Partially homomorphic encryption schemes over finite fields[*]

Jian Liu[†] Lusheng Chen [‡] Sihem Mesnager[§]

Abstract

Homomorphic encryption scheme enables computation in the encrypted domain, which is of great importance because of its wide and growing range of applications. The main issue with the known fully (or partially) homomorphic encryption schemes is the high computational complexity and large communication cost required for their execution. In this work, we study symmetric partially homomorphic encryption schemes over finite fields, establishing relationships between homomorphisms over finite fields with q-ary functions. Our proposed partially homomorphic encryption schemes have perfect secrecy and resist cipher-only attacks to some extent.

Keywords: Homomorphic encryption; q-ary functions; perfect secrecy; finite fields.

1 Introduction

Homomorphic encryption schemes are cryptographic constructions which enable to securely perform operations on encrypted data without ever decrypting them. More precisely, a (group) homomorphic encryption scheme over a group $(G, *)$ satisfies that given two encryptions $c_1 = \mathrm{E}_k(m_1)$ and $c_2 = \mathrm{E}_k(m_2)$, where $m_1, m_2 \in G$ and k is the encryption key, one can efficiently compute $\mathrm{E}_k(m_1 * m_2)$ without decrypting c_1 and c_2. Homomorphic encryption schemes are widely used in many interesting applications, such as private information retrieval [6], electronic voting [2], multiparty computation [7], and cloud computing etc. Generally, fully homomorphic encryption schemes that support two operations over the underlying algebraic structure, i.e., addition and multiplication, will benefit more problems with different notions of security and cost.

The possibilities of homomorphic encryption were first explored by Rivest, Adleman, and Dertouzos in [18] shortly after the presentation of RSA, where homomorphic encryption was

[*] This work is supported by the National Key Basic Research Program of China under Grant 2013CB834204.

[†] School of Computer Software, Tianjin University, Tianjin 300072, P. R. China and CNRS, UMR 7539 LAGA, Paris, France, email: jianliu.nk@gmail.com

[‡] School of Mathematical Sciences, Nankai University, Tianjin 300071, P. R. China, email: lschen@nankai.edu.cn

[§] Department of Mathematics, University of Paris VIII, University of Paris XIII, CNRS, UMR 7539 LAGA and Telecom ParisTech, Paris, France, email: smesnager@univ-paris8.fr

called "privacy homomorphism". Multiplicative homomorphic encryption scheme based on basic RSA [18] is an asymmetric encryption system, which is useful for many applications. ElGamal [9] is also a multiplicative homomorphic encryption scheme which is asymmetric. Some additive homomorphic encryption schemes exist, see e.g. [16,17]. The first candidate for fully homomorphic encryption scheme was presented by Gentry [10]. After that, a number of fully homomorphic encryption schemes were proposed [4, 5, 21]. The security of these homomorphic encryption schemes (including partially and fully) relies on the hardness of some problems. Most known homomorphic encryption schemes are bit-by-bit encryption schemes, which makes them difficult to realize in practice, since it reduces the storage and communication efficiency.

Homomorphic encryption schemes allow to securely delegate computation, which have important significance in many client-server applications (e.g. cloud computing). In a client-server framework, it is more preferable to select efficient symmetric encryption schemes which are computationally "light" (e.g. over finite fields or rings), since the clients have limited computation ability and want to make communication cost small. However, such homomorphic encryption schemes are not easy to design, and the known constructions cannot completely suffice the needs of practical applications. In [8], Domingo-Ferrer proposed a symmetric fully homomorphic encryption scheme over polynomial rings, but at each time we multiply the ciphertexts, the size of the ciphertexts grows. Domingo-Ferrer's scheme has been broken by using a small pool of known plaintexts (see e.g. [22]). Armknecht and Sadeghi [1] also construct a symmetric additive homomorphic encryption scheme based on Reed-Solomon code, which also allows few number of multiplications. However, Armknecht's scheme suffers from the weakness that at some point, the error may become large enough to cause incorrect decryption (see [11]). In [4], there is a symmetric fully homomorphic encryption scheme based on the ring learning with errors assumption.

In the previous work, it was proved by Boneh and Lipton [3] that under a number theoretic assumption, any fully homomorphic encryption scheme over a ring $\mathbb{Z}_n$ can be broken in sub-exponential time by cipher-only attacks. More explicitly, given any ciphertext, the cryptanalyst who knows nothing about the secret key can find the encrypted plaintext in sub-exponential time. Later, Maurer and Raub [15] extended Boneh et al's work to finite fields of small characteristic. Thus, fully homomorphic encryption schemes over finite fields or rings would be vulnerable to cipher-only attacks. In this paper, we mainly consider symmetric partially homomorphic encryption schemes over finite fields, which are not based on hardness assumptions. We propose two symmetric partially homomorphic encryption schemes. After some security analyses, we show that the multiplicative homomorphic encryption scheme and the additive homomorphic encryption scheme can achieve perfect secrecy, i.e., given any ciphertext, the cryptanalyst who does not know the secret key can determine nothing about the encrypted plaintext. Furthermore, we claim that even the presented schemes are not in a one-time pad setting, they can resist against cipher-only attacks to some extent (if the size of the finite field is large enough). In addition, it is proved that over finite fields, non-zero multiplicative homomorphisms are equivalent to q-ary power functions, and non-zero additive homomorphisms are equivalent to non-constant homogeneous q-ary affine functions.

2 Preliminaries

Let $(G, *)$ and $(H, \cdot)$ be two groups. A mapping f of G into H is called a *homomorphism* if it preserves the operation of G, i.e., for all $x, y \in G$, we have $f(x * y) = f(x) \cdot f(y)$.

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime. A function $F : \mathbb{F}_q \to \mathbb{F}_q$ is called a *q-ary function*, which admits a unique univariate polynomial representation over $\mathbb{F}_q$:

$$F(x) = \sum_{i=0}^{q-1} \delta_i x^i, \qquad \delta_i \in \mathbb{F}_q, \tag{1}$$

where the multiple sum is calculated in finite field $\mathbb{F}_q$. The representation (1) of F can be obtained by the interpolation formula below

$$F(x) = \sum_{a \in \mathbb{F}_q} F(a) \left(1 - (x-a)^{q-1}\right).$$

In fact, denote by $\mathcal{P}$ and $\mathcal{Q}$ the set of all the polynomials in (1) and the set of all q-ary functions respectively. Then, define a mapping $L : \mathcal{P} \to \mathcal{Q}$, which maps any polynomial in $\mathcal{P}$ to the corresponding q-ary function. Because of the interpolation formula, we know that L is surjective. Since it is clear that $|\mathcal{P}| = |\mathcal{Q}| = q^q$, then L is bijective. A q-ary function F is called a *power function* if $F(x) = x^d$ for some $d \in \mathbb{Z}_q$, where $\mathbb{Z}_q$ is the residue class ring modulo q. Let $q = p^s$ for some positive integer s, where p is a prime. For $i \in \mathbb{Z}_q$, we use $\mathrm{wt}_p(i)$ to denote the sum of nonzero coefficients in the p-ary expansion $i = \sum_{k=0}^{s-1} i_k p^k$, i.e., $\mathrm{wt}_p(i) = \sum_{k=0}^{s-1} i_k$. Then, for a non-zero q-ary function $F(x) = \sum_{i=0}^{q-1} \delta_i x^i$, the *algebraic degree* of F is defined as $AD(F) = \max\{\mathrm{wt}_p(i) \mid \delta_i \neq 0, i \in \mathbb{Z}_q\}$. In this paper, if all the terms of F have the same algebraic degree, then F is called *homogeneous*. A function F is called *affine* if $AD(F) \leqslant 1$.

A function $G : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$, where q is a power of a prime, can be represented as a bivariate polynomial over $\mathbb{F}_q$,

$$G(x, y) = \sum_{i,j \in \mathbb{Z}_q} \gamma_{i,j} x^i y^j, \qquad \gamma_{i,j} \in \mathbb{F}_q, \tag{2}$$

where the multiple sum is calculated in finite field $\mathbb{F}_q$. All such polynomials form a vector space over $\mathbb{F}_q$ which has dimension q^2 and $\{x^i y^j \mid i, j \in \mathbb{Z}_q\}$ as its basis. For $i, j \in \mathbb{Z}_q$, the *degree* of $x^i y^j$, denoted by $\deg(x^i y^j)$, equals $i + j$, where the addition is calculated in characteristic 0.

Let q be a power of a prime and n be a positive integer. The *trace function* from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined as

$$\mathrm{Tr}_1^n(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}, \qquad x \in \mathbb{F}_{q^n}.$$

The trace function $\mathrm{Tr}_1^n(\cdot)$ is a linear transformation from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$, i.e., $\mathrm{Tr}_1^n(\cdot)$ is surjective, for any $a, b \in \mathbb{F}_{q^n}$, $\mathrm{Tr}_1^n(a+b) = \mathrm{Tr}_1^n(a) + \mathrm{Tr}_1^n(b)$, and for any $c \in \mathbb{F}_q$, any $a \in \mathbb{F}_{q^n}$, $\mathrm{Tr}_1^n(ca) = c\mathrm{Tr}_1^n(a)$.

We consider that in a cryptosystem, a particular key is used for one encryption, then *perfect secrecy* provides unconditional security.

Definition 2.1. *Let $\mathcal{P}$ and $\mathcal{C}$ be the plaintext space and the ciphertext space respectively. A cryptosystem has* perfect secrecy *if for any $m \in \mathcal{P}$ and any $c \in \mathcal{C}$,*

$$\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = \Pr(\mathbf{m} = m).$$

3 Relationships between homomorphisms over finite fields with q-ary functions

In this section, we study q-ary functions which are homomorphisms over finite fields. These functions preserve the multiplication and addition operations respectively. Despite of the simplicity of the results, it is difficult to find explicit references in the books.

Theorem 3.1. *A non-zero q-ary function F is a homomorphism preserving the multiplication operation if and only if F is a power function.*

Proof The sufficiency is obvious since that for any $x, y \in \mathbb{F}_q$, we have $F(xy) = (xy)^d = x^d y^d = F(x)F(y)$. We prove the necessity below.

Since F is a homomorphism, we have $F(0) = F(0)^2$, which implies $F(0) = 1$ or 0. If $F(0) = 1$, then for any $x \in \mathbb{F}_q$, $F(x) = F(x)F(0) = F(0) = 1$. Define $0^0 = 1$, and thus $F(x) = x^0$ is a power function. In the following, we consider the case $F(0) = 0$.

From $F(1) = F(1)^2$, one can deduce $F(1) = 1$, since if $F(1) = 0$, then for any $x \in \mathbb{F}_q$, $F(x) = F(x)F(1) = 0$, which contradicts that F is non-zero. Let α be a primitive element of $\mathbb{F}_q$. Note that $F(\alpha) \neq 0$, since otherwise, we have $0 = F(\alpha^{q-2})F(\alpha) = F(\alpha^{q-1}) = F(1) = 1$, a contradiction. Thus, for any $i \in \mathbb{Z}_q$,

$$F(\alpha^i) = F(\alpha)^i = \alpha^{\log_\alpha F(\alpha)^i} = \alpha^{i \log_\alpha F(\alpha)}. \tag{3}$$

Combining $F(0) = 0$ with (3), we have that for any $x \in \mathbb{F}_q$,

$$F(x) = x^{\log_\alpha F(\alpha)}.$$

Therefore, F is a power function. □

Theorem 3.2. *A non-zero q-ary function F is a homomorphism preserving the addition operation if and only if F is a non-constant homogeneous q-ary affine function.*

Proof *Sufficiency.* Let $F(x) = \sum_{i=1}^{s-1} \delta_i x^{p^i}$, where $\delta_i \in \mathbb{F}_q$. Then, for any $x, y \in \mathbb{F}_q$,

$$F(x+y) = \sum_{i=1}^{s-1} \delta_i (x+y)^{p^i} = \sum_{i=1}^{s-1} \delta_i x^{p^i} + \sum_{i=1}^{s-1} \delta_i y^{p^i} = F(x) + F(y).$$

Necessity. Let $F(x) = \sum_{i=0}^{q-1} \delta_i x^i$, where $\delta_i \in \mathbb{F}_q$. Define a function from $\mathbb{F}_q \times \mathbb{F}_q$ to $\mathbb{F}_q$ as

$$\Delta(x,y) = F(x+y) - F(x) - F(y), \quad (x,y) \in \mathbb{F}_q \times \mathbb{F}_q. \tag{4}$$

Since for any integer k, $(x+y)^{p^k} = x^{p^k} + y^{p^k}$, then from (4), we have

$$\Delta(x,y) = \sum_{i \in I} \delta_i (x+y)^i - \sum_{i \in I} \delta_i x^i - \sum_{i \in I} \delta_i y^i, \tag{5}$$

where the set I satisfies for any $i \in I$, $\delta_i \neq 0$ and $\mathrm{wt}_p(i) \geqslant 2$. Suppose that $AD(F) = \max\{\mathrm{wt}_p(i) \mid \delta_i \neq 0, i \in \mathbb{Z}_q\} \geqslant 2$, then it follows that $I \neq \emptyset$. Let $j = \sum_{k=0}^{s-1} j_k p^k \in I$, then we have

$$\begin{aligned} \delta_j (x+y)^j &= \delta_j (x+y)^{\sum_{k=0}^{s-1} j_k p^k} \\ &= \delta_j \prod_{k=0}^{s-1} \left(x^{p^k} + y^{p^k} \right)^{j_k} \\ &= \delta_j \prod_{k=0}^{s-1} \left(\sum_{l=0}^{j_k} \binom{j_k}{l} x^{lp^k} y^{(j_k - l)p^k} \right). \end{aligned}$$

If there exists $k_0 \in \mathbb{Z}_s$ such that $2 \leqslant j_{k_0} \leqslant p-1$, then since $p \nmid \binom{j_{k_0}}{l}$, there must exist a nonzero term with degree j in the expansion of $\delta_j (x+y)^j$, which can be divided by $x^{p^{k_0}} y^{p^{k_0}}$. Thus, combining (5) with the fact that $x^i y^j$, $i, j \in \mathbb{Z}_q$ are linearly independent over $\mathbb{F}_q$, we have that $\Delta(x,y)$ is a nonzero function. On the other hand, if there exist distinct $k_1, k_2 \in \mathbb{Z}_s$ such that $j_{k_1} = j_{k_2} = 1$, then there must exist a nonzero term with degree j in the expansion of $\delta_j (x+y)^j$, which can be divided by $x^{p^{k_1}} y^{p^{k_2}}$. Similarly, it follows that $\Delta(x,y)$ is a nonzero function. Hence, $F(x+y) \neq F(x) + F(y)$, a contradiction to that F is an additive homomorphism. Therefore, since $F(0) = F(0) + F(0)$, we have $AD(F) = 1$ with $F(0) = 0$. □

Combining Theorem 3.1 with Theorem 3.2, one can obtain the following corollary immediately.

Corollary 3.3. *A non-zero q-ary function F is a homomorphism preserving both the multiplication and the addition operations if and only if $F(x) = x^{p^i}$ for some integer $i \geqslant 0$, where p is the characteristic of the finite filed $\mathbb{F}_q$.*

Remark 3.4. *It is well known that the only automorphisms of a finite field $\mathbb{F}_{p^s}$ are the Frobenius automorphisms $x \mapsto x^{p^i}$ for $i = 0, \ldots, s-1$, where p is a prime. In Corollary 3.3, we claim that the only non-zero homomorphisms of $\mathbb{F}_{p^s}$ into itself are Frobenius automorphisms.*

Remark 3.5. *Corollary 3.3 essentially states that any non-zero homomorphism of finite field $\mathbb{F}_q$ into itself is an automorphism. In fact, let F be a non-zero homomorphism of $\mathbb{F}_q$, then $\mathrm{Ker}(F) = \{x \in \mathbb{F}_q \mid F(x) = 0\}$ is an ideal of $\mathbb{F}_q$, and thus $\mathrm{Ker}(F) = \{0\}$ or $\mathrm{Ker}(F) = F_q$. Since F is non-zero, then $\mathrm{Ker}(F) = \{0\}$, which implies that F is bijective. Hence, F is an automorphism.*

4 Partially homomorphic encryption schemes

In this section, we provide two partially homomorphic encryption schemes over finite fields and give the security analysis. These encryption schemes are symmetric.

4.1 A multiplicative homomorphic encryption scheme

Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and $\mathbb{Z}_{q-1}^* = \{k \in \mathbb{Z}_{q-1} \mid \gcd(k, q-1) = 1\}$, where q is a power of a prime. For a positive integer n, let η be a primitive element of $\mathbb{F}_{q^n}$, then $\beta = \eta^{(q^n-1)/(q-1)}$ is a primitive element of $\mathbb{F}_q$. For integers a and b such that $a|b$, we use a/b or $\frac{a}{b}$ to denote division of a by b. For a ring R, if $a \in R$ is invertible, then we use a^{-1} to denote the inverse of a.

- *Key-Generation*

  Choose a positive integer d such that $d|(q^n-1)/(q-1)$ and $\gcd(d, q-1) = 1$, and choose $l \in \mathbb{Z}_{q-1}^*$. The tuple (d, l) is the secret key.

- *Encryption*

  Let $\alpha = \eta^{(q^n-1)/d}$, which is a primitive d-th root of unity over $\mathbb{F}_q$. To encrypt a plaintext $m \in \mathbb{F}_q^*$, one randomly chooses $r \in \{0, 1, \ldots, d-1\}$ and computes the ciphertext as
  $$c = \gamma^{\log_\beta m} \alpha^r,$$
  where $\gamma = \eta^{l(q^n-1)/d(q-1)}$, the discrete logarithm $\log_\beta m = a$ if $\beta^a = m$.

- *Decryption*

  For $c \in \mathbb{F}_{q^n}^*$, one computes
  $$m' = c^{d \cdot l^{-1}},$$
  where l^{-1} is the inverse of l in $\mathbb{Z}_{q-1}^*$.

Remark 4.1. *In the encryption phase, since $d|(q^n-1)/(q-1)$ implies $d|(q^n-1)$, then the splitting field of x^d-1 over $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^n}$. Thus, $\{x \in \mathbb{F}_{q^n} \mid x^d = 1\} = \{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$. We also assume that the discrete logarithm over $\mathbb{F}_q$ is easy to find (that is to say, the parameter q is much less than 2^{1880}, see Footnote 1 on Page 8).*

Theorem 4.2. *The multiplicative homomorphic encryption scheme described above is correct, and it is multiplicative homomorphic.*

Proof To show the correctness, we have to prove that the decryption of an encrypted plaintext yields the same plaintext again. To decrypt a ciphertext $c = \gamma^{\log_\beta m}\alpha^r$, one computes

$$\begin{aligned} m' = c^{d\cdot l^{-1}} &= (\gamma^{\log_\beta m})^{d\cdot l^{-1}}(\alpha^r)^{d\cdot l^{-1}} \\ &= (\gamma^d)^{l^{-1}\cdot\log_\beta m}(\alpha^d)^{r\cdot l^{-1}} \\ &= \beta^{l\cdot l^{-1}\cdot\log_\beta m} \qquad (6) \\ &= m, \end{aligned}$$

where Eq.(6) is due to the facts that $\gamma^d = \beta^l$ and $\alpha^d = 1$.

The multiplicative homomorphic property is an immediate consequence of Theorem 3.1. More explicitly, let c_1 and c_2 be two encryptions of the plaintexts m_1 and m_2 respectively. Since the decryption function $F(x) = x^{d\cdot l^{-1}}$ is a power function, then F is a multiplicative homomorphism, i.e., decrypting $c_1 \cdot c_2$ yields $(c_1\cdot c_2)^{d\cdot l^{-1}} = c_1^{d\cdot l^{-1}} \cdot c_2^{d\cdot l^{-1}} = m_1 \cdot m_2$. □

4.1.1 Security analysis

In this paper, we only consider ciphertext-only attacks. We argue that the multiplicative homomorphic encryption scheme described above cannot be broken in general by ciphertext-only attacks if the parameter q satisfies some restrictions.

We first give some notations. Let n be an integer. For $i|n$, define

$$\mathcal{O}_i(n) = \{il \mod n \mid l \in \mathbb{Z}_n^*\},$$

where $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k,n) = 1\}$. Clearly, if i and j are distinct factors of n, then $\mathcal{O}_i(n) \bigcap \mathcal{O}_j(n) = \emptyset$, and we have $\bigcup_{i|n} \mathcal{O}_i(n) = \mathbb{Z}_n$. Hence, the sets $\mathcal{O}_i(n)$, $i|n$, form a partition of $\mathbb{Z}_n$.

In the above multiplicative homomorphic encryption scheme, we know that $\alpha = \eta^{(q^n-1)/d}$ is a primitive d-th root of unity over $\mathbb{F}_q$, and $\gamma = \eta^{l(q^n-1)/d(q-1)}$, where $d|(q^n-1)/(q-1)$, $\gcd(d, q-1) = 1$, $l \in \mathbb{Z}_{q-1}^*$, and η is a primitive element of $\mathbb{F}_{q^n}$. Suppose that the cryptanalyst gets c as a ciphertext. Then, there exists a plaintext $m \in \mathbb{F}_q^*$ and an integer $r \in \{0, 1, \dots, d-1\}$ such that $c = \gamma^{\log_\beta m}\alpha^r$, where $\beta = \eta^{(q^n-1)/(q-1)}$. Hence, the cryptanalyst has

$$c = \eta^{\frac{q^n-1}{q-1}\cdot\frac{1}{d}(l\log_\beta m + r(q-1))},$$

and thus $x := \frac{1}{d}(l \log_\beta m + r(q-1))$ is known.[1] The cryptanalyst will try to guess m from x, but d, l, r are unknown to him. Let $d_0 := \gcd(l \log_\beta m + r(q-1), d)$ and $d_1 := \min\{d' \mid c^{d'(q-1)} = 1\} = d/d_0 \leqslant d$. From the cryptanalyst's point of view, he can compute d_1 and

$$\begin{aligned} c^{d_1} = \eta^{\frac{q^n-1}{q-1}\cdot\frac{1}{d_0}(l \log_\beta m + r(q-1))} &= \beta^{\frac{1}{d_0}(l \log_\beta m + r(q-1))} \\ &= \beta^{\frac{1}{d_0}(l' \log_\beta m' + r'(q-1))} \end{aligned} \tag{7}$$

where l', r' are the guessed parameters, $m' \in \mathbb{F}_q^*$ is the guessed plaintext, and d_0 is unknown to the cryptanalyst.

From the above discussion, we now prove the following lemma.

Lemma 4.3. *For $m, m' \in \mathbb{F}_q^*$, there exists $l' \in \mathbb{Z}_{q-1}^*$ such that (7) holds if and only if $\gcd(\log_\beta m, q-1) = \gcd(\log_\beta m', q-1)$, i.e., $\log_\beta m, \log_\beta m' \in \mathcal{O}_i(q-1)$ for some $i|(q-1)$.*

Proof It is clear that (7) holds if and only if

$$\frac{1}{d_0}(l \log_\beta m + r(q-1)) \equiv \frac{1}{d_0}(l' \log_\beta m' + r'(q-1)) \pmod{q-1}. \tag{8}$$

Since $\gcd(d, q-1) = 1$, which implies $\gcd(d_0, q-1) = 1$, and thus d_0 is invertible modulo $q-1$. Hence, (8) holds if and only if $l \log_\beta m \equiv l' \log_\beta m' \pmod{q-1}$. This is equivalent to saying that $\gcd(l \log_\beta m, q-1) = \gcd(l' \log_\beta m', q-1)$, or equivalently, $\gcd(\log_\beta m, q-1) = \gcd(\log_\beta m', q-1)$, because l and l' are in $\mathbb{Z}_{q-1}^*$. □

Theorem 4.4. *In the above multiplicative homomorphic encryption scheme, if a cryptanalyst gets a ciphertext c and knows nothing about the secret key, then he can only find a factor i of $q-1$ such that the encrypted plaintext m satisfies $\log_\beta m \in \mathcal{O}_i(q-1)$. Moreover, for any m such that $\log_\beta m \in \mathcal{O}_i(q-1)$, the conditional probability of m given c is*

$$\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = \frac{1}{|\mathcal{O}_i(q-1)|},$$

which implies that the cryptanalyst will succeed in guessing which plaintext was encrypted with probability $1/|\mathcal{O}_i(q-1)|$.

Proof From the discussion above, we know that given a ciphertext c, a cryptanalyst can compute $d_1 = \min\{d' \mid c^{d'(q-1)} = 1\}$ and

$$c^{d_1} = \beta^{\frac{1}{d_0}(l \log_\beta m + r(q-1))} = \beta^{e_c}, \tag{9}$$

[1] Note that here we do not need to make a requirement on q such that the *Discrete Logarithm* problem (DLP) in $\mathbb{F}_{q^n}^*$ is hard to solve. Indeed, it is suggested that q^n needs to be at least 2^{1880} to make known discrete logarithm algorithms infeasible [20, Chapter 6]. Nowadays DLP can be solved for some special fields (especially with small characteristic) of size larger than 1880 bits, e.g., discrete logarithm in $\mathbb{F}_{2^{6168}}$ is solved [13].

where $e_c := \frac{1}{d_0}(l \log_\beta m + r(q-1))$ is known but $d_0 = \gcd(l \log_\beta m + r(q-1), d)$, l, r, and m are unknown. Since $\gcd(d_0, q-1) = 1$, then $\log_\beta m \in \mathcal{O}_i(q-1)$ if and only if $\gcd(e_c, q-1) = i$. Therefore, the cryptanalyst determines the factor i of $q-1$ such that $\log_\beta m \in \mathcal{O}_i(q-1)$. Thanks to Lemma 4.3, there exists $l' \in \mathbb{Z}_{q-1}^*$ such that (7) holds if and only if $\log_\beta m' \in \mathcal{O}_i(q-1)$. Hence, the cryptanalyst cannot find the exact plaintext m.

Suppose that the encrypted plaintext m satisfies $\log_\beta m \in \mathcal{O}_i(q-1)$, where $i|(q-1)$. It is easy to see that for any $j \in \mathcal{O}_i(q-1)$, the number of $l \in \mathbb{Z}_{q-1}^*$ such that $lj \mod (q-1) = j$ is exactly $\phi(q-1)/|\mathcal{O}_i(q-1)|$, where ϕ is the Euler phi function. For a fixed d, let $\mathcal{C}$ be the ciphertext space. For any $c \in \mathcal{C}$, denote by e_c the exponent of c^{d_1} based on β defined in (9). Hence, for any $m \in \mathbb{F}_q^*$ and any $c \in \mathcal{C}$, since r is randomly chosen from $\{0, \ldots, d-1\}$, then one can obtain

$$\Pr(\mathbf{c} = c \mid \mathbf{m} = m) = \frac{\phi(q-1)}{|\mathcal{O}_i(q-1)|} \cdot \frac{1}{d \cdot \phi(q-1)} = \frac{1}{d \cdot |\mathcal{O}_i(q-1)|}$$

if $\log_\beta m \in \mathcal{O}_i(q-1)$ and $\gcd(e_c, q-1) = i$, and $\Pr(\mathbf{c} = c \mid \mathbf{m} = m) = 0$ otherwise. Since for any $m \in \mathbb{F}_q^*$, $\Pr(\mathbf{m} = m) = 1/(q-1)$, then for any c such that $\gcd(e_c, q-1) = i$,

$$\begin{aligned}\Pr(\mathbf{c} = c) &= \sum_{m \in \mathbb{F}_q^*} \Pr(\mathbf{m} = m)\Pr(\mathbf{c} = c \mid \mathbf{m} = m) \\ &= \sum_{\substack{m \in \mathbb{F}_q^* \\ \log_\beta m \in \mathcal{O}_i(q-1)}} \frac{1}{q-1} \cdot \frac{1}{d \cdot |\mathcal{O}_i(q-1)|} = \frac{1}{(q-1)d}.\end{aligned}$$

By using Bayes' theorem, we have that for any $m \in \mathbb{F}_q^*$ and any $c \in \mathcal{C}$,

$$\begin{aligned}\Pr(\mathbf{m} = m \mid \mathbf{c} = c) &= \frac{\Pr(\mathbf{c} = c \mid \mathbf{m} = m)\Pr(\mathbf{m} = m)}{\Pr(\mathbf{c} = c)} \\ &= \begin{cases} \frac{1}{|\mathcal{O}_i(q-1)|}, & \text{if } \log_\beta m \in \mathcal{O}_i(q-1) \text{ and } \gcd(e_c, q-1) = i, \\ 0, & \text{otherwise.} \end{cases}\end{aligned}$$

Therefore, the cryptanalyst will succeed in guessing the encrypted plaintext with probability $1/|\mathcal{O}_i(q-1)|$. □

Corollary 4.5. *In the above multiplicative homomorphic encryption scheme, if the plaintext space is restricted to $\mathbb{F}_q^* \setminus \{1\}$, then for a cryptanalyst, by cipher-only attacks, the probability of success of guessing the plaintext from a known ciphertext is at most $1/\min_{i|(q-1), i<q-1} |\mathcal{O}_i(q-1)|$.*

Proof From Theorem 4.4, it is known that for a plaintext m satisfying $\log_\beta m \in \mathcal{O}_i(q-1)$, where $i|(q-1)$, a cryptanalyst will succeed in guessing m from the corresponding ciphertext c with probability $1/|\mathcal{O}_i(q-1)|$. Note that the set $\{\mathcal{O}_i(q-1) \mid i|(q-1), i < q-1\}$ forms a partition of $\mathbb{Z}_{q-1} \setminus \{0\}$. Since the plaintext space is restricted to $\mathbb{F}_q^* \setminus \{1\}$, then for a cryptanalyst, the probability of success of guessing the plaintext m is at most $1/\min_{i|(q-1), i<q-1} |\mathcal{O}_i(q-1)|$. □

Table 1: All numbers $9 \leqslant q \leqslant 3^{100}$ satisfying $q = 3^s$ and $(q-1)/2$ is a prime

q	$(q-1)/2$
3^3	13
3^7	1093
3^{13}	797161
3^{71}	3754733257489862401973357979128773

Remark 4.6. *If q is odd, then $\min_{i\mid(q-1), i<q-1} |\mathcal{O}_i(q-1)| = |\mathcal{O}_{(q-1)/2}(q-1)| = 1$. Thus, from Corollary 4.5, a cryptanalyst may succeed in guessing the plaintext from the ciphertext with probability 1. In fact, if $m = \beta^{(q-1)/2}$ is encrypted as c, where β is a primitive element of $\mathbb{F}_q$, then for a cryptanalyst, the probability of success of guessing m from c is 1. To increase the security of the system, we can choose odd q such that $(q-1)/2$ is a prime, and then restrict the plaintext space to $\mathbb{F}_q^* \setminus \{1, \beta^{(q-1)/2}\}$. In this case, it is easy to check that*

$$\min_{i\mid(q-1), i<q-1, i\neq(q-1)/2} |\mathcal{O}_i(q-1)| = |\mathcal{O}_1(q-1)| = \phi(q-1) = (q-3)/2.$$

Hence, a cryptanalyst can succeed in guessing the plaintext with probability at most $2/(q-3)$. In Table 1, we list some examples of $q = 3^s$, where $2 \leqslant s \leqslant 100$, which satisfy $(q-1)/2$ is a prime.

Corollary 4.7. *Let the plaintext space be restricted to $\mathbb{F}_q^* \setminus \{1\}$. Then, the multiplicative homomorphic encryption scheme described above has perfect secrecy if and only if $q-1$ is a Mersenne prime (see e.g. [19]), i.e., $q-1 = 2^s - 1$ is a prime for some prime s.*

Proof *Sufficiency.* Since $q-1$ is a prime, then $\mathbb{Z}_{q-1} \setminus \{0\} = \mathcal{O}_1(q-1)$. Let β be a primitive element of $\mathbb{F}_q$, then for any $m \in \mathbb{F}_q^* \setminus \{1\}$, we have $\log_\beta m \in \mathbb{Z}_{q-1} \setminus \{0\} = \mathcal{O}_1(q-1)$. According to Theorem 4.4, we have that for every $m \in \mathbb{F}_q^* \setminus \{1\}$ and every $c \in \mathcal{C}$, the conditional probability of m given a ciphertext c, is

$$\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = \frac{1}{|\mathcal{O}_1(q-1)|} = \Pr(\mathbf{m} = m).$$

Therefore, from Definition 2.1, the multiplicative homomorphic encryption scheme has perfect secrecy.

Necessity. It is known that for every $m \in \mathbb{F}_q^* \setminus \{1\}$ and every $c \in \mathcal{C}$,

$$\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = \Pr(\mathbf{m} = m) = \frac{1}{q-2}.$$

From Theorem 4.4, we have that $\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = 1/|\mathcal{O}_i(q-1)|$ for some $i|(q-1)$. Therefore, for every integer i satisfying $i|(q-1)$ and $i < q-1$, we have $|\mathcal{O}_i(q-1)| = q-2$, which implies that $q-1$ is a prime. Note that q is a power of a prime. If q is odd, then $q-1$ is even which cannot be a prime. Hence, q is a power of 2 such that $q-1$ is a prime, i.e., $q-1$ is a Mersenne prime. □

Remark 4.8. *From Corollary 4.7, we know that to achieve perfect secrecy, the parameter q chosen in the multiplicative homomorphic encryption scheme should satisfy $q-1$ is a Mersenne prime. In practice, it would be suitable to choose some prime power q such that $\min_{i|(q-1), i\notin A} |\mathcal{O}_i(q-1)|$ takes a high value, where $A \subseteq \{1, 2, \ldots, q-1\}$, and the plaintext space is restricted to $m \in \mathbb{F}_q^* \setminus \{\beta^i \mid i \in A\}$. See Remark 4.6 for example.*

Remark 4.9. *In the multiplicative homomorphic encryption scheme with constraints in Corollary 4.7, we have proved that for only one encryption, the scheme has perfect secrecy. In fact, homomorphic encryption schemes cannot in a one-time pad setting, and a reuse of the secret key could lead to a break of the scheme. However, if the size of the finite field is chosen to be large enough, we can show that the proposed multiplicative homomorphic encryption scheme can resist cipher-only attacks to some extent. Suppose that the cryptanalyst gets a sequence of ciphertexts $c_1, \ldots, c_s$ encrypted by the secret key (d, l). Then, he can compute $\bar{d} = \max_{1\leqslant i\leqslant s} \left\{ \min \left\{ d' \mid c_i^{d'(q-1)} = 1 \right\} \right\}$ and get the multiset $C = \{\ast\ c_1^{\bar{d}}, \ldots, c_s^{\bar{d}}\ \ast\}$. In the case $\bar{d} = d$, the cryptanalyst can only guess the encrypted plaintext sequence $m_1, \ldots, m_s$ correctly with probability $1/(q-2)$, since he knows nothing about the parameter l. Thus, when q is large enough (but much less than 2^{1880}, see Remark 4.1), the probability of success of guessing the correct plaintext sequence is still very small.*

4.2 An additive homomorphic encryption scheme

Let q be a power of a prime and n be a positive integer, and $F(x) = \sum_{i=0}^{n-1} \delta_i x^{q^i} - \alpha$ be a q^n-ary affine function, where $\alpha \in \mathbb{F}_{q^n}$ and $\delta_i \in \mathbb{F}_{q^n}$, $i = 0, \ldots, n-1$. An element $\beta \in \mathbb{F}_{q^n}$ is a *root* of $F(x)$ if and only if $F(\beta) = \alpha$. For a q^n-ary affine function F, the determination of all the roots of F in $\mathbb{F}_{q^n}$ is an easy task (see e.g. [14, Chapter 3]).

- *Key-Generation*

  Choose $\alpha \in \mathbb{F}_{q^n}^*$ as the secret key. Define a q^n-ary function $F(x) = \mathrm{Tr}_1^n(\alpha x)$.

- *Encryption*

  To encrypt a plaintext $m \in \mathbb{F}_q$, one randomly chooses a root $c \in \mathbb{F}_{q^n}$ of the affine q-polynomial $F(x) - m$. Then, c is the ciphertext.

- *Decryption*

  For $c \in \mathbb{F}_{q^n}$, one computes $m' = F(c)$.

Theorem 4.10. *The additive homomorphic encryption scheme described above is correct, and it is additive homomorphic.*

Proof The correctness of the scheme is obvious. The additive homomorphic property is an immediate consequence of the fact that the trace function is linear, i.e., decrypting c_1+c_2 yields $F(c_1+c_2) = \mathrm{Tr}_1^n(\alpha(c_1+c_2)) = \mathrm{Tr}_1^n(\alpha c_1) + \mathrm{Tr}_1^n(\alpha c_2) = F(c_1)+F(c_2) = m_1+m_2$. □

4.2.1 Security analysis

In this paper, we only consider ciphertext-only attacks. In the above additive homomorphic encryption scheme, if a ciphertext $c = 0$, then the encrypted plaintext m must be 0. Therefore, we always assume that $m = 0$ is encrypted as a nonzero element in $\mathbb{F}_{q^n}$.

Theorem 4.11. *The additive homomorphic encryption scheme described above has perfect secrecy.*

Proof Let $\{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For a ciphertext $c \in \mathbb{F}_{q^n}^*$, there must exist $j \in \{1, \ldots, n\}$ such that $\mathrm{Tr}_1^n(\beta_j c) \neq 0$. For any $m \in \mathbb{F}_q$ and any $a_i \in \mathbb{F}_q$, $i \in \{1, \ldots, n\} \setminus \{j\}$, define

$$a_j = \left(m - \sum_{i \in \{1,\ldots,n\} \setminus \{j\}} a_i \mathrm{Tr}_1^n(\beta_i c) \right) \left(\mathrm{Tr}_1^n(\beta_j c)\right)^{-1}.$$

Then, we have $\sum_{i=1}^n a_i \mathrm{Tr}_1^n(\beta_i c) = m$, i.e., $\mathrm{Tr}_1^n(\sum_{i=1}^n a_i \beta_i c) = m$. Define $\alpha = \sum_{i=1}^n a_i \beta_i$, then $\mathrm{Tr}_1^n(\alpha c) = m$. For $m \in \mathbb{F}_q^*$, there are q^{n-1} possible $\alpha \in \mathbb{F}_{q^n}^*$ such that $\mathrm{Tr}_1^n(\alpha c) = m$. If $m = 0$ and $a_i = 0$ for $i \in \{1, \ldots, n\} \setminus \{j\}$, then $a_j = 0$, which leads to $\alpha = 0$. So, for $m = 0$, there are only $q^{n-1} - 1$ possible $\alpha \in \mathbb{F}_{q^n}^*$ such that $\mathrm{Tr}_1^n(\alpha c) = m$. Note that we always assume that $m = 0$ is encrypted as a nonzero element in $\mathbb{F}_{q^n}$. Hence, for any $m \in \mathbb{F}_q$ and any $c \in \mathbb{F}_{q^n}^*$, since a root $c \in \mathbb{F}_{q^n}^*$ is randomly chosen from the solution space of dimension $n-1$, then we have

$$\Pr(\mathbf{c} = c \mid \mathbf{m} = m) = \begin{cases} \frac{q^{n-1}}{q^n-1} \cdot \frac{1}{q^{n-1}} = \frac{1}{q^n-1}, & \text{if } m \in \mathbb{F}_q^*, \\ \frac{q^{n-1}-1}{q^n-1} \cdot \frac{1}{q^{n-1}-1} = \frac{1}{q^n-1}, & \text{if } m = 0. \end{cases}$$

Since for any $m \in \mathbb{F}_q$, $\Pr(\mathbf{m} = m) = 1/q$, then for any $c \in \mathbb{F}_{q^n}^*$,

$$\Pr(\mathbf{c} = c) = \sum_{m \in \mathbb{F}_q} \Pr(\mathbf{m} = m)\Pr(\mathbf{c} = c \mid \mathbf{m} = m) = \frac{1}{q^n - 1}.$$

By using Bayes' theorem, we have that for any $m \in \mathbb{F}_q$ and any $c \in \mathbb{F}_{q^n}^*$,

$$\Pr(\mathbf{m} = m \mid \mathbf{c} = c) = \frac{\Pr(\mathbf{c} = c \mid \mathbf{m} = m)\Pr(\mathbf{m} = m)}{\Pr(\mathbf{c} = c)} = \frac{1}{q} = \Pr(\mathbf{m} = m).$$

Therefore, from Definition 2.1, the additive homomorphic encryption scheme has perfect secrecy. □

Remark 4.12. *In the additive homomorphic encryption scheme described above, we have proved that for only one encryption, the scheme has perfect secrecy. Similar to the discussion in Remark 4.9, we will show that if the size of the finite field is chosen to be large enough, the proposed additive homomorphic encryption scheme can resist cipher-only attacks to some extent. Suppose that the cryptanalyst gets a sequence of ciphertexts* $c_1, \ldots, c_s$ *encrypted by the secret key* α*. If* $c_1, \ldots, c_s$ *span a* t*-dimensional vector space over* F_q*, then the cryptanalyst can only guess the encrypted plaintext sequence* $m_1, \ldots, m_s$ *correctly with probability* $1/q^t$ *if* $t < n$*, and* $1/(q^n - 1)$ *otherwise, since he knows nothing about the parameter* α*. Thus, when* q *is large enough, the probability of success of guessing the correct plaintext sequence is still very small.*

5 Concluding remarks

In this paper, we studied symmetric partially homomorphic encryption schemes over finite fields. We showed that non-zero multiplicative (or additive) homomorphisms over finite fields are equivalent to q-ary power functions (or non-constant homogeneous q-ary affine functions). We proposed two homomorphic encryption schemes with reasonable computation and communication costs, and discussed security of our schemes in terms of cipher-only attacks. Since our schemes are not based on hardness assumptions, semantic security (see [12]) is not considered here (this concept is mainly discussed under a given hardness assumption). In [3] and [15], it is proved that any fully homomorphic encryption scheme over finite fields (or rings) cannot resist against cipher-only attacks. As an extended work, we find two partially homomorphic encryption schemes which have perfect secrecy and can resist against cipher-only attacks to some extent.

References

[1] F. Armknecht and A.-R. Sadeghi, A new approach for algebraically homomorphic encryption, IACR Cryptology ePrint Archive, 2008/422, 2008.

[2] J. Benaloh, Verifiable Secret-Ballot Elections, PhD thesis, Yale University, New Haven, USA, 1987.

[3] D. Boneh and R. Lipton, Searching for elements in black-box fields and applications, In: *Advances in Cryptology—CRYPTO'96,* Lecture Notes in Computer Science, vol.1109, Berlin: Springer-Verlag, pp.283–297, 1996.

[4] Z. Brakerski and V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent messages, In: *Advances in Cryptology—CRYPTO 2011,* Lecture Notes in Computer Science, vol.6841, Berlin: Springer-Verlag, pp.505–524, 2011.

[5] Z. Brakerski, Fully homomorphic encryption without modulus switching from classical gapSVP, In: *Advances in Cryptology—CRYPTO 2012,* Lecture Notes in Computer Science, vol.7417, Berlin: Springer-Verlag, pp.868–886, 2012.

[6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, Private information retrieval, *Journal of the ACM,* vol.45, no.6, pp.965-981, 1998.

[7] R. Cramer, I. Damgaard, and J. Nielsen, Multiparty computation from threshold homomorphic encryption, In: *Advances in Cryptology—EUROCRYPT 2001,* Lecture Notes in Computer Science, vol.2045, Berlin: Springer-Verlag, pp.280–300, 2001.

[8] J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism, In: *Proceedings of the 5th International Conference, ISC 2002,* Lecture Notes in Computer Science, vol.2433, Berlin: Springer-Verlag, pp.471–483, 2002.

[9] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, In: *Advances in Cryptology—CRYPTO'84,* Lecture Notes in Computer Science, vol.196, Berlin: Springer-Verlag, pp.10–18, 1985.

[10] C. Gentry, Fully homomorphic encryption using ideal lattices, In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC'09,* pp.169–178, 2009.

[11] C. Gentry, A Fully Homomorphic Encryption Scheme, PhD thesis, Stanford University, California, USA, 2009.

[12] S. Goldwasser and S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information, In: *Proceedings of the 14th Annual ACM Symposium on Theory of Computing, STOC'82,* pp.365–377, 1982.

[13] A. Joux, Discrete logarithm in $\mathbb{F}_{2^{6168}}$, announcement to the Number Theory List, 2013.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol.20, New York: Cambridge University Press, 1997.

[15] U. Maurer and D. Raub, Black-box extension fields and the inexistence of field homomorphic one-way permutations, In: *Advances in Cryptology—ASIACRYPT 2007,* Lecture Notes in Computer Science, vol.4833, Berlin: Springer-Verlag, pp.427–443, 2007.

[16] T. Okamoto and S. Uchiyama, A new public-key cryptosystem as secure as factoring, In: *Advances in Cryptology—EUROCRYPT'98,* Lecture Notes in Computer Science, vol.1403, Berlin: Springer-Verlag, pp.308–318, 1998.

[17] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, In: *Advances in Cryptology—EUROCRYPT'99,* Lecture Notes in Computer Science, vol.1592, Berlin: Springer-Verlag, pp.223–238, 1999.

[18] R. Rivest, L. Adleman, and M. Dertouzos, On data banks and privacy homomorphisms, In: *Foundations of Secure Computation,* New York: Academic Press, pp.169–179, 1978.

[19] N. J. A. Sloane, *A Handbook of Integer Sequences,* Academic Press, 1973.

[20] D. R. Stinson, *Cryptography: Theory and Practice (third edition),* Boca Raton: CRC Press, 2006.

[21] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, Fully homomorphic encryption over the integers, In: *Advances in Cryptology—EUROCRYPT 2010,* Lecture Notes in Computer Science, vol.6110, Berlin: Springer-Verlag, pp.24–43, 2010.

[22] D. Wagner, Cryptanalysis of an algebraic privacy homomorphism, In: *Proceedings of the 6th International Conference, ISC 2003,* Lecture Notes in Computer Science, vol.2851, Berlin: Springer-Verlag, pp.234-239, 2003.