mathematics

MDPI

Article

Secure Group Communications Using Twisted Group Rings

María Dolores Gómez Olvera, Juan Antonio López Ramos * and Blas Torrecillas Jover

Department of Mathematics, University of Almeria, 04120 Almeria, Spain
* Correspondence: jlopez@ual.es

Abstract: In this paper we introduce a Group Key Management protocol following the idea of the classical protocol that extends the well-known Diffie–Hellman key agreement to a group of users. The protocol is defined in a non-commutative setting, more precisely, in a twisted dihedral group ring. The protocol is defined for an arbitrary cocycle, extending previous key agreements considered for two users. The main objective of this work is to show that there is no lack of security derived from the fact that a larger amount of public information is known by an external observer.

Keywords: group key management; twisted group ring; cocycle

MSC: 94A60

1. Introduction

In recent years, new hard problems have been proposed in public key cryptography, since those that we are using might be not secure soon. When two parties want to communicate through an insecure channel, they need to undertake a key agreement, which consists of agreeing on a secret shared key by exchanging information that does not compromise the common key.

The first widely used protocol that allows this to happen was proposed in 1976 by W. Diffie and M. Hellman [1], and works as follows:

> Let Alice and Bob be two users, who want to agree on a common key through an insecure channel. Consider p a prime number, $\mathbb{Z}_p^*$ the multiplicative group of integers modulo p, and g a primitive root modulo p, all of them public.
>
> (i) Alice chooses a secret integer a, and sends Bob $p_A = g^a \pmod p$.
> (ii) Bob chooses a secret integer b, and sends Alice $p_B = g^b \pmod p$.
> (iii) Alice computes $p_B^a \pmod p$, and Bob computes $p_A^b \pmod p$, so both obtain the same value, which is the secret shared key $K = g^{ab} \pmod p$.

Information shared does not compromise the shared key since the underlying problem an attacker would need to solve, the so-called Discrete Logarithm Problem (DLP) is believed to be hard. This key agreement can be seen as an example of the protocol by Maze et al. [2] in a general setting:

> Let S be a finite set, G an abelian semigroup, ϕ a $G-$action on S, and a public element $s \in S$.
>
> (i) Alice chooses $a \in G$, and sends Bob $p_A = \phi(a, s)$.
> (ii) Bob chooses $b \in G$, and sends Alice $p_B = \phi(b, s)$.
> (iii) Alice computes $\phi(a, p_B)$, and Bob computes $\phi(b, p_A)$, so both obtain the secret shared key $K = \phi(a, \phi(b, s)) = \phi(b, \phi(a, s))$.

The underlying problem that gives sense to its security is known as the Semigroup Action Problem (SAP).

check for updates

Citation: Gómez Olvera, M.D.; López Ramos, J.A.; Torrecillas Jover, B. Secure Group Communications Using Twisted Group Rings. *Mathematics* **2022**, *10*, 2845. https://doi.org/10.3390/math10162845

Academic Editors: Juan Ramón García Rozas, Luis Oyonarte Alcalá and Driss Bennis

Received: 27 June 2022
Accepted: 9 August 2022
Published: 10 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Semigroup Action Problem. Given a semigroup action ϕ of the group G on a set S and elements $x \in S$ and $y \in G$, find $g \in G$ such that $\phi(g, x) = y$.

Motivated by this, the authors proposed in [3] a new setting, and some protocols, which extend these techniques to a non-commutative setting. In this case this is a twisted group ring, an extension of group rings, that have also been recently used in cryptography (cf. [4–7]). The action proposed in [3] is the two-sided multiplication in a twisted group ring. Thus the problem which the security of this new proposal is based on, is a modification in the twisted case of the so-called Decomposition Problem (DP).

Decomposition Problem. Given a group G, $(x, y) \in G \times G$ and $S \subset G$, the problem is to find $z_1, z_2 \in S$ such that $y = z_1 x z_2$.

A natural problem is how to extend this kind of key management protocol for two users to a greater set of these. In the classic Diffie–Hellman protocol, a solution is proposed in [8]; and in the more general case of SAP, this solution can be found in [9]. In both cases, it is shown that the extra information shared in the case of a n users, key exchange ($\geq$2) does not imply any information leakage than in to the 2-users case.

Our aim in this work is to show that in this new setting, which differs from those above, given the non-commutativity of twisted group rings, these kind of protocols could be useful as well. Moreover, they could even avoid possible threats in the known cases.

2. Results

2.1. Algebraic Setting

In this section, twisted group rings are defined, and we also show some properties that allow the key exchange.

Definition 1. *Let K be a ring and G a finite multiplicative group. Let $U(K)$ be the units of K. We call the map $\alpha : G \times G \to U(K)$ a 2-cocycle if $\alpha(1, 1) = 1$ and for all $g, h, k \in G$ it satisfies the equation*

$$\alpha(g, hk)\alpha(h, k) = \alpha(gh, k)\alpha(g, h) \tag{1}$$

We denote the set of all 2-cocycles of G by $Z^2(G, U(K))$.

Definition 2. *Let K be a ring, G be a multiplicative group, and $\alpha \in Z^2(G, U(K))$. The group ring $K^\alpha G$ is defined to be the set of all finite sums of the form*

$$\sum_{g_i \in G} r_i g_i,$$

where $r_i \in K$ and all but a finite number of r_i are zero.

The sum of two elements in $K^\alpha G$ is defined by

$$\Big(\sum_{g_i \in G} r_i g_i\Big) + \Big(\sum_{g_i \in G} s_i g_i\Big) = \sum_{g_i \in G} (r_i + s_i) g_i.$$

and their product, which is twisted by a cocycle, is given by

$$\Big(\sum_{g_i \in G} r_i g_i\Big) \cdot \Big(\sum_{g_i \in G} s_i g_i\Big) = \sum_{g_i \in G} \Big(\sum_{g_j g_k = g_i} r_j s_k \, \alpha(g_j, g_k)\Big) g_i.$$

Let K be a finite field, G the dihedral group of $2m$ elements [10],

$$D_{2m} = \langle x, y : x^m = y^2 = 1, yx^a = x^{m-a} y \rangle$$

and $\alpha \in Z^2(D_{2m}, K)$. Let $C_m = \langle x \rangle$ be the cyclic subgroup of D_{2m} generated by x. Then we have that $K^\alpha D_{2m}$ is a free $K^\alpha C_m$ module with basis $\{1, y\}$, and therefore $K^\alpha D_{2m}$ is the direct sum of the $K-$vector spaces:

$$K^\alpha D_{2m} = K^\alpha C_m \oplus K^\alpha C_m y$$

Definition 3. *For a given 2-cocycle $\alpha \in Z^2(D_{2m}, U(K))$, we define the reversible subspace of $R = K^\alpha G$ (where G is either C_m or $C_m y$) as the vector subspace*

$$\Gamma[R] = \Big\{ \sum_{i=0}^{m-1} r_i x^i y^k \in R : r_i = r_{m-i} \Big\}.$$

We will denote $\Gamma_\alpha = \Gamma[K^\alpha C_m y] = \Big\{ \sum_{i=0}^{m-1} r_i x^i y^k \in K^\alpha C_m y : r_i = r_{m-i} \Big\}.$

Now we establish some useful properties that will allow the introduction of the group key management protocol.

Definition 4. *Let $R = K^\alpha D_{2m}$ and α be a 2-cocycle. Given $h \in R$,*

$$h = \sum_{\substack{0 \le i \le m-1 \\ k=0,1}} r_i x^i y^k,$$

where $r_i \in K$ and $x, y \in D_{2m}$, we define $h^* \in K^\alpha D_{2m}$ as

$$h^* = \sum_{\substack{0 \le i \le m-1 \\ k=0,1}} r_i \alpha(x^i y, x^j y^k)^{-1} x^i y^k,$$

Lemma 1. *There exist group rings $R = K^\alpha D_{2m}$, such that, given two elements $h_1, h_2 \in R$,*

(a) If $h_1, h_2 \in K^\alpha C_n$, then $h_1 h_2 = h_2 h_1$.
(b) If $h_1, h_2 \in \Gamma_\alpha$, then $h_1 h_2^* = h_2 h_1^*$, and $h_1^* h_2 = h_2^* h_1$.

Before giving a proof of this lemma, let us give a couple of illustrative examples.

Example 1. *Let K and D_{2m} be as previously introduced.*

- *Let t be a primitive root of unity of K. The map $\alpha_1 \in Z^2(D_{2m}, K^*)$ defined by $\alpha_1(\delta, \mu) = 1$ for $\delta = x^i, \mu = x^j y^k$, and $\alpha_1(\delta, \mu) = t^j$ for $\delta = x^i y, \mu = x^j y^k$, where $i, j = 1, ..., 2m-1$, is a 2-cocycle that verifies Lemma 1. A proof can be found in [3].*
- *Let λ an element in K^*. The map $\alpha_2 \in Z^2(D_{2m}, K^*)$ defined by $\alpha_2(\delta, \mu) = \lambda$ for $\delta = x^i y, \mu = x^j y$, and $\alpha_2(\delta, \mu) = 1$ otherwise, where $i, j = 1, ..., 2m-1$, is a 2-cocycle that verifies Lemma 1. A proof of (a) and (b.1) can be found in [11]. We now provide a proof for (b.2).*

Proof of Lemma 1. Let $R = K^{\alpha_2} D_{2m}$, where α_2 is the 2-cocycle defined above. Let $h_1, h_2 \in \Gamma_\alpha$, Φ and $\varphi(h_1) = \widehat{h_1}$ as defined in [11]. The equalities (a) and (b) $h_1 h_2^* = h_2 h_1^*$ were proven in [11]. It remains to prove that $h_1^* h_2 = h_2^* h_1$. Using ([11], Lemma 3.8), we can prove the following:

$$\begin{aligned} h_1^* h_2 &= \widehat{\Phi(h_1)} \bar{y} \Phi(h_2) y = \Phi(h_1) \widehat{\bar{y}} \bar{y} \Phi(h_2) = \lambda^2 \Phi(h_1) \Phi(h_2) \\ &= \lambda^2 \Phi(h_2) \Phi(h_2) = \Phi(h_1) \widehat{\bar{y}} \bar{y} \Phi(h_1) = \widehat{\Phi(h_2)} y \Phi(h_1) y = h_2^* h_1 \end{aligned}$$

□

2.2. Key Management over Twisted Group Rings

In this section, we propose a key management protocol for n users. Let us define the action ϕ

$$\phi : (K^{\alpha}C_m \times K^{\alpha}C_m y) \times R \longrightarrow R$$
$$\phi(s_i, h) = \delta_i h \mu_i$$

where $s_i = (\delta_i, \mu_i)$. Note that

$$\phi(s_i \phi(s_j, h)) = \phi(s_i s_j, h)$$

We will sometimes write $\phi(s_i s_j, h)$ to refer to $\phi(s_i, \phi(s_j, h))$, to make some definitions more readable.

Let $h \in R$ be a random public element and assume that $R = K^{\alpha}C_m \oplus K^{\alpha}C_m y$ verifies Lemma 1. For $i = 1, ..., n$, user U_i holds a secret pair $s_i = (\delta_i, \mu_i)$, where $\delta_i \in K^{\alpha}C_m$ and $\mu_i \in \Gamma_{\alpha} \subset K^{\alpha}C_m y$. Let us define the action ϕ by means of a two-sided product $\phi(s_i, h) = \delta_i h \mu_i$. We will denote $s_i^* = (\delta_i, \mu_i^*)$. The initial key agreement for n users is given by the following steps:

(i) For $i = 1, \ldots, n-1$, user U_i sends to user U_{i+1} the message

$$\{C_i^1, C_i^2, ..., C_i^{i+1}\},$$

where $C_1^1 = h$, $C_1^2 = \delta_1 h \mu_1$ and

- for $i > 1$ even, $C_i^j = \phi(s_i, C_{i-1}^j)$, when $j < i$, $C_i^i = C_{i-1}^i$, $C_i^{i+1} = \phi(s_i^*, C_{i-1}^i)$,
- for $i > 1$ odd, $C_i^j = \phi(s_i^*, C_{i-1}^j)$, when $j < i$, $C_i^i = C_{i-1}^i$, $C_i^{i+1} = \phi(s_i, C_{i-1}^i)$.

(ii) User U_n computes the shared key $\phi(s_n, C_{n-1}^n)$ in case n is odd and $\phi(s_n^*, C_{n-1}^n)$ if n otherwise.

(iii) User U_n broadcasts

$$\{C_n^1, C_n^2, ..., C_n^{n-1}\}.$$

(iv) User U_i ($i = 1, \ldots, n-1$) computes $\phi(s_i, C_n^i)$ if n is odd or $\phi(s_i^*, C_n^i)$ if n is even.

This protocol allows all users to obtain a common shared key. For $\alpha = \alpha_1$, this was shown in Proposition 3 of [3]. Now we prove it for $\alpha = \alpha_2$.

Proposition 1. *Let $R = K^{\alpha_2}D_{2m}$. After this protocol, users $U_1, \ldots, U_n$ agree on a common key.*

Proof of Proposition 1. Firstly, we will consider that n is odd. Let us show that users $U_1, \ldots, U_{n-1}$ get the same key and that this is equal to U_n key. To do so, we will prove by induction that

$$\phi(s_i, C_n^i) = \phi(s_j, C_n^j)$$

for $i \neq j$, $i, j \in \{1, \ldots, n-1\}$ and that these are also equal to the key that U_n recovers, $\phi(s_n, C_{n-1}^n)$. For $n = 3$,

$$\begin{aligned} \phi(s_1, C_3^1) &= \phi(s_1, \delta_3\delta_2 h \mu_2 \mu_3^*) \\ &= \delta_1\delta_3\delta_2 h \mu_2 \mu_3^* \mu_1 \\ &= \delta_2\delta_3\delta_1 h \mu_1 \mu_3^* \mu_2 \\ &= \phi(s_2, \delta_3\delta_1 h \mu_1 \mu_3^*) \\ &= \phi(s_2, C_3^2) \end{aligned}$$

using the commutativity rules given by in Lemma 1,

$$\mu_2\mu_3^*\mu_1 = \mu_2\mu_1^*\mu_3 = \mu_1\mu_2^*\mu_3 = \mu_1\mu_3^*\mu_2.$$

Moreover, $\phi(s_3, C_2^3) = \delta_3\delta_2\delta_1 h \mu_1 \mu_2^* \mu_3 = \delta_2\delta_3\delta_1 h \mu_1 \mu_3^* \mu_2 = \phi(s_2, C_3^2)$.

Now, suppose that

$$\phi(s_i, C_n^i) = \phi(s_j, C_n^j).$$

Then we have

$$\begin{aligned}
\phi(s_i^*, C_{n+1}^i) &= \phi(s_i^*, \phi(s_{n+1}, C_n^i)) \\
&= \phi(s_i^* s_{n+1}, C_n^i) \\
&= \phi(s_{n+1}^* s_i, C_n^i) \\
&= \phi(s_{n+1}^*, \phi(s_i, C_n^i)) \\
&= \phi(s_{n+1}^*, \phi(s_j, C_n^j)) \\
&= \phi(s_{n+1}^* s_j, C_n^j) \\
&= \phi(s_j^* s_{n+1}, C_n^j) \\
&= \phi(s_j^*, \phi(s_{n+1}, C_n^j)) \\
&= \phi(s_j^*, C_{n+1}^j)
\end{aligned}$$

and

$$\begin{aligned}
\phi(s_n, C_{n-1}^n) &= \phi(s_n, \phi(s_{n-1}^*, C_{n-1}^{n-2})) \\
&= \phi(s_n s_{n-1}^*, C_{n-1}^{n-2}) \\
&= \phi(s_{n-1} s_n^*, C_{n-1}^{n-1}) \\
&= \phi(s_{n-1}, \phi(s_n^*, C_{n-1}^{n-1})) \\
&= \phi(s_{n-1}, C_n^{n-1})
\end{aligned}$$

So all users $U_1, \ldots, U_n$ get the same key for n odd.
Secondly, we show that this also works for n even. We prove by induction that

$$\phi(s_i^*, C_n^i) = \phi(s_j^*, C_n^j)$$

for $i \neq j$, $i, j \in \{1, \ldots, n-1\}$. And this also equals U_n key, $\phi(s_n, C_{n-1}^n)$. For $n = 4$,

$$\begin{aligned}
\phi(s_1^*, \phi(s_4, C_3^1)) &= \phi(s_1^*, \delta_4\delta_3\delta_2 h \mu_2 \mu_3^* \mu_4) \\
&= \delta_1\delta_4\delta_3\delta_2 h \mu_2 \mu_3^* \mu_4 \mu_1^* \\
&= \delta_2\delta_4\delta_3\delta_1 h \mu_1 \mu_3^* \mu_4 \mu_2^* \\
&= \phi(s_2^*, \delta_4\delta_3\delta_1 h \mu_1 \mu_3^* \mu_4) \\
&= \phi(s_2^*, \phi(s_4, C_3^2)),
\end{aligned}$$

$$\begin{aligned}
\phi(s_1^*, \phi(s_4, C_3^1)) &= \phi(s_1^*, \delta_4\delta_3\delta_2 h \mu_2 \mu_3^* \mu_4) \\
&= \delta_1\delta_4\delta_3\delta_2 h \mu_2 \mu_3^* \mu_4 \mu_1^* \\
&= \delta_3\delta_4\delta_2\delta_1 h \mu_1 \mu_2^* \mu_4 \mu_3^* \\
&= \phi(s_3^*, \delta_4\delta_2\delta_1 h \mu_1 \mu_2^* \mu_4) \\
&= \phi(s_3^*, \phi(s_4, C_3^3))
\end{aligned}$$

using that $\delta_i \in K^\alpha C_m$ commute and

$$\mu_2\mu_3^*\mu_4\mu_1^* = \mu_3\mu_2^*\mu_4\mu_1^* = \mu_3\mu_4^*\mu_2\mu_1^* = \mu_3\mu_4^*\mu_1\mu_2^* = \mu_3\mu_1^*\mu_4\mu_2^* = \mu_1\mu_3^*\mu_4\mu_2^*,$$

$$\mu_2\mu_3^*\mu_4\mu_1^* = \mu_2\mu_4^*\mu_1\mu_3^* = \mu_2\mu_1^*\mu_4\mu_3^* = \mu_1\mu_2^*\mu_4\mu_3^*.$$

In addition, $\phi(s_4^*, C_3^4) = \delta_4\delta_3\delta_2\delta_1 h \mu_1 \mu_2^* \mu_3 \mu_4^* = \delta_3\delta_4\mu_2\mu_1 h \mu_1 \mu_2^* \mu_4 \mu_3^* = \phi(s_3^*, \phi(s_4, C_3^3))$.

Suppose now that

$$\phi(s_i^*, C_n^i) = \phi(s_j^*, C_n^j).$$

Then we have

$$\begin{aligned}
\phi(s_i, C^i_{n+1}) &= \phi\big(s_i, \phi(s^*_{n+1}, C^i_n)\big)\\
&= \phi\big(s_i, \phi(s^*_{n+1}, C^i_n)\big)\\
&= \phi\big(s_i s^*_{n+1}, C^i_n)\big)\\
&= \phi\big(s_{n+1} s^*_i, C^i_n)\big)\\
&= \phi\big(s_{n+1}, \phi(s^*_i, C^i_n)\big)\\
&= \phi\big(s_{n+1}, \phi(s^*_j, C^j_n)\big)\\
&= \phi\big(s_{n+1} s^*_j, C^j_n)\big)\\
&= \phi\big(s_j s^*_{n+1}, C^j_n\big)\\
&= \phi\big(s_j, \phi(s^*_{n+1}, C^j_n)\big)\\
&= \phi(s_j, C^j_{n+1}).
\end{aligned}$$

So the shared key $\phi\big(s_i, \phi(s^*_{n+1}, C^i_n)\big)$ is the same for every $i \in \{1, \ldots, n-1\}$, and also,

$$\begin{aligned}
\phi(s^*_n, C^n_{n-1}) &= \phi(s^*_n, \phi(s_{n-1}, C^{n-2}_{n-1}))\\
&= \phi(s^*_n s_{n-1}, C^{n-2}_{n-1})\\
&= \phi(s^*_{n-1} s_n, C^{n-1}_{n-1})\\
&= \phi(s^*_{n-1}, \phi(s_n, C^{n-1}_{n-1}))\\
&= \phi(s^*_{n-1}, C^{n-1}_n)
\end{aligned}$$

so all users $U_1, \ldots, U_n$ have the same shared key, and we are done. □

Note that this protocol in $K^{\alpha_2} D_{2m}$, for $n = 2$ users, is described in ([3], Section 3) and later in ([11], Protocol 1) using the cocycles of Example 1 respectively.

For clarity, we include an example for a small number n of users ($n > 2$):

Example 2. *For a small number of users, n, the key establishment is as follows:*

(i) *For $i = 1, \ldots, n-1$, user U_i sends to user U_{i+1} the following messages:*
- *U_1 sends to U_2 $\{C^1_1, C^2_1\} = \{h, \delta_1 h \mu_1\}$.*
- *U_2 sends to U_3 $\{C^1_2, C^2_2, C^3_2\} = \{\delta_2 h \mu_2, \delta_1 h \mu_1, \delta_2 \delta_1 h \mu_1 \mu^*_2\}$.*

(ii) *Then if $n = 3$, given that n is odd, user U_3 computes the shared key $\phi(s_3, C^3_2) = \delta_3 \delta_2 \delta_1 h \mu_1 \mu^*_2 \mu_3$.*

(iii) *User U_3 broadcast $\{C^1_3, C^2_3\} = \{\delta_3 \delta_2 h \mu_2 \mu^*_3, \delta_3 \delta_1 h \mu_1 \mu^*_3\}$*

(iv) *Then users U_1 and U_2 compute the shared key as follows:*
- *U_1 computes $\phi(s^*_1, C^1_4) = \delta_1 \delta_3 \delta_2 h \mu_2 \mu^*_3 \mu_1$.*
- *U_2 computes $\phi(s^*_2, C^2_4) = \delta_2 \delta_3 \delta_1 h \mu_1 \mu^*_3 \mu_2$.*

These are equal to the key computed by U_3, as shown in Proposition 1.

If $n = 4$, given that n is even, the protocol works as follows:

(i) *Users U_1, U_2 send the same messages as before, and U_3 sends to U_4 $\{C^1_3, C^2_3, C^3_3, C^4_3\} = \{\delta_3 \delta_2 h \mu_2 \mu^*_3, \delta_3 \delta_1 h \mu_1 \mu^*_3, \delta_2 \delta_1 h \mu_1 \mu^*_2, \delta_3 \delta_2 \delta_1 h \mu_1 \mu^*_2 \mu_3\}$.*

(ii) *Then user U_4 computes the shared key $\phi(s^*_4, C^4_3) = \delta_4 \delta_3 \delta_2 \delta_1 h \mu_1 \mu^*_2 \mu_3 \mu^*_4$.*

(iii) *User U_4 broadcast $\{C^1_4, C^2_4, C^3_4\} = \{\delta_4 \delta_3 \delta_2 h \mu_2 \mu^*_3 \mu_4, \delta_4 \delta_3 \delta_1 h \mu_1 \mu^*_3 \mu_4, \delta_4 \delta_2 \delta_1 h \mu_1 \mu^*_2 \mu_4\}$*

(iv) *Then users $U_1, \ldots, U_3$ compute the shared key as follows:*
- *U_1 computes $\phi(s^*_1, C^1_4) = \delta_1 \delta_4 \delta_3 \delta_2 h \mu_2 \mu^*_3 \mu_4 \mu^*_1$.*
- *U_2 computes $\phi(s^*_2, C^2_4) = \delta_2 \delta_4 \delta_3 \delta_1 h \mu_1 \mu^*_3 \mu_4 \mu^*_2$.*
- *U_3 computes $\phi(s^*_3, C^3_4) = \delta_3 \delta_4 \delta_2 \delta_1 h \mu_1 \mu^*_2 \mu_4 \mu^*_3$.*

All users obtain the same key, as shown in Proposition 1.

We have described the so-called Initial Key Agreement (IKA), but another important process in group communications is rekeying through the Auxiliary Key Agreement (AKA), which takes advantage of the information that was sent before to create a new key in a group when necessary, and is more computationally efficient than IKA. There exist three situations: the members of the group stay the same, a member leaves the group, or someone

new joins it. It is important than the AKA happens in all these three situations, to ensure forward and backward security, as shown in [8,12,13].

In the first situation, every user U_i has the information C_n^i received from the user U_n. The rekeying process can be carried out by any of them. We call this user U_c. He chooses a new element $\widetilde{s_c} = (\widetilde{\delta_c}, \widetilde{\mu_c})$, where $\widetilde{\delta_c} \in K^\alpha C_m$ and $\widetilde{\mu_c} \in \Gamma_\alpha \subset K^\alpha C_m y$. If n is odd, he changes his private key to $\widetilde{s_c}^* s_c$ and broadcasts the message

$$\{\phi(\widetilde{s_c}^*, C_n^1), \phi(\widetilde{s_c}^*, C_n^2), \ldots, \phi(\widetilde{s_c}^*, C_n^{c-1}), C_n^c, \phi(\widetilde{s_c}^*, C_n^{c+1}), \ldots, \phi(\widetilde{s_c}^*, C_n^n)\}.$$

If n is even, he changes his private key to $\widetilde{s_c} s_c^*$ and broadcasts the message

$$\{\phi(\widetilde{s_c}, C_n^1), \phi(\widetilde{s_c}, C_n^2), \ldots, \phi(\widetilde{s_c}, C_n^{c-1}), C_n^c, \phi(\widetilde{s_c}, C_n^{c+1}), \ldots, \phi(\widetilde{s_c}, C_n^n)\}.$$

Then every user recovers the common key using the private key s_i if n is even, and s_i^* if n is odd. A proof can be found in [3].

In the second case, when some user leaves the group, the corresponding position in the rekeying message is omitted.

In the last case, when a new user U_{n+1} joins the group, if n is odd, then U_c adds the element $\phi(\widetilde{s_c}, C_n^n)$ and sends the new user the following

$$\{\phi(\widetilde{s_c}, C_n^1), \phi(\widetilde{s_c}, C_n^2), \ldots, \phi(\widetilde{s_c}, C_n^{c-1}), C_n^c, \phi(\widetilde{s_c}, C_n^{c+1}), \ldots, \phi(\widetilde{s_c}, C_n^{n-1}), \phi(\widetilde{s_c}, C_n^n)\}.$$

If n is even, U_c adds the element $\phi(\widetilde{s_c}^*, C_n^n)$ and sends to U_{n+1} the following:

$$\{\phi(\widetilde{s_c}^*, C_n^1), \phi(\widetilde{s_c}^*, C_n^2), \ldots, \phi(\widetilde{s_c}^*, C_n^{c-1}), C_n^c, \phi(\widetilde{s_c}^*, C_n^{c+1}), \ldots, \phi(\widetilde{s_c}^*, C_n^{n-1}), \phi(\widetilde{s_c}^*, C_n^n)\}.$$

Finally, user U_{n+1} proceeds to step 3 of the group key protocol and sends the other users the information to obtain the shared key using their private keys.

2.3. Security of the Group Key Management

In this section, we show that the extra information sent in the protocol for n users does not implies aditional information leakage for an attacker respect to the 2-users case. For this purpose, we define the following random variables, choosing X randomly from $(K^\alpha C_m \times \Gamma_\alpha)^n$:

$$A_n = \Big(view(n, X), y\Big), \text{ for } y \in R \text{ randomly chosen.}$$

$$D_n = \begin{cases} \Big(view(n, X), \phi(s_n^* s_{n-1} s_{n-2}^* \ldots s_3 s_2^* s_1, h), h)\Big), & \text{if } n \text{ is even.} \\ \Big(view(n, X), \phi(s_n s_{n-1}^* s_{n-2} \ldots s_3 s_2^* s_1, h)\Big), & \text{if } n \text{ is odd.} \end{cases}$$

where

- $view(n, X) :=$ the ordered set of all $\phi(s_{i_1} s_{i_2}^* s_{i_3} \ldots s_{m-2}^* s_{m-1} s_m^*, h)$, for all proper subsets $\{i_1, \ldots, i_m\}$ of $\{1, \ldots, n\}$; $m \in \{1, \ldots, n-1\}$.

when n is even, and

- $view(n, X) :=$ the ordered set of all $\phi(s_{i_1} s_{i_2}^* s_{i_3} \ldots s_{m-2} s_{m-1}^* s_m, h)$, for all proper subsets $\{i_1, \ldots, i_m\}$ of $\{1, \ldots, n\}$; $m \in \{1, \ldots, n-1\}$.

when n is odd.

Also note that $\phi(s_n^* s_{n-1} s_{n-2}^* \ldots s_3 s_2^* s_1, h)$, or $\phi(s_n s_{n-1}^* s_{n-2} \ldots s_3 s_2^* s_1, h)$, is the common secret key, is case n is even or odd respectively.

Let the relation $\sim$ be polynomial indistinguishability, as defined in [8]. In this context, it means that no polynomial-time algorithm can distinguish between a key and a random value in $K^\alpha D_{2m}$ with probability significantly greater than $\frac{1}{2}$. We can derive the following result on $\sim$.

Proposition 2. *The relation $\sim$ is an equivalence relation.*

A proof of this proposition can be found in [14]. Before we prove the main result, let us show that

Lemma 2. *We can write* $view(n, \{s_1, s_2\} \cup X)$, *with* $X = \{s_3, \ldots, s_n\}$ *as a permutation of*

$$V = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n s_{n-1}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X),$$

$$\phi(s_n s_{n-1}^* s_{n-2} \ldots s_3^* s_1, h), view(n-1, \{s_2^* s_1\} \cup X)\Big)$$

when n is even, and as a permutation of

$$V = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n^* s_{n-1} s_{n-2}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X),$$

$$\phi(s_n^* s_{n-1} \ldots s_3^* s_1, h), view(n-1, \{s_1 s_2^*\} \cup X)\Big)$$

when n is odd.

Proof of Lemma 2. Now we show that both sets are equal. First, we prove that $view(n, \{s_1, s_2\} \cup X) \subset V$: Let $a \in view(n, \{s_1, s_2\} \cup X)$:

- If n is even:
  - (i) If a contains $s_2^* s_1 (= s_1^* s_2)$, then it belongs to $view(n-1, \{s_2^* s_1\} \cup X) \subset V$.
  - (ii) If a does not contain s_1 (or s_1^*),
    - but it contains all the remaining elements, $s_2^{(*)}, \ldots, s_n^{(*)}$, then it belongs to $\phi(s_n s_{n-1}^* \ldots s_3^* s_2, h) \subset V$.
    - and if it does not contain all the remaining elements, then it belongs to $view(n-1, \{s_2\} \cup X) \subset V$.
  - (iii) If a does not contain s_2 (or s_2^*),
    - but it contains all the remaining elements, $s_1^{(*)}, s_3^{(*)}, \ldots, s_n^{(*)}$, then it belongs to $\phi(s_n s_{n-1}^* \ldots s_3^* s_1, h) \subset V$.
    - and if it does not contain all the remaining elements, then it belongs to $view(n-1, \{s_1\} \cup X) \subset V$.
  - (iv) Finally, if a does not contain s_1 neither s_2, it belongs to any of the following $view(n-1, \{s_1\} \cup X), view(n-1, \{s_2\} \cup X), view(n-1, \{s_1 s_2^*\} \subset V$.
- If n is odd:
  - (i) If a contains $s_2^* s_1 (= s_1^* s_2)$, then it belongs to $view(n-1, \{s_2^* s_1\} \cup X) \subset V$.
  - (ii) If a does not contain s_1 (or s_1^*),
    - but it contains all the remaining elements, $s_2^{(*)}, \ldots, s_n^{(*)}$, then it belongs to $\phi(s_n^* s_{n-1} \ldots s_3^* s_2, h) \subset V$.
    - and if it does not contain all the remaining elements, then it belongs to $view(n-1, \{s_2\} \cup X) \subset V$.
  - (iii) If a does not contain s_2 (or s_2^*),
    - but it contains all the remaining elements, $s_1^{(*)}, s_3^{(*)}, \ldots, s_n^{(*)}$, then it belongs to $\phi(s_n^* s_{n-1} \ldots s_3^* s_1, h) \subset V$.
    - and if it does not contain all the remaining elements, then it belongs to $view(n-1, \{s_1\} \cup X) \subset V$.
  - (iv) Finally, if a does not contain s_1 neither s_2, it belongs to any of the following $view(n-1, \{s_1\} \cup X), view(n-1, \{s_2\} \cup X), view(n-1, \{s_1 s_2^*\} \subset V$.

The reverse inclusion, $V \subset view(n, \{s_1, s_2\})$ is true since all the elements in V belong to $view(n, \{s_1, s_2\} \cup X)$ by definition. □

In ([3], Section 3) it is first described a decisional problem related to the key agreement protocol for $n = 2$. Let us recall from ([11], Definition 4.7) a formal definition of this decisional problem.

For a given adversary $\mathcal{A}$ we define the following experiment:

- The challenger computes
  - (i) $(\delta_1, \mu_1) \xleftarrow{R} K^{\alpha}C_m \times \Gamma_{\alpha}$;
  - (ii) $(\delta_2, \mu_2) \xleftarrow{R} K^{\alpha}C_m \times \Gamma_{\alpha}$;
  - (iii) $(\delta_3, \mu_3) \xleftarrow{R} K^{\alpha}C_m \times \Gamma_{\alpha}$;
  - (iv) $\text{pub}_1 \leftarrow \delta_1 h \mu_1$; $\text{pub}_2 \leftarrow \delta_2 h \mu_2$;
  - (v) $r_0 \leftarrow \delta_2 \text{pub}_1 \mu_2^*$; $r_1 = \delta_3 h \mu_3$;
    and gives the triple $(\text{pub}_1, \text{pub}_2, k_b)$ to the adversary.
- The adversary outputs a bit $\overline{b} \in \{0, 1\}$.

If W_b is the event that $\mathcal{A}$ outputs 1 in the experiment, we define $\mathcal{A}$'s advantage in solving the Decisional Dihedral Product Problem for $K^{\alpha}D_{2m}$ as

$$\text{DDPadv}[\mathcal{A}, K^{\alpha}D_{2m}] = |\Pr[W_0] - \Pr[W_1]|.$$

We say then that the Decisional Dihedral Product Problem is hard or that the Decisional Dihedral Product Assumption holds for $K^{\alpha}D_{2m}$ if for all efficient adversaries $\mathcal{A}$, the quantity $\text{DDPadv}[\mathcal{A}, K^{\alpha}D_{2m}]$ is negligible.

Let us finally prove, following the idea of [8], that if the Decisional Dihedral Product Assumption holds, then the Group Key Management verifies that an adversary cannot distinguish the shared group key from an arbitrary element. To do so we prove the following:

Theorem 1. *For any $n > 2$, $A_2 \sim D_2$ implies that $A_n \sim D_n$.*

Proof of Theorem 1. We show this is true by induction on n. Assume that $A_2 \sim D_2$ and $A_i \sim D_i$, $i \in \{3, \ldots, n-1\}$. Thus, we have to show that $A_n \sim D_n$. We define the random variables B_n, C_n, and show that $A_n \sim B_n \sim C_n \sim D_n$, and since $\sim$ is a equivalence relation, by transitivity, this implies that $A_n \sim D_n$.

We split the proof in two cases:

(a) Assume n is even:
We redefine A_n, D_n using Lemma 2, and define B_n, C_n as follows:

- $A_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n s_{n-1}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X), \phi(s_n s_{n-1}^* s_{n-2} \ldots s_3^* s_1, h), view(n-1, \{s_2^* s_1\} \cup X), y\Big)$
- $B_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n s_{n-1}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X), \phi(s_n s_{n-1}^* s_{n-2} \ldots s_3^* s_1, h), view(n-1, \{c\} \cup X), y\Big)$
- $C_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n s_{n-1}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X), \phi(s_n s_{n-1}^* s_{n-2} \ldots s_3^* s_1, h), view(n-1, \{c\} \cup X), \phi(s_n^* s_{n-1} \ldots s_4^* s_3 c, h)\Big)$
- $D_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n s_{n-1}^* \ldots s_2, h), view(n-1, \{s_2\} \cup X), \phi(s_n s_{n-1}^* s_{n-2} \ldots s_3^* s_1, h), view(n-1, \{s_2^* s_1\} \cup X), \phi(s_n^* s_{n-1} \ldots s_4^* s_3 s_2^* s_1, h)\Big)$

choosing $s_1, s_2 \in R_1 \times A_2$, $c \in R_1 \times A_1$; and $X \in (R_1 \times A_2)^{n-2}$, $y \in R_1 h A_1$ randomly. Note that only the last two components vary.
$\underline{A_2 \sim D_2 \Longrightarrow A_n \sim B_n}$

Suppose, for the sake of contradiction, that an adversary Eve distinguishes A_n and B_n. We produce an instance of $A_n \not\sim B_n$ for Eve

$$\begin{aligned} A_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{s_2^* s_1\}\cup X), y\Big) \\ &= \Big(\boldsymbol{\delta_1 h \mu_1}, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{\delta_2 h \mu_2}, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{\delta_2 \delta_1 h \mu_1 \mu_2^*}, \dots, \delta_{n-1} \delta_{n-2} \dots \delta_3 (\delta_2 \delta_1) h (\mu_1 \mu_2^*) \mu_3 \dots \mu_{n-2}^* \mu_{n-1}, y\Big) \end{aligned}$$

$$\begin{aligned} B_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), y\Big) \\ &= \Big(\boldsymbol{\delta_1 h \mu_1}, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{\delta_2 h \mu_2}, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{c_1 h c_2}, \dots, \delta_{n-1} \delta_{n-2} \dots \delta_3 (c_1) h (c_2) \mu_3 \dots \mu_{n-2}^* \mu_{n-1}, y\Big) \end{aligned}$$

if Eve distinguishes A_n and B_n, then in particular, she distinguishes $\delta_2 \delta_1 h \mu_1 \mu_2^*$ from $c_1 h c_2$ (given $\delta_1 h \mu_1$ and $\delta_2 h \mu_2$), which means that she distinguishes

$$\begin{aligned} A_2 &= \Big(view(2,\{s_1,s_2\}), y\Big) \\ &= \Big(\delta_1 h \mu_1, \delta_2 h \mu_2, y\Big) \end{aligned}$$

$$\begin{aligned} D_2 &= \Big(view(2,\{s_1,s_2\}), \phi(s_2^* s_1, h)\Big) \\ &= \Big(\delta_1 h \mu_1, \delta_2 h \mu_2, \delta_2 \delta_1 h \mu_1 \mu_2^*\Big) \end{aligned}$$

which contradicts our hypothesis.

$\underline{A_{n-2} \sim D_{n-2} \Longrightarrow B_n \sim C_n}$

Suppose towards the sake of contradiction that an adversary Eve distinguishes B_n and C_n. We produce and instance of $B_n \not\sim C_n$ for Eve

$$\begin{aligned} B_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n^* s_{n-1} \dots s_3^* s_2, h), \\ &\quad view(n-1,\{s_2\}\cup X), \phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), y\Big) \\ &= \Big(\delta_1 h \mu_1, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \delta_2 h \mu_2, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{c_1 h c_2, \dots, \delta_{n-1} \dots \delta_5 \delta_4 (\delta_3 c_1) h (c_2 \mu_3) \mu_4^* \mu_5 \dots \mu_{n-2} \mu_{n-1}^*, y}\Big) \end{aligned}$$

$$\begin{aligned} C_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n^* s_{n-1} \dots s_3^* s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), \phi(s_n s_{n-1}^* \dots s_5 s_4^* s_3 c, h)\Big) \\ &= \Big(\delta_1 h \mu_1, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \delta_2 h \mu_2, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1}^* \mu_n, \\ &\quad \boldsymbol{c_1 h c_2, \dots, \delta_{n-1} \dots \delta_5 \delta_4 (\delta_3 c_1) h (c_2 \mu_3) \mu_4^* \mu_5 \dots \mu_{n-2} \mu_{n-1}^*, \delta_n \dots \delta_4 (\delta_3 c_1) h (c_2 \mu_3) \mu_4^* \mu_5 \dots \mu_n}\Big) \end{aligned}$$

if Eve distinguishes B_n and C_n in polynomial time, in particular, she distinguishes y and $\phi(s_n^* s_{n-1} \dots s_4^* (s_3 c), h)$ (given $view(n-1,\{c\}\cup X)$). Let

$$\Big((view(n-2,\{cs_3, s_4, s_5, \dots, s_{n-1}, s_n\}), y\Big)$$

be an instance of A_{n-2}, D_{n-2}:

$$\begin{aligned} A_{n-2} &= \Big((view(n-2,\{s_3c,s_4,s_5,\ldots,s_{n-1},s_n\}),y\Big) \\ &= \Big((\delta_3c_1)h(c_2\mu_3),\delta_4h\mu_4,\ldots,\delta_nh\mu_n,\delta_4(\delta_3c_1)h(c_2\mu_3)\mu_4^*\ldots,\delta_n(\delta_3c_1)h(c_2\mu_3)\mu_n^*, \\ &\quad \delta_5\delta_4(\delta_3c_1)h(c_2\mu_3)\mu_4^*\mu_5,\ldots,\delta_n\delta_{n-1}\ldots\delta_4\delta_3h\mu_3\mu_4^*\ldots\mu_{n-1}\mu_n,y\Big) \end{aligned}$$

$$\begin{aligned} D_{n-2} &= \Big(view(n-2,\{s_3c,s_4,s_5,\ldots,s_{n-1},s_n\}),\phi(s_n^*s_{n-1}\ldots s_4^*(s_3c),h)\Big) \\ &= \Big((\delta_3c_1)h(c_2\mu_3),\delta_4h\mu_4,\ldots,\delta_nh\mu_n,\delta_4(\delta_3c_1)h(c_2\mu_3)\mu_4^*\ldots,\delta_n(\delta_3c_1)h(c_2\mu_3)\mu_n^*, \\ &\quad \delta_5\delta_4(\delta_3c_1)h(c_2\mu_3)\mu_4^*\mu_5,\ldots,\delta_n\delta_{n-1}\ldots\delta_5\delta_4h\mu_4\mu_5^*\ldots\mu_{n-1}\mu_n,\delta_n\delta_{n-1}\ldots\delta_4(\delta_3c_1) \\ &\quad h(c_2\mu_3)\mu_4^*\ldots\mu_{n-1}\mu_n\Big) \end{aligned}$$

since Eve can distinguish y and $\phi(s_n^*s_{n-1}\ldots s_4^*(s_3c),h)$ given $view(n-1,\{c\}\cup X)$, then in particular she distinguishes y and $\phi(s_n^*s_{n-1}\ldots s_4^*(s_3c),h)$ given $view(n-2,\{s_3c,s_4,s_5,\ldots,s_{n-1},s_n\}) \subset view(n-1,\{c\}\cup X)$, and this means $A_{n-2} \not\sim D_{n-2}$, but this contradicts our hypothesis.

$\underline{A_2 \sim D_2 \Longrightarrow C_n \sim D_n}$

Suppose, for the sake of contradiction, that an adversary Eve distinguishes C_n and D_n. We produce and instance of $C_n \not\sim D_n$ for Eve

$$\begin{aligned} C_n &= \Big(view(n-1,\{s_1\}\cup X),\phi(s_ns_{n-1}^*\ldots s_2,h),view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_ns_{n-1}^*s_{n-2}\ldots s_3^*s_1,h),view(n-1,\{c\}\cup X),\phi(s_n^*s_{n-1}\ldots s_4^*s_3c,h)\Big) \\ &= \Big(\delta_1h\mu_1,\ldots,\delta_n\delta_{n-1}\ldots\delta_4\delta_3h\mu_3\mu_4^*\ldots\mu_{n-1}\mu_n^*,\delta_n\delta_{n-1}\ldots\delta_3\delta_1h\mu_1\mu_3^*\mu_4\ldots\mu_{n-1}^*\mu_n, \\ &\quad \delta_2h\mu_2,\ldots,\delta_{n-1}\ldots\delta_3\delta_2h\mu_2\mu_3^*\ldots\mu_{n-2}^*\mu_{n-1},\delta_n\delta_{n-1}\ldots\delta_3\delta_2h\mu_1\mu_2^*\mu_4\ldots\mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{c_1hc_2},\ldots,\delta_{n-1}\delta_{n-2}\ldots\delta_3c_1hc_2\mu_3\ldots\mu_{n-2}^*\mu_{n-1},\delta_n\delta_{n-1}\ldots\delta_4\delta_3c_1hc_2\mu_3\mu_4^*\ldots\mu_{n-1}\mu_n\Big) \end{aligned}$$

$$\begin{aligned} D_n &= \Big(view(n-1,\{s_1\}\cup X),K(n-1,\{s_1\}\cup X),view(n-1,\{s_2\}\cup X), \\ &\quad K(n-1,\{s_2\}\cup X),view(n-1,\{s_2^*s_1\}\cup X),\phi(s_n^*s_{n-1}\ldots s_4^*s_3s_2^*s_1,h)\Big) \\ &= \Big(\delta_1h\mu_1,\ldots,\delta_n\delta_{n-1}\ldots\delta_4\delta_3h\mu_3\mu_4^*\ldots\mu_{n-1}\mu_n^*,\delta_n\delta_{n-1}\ldots\delta_3\delta_1h\mu_1\mu_3^*\mu_4\ldots\mu_{n-1}^*\mu_n, \\ &\quad \delta_2h\mu_2,\ldots,\delta_{n-1}\ldots\delta_3\delta_2h\mu_2\mu_3^*\ldots\mu_{n-2}^*\mu_{n-1},\delta_n\delta_{n-1}\ldots\delta_3\delta_2h\mu_1\mu_2^*\mu_4\ldots\mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{\delta_2\delta_1h\mu_1\mu_2^*},\ldots,\delta_{n-1}\delta_{n-2}\ldots\delta_3(\delta_2\delta_1)h(\mu_1\mu_2^*)\mu_3\ldots\mu_{n-2}^*\mu_{n-1},\delta_n\delta_{n-1}\ldots\delta_3(\delta_2\delta_1) \\ &\quad h(\mu_1\mu_2^*)\mu_3\ldots\mu_{n-1}\mu_n^*\Big) \end{aligned}$$

as in the first case, if Eve distinguishes A_n and B_n, then in particular, she distinguishes $\delta_2\delta_1h\mu_1\mu_2^*$ from c_1hc_2 (given $\delta_1h\mu_1$ and $\delta_2h\mu_2$), which means that she distinguishes

$$\begin{aligned} A_2 &= \Big(view(2,\{s_1,s_2\}),y\Big) \\ &= \Big(\delta_1h\mu_1,\delta_2h\mu_2,y\Big) \end{aligned}$$

$$\begin{aligned} D_2 &= \Big(view(2,\{s_1,s_2\}),\phi(s_2^*s_1,h)\Big) \\ &= \Big(\delta_1h\mu_1,\delta_2h\mu_2,\delta_2\delta_1h\mu_1\mu_2^*\Big) \end{aligned}$$

which contradicts our hypothesis.

(b) Similarly, if n is odd:
We redefine A_n, D_n using Lemma 2, and define B_n, C_n as follows:

- $A_n = \Big(view(n-1,\{s_1\}\cup X),\phi(s_n^*s_{n-1}\ldots s_3^*s_2,h),view(n-1,\{s_2\}\cup X),$
  $\phi(s_n^*s_{n-1}\ldots s_3^*s_1,h),view(n-1,\{s_2^*s_1\}\cup X),y\Big)$
- $B_n = \Big(view(n-1,\{s_1\}\cup X),\phi(s_n^*s_{n-1}\ldots s_2,h),view(n-1,\{s_2\}\cup X),$

$\phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1, \{c\} \cup X), y\Big)$

- $C_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n^* s_{n-1} \dots s_2, h), view(n-1, \{s_2\} \cup X),$
  $\phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1, \{c\} \cup X), \phi(s_n s_{n-1}^* \dots s_5 s_4^* s_3 c, h)\Big)$
- $D_n = \Big(view(n-1, \{s_1\} \cup X), \phi(s_n^* s_{n-1} \dots s_2, h), view(n-1, \{s_2\} \cup X),$
  $\phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1, \{s_2^* s_1\} \cup X), \phi(s_n s_{n-1}^* \dots s_5 s_4^* s_3 s_2^* s_1, h)\Big)$

choosing $s_1, s_2 \in R_1 \times A_2$, $c \in R_1 \times A_1$; and $X \in (R_1 \times A_2)^{n-2}$, $y \in R_1 h A_2$ randomly.
$\underline{A_2 \sim D_2 \Longrightarrow A_n \sim B_n}$.
Suppose towards the sake of contradiction that an adversary Eve distinguishes A_n and B_n. We produce an instance of $A_n \not\sim B_n$ for Eve

$$\begin{aligned} A_n &= \Big(view(n-1, \{s_1\} \cup X), \phi(s_n^* s_{n-1} \dots s_2, h), view(n-1, \{s_2\} \cup X), \\ &\quad \phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1, \{s_2^* s_1\} \cup X), y\Big) \\ &= \Big(\boldsymbol{\delta_1 h \mu_1}, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1} \mu_n^*, \\ &\quad \boldsymbol{\delta_2 h \mu_2}, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1} \mu_n^*, \\ &\quad \boldsymbol{\delta_2 \delta_1 h \mu_1 \mu_2^*}, \dots, \delta_{n-1} \delta_{n-2} \dots \delta_3 (\delta_2 \delta_1) h (\mu_1 \mu_2^*) \mu_3 \dots \mu_{n-2} \mu_{n-1}^*, y\Big) \end{aligned}$$

$$\begin{aligned} B_n &= \Big(view(n-1, \{s_1\} \cup X), \phi(s_n^* s_{n-1} \dots s_2, h), view(n-1, \{s_2\} \cup X), \\ &\quad \phi(s_n^* s_{n-1} \dots s_3^* s_1, h), view(n-1, \{c\} \cup X), y\Big) \\ &= \Big(\boldsymbol{\delta_1 h \mu_1}, \dots, \delta_n \delta_{n-1} \dots \delta_4 \delta_3 h \mu_3 \mu_4^* \dots \mu_{n-1} \mu_n^*, \delta_n \delta_{n-1} \dots \delta_3 \delta_1 h \mu_1 \mu_3^* \mu_4 \dots \mu_{n-1} \mu_n^*, \\ &\quad \boldsymbol{\delta_2 h \mu_2}, \dots, \delta_{n-1} \dots \delta_3 \delta_2 h \mu_2 \mu_3^* \dots \mu_{n-2}^* \mu_{n-1}, \delta_n \delta_{n-1} \dots \delta_3 \delta_2 h \mu_1 \mu_2^* \mu_4 \dots \mu_{n-1} \mu_n^*, \\ &\quad \boldsymbol{c_1 h c_2}, \dots, \delta_{n-1} \delta_{n-2} \dots \delta_3 (c_1) h (c_2) \mu_3 \dots \mu_{n-2} \mu_{n-1}^*, y\Big) \end{aligned}$$

if Eve distinguishes A_n and B_n, then in particular, she distinguishes $\delta_2 \delta_1 h \mu_1 \mu_2^*$ from $c_1 h c_2$ (given $\delta_1 h \mu_1$ and $\delta_2 h \mu_2$), which means that she distinguishes

$$\begin{aligned} A_2 &= \Big(view(2, \{s_1, s_2\}), y\Big) \\ &= \Big(\delta_1 h \mu_1, \delta_2 h \mu_2, y\Big) \end{aligned}$$

$$\begin{aligned} D_2 &= \Big(view(2, \{s_1, s_2\}), \phi(s_2^* s_1, h)\Big) \\ &= \Big(\delta_1 h \mu_1, \delta_2 h \mu_2, \delta_2 \delta_1 h \mu_1 \mu_2^*\Big) \end{aligned}$$

which contradicts our hypothesis.
$\underline{A_{n-2} \sim D_{n-2} \Longrightarrow B_n \sim C_n}$.

Suppose, for the sake of contradiction, that an adversary Eve distinguishes B_n and C_n. We produce and instance of $B_n \not\sim C_n$ for Eve

$$\begin{aligned} B_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), y\Big) \\ &= \Big(\delta_1 h\mu_1, \dots, \delta_n\delta_{n-1}\dots\delta_4\delta_3 h\mu_3\mu_4^* \dots \mu_{n-1}\mu_n^*, \delta_n\delta_{n-1}\dots\delta_3\delta_1 h\mu_1\mu_3^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \delta_2 h\mu_2, \dots, \delta_{n-1}\dots\delta_3\delta_2 h\mu_2\mu_3^* \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_3\delta_2 h\mu_1\mu_2^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{c_1 h c_2, \dots, \delta_{n-1}\dots\delta_5\delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^*\mu_5\dots\mu_{n-2}^*\mu_{n-1}, y}\Big) \end{aligned}$$

$$\begin{aligned} C_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), \phi(s_n s_{n-1}^* \dots s_4^* s_3 c, h)\Big) \\ &= \Big(\delta_1 h\mu_1, \dots, \delta_n\delta_{n-1}\dots\delta_4\delta_3 h\mu_3\mu_4^* \dots \mu_{n-1}\mu_n^*, \delta_n\delta_{n-1}\dots\delta_3\delta_1 h\mu_1\mu_3^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \delta_2 h\mu_2, \dots, \delta_{n-1}\dots\delta_3\delta_2 h\mu_2\mu_3^* \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_3\delta_2 h\mu_1\mu_2^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{c_1 h c_2, \dots, \delta_{n-1}\dots\delta_5\delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^*\mu_5\dots\mu_{n-2}^*\mu_{n-1}, \delta_n\dots\delta_4(\delta_3 c_1)} \\ &\quad \boldsymbol{h(c_2\mu_3)\mu_4^*\mu_5\dots\mu_n^*}\Big) \end{aligned}$$

if Eve distinguishes B_n and C_n in polynomial time, in particular, she distinguishes y and $\phi(s_n s_{n-1}^* \dots s_5 s_4^*(s_3 c), h)$ (given $view(n-1,\{c\}\cup X)$). Let

$$\Big((view(n-2,\{cs_3, s_4, s_5, \dots, s_{n-1}, s_n\}), y\Big)$$

be an instance of A_{n-2}, D_{n-2}:

$$\begin{aligned} A_{n-2} &= \Big((view(n-2,\{s_3 c, s_4, s_5, \dots, s_{n-1}, s_n\}), y\Big) \\ &= \Big((\delta_3 c_1)h(c_2\mu_3), \delta_4 h\mu_4, \dots, \delta_n h\mu_n, \delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^* \dots, \delta_n(\delta_3 c_1)h(c_2\mu_3)\mu_n^*, \\ &\quad \delta_5\delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^*\mu_5, \dots, \delta_n\delta_{n-1}\dots\delta_4\delta_3 h\mu_3\mu_4^* \dots \mu_{n-1}^*\mu_n, y\Big) \end{aligned}$$

$$\begin{aligned} D_{n-2} &= \Big(view(n-2,\{s_3 c, s_4, s_5, \dots, s_{n-1}, s_n\}), \phi(s_n s_{n-1}^* \dots s_5 s_4^*(s_3 c), h)\Big) \\ &= \Big((\delta_3 c_1)h(c_2\mu_3), \delta_4 h\mu_4, \dots, \delta_n h\mu_n, \delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^* \dots, \delta_n(\delta_3 c_1)h(c_2\mu_3)\mu_n^*, \\ &\quad \delta_5\delta_4(\delta_3 c_1)h(c_2\mu_3)\mu_4^*\mu_5, \dots, \delta_n\delta_{n-1}\dots\delta_5\delta_4 h\mu_4\mu_5^* \dots \mu_{n-1}^*\mu_n, \delta_n\delta_{n-1}\dots\delta_4(\delta_3 c_1) \\ &\quad h(c_2\mu_3)\mu_4^* \dots \mu_{n-1}^*\mu_n\Big) \end{aligned}$$

since Eve can distinguish y and $\phi(s_n s_{n-1}^* \dots s_5 s_4^*(s_3 c), h)$ given $view(n-1,\{c\}\cup X)$, then in particular she distinguishes y and $\phi(s_n^* s_{n-1} \dots s_4^*(s_3 c), h)$ given $view(n-2,\{s_3 c, s_4, s_5, \dots, s_{n-1}, s_n\}) \subset view(n-1,\{c\}\cup X)$, and this means $A_{n-2} \not\sim D_{n-2}$, but this contradicts our hypothesis.

$\underline{A_2 \sim D_2 \Longrightarrow C_n \sim D_n}$.

Suppose towards the sake of contradiction that an adversary Eve distinguishes C_n and D_n. We produce and instance of $C_n \not\sim D_n$ for Eve

$$\begin{aligned} C_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{c\}\cup X), \phi(s_n s_{n-1}^* \dots s_4^* s_3 c, h)\Big) \\ &= \Big(\delta_1 h\mu_1, \dots, \delta_n\delta_{n-1}\dots\delta_4\delta_3 h\mu_3\mu_4^* \dots \mu_{n-1}\mu_n^*, \delta_n\delta_{n-1}\dots\delta_3\delta_1 h\mu_1\mu_3^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \delta_2 h\mu_2, \dots, \delta_{n-1}\dots\delta_3\delta_2 h\mu_2\mu_3^* \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_3\delta_2 h\mu_1\mu_2^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{c_1 h c_2}, \dots, \delta_{n-1}\delta_{n-2}\dots\delta_3 c_1 h c_2\mu_3 \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_4\delta_3 c_1 h c_2\mu_3\mu_4^* \dots \mu_{n-1}\mu_n\Big) \end{aligned}$$

$$\begin{aligned} D_n &= \Big(view(n-1,\{s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_2, h), view(n-1,\{s_2\}\cup X), \\ &\quad \phi(s_n s_{n-1}^* s_{n-2} \dots s_3^* s_1, h), view(n-1,\{s_2^* s_1\}\cup X), \phi(s_n s_{n-1}^* \dots s_4^* s_3 s_2^* s_1, h)\Big) \\ &= \Big(\delta_1 h\mu_1, \dots, \delta_n\delta_{n-1}\dots\delta_4\delta_3 h\mu_3\mu_4^* \dots \mu_{n-1}\mu_n^*, \delta_n\delta_{n-1}\dots\delta_3\delta_1 h\mu_1\mu_3^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \delta_2 h\mu_2, \dots, \delta_{n-1}\dots\delta_3\delta_2 h\mu_2\mu_3^* \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_3\delta_2 h\mu_1\mu_2^*\mu_4 \dots \mu_{n-1}^*\mu_n, \\ &\quad \boldsymbol{\delta_2\delta_1 h\mu_1\mu_2^*}, \dots, \delta_{n-1}\delta_{n-2}\dots\delta_3(\delta_2\delta_1)h(\mu_1\mu_2^*)\mu_3 \dots \mu_{n-2}^*\mu_{n-1}, \delta_n\delta_{n-1}\dots\delta_3(\delta_2\delta_1) \\ &\quad h(\mu_1\mu_2^*)\mu_3 \dots \mu_{n-1}\mu_n^*\Big) \end{aligned}$$

as in the first case, if Eve distinguishes A_n and B_n, then in particular, she distinguishes $\delta_2\delta_1 h\mu_1\mu_2^*$ from $c_1 h c_2$ (given $\delta_1 h\mu_1$ and $\delta_2 h\mu_2$), which means that she distinguishes

$$\begin{aligned} A_2 &= \Big(view(2,\{s_1,s_2\}), y\Big) \\ &= \Big(\delta_1 h\mu_1, \delta_2 h\mu_2, y\Big) \end{aligned}$$

$$\begin{aligned} D_2 &= \Big(view(2,\{s_1,s_2\}), \phi(s_2^* s_1, h)\Big) \\ &= \Big(\delta_1 h\mu_1, \delta_2 h\mu_2, \delta_2\delta_1 h\mu_1\mu_2^*\Big) \end{aligned}$$

which contradicts our hypothesis.

□

So in the Initial Key Agreement the n-users underlying decisional problem is as hard as the 2-users decisional problem. This is also true in the Auxiliary Key Agreement. We can say the protocol provides forward and backward security, i.e. any former or future users cannot distinguish future or past distributed keys, as it is shown in the following result.

Corollary 1. *The AKA provides forward and backward security.*

Proof of Corollary 1. Let Eve be a powerful adversary, that knows all the information of a past user or a future user. She would know a subset of $view(k,\varepsilon)$, where k is the number of current users, and ε the secret keys.

In the first case, when the members of the group stay the same, note that the key update adds a new secret key (and we consider it as a new user). Then we substitute n with $k = n+1$, $\phi(s_n^* s_{n-1} \dots s_4^* s_3 s_2^* s_1, h)$ (or $\phi(s_n s_{n-1}^* \dots s_3 s_2^* s_1, h)$) with $\phi(\widetilde{s_c} s_n^* s_{n-1} \dots s_3 s_2^* s_1, h)$ (resp. $\phi(\widetilde{s_c}^* s_n s_{n-1}^* \dots s_3 s_2^* s_1, h)$) if n is even (if n is odd), and X with $\varepsilon = \{s_1, s_2, \dots, s_{c-1}, s_c, s_{c+1}, \dots, s_{n-1}, s_n, s_c'\}$ in Theorem 1. It follows that

$$A_k = \Big(view(k,\varepsilon), y\Big), \text{ for } y \in R \text{ randomly chosen.}$$

$$D_k = \begin{cases} \Big(view(k,\varepsilon), \phi(\widetilde{s_c} s_n^* s_{n-1} \dots s_3 s_2^* s_1, h)\Big), & \text{if } k \text{ is odd.} \\ \Big(view(k,\varepsilon), \phi(\widetilde{s_c}^* s_n s_{n-1}^* \dots s_3 s_2^* s_1, h))\Big), & \text{if } k \text{ is even.} \end{cases}$$

and it still verifies that if $A_2 \sim D_2$, then $A_k \sim D_k$.

When a user leaves, the key update also adds a new secret key, so we replace n with $k = n+1$ (the user left, but we suppose that Eve had access to the communications before

that happened, and that private key is still part of the common secret key). The rest is the same, so we get again the first case, and the AKA benefits form the same security benefits in this case.

When a new users joins the group, we need to replace $k = n+2$ (the new secret key and the key update), $\phi(s_n^* s_{n-1} \dots s_4^* s_3 s_2^* s_1, h)$ (or $\phi(s_n s_{n-1}^* \dots s_3 s_2^* s_1, h)$) with $\phi(s_{n+1}^* \widetilde{s_c} s_n^* s_{n-1} \dots s_3 s_2^* s_1, h)$ (resp. $\phi(s_{n+1} \widetilde{s_c}^* s_n s_{n-1}^* \dots \ s_3 s_2^* s_1, h)$) if n is even (resp. if n is odd), and X with $\varepsilon = \{s_1, s_2, \dots, s_{n-1}, s_n, s_{n+1}, s_c'\}$ in Theorem 1. It follows that

$$A_k = \Big(view(k, \varepsilon), y\Big), \text{ for } y \in R \text{ randomly chosen.}$$

$$D_k = \begin{cases} \Big(view(k, \varepsilon), \phi(s_{n+1}^* \widetilde{s_c} s_n^* s_{n-1} \dots s_3 s_2^* s_1, h)\Big), \text{ if } k \text{ is even.} \\ \Big(view(k, \varepsilon), \phi(s_{n+1} \widetilde{s_c}^* s_n s_{n-1}^* \dots s_3 s_2^* s_1, h))\Big), \text{ if } k \text{ is odd.} \end{cases}$$

and it still verifies that if $A_2 \sim D_2$, then $A_k \sim D_k$, so the Auxiliary Key Agreement benefits from the same security properties. □

Note that we could also consider D_k as

$$D_k = \begin{cases} \Big(view(k, \varepsilon), \phi(\widetilde{s_c}, K_p))\Big), \text{ if } k \text{ is odd.} \\ \Big(view(k, \varepsilon), \phi(\widetilde{s_c}^*, K_p))\Big), \text{ if } k \text{ is even.} \end{cases}$$

where K_p would be the former key, when the number of users stay the same or someone left, and

$$D_k = \begin{cases} \Big(view(k, \varepsilon), \phi(s_{n+1}^* \widetilde{s_c}, K_p))\Big), \text{ if } k \text{ is even.} \\ \Big(view(k, \varepsilon), \phi(s_{n+1} \widetilde{s_c}^*, K_p))\Big), \text{ if } k \text{ is odd.} \end{cases}$$

when a new user joins the group.

Also note that in the key refresh, we consider $k = n+1$ in the first two cases, but the set of secret keys are $\{s_1, s_2, \dots, s_{c-1}, \widetilde{s_c}^* s_c, s_{c+1}, \dots, s_{n-1}, s_n\}$ when n is odd, and $\{s_1, s_2, \dots, s_{c-1}, \widetilde{s_c} s_c^*, s_{c+1}, \dots, s_n\}$ when n is even, i.e. the number of stored keys stay the same, and the private key of the user U_c is $\widetilde{s_c}^* s_c$ or $\widetilde{s_c} s_c^*$ depending on whether the number of users is even or odd. Finally when $k = n+2$, the set of secret keys has just one new key, from the new user U_{n+1}, so it is $\{s_1, s_2, \dots, s_{c-1}, \widetilde{s_c}^* s_c, s_{c+1}, \dots, s_{n-1}, s_n, s_{n+1}\}$ when n is odd, and $\{s_1, s_2, \dots, s_{c-1}, \widetilde{s_c} s_c^*, s_{c+1}, \dots, s_n, s_{n+1}\}$ whenever n is even.

3. Discussion

In [8], Steiner et al. showed that Diffie–Hellman classical key exchange could be extended to a group of users. Many authors have studied similar Diffie–Hellman protocols until Maze et al. in [2] introduced a protocol in a more general setting as is the case of the action of a commutative semigroup over any set, extending all previous cases, and this was extended to a group of users in [9]. In this paper, we have shown a general result, concerning not only the number of users involved, but also a more general setting, as is the case of a noncommutative ring. The commutativity condition which is fundamental in [9] is substituted by a setting where non-commutativity is somehow controlled by a relation, in this case, given by a cocycle. In Proposition 1 we extend the protocols introduced in [3] and [11] for two users to a finite set of users and for every cocycle. Later, in Theorem 1, we prove that the security of this new protocol does not depend on the number of users, i.e., there is no information leakage even in this case where the amount of public information is noticeably greater.

Author Contributions: Conceptualization, investigation, writing original draft preparation, writing review and editing, supervision, M.D.G.O., J.A.L.R. and B.T.J.; funding acquisition, B.T.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministerio de Economía, Industria y Competitividad grant number MTM2017-86987-P; Junta de Andalucía grant number PY20-00770; and European Union-Junta de Andalucía-Universidad de Almería grant number FEDER- UAL18-FQM-B042-A.

Institutional Review Board Statement: Not aplicable.

Informed Consent Statement: Not aplicable.

Data Availability Statement: Not aplicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DLP	Discrete Logarithm Problem
SAP	Semigroup Action Problem
DP	Decomposition Problem
IKA	Initial Key Agreement
AKA	Auxiliary Key Agreement

References

1. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *6*, 644–654. [CrossRef]
2. Maze, G.; Monico, C.; Rosenthal, J. Public key cryptography based on semigroup actions. *Adv. Math. Commun.* **2007**, *1*, 489–507. [CrossRef]
3. Gómez Olvera, M.D.; López Ramos, J.A.; Torrecillas Jover, B. Public Key Protocols over Twisted Dihedral Group Rings. *Symmetry* **2019**, *11*, 1019. [CrossRef]
4. Eftekhari, M. A Diffie-Hellman key exchange protocol using matrices over group rings. *Groups Complex. Cryptol.* **2012**, *4*, 167–176. [CrossRef]
5. Gupta I.; Pandey A.; Kant Dubey, U. A Key Exchange Protocol using Matrices over Group Rings. *Asian-Eur. J. Math.* **2018**, *5*, 1950075. [CrossRef]
6. Habeeb, M.; Kahrobaei, D.; Koupparis, C.; Shpilrain, V. Public key exchange using semidirect product of (semi)groups. In *A*pplied Cryptography and Network Security; ACNS 2013. Lecture Notes Comp. Sc.; Jacobson, M., Locasto, M. Mohasesel, P., Safavi-Naini, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7954, pp. 475–486.
7. Kahrobaei, D.; Koupparis, C.; Shpilrain, V. Public key exchange using matrices over group rings. *Groups Complex. Cryptol.* **2013**, *5*, 97–115. [CrossRef]
8. Steiner, M.; Tsudik, G.; Waidner, M. Key Agreement in Dynamic Peer Groups. *IEEE Trans. Parallel Distrib. Syst.* **2000**, *11*, 769–780. [CrossRef]
9. López Ramos, J.A.; Rosenthal, J.; Schipani, D.; Schnyder, R. Group key management based on semigroup actions. *J. Algebra Appl.* **2017**, *16*, 1750148. [CrossRef]
10. Rotman, J.J. *An Introduction to the Theory of Groups*; Springer: New York, NY, USA, 1999; 68p.
11. De la Cruz, J.; Villanueva-Polanco, R. Public Key Cryptography based on Twisted Dihedral Group Algebras. *Adv. Math. Commun.* **2021**; doi: 10.3934/amc.2022031. [CrossRef]
12. Lopez-Ramos, J.A.; Rosenthal, J.; Schipani, D.; Schnyder, R. An application of group theory in confidential network communications. *Math. Meth. Apply. Sci.* **2018**, *41*, 2294–2298. [CrossRef]
13. Steiner, M.; Tsudik, G.; Waidner, M. Diffie-Hellman key distribution extended to group communication. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, 14–15 March 1996; ACM: New York, NY, USA, 1996; pp. 31–37.
14. Barak, B. *Computational Indistinguishability, Pseudorandom Generators*; Lecture Notes; Princeton University: Princeton, NJ, USA, 2007.