Partially homomorphic encryption schemes over finite fields

Jian Liu[1], Sihem Mesnager[2] and Lusheng Chen[3]

[1]School of Computer Software, Tianjin University, Tianjin, China
and CNRS, LAGA, UMR 7539, Paris, France
[2]University of Paris VIII, Department of mathematics
and University of Paris XIII LAGA, CNRS, UMR 7539 and Telecom Paris-Tech, France
[3] School of Mathematical Sciences, Nankai University, Tianjin, China

Homomorphic encryption

Homomorphic encryption schemes are cryptographic constructions which enable to securely perform operations on encrypted data without ever decrypting them.

- ☞ Let $(G, *)$ be a group, $m_1, m_2 \in G$ and k the encryption key. Compute efficiently $\mathrm{E}_k(m_1 * m_2)$ without decrypting $c_1 := \mathrm{E}_k(m_1)$ and $c_2 = \mathrm{E}_k(m_2)$.

Outline

1. Some background
2. Partially homomorphic encryption schemes over finite fields :
   - A multiplicative homomorphic encryption scheme ;
   - A additive homomorphic encryption scheme.
3. Conclusions

Definition

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

Definition

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 $\mathbb{F}_q$:

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

The representation (1) of F can be obtained by the interpolation formula below

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

DEFINITION

Let $q = p^s$ for some positive integer s, where p is a prime.

- *For $i \in \mathbb{Z}_q$, (where $\mathbb{Z}_q$ is the residue class ring modulo q) $i = \sum_{k=0}^{s-1} i_k p^k$, $\mathrm{wt}_p(i) = \sum_{k=0}^{s-1} i_k$.*
- *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 $AD(F) = \max\{\mathrm{wt}_p(i) \mid \delta_i \neq 0, i \in \mathbb{Z}_q\}$.*
- *A function F is called affine if $AD(F) \leqslant 1$.*

☞ In this talk, if all the terms of F have the same algebraic degree, then F is called *homogeneous*.

Definition

A q-ary function F is called a power function if $F(x) = x^d$ for some $d \in \mathbb{Z}_q$.

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 $\mathbb{F}_q$,

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

where the multiple sum is calculated in finite field $\mathbb{F}_q$.

Definition

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

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

Relationships between homomorphisms over finite fields with q-ary functions

THEOREM

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

THEOREM

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

Relationships between homomorphisms over finite fields with q-ary functions

From the previous statements, one gets :

Corollary

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 field $\mathbb{F}_q$.

Remark

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 the above corollary, we claim that the only non-zero homomorphisms of $\mathbb{F}_{p^s}$ into itself are Frobenius automorphisms.

Homomorphic encryption

- Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.
- This is sometimes a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services.
- Homomorphic encryption schemes are malleable by design. This enables their use in cloud computing environment for ensuring the confidentiality of processed data. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems.
  1. Partially homomorphic encryption
  2. Fully homomorphic encryption

Homomorphic encryption

☞ In this talk we are interested in partially homomorphic crypto-systems

Examples of partially homomorphic crypto-systems :

- Unpadded RSA (1977)
- In the Goldwasser-Micali cryptosystem (1982)
- In the ElGamal cryptosystem (1984)
- In the Benaloh cryptosystem (1994)
- The Okamoto-Uchiyama cryptosystem (1998)
- The Naccache-Stern cryptosystem (1998)
- In the Paillier cryptosystem (1999)
- Damgard-Jurik cryptosystem (2001)
- Boneh-Goh-Nissim cryptosystem (2005)
- etc.

Partially homomorphic encryption schemes

- ☞ We provide two partially homomorphic encryption schemes over finite fields and give the security analysis. Our encryption schemes are symmetric.

- ☞ Symmetric ciphers purposed for Fully Homomorphic Encryption (FHE) have recently been proposed for two main reasons. First, minimizing the implementation (time and memory) overheads that are inherent to current FHE schemes. Second, improving the homomorphic capacity. [Meaux-Journault-Standaert-Carlet 2016] have proposed stream ciphers for efficient FHE with low-noise ciphertexts.

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 $\mathbb{F}_q$.

Partially homomorphic encryption schemes : a multiplicative homomorphic encryption scheme

- 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 $\mathbb{Z}^*_{q-1}$.

THEOREM

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

Proof The decryption of an encrypted plaintext yields the same plaintext again : to decrypt a ciphertext $c = \gamma^{\log_\beta m}\alpha^r$, one computes

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

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 $(c_1 \cdot c_2)^{d\cdot l^{-1}} = c_1^{d\cdot l^{-1}} \cdot c_2^{d\cdot l^{-1}} = m_1 \cdot m_2$.

Security analysis :

- ☞ We only consider ciphertext-only attacks.

Notation : for $i|n$, define $\mathcal{O}_i(n) = \{il \mod n \mid l \in \mathbb{Z}_n^*\}$, where $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$.

THEOREM

In the above 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

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

Security analysis :

Corollary

In the previous 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* $1/\min_{i|(q-1),i<q-1} |\mathcal{O}_i(q-1)|$.

Remark

If q *is odd, then* $\min_{i|(q-1),i<q-1} |\mathcal{O}_i(q-1)| = |\mathcal{O}_{(q-1)/2}(q-1)| = 1$*. Thus, from Corollary 6, 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*

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

Perfect secrecy

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

Definition

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 $c \in \mathcal{C}$,

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

Security analysis :

Proposition

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, i.e., $q-1 = 2^s - 1$ is a prime for some prime s.

Remark

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 $m \in \mathbb{F}_q^* \setminus \{\beta^i \mid i \in A\}$.

Security analysis :

Remark

- *Our 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.*
- *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* $C = \{* \, c_1^{\bar{d}}, \ldots, c_s^{\bar{d}} \, *\}$*. 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, the probability of success of guessing the correct plaintext sequence is still very small.*

Partially homomorphic encryption schemes : 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.

- 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 $m' = F(c)$.

An additive homomorphic encryption scheme

Theorem

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
$F(c_1 + c_2) = \mathrm{Tr}_1^n(\alpha(c_1 + c_2)) = \mathrm{Tr}_1^n(\alpha c_1) + \mathrm{Tr}_1^n(\alpha c_2) = F(c_1) + F(c_2) = m_1 + m_2$.

Security analysis :

- ☞ 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

The additive homomorphic encryption scheme described above has perfect secrecy.

Proof (1/2) 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 $\mathrm{Tr}_1^n(\alpha c) = m$. For $m = 0$, there are only $q^{n-1} - 1$ possible $\alpha \in \mathbb{F}_{q^n}^*$ such that $\mathrm{Tr}_1^n(\alpha c) = m$. 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 $c \in \mathbb{F}_{q^n}^*$,

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

Proof (2/2) 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 the definition of perfect secrecy, the additive homomorphic encryption scheme has perfect secrecy.

Security analysis :

Remark

In the additive homomorphic encryption scheme described above, we have proved that for only one encryption, the scheme has perfect secrecy. We can 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.*

Conclusions

We have studied symmetric partially homomorphic encryption schemes over finite fields.

- We showed that non-zero multiplicative (or additive) homomorphisms over finite fields are equivalent to power functions (or non-constant homogeneous 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.
- In [Boneh-Lipton 1996] and [Maurer-Raub 2007], 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.
- Since our schemes are not based on hardness assumptions, semantic security [Goldwasser-Micali 1982] is not considered here (this concept is mainly discussed under a given hardness assumption).