Cryptanalysis of a System Based on Twisted Dihedral Group Algebras

Simran Tinani

Institute of Mathematics, University of Zurich

Received: 18th October 2022 | Revised: 8th January 2024 | Accepted: 1st May 2024

Abstract *Several cryptographic protocols constructed based on less-known algorithmic problems, such as those in non-commutative groups, group rings, semigroups, etc., which claim quantum security, have been broken through classical reduction methods within their specific proposed platforms. A rigorous examination of the complexity of these algorithmic problems is therefore an important topic of research. In this paper, we present a cryptanalysis of a public key exchange system based on a decomposition-type problem in the so-called twisted group algebras of the dihedral group D_{2n} over a finite field $\mathbb{F}_q$. Our method of analysis relies on an algebraic reduction of the original problem to a set of equations over $\mathbb{F}_q$ involving circulant matrices, and a subsequent solution to these equations. Our attack runs in polynomial time and succeeds with probability at least* 90 *percent for the parameter values provided by the authors. We also show that the underlying algorithmic problem, while based on a non-commutative structure, may be formulated as a commutative semigroup action problem.*

Keywords: Group Algebra, Asymmetric key exchange, Twisted Multiplication

2010 Mathematics Subject Classification: 94A60, 11Y40

1 INTRODUCTION

The design of efficient cryptographic systems that resist quantum attacks presently constitutes the important area of research called post-quantum cryptography. Non-commutative structures such as nonabelian groups, group rings, semigroups, etc., along with pertinent algorithmic problems, have been used for the construction of public key cryptosystems in a plethora of works in this field. Two algorithmic problems that have found great mention in this realm are the so-called conjugacy search problem and the decomposition problem (see [22], [3], [8]). Since such problems in general cannot be formulated as a version of the hidden subgroup problem in a finite abelian group, they have been suggested to render the corresponding cryptographic systems secure from known quantum attacks. However, specific instances of these problems are often solvable through other classical methods and do not have the presumed complexity in the specific suggested platform (see, for instance [23], [1]). Several linear algebra attacks on such cryptosystems have been devised that retrieve the shared key, often without solving the underlying algorithmic problem [24], [14].

In [4], the authors construct a key exchange system based on so-called twisted group algebras over a finite field $\mathbb{F}_q$, which are similar to group algebras but have a more complicated multiplicative structure. Group algebras have found mention in some other proposed public key cryptographic schemes. In [9], the authors construct a key exchange protocol based on the discrete logarithm problem in the semigroup $\mathrm{Mat}_3(\mathbb{F}_7[S_5])$ of 3×3 matrices over the group ring $\mathbb{F}_7[S_5]$, where S_5 is the group of permutation on five symbols. In [15], an attack was devised by showing that $\mathrm{Mat}_3(\mathbb{F}_7[S_5])$ embeds into $\mathrm{Mat}_{360}(\mathbb{F}_7)$, for which the discrete logarithm problem can then be solved using the method in [12] adapted to singular matrices. The attack in [6] on the same system uses the fact that the algebra $\mathbb{F}_7[S_5]$ is semisimple, and so by Maschke's theorem it is isomorphic to a direct sum of matrix algebras over $\mathbb{F}_7$.

The authors of [4] assert that since Maschke's Theorem is valid also for twisted group algebras, a similar attack might break the underlying problem of their system. However, to resolve this they choose q such that the twisted group algebra is not semisimple. Further, they assert that the general methods of cryptanalysis in [17] and [18], which require the construction of bases over some vector spaces, do not apply to their system. This is attributed to the facts that the twisted group algebra is not a group under the twisted multiplication and that there is an added dimension of non-commutativity with the twisted multiplication.

*Corresponding Author: simran.tinani@cnlab.ch

The underlying platform of the system in [4] is a twisted group algebra of the dihedral group D_{2n} over a finite field $\mathbb{F}_q$ with twisted multiplication defined with the help of a function called a 2-cocycle. The 2-cocycle α is chosen by the authors such that $\mathbb{F}_q^\alpha D_{2n}$ and $\mathbb{F}_q D_{2n}$ are not isomorphic, so that one is no longer working over a group algebra. Some recent relevant works on twisted group algebras are [16] and [5]. In [5], the authors study right ideals of twisted group algebras, endowing them with a natural distance and thus studying them as codes; they show that that all perfect linear codes are twisted group codes. In [16], the authors use twisted dihedral group rings as a platform for a public key protocol as a non-commutative variation of the Diffie-Hellman protocol. This protocol has a similar platform to the one in [4], but with the twisted multiplication and 2-cocycle defined differently. The authors show in [4] that the twisted group algebra platforms are structurally different.

The security of the protocol in [4] relies on a newly introduced algorithmic assumption, which the authors call Dihedral Product Decomposition (DPD) Assumption. Under this assumption, the authors prove that their protocol is session-key secure in the authenticated-links adversarial model of Canetti and Krawczyk [2]. The underlying algorithmic problem can be seen as a special form of the decomposition problem over the multiplicative monoid of an algebra A: given $(x, y) \in A$ and $S \subseteq G$, the problem is to find $z_1, z_2 \in S$ such that $y = z_1 x z_2$. The Dihedral Product Decomposition Problem constitutes finding (z_1, z_2) given $z_1 x z_2$ and x in the platform, where z_1 and z_2 lie in specific predefined subalgebras of $\mathbb{F}_q^\alpha D_{2n}$. It is therefore a more restricted version of the general decomposition problem in the platform. The authors claim that the protocol proposed is quantum-safe, with justification based on the fact that the decomposition problem is a generalization of the conjugacy search problem, which is believed to be difficult even for quantum computers, in certain platform groups.

In this paper we show that in most cases, the underlying Dihedral Product Decomposition (DPD) Problem can be solved algebraically with a classical polynomial time algorithm. As a result, the Dihedral Product Decomposition Assumption does not hold, and the security of the system breaks down completely. We do this by producing an algebraic reduction of the original problem to a set of equations over $\mathbb{F}_q$ involving circulant matrices, which we show can be solved in polynomial time in a majority of cases. We show that our algorithm succeeds with probability $(1 - \frac{1}{q})^2$, which gives a lower bound of a 90 percent success rate with the values of q and n proposed by the authors. We also show that the underlying DPD problem may be formulated as a semigroup action problem [11], with multiplication in the multiplicative monoid of a twisted dihedral group algebra. Some other protocols using this method have been proposed in [10], [9], [11].

The paper is structured as follows. In Section 2 we describe the structure and some properties of the underlying platform, viz. the twisted group algebra $\mathbb{F}_q^\alpha D_{2n}$, closely following the results of [4]. In Section 3, we describe the key exchange protocol proposed in [4] and state the DPD problem, which forms the basis of its security assumption. We show that despite the use of a non-commutative structure, this algorithmic problem is equivalent to a commutative semigroup action problem. In Section 4, we present some background definitions and results on circulant matrices, which are needed for our reduction and cryptanalysis. In Section 5, we describe an algebraic reduction of the DPD problem to a set of simultaneous equations over $\mathbb{F}_q$ and show that in a majority of cases, they can be solved by linear algebra in polynomial time. Using these results, we provide a polynomial time algorithm which performs the cryptanalysis of the system of [4].

Throughout, we let $\mathbb{F}$ denote a field, G denote a finite group and $\mathbb{F}_q$ denote the finite field with q elements, where q is a power of a prime. Also let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We denote by D_{2n} the dihedral group of size $2n$.

2 STRUCTURE OF THE PLATFORM

Definition 1 (Group Algebra)**.** *The group algebra $\mathbb{F}[G]$ is the set of the formal sums $\sum_{g\in G} a_g g$, with $a_g \in \mathbb{F}$, $g \in G$. Addition is defined componentwise: $\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g$. Multiplication is defined as $\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g := \sum_{g\in G} \sum_{h\in G} (a_g b_h) gh = \sum_{k\in G} \sum_{g\in G,\ h\in G: gh=k} a_g b_h k$.*

Clearly, $\mathbb{F}[G]$ is an algebra over $\mathbb{F}$ with dimension $|G|$. If G is non-commutative, so is $\mathbb{F}[G]$.

In [7], the authors apply the structure of twisted group algebra to construct a public-key exchange system. The multiplication operation in these twisted group algebras is defined using the concept of 2-cocycles.

Definition 2 (2-Cocycle)**.** *A map $\alpha : G \times G \to \mathbb{F}_q^*$ is called a 2-cocycle of G if $\alpha(1, 1) = 1$ and for all $g, h, k \in G$ we have $\alpha(g, hk)\alpha(h, k) = \alpha(gh, k)\alpha(g, h)$.*

Definition 3 (Twisted Group Algebra)**.** *Let α be a 2-cocycle of G. The twisted group algebra $\mathbb{F}^\alpha G$ is the set of all formal sums $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{F}$, with the following twisted multiplication: $g \cdot h = \alpha(g, h)gh$, for $g, h \in G$. The*

multiplication rule extends linearly to all elements of the algebra: $(\sum_{g\in G} a_g g)\cdot(\sum_{h\in G} b_h h) = \sum_{g\in G}\sum_{h\in G} a_g b_h \alpha(g,h)gh$. *Addition is given componentwise as in Definition 1.*

We note that the associativity of a twisted group algebra follows from the condition on α being a 2-cocycle. In fact, it is an if and only if condition.

Remark 1. *Throughout the rest of the paper, we will be concerned with twisted group algebras, and so it is understood that the product* $(\sum_{g\in G} a_g g)\cdot(\sum_{h\in G} a_h h)$ *denotes twisted multiplication. Further, we will usually omit the* $\cdot$ *symbol, so that multiplication in the group G and in the twisted group algebra are not differentiated by operation notation. To avoid confusion we ensure that the symbols used for elements of the group and group algebra do not intersect.*

Denote the set of all 2-cocycles of G into $\mathbb{F}_q$ by $Z^2(G,\mathbb{F}_q^*)$. For $\alpha,\beta \in Z^2(G,\mathbb{F}_q^*)$, one may define the cocycle $\alpha\beta \in Z^2(G,\mathbb{F}_q^*)$ by $\alpha\beta(g,h) = \alpha(g,h)\beta(g,h)$ for all $g,h \in G$. With this operation, $Z^2(G,\mathbb{F}_q^*)$ becomes a multiplicative abelian group.

Definition 4 (Adjunct)**.** *For an element* $a = \sum_{g\in G} a_g g \in \mathbb{F}_q^\alpha G$ *we define its adjunct as* $\hat{a} := \sum_{g\in G} a_g \alpha(g,g^{-1})g^{-1}$.

2.1 A TWISTED DIHEDRAL GROUP ALGEBRA

For the rest of this paper, we set $G = D_{2n}$, where $D_{2n} = \langle x, y : x^n = y^2 = 1, yxy^{-1} = x^{-1}\rangle$ is the dihedral group of order $2n$. Further, we let $C_n = \langle x^i\rangle$ be the cyclic subgroup of D_{2n} generated by x and α be a 2-cocycle of D_{2n}.

The following lemma from [4] can be verified in a straightforward manner.

Lemma 1 ([4])**.** *We have*

1. $\mathbb{F}_q^\alpha D_{2n}$ *is a free* $\mathbb{F}_q^\alpha C_n$*-module with basis* $\{1, y\}$. *Therefore* $\mathbb{F}_q^\alpha D_{2n} = \mathbb{F}_q^\alpha C_n \oplus \mathbb{F}_q^\alpha C_n y$ *as a direct sum of* $\mathbb{F}_q$*-vector spaces.*
2. $\mathbb{F}_q^\alpha C_n y \cong \mathbb{F}_q^\alpha C_n$ *as* $\mathbb{F}_q^\alpha C_n$*-modules.*
3. *For* $a \in \mathbb{F}_q^\alpha C_n y$, $ab \in \mathbb{F}_q^\alpha C_n$ *if* $b \in \mathbb{F}_q^\alpha C_n y$ *and* $ab \in \mathbb{F}_q^\alpha C_n y$ *if* $b \in \mathbb{F}_q^\alpha C_n$.
4. *If* $a \in \mathbb{F}_q^\alpha C_n$, *then* $\hat{a} \in \mathbb{F}_q^\alpha C_n$. *Similarly, if* $a \in \mathbb{F}_q^\alpha C_n y$, *then* $\hat{a} \in \mathbb{F}_q^\alpha C_n y$.

Definition 5.

1. *For a 2-cocycle* α *of* D_{2n} *we define the reversible subspace of* $\mathbb{F}_q^\alpha C_n y$ *as the vector subspace*

$$\Gamma_\alpha = \{a = \sum_{i=0}^{n-1} a_i x^i y \in \mathbb{F}_q^\alpha C_n y \mid a_i = a_{n-i} \text{ for } i = 1,\ldots,n-1\}.$$

2. *Define a map* $\psi : \mathbb{F}_q^\alpha C_n y \to \mathbb{F}_q^\alpha C_n$ *as follows. Given* $a = \sum_{i=0}^{n-1} a_i x^i y \in \mathbb{F}_q^\alpha C_n y$ *we define* $\psi(a) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q^\alpha C_n$. *Clearly,* ψ *is an* $\mathbb{F}_q$*-linear isomorphism.*

In this paper, we will refer to an element $\sum_{i=1}^{n-1} a_i x^i y$ of the reversible subspace Γ_α as a reversible element of $\mathbb{F}_q^\alpha C_n y$ and to the corresponding vector $(a_0,\ldots,a_{n-1}) \in \mathbb{F}_q^n$ as a reversible vector.

Lemma 2 ([4])**.** *Let* α *be a 2-cocycle of* D_{2n}. *Then we have*

1. *If*

$$\alpha(x^i, x^{j-i}) = \alpha(x^{j-i}, x^i) \tag{1}$$

   for all $i, j \in \{0,\ldots,n-1\}$, *then* $ab = ba$ *for* $a, b \in \mathbb{F}_q^\alpha C_n$.

2. *If*

$$\alpha(x^{i-j}y, x^{i-j}y)\alpha(x^i y, x^{i-j}y) = \alpha(x^{n-i}y, x^{n-i}y)\alpha(x^{j-i}y, x^{n-i}y) \tag{2}$$

   for all $i, j \in \{0,\ldots,n-1\}$, *then* $a\hat{b} = b\hat{a}$ *for* $a, b \in \Gamma_\alpha$.

The following lemma provides an explicit construction of the 2-cocycle that will be used throughout in the cryptographic construction of [4].

Lemma 3 ([4]). *Let $\lambda \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The map $\alpha_\lambda : D_{2n} \times D_{2n} \to \mathbb{F}_q^*$ defined by*

$$\begin{aligned} &\alpha_\lambda(g,h) = \lambda \text{ for } g = x^i y,\ h = x^j y \text{ with } i,j \in \{0,\dots,n-1\} \text{ and} \\ &\alpha_\lambda(g,h) = 1 \text{ otherwise} \end{aligned} \tag{3}$$

is a 2-cocycle. Further, α_λ satisfies the two conditions (1) *and* (2)*.*

Proof. By definition, $\alpha_\lambda(1,1) = 1$. Thus one only needs to verify that $\alpha_\lambda(g,h)\alpha_\lambda(gh,k) = \alpha_\lambda(g,hk)\alpha_\lambda(h,k)$ for all $g,h,k \in D_{2n}$. Write $h = x^{j_1}y^{k_1}$ and $k = x^{j_2}y^{k_2}$ with $i, j_1, j_2 \in \{0,\dots,n-1\}$. The condition may then be directly verified separately in a straightforward way for the two possible cases $g = x^i$ and $g = x^i y$. The fact that α_λ satisfies conditions (1) and (2) follows from the definition. □

Lemma 4 ([4]). *$\mathbb{F}_q D_{2n}$ and $\mathbb{F}_q{}^{\alpha_\lambda} D_{2n}$ are isomorphic if and only if λ is a square in $\mathbb{F}_q$, i.e. if and only if $\lambda^{(q-1)/2} = 1$.*

Lemma 5 ([4]). *If λ_1, λ_2 are not squares in $\mathbb{F}_q$, then $\mathbb{F}_q{}^{\alpha_{\lambda_1}} D_{2n}$ and $\mathbb{F}_q{}^{\alpha_{\lambda_2}} D_{2n}$ are isomorphic.*

From Lemma 2 we thus have that for the choice $\alpha = \alpha_\lambda$ of 2-cocycle, the multiplicative ring of $\mathbb{F}_q^\alpha C_n$ is commutative, and that $a\hat{b} = b\hat{a}$ for all $a, b \in \Gamma_\alpha$. The form (3) of $\alpha = \alpha_\lambda$ is adopted throughout for the cryptosystem in [4] and thus we restrict our study to this cocycle. Thus, henceforth we take $\alpha = \alpha_\lambda$.

3 THE KEY EXCHANGE PROTOCOL

Having described the relevant structural properties of the underlying platform, we now describe the key exchange protocol in [4]. This uses two-sided multiplications in $\mathbb{F}_q^\alpha D_{2n}$.

3.1 PUBLIC PARAMETERS

1. A number $m \in \mathbb{N}$ and a prime $p > 2$ with $p \mid 2n$ and set $q = p^m$.
2. A 2-cocycle $\alpha = \alpha_\lambda$ for a non-square λ in $\mathbb{F}_q$. This ensures that the platform $\mathbb{F}_q^\alpha D_{2n}$ is not isomorphic to $\mathbb{F}_q D_{2n}$.
3. An element $h = h_1 + h_2$ for a random $0 \neq h_1 \in \mathbb{F}_q^\alpha C_n$ and a random $0 \neq h_2 \in \mathbb{F}_q^\alpha C_n y$. (Clearly, since h is public, so are h_1 and h_2.)

Protocol 1 describes the key exchange protocol of [4].

Protocol 1.

1. *Alice chooses a secret pair $(s_1, t_1) \in \mathbb{F}_q^\alpha C_n \times \Gamma_\alpha$, and sends $\mathrm{pk}_A = s_1 h t_1$ to Bob.*
2. *Bob chooses a secret pair $(s_2, t_2) \in \mathbb{F}_q^\alpha C_n \times \Gamma_\alpha$ and sends $\mathrm{pk}_B = s_2 h t_2$ to Alice.*
3. *Alice computes $K_A = s_1 \mathrm{pk}_B \hat{t_1}$,*
4. *Bob computes $K_B = s_2 \mathrm{pk}_A \hat{t_2}$*
5. *The shared key is $K = K_A = K_B$*

The authors' proposed values for parameters q and n are $q = n = 19$, $q = n = 23$, $q = n = 31$, $q = n = 41$.

3.2 CORRECTNESS

It is easy to show that within an uncorrupted session, both Alice and Bob establish the same key. Indeed, because of the choice of $\alpha = \alpha_\lambda$, we have $s_i s_j = s_j s_i$ in $\mathbb{F}_q^\alpha C_n$ and $t_i \hat{t_j} = t_j \hat{t_i}$ in $\mathbb{F}_q^\alpha C_n y$ for $i, j \in \{1, 2\}$, so

$$K_A = s_1 \mathrm{pk}_B \hat{t_1} = s_1 s_2 h t_2 \hat{t_1} = s_2 s_1 h t_1 \hat{t_2} = s_2 \mathrm{pk}_A \hat{t_2} = K_B.$$

3.3 SECURITY ASSUMPTION

The security of the protocol depends on the assumption of the difficulty of the following algorithmic problem.

Definition 6 (Dihedral Product Decomposition (DPD) Problem). *Let $(s,t) \in \mathbb{F}_q^\alpha C_n \times \Gamma_{\alpha_\lambda}$ be a secret key. Given a public element $h = h_1 + h_2 \in \mathbb{F}_q^\alpha D_{2n}$, $h_1 \in \mathbb{F}_q^\alpha C_n$, $h_2 \in \mathbb{F}_q^\alpha C_n y$, and a public key $\mathrm{pk} = sht$, the DPD problem requires an adversary to compute $(\tilde{s}, \tilde{t}) \in \mathbb{F}_q^\alpha C_n \times \Gamma_\alpha$ such that $\mathrm{pk} = \tilde{s} h \tilde{t}$.*

Let $(\tilde{s}, \tilde{t})$ be the output of an adversary $\mathcal{A}$ attempting to solve the DPD problem for $\mathbb{F}_q^\alpha D_{2n}$. The authors define $\mathcal{A}$'s advantage $DPD_{adv}[\mathcal{A}, \mathbb{F}_q^\alpha D_{2n}]$ in solving the DPD problem as the probability that $\tilde{s}h\tilde{t} = sht$.

Definition 7 (DPD Assumption)**.** *The DPD assumption is said to hold for $\mathbb{F}_q^\alpha D_{2n}$ if for all efficient adversaries $\mathcal{A}$ the quantity $DPD_{adv}[\mathcal{A}, \mathbb{F}_q^\alpha D_{2n}]$ is negligible.*

In Section 5, we provide a cryptanalysis of Protocol 1 by solving the DPD problem. We show that in most cases, a polynomial time solution is possible, and so the DPD assumption does not hold. For our method of cryptanalysis, we need some prerequisites on circulant matrices, which we provide in the next section. However, we first show below how the DPD problem can be formulated as a special case of a commutative semigroup action problem, in the framework introduced in [11].

3.3.1 DPD PROBLEM AS A COMMUTATIVE SEMIGROUP ACTION

The authors of [4] assert that given a fixed $h \in \mathbb{F}_q^\alpha D_{2n}$, the set of keys $\{sht \mid (s,t) \in \mathbb{F}_q^\alpha C_n \times \Gamma_\alpha\}$ is not even a semigroup under the twisted algebra multiplication. From this observation, they claim that their system is immune to the quantum cycle-finding algorithm of Shor [21] which is known to solve the hidden subgroup problem in abelian groups.

Further, the security of the system of [4] is based on the presence of a non-commutative multiplication in the twisted group algebra. However, we now show that the DPD problem can be formulated as a commutative semigroup action problem, and so any classical or quantum solution to the latter also applies to the former. In [13], a Pollard-rho type square root algorithm was provided to solve an abelian group action problem, whereas the possibility for a modification to the commutative semigroup case was left open.

As observed before, the cocycle $\alpha = \alpha_\lambda$ satisfies conditions (1) and (2). Thus, $ab = ba$ for $a, b \in \mathbb{F}_q^\alpha C_n$ and $a\hat{b} = b\hat{a}$ for $a, b \in \Gamma_\alpha$. In particular, $\mathbb{F}_q^\alpha C_n$ is a commutative subalgebra of $\mathbb{F}_q^\alpha D_{2n}$. Recall the $\mathbb{F}_q$-linear isomorphism $\psi : \mathbb{F}_q^\alpha C_n y \to \mathbb{F}_q^\alpha C_n$ given by $\psi(a) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q^\alpha C_n$ for $a = \sum_{i=0}^{n-1} a_i x^i y \in \mathbb{F}_q^\alpha C_n y$. Below, we show that $\psi(\Gamma_\alpha)$ is a commutative semigroup under the multiplication defined by $\psi(t) \star \psi(t') := tt' \in \psi(\Gamma_\alpha)$.

Lemma 6. *Let α be a cocycle on $\mathbb{F}_q^\alpha D_{2n}$.*

1. *Suppose that for all i and j, $\alpha(x^i y, x^j y) = \alpha(x^j y, x^i y)$ and $\alpha(x^i y, x^j y) = \alpha(x^{n-i} y, x^{n-j} y)$ where all exponents are taken modulo n. Then, $\psi(\Gamma_\alpha)$ is closed under $\star$, and $\star$ is commutative.*

2. *Suppose that for all $0 \le i, j, m \le n-1$,*

$$\alpha(x^i, x^j y)\alpha(x^{i-j} y, x^{i-j} y) = \alpha(x^{i+j+m} y, x^i y)\alpha(x^{j+m} y, x^j y),$$

where all exponents are taken modulo n. Then, $\star$ is associative.

Therefore, if both conditions (1) and (2) are satisfied, $\psi(\Gamma_\alpha)$ is a commutative semigroup under the operation $\star$.

Proof. 1. Let $a = \sum_{i=0}^{n-1} a_i x^i y, b = \sum_{i=0}^{n-1} b_i x^i y \in \Gamma_\alpha$. We have

$$\begin{aligned}\psi(a) \star \psi(b) = ab &= \left(\sum_{i=0}^{n-1} a_i x^i y\right)\left(\sum_{j=0}^{n-1} b_j x^j y\right) \\ &= \sum_{m=0}^{n-1}\left(\sum_{k=0}^{n-1} a_k b_{k-m}\alpha(x^k y, x^{k-m} y)\right) x^m\end{aligned}$$

Since $a, b \in \Gamma_\alpha$, $a_{n-k} = a_k$ and $b_{k-m} = b_{m-k}$ for each m, k, so, the applying the assumption on α, $\sum_{k=0}^{n-1} a_k b_{k-m}\alpha(x^k y, x^{k-m} y) = \sum_{k=0}^{n-1} a_{n-k} b_{m-k}\alpha(x^{n-k} y, x^{m-k} y)$, i.e. the coefficients of x^m and x^{n-m} are equal, so $\psi(a) \star \psi(b) = ab \in \psi(\Gamma_\alpha)$. Further, since for all i, j, $\alpha(x^i y, x^j y) = \alpha(x^j y, x^i y)$, we have $\psi(a) \star \psi(b) = ab = ba = \psi(b) \star \phi(a)$, so $\star$ is commutative.

2. Now, let $a = \sum_{i=0}^{n-1} a_i x^i y, b = \sum_{i=0}^{n-1} b_i x^i y \in \Gamma_\alpha, c = \sum_{i=0}^{n-1} c_i x^i y \in \Gamma_\alpha$. We have

$$\begin{aligned}(\psi(a) \star \psi(b)) \star \psi(c) =& \psi^{-1}(ab) \cdot c = \left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j \alpha(x^i y, x^j y) x^{i-j} y\right) \cdot \left(\sum_{i=0}^{n-1} c_i x^i y\right) \\ =& \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} a_i b_j c_k \alpha(x^i y, x^j y)\alpha(x^{i-j} y, x^k y) x^{i-j-k}, \text{ and} \\ \psi(a) \star (\psi(b)) \star \psi(c)) =& a \cdot \psi^{-1}(bc) = \left(\sum_{i=0}^{n-1} a_i x^i y\right) \cdot \left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} b_j c_k \alpha(x^j y, x^k y) x^{j-k} y\right) \\ =& \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} a_i b_j c_k \alpha(x^i y, x^{j-k} y)\alpha(x^j y, x^k y) x^{i-j+k}\end{aligned}$$

The condition for associativity requires $(\psi(a) \star \psi(b)) \star \psi(c) = \psi(a) \star (\psi(b)) \star \psi(c))$. Equating the above expressions quickly gives the condition stated in (1).

□

Clearly, the choice of $\alpha = \alpha_\lambda$ in the protocol satisfies both the properties in Lemma 6, and therefore $\psi(\Gamma_{\alpha_\lambda})$ is a commutative semigroup. We can now look at the key exchange in Protocol 1 as an instance of a semigroup action problem, introduced in [11].

Definition 8 (Semigroup Action Problem)**.** *Let S be any semigroup acting on a set X*

$$\begin{aligned} S \times X &\to X \\ (s, x) &\mapsto s \cdot x \end{aligned}$$

Given an element $y = s \cdot x \in X$, where $x \in X$ is known and $s \in S$ is a secret, the semigroup action problem is to find some $\tilde{s} \in S$ such that $\tilde{s} \cdot x = y$.

Proposition 1. *The commutative semigroup $\mathbb{F}_q^\alpha C_n \times \psi(\Gamma_\alpha)$ acts on $\mathbb{F}_q^\alpha D_{2n}$ as follows*

$$\begin{aligned}(\mathbb{F}_q^\alpha C_n \times \psi(\Gamma_\alpha)) \times \mathbb{F}_q^\alpha D_{2n} &\to \mathbb{F}_q^\alpha D_{2n} \\ (s, \psi(t)) \cdot h &= sht \end{aligned} \tag{4}$$

Proof. Clearly, $(1, 1) \cdot h = h$ for all $h \in \mathbb{F}_q^\alpha D_{2n}$. Further,

$$(s, \psi(t))((s', \psi(t')) \cdot h) = ss'ht't = ss'ht = (ss', tt') \cdot h = (ss', \psi(t) \star \psi(t')) \cdot h.$$

□

Lemma 7. *The DPD problem is equivalent to the semigroup action problem for the commutative semigroup action* (4)*.*

Proof. Clearly, t and $\psi(t)$ can easily be read from each other without any significant computational cost. Suppose that given public element h and public key pk, the adversary can find s, t such that $sht = \text{pk}$. Then, $(s, \psi(t))$ is a solution to the SAP (4). Conversely, any solution $(s, \psi(t))$ of the SAP (4) gives the solution (s, t) of the DPD problem. □

The next section highlights some prerequisites on circulant matrices which will be used in the cryptanalysis of the system in Section 5.

4 CIRCULANT MATRICES

Definition 9. *A matrix over $\mathbb{F}_q$ of the form* $\begin{pmatrix} c_0 & c_{n-1} & \dots & c_1 \\ c_1 & c_0 & \dots & c_2 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & \dots & c_0 \end{pmatrix}$ *with $c_i \in \mathbb{F}_q$, is called circulant. Given a vector* $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})^T \in \mathbb{F}_q^n$, *we use the notation $M_{\mathbf{c}}$ to denote the circulant matrix* $M_{\mathbf{c}} := \begin{pmatrix} c_0 & c_{n-1} & \dots & c_1 \\ c_1 & c_0 & \dots & c_2 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & \dots & c_0 \end{pmatrix}$.

Definition 10. *Given vectors* $\mathbf{b} = (b_0, b_1, \dots, b_{n-1})^T \in \mathbb{F}_q^n$, $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})^T \in \mathbb{F}_q^n$, *define, for* $0 \le \ell \le n-1$ *the constants*

$$z_\ell(\mathbf{b}, \mathbf{c}) = \sum_{i+j=\ell \mod n} b_i c_j = \begin{pmatrix} c_\ell, & c_{\ell-1}, & \dots, & c_{\ell+1} \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}, 0 \le \ell \le n-1.$$

Also define the vector $\mathbf{z}_{\mathbf{b},\mathbf{c}} = (z_0(\mathbf{b}, \mathbf{c}), \dots, z_\ell(\mathbf{b}, \mathbf{c}), \dots, z_{n-1}(\mathbf{b}, \mathbf{c}))^T$. *In other words,*

$$\mathbf{z}_{\mathbf{b},\mathbf{c}} = \begin{pmatrix} c_0 & \dots & c_1 \\ c_1 & \dots & c_2 \\ \vdots & \ddots & \vdots \\ c_{n-1} & \dots & c_0 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = M_{\mathbf{c}} \cdot \mathbf{b}.$$

As in Definition 9, denote by $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c})$ the circulant matrix $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) = \begin{pmatrix} z_0(\mathbf{b}, \mathbf{c}) & \dots & z_1(\mathbf{b}, \mathbf{c}) \\ z_1(\mathbf{b}, \mathbf{c}) & \dots & z_2(\mathbf{b}, \mathbf{c}) \\ \vdots & \ddots & \vdots \\ z_{n-1}(\mathbf{b}, \mathbf{c}) & \dots & z_0(\mathbf{b}, \mathbf{c}) \end{pmatrix}$. *The following result is easy to verify by direct computation.*

Lemma 8. $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) = M_{\mathbf{c}} \cdot M_{\mathbf{b}}$.

4.1 PROBABILITY OF A CIRCULANT MATRIX BEING INVERTIBLE

We will require the invertibility of some random circulant matrices over $\mathbb{F}_q$ for our reduction of the system. For this reason, we discuss the criteria for a random circulant matrix being invertible, and study this probability. We have the following result from [20].

Proposition 2 ([20])**.** *Let $x^n - 1 = f_1^{\alpha_1}(x) \dots f_\tau^{\alpha_\tau}(x)$ be the factorization of $x^n - 1$ over $\mathbb{F}_{q^m}$ into powers of irreducible factors. The number of invertible circulant matrices in $Mat_n(\mathbb{F}_{q^m})$ is equal to $\prod_{i=1}^{\tau}(q^{md_i\alpha_i} - q^{md_i(\alpha_i-1)})$, where d_i is the degree of $f_i(x)$ in the factorization of $x^n - 1$.*

Note that the number of circulant matrices over $\mathbb{F}_{q^m}$ is q^{mn}. As a direct consequence, the probability of a randomly chosen circulant matrix over $\mathbb{F}_{q^m}$ being invertible is

$$\prod_{i=1}^{\tau} \frac{q^{md_i\alpha_i} - q^{md_i(\alpha_i-1)}}{q^{nm}} = \prod_{i=1}^{\tau} \left(1 - \frac{1}{q^{md_i}}\right)$$

It is now easy to see that a lower bound for this quantity is $(1 - \frac{1}{q^m})^n$, which is achieved if $x^n - 1$ splits into distinct linear factors, i.e. $\tau = n$, $d_i = 1$, $\alpha_i = 1$. Similarly, an upper bound is achieved when there is a single factor in the factorization, i.e. $\tau = 1$ and $\alpha_1 = n$, in which case the quantity is $(1 - \frac{1}{q^m})$. Note that this upper bound is achieved when n is a power of the characteristic p of $\mathbb{F}_{q^m}$. $(x^n - 1 = (x-1)^n \mod p)$. In general, we have the following corollary.

Corollary 1. *Let e be the largest number such that $p^e \mid n$. Then the probability that a randomly chosen $n \times n$ circulant matrix over $\mathbb{F}_q$ is invertible is at least $(1 - \frac{1}{q})^{\frac{n}{p^e}}$. If n is a power of p, then the probability is exactly equal to $1 - \frac{1}{q}$.*

In [4], the authors deliberately choose the case $p \mid n$, so as to avoid having $\mathbb{F}_{q^m} D_{2n}$ semisimple. In fact, in all of their proposed parameters, ones has $n = p = q$, and so, the probability $1 - \frac{1}{q}$ applies for a random circulant matrix being invertible.

5 CRYPTANALYSIS

Note that the adversary is given an equation of the form $sht = \gamma$ over $\mathbb{F}_q^{\alpha} D_{2n}$, where

$$s = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q^{\alpha} C_n,\ t = \sum_{i=0}^{n-1} b_i x^i y \in \Gamma_\alpha \subseteq \mathbb{F}_q{}^{\alpha_\lambda} D_{2n} \tag{5}$$

are unknown, and $h = \sum_{i=0}^{n-1} c_i x^i + \sum_{i=0}^{n-1} d_i x^i y$ is known. Since $t \in \Gamma_\alpha$, the coefficients in t satisfy $b_k = b_{n-k}$ for $k = 1, \ldots, n-1$. We write

$$\gamma = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y$$

for known constants v_i, w_i. Substituting the above expansions into the equation $sht = \gamma$, we have

$$\begin{aligned}
&(\sum_{i=0}^{n-1} a_i x^i)(\sum_{i=0}^{n-1} c_i x^i + \sum_{i=0}^{n-1} d_i x^i y)(\sum_{i=0}^{n-1} b_i x^i y) = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y \\
\implies &(\sum_{i,j=0}^{n-1} a_i c_j x^{i+j} + \sum_{i,j=0}^{n-1} a_i d_j x^{i+j} y)(\sum_{k=0}^{n-1} b_k x^k y) = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y \\
\implies &\sum_{i,j,k=0}^{n-1} a_i c_j b_k x^{i+j+k} y + \sum_{i,j,k=0}^{n-1} a_i d_j b_k \lambda x^{i+j+k} = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y
\end{aligned}$$

Comparing coefficients, we have the following two equations

$$\sum_{i,j,k=0}^{n-1} a_i c_j b_k x^{i+j+k} y = \sum_{i=0}^{n-1} w_i x^i y, \tag{6}$$

$$\lambda \sum_{i,j,k=0}^{n-1} a_i d_j b_k x^{i+j+k} = \sum_{i=0}^{n-1} v_i x^i \tag{7}$$

Define vectors $\mathbf{a} = (a_0, \ldots, a_{n-1})^T$, $\mathbf{b} = (b_0, \ldots, b_{n-1})^T$, $\mathbf{c} = (c_0, \ldots, c_{n-1})^T$, $\mathbf{d} = (d_0, \ldots, d_{n-1})^T$, $\mathbf{w} = (w_0, \ldots, w_{n-1})^T$, $\mathbf{v} = (v_0, \ldots, v_{n-1})^T$ in $\mathbb{F}_q^n$. Here, $\mathbf{b}$ is a reversible vector, i.e. $b_i = b_{n-i}$ for each $i = 1, \ldots, n-1$. The vectors $\mathbf{a}$ and $\mathbf{b}$ are unknown to the adversary, while $\mathbf{c}$, $\mathbf{d}$, $\mathbf{v}$, and $\mathbf{w}$ are publicly known.

5.1 REDUCTION TO MATRIX EQUATIONS

In the below discussion, all subscripts are taken modulo n. The following lemma shows that Equation (6) can be reduced to a matrix equation over $\mathbb{F}_q$.

Lemma 9. *Equation* (6) *is equivalent to the matrix equation* $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) \cdot \mathbf{a} = \mathbf{w}$ *over* $\mathbb{F}_q$.

Proof. Equating the coefficients of the basis vectors $x^i y$ in Equation (6), we have

$$\begin{aligned}
w_i &= \sum_{\ell=0}^{n-1} \sum_{(j,k) \mid j+k=\ell \mod n} c_j b_k a_{i-\ell} \\
&= \sum_{\ell=0} \sum_{(j,k) \mid j+k=i-\ell \mod n} c_j b_k a_\ell \\
&= \begin{pmatrix} z_i(\mathbf{b}, \mathbf{c}) & z_{i-1}(\mathbf{b}, \mathbf{c}) & \ldots & z_0(\mathbf{b}, \mathbf{c}) & z_{n-1}(\mathbf{b}, \mathbf{c}) & \ldots & z_{i+1}(\mathbf{b}, \mathbf{c}) \end{pmatrix} \cdot \mathbf{a}
\end{aligned}$$

Thus, we can rewrite Equation (6) equivalently as the system

$$\begin{aligned} w_0 &= \big(z_0(\mathbf{b},\mathbf{c}) \quad z_{n-1}(\mathbf{b},\mathbf{c}) \quad \dots \quad z_1(\mathbf{b},\mathbf{c})\big)\cdot\mathbf{a} \\ w_1 &= \big(z_1(\mathbf{b},\mathbf{c}) \quad z_0(\mathbf{b},\mathbf{c}) \quad \dots \quad z_2(\mathbf{b},\mathbf{c})\big)\cdot\mathbf{a} \\ &\vdots \\ w_{n-1} &= \big(z_{n-1}(\mathbf{b},\mathbf{c}) \quad z_{n-2}(\mathbf{b},\mathbf{c}) \quad \dots \quad z_0(\mathbf{b},\mathbf{c})\big)\cdot\mathbf{a} \end{aligned}$$

In other words, $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\cdot\mathbf{a} = \mathbf{w}$. □

One may similarly rewrite Equation (7) as above, so that we have the following lemma.

Lemma 10. *Equation* (7) *is equivalent to the matrix equation* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\cdot\mathbf{a} = \mathbf{v}$ *over* $\mathbb{F}_q$.

Combining the results of Lemmas 9 and 10, if the vectors **b**,**c** and **d** are given, then **a** is a simultaneous solution to the matrix equations $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\cdot\mathbf{a} = \mathbf{w}$ and $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\cdot\mathbf{a} = \mathbf{v}$. However, a priori the vector **b** is unknown to the adversary. If we can find **b** such that this system of equations has a simultaneous solution, then we are done with reducing the DPD problem to a solving a single system of linear equations, which can be done in polynomial time. Summarizing this discussion, we have the following result.

Proposition 3. *Suppose that a vector* $\mathbf{b} = (b_0,\dots,b_{n-1})$ *is such that the system of simultaneous equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$ *has a simultaneous solution* $\mathbf{a} = (a_0,\dots,a_{n-1})$. *Then,* $s = \sum_{i=0}^{n-1} a_i x^i$, $t = \sum_{i=0}^{n-1} b_i x^i y$ *is a solution of the equation* $sht = \gamma$.

Now, for an adversary, the vectors **a** and **b** are both unknown. We will show below that in most cases, it suffices for the adversary to fix a suitable value for **b** and then proceed to solve any one of the linear equations in Lemmas 9 and 10 for **a**. More precisely, we show that if $M_{\mathbf{c}}$ and $M_{\mathbf{d}}$ are invertible, then a solution is possible for any randomly chosen $\mathbf{b} \in \Gamma_\alpha$ for which the correponding circulant matrix $M_{\mathbf{b}}$ is invertible. Since the values arise from a legitimate public key, we know that there exists a vector $\mathbf{b} \in \Gamma_\alpha$ such that the equations $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ and $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$ have a simultaneous solution **a**.

Proposition 4. *Let the vectors* **c** *and* **d** *be such that* $M_{\mathbf{c}}$ *and* $M_{\mathbf{d}}$ *are invertible. Assume that at least one simultaneous solution* $(\mathbf{a},\mathbf{b})$ *exists to the matrix equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$. *Then, for any randomly chosen* $\mathbf{b} \in \Gamma_\alpha$ *such that* $M_{\mathbf{b}}$ *is invertible, the equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$ *have a simultaneous solution* **a** *computable in polynomial time.*

Proof. Here, **b**, **c**, and **d** are invertible, and thus so are $M_{\mathbf{z}}(\mathbf{b},\mathbf{d}) = M_{\mathbf{d}}\cdot M_{\mathbf{b}}$ and $M_{\mathbf{z}}(\mathbf{b},\mathbf{c}) = M_{\mathbf{c}}\cdot M_{\mathbf{b}}$. Now, we know that a solution $(\mathbf{a},\mathbf{b})$ exists, and so for some vectors **a** and **b** we have

$$\lambda M_{\mathbf{d}} M_{\mathbf{b}}\mathbf{a} = \mathbf{v}, \quad M_{\mathbf{c}} M_{\mathbf{b}}\mathbf{a} = \mathbf{w},\ i.e.\ \lambda^{-1} M_{\mathbf{d}}^{-1}\mathbf{v} = M_{\mathbf{b}}\mathbf{a},\ M_{\mathbf{c}}^{-1}\mathbf{w} = M_{\mathbf{b}}\mathbf{a}$$

So, independently of **a** and **b** we necessarily have

$$\lambda^{-1} M_{\mathbf{d}}^{-1}\mathbf{v} = M_{\mathbf{c}}^{-1}\mathbf{w} \tag{8}$$

Now let **b** be any random vector such that $M_{\mathbf{b}}$ is invertible. Multiplying equation (8) by $M_{\mathbf{b}}^{-1}$, we get

$$\begin{aligned} &\lambda^{-1} M_{\mathbf{b}}^{-1} M_{\mathbf{d}}^{-1}\mathbf{v} = M_{\mathbf{b}}^{-1} M_{\mathbf{c}}^{-1}\mathbf{w} \\ \implies &\lambda^{-1} M_{\mathbf{z}}(\mathbf{b},\mathbf{d})^{-1}\mathbf{v} = M_{\mathbf{z}}(\mathbf{b},\mathbf{c})^{-1}\mathbf{w} \end{aligned}$$

Setting $\mathbf{a} := \lambda^{-1} M_{\mathbf{z}}(\mathbf{b},\mathbf{d})^{-1} M_{\mathbf{v}} = M_{\mathbf{z}}(\mathbf{b},\mathbf{c})^{-1}\mathbf{w}$, we get **a** as the simultaneous solution $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ and $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$. □

5.2 THE ALGORITHM FOR CRYPTANALYSIS

Before describing the cryptanalysis algorithm, we state the following assumption, which we will make for the sake of our complexity argument. We do not have a proof of its truth, but experimental evidence strongly suggests that it holds to a good approximation.

Assumption 1. *Let P_1 denote the probability of a uniformly sampled $n \times n$ circulant matrix over $\mathbb{F}_q$ being invertible and P_2 denote the probability that the circulant matrix corresponding to a uniformly samples reversible vector is invertible. Then $P_1 = P_2$. In other words, the probability distribution function corresponding to invertibility remains the same when restricted to matrices corresponding to reversible vectors.*

We have the following result.

Corollary 2. *Let $M_{\mathbf{c}}$ and $M_{\mathbf{d}}$ be invertible and γ be a legitimate public key. Let e denote the largest power of p dividing n. Further, assume that Assumption 1 holds. Then, the equation $sht = \gamma$ in the unknowns $s \in \mathbb{F}_q^{\alpha} C_n$, $t \in \Gamma_\alpha$ can be solved for a legitimate secret key (s,t) in an expected $O\left(\left(1 - \frac{1}{q}\right)^{-n/p^e}\right)$ steps. If n is a power of p then we have a constant time solution.*

Proof. Since γ is a legitimate public key, a least one simultaneous solution $(\mathbf{a}, \mathbf{b})$ exists (the one corresponding to the initial secret key) to the matrix equations $\lambda M_{\mathbf{z}}(\mathbf{b}, \mathbf{d})\mathbf{a} = \mathbf{v}$ and $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c})\mathbf{a} = \mathbf{w}$. Now, from Corollary 1, a vector $\mathbf{b} \in \mathbb{F}_q^n$ such that $\mathbf{b}$ is invertible can be found in an expected $\left\lceil \frac{1}{\left(1-\frac{1}{q}\right)^{n/p^e}} \right\rceil$ number of steps. For the solution of the DPD problem, one further requires that the vector $\mathbf{b}$ satisfies $b_i = b_{n-1}$ for $1 \leq i \leq n-1$, i.e. that $\mathbf{b} \in \Gamma_\alpha$. From Assumption 1, we may assume the same number of expected steps. Thus, by Proposition 4, we can set b to be any vector in Γ_α such that $M_{\mathbf{b}}$ is invertible. If n is a power of p, this quantity is $\left\lceil \frac{1}{1-\frac{1}{q}} \right\rceil$, which is decreasing in q, with the smallest value being 2, for $q = 2$. Thus, in this case the time complexity is $O(1)$. This is also confirmed by experimental results, where randomly chosen symmetric vectors $\mathbf{b} \in \Gamma_\alpha$ were invertible in almost all trials. Once such a vector $\mathbf{b}$ is found, one can compute $\mathbf{a} = \lambda^{-1} M_{\mathbf{z}}(\mathbf{b}, \mathbf{d})^{-1} M_{\mathbf{v}} = M_{\mathbf{z}}(\mathbf{b}, \mathbf{c})^{-1}\mathbf{w}$. By Proposition 3, this gives a solution to the DPD problem $sht = \gamma$. □

We now state an algorithm to cryptanalyze the key exchange. Its correctness follows from the above discussion. All the parameters suggested for Protocol 1 by the authors of [4] use $n = p$, so this algorithm provides a constant-time cryptanalysis.

Algorithm 1: Cryptanalysis of Key Exchange over $\mathbb{F}_q^{\alpha} D_{2n}$

Input Parameter λ and the cocycle $\alpha = \alpha_\lambda$, public element $h = \sum_{i=0}^{n-1} c_i x^i + \sum_{i=0}^{n-1} d_i x^i y$, public key $\gamma = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y$.

Output A solution $(s,t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$ satisfying $sht = \gamma$. This tuple is a solution to the DPD problem.

1: Define vectors in $\mathbb{F}_q^n$: $\mathbf{c} = (c_0, \ldots, c_{n-1})$, $\mathbf{d} = (d_0, \ldots, d_{n-1})$, $\mathbf{v} = (v_0, \ldots, v_{n-1})$, $\mathbf{w} = (w_0, \ldots, w_{n-1})$.
2: If $M_{\mathbf{c}}$ or $M_{\mathbf{d}}$ is not invertible
    Return Fail
3: Pick a vector $\mathbf{b} = (b_0, \ldots, b_{n-1}) \leftarrow \Gamma_\alpha$ at random.
4: If $M_{\mathbf{b}}$ is not invertible, repeat step (3). If it is invertible, go to step (5).
5: Compute $\mathbf{a} = \lambda^{-1} M_{\mathbf{z}}(\mathbf{b}, \mathbf{c})^{-1}\mathbf{w}$ $(= M_{\mathbf{b}}^{-1} M_{\mathbf{d}}^{-1}\mathbf{v})$.
6: With $\mathbf{a} = (a_0, \ldots, a_{n-1})$, set $s = \sum_{i=0}^{n-1} a_i x^i$ and $t = \sum_{i=0}^{n-1} b_i x^i y$.
7: Return (s,t).

Remark 2. *The solution (s,t) to the DPD returned by Algorithm 1 and referenced in Corollary 2 is a legitimate secret key, but not necessarily the same as the originally chosen secret key. In fact, as is clear from the discussion above, $t = \sum_{i=0}^{n-1} b_i x^i y \in \Gamma_\alpha$ can be selected at random, and a solution for $s \in \mathbb{F}_q^{\alpha} C_n$ is found long as $M_{\mathbf{b}}$ is invertible..*

Now, since $\mathbf{c}$ and $\mathbf{d}$ are random in $\mathbb{F}_q^n$, the circulant matrices $M_{\mathbf{c}}$ and $M_{\mathbf{d}}$ are invertible with high probability. The probability that the algorithm fails is the probability that at least one of them is not invertible, which is given by $1 - (1 - \frac{1}{q})^2$. Clearly this quantity shrinks with increasing values of q and n. In [4] the smallest values of these parameters are $q = n = 19$, for which this probability is ≈ 0.1. Thus, Algorithm 1 succeeds in cryptanalyzing the system with a probability of at least 90 percent.

An immediate corollary of the above argument is that the two-sided multiplication action

$$(\mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha) \times \mathbb{F}_q^{\alpha} D_{2n} \to \mathbb{F}_q^{\alpha} D_{2n}$$

$$(s,t)\cdot h \mapsto sht,\ s \in \mathbb{F}_q^{\alpha} C_n,\ t \in \Gamma_\alpha$$

is far from being injective, contrary to the assumption of the authors. In fact, for most values of t and $\gamma \in \mathbb{F}_q^{\alpha} D_{2n}$, there is a unique pre-image $s \in \mathbb{F}_q^{\alpha} C_n$ such that $sht = \gamma$. Thus, the probability that random choosing yields the right solution is not $1/|\mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha|$, as claimed by the authors. The real probability is greater than or equal to probability that the matrices $M_{\mathbf{c}}$ and $M_{\mathbf{d}}$ are invertible and that the correct value of s corresponding to t is chosen, which is $\approx 1/|\mathbb{F}_q^{\alpha} C_n|$ (we already saw that the probability of the matrices being invertible is very close to 1). From this, one also sees that the run time of an exhaustive search would be linear in $|\mathbb{F}_q^{\alpha} C_n| = p^{nm}$, rather than in $|\mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha| = p^{nm} p^{m\lfloor \frac{n+1}{2} \rfloor}$, as claimed by the authors of [4].

5.3 EXAMPLES

In this subsection, we present some examples generated by computer search, using the algebra software package SageMath [19]. For the structure of the twisted group algebra and the generation of the keys, we made use of the original source code of the authors. Our entire working code including the cryptanalysis can be found at: https://github.com/simran-tinani/Cryptanalysis-of-twisted-group-algebra-system

In the following examples, an element $\sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i y$ of $\mathbb{F}_q^{\alpha} D_{2n}$ is denoted by the $2n$-tuple $(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1})$.

Example 1. *For parameters $n = 23,\ q = 23,\ \lambda = 11$, and using the notations above, consider the randomly generated public element h, and secret key $(s,t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$.*

h =(19, 9, 4, 14, 6, 13, 21, 18, 18, 10, 9, 2, 5, 15, 13, 22, 18, 13, 16, 20, 11, 2, 11, 6, 18, 7, 17, 8, 20, 20, 17, 7, 15, 1, 11, 9, 17, 4, 11, 16, 5, 17, 19, 18, 19, 20),
s =(20, 17, 20, 22, 18, 18, 11, 12, 2, 3, 18, 11, 2, 18, 3, 14, 10, 2, 13, 14, 3, 9, 17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
t =(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 22, 0, 14, 3, 2, 19, 4, 15, 1, 21, 3, 6, 6, 3, 21, 1, 15, 4, 19, 2, 3, 14, 0)

Using the method in Section 5, the program computed the solution $(\tilde{s}, \tilde{t})$ to the DPD, where

$\tilde{s}$ =(13, 16, 5, 1, 21, 1, 2, 8, 17, 2, 12, 11, 4, 0, 20, 7, 19, 16, 3, 14, 22, 6, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
$\tilde{t}$ =(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 2, 17, 16, 12, 16, 12, 10, 6, 8, 3, 0, 0, 3, 8, 6, 10, 12, 16, 12, 16, 17, 2)

It was verified that $sht = \tilde{s}h\tilde{t}$, so a legitimate private key was recovered.

Example 2. *For parameters $n = 19,\ q = 19,\ \lambda = 18$, and using the notations above, consider the randomly generated public element h, and secret key $(s,t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$.*

h =(14, 5, 13, 4, 10, 12, 8, 6, 17, 18, 15, 1, 14, 14, 15, 15, 13, 4, 6, 7, 7, 11, 13, 4, 11, 12, 3, 11, 18, 8, 3, 3, 6, 11, 17, 1, 7, 10),
s =(18, 14, 1, 0, 15, 5, 7, 0, 1, 7, 10, 5, 9, 18, 2, 12, 17, 12, 14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
t =(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 17, 4, 10, 18, 5, 5, 9, 15, 18, 18, 15, 9, 5, 5, 18, 10, 4, 17)

Using the method in Section 5, the program computed the solution $(\tilde{s}, \tilde{t})$ to the DPD, where

$\tilde{s}$ =(12, 6, 4, 10, 12, 4, 5, 7, 0, 15, 8, 7, 1, 0, 2, 15, 6, 7, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
$\tilde{t}$ =(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 14, 13, 11, 10, 3, 3, 1, 1, 3, 16, 16, 3, 1, 1, 3, 3, 10, 11, 13)

It was verified that $sht = \tilde{s}h\tilde{t}$, so a legitimate private key was recovered.

Example 3. *For parameters $n = 41,\ q = 41,\ \lambda = 29$, and using the notations above, consider the randomly generated public element h, and secret key $(s,t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$.*

h =(33, 2, 29, 20, 9, 5, 36, 13, 26, 15, 38, 27, 33, 4, 20, 4, 14, 23, 12, 0, 35, 5, 38, 40, 1, 6, 16, 26, 9, 0, 29, 6, 32, 26, 14, 32, 18, 29, 13, 35, 7, 8, 38, 26, 20, 25, 24, 18, 30, 28, 22, 8, 21, 1, 33, 29, 2, 22, 25, 6, 13, 24, 18, 26, 30, 38, 3, 1, 39, 11, 15, 10, 9, 16, 3, 7, 36, 26, 22, 6, 0, 15),
s =(24, 2, 12, 32, 10, 2, 27, 1, 5, 7, 17, 32, 7, 24, 28, 26, 17, 8, 32, 18, 13, 8, 19, 17, 0, 11, 33, 17, 27, 1, 36, 3, 33, 9, 30, 34, 22, 26, 21, 5, 29, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
t =(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 13, 8, 18, 11, 31, 9, 34, 3, 16, 39, 32, 0, 15, 31, 3, 26, 0, 31, 39, 4, 40, 40, 4, 39, 31, 0, 26, 3, 31, 15, 0, 32, 39, 16, 3, 34, 9, 31, 11, 18, 8)

Using the method in Section 5, the program computed the solution $(\tilde{s}, \tilde{t})$ *to the DPD, where*

$$\tilde{s} = (39, 9, 4, 23, 8, 8, 10, 40, 31, 27, 22, 36, 11, 14, 35, 28, 25, 0, 0, 10, 16, 33, 24, 6, 33, 17, 15, 13, 17, 10, 18, 31, 33, 16, 13, 28, 2, 36, 37, 13, 30, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\tilde{t} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 35, 6, 8, 35, 23, 22, 39, 12, 22, 36, 34, 1, 29, 8, 16, 40, 29, 16, 24, 14, 31, 31, 14, 24, 16, 29, 40, 16, 8, 29, 1, 34, 36, 22, 12, 39, 22, 23, 35, 8, 6)$$

It was verified that $sht = \tilde{s}h\tilde{t}$*, so a legitimate private key was recovered.*

Clearly, in each of the above examples, $s \neq \tilde{s}$ and $t \neq \tilde{t}$, but $sht = \tilde{s}h\tilde{t}$. Thus, each of these examples also serves as a counterexample to the injectivity of the two-sided action.

6 CONCLUSION

In this paper, we provided a method for cryptanalysis of the protocol in [4] which is based on a double-sided multiplication problem in the twisted dihedral group algebra $\mathbb{F}_q^{\alpha} D_{2n}$. We first showed that the underlying DPD algorithmic problem is equivalent to a commutative semigroup action problem. For our cryptanalysis, we showed that the task for an adversary attempting to solve the underlying DPD problem is equivalent to the solution of two equations in $\mathbb{F}_q$ involving circulant matrices. We further demonstrated a solution for these equations using linear algebra, which works with a success rate of at least 90 percent for the proposed values of the parameters in [4]. The key exchange system in [4] and its underlying algorithmic problem are both therefore clearly insecure, even in a classical setting.

REFERENCES

[1] Adi Ben-Zvi, Arkadius Kalka, and Boaz Tsaban. "Cryptanalysis via algebraic spans". In: *Annual International Cryptology Conference*. Springer. 2018, pp. 255–274.

[2] Ran Canetti and Hugo Krawczyk. "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels". In: *Advances in Cryptology — EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 453–474. ISBN: 978-3-540-44987-4.

[3] Bren Cavallo and Delaram Kahrobaei. "A family of polycyclic groups over which the uniform conjugacy problem is NP-complete". In: *International Journal of Algebra and Computation* 24.04 (2014), pp. 515–530. DOI: 10.1142/S0218196714500234. eprint: https://doi.org/10.1142/S0218196714500234. URL: https://doi.org/10.1142/S0218196714500234.

[4] Javier de la Cruz and Ricardo Villanueva-Polanco. "Public key cryptography based on twisted dihedral group algebras". In: *Advances in Mathematics of Communications* 16.2 (2022), pp. 195–215.

[5] Javier De La Cruz and Wolfgang Willems. "Twisted Group Codes". In: *IEEE Transactions on Information Theory* 67.8 (2021), pp. 5178–5184. DOI: 10.1109/TIT.2021.3089003.

[6] Mohammad Eftekhari. "Cryptanalysis of Some Protocols Using Matrices over Group Rings". In: Apr. 2017, pp. 223–229. ISBN: 978-3-319-57338-0. DOI: 10.1007/978-3-319-57339-7_13.

[7] María Dolores Gómez Olvera, Juan Antonio López Ramos, and Blas Torrecillas Jover. "Public Key Protocols over Twisted Dihedral Group Rings". In: *Symmetry* 11.8 (2019). ISSN: 2073-8994. DOI: 10.3390/sym11081019. URL: https://www.mdpi.com/2073-8994/11/8/1019.

[8] Lize Gu and Shihui Zheng. "Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography". In: *J. Appl. Math.* 2014 (2014), 630607:1–630607:10.

[9] Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. "Public key exchange using matrices over group rings". In: *Groups - Complexity - Cryptology* 5.1 (2013), pp. 97–115. DOI: doi:10.1515/gcc-2013-0007. URL: https://doi.org/10.1515/gcc-2013-0007.

[10] Juan Antonio López-Ramos et al. "An application of group theory in confidential network communications". In: *Mathematical Methods in the Applied Sciences* 41 (2016), pp. 2294–2298.

[11] Gérard Maze, Chris Monico, and Joachim Rosenthal. "Public Key Cryptography based on Semigroup Actions". In: *Adv. in Math. of Communications* 1.4 (2007), pp. 489–507. DOI: 10.3934/amc.2007.1.489.

[12] Alfred Menezes and Yihong Wu. "The Discrete Logarithm Problem in $GL(n, q)$". In: *Ars Comb.* 47 (1997).

[13] C. Monico. "Semirings and Semigroup Actions in Public-Key Cryptography". PhD thesis. University of Notre Dame, May 2002.

[14] Alexei Myasnikov and Vitaliĭ Roman'kov. "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1 (2015), pp. 81–94. DOI: doi:10.1515/gcc-2015-0007. URL: https://doi.org/10.1515/gcc-2015-0007.

[15] Alexey D. Myasnikov and Alexander Ushakov. "Quantum algorithm for discrete logarithm problem for matrices over finite group rings". In: *Groups Complexity Cryptology* 6.1 (2014), pp. 31–36. DOI: doi:10.1515/gcc-2014-0003. URL: https://doi.org/10.1515/gcc-2014-0003.

[16] María-Dolores Olvera-Lobo, Juan Antonio López-Ramos, and Blas Torrecillas. "Public Key Protocols over Twisted Dihedral Group Rings". In: *Symmetry* 11 (2019), p. 1019.

[17] Vitaly Roman'kov. "A general encryption scheme using two-sided multiplications with its cryptanalysis". In: *arXiv: Group Theory* (2017).

[18] Vitaly Roman'kov. "Two general schemes of algebraic cryptography". In: *Groups Complexity Cryptology* 10.2 (2018), pp. 83–98. DOI: doi:10.1515/gcc-2018-0009. URL: https://doi.org/10.1515/gcc-2018-0009.

[19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.6)*. https://www.sagemath.org. 2020.

[20] Simona Samardjiska et al. "A Reaction Attack Against Cryptosystems Based on LRPC Codes". In: *Progress in Cryptology – LATINCRYPT 2019*. Ed. by Peter Schwabe and Nicolas Thériault. Cham: Springer International Publishing, 2019, pp. 197–216. ISBN: 978-3-030-30530-7.

[21] Peter W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, pp. 124–134.

[22] Vladimir Shpilrain and Alexander Ushakov. "A new key exchange protocol based on the decomposition problem". In: *arXiv preprint arXiv:0512140* (2005).

[23] Simran Tinani, Carlo Matteotti, and Joachim Rosenthal. *Complexity of Conjugacy Search in some Polycyclic and Matrix Groups*. 2022. DOI: 10.48550/ARXIV.2203.03525. URL: https://arxiv.org/abs/2203.03525.

[24] Boaz Tsaban. "Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography". In: *Journal of Cryptology* 28.3 (2015), pp. 601–622.