Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information Processing Letters 97 (2006) 118–123
Information Processing Letters
www.elsevier.com/locate/ipl

# Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme

Jung Hee Cheon [a], Woo-Hwan Kim [b,*], Hyun Soo Nam [a]

[a] *ISaC and Department of Mathematical Sciences, Seoul National University, San 56-1 Shinrim-dong, Kwanak-gu, Seoul 151-747, Republic of Korea*

[b] *National Security Research Institute, 161 Gajeong-dong, Yuseong-gu, Daejeon 305-350, Republic of Korea*

Received 11 May 2004; received in revised form 28 February 2005; accepted 27 September 2005

Available online 7 November 2005

Communicated by Y. Desmedt

**Abstract**

We propose cryptanalysis of the First Domingo-Ferrer's algebraic privacy homomorphism $\mathcal{E}:\mathbb{Z}_n \to (\mathbb{Z}_p \times \mathbb{Z}_q)^d$ where $n = pq$. We show that the scheme can be broken by $(d+1)$ known plaintexts in $O(d^3 \log^2 n)$ time. Even when the modulus $n$ is kept secret, it can be broken by $2(d+1)$ known plaintexts in $O(d^4 \log dn + d^3 \log^2 n + \varepsilon(m))$ time with overwhelming probability.


*Keywords:* Privacy homomorphism; Cryptanalysis; Safety/security in digital systems

## 1. Introduction

The concept of *processing encrypted data* was firstly introduced by Rivest et al. [11] in 1978. A privacy homomorphism is an encryption function which allows processing the encrypted data without knowledge of the decryption function. More precisely, an *algebraic* privacy homomorphic encryption $\mathcal{E}$ over a ring $\mathcal{R}$ is an encryption function which has efficient algorithms to compute $\mathcal{E}(xy)$ and $\mathcal{E}(x+y)$ from $\mathcal{E}(x)$ and $\mathcal{E}(y)$ without revealing $x$ and $y$. One example of an algebraic privacy homomorphism [11] is as follows:

**Example 1.** Let $p, q$ be large primes, and $n = pq$.

$$\mathcal{P} = \mathbb{Z}_n, \qquad \mathcal{C} = \mathbb{Z}_p \times \mathbb{Z}_q,$$
$$\mathcal{E}(x) = (x \bmod p, x \bmod q)$$

and decryption is done using the Chinese remainder theorem.

This function is an algebraic privacy homomorphism under the usual modular addition and modular multiplication. Unfortunately, it is shown that this algebraic privacy homomorphism can be broken using a known-plaintext attack [5].

In 1991, Feigenbaum and Merritt [8] questioned directly whether an algebraic privacy homomorphism does exist. Many schemes are suggested, but almost all of them are shown to be insecure [5,3,13,14]. In particular, Ahituv et al. showed that any algebraic privacy homomorphism can be broken efficiently by cho-

* Corresponding author.
*E-mail addresses:* jhcheon@math.snu.ac.kr (J.H. Cheon), whkim5@etri.re.kr (W.-H. Kim), hsnam@math.snu.ac.kr (H.S. Nam).

0020-0190/$ – see front matter 
doi:10.1016/j.ipl.2005.09.016

sen ciphertext attacks [2]. Boneh and Lipton proved that any deterministic algebraic privacy homomorphism over rings $\mathbb{Z}_n$ can be broken in sub-exponential time under a (reasonable) number theoretic assumption [4]. Domingo-Ferrer proposed two algebraic privacy homomorphisms in 1996 and 2002 [6,7]. The second one is broken by Bao [3] and Wagner [13,14]. But there is no serious attack on the first scheme. It is the only algebraic privacy homomorphism that remains secure to the authors' knowledge.

In this paper, we analyze the original privacy homomorphism of Domingo-Ferrer [6], and show that it is not secure against known-plaintext attacks. When we consider an encryption function from $\mathbb{Z}_n$ to $(\mathbb{Z}_p \times \mathbb{Z}_q)^d$ for $n = pq$, it can be broken by $d+1$ plaintext–ciphertext pairs in $O(d^3 \log^2 n)$ with the probability larger than $1 - 2/(p-1)$. Even when $n$ is kept secret, it can be broken by $d+1$ more pairs in $O(d^4 \log dn + d^3 \log^2 n + \varepsilon(m))$ with the probability larger than $(1 - 1/2^{m-2}) \cdot (1 - 2/(p-1))$ where $\varepsilon(m) = O(2^{2m})$.

The outline of the paper is as follows: In Section 2, we introduce the Domingo-Ferrer's scheme. In Section 3, we propose known-plaintext attacks for the scheme. The analysis consists of two parts. One is the case that the modulus of the input space is public and the second is the case that the modulus is kept secret. We conclude in Section 4.

## 2. Domingo-Ferrer's algebraic privacy homomorphism

In this section, we introduce the first Domingo-Ferrer scheme [6]. Let $p, q$ be large primes and $n = pq$. For a positive integer $d$, we set $\mathcal{P} = \mathbb{Z}_n$, $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_q)^d$.

(1) **Setup**. Take two large primes $p$ and $q$ and compute $n = pq$. Choose a positive integer $d$. $r_p \in \mathbb{Z}_p^*$ and $r_q \in \mathbb{Z}_q^*$ are randomly selected so that each of them generates a large subgroup of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively. The public parameter is $(d, n)$ and the secret parameter is $(p, q, r_p, r_q)$. To increase the security $n$ can be kept secret, but in this case encrypted data can be processed less efficiently.

(2) **Encrypt**. *Randomly split* $x \in \mathbb{Z}_n$ into $x_1, x_2, \ldots, x_d$ so that $x = \sum_{i=1}^{d} x_i \bmod n$ and $x_i \in \mathbb{Z}_n$.

$$\mathcal{E}(x) = \big([x_1 r_p \bmod p, x_1 r_q \bmod q], \ldots, [x_d r_p^d \bmod p, x_d r_q^d \bmod q]\big).$$

(3) **Decrypt**. For each $j$, to retrieve the $[x_j \bmod p, x_j \bmod q]$, compute the scalar product of the $j$th coordinate $[x_j r_p^j \bmod p, x_j r_q^j \bmod q]$ pair by $([r_p^{-j} \bmod p, r_q^{-j} \bmod q])$. Add them up to get $[x \bmod p, x \bmod q]$. Use the Chinese remainder theorem to get $x \bmod n$.

To explain the operation of ciphertexts, we adopt a polynomial notation: Denote a polynomial $f(X) = a_1 X + a_2 X^2 + \cdots + a_d X^d$ by its coefficient vectors $(a_1, a_2, \ldots, a_d)$. Then we have $\mathcal{E}(x) = (f_x(r_p X) \bmod p, f_x(r_q X) \bmod q)$ for a polynomial $f_x(X) \in \mathbb{Z}_n[X]$ with $f_x(0) \equiv 0 \bmod n$ and $f_x(1) \equiv x \bmod n$. Given $\mathcal{E}(x) = (p_x(X), q_x(X))$ and $\mathcal{E}(x') = (p_{x'}(X), q_{x'}(X))$, we have

$$\mathcal{E}(x+y) = \big(p_x(X) + p_{x'}(X) \bmod n, q_x(X) + q_{x'}(X) \bmod n\big),$$
$$\mathcal{E}(xy) = \big(p_x(X) p_{x'}(X) \bmod n, q_x(X) q_{x'}(X) \bmod n\big).$$

Note that a multiplication doubles up the number of components in a ciphertext. If $n$ is secret, the operations are done in $\mathbb{Z}[x]$. Domingo-Ferrer's scheme is an algebraic privacy homomorphism with respect to the operation of addition and multiplication in $\mathbb{Z}_n[X]$ or $\mathbb{Z}[X]$. This scheme is claimed to be secure against known-plaintext attacks when $d > 1$. Note that if $d = 1$, $r_p = 1$, and $r_q = 1$, Domingo-Ferrer's scheme is simply the scheme in Example 1.

## 3. Cryptanalysis of Domingo-Ferrer's scheme

We show that Domingo-Ferrer's scheme can be broken with $d+1$ known plaintexts when $n$ is known and with one more known plaintexts when $n$ is unknown. Without loss of generality, we assume $p < q$ throughout this paper.

### 3.1. The case that n is public

Assume we have $d+1$ plaintext–ciphertext pairs $\{(x_i, Y_i, Z_i) \mid i = 1, \ldots, d+1\}$ where $x_i = x_{i1} + \cdots + x_{id} \bmod n$ and

$$Y_i = (y_{i1}, \ldots, y_{id}) = \big(x_{i1} r_p \bmod p, \ldots, x_{id} r_p^d \bmod p\big),$$
$$Z_i = (z_{i1}, \ldots, z_{id}) = \big(x_{i1} r_q \bmod q, \ldots, z_{id} r_q^d \bmod q\big)$$

for $i = 1, \ldots, d+1$. By letting $t = r_p^{-1}$, we have

$$f_i(t) = -x_i + y_{i1} t + y_{i2} t^2 + \cdots + y_{id} t^d \equiv 0 \bmod p$$

for $i = 1, \ldots, d+1$. This can be written as the following matrix:

$$\begin{pmatrix} x_1 & y_{11} & y_{12} & \cdots & y_{1d} \\ x_2 & y_{21} & y_{22} & \cdots & y_{2d} \\ & & \vdots & & \\ x_{d+1} & y_{d+1,1} & y_{d+1,2} & \cdots & y_{d+1,d} \end{pmatrix} \begin{pmatrix} -1 \\ t \\ \vdots \\ t^d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod p. \quad (1)$$

Since the homogeneous equation (1) has a nontrivial solution in $\mathbb{Z}_p^{d+1}$, the determinant $\det(A_p)$ of the coefficient matrix $A_p$ of Eq. (1) is zero mod $p$. We may apply Gaussian elimination to $A_p$ over $\mathbb{Z}_n$ to compute $\det(A_p)$ since a prime factor of $n$ can be obtained when a failure happens in Gaussian elimination. Gaussian elimination of a $(d+1)\times(d+1)$ matrix over $\mathbb{Z}_n$ takes $O(d^3 \log^2 n)$ bit operations. On the other hand, $\Pr[\det(A_p) \neq 0 \bmod q]$ is overwhelming as in the following lemma:

**Lemma 2.** *Let $p$ and $q$ be primes with $p < q$ and $M = (v_{ij})$ be an $\ell \times \ell$ random matrix with $0 \leqslant v_{ij} < p$. Then the probability that $\det(M) \not\equiv 0 \bmod q$ is larger than $e^{-3/2(p-1)}$.*

**Proof.** Let $v_i = (v_{1i}, \ldots, v_{\ell i})$ be the $i$th column vector of $M$. Then $\det(M) \not\equiv 0 \bmod q$ if and only if $\{v_1, \ldots, v_\ell\}$ is linearly independent over $\mathbb{Z}_q$. Thus we estimate the size of the set

$$I = \big\{(v_1, \ldots, v_\ell) \mid \{v_1, \ldots, v_\ell\} \text{ is linearly independent over } \mathbb{Z}_q, 0 \leqslant v_{ij} < p\big\}.$$

Suppose that $\{v_1, \ldots, v_k\}$ is linearly independent over $\mathbb{Z}_q$ and each entry of $v_i$ is contained in $[0, p-1]$. Consider an $\ell \times k$ matrix whose $i$th column is $v_i$. Since the rank of the matrix is $k$, there is a submatrix of rank $k$ made by $k$ rows of the matrix:

$$\begin{pmatrix} v_{j_1 1} & v_{j_1 2} & \cdots & v_{j_1 k} \\ & \vdots & & \\ v_{j_k 1} & v_{j_k 2} & \cdots & v_{j_k k} \end{pmatrix}.$$

Denote the set of linear combinations of $\{v_1, \ldots, v_k\}$ over $\mathbb{Z}_q$ by $\langle v_1, \ldots, v_k\rangle$. Suppose $v_{k+1}$ is contained in $\langle v_1, \ldots, v_k\rangle$ and $v_{j,k+1} \in [0, p-1]$ for all $j$. Then $a_1, \ldots, a_k \in \mathbb{Z}_q$ are uniquely determined such that

$$\begin{pmatrix} v_{j_1 k+1} \\ \vdots \\ v_{j_k k+1} \end{pmatrix} = a_1 \begin{pmatrix} v_{j_1 1} \\ \vdots \\ v_{j_k 1} \end{pmatrix} + \cdots + a_k \begin{pmatrix} v_{j_1 k} \\ \vdots \\ v_{j_k k} \end{pmatrix}.$$

Other places of $v_{k+1}$ are determined according to $v_{k+1} = \sum a_i v_i$ and the number of such $v_{k+1}$'s cannot exceed $p^k$. Therefore $|I|$ is larger than $(p^\ell - 1)(p^\ell - p)\cdots(p^\ell - p^{\ell-1})$. The probability that $\{v_1, v_2, \ldots, v_\ell\}$ is linearly independent is larger than

$$\begin{aligned} &\frac{(p^\ell - 1)(p^\ell - p)\cdots(p^\ell - p^{\ell-1})}{(p^\ell)^\ell} \\ &= \left(1 - \frac{1}{p^\ell}\right)\left(1 - \frac{1}{p^{\ell-1}}\right)\cdots\left(1 - \frac{1}{p}\right) \\ &\geqslant e^{-\frac{3}{2}\frac{1}{p^\ell}(1+p+\cdots+p^\ell)} \geqslant e^{-\frac{3}{2(p-1)}} \\ &\left(\because 1 - x \geqslant e^{-\frac{3}{2}x} \quad \text{for } 0 \leqslant x \leqslant \frac{1}{2}\right). \qquad \square \end{aligned}$$

From Lemma 2, we can obtain $\gcd(\det(A) \bmod n, n) = p$ and $q = n/p$ with probability larger than $e^{-\frac{3}{2(p-1)}}$. Once $p$ is known, $r_p$ can be obtained by computing

$$g(t) := \gcd\big(f_1(t), \ldots, f_{d+1}(t)\big)$$

since $(t - r_p^{-1})$ divides $g(t)$. The greatest common divisor of two polynomials in $\mathbb{Z}_p[x]$ of degrees less than $d$ can be computed by $O(d^2 \log^2 p)$ bit operations [10]. Thus $g(t)$ can be computed by $O(d^3 \log^2 p)$ bit operations. The degree of $g(t)$ may not be 1 but we show that the probability is negligible. Let $f_i' = f_i/(t - r_p^{-1})$ for $i = 1, \ldots, d+1$. We may assume that $f_i'$'s are random polynomials of degree $d-1$ over $\mathbb{Z}_p$.

**Lemma 3.** *Let $g_1, \ldots, g_k$ be random polynomials of degree $\ell$ over $\mathbb{Z}_p$. Then there is no common root of $g_i$'s with probability larger than $(1 - 1/p^{k-1})^\ell$.*

**Proof.** Assume $g_1$ has $\ell$ distinct roots $x_1, \ldots, x_\ell$. For each $i = 2, \ldots, k$, the probability that $g_i(x_1) = 0$ is $1/p$. Thus

$$\Pr\big[\exists i \text{ such that } g_i(x_1) \neq 0\big] = 1 - 1/p^{k-1},$$
$$\Pr\big[\forall j,\ \exists j_i \text{ such that } g_{j_i}(x_j) \neq 0\big] = (1 - 1/p^{k-1})^\ell.$$

Since the number of distinct roots of $g_1$ may be less than $\ell$, the probability is larger than $(1 - 1/p^{k-1})^\ell$. $\square$

By Lemma 3, $f_i'$'s have no common root other than $r_p^{-1}$ with the probability larger than $(1 - 1/p^d)^{d-1}$. Similarly $r_q$ can be computed. The success probability of determining $r_p$ and $r_q$ uniquely is larger than

$$\begin{aligned} &(1 - 1/p^d)^{d-1} \cdot (1 - 1/q^d)^{d-1} \\ &\geqslant e^{-3(d-1)/2p^d - 3(d-1)/2q^d} \geqslant e^{-3(d-1)p^d} \\ &\geqslant e^{-1/2(p-1)} \end{aligned}$$

if $d \geqslant 2$ and $q > p > 6d$. Hence the overall success probability is larger than

$$e^{-3/2(p-1)} \cdot e^{-1/2(p-1)} \geqslant e^{-2/(p-1)} \geqslant 1 - \frac{2}{p-1}$$

because $e^{-x} \geqslant 1 - x$ for $0 < x < \frac{1}{2}$.

In summary, we have the following theorem.

**Theorem 4.** *Suppose the modulus $n = pq$ is public with $6d < p < q$ and $d \geqslant 2$ in Domingo-Ferrer's privacy homomorphism. The scheme can be broken by $d+1$ known plaintext–ciphertext pairs in time $O(d^3 \log^2 n)$ with probability larger than $1 - 2/(p-1)$.*

For example, when $n \approx 2^{1024}$ and $p \approx q \approx 2^{512}$, the probability that the algorithm fails is less than $2/(p-1) \leqslant 2^{-511}$.

### 3.2. The case that n is not public

Domingo-Ferrer suggested that his scheme could be more secure by hiding the modulus $n$. In this case, however, we can not perform many multiplications since one multiplication makes the length of ciphertexts four times longer. We will show that even if $n$ is not public, a similar cryptanalysis can be applied.

Assume that we have $2(d+1)$ known plaintext–ciphertext pairs.

From each $d+1$ pairs, we can induce two $(d+1) \times (d+1)$ coefficient matrices, $A_1$ and $A_2$ as (1).

First, we compute the determinant of $A_i$'s viewed as integer matrices. When $A = (a_{ij})$ is a $(d+1) \times (d+1)$ integer matrix, it is known that $\det(A)$ can be computed by $O(d^4(\log d + \log \|A\|) + d^3 \log^2 \|A\|)$ bit operations where $\|A\| = \max_{i,j}\{|a_{ij}|\}$ [1] (and there are algorithms with the lower complexity. For more detail, see [9]). For the matrix $A_i$, we may assume that $\|A_i\| \leqslant n$ and $\det(A_i)$ can be computed by $O(d^4 \log dn + d^3 \log^2 n)$ bit operations.

Second, we compute $p$ from the gcd of determinants of $A_i$'s. We claim that $\gcd(\det(A_1), \det(A_2)) = p$, equivalently

$$\gcd\big(\det(A_1)/p, \det(A_2)/p\big) = 1$$

with high probability. More precisely, we have

**Lemma 5.** *Assume that divisibility of an integer by different primes is independent. Let $N$ be a positive integer. If positive integers $n_1, \ldots, n_k$ are randomly drawn from the interval $(0, N)$, then the probability $P_k(i)$ of the greatest common divisor of $k$ integers $n_1, \ldots, n_k$ is equal to $i$,*

$$P_k(i) = \lim_{N\to\infty} \Pr\big\{\gcd(n_1, n_2, \ldots, n_k) = i\big\} \approx \frac{1}{i^k \zeta(k)},$$

*where $\zeta(k)$ is the Riemann's zeta function.*[1]

**Proof.** See [12, Section 4.4]. □

If $\ell = \gcd(\det(A_1), \det(A_2))$ is not prime and $\ell$ has only small factors other than $p$, then we can easily calculate $p$ by trial divisions or some integer factoring algorithms. By Lemma 5, we have the probability for finding $p$ greater than

$$\sum_{i=1}^{2^m} P_2(i) = \sum_{i=1}^{2^m} \frac{1}{i^2 \zeta(2)} = \frac{1}{\zeta(2)} \sum_{i=1}^{2^m} \frac{1}{i^2} = 1 - \frac{1}{\zeta(2)} \sum_{i=2^m+1}^{\infty} \frac{1}{i^2}$$

assuming that prime factors of $\ell$ smaller than $2^m$ can be easily calculated. We can find $q$ by the same method. After getting $p$ and $q$, we can compute the other secret keys $r_p$ and $r_q$ as the case that $n$ is known.

**Theorem 6.** *Suppose the modulus $n = pq$ is secret with $2p > q > p \geqslant 6d$ and $d \geqslant 2$ in Domingo-Ferrer's algebraic privacy homomorphism. The scheme can be broken by $2(d+1)$ known plaintext–ciphertext pairs in time $O(d^4 \log dn + d^3 \log^2 n + \varepsilon(m))$ with the success probability larger than $(1 - 1/2^{m-2})(1 - 2/(p-1))$ where $\varepsilon(m) = O(2^{2m})$ is the complexity of a factorization algorithm to find all factors less than $2^m$.*

**Proof.** The computing time of $\det(A_i)$ for $i = 1, 2$ in $\mathbb{Z}$ is estimated as $O(d^4 \log dn + d^3 \log^2 n)$. Next, using a suitable factorization algorithm (whose complexity is $\varepsilon(m)$), we can discard prime factors smaller than $2^m$ and obtain $p$ by computing the gcd of $\det(A_i)$'s. The number of primes less than $2^m$ is approximately $2^m/(\log 2^m) = 2^m/(m \log 2)$. Let $M$ be the product of primes less than $2^m$, then

$$M = \prod_{p_i < 2^m} p_i \leqslant 2^{m \cdot 2^m/(\log 2^m)} = 2^{2^m/(\log 2)}$$

[1] The approximate value of $\frac{1}{\zeta(k)}$ for $k = 2, 4, 6, 8, 10$ is 0.6079271016, 0.9239384016, 0.9829525910, 0.9959391987, 0.9990064106.

and $\log M \leqslant 2^m/(\log 2) \leqslant 2^{m+1}$. The computation of $\gcd(M, \det A_i)$ takes $O((2^{m+1})^2)$ bit operations and $\varepsilon(m) = O(2^{2m})$ follows. By Lemma 5, we have

$$\Pr\big[\gcd\big(\det(A_1), \det(A_2)\big) = p\big] \geqslant 1 - \frac{1}{\zeta(2)} \sum_{i=2^m+1}^{\infty} \frac{1}{i^2}.$$

Also the same probability holds for computing $q$. Let Error be the event that $p$ or $q$ is not determined. Since $\sum_{i=2^m+1}^{\infty} \frac{1}{i^2} \leqslant \frac{1}{2^{m-1}}$ and $\zeta(2) \geqslant 1$,

$$\Pr[\text{Error}] \leqslant 1 - \left(1 - \frac{1}{\zeta(2)} \sum_{i=2^m+1}^{\infty} \frac{1}{i^2}\right)^2 \leqslant 1 - \left(1 - \frac{1}{2^{m-1}}\right)^2 \leqslant \frac{1}{2^{m-2}}.$$

The computation of $r_p, r_q$ and its complexity is the same as the case when $n$ is known. The total complexity is

$$O\big(d^4 \log dn + d^3 \log^2 n + 2^{2m}\big).$$

The success probability is

$$\Pr\big[\neg\text{Error} \wedge \text{Find}r_p \wedge \text{Find}r_q\big] \geqslant \left(1 - \frac{1}{2^{m-2}}\right)\left(1 - \frac{2}{p-1}\right). \qquad \square$$

Note that the probability that the algorithm fails, is less than $10^{-3}$ if $m \geqslant 12$, $n \approx 2^{1024}$ and $d \approx 10$.

**Remark 7.** In fact, $(d+2)$ known plaintext–ciphertext pairs are enough to make two $(d+1) \times (d+1)$ matrices by use of a plaintext–ciphertext pair twice. In Lemma 5, it is assumed that the integers are chosen randomly and in order to apply the lemma, we assume $2(d+1)$ known plaintext–ciphertext pairs.

Table 1
The summary of the proposed attacks

| Case | $n$ is known ($p \approx 2^{512}$) | $n$ is unknown ($m \geqslant 12$, $d \approx 10$) |
|---|---|---|
| The number of known-plaintexts | $d+1$ | $2(d+1)$ |
| The success probability | $1 - \frac{2}{p-1}$ ($\approx 1 - 2^{-511}$) | $(1 - \frac{1}{2^{m-2}})(1 - \frac{2}{p-1})$ ($\approx 1 - 10^{-3}$) |
| Time complexity (bit operations) | $O(d^3 \log^2 n)$ | $O(d^4 \log dn + d^3 \log^2 n + 2^{2m})$ |

*3.2.1. Example*

This example is in the paper of Domingo-Ferrer [6]. We illustrate the above analysis by this example. Let $p = 17$, $q = 13$, $r_p = 2$, and $r_q = 3$ be secret key. We can encrypt $-1, 3, 1, 2, 4$, and $5$ as follows:

$$\mathcal{E}(-1) = \mathcal{E}(2, -3) = \big([4, 6], [5, 12]\big),$$
$$\mathcal{E}(3) = \mathcal{E}(2, 1) = \big([4, 6], [4, 9]\big),$$
$$\mathcal{E}(1) = \mathcal{E}(4, -3) = \big([8, 12], [5, 12]\big),$$
$$\mathcal{E}(2) = \mathcal{E}(3, -1) = \big([6, 9], [13, 4]\big),$$
$$\mathcal{E}(4) = \mathcal{E}(3, 1) = \big([6, 9], [4, 9]\big),$$
$$\mathcal{E}(5) = \mathcal{E}(6, -1) = \big([12, 5], [13, 4]\big).$$

We use three plaintext–ciphertext pairs, $\{(-1, \mathcal{E}(-1)), (3, \mathcal{E}(3)), (1, \mathcal{E}(1))\}$ to make a coefficient matrix $A$ where

$$A = \begin{pmatrix} -1 & 4 & 5 \\ 3 & 4 & 4 \\ 1 & 8 & 5 \end{pmatrix}, \qquad \det(A) = 68,$$

$$\gcd\big(\det(A), 13 \cdot 17 = 221\big) = 17.$$

If $n = 221$ is unknown, with three more plaintext–ciphertext pair, make another matrix for $\{(2, \mathcal{E}(2)), (4, \mathcal{E}(4)), (5, \mathcal{E}(5))\}$,

$$B = \begin{pmatrix} 2 & 6 & 13 \\ 4 & 6 & 4 \\ 5 & 12 & 13 \end{pmatrix}, \qquad \det(B) = 102,$$

$$\gcd\big(\det(A), \det(B)\big) = 34.$$

We next calculate $r_p$ by using $1 + 4t + 5t^2 = 0$, $-3 + 4t + 4t^2 = 0$ then by elimination $-19 + 4t = 0 \bmod 17$ so $t = 9 \bmod 17$, $r_p = t^{-1} \bmod 17 = 2$.

## 4. Conclusion

Domingo-Ferrer proposed two algebraic privacy homomorphisms in 1996 [6] and 2002 [7]. The second was analyzed by Bao [3] and Wagner [13,14], but no attack against the first one was announced. In this paper we firstly analyzed the first Domingo-Ferrer's algebraic privacy homomorphism. It can be broken by $(d+1)$ plaintext–ciphertext pairs by known plaintext attacks when the modulus is public. Even when the modulus is kept secret, it can be broken by $2(d+1)$ pairs. Therefore, it is still open to decide whether an algebraic privacy homomorphism exists.

## References

[1] J. Abbot, M. Bronstein, T. Mulders, Fast deterministic computation of determinants of dense matrices, in: International Conference on Symbolic and Algebraic Computation Proceedings of

the 1999 International Symposium on Symbolic and Algebraic Computation, pp. 197–204.
[2] N. Ahituv, Y. Lapid, S. Neumann, Processing encrypted data, Comm. ACM 20 (1987) 777–780.
[3] F. Bao, Cryptanalysis of a provable secure additive and multiplicative privacy homomorphism, in: International Workshop on Coding and Cryptography (WCC), 2003.
[4] D. Boneh, R. Lipton, Searching for elements in black-box fields and applications, in: Advances in Cryptology, Crypto'96, in: Lecture Notes in Comput. Sci., vol. 1109, Springer-Verlag, Berlin, 1996, pp. 283–297.
[5] E. Brickell, Y. Yacobi, On privacy homomorphisms, in: Advances in Cryptology, Eurocrypt'87, in: Lecture Notes in Comput. Sci., vol. 304, Springer-Verlag, Berlin, 1988, pp. 117–125.
[6] J. Domingo-Ferrer, A new privacy homomorphism and applications, Inform. Process. Lett. 60 (5) (1996) 277–282.
[7] J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism, in: ISC2002, in: Lecture Notes in Comput. Sci., vol. 2443, Springer-Verlag, Berlin, 2002, pp. 471–483.
[8] J. Feigenbaum, M. Merritt, Open questions, talk abstracts, and summary of discussions, in: DIMACS series in Discrete Mathematics and Theoretical Computer Science, vol. 2, Amer. Math. Soc., 1991, pp. 1–45.
[9] E. Kaltofen, G. Villard, Computing the sign or the value of the determinant of an integer matrix, a complexity survey, J. Comput. Appl. Math. 162 (2004) 133–146.
[10] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Inc., Boca Raton, FL, 1997.
[11] R. Rivest, L. Adleman, M. Dertouzos, On data banks and privacy homomorphisms, in: Foundations of Secure Computation, Academic Press, New York, 1978, pp. 169–179.
[12] M. Schroeder, Number Theory in Science and Communication, second ed., Springer-Verlag, Berlin, 1986.
[13] D. Wagner, Cryptanalysis of an algebraic privacy homomorphism, in: ISC2003, in: Lecture Notes in Comput. Sci., vol. 2851, Springer-Verlag, Berlin, 2003, pp. 234–239.
[14] D. Wagner, Erratum concerning "Cryptanalysis of an Algebraic Privacy Homomorphism", available at http://www.cs.berkeley.edu/~daw/papers/.