0. \tag{6.2.5}$$

There are four options for (z, w):

- $z = w = 0$: Since $\lambda(\alpha_1, \alpha_2) \neq 0$, by (6.2.5) we have $a_3b_3 = 0$. If, say, $a_3 = 0$, we get by (6.2.2) and (6.2.3) that $a_2 = a_1 = 0$ as well, which gives $v = (0, 0, 0, 0, 0, 0)$. The case $b_3 = 0$ is analogous. So the only valid solution for this case is $v = (0, 0, 0, 0, 0, 0)$.
- $z \neq 0, w = 0$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} z\frac{\alpha_1}{\alpha_2} & z \\ 0 & 0 \end{smallmatrix}\right)$. By (6.2.5) we have $b_3\big(z + a_3 \cdot \frac{\lambda(\alpha_1,\alpha_2)}{\alpha_1(\alpha_2-\alpha_1)}\big) = 0$. As in the previous option, solutions with $b_3 = 0$ are not valid. Hence $a_3 = -z \cdot \frac{\lambda(\alpha_1,\alpha_2)}{\alpha_1(\alpha_2-\alpha_1)}$, and since $z \neq 0$ we get $p - 1$ valid solutions with $b_3 \neq 0$ for each of the elements $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$ in this case.
- $z = 0, w \neq 0$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ w\frac{\alpha_1}{\alpha_2} & w \end{smallmatrix}\right)$. As in the previous option, we get $p-1$ valid solutions for each of the elements in this case.
- $z \neq 0, w \neq 0$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} z\frac{\alpha_1}{\alpha_2} & z \\ w\frac{\alpha_1}{\alpha_2} & w \end{smallmatrix}\right)$. Since $w \neq 0$ we can rearrange (6.2.5) and write: $a_3\big(b_3 \cdot \frac{\lambda(\alpha_1,\alpha_2)}{\alpha_1(\alpha_2-\alpha_1)} + 1\big) = -b_3\frac{z}{w}$. Now, if $b_3 = -\frac{\alpha_1(\alpha_2-\alpha_1)}{\lambda(\alpha_1,\alpha_2)}$ there is no solution. We are left with $p - 1$ ways to pick b_3 and get a unique a_3. Observe that all of these solutions are valid: if $b_3 = 0$ then $a_3 = 0$, and then by (6.2.3) we have $a_2 = b_2 = 0$ as well. Since $x, y \neq 0$ here we get by (6.2.2) that $a_1, b_1 \neq 0$. Thus, we have $p - 1$ valid solutions for each of the elements in this case.

Case 2: $x \neq z \cdot \frac{\alpha_1}{\alpha_2}$, $y \neq w \cdot \frac{\alpha_1}{\alpha_2}$.

We start with an important observation. The coefficients of a_3 and b_3 in (6.2.4) contain the expressions $2\alpha_2 + \alpha_1$ and $2\alpha_1 + \alpha_2$. These expressions cannot be zero together, since this would imply $\alpha_1 = \alpha_2$. Without loss of generality we may assume now $2\alpha_2 + \alpha_1 \neq 0$, and denote $k = \frac{\alpha_1(2\alpha_1+\alpha_2)}{\alpha_2(2\alpha_2+\alpha_1)}$. Observe that it is possible that $k = 0$, but not that $k = \frac{\alpha_1}{\alpha_2}$, since it too would imply $\alpha_1 = \alpha_2$. We now divide this case into the following options:

- $x = z \cdot k, y = w \cdot k$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} z\cdot k & z \\ w\cdot k & w \end{smallmatrix}\right)$. We get from (6.2.4) that $a_3b_3 \cdot \lambda(\alpha_1, \alpha_2) = \frac{zw\cdot\alpha_1(\alpha_1-\alpha_2)}{\alpha_2(2\alpha_2+\alpha_1)^2}$. The right-hand side of this equation is $\neq 0$. Indeed, if $z = 0$, the condition $x = z \cdot k$ yields $x = 0$, and together it implies $x = z \cdot \frac{\alpha_1}{\alpha_2}$. But in this case we assume $x \neq z \cdot \frac{\alpha_1}{\alpha_2}$, so $z \neq 0$. The same arguments show that $w \neq 0$. Since there are no solutions with $a_3 = 0$ or $b_3 = 0$ we can choose $a_3 \neq 0$ in $p - 1$ different ways and get a unique $b_3 \neq 0$. That is, there are $p - 1$ valid solutions for each of the elements in this case.

- $x \neq z \cdot k, y \neq w \cdot k$: In this case all coefficients of (6.2.4) are $\neq 0$. We observe the possible values of a_3 looking for solutions. If $a_3 = 0$ then b_3 is uniquely determined and we get a single valid solution. This solution is valid since (6.2.3) implies that $a_2 \neq 0$, and the same holds for b_3. If $a_3 \neq 0$ we can rearrange (6.2.4) to get

$$b_3\Big(\frac{x \cdot \alpha_2(2\alpha_2+\alpha_1) - z \cdot \alpha_1(2\alpha_1+\alpha_2)}{a_3} + \lambda(\alpha_1,\alpha_2)\Big) = \frac{(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{a_3\alpha_1\alpha_2(\alpha_2-\alpha_1)} - [y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2)]. \tag{6.2.6}$$

Now denote $l = \frac{x\cdot\alpha_2(2\alpha_2+\alpha_1) - z\cdot\alpha_1(2\alpha_1+\alpha_2)}{-\lambda(\alpha_1,\alpha_2)}$. Since $l \neq 0$ we have $p-2$ different ways to pick $a_3 \neq 0$ and l. For each of these, b_3 is uniquely determined by (6.2.6) which yields a single valid solution. The solution is valid since $a_3 \neq 0$, and if $b_3 = 0$ then by (6.2.3) we have $b_2 \neq 0$. We are left with the special case $a_3 = l$. Assume $a_3 = l$. By (6.2.6) we get

$$b_3 \cdot 0 = \frac{(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{l\alpha_1\alpha_2(\alpha_2-\alpha_1)} - [y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2)].$$

If the right-hand side of this equation is not zero then there are no more solutions. If it is 0, then we have p different ways to pick b_3 and get a solution. The solution is valid for the same reasons as when $a_3 \neq l$. This gives a total of $2p-1$ solutions for each of the elements $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$ that yield 0 on the right-hand side of (6.2.6). These elements satisfy

$$\frac{(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{l\alpha_1\alpha_2(\alpha_2-\alpha_1)} = [y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2)].$$

Since l is set we can write that condition differently:

$$\frac{-\lambda(\alpha_1,\alpha_2)(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{\alpha_1\alpha_2(\alpha_2-\alpha_1)\big[x\alpha_2(2\alpha_2+\alpha_1) - z\alpha_1(2\alpha_1+\alpha_2)\big]} = [y\alpha_2(2\alpha_2+\alpha_1) - w\alpha_1(2\alpha_1+\alpha_2)].$$

Computation shows that there are less than $2(p-1)^3$ such elements $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$ which yield $2p-1$ valid solutions. Other elements of that case yield $p-1$ valid solutions. We will use that observation later as it indicates the cardinality of Ω.

- $x \neq z \cdot k, y = w \cdot k$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & z \\ w\cdot k & w \end{smallmatrix}\right)$.

  We get from (6.2.4):

$$b_3[x \cdot \alpha_2(2\alpha_2+\alpha_1) - z \cdot \alpha_1(2\alpha_1+\alpha_2)] + a_3 b_3 \cdot \lambda(\alpha_1,\alpha_2) = \frac{(\alpha_2 x - \alpha_1 z)(\alpha_1 w - \alpha_2 y)}{\alpha_1\alpha_2(\alpha_2-\alpha_1)}. \tag{6.2.7}$$

  Since the right-hand side of (6.2.7) is non-zero, $a_2 \neq 0$. We have $p-1$ options to pick b_3 and get a unique a_3. Altogether there are $p-1$ valid solutions for each of the elements in this case.

- $x = z \cdot k, y \neq w \cdot k$: By the same token as in the previous case, we have here $p-1$ valid solutions for each of the elements.

Case 3: $x = z \cdot \frac{\alpha_1}{\alpha_2}$, $y \neq w \cdot \frac{\alpha_1}{\alpha_2}$.

Here we can rearrange and rewrite (6.2.4) as:

$$a_3\big[y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2)\big] + b_3 \cdot z\alpha_1(\alpha_2-\alpha_1) + a_3 b_3 \cdot \lambda(\alpha_1,\alpha_2) = 0. \tag{6.2.8}$$

We divide this case into two subcases:

- $y = w \cdot k$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} z\cdot\frac{\alpha_1}{\alpha_2} & z \\ w\cdot k & w \end{smallmatrix}\right)$. We can rearrange (6.2.8) and get:

$$b_3 \cdot \big[z\alpha_1(\alpha_2-\alpha_1) + a_3 \cdot \lambda(\alpha_1,\alpha_2)\big] = 0. \tag{6.2.9}$$

  There are two options:

  * $z = 0$: Here (6.2.9) gives $a_3 b_3 \cdot \lambda(\alpha_1,\alpha_2) = 0$. Observe that $a_3 \neq 0$, since otherwise we get by (6.2.3) and (6.2.2) that $a_1 = a_2 = 0$. We set $b_3 = 0$ and have $p-1$ options to pick $a_3 \neq 0$. By (6.2.3) we have $b_2 \neq 0$, and hence we get a total of $p-1$ valid solutions for each of the elements.
  * $z \neq 0$: In (6.2.9) we can set $b_3 = 0$ and pick a_3 in p different ways. The option $a_3 = 0$ is also valid since it implies $a_1 \neq 0$. If we take $a_3 = -\frac{z\alpha_1(\alpha_2-\alpha_1)}{\lambda(\alpha_1,\alpha_2)}$, then all p options for b_3 are possible. One of the solutions has been counted twice, so we get a total of $2p-1$ valid solutions for each of the elements. Observe that there are $(p-1)^2$ elements $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in M_2(\mathbb{F}_p)$ in this case: z can be picked in $p-1$ ways and then x is determined, and the same for w and y. This observation is not crucial to the proof of the lemma, but we will use it later as it indicates the cardinality of Ω.

- $y \neq w \cdot k$: Here $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} z\cdot\frac{\alpha_1}{\alpha_2} & z \\ y & w \end{smallmatrix}\right)$. Two options to deal with:

  * $z = 0$: Here we can rearrange (6.2.8) and get:

$$a_1\Big(y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2) + a_2 \cdot \lambda(\alpha_1,\alpha_2)\Big) = 0. \tag{6.2.10}$$

    If $a_3 = 0$ then by (6.2.3) and (6.2.2) we have $a_2 = a_1 = 0$ too. Then we set

$$b_3 = -\frac{y \cdot \alpha_2(2\alpha_2+\alpha_1) - w \cdot \alpha_1(2\alpha_1+\alpha_2)}{\lambda(\alpha_1,\alpha_2)}$$

    and we have $p-1$ options to pick $a_3 \neq 0$ and get a valid solution.
  * $z \neq 0$: The trivial solution $a_3 = b_3 = 0$ is valid here, and it is the only solution with $a_3 = 0$. If $a_3 \neq 0$ we can rearrange (6.2.8):

$$b_3\Big[\frac{z\alpha_1(\alpha_2-\alpha_1)}{a_3} + \lambda(\alpha_1,\alpha_2)\Big] = w \cdot \alpha_1(2\alpha_1+\alpha_2) - y \cdot \alpha_2(2\alpha_2+\alpha_1). \tag{6.2.11}$$

    If $a_3 = -\frac{z\alpha_1(\alpha_2-\alpha_1)}{\lambda(\alpha_1,\alpha_2)}$ we get no solution. So we are left with $p-2$ more ways to pick a_3 and get a valid solution. Altogether there is a total of $p-1$ valid solutions for each of the elements in this case.

Case 4: $x \neq z \cdot \frac{\alpha_1}{\alpha_2}$, $y = w \cdot \frac{\alpha_1}{\alpha_2}$. Same as in the previous case.

To conclude, if $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ then the only options for $\left|\rho^{-1}\left(\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\right)\right|$ are $p-1$ or $2p-1$, and $\rho^{-1}\left(\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\right) = (0,0,0,0,0,0)$. Now denote:

$$\Omega = \left\{\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in M_2(\mathbb{F}_p) : \left|\rho^{-1}\left(\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\right)\right| = 2p-1\right\}.$$

From the definition of Q it immediately follows that:

$$P\left[U = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)\right] = \begin{cases} \frac{1}{p^3}, & \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \\ \frac{2p-1}{p^3(p^2-1)}, & \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in \Omega, \\ \frac{p-1}{p^3(p^2-1)}, & \text{otherwise.} \end{cases}$$

As we have seen along the proof (in case 2, second option, and in case 3 at the first subcase, second option), $|\Omega| \leq 2p(p-1)^2$. That proves Lemma 3. $\square$