Scientific Research Publishing

Journal of Computer and Communications, 2016, 4, 63-107
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Cryptographic Protocols Based on Nielsen Transformations

Benjamin Fine[1], Anja I. S. Moldenhauer[2], Gerhard Rosenberger[2]

[1]Department of Mathematics, Fairfield University, Fairfield, CT, USA
[2]Fachbereich Mathematik, Universität Hamburg, Hamburg, Germany
Email: fine@fairfield.edu, anja.moldenhauer@uni-hamburg.de, gerhard.rosenberger@math.uni-hamburg.de

How to cite this paper: Fine, B., Moldenhauer, A.I.S. and Rosenberger, G. (2016) Cryptographic Protocols Based on Nielsen Transformations. *Journal of Computer and Communications*, **4**, 63-107.
http://dx.doi.org/10.4236/jcc.2016.412004

Received: August 14, 2016
Accepted: October 28, 2016
Published: October 31, 2016

Abstract

We introduce in this paper cryptographic protocols which use combinatorial group theory. Based on a combinatorial distribution of shares we present secret sharing schemes and cryptosystems using Nielsen transformations. Nielsen transformations are a linear technique to study free groups and general infinite groups. In addition the group of all automorphisms of a free group F, denoted by $Aut(F)$, is generated by a regular Nielsen transformation between two basis of F, and each regular Nielsen transformation between two bases of F defines an automorphism of F.

Keywords

Nielsen Transformation, Matrix Group $SL(2,\mathbb{Q})$, Secret Sharing Protocol, Private Key Cryptosystem, Public Key Cryptosystem

1. Introduction

This paper is located in the area of group based cryptography. A cryptographic protocol consists of the collection of rules, formulas and methods to handle a cryptographic task. In cryptology it is common to call the parties who want to communicate privately with each other Alice and Bob.

The traditional cryptographic protocols, both symmetric key and public key, such as the RSA algorithm, Diffie-Hellman and elliptic curve methods, are number theory based. Hence, from a theoretical point of view, they depend on the structure of abelian groups. Although there have been no successful attacks on the standard protocols, there is a feeling that the strength of computing machinery has made the techniques less secure. As a result of this, there has been an active line of research to develop and analyse new cryptographic protocols, as for example cryptosystems and key exchange

protocols, based on non-commutative cryptographic platforms. Up to this point the main sources for non-commutative platforms have been nonabelian groups. For an overwiev about mathematical cryptography see [1] and especially for a book about non-commutative group based cryptography see [2].

Important along the line of cryptographic protocols are secret sharing protocols. These consist of methods to distribute a secret among a group of users by giving a share of the secret to each. The secret can be recovered only if a sufficient number of users (but perhaps not all) combine their pieces. There are many different motivations for the secret sharing problem. One of the most important is the problem of maintaining sensitive information. There are two crucial issues here: availability and secrecy. If only one person keeps the entire secret, then there is a risk that the person might lose the secret or the person might not be available when the secret is needed. Hence it is often useful to utilize several people in order to access a secret. On the other hand, the more people who can access the secret, the higher the chance the secret will be leaked. By sharing a secret in a threshold scheme the availability and reliability issues can be addressed. The paper by C. Chum, B. Fine and X. Zhang [3] contains a wealth of information on secret sharing schemes in general and managing an access control group.

This paper is organized as follows. We first describe secret sharing protocols and a combinatorial distributions of shares, which are given by D. Panagopoulos in [4]. After introductory definitions we start with a secret sharing scheme using directly the combinatorial distribution of shares. Based on this we present two schemes in which we apply regular Nielsen transformations in connections with faithful representations of free groups and the Nielsen reduction theory. We also modify the secret sharing schemes to a private key cryptosystem and finally Nielsen transformations are used for a public key cryptosystem which is inspired by the ElGamal cryptosystem. The new cryptographic protocols are in the dissertation of A. Moldenhauer [5] under her supervisor G. Rosenb-erger at the University of Hamburg. Thus, parts of this paper are from [5].

2. Preliminaries for the Newly Developed Cryptographic Protocols

A (n,t)-secret sharing protocol, with $n,t \in \mathbb{N}$ and $t \le n$, is a method to distribute a secret among a group of n participants in such a way that it can be recovered only if at least t of them combine their shares. Hence any group of $t-1$ or fewer participants cannot calculate the secret. The number t is called threshold. The person who distributes the shares is called dealer.

One of the first (n,t)-secret sharing schemes is introduced by A. Shamir in [6]. It has become the standard method for solving the (n,t)-secret sharing problem.

A. Shamir uses polynomial interpolation for his (n,t)-secret sharing scheme. Let $\mathbb{F}$ be any field and let $(x_1,y_1),(x_2,y_2),\cdots,(x_t,y_t)$ be t points in $\mathbb{F}^2$ with pairwise distinct x_i, $1 \le i \le t$. We say a polynomial $g(x)$ over $\mathbb{F}$ interpolates these points if

$g(x_i) = y_i$, $1 \le i \le t$. A. Shamir's secret sharing scheme is based on the following theorem.

Theorem 1. [7]

Let $\mathbb{F}$ be any field and let $x_1, x_2, \cdots, x_t$ be t pairwise distinct elements of $\mathbb{F}$ and let $y_1, y_2, \cdots, y_t$ be any elements of $\mathbb{F}$. Then there exists a unique polynomial of degree less than or equal to $t-1$ that interpolates the t points (x_i, y_i), $1 \le i \le t$.

A. Shamir's (n,t)-secret sharing scheme is roughly this: The dealer chooses a field $\mathbb{F}$. The secret S is an element in $\mathbb{F}$. The dealer picks a polynomial $g(x)$ of degree $t-1$ with the secret S as constant term, that is, $g(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$, $a_i \in \mathbb{F}$ and $a_{t-1} \ne 0$. He chooses pairwise distinct elements $x_1, x_2, \cdots, x_n \in \mathbb{F}$, with $x_i \ne 0$ for all $1 \le i \le n$ and distributes to each of the n participants a point $(x_i, g(x_i))$ as a share. By Theorem 1 any t participants can determine the polynomial $g(x)$ (for example with Lagrange interpolation, see [7]) and hence recover the secret S. If less than t people combine their shares any element in $\mathbb{F}$ can be the constant term and hence the secret. A. Shamir suggested to use $\mathbb{F} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a large prime number.

D. Panagopoulos presents in his paper [4] a (n,t)-secret sharing scheme using group presentations with solvable word problem. For the secret sharing schemes in the following sections we use a combinatorial distribution of the shares, which is explained in the paper of D. Panagopoulos.

Share distribution method explained by D. Panagopoulos.

To distribute the shares in a (n,t)-secret sharing scheme the dealer does the following steps:

1) Calculate $m = \binom{n}{t-1}$, the number of all elements, for example $\{a_1, a_2, \cdots, a_m\}$, the participants need to know for the reconstruction of the secret.

2) Let $A_1, A_2, \cdots, A_m$ be an enumeration of the subsets of $\{1, 2, \cdots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \cdots, R_n$ of the set $\{a_1, a_2, \cdots, a_m\}$ with the property.

$$a_j \in R_i \Leftrightarrow i \notin A_j \quad \text{for } j = 1, 2, \cdots, m \text{ and } i = 1, 2, \cdots, n. \tag{1}$$

3) The dealer distributes to each of the n participants one of the sets $R_1, R_2, \cdots, R_n$.

In addition to this share distribution method the new protocols in this paper are based on combinatorial group theory and Nielsen transformations. Therefore, we review some basic definitions concerning regular Nielsen transformations and Nielsen reduced sets (see [8] or [9]).

Combinatorial group theory is the branch of algebra which studies groups with the help of group presentations. A group presentation for a group G consists of a set X of generators and a set R of defining relators on X. We write.

$$G = \langle X \mid R \rangle.$$

The group G is called finitely generated if both sets X and R are finite. The newly developed cryptographic protocols use finitely generated free groups. Let F be a finitely generated free group with free generating set $X = \{x_1, x_2, \cdots, x_q\}$, $q \in \mathbb{N}$, then the

group F is the set of all reduced words in $X^{\pm 1}$, which is defined as $X^{\pm 1} = \{x_1, x_1^{-1}, x_2, x_2^{-1}, \cdots, x_q, x_q^{-1}\}$, where a word is called reduced if it does not contain subwords of the form $x_j^{-1}x_j$ or $x_j x_j^{-1}$, $1 \le j \le q$. The identity is considered as the empty word, which is 1. The set of relators for a free group consists only of trivial relators, which are of the form $w_j w_j^{-1}$ or $w_j^{-1}w_j$, with w_j a word in X, thus we denote F by

$$F = \langle X \mid \rangle.$$

The empty space on the right symbolized, that there are only trivial relators. For more information about group theory see for instance [8], [9] or [10].

Let F be a finitely generated free group on the free generating set $X = \{x_1, x_2, \cdots, x_q\}$, $q \ge 2$, and let $U = \{u_1, u_2, \cdots, u_t\} \subset F$, $t \ge 2$, with u_i reduced words in X.

Definition 2 *An* ***elementary Nielsen transformation*** *on* $U = \{u_1, u_2, \cdots, u_t\} \subset F$ *is one of the following transformations.*

(T1) replace some u_i by u_i^{-1};

(T2) replace some u_i by $u_i u_j$ where $j \ne i$;

(T3) delete some u_i where $u_i = 1$.

In all three cases the u_k for $k \ne i$ are not changed. A (finite) product of elementary Nielsen transformations is called a **Nielsen transformation**. A Nielsen transformation is called **regular** if it is a finite product of the transformations (T1) and (T2), otherwise it is called **singular**. The set U is called **Nielsen-equivalent** to the set V, if there is a regular Nielsen transformation from U to V.

Nielsen transformations are a linear technique to study free groups and general infinite groups. In addition the group of all automorphisms of a free group F, denoted by $Aut(F)$, is generated by a regular Nielsen transformation between two basis of F, and each regular Nielsen transformation between two basis of F defines an automorphism of F, see ([8], Korollar 2.10).

Definition 3. *A finite set U in F is called* ***Nielsen reduced****, if for any three elements* v_1, v_2, v_3 *from* $U^{\pm 1} = \{u_1, u_1^{-1}, u_2, u_2^{-1}, \cdots, u_t, u_t^{-1}\}$ the following conditions hold:

(N0) $v_1 \ne 1$;

(N1) $v_1 v_2 \ne 1$ implies $|v_1 v_2| \ge |v_1|, |v_2|$;

(N2) $v_1 v_2 \ne 1$ and $v_2 v_3 \ne 1$ implies $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

Here $|v|$ denotes the **free length** of $v \in F$.

Proposition 4. ([8], Theorem 2.3) or ([9], Proposition 2.2)

If $U = \{u_1, u_2, \cdots, u_n\}$ is finite, then U can be carried by a Nielsen transformation into some V such that V is Nielsen reduced.

For the secret sharing schemes based on Nielsen transformations we will only use regular Nielsen transformations. We agree on some notations.

We write $(T1)_i$ if we replace u_i by u_i^{-1} and we write $(T2)_{i.j}$ if we replace u_i by $u_i u_j$. If we want to apply t-times one after the other the same Nielsen transformation $(T2)$ we write $\left[(T2)_{i.j}\right]^t$ and hence replace u_i by $u_i u_j^t$. In all cases the u_k for $i \ne k$ are not changed.

Corollary 5. ([8], Korollar 2.9)

Let F be a free group with basis X and let U be a subset of X which is Nielsen reduced. Then it is

$$X^{\pm 1} \cap \langle U \rangle = X^{\pm 1} \cap U^{\pm 1}. \tag{2}$$

Especially, if U is also a basis for F, then $X^{\pm 1} = U^{\pm 1}$.

Theorem 6. ([8], Satz 2.6)

Let U be Nielsen reduced, then $\langle U \rangle$ is free on U.

For the next lemma we need some notations. Let $w \neq 1$ be a freely reduced word in X. The initial segment s of w which is "a little more than half" of w (that is, $\frac{1}{2}|w| < |s| \leq \frac{1}{2}|w|+1$) is called the **major initial segment** of w. The **minor initial segment** of w is that initial segment s' which is "a little less than half" of w (that is, $\frac{1}{2}|w|-1 \leq |s'| < \frac{1}{2}|w|$). Similarly, **major** and **minor terminal segments** are defined.

If the free length of the word w is even, we call the initial segment s of w, with $|s| = \frac{1}{2}|w|$ the **left half** of w. Analogously, we call the terminal segment s' of w with $|s'| = \frac{1}{2}|w|$ the **right half** of w.

Let $\{w_1, w_2, \cdots, w_m\}$ be a set of freely reduced words in X, which are not the identity. An initial segment of a w-symbol (that is, of either w_i or w_i^{-1}, which are different w-symbols) is called **isolated** if it does not occur as an initial segment of any other w-symbol. Similarly, a terminal segment is isolated if it is a terminal segment of a unique w-symbol.

Lemma 7. ([10], Lemma 3.1)

Let $M = \{w_1, w_2, \cdots, w_m\}$ be a set of freely reduced words in X with $w_j \neq 1$, $1 \leq j \leq m$. Then M is Nielsen reduced if and only if the following conditions are satisfied:

1) Both the major initial and major terminal segments of each $w_i \in M$ are isolated.

2) For each $w_i \in M$ of even free length, either its left half or its right half is isolated.

There are different problems known in combinatorial group Theory, for example:

Theorem 8. ([8], Satz 1.9) Isomorphism problem in free groups:

Let X and Y be two sets. Let $G = \langle X \mid \rangle$ and $H = \langle Y \mid \rangle$ be two free groups on X and Y, respectively. The free group G is isomorphic to the free group H if and only if $|X| = |Y|$.

Problem 9. Word problem:

Let $G = \langle X \mid R \rangle$ be a presentation of a group and $g \in G$ a given word in X. Determine algorithmically (in finitely many steps) if g represents the identity or not.

A further problem, which is a more general problem than the word problem and is needed for some of the developed cryptographic protocols based on combinatorial group theory, is the membership problem or also called extended word problem.

Problem 10. Membership problem:

Given a recursively presented group G, a subgroup H of G generated by $h_1, h_2, \cdots, h_k$

and an element $g \in G$, determine whether or not $g \in H$.

A related problem (to the membership problem) is the constructive membership problem.

Problem 11. Constructive membership problem:

Given a recursively presented group G, a subgroup H of G generated by $h_1, h_2, \cdots, h_k$ and an element $h \in H$, find an expression of h in terms of $h_1, h_2, \cdots, h_k$.

Theorem 12. ([8], Satz 1.9) Isomorphism problem in free groups:

Let X and Y be two sets. Let $G = \langle X \mid \rangle$ and $H = \langle Y \mid \rangle$ be two free groups on X and Y, respectively. The free group G is isomorphic to the free group H if and only if $|X| = |Y|$.

Furthermore, we introduce a linear congruence generator because it is also used for the cryptosystems in this paper.

For $n \in \mathbb{N}$ let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ be the ring of integers modulo n. The corresponding residue class in $\mathbb{Z}_n$ for an integer β is denoted by $\overline{\beta}$ (see also [1]).

Definition 13. [1]

Let $n \in \mathbb{N}$ and $\overline{\beta}, \overline{\gamma} \in \mathbb{Z}_n$. A bijective mapping $h: \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\mathrm{x} \mapsto \overline{\beta}\mathrm{x} + \overline{\gamma}$ is called a linear congruence generator.

Theorem 14. [1] (Maximal period length for $n = 2^m$, $m \in \mathbb{N}$)

Let $n \in \mathbb{N}$, with $n = 2^m$, $m \geq 1$ and let $\beta, \gamma \in \mathbb{Z}$ such that $h: \mathbb{Z}_n \to \mathbb{Z}_n$, with $\mathrm{x} \mapsto \overline{\beta}\mathrm{x} + \overline{\gamma}$, is a linear congruence generator. Further let $\alpha \in \{0,1,\cdots,n-1\}$ be given and $\mathrm{x}_1 = \overline{\alpha}$, $\mathrm{x}_2 = h(\mathrm{x}_1)$, $\mathrm{x}_3 = h(\mathrm{x}_2)$, $\cdots$.

Then the sequence $\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \cdots$ is periodic with maximal periodic length $n = 2^m$ if and only if the following holds:

1) β is odd, consequently $\overline{\beta} \neq \overline{0}$.

2) If $m \geq 2$ then $\beta \equiv 1 (\mathrm{mod}\, 4)$.

3) γ is odd, consequently $\overline{\gamma} \neq \overline{0}$.

3. A Combinatorial Secret Sharing Scheme

Now we present a (n,t)-secret sharing scheme, whereby the secret is the sum of the multiplicative inverse of elements in the natural numbers. For the distribution of the shares the dealer uses the method by D. Panagopoulos described in Section 2.

The numbers n and t are given, whereby n is the number of participants and t is the threshold.

1) The dealer first calculates the number $m = \binom{n}{t-1}$.

2) He chooses m elements $a_1, a_2, \cdots, a_m \in \mathbb{N}$. From these elements he constructs analogously as in Section 0 the sets $R_1, R_2, \cdots, R_n$. The secret S is the sum

$$S := \sum_{i=1}^{m} \frac{1}{a_i} \in \mathbb{Q}^+. \tag{3}$$

3) Each participant p_i gets one share R_i, $1 \leq i \leq n$.

If t of the n participants come together they can reconstruct the secret while they first combine their t private sets R_i and get by construction the set $\tilde{R} = \{a_1, a_2, \cdots, a_m\}$.

The secret is the sum of the inverse elements in the set $\tilde{R}$, that is

$$S = \sum_{i=1}^{m} \frac{1}{a_i}. \tag{4}$$

This cryptographic protocol is summarized in **Table 1**.

If the dealer needs a special secret $\tilde{S} \in \mathbb{Q}$ he gives every participant one more element $x \in \mathbb{Q}$ in each R_i, with

$$x := \frac{\tilde{S}}{S}. \tag{5}$$

The participants get $\tilde{S}$ by multiplying the reconstructed secret S with x.

Security 15. *Each element a_j is exactly contained in $n-(t-1)$ subsets. Hence for each $j=1,2,\cdots,m$ the element a_j is not contained in $t-1$ subsets from $\{R_1, R_2, \cdots, R_n\}$. As a consequence, a_j is in each union of t subsets. Otherwise, if just $t-1$ arbitrary sets from $\{R_1, R_2, \cdots, R_n\}$ are combined, there exist a j such that the element a_j is not included in the union of this sets.*

Table 1. Summary of the combinatorial (n,t)-secret sharing scheme.

(n,t)-secret sharing scheme	
Dealer	Participants $p_1, p_2, \cdots, p_n$
Calculate $m = \binom{n}{t-1}$.	
Choose $a_1, a_2, \cdots, a_m \in \mathbb{N}$.	
Construct sets $R_j \subseteq \{a_1, a_2, \cdots, a_m\}$ with share distribution method given by D. Panagopoulos; it is $\lvert R_j \rvert = \binom{n-1}{t-1}$ for $j=1,2,\cdots,n$.	
Distribute shares to the participants.	$\xrightarrow{R_1} p_1$ $\xrightarrow{R_2} p_2$ $\vdots$ $\xrightarrow{R_n} p_n$
	t participants combine their shares and thus get the set $\{a_1, a_2, \cdots, a_m\}$. The secret is $S = \sum_{i=1}^{m} \frac{1}{a_i}$.

If just one element a_j is absent, the participants do not get the correct sum *S*, and hence cannot compute the correct secret.

Remark 16. We realize that the share distribution method by D. Panagopoulos is also given as a special case by M. Ito, A. Saito and T. Nishizeki in [11]. In [5] it is shown that if the method in [11] is used to generate a (n,t)-secret sharing scheme then the same share distribution method as by D. Panagopoulos is described. M. Ito, A. Saito and T. Nishizeki use a multiple assignment scheme, which is a method to distribute to each participant more than only one share, together with a (m,m)-secret sharing scheme. Thus, the share distribution method by D. Panagopoulos is a special case of paper [11].

In addition, in [5] it is shown in detail, that the purely combinatorial secret sharing scheme is very similar to a scheme, which J. Benaloh and J. Leichter obtain if they realize a (n,t)-secret sharing scheme using minimal CNF-formula, described in their paper [12].

Remark 17. It is important in terms of practicability, that the dealer calculates and distributes the shares for the participants long before the secret is needed by the participants. Hence, the dealer has enough time to execute the share distribution method and his computational cost should be of no consequence for the cryptographic protocol. If t participants reconstruct the secret, they add up only m elements, which is feasible in linear time.

Example 18. *We perform the steps for a* $(4,3)$*-secret sharing scheme. It is* $n=4$ *and* $t=3$.

The dealer follows the steps:

1) He first calculates $m=\binom{n}{t-1}=\binom{4}{2}=6$.

2) The dealer chooses the numbers $a_1:=2, a_2:=1, a_3:=2, a_4:=8$, $a_5:=4$ and $a_6:=2$. The secret is

$$S:=\sum_{i=1}^{m}\frac{1}{a_i}=\frac{23}{8}.$$

(a) The six subsets with size 2 of the set $\{1,2,3,4\}$ are

$$A_1=\{1,2\},\quad A_2=\{1,3\},\quad A_3=\{1,4\},$$

$$A_4=\{2,3\},\quad A_5=\{2,4\},\quad A_6=\{3,4\}.$$

With help of the A_i the dealer gets the sets R_1,R_2,R_3 and R_4, which contain elements from $\{a_1,\cdots,a_6\}$. He puts the element a_j for which *i* is not contained in the set A_j for $i=1,\cdots,4$ and $j=1,\cdots,6$, into the set R_i, thus it is:

$$1\notin A_4,A_5,A_6\Rightarrow R_1=\{a_4,a_5,a_6\},$$

$$2\notin A_2,A_3,A_6\Rightarrow R_2=\{a_2,a_3,a_6\},$$

$$3\notin A_1,A_3,A_5\Rightarrow R_3=\{a_1,a_3,a_5\},$$

$$4\notin A_1,A_2,A_4\Rightarrow R_4=\{a_1,a_2,a_4\}.$$

3) The dealer distributes the set R_i to the participant p_i, for $i=1,\cdots,4$.

If three of the four participants come together, they can calculate the secret S. For example the participants p_1, p_2 and p_3 hold the set

$$\begin{aligned}\tilde{R} &:= R_1 \cup R_2 \cup R_3 \\ &= \{a_4, a_5, a_6\} \cup \{a_2, a_3, a_6\} \cup \{a_1, a_3, a_5\} \\ &= \{a_1, a_2, a_3, a_4, a_5, a_6\},\end{aligned}$$

and hence get the secret

$$S = \sum_{i=1}^{6} \frac{1}{a_i} = \frac{23}{8} \quad \text{with } a_i \in \tilde{R}.$$

4. A Secret Sharing Scheme Using a Regular Nielsen Transformation

In this section we describe a (n,t)-secret sharing scheme extends the ideas in Section 3 by using Nielsen transformations. We consider free groups as abstract groups but also as subgroups of the special linear group of all 2×2 matrices over $\mathbb{Q}$, that is,

$$\mathrm{SL}(2,\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Q} \text{ and } ad-bc=1 \right\}.$$

We use the special linear group over the rational numbers because these numbers can be stored and computed more efficiently on a computer than irrational numbers.

Let F be a free group in $\mathrm{SL}(2,\mathbb{Q})$ of rank $m := \binom{n}{t-1}$. The dealer wants to distribute the shares for the participants as described in Section 2. The shares will be subsets of a free generating set of the group F (in an abstract and an explicit version).

The numbers n and t are given, whereby n is the number of participants and t is the threshold. The dealer does the following steps:

1) He chooses an abstract free generating set X for the free group F of rank $m := \binom{n}{t-1}$, that is

$$F = \langle X \mid \rangle \quad \text{with } X := \{x_1, x_2, \cdots, x_m\}. \tag{6}$$

He also needs an explicit free generating set M, that is

$$F = \langle M \mid \rangle \quad \text{with } M := \{M_1, M_2, \cdots, M_m\} \tag{7}$$

and $M_i \in \mathrm{SL}(2,\mathbb{Q})$.

2) With the known matrices in the set M he computes the secret

$$S := \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \quad \text{with } a_j := tr(M_j) \in \mathbb{Q}, \tag{8}$$

$tr(M_j)$ is the trace for the matrix $M_i := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Q})$, that is, $tr(M_i) := a+d$.

If the dealer needs a special secret he can act as in Section 3 described.

3) The dealer constructs the shares for the participants in the following way:

(a) He first applies a regular Nielsen transformation simultaneously for both sets X and M to get Nielsen-equivalent sets U and N to X and M, respectively (see **Figure 1**).

The elements u_i are words in X and the elements N_i are words in M. Hence, it is $N_i \in \mathrm{SL}(2,\mathbb{Q})$.

(b) The dealer now uses the method of D. Panagopoulos to split U and N and to get the shares (R_i, S_j) for the participants with $R_i \subset U$ and $S_j \subset N$.

4) The dealer distributes the shares.

If t of the n participants combine their parts they obtain the sets U and N. The secret can be recovered as follows:

1. The participants apply regular Nielsen transformations in a Nielsen reduction manner for U and step by step simultaneously for N. By Proposition 4 they get Nielsen reduced sets $X' = \left\{x_1^{\epsilon_1}, x_2^{\epsilon_2}, \cdots, x_m^{\epsilon_m}\right\}$ and $M' = \left\{M_1^{\delta_1}, M_2^{\delta_2}, \cdots, M_m^{\delta_m}\right\}$ with $\epsilon_i, \delta_i \in \{+1, -1\}$, see **Figure 2**.

Because of Corollary 5 it is $X^{\pm 1} = X'^{\pm 1}$ and $M^{\pm 1} = M'^{\pm 1}$, respectively. Hence, $(x_1', x_2', \cdots, x_m')$ differs to $(x_1, x_2, \cdots, x_m)$ just in the position order and inverses. That means the set X' is the set X up to inverses. The same is true for M' and M. Thus, it is $X' = \left\{x_1^{\epsilon_1}, x_2^{\epsilon_2}, \cdots, x_m^{\epsilon_m}\right\}$ and also $M' = \left\{M_1^{\delta_1}, M_2^{\delta_2}, \cdots, M_m^{\delta_m}\right\}$ with $\epsilon_i, \delta_i \in \{1, -1\}$.

The cryptographic protocol is summarized in **Table 2** (page 73).

Less than t participants can neither get the whole set U, which is Nielsen-equivalent to X, nor the set N, which is Nielsen-equivalent to M.

For the calculation of the secret, the participants need the set M, because the secret depends on the traces of the matrices $M_i \in M$. The participants need both sets U and N. If they just have one set U or N they cannot get information about the set M.

If the set U is known, it is only known which Nielsen transformation should be done to get the Nielsen-equivalent set X, but it is unknown on which matrices they should be done simultaneously.

If only the set N is known, then the matrices in $\mathrm{SL}(2,\mathbb{Q})$ are known, but nobody knows which Nielsen transformation should be done on N to get the set M. It is also unknown how many Nielsen transformations were used.

In the book ([13], page 247) of J. Lehner a method is given to explicitly obtain a free

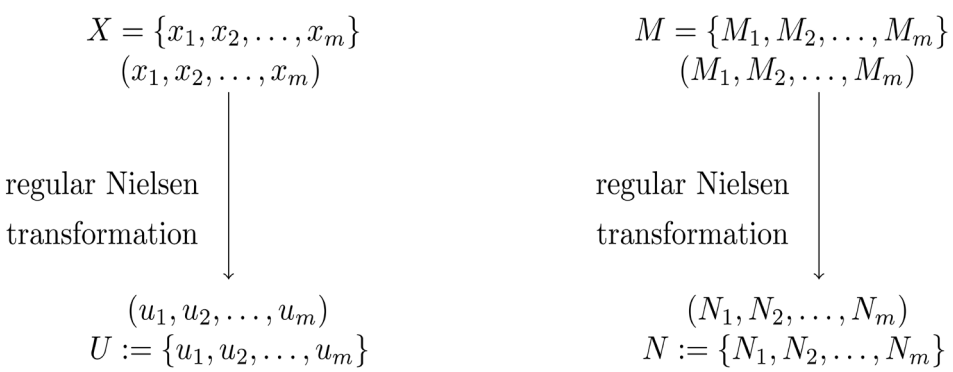

Figure 1. Simultaneously regular Nielsen transformations for the dealer.

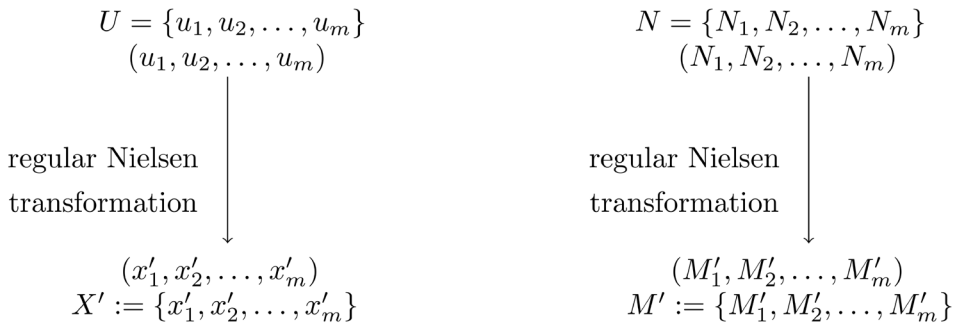

Figure 2. Simultaneously regular Nielsen transformations for the participants.

Table 2. Summary of the secret sharing scheme using Nielsen transformations and $\mathrm{SL}(2,\mathbb{Q})$.

(n,t) -secret sharing scheme	
Dealer	Participants $p_1, p_2, \cdots, p_n$
Calculate $m = \binom{n}{t-1}$.	
Choose abstract free generating set $X := \{x_1, x_2, \cdots, x_m\}$ and explicit free generating set $M := \{M_1, M_2, \cdots, M_m\}$ with $M_i \in \mathrm{SL}(2,\mathbb{Q})$ (all or almost all $M_i \notin \mathrm{SL}(2,\mathbb{Z})$).	
Apply simultaneously regular Nielsen transformation (NT) on X and M: $(x_1, x_2, \cdots, x_m)$ $(M_1, M_2, \cdots, M_m)$ ↓ NT ↓ NT $(u_1, u_2, \cdots, u_m)$ $(N_1, N_2, \cdots, N_m)$ $U := \{u_1, u_2, \cdots, u_m\}$; $N := \{N_1, N_2, \cdots, N_m\}$.	
Construct sets $R_j \subseteq U$ and $S_j \subseteq N$ with share distribution method given by D. Panagopoulos; it is $\lvert R_j\rvert = \lvert S_j\rvert = \binom{n-1}{t-1}$ for $j = 1, 2, \cdots, n$.	
Distribute shares to the participants.	$\xrightarrow{(R_1, S_1)} p_1$ $\xrightarrow{(R_2, S_2)} p_2$ ⋮ $\xrightarrow{(R_n, S_n)} p_n$
	t participants combine their shares and thus get the sets U and N. Apply simultaneously regular Nielsen transformation (NT) on U and N: $(u_1, u_2, \cdots, u_m)$ $(N_1, N_2, \cdots, N_m)$ ↓ NT ↓ NT $(x'_1, x'_2, \cdots, x'_m)$ $(M'_1, M'_2, \cdots, M'_m)$ The secret is $S := \sum_{j=1}^{m} \frac{1}{\lvert a'_j\rvert} \in \mathbb{Q}^+$ with $a'_j := tr(M'_j) \in \mathbb{Q}$.

generating set M for a free group F on the abstract generating set $X := \{x_1, x_2, \cdots, x_m\}$:

Theorem 19. [13] Let F be a free group with countably many free generators $x_1, x_2, \cdots$. Corresponding to x_j define the matrix

$$M_j = \begin{pmatrix} -r_j & -1+r_j^2 \\ 1 & -r_j \end{pmatrix} \tag{9}$$

with $r_j \in \mathbb{Q}$ such that the following inequalities hold:

$$r_{j+1} - r_j \geq 3 \quad \text{and} \quad r_1 \geq 2. \tag{10}$$

The group G generated by $\{M_1, M_2, \cdots\}$ is isomorphic to F.

We now present an example for this secret sharing scheme.

Example 20. *We perform the steps for a* $(3,2)$ *-secret sharing scheme with the help of the computer program Maple* 16. *It is* $n=3$, $t=2$ *and hence* $m = \binom{3}{1} = 3$.

First the Dealer generates the shares for the participants.

1) The dealer chooses an abstract presentation for the free group F of rank 3

$$F = \langle X \mid \rangle \quad \text{with } X := \{x_1, x_2, x_3\}.$$

He takes an explicit presentation

$$F = \langle M \mid \rangle \quad \text{with } M := \{M_1, M_2, M_3\},$$

$M_i \in \mathrm{SL}(2, \mathbb{Q})$ as above. We first mention that the inequalities (10) hold for

$$r_1 = \frac{7}{2}, \quad r_2 = \frac{15}{2}, \quad r_3 = 11$$

and hence the set of the matrices

$$M_1 = \begin{pmatrix} -\frac{7}{2} & -1+\left(\frac{7}{2}\right)^2 \\ 1 & -\frac{7}{2} \end{pmatrix} = \begin{pmatrix} -\frac{7}{2} & \frac{45}{4} \\ 1 & -\frac{7}{2} \end{pmatrix},$$

$$M_2 = \begin{pmatrix} -\frac{15}{2} & -1+\left(\frac{15}{2}\right)^2 \\ 1 & -\frac{15}{2} \end{pmatrix} = \begin{pmatrix} -\frac{15}{2} & \frac{221}{4} \\ 1 & -\frac{15}{2} \end{pmatrix},$$

$$M_3 = \begin{pmatrix} -11 & -1+11^2 \\ 1 & -11 \end{pmatrix} = \begin{pmatrix} -11 & 120 \\ 1 & -11 \end{pmatrix}$$

is a free generating set for a free group of rank 3.

2) The dealer chooses

$$a_1 := tr(M_1) = -7, \quad a_2 := tr(M_2) = -15, \quad a_3 := tr(M_3) = -22,$$

and hence the secret is

$$S := \sum_{j=1}^{3} \frac{1}{|a_j|} = \frac{589}{2310}.$$

3) Construction of the shares for the participants:

(a) First the dealer applies regular Nielsen transformations (NTs) simultaneously for both sets X and M to get Nielsen-equivalent sets U and N to X and M, respectively. These transformations are shown in Table 3 (see page 75) and Table 4 (see page 76).

The Dealer obtains the sets

$$U=\{u_1,u_2,u_3\}:=\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3},x_2^{-1}x_3x_2^{-3},x_2^3x_3^{-1}x_2^{-1}x_3x_2^{-3}\right\}$$

and

$$N=\{N_1,N_2,N_3\}$$
$$:=\left\{\begin{pmatrix}-\frac{3452369}{4} & -\frac{25661603}{4}\\ \frac{237917}{2} & \frac{1768447}{2}\end{pmatrix},\begin{pmatrix}\frac{80371}{4} & \frac{597401}{4}\\ \frac{5145}{2} & \frac{38243}{2}\end{pmatrix},\begin{pmatrix}\frac{1132425929}{4} & \frac{8417369243}{4}\\ -\frac{152350279}{4} & -\frac{1132425989}{4}\end{pmatrix}\right\}.$$

(b) He gets the shares $\left(R_i,S_j\right)$ for the participants with $R_i\subset U$ and $S_j\subset N$ as follows:

Table 3. Nielsen transformations (NTs) of the dealer I.

NTs	theoretical set X	explicit set M
	$\{x_1,x_2,x_3\}$	$\left\{\begin{pmatrix}-\frac{7}{2} & \frac{45}{4}\\ 1 & -\frac{7}{2}\end{pmatrix},\begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix},\begin{pmatrix}-11 & 120\\ 1 & -11\end{pmatrix}\right\}$
$(T1)_2$	$\{x_1,x_2^{-1},x_3\}$	$\left\{\begin{pmatrix}-\frac{7}{2} & \frac{45}{4}\\ 1 & -\frac{7}{2}\end{pmatrix},\begin{pmatrix}-\frac{15}{2} & -\frac{221}{4}\\ -1 & -\frac{15}{2}\end{pmatrix},\begin{pmatrix}-11 & 120\\ 1 & -11\end{pmatrix}\right\}$
$(T2)_{1.2}$	$\{x_1x_2^{-1},x_2^{-1},x_3\}$	$\left\{\begin{pmatrix}15 & 109\\ -4 & -29\end{pmatrix},\begin{pmatrix}-\frac{15}{2} & -\frac{221}{4}\\ -1 & -\frac{15}{2}\end{pmatrix},\begin{pmatrix}-11 & 120\\ 1 & -11\end{pmatrix}\right\}$
$\left[(T2)_{3.2}\right]^3$	$\{x_1x_2^{-1},x_2^{-1},x_3x_2^{-3}\}$	$\left\{\begin{pmatrix}15 & 109\\ -4 & -29\end{pmatrix},\begin{pmatrix}-\frac{15}{2} & -\frac{221}{4}\\ -1 & -\frac{15}{2}\end{pmatrix},\begin{pmatrix}-8565 & -63664\\ 799 & 5939\end{pmatrix}\right\},$
$(T2)_{2.3}$	$\{x_1x_2^{-1},x_2^{-1}x_3x_2^{-3},x_3x_2^{-3}\}$	$\left\{\begin{pmatrix}15 & 109\\ -4 & -29\end{pmatrix},\begin{pmatrix}\frac{80371}{4} & \frac{597401}{4}\\ \frac{5145}{2} & \frac{38243}{2}\end{pmatrix},\begin{pmatrix}-8565 & -63664\\ 799 & 5939\end{pmatrix}\right\}$
$(T1)_1$	$\{x_2x_1^{-1},x_2^{-1}x_3x_2^{-3},x_3x_2^{-3}\}$	$\left\{\begin{pmatrix}-29 & -109\\ 4 & 15\end{pmatrix},\begin{pmatrix}\frac{80371}{4} & \frac{597401}{4}\\ \frac{5145}{2} & \frac{38243}{2}\end{pmatrix},\begin{pmatrix}-8565 & -63664\\ 799 & 5939\end{pmatrix}\right\},$
$(T2)_{1.2}$	$\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3},x_2^{-1}x_3x_2^{-3},x_3x_2^{-3}\}$	$\left\{\begin{pmatrix}-\frac{3452369}{4} & -\frac{25661603}{4}\\ \frac{237917}{2} & \frac{1768447}{2}\end{pmatrix},\begin{pmatrix}\frac{80371}{4} & \frac{597401}{4}\\ \frac{5145}{2} & \frac{38243}{2}\end{pmatrix},\begin{pmatrix}-8565 & -63664\\ 799 & 5939\end{pmatrix}\right\},$

Table 4. Nielsen transformations (NTs) of the dealer II.

NTs	theoretical set X	explicit set M
$(T1)_3$	$\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{80371}{4} & \frac{597401}{4} \\ \frac{5145}{2} & \frac{38243}{2} \end{pmatrix}, \begin{pmatrix} 5939 & 63664 \\ -799 & -8565 \end{pmatrix}\right\}$,
$(T2)_{3,2}$	$\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}x_2^{-1}x_3x_2^{-3}\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{80371}{4} & \frac{597401}{4} \\ \frac{5145}{2} & \frac{38243}{2} \end{pmatrix}, \begin{pmatrix} \frac{1132425929}{4} & \frac{8417369243}{4} \\ -\frac{152350279}{4} & -\frac{1132425989}{4} \end{pmatrix}\right\}$

i) It is $m = \binom{n}{t-1} = \binom{3}{1} = 3$.

ii) The dealer chooses the elements $\tilde{a}_1, \tilde{a}_2, \tilde{a}_3$ and gets the three sets

$$4A_1 = \{1\}, \quad A_2 = \{2\}, \quad A_3 = \{3\}.$$

With the help of the A_i the dealer gets the sets R_1', R_2' and R_3' which contain elements from the set $\{\tilde{a}_1, \tilde{a}_2, \tilde{a}_3\}$. He puts the element $\tilde{a}_j$ by which i is not contained in the set A_j for $i = 1,2,3$ and $j = 1,2,3$, into the set R_i'.

$$1 \notin A_2, A_3 \Rightarrow R_1' = \{\tilde{a}_2, \tilde{a}_3\},$$

$$2 \notin A_1, A_3 \Rightarrow R_2' = \{\tilde{a}_1, \tilde{a}_3\},$$

$$3 \notin A_1, A_2 \Rightarrow R_3' = \{\tilde{a}_1, \tilde{a}_2\}.$$

Now we apply this to U and N to create the share-sets for the participants, respectively:

$$R_1 = \{u_2, u_3\}, \quad S_1 = \{N_2, N_3\},$$

$$R_2 = \{u_1, u_3\}, \quad S_2 = \{N_1, N_3\},$$

$$R_3 = \{u_1, u_2\}, \quad S_2 = \{N_1, N_2\},$$

4) The Dealer distributes to each participant a tuple (R_i, S_j). Participant p_1 gets (R_1, S_2), p_2 gets (R_2, S_3) and p_3 gets (R_3, S_1).

Assume the participants p_1 and p_2 come together to reconstruct the secret. They are able to generate the sets $U = \{u_1, u_2, u_3\}$ and $N = \{N_1, N_2, N_3\}$. The secret can be recovered as follows.

The participants apply regular Nielsen transformations step by step simultaneously for both sets U and N to get X' and M'. The steps are shown in the Table 5 (see page 77) and Table 6 (see page 78).

With the knowledge of the set $M' = \left\{\begin{pmatrix} -\frac{7}{2} & \frac{45}{4} \\ 1 & -\frac{7}{2} \end{pmatrix}, \begin{pmatrix} -\frac{15}{2} & \frac{221}{4} \\ 1 & -\frac{15}{2} \end{pmatrix}, \begin{pmatrix} -11 & 120 \\ 1 & -11 \end{pmatrix}\right\}$ the participants can reconstruct the secret easily. It is

Table 5. Nielsen transformations (NTs) from the participants I.

NTs	theoretical set U	explicit set N
	$\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}x_2^{-1}x_3x_2^{-3}\right\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{80371}{4} & \frac{597401}{4} \\ \frac{5145}{2} & \frac{38243}{2} \end{pmatrix}, \begin{pmatrix} \frac{1132425929}{4} & \frac{8417369243}{4} \\ -\frac{152350279}{4} & -\frac{1132425989}{4} \end{pmatrix}\right\}$
$(T1)_2$	$\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}x_2, x_2^3x_3^{-1}x_2^{-1}x_3x_2^{-3}\right\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{38243}{2} & -\frac{597401}{4} \\ -\frac{5145}{2} & \frac{80371}{4} \end{pmatrix}, \begin{pmatrix} \frac{1132425929}{4} & \frac{8417369243}{4} \\ -\frac{152350279}{4} & -\frac{1132425989}{4} \end{pmatrix}\right\}$
$(T2)_{3.2}$	$\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}x_2, x_2^3x_3^{-1}\right\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{38243}{2} & -\frac{597401}{4} \\ -\frac{5145}{2} & \frac{80371}{4} \end{pmatrix}, \begin{pmatrix} 5939 & 63664 \\ -799 & -8565 \end{pmatrix}\right\}$
$(T1)_2$	$\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^{-1}x_3x_2^{-3}, x_2^3x_3^{-1}\right\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} \frac{80371}{4} & \frac{597401}{4} \\ \frac{5145}{2} & \frac{38243}{2} \end{pmatrix}, \begin{pmatrix} 5939 & 63664 \\ -799 & -8565 \end{pmatrix}\right\}$
$(T2)_{2.3}$	$\left\{x_2x_1^{-1}x_2^{-1}x_3x_2^{-3}, x_2^{-1}, x_2^3x_3^{-1}\right\}$	$\left\{\begin{pmatrix} -\frac{3452369}{4} & -\frac{25661603}{4} \\ \frac{237917}{2} & \frac{1768447}{2} \end{pmatrix}, \begin{pmatrix} -\frac{15}{2} & -\frac{221}{4} \\ -1 & -\frac{15}{2} \end{pmatrix}, \begin{pmatrix} 5939 & 63664 \\ -799 & -8565 \end{pmatrix}\right\}$
$(T2)_{1.3}$	$\left\{x_2x_1^{-1}x_2^{-1}, x_2^{-1}, x_2^3x_3^{-1}\right\}$	$\left\{\begin{pmatrix} \frac{653}{2} & \frac{9679}{4} \\ -45 & -\frac{667}{2} \end{pmatrix}, \begin{pmatrix} -\frac{15}{2} & -\frac{221}{4} \\ -1 & -\frac{15}{2} \end{pmatrix}, \begin{pmatrix} 5939 & 63664 \\ -799 & -8565 \end{pmatrix}\right\}$

$$a_1 := tr(M_1) = -7, \quad a_2 := tr(M_2) = -15, \quad a_3 := tr(M_3) = -22$$

and hence it is

$$S := \sum_{j=1}^{3} \frac{1}{|a_j|} = \frac{1}{7} + \frac{1}{15} + \frac{1}{22} = \frac{589}{2310}.$$

In general we can use any free matrix group F of rank $m := \binom{n}{t-1}$ for a (n,t)-secret sharing scheme as it is described in this section. The shares can be generated by the above method and are tuples (R_i, S_j) with $R_i \subset U$ and $S_j \subset N$. Some other ideas for the secret S are

$$S := \prod_{i=1}^{m} |tr(M_i)| \text{ or } S := \sum_{i=1}^{m} |tr(M_i)| \text{ or} \tag{11}$$

$$S := \prod_{i=1}^{m} (tr(M_i))^2 \text{ or } S := \sum_{i=1}^{m} (tr(M_i))^2 \text{ or} \tag{12}$$

$$S := \prod_{i=1}^{\frac{m}{2}} tr(M_{2i-1}, M_{2i}) \text{ if } m \text{ is even or } S := \sum_{i=1}^{m} tr(M_i^2). \tag{13}$$

Table 6. Nielsen transformations (NTs) from the participants II.

NTs	theoretical set U	explicit set N
$(T1)_2$	$\{x_2x_1^{-1}x_2^{-1}, x_2, x_2^3x_3^{-1}\}$	$\left\{\begin{pmatrix}\frac{653}{2} & \frac{9679}{4}\\ -45 & -\frac{667}{2}\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}5939 & 63664\\ -799 & -8565\end{pmatrix}\right\}$
$(T2)_{1.2}$	$\{x_2x_1^{-1}, x_2, x_2^3x_3^{-1}\}$	$\left\{\begin{pmatrix}-29 & -109\\ 4 & 15\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}5939 & 63664\\ -799 & -8565\end{pmatrix}\right\}$
$(T1)_1$	$\{x_1x_2^{-1}, x_2, x_2^3x_3^{-1}\}$	$\left\{\begin{pmatrix}15 & 109\\ -4 & -29\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}5939 & 63664\\ -799 & -8565\end{pmatrix}\right\}$
$(T2)_{1.2}$	$\{x_1, x_2, x_2^3x_3^{-1}\}$	$\left\{\begin{pmatrix}-\frac{7}{2} & \frac{45}{4}\\ 1 & -\frac{7}{2}\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}5939 & 63664\\ -799 & -8565\end{pmatrix}\right\}$
$(T1)_3$	$\{x_1, x_2, x_3x_2^{-3}\}$	$\left\{\begin{pmatrix}-\frac{7}{2} & \frac{45}{4}\\ 1 & -\frac{7}{2}\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}-8565 & -63664\\ 799 & 5939\end{pmatrix}\right\}$
$\left[(T2)_{3.2}\right]^3$	$\{x_1, x_2, x_3\}$	$\left\{\begin{pmatrix}-\frac{7}{2} & \frac{45}{4}\\ 1 & -\frac{7}{2}\end{pmatrix}, \begin{pmatrix}-\frac{15}{2} & \frac{221}{4}\\ 1 & -\frac{15}{2}\end{pmatrix}, \begin{pmatrix}-11 & 120\\ 1 & -11\end{pmatrix}\right\}$

5. Another Secret Sharing Scheme Based on Nielsen Transformations

We explain another secret sharing scheme which arises of the protocol in Section 4. As in the previous section, let F be a finitely generated free group with the abstract free generating set $X := \{x_1, x_2, \cdots, x_q\}$, $q \in \mathbb{N} \setminus \{1\}$, that is,

$$F = \langle X \mid \ \rangle.$$

For a (n,t)-secret sharing scheme the dealer chooses a Nielsen reduced set $U = \{u_1, u_2, \cdots, u_m\} \subset F$, with $m = \binom{n}{t-1}$. The u_i are given as words in X. The secret is the sum

$$S := \sum_{i=1}^{m} \frac{1}{|u_i|}, \tag{14}$$

with $|u_i|$ the length of the word u_i.

The dealer does a regular Nielsen transformation on the set U to get the Nielsen-equivalent set V (see Figure 3).

Each participant p_i, $1 \le i \le n$, gets one set $R_i \subset V$, as in the previous secret sharing scheme above.

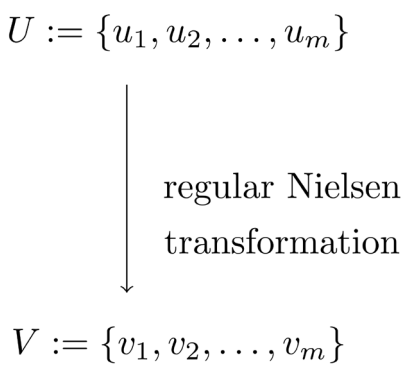

Figure 3. Regular Nielsen transformation.

If t of the n participants come together to reconstruct the secret, they combine their shares and get the set $V = \{v_1, v_2, \cdots, v_m\}$. They have to find a Nielsen-reduced set $U' := \{u_1', u_2', \cdots, u_m'\}$ to V. They apply Nielsen transformations in a Nielsen reducing manner as described in [8] and [9], and get from V a Nielsen-reduced set U'. The secret is the sum

$$S = \sum_{i=1}^{m} \frac{1}{|u_i'|}, \quad \text{with } u_i' \in U' \tag{15}$$

because for each i it is $|u_i'|_X = |u_j|_X$ for some j (see the proof of Corollary 3.1 in [10]). From U' we get U by permutations and length preserving Nielsen transformations.

This (n,t)-secret sharing scheme is summarized in **Table 7** (page 80).

6. A Symmetric Key Cryptosystem Using Nielsen Transformations

In this section we introduce a symmetric key cryptosystem using Nielsen transformations. Before Alice and Bob are able to communicate with each other, they have to make some arrangements.

We speak about public parameters also in private key cryptosystems, because these are parameters which each person, also an eavesdropper, Eve, gets, if she looks at the sent ciphertext. Public parameters are also elements, which Alice and Bob communicate with each other publicly. It is also not a secret which plaintext alphabet is used for the communication.

Public Parameters.

They first agree on the following public parameters.

1) A finitely generated free group F with free generating set $X = \{x_1, x_2, \cdots, x_q\}$ with $q \geq 2$.

2) A plaintext alphabet $A = \{a_1, a_2, \cdots, a_N\}$ with $N \geq 2$.

3) An abstract free group $H = \langle U | \ \rangle$ with $rank(H) = |A| = N$ and an abstract free generating set $U = \{u_1, u_2, \cdots, u_N\}$, with u_i, $1 \leq i \leq N$, abstract letters.

4) A subset $\mathcal{H}_{Aut} := \{f_0, f_1, \cdots, f_{2^{128}-1}\} \subset Aut(H)$ of automorphisms of H. It is $f_i : H \to H$ and the f_i, $i = 0,1,\cdots,2^{128}-1$, pairwise different, are generated with the help of 0-1-sequence (of different length) and random numbers, see ([5], Section 4.4).

Table 7. Summary of the (n,t)-secret sharing scheme using Nielsen transformations together with Nielsen reduced sets and free lengths of certain words.

(n,t)-secret sharing scheme	
Dealer	Participants $p_1, p_2, \cdots, p_n$
Calculate $m = \binom{n}{t-1}$. Choose abstract free generating set $X = \{x_1, x_2, \cdots, x_q\}$ with $q \in \mathbb{N} \setminus \{1\}$ and a Nielsen reduced set $U = \{u_1, u_2, \cdots, u_m\} \subset F$, u_i words in X. Apply regular Nielsen transformation (NT) on U: $(u_1, u_2, \cdots, u_m)$ $\downarrow$ NT $(v_1, v_2, \cdots, v_m)$ $V := \{v_1, v_2, \cdots, v_m\}$. Construct sets $R_j \subseteq V$ with share distribution method given by D. Panagopoulos; it is $\lvert R_j \rvert = \binom{n-1}{t-1}$ for $j = 1, 2, \cdots, n$. Distribute shares to the participants.	$\xrightarrow{R_1} p_1$ $\xrightarrow{R_2} p_2$ $\vdots$ $\xrightarrow{R_n} p_n$
	t participants combine their shares and thus get the set V. Apply regular Nielsen transformation (NT) on V: $(v_1, v_2, \cdots, v_m)$ $\downarrow$ NT $(u_1', u_2', \cdots, u_m')$ The secret is $S = \sum_{i=1}^{m} \frac{1}{\lvert u_i' \rvert_X}$.

The set $\mathcal{H}_{Aut}$ is part of the key space.

5) They agree on a linear congruence generator $h : \mathbb{Z}_{2^{128}} \to \mathbb{Z}_{2^{128}}$ with a maximal period length.

Private Parameters.

Now, they agree on the private parameters.

1) Alice and Bob choose an explicit Nielsen reduced set U with N elements, which are words in X. Such systems U are easily to construct (see Lemma 7 and Theorem 6 or also [8] and [9]).

Now, it is $F_U = \langle U \mid \rangle$ a free subgroup of F with rank N. It is $\mathcal{U}_{Nred}$ the set of all minimal Nielsen reduced sets with N elements in F, which is part of the key space.

2) They use a one-to-one correspondence

$$\begin{aligned} &A \to U \\ &a_j \mapsto u_j \quad \text{for } j = 1, \cdots, N. \end{aligned} \tag{16}$$

3) Alice and Bob agree on an automorphism $f_{\bar{\alpha}} \in \mathcal{H}_{Aut}$, hence α is the common secret starting point $\alpha \in \{0,1,\cdots,2^{128}-1\}$, with $\mathrm{u}_1 = \bar{\alpha} \in \mathbb{Z}_{2^{128}}$, for the linear congruence generator. With this α they are able to generate the sequence $f_{\mathrm{u}_1}, f_{\mathrm{u}_2}, \cdots, f_{\mathrm{u}_z}$ (with z the number of the plaintext units, which are letters from A) of automorphisms of the set $\mathcal{H}_{Aut}$, which they need for encryption and decryption, respectively.

Remark 21. *If the explicit set* $U \coloneqq \{u_1, u_2, \cdots, u_N\}$, u_i *word in X, is used, then* F_U *is a free subgroup of F and with the automorphism* $f_{\mathrm{u}_j} \in \mathcal{H}_{Aut}$ *with* $f_{\mathrm{u}_j} : F_U \to F_U$, *the set* $U_{f_{\mathrm{u}_j}} = \{f_{\mathrm{u}_j}(u_1), f_{\mathrm{u}_j}(u_2), \cdots, f_{\mathrm{u}_j}(u_N)\}$ *is generated, which is Nielsen equivalent to the set U.*

The key space: The set $\mathcal{U}_{Nred}$ of all minimal (with respect to a lexicographical order) Nielsen reduced set of F with N elements. The set $\mathcal{H}_{Aut}$ of 2^{128} randomly chosen automorphism of F_U.

Private Key Cryptosystem.

Now, we explain the private key cryptosystem and look carefully at the steps for Alice and Bob.

Public knowledge: $F = \langle X \mid \rangle$, $X = \{x_1, x_2, \cdots, x_q\}$ with $q \geq 2$; plaintext alphabet $A = \{a_1, a_2, \cdots, a_N\}$ with $N \geq 2$; the set $\mathcal{H}_{Aut}$; a linear congruence generator *h*.

Encryption and Decryption Procedure:

1) Alice and Bob agree privately on the private parameters: a set $U \in \mathcal{U}_{Nred}$ and an automorphism $f_{\bar{\alpha}} \in \mathcal{H}_{Aut}$. They also know the one-to-one correspondence between U and A.

2) Alice wants to transmit the message

$$S = s_1 s_2 \cdots s_z, \quad z \geq 1, \tag{17}$$

with $s_i \in A$ to Bob.

2.1) She generates with the linear congruence generator h and the knowledge of $f_{\bar{\alpha}}$ the z automorphisms $f_{\mathrm{u}_1}, f_{\mathrm{u}_2}, \cdots, f_{\mathrm{u}_z}$, which she needs for encryption. It is $\mathrm{u}_1 = \bar{\alpha}$, $\mathrm{u}_2 = h(\mathrm{u}_1)$, $\cdots$, $\mathrm{u}_z = h(\mathrm{u}_{z-1})$.

2.2) The encryption is as follows.

$$\text{if } s_i = a_t \text{ then } s_i \mapsto c_i \coloneqq f_{\mathrm{u}_i}(u_t), \ 1 \leq i \leq z, 1 \leq t \leq N. \tag{18}$$

Recall that the one-to-one correspondence $A \to U$ with $a_j \mapsto u_j$, for $j = 1, 2, \cdots, N$, holds. The ciphertext

$$\begin{aligned} C &= f_{\mathrm{u}_1}(s_1) f_{\mathrm{u}_2}(s_2) \cdots f_{\mathrm{u}_z}(s_z) \quad \text{with } s_i \mathrel{\hat{=}} u_t \Leftrightarrow s_i = a_t \\ &= c_1 c_2 \cdots c_z \end{aligned} \tag{19}$$

is sent to Bob. The c_j are called the ciphertext units and we do not perform cancellations between c_i and c_{i+1} and the end of each c_i is marked, $1 \leq i \leq z-1$, for example with the symbol "$\wr$". On the one hand the ciphertext unit c_j can be seen as a

word in U, because the set $U_{f_{u_j}} = \left\{ f_{u_j}(u_1), f_{u_j}(u_2), \cdots, f_{u_j}(u_N) \right\}$ is Nielsen equivalent to U and $f_{u_j}(s_j) \hat{=} f_{u_j}(u_k) =: c_j$, for $s_j = a_k$, is an element in $U_{f_{u_j}}$. On the other hand it can be written as a word in X, because the explicit elements in U are words in X and so are the elements in the Nielsen equivalent set $U_{f_{u_j}}$ to U.

3) Bob gets the ciphertext

$$C = c_1 c_2 \cdots c_z, \tag{20}$$

with c_j, $1 \le j \le z$, words in X. He knows where each ciphertext unit c_j begins and ends. Hence, he gets the information that he has to use z automorphisms of F from the set $\mathcal{H}_{Aut}$ for decryption. He has two possibilities for decryption.

3.1.a) With the knowledge of $f_{\bar{\alpha}}$, the set $U = \{u_1, u_2, \cdots, u_N\}$, the linear congruence generator h and the number z, he computes for each automorphism f_{u_i}, $i = 1, 2, \cdots, z$, the set

$$U_{f_{u_i}} = \left\{ f_{u_i}(u_1), f_{u_i}(u_2), \cdots, f_{u_i}(u_N) \right\}, \tag{21}$$

with $f_{u_i}(u_j)$ written as a reduced word in X. Hence, with the one-to-one correspondence between U and A, he gets a one-to-one correspondence between the letters in the alphabet A and the words of the ciphertext depending on the automorphisms f_{u_i}. This is shown in **Table 8** (page 82).

With the knowledge of the **Table 8** (page 82) the decryption is as follows

$$\text{if } c_i = f_{u_i}(u_t) \quad \text{then } c_i \mapsto s_i = a_t, \quad 1 \le i \le z, \quad 1 \le t \le N. \tag{22}$$

He generates the plaintext message

$$S = s_1 s_2 \cdots s_z, \tag{23}$$

with $s_i \in A$, from Alice.

3.1.b) Bob knows the Nielsen reduced set U, hence with an algorithm as for example explained in the book ([8], page~33) he is able to write the elements c_i as words in U. With the knowledge of the automorphism $f_{\bar{\alpha}}$, the set $U = \{u_1, u_2, \cdots, u_N\}$, the linear congruence generator h and the number z, he gets the automorphisms f_{u_i} which Alice used for encryption of c_i. Because of the fact that a one-to-one correspondence between A and U is used and the ciphertext unit c_i is an image of an element in U under the automorphism f_{u_i}, Bob knows with the automorphism f_{u_i} and the ciphertext unit c_i written as word in U, the plaintext letter $a_j \in A$ which corresponds to the ciphertext unit c_i.

This cryptographic protocol is summarized in **Table 9** (page 83).

Table 8. Plaintext alphabet $A = \{a_1, a_2, \cdots, a_N\}$ corresponding to ciphertext alphabet $U_{f_{u_i}}$ depending on the automorphisms f_{u_i}.

	$U_{f_{u_1}}$	$U_{f_{u_2}}$	…	$U_{f_{u_z}}$
a_1	$f_{u_1}(u_1)$	$f_{u_2}(u_1)$	…	$f_{u_z}(u_1)$
a_2	$f_{u_1}(u_2)$	$f_{u_2}(u_2)$	…	$f_{u_z}(u_2)$
⋮	⋮	⋮	…	⋮
a_N	$f_{u_1}(u_N)$	$f_{u_2}(u_N)$	…	$f_{u_z}(u_N)$

Remark 22. As soon as Alice and Bob agree on the starting seed automorphism and the Nielsen reduced set U, Bob is able to calculate the first columns of Table 8 (page 82) for decryption (he does not know how many columns he will need because he does not know yet how long the plaintext from Alice will be). If he gets the ciphertext C from Alice, he only has to do a search in the table to get the corresponding plaintext units to

Table 9. Summary of the private key cryptosystem.

Public Knowledge

$F = \langle X \mid \rangle$, $X = \{x_1, x_2, \cdots, x_q\}$, $q \geq 2$; plaintext alphabet $A = \{a_1, a_2, \cdots, a_N\}$, $N \geq 2$;
abstract free group $H = \langle U \rangle$, $U = \{u_1, u_2, \cdots, u_N\}$ with u_i abstract letters;
set $\mathcal{H}_{Aut} \subset Aut(H)$; linear congruence generator h of maximal periodic length.

Alice | **Bob**

Private keys

Explicit set $U = \{u_1, u_2, \cdots, u_N\}$ with u_i words in X, $U \subset F$ Nielsen reduced set,
$|U| = N$; seed $f_{\bar{\alpha}} \in \mathcal{F}_{Aut}$, one-to-one correspondence $A \to U$, $a_j \mapsto u_j$.

Encryption

Choose message

$$S = s_1 s_2 \cdots s_z, \quad z \geq 1,$$

with $s_i \in A$.

Calculate

$u_1 = \bar{\alpha}, u_2 = h(u_1), \cdots, u_z = h(u_{z-1})$, obtain

$f_{u_1}, f_{u_2}, \cdots, f_{u_z}$.

Encryption procedure:

if $s_i = a_t$ then $s_i \mapsto c_i := f_{u_i}(u_t)$, $1 \leq i \leq z$

$1 \leq t \leq N$.

Ciphertext:

$C = f_{u_1}(s_1) f_{u_2}(s_2) \cdots f_{u_z}(s_z) = c_1 c_2 \cdots c_z$,

with c_i written as words in X.

$\xrightarrow{C = c_1 c_2 \cdots c_z}$

Decryption

Compute z automorphism:

$u_1 = \bar{\alpha}, u_2 = h(u_1), \cdots, u_z = h(u_{z-1})$, obtain

$f_{u_1}, f_{u_2}, \cdots, f_{u_z}$.

Two possibilities:

1. For each f_{u_i}, $i = 1, 2, \cdots, z$ compute

$U_{f_{u_i}} = \{f_{u_i}(u_1), f_{u_i}(u_2), \cdots, f_{u_i}(u_N)\}$

and get a table like Table 8 (page 82). (Decryption: Search in this table.)

if $c_i = f_{u_i}(u_t)$ then $c_i \mapsto s_i = a_t$, $1 \leq i \leq z$

$1 \leq t \leq N$.

2. Use Nielsen reduced set U and an algorithm to write the ciphertext units c_i (given as words in X) as words in U. Together with the used automorphism, the ciphertext is decrypted correctly.

Reconstruct plaintext message

$S = s_1 s_2 \cdots s_z$, with $s_i \in A$.

the ciphertext units. If columns are missing to decrypt the ciphertext, he calculates the missing columns. Thus, in Version 3.1.a. instead of Version 3.1.b. for decryption Bob is able to do calculations for decryption even before he knows the ciphertext.

Remark 23. The cryptosystem is a polyalphabetic system, that means, a word $u_i \in U$, and hence a letter $a_i \in A$, is encrypted differently at different positions in the plaintext, because different automorphisms are used during the encryption procedure for each ciphertext unit. Thus, for the ciphertext, a statistical frequency attack (see for instance [1]) over the frequency of words, which correspond to letters in the plaintext alphabet, or groups of words, is useless.

It follows an example, in which for decryption a table (see **Table 8** (page 82)) is used, which stores the ciphertext alphabet $U_{f_{u_i}}$ and is generated with the automorphisms Alice uses for encryption, see Example 24.

Additionally, in [5] an example is given, in which Bob knows the Nielsen reduced set U, hence with a known algorithm he is able to write the ciphertext as a sequence of words in U. With the automorphisms Alice uses for encryption he is able to decrypt the ciphertext correctly.

Example 24. This example was executed in GAP[1]. All details are given in Appendix A. Firstly, Alice and Bob agree on **public parameters**.

1) Let F be the free group on the free generating set $X = \{x, y, z\}$.

2) Let $\tilde{A} = \{a_1, a_2, \cdots, a_8\} = \{\mathsf{L}, \mathsf{E}, \mathsf{I}, \mathsf{O}, \mathsf{U}, \mathsf{A}, \mathsf{V}, \mathsf{B}\}$ be the plaintext alphabet.

3) Let H be the abstract free group of rank $|\tilde{A}| = 8$ with free generating set $U = \{u_1, u_2, \cdots, u_8\}$.

4) A set $\mathcal{H}_{Aut} \subset Aut(H)$ is determined. In this example we give the automorphisms, which Alice and Bob use for encryption and decryption, respectively, just at the moment when they are needed.

5) The linear congruence generator with maximal periodic length is

$$h : \mathbb{Z}_{2^{128}} \to \mathbb{Z}_{2^{128}}$$

$$\mathrm{u} \mapsto \overline{133}\mathrm{u} + \overline{51}.$$

The **private parameters** for this example are the following:

1) Let F_U be the explicit finitely generated free group, which is generated with the free generating set $U = \{u_1, u_2, \cdots, u_8\}$ with words in X, for this example it is

$$u_1 := xyz, \quad u_2 := yzy^{-1}, \quad u_3 := x^{-1}zx^{-1}, \quad u_4 := y^{-1}x^2,$$

$$u_5 := z^{-1}xyx, \quad u_6 := z^{-1}yx^{-1}, \quad u_7 := x^3y, \quad u_8 := y^3z^{-2}.$$

The starting automorphism f_{u_1} is $f_{\overline{23442}}$, hence it is $\mathrm{u}_1 = \bar{\alpha} = \overline{23442}$. It is known, that $a_i \mapsto u_i$, $i = 1, 2, \cdots, 12$, for $u_i \in U$ and $a_i \in \tilde{A}$, therefore.

$$\mathsf{L} \hat{=} u_1 = xyz, \quad \mathsf{E} \hat{=} u_2 = yzy^{-1}, \quad \mathsf{I} \hat{=} u_3 = x^{-1}zx^{-1}, \quad \mathsf{O} \hat{=} u_4 = y^{-1}x^2,$$

$$\mathsf{U} \hat{=} u_5 = z^{-1}xyx, \quad \mathsf{A} \hat{=} u_6 = z^{-1}yx^{-1}, \quad \mathsf{V} \hat{=} u_7 = x^3y, \quad \mathsf{B} \hat{=} u_8 = y^3z^{-2}.$$

[1]Groups, Algorithms and Programming [14].

We now look at the encryption and decryption procedure for Alice and Bob.

2) With the above agreements **Alice** is able to encrypt her message

$$S = \mathrm{LOVE}.$$

Her message is of length 4. She generates the ciphertext as follows:

2.1) First, she determines, with the help of the linear congruence generator $h:\mathbb{Z}_{2^{128}} \to \mathbb{Z}_{2^{128}}$ with $\mathrm{u} \mapsto \overline{133}\mathrm{u} + \overline{51}$ and the starting seed $\bar{\alpha} = \overline{23442}$, the four automorphisms $f_{\mathrm{u}_i} \in \mathcal{H}_{Aut}$, $1 \le i \le 4$, which she needs for encryption. It is

$$\mathrm{u}_1 = \bar{\alpha} = \overline{23442}, \mathrm{u}_2 = h(\mathrm{u}_1) = \overline{3117837},$$

$$\mathrm{u}_3 = h(\mathrm{u}_2) = \overline{414672372} \quad \text{and} \quad \mathrm{u}_4 = h(\mathrm{u}_3) = \overline{55151425527}.$$

The automorphisms are describable with the help of regular Nielsen transformations, it is

$$f_{\mathrm{u}_1} \hat{=} (N2)_{1.7}(N2)_{2.4}(N1)_5(N2)_{7.8}\left[(N2)_{3.4}\right]^2(N2)_{4.6}(N2)_{5.1}(N1)_7 (N2)_{6.3}(N2)_{8.1}(N2)_{7.4}(N1)_7(N2)_{1.2}(N2)_{2.3}(N2)_{4.5},$$

$$f_{\mathrm{u}_1}: H \to H$$

$$u_1 \mapsto u_1u_7u_2u_4, \quad u_5 \mapsto u_5^{-1}u_1u_7,$$

$$u_2 \mapsto u_2u_4u_3u_4^2, \quad u_6 \mapsto u_6u_3u_4^2,$$

$$u_3 \mapsto u_3u_4^2, \quad u_7 \mapsto u_6^{-1}u_4^{-1}u_7u_8,$$

$$u_4 \mapsto u_4u_6u_5^{-1}u_1u_7, \quad u_8 \mapsto u_8u_1u_7.$$

$$f_{\mathrm{u}_2} \hat{=} (N2)_{1.3}(N2)_{3.5}(N1)_2(N1)_4(N2)_{6.5}(N1)_1\left[(N2)_{3.4}\right]^2(N2)_{5.2}(N2)_{7.6} (N2)_{4.2}(N2)_{2.8}(N2)_{8.4}(N1)_4(N2)_{1.4}(N2)_{2.6}(N2)_{5.6}(N2)_{6.4}(N2)_{4.7},$$

$$f_{\mathrm{u}_2}: H \to H$$

$$u_1 \mapsto u_3^{-1}u_1^{-1}u_2u_4, \quad u_5 \mapsto u_5u_2^{-1}u_6u_5,$$

$$u_2 \mapsto u_2^{-1}u_8u_6u_5, \quad u_6 \mapsto u_6u_5u_2u_4,$$

$$u_3 \mapsto u_3u_5u_4^{-2}, \quad u_7 \mapsto u_7u_6u_5,$$

$$u_4 \mapsto u_2u_4u_7u_6u_5, \quad u_8 \mapsto u_8u_4^{-1}u_2^{-1}.$$

$$f_{\mathrm{u}_3} \hat{=} (N1)_2(N1)_5(N1)_8(N2)_{6.3}(N2)_{3.7}(N2)_{1.2}\left[(N2)_{4.8}\right]^2(N2)_{5.6}(N2)_{8.3} (N2)_{6.3}(N1)_8(N2)_{2.3}(N2)_{7.4}(N2)_{1.8}(N2)_{3.4},$$

$$f_{\mathrm{u}_3}: H \to H$$

$$u_1 \mapsto u_1u_2^{-1}u_7^{-1}u_3^{-1}u_8, \quad u_5 \mapsto u_5^{-1}u_6u_3,$$

$$u_2 \mapsto u_2^{-1}u_3u_7, \quad u_6 \mapsto u_6u_3^2u_7,$$

$$u_3 \mapsto u_3u_7u_4u_8^{-2}, \quad u_7 \mapsto u_7u_4u_8^{-2},$$

$$u_4 \mapsto u_4u_8^{-2}, \quad u_8 \mapsto u_7^{-1}u_3^{-1}u_8.$$

$$f_{u_4} \hat{=} (N1)_1 (N1)_3 (N1)_4 (N2)_{6.2} \left[(N2)_{8.2}\right]^3 (N2)_{2.3} (N2)_{3.4} (N2)_{5.2} (N2)_{7.4} (N2)_{1.3} (N2)_{4.5} (N2)_{8.3} (N1)_1 (N1)_2 (N2)_{7.2} (N1)_3 (N2)_{2.3} (N2)_{3.5} (N2)_{6.1},$$

$$f_{u_4} : H \to H$$

$$u_1 \mapsto u_4 u_3 u_1, \quad u_5 \mapsto u_5 u_2 u_3^{-1},$$

$$u_2 \mapsto u_3 u_2^{-1} u_4 u_3, \quad u_6 \mapsto u_6 u_2 u_4 u_3 u_1,$$

$$u_3 \mapsto u_4 u_3 u_5 u_2 u_3^{-1}, \quad u_7 \mapsto u_7 u_4^{-1} u_3 u_2^{-1},$$

$$u_4 \mapsto u_4^{-1} u_5 u_2 u_3^{-1}, \quad u_8 \mapsto u_8 u_2^3 u_3^{-1} u_4^{-1}.$$

the Nielsen transformations are applied from the left to the right.

2.2) Secondly, she encrypts her message. The ciphertext is

$$\begin{aligned} C &= f_{u_1}(\mathsf{L})\, f_{u_2}(\mathsf{O})\, f_{u_3}(\mathsf{V})\, f_{u_4}(\mathsf{E}) \\ &= f_{u_1}(u_1)\, f_{u_2}(u_4)\, f_{u_3}(u_7)\, f_{u_4}(u_2) \\ &= u_1 u_7 u_2 u_4 \wr u_2 u_4 u_7 u_6 u_5 \wr u_7 u_4 u_8^{-2} \wr u_3 u_2^{-1} u_4 u_3 \end{aligned}$$

The ciphertext C is written as words in X, it is

$$\begin{aligned} C &= u_1 u_7 u_2 u_4 \wr u_2 u_4 u_7 u_6 u_5 \wr u_7 u_4 u_8^{-2} \wr u_3 u_2^{-1} u_4 u_3 \\ &= xyzx^3 y^2 z y^{-2} x^2 \wr yzy^{-2} x^5 y z^{-1} y x^{-1} z^{-1} x y x \wr x^5 \left(z^2 y^{-3}\right)^2 \wr x^{-1} z x^{-1} y z^{-1} y^{-2} x z x^{-1} \end{aligned}$$

3) Bob gets the ciphertext

$$C = xyzx^3 y^2 z y^{-2} x^2 \wr yzy^{-2} x^5 y z^{-1} y x^{-1} z^{-1} x y x \wr x^5 \left(z^2 y^{-3}\right)^2 \wr x^{-1} z x^{-1} y z^{-1} y^{-2} x z x^{-1}$$

from Alice. Thus, he knows that he needs 4 automorphisms for decryption.

3.1) Bob knows the set U, the linear congruence generator h and the starting seed automorphism $f_{\overline{23442}}$. For decryption he uses tables like Table 8 (page 82).

Now, he is able to compute for each automorphism f_{u_i} the set $U_{f_{u_i}}$, $1 \le i \le 4$, and to generate Table 10 (page 86) and Table 11 (page 87).

With these tables he is able to reconstruct the plaintext from Alice. He searches for the plaintext element s_i the ciphertext unit c_i in the column $U_{f_{u_i}}$, $1 \le i \le 4$, and hence gets the alphabet letter $a_j = s_i$ for a $j \in \{1, 2, \cdots, 8\}$. Therefore, he decrypts the ciphertext to the message.

Table 10. Correspondence: Plaintext alphabet to ciphertext alphabet I.

	$U_{f_{u_1}}$	$U_{f_{u_2}}$
L	$xyzx^3 y^2 z y^{-2} x^2$	$\left(xz^{-1}\right)^2 y^{-1} x^{-1} y z y^{-2} x^2$
E	$yzy^{-2} x z x^{-1} \left(y^{-1} x^2\right)^2$	$yz^{-1} y^2 z^{-3} y x^{-1} z^{-1} x y x$
I	$x^{-1} z x^{-1} \left(y^{-1} x^2\right)^2$	$x^{-1} z x^{-1} z^{-1} x \left(y x^{-1}\right)^2 x^{-1} y$
O	$y^{-1} x^2 z^{-1} y x^{-2} y^{-1} x^{-1} z x y z x^3 y$	$yzy^{-2} x^5 y z^{-1} y x^{-1} z^{-1} x y x$
U	$x^{-1} y^{-1} x^{-1} z x y z x^3 y$	$z^{-1} \left(xy\right)^2 z^{-1} y^{-1} z^{-1} y x^{-1} z^{-1} x y x$
A	$z^{-1} y x^{-2} z x^{-1} \left(y^{-1} x^2\right)^2$	$z^{-1} y x^{-1} z^{-1} \left(xy\right)^2 z y^{-2} x^2$
V	$xy^{-1} z x^{-2} y x^3 y^4 z^{-2}$	$x^3 y z^{-1} y x^{-1} z^{-1} x y x$
B	$y^3 z^{-2} x y z x^3 y$	$y^3 z^{-2} x^{-2} y^2 z^{-1} y^{-1}$

Table 11. Correspondence: Plaintext alphabet to ciphertext alphabet II.

	$U_{f_{u_3}}$	$U_{f_{u_4}}$
L	$xyzyz^{-1}y^{-2}x^{-2}z^{-1}xy^3z^{-2}$	$y^{-1}xzyz$
E	$yz^{-1}y^{-1}x^{-1}zx^2y$	$x^{-1}zx^{-1}yz^{-1}y^{-2}xzx^{-1}$
I	$x^{-1}zx^4\left(z^2y^{-3}\right)^2$	$y^{-1}xzx^{-1}z^{-1}\left(xy\right)^2zy^{-1}xz^{-1}x$
O	$y^{-1}x^2\left(z^2y^{-3}\right)^2$	$x^{-2}yz^{-1}\left(xy\right)^2zy^{-1}xz^{-1}x$
U	$x^{-1}y^{-1}x^{-1}yx^{-2}zx^{-1}$	$z^{-1}\left(xy\right)^2zy^{-1}xz^{-1}x$
A	$z^{-1}y\left(x^{-2}z\right)^2x^2y$	$z^{-1}yx^{-1}yzy^{-2}xzyz$
V	$x^5\left(z^2y^{-3}\right)^2$	$x^3yx^{-2}yx^{-1}zx^{-1}yz^{-1}y^{-1}$
B	$y^{-1}x^{-2}z^{-1}xy^3z^{-2}$	$y^3z^{-2}yz^3y^{-1}xz^{-1}x^{-1}y$

$$C = xyzx^3y^2zy^{-2}x^2 \wr yzy^{-2}x^5yz^{-1}yx^{-1}z^{-1}xyx \wr x^5\left(z^2y^{-3}\right)^2 \wr x^{-1}zx^{-1}yz^{-1}y^{-2}xzx^{-1}$$

$$S = \text{LOVE}.$$

Security 25. The cryptosystem is a polyalphabetic system, that means, a word $u_i \in U$, and hence a letter $a_i \in A$, is encrypted differently at different positions in the plaintext, because different automorphisms are used during the encryption procedure for each ciphertext unit. Thus, for the ciphertext, a statistical frequency attack (see for instance [1]) over the frequency of words, which correspond to letters in the plaintext alphabet, or groups of words, is useless.

The security depends on the fact, that the set U is private. Note, that the ciphertext units c_i are elements in F_U, with $F_U = \langle U \mid \rangle$. An eavesdropper, Eve, knows that the elements of the set U, which where used for the encryption, can be found in the ball $B\left(F, L_1\right)$ of the Cayley graph from F, with

$$L_1 = \max\left\{\left|c_i\right|_X \mid i = 1, 2, \cdots, z\right\} \tag{24}$$

and c_i ciphertext units of an intercepted ciphertext

$$C = c_1 \wr c_2 \wr \cdots \wr c_z. \tag{25}$$

The symbol "$\wr$" marks the end of each ciphertext unit c_i, $1 \le i \le z-1$.

Let

$$\tilde{C} = \left\{c_1, c_2, \cdots, c_z\right\} \tag{26}$$

be the set of ciphertext units and let $\tilde{C}_{Nred}$ be a Nielsen reduced set of $\tilde{C}$, hence the group $F_{\tilde{C}_{Nred}}$, generated by $\tilde{C}_{Nred}$, is a free subgroup of F_U and $rank\left(F_{\tilde{C}_{Nred}}\right) \le z$. The main security certification depends on the fact, that for a single subset V of F_U with K elements Eve finds a Nielsen reduced set in the running time $\mathcal{O}\left(\lambda^2K^2\right)$, with λ the maximum over the free length of the elements in the subset V with K primitive elements, but she has to test all possible subsets of K elements for which she needs exponential running time, because the number of primitive elements grows exponentially with the free length, here with L_1. She searches in a ball $B\left(F, L_1\right)$, with $L_1 = \max\left\{\left|c_i\right| \mid c_i \in \tilde{C}\right\}$ for these primitive elements.

A subset of V is also known, it is $\tilde{C}_{Nred} \subset V$ but she has to put all other primitive elements to this set and proves if V', which is Nielsen reduced to V, is of order N and

hence a candidate for U.

Furthermore, the security depends on the way how Alice and Bob choose the automorphisms of the set $\mathcal{H}_{Aut}$. To verify, whether a candidate set V' is very likely the set U used by Alice and Bob, it is likely that Eve writes the ciphertext units c_i with letters of her candidate set $V'^{\pm 1}$. This is possible because the constructive membership problem (see Problem 11) is solvable in abstract free groups and Nielsen reduced sets. Thus, she could get hints for the automorphisms used for encryption and it is not only a brute force search through the set $\mathcal{H}_{Aut}$.

A more detailed cryptographical analysis can be found in [5] and there are also three modifications given, which are summarized as follows:

1) We present a modification where the ciphertext is only one reduced word in X instead of a sequence of words, in this case it is possible that additional information is needed for decryption, thus these are sent with the ciphertext if required. The ciphertext can be interpreted as words in X and as words in U, thus the additional information could be given about the ciphertext written as a word in U or as a word in X.

Security: The security certification is extended to the fact that Eve is in general not able to identify the beginning and end of a ciphertext unit c_i, $i = 1, 2, \cdots, z$. There could also be cancellations, which she is not able to recognize. Eve is neither able to determine the number L_1 because she does not know what the ciphertext units c_i exactly look like, nor is she able to generate the set $\tilde{C}_{Nred}$. This worsens her attacks of the unmodified cryptographic protocol above.

2) We present a modification, which uses a faithful representation from F into the special linear group $\mathrm{SL}(2,\mathbb{Q})$ such that the ciphertext is a sequence of matrices in $\mathrm{SL}(2,\mathbb{Q})$. Furthermore, a variation can be used, where the ciphertext is not a sequence of matrices but a sequence of entries of matrices. This reduces the space for the ciphertext and the memory space for the decryption table.

Security: The security certification is extended to the fact, that there is no algorithm known to solve the (constructive) membership problem for (discrete) free subgroups of $\mathrm{SL}(2,\mathbb{Q})$ which are of rank greater than or equal to 2 and not subgroups of $\mathrm{SL}(2,\mathbb{Z})$, see [15]. Therefore, the attack which uses a Cayley graph and automorphisms of $\mathcal{F}_{Aut}$ in the unmodified cryptographic protocol is not realizable in this modification.

3) We present a modification, which utilizes the negative solution of Hilbert's Tenth Problem. Instead of a presentation of the ciphertext as a sequence of matrices in $\mathrm{SL}(2,\mathbb{Q})$ the ciphertext is represented as a sequence of matrices in $\mathrm{GL}(2,R)$ with $R := \mathbb{Z}[y_1, y_2, \cdots, y_n]$, the integral polynomial ring in $n \geq 2$ variables. Here we get two subcases, the first applies the modification with Hilbert's Tenth Problem on a text given as a sequence of words in X and the second applies it to a text given as a sequence of words in U.

Security: The security certification is extended to Hilbert's Tenth Problem. In addition the security is improved by the fact, that for each encryption Alice and Bob can take privately ephemeral matrices in $GL(2,R)$, $R = \mathbb{Z}[y_1, y_2, \cdots, y_n]$, with the property that the common private point $D \in \mathbb{Z}^n$ generates the correct matrices in

$\mathrm{PSL}(2,\mathbb{Z})$. This gives randomness to ciphertexts, which complicates attacks for Eve. The attack which uses a Cayley graph and automorphisms of $\mathcal{F}_{Aut}$ in the unmodified cryptographic protocol is not realizable in this modification.

Remark 26. In [5] are two more private key cryptosystems given, which use finitely generated free groups, Nielsen transformations and automorphisms on finitely generated free group. The first one uses automorphisms on F instead of a subgroup of F, as in the above described private key cryptosystem. It also has three modifications, which use the ideas for the modifications above. The second protocol uses automorphisms on plaintext units and in addition randomly chosen ephemeral keys (matrices of $(2,\mathbb{Q})$), which give randomness to the ciphertexts.

7. Cryptosystem with Nielsen Transformation Inspired by the ElGamal Cryptosystem

Now we describe a public key cryptosystem for Alice and Bob which is inspired by the ElGamal cryptosystem (see [16] or ([2], Section 1.3)), based on discrete logarithms, that is:

1) Alice and Bob agree on a finite cyclic group G and a generating element $g \in G$.

2) Alice picks a random natural number a and publishes the element $c := g^a$.

3) Bob, who wants to send a message $m \in G$ to Alice, picks a random natural number b and sends the two elements $m \cdot c^b$ and g^b, to Alice. Note that $c^b = g^{ab}$.

4) Alice recovers $m = \left(m \cdot c^b\right) \cdot \left(\left(g^b\right)^a\right)^{-1}$.

For the new public key cryptosystem in this section let $X = \{x_1, x_2, \cdots, x_N\}$, $N \geq 3$, be the free generating set of the finitely generated free group $F = \langle X \mid \rangle$. It is $X^{\pm 1} = X \cup X^{-1}$. The message is an element $m \in S^*$, S^* denotes the set of all freely reduced words with letters in $X^{\pm 1}$. Public are the free group F, its free generating set X and an element $a \in S^*$. The automorphism f, given as a Nielsen transformation or a Whitehead-Automorphism (see for instance the book [17]), should be chosen randomly, an approach is given in ([5], Section 4.4).

An ElGamal like public key cryptosystem, with public parameters determined by Alice, is now as follows:

Public parameters: The finitely generated free group $F = \langle X \mid \rangle$, a freely reduced word $a \neq 1$ in the free group F and an automorphism $f : F \to F$ of infinite order.

Encryption and Decryption Procedure:

1) Alice chooses privately a natural number n and publishes the element $f^n(a) =: c \in S^*$.

2) Bob picks privately a random $t \in \mathbb{N}$ and his message $m \in S^*$. The number t is an ephemeral key for this message, he changes t for each message m, because of Remark 27. He calculates the freely reduced elements

$$m \cdot f^t(c) =: c_1 \in S^* \text{ and } f^t(a) =: c_2 \in S^*. \tag{27}$$

He sends the ciphertext $(c_1, c_2) \in S^* \times S^*$ to Alice.

3) Alice calculates

$$\begin{aligned} c_1 \cdot \left(f^n(c_2)\right)^{-1} &= m \cdot f^t(c) \cdot \left(f^n(c_2)\right)^{-1} \\ &= m \cdot f^t\left(f^n(a)\right) \cdot \left(f^n\left(f^t(a)\right)\right)^{-1} \\ &= m \cdot f^{t+n}(a) \cdot \left(f^{n+t}(a)\right)^{-1} \\ &= m, \end{aligned} \tag{28}$$

and gets the message *m*.

The ElGamal like public key cryptosystem is summarized in Table 12 (page 90).

Remark 27. It is important that different random ephemeral keys t are used to encrypt different messages. As it is for the standard ElGamal cryptosystem (see [18]). Suppose that Bob uses the same ephemeral key t to encrypt two messages m_1 and m_2 and assume that m_1 is known. The ciphertext pairs are (c_1, c_2) and (c_1', c_2'), with $c_2 = c_2'$, $c_1 = m_1 \cdot f^t(c)$ and $c_1' = m_2 \cdot f^t(c)$. Eve only has to calculate $c_1' \cdot (c_1)^{-1} \cdot m_1$ to get the message m_2.

Security 28. A possible attacker, Eve, can see the elements $c, c_1, c_2 \in S^*$. She does not know the free length of m and the cancellations between m and $f^t(c)$ in c_1. It could be possible that m is completely canceled by the first letters of $f^t(c)$. Hence, she cannot determine m from the given c_1. Eve just sees words, $f^t(a)$ and $f^n(a)$,

Table 12. Summary of the ElGamal like public key cryptosystem using automorphisms on a finitely generated free group *F*.

Public Parameters	
Free group $F = \langle X \mid \ \rangle$, a freely reduced word $a \neq 1$ in F and an automorphism $f: F \to F$ of infinite order.	
Alice	**Bob**
Key Creation	
Choose private key $n \in \mathbb{N}$. Compute $f^n(a) =: c \in S^*$. (S^* denotes the set of all freely reduced words with letters in $X^{\pm 1}$.) Publish *c*.	
	Encryption
	Choose plaintext $m \in S^*$. Choose random ephemeral key $t \in \mathbb{N}$. Compute $m \cdot f^t(c) =: c_1 \in S^*$ and $f^t(a) =: c_2 \in S^*$. Send ciphertext $(c_1, c_2) \in S^* \times S^*$ to Alice.
	$\xleftarrow{(c_1, c_2)}$
	Decryption
Compute $c_1 \cdot \left(f^n(c_2)\right)^{-1} = m \cdot f^t(c) \cdot \left(f^n(c_2)\right)^{-1} = m \cdot f^t\left(f^n(a)\right) \cdot \left(f^n\left(f^t(a)\right)\right)^{-1} = m \cdot f^{t+n}(a) \cdot \left(f^{n+t}(a)\right)^{-1} = m,$ which is the message from Bob.	

in the free generating set X from which it is unlikely to realize the exponents n and t, that is, the private keys from Alice and Bob, respectively. The security is based on the Diffie-Hellman problem and discrete logarithm problem in cyclic subgroups of automorphisms in free groups.

Variation 29. We give some ideas to enhance the security, they can also be combined:

1) The element $a \in S^*$ could be taken as a common private secret between Alice and Bob. They could use for example the Anshel-Anshel-Goldfeld key exchange protocol (see for instance [2]) to agree on the element *a*.

2) Alice and Bob agree on a faithful representation from *F* into the special linear group of all 2×2 matrices with entries in $\mathbb{Q}$, that is, $g: F \to \mathrm{SL}(2,\mathbb{Q})$. Now, $m \in S^*$ and Bob sends the element $g(m)\cdot g\left(f^t(c)\right) =: c_1 \in \mathrm{SL}(2,\mathbb{Q})$ instead of $m \cdot f^t(c) =: c_1 \in S^*$; *c* and c_2 remain the same. Therefore, Alice calculates $c_1 \cdot \left(g\left(f^n(c_2)\right)\right)^{-1} = g(m)$ and hence the message $m = g^{-1}\left(g(m)\right) \in S^*$. This variation in addition extends the security certification to the constructive membership problem in the matrix group $\mathrm{SL}(2,\mathbb{Q})$ (see [15]).

We now explain this variation in more details.

In addition to $X = \{x_1, x_2, \cdots, x_N\}$ Alice chooses a second abstract set $Y = \{y_1, y_2, \cdots, y_N\}$, with $X \cap Y = \varnothing$, which generates a free group $F' = \langle Y \mid \rangle$ of rank *N*. The automorphism *f* from Alice is an automorphism on a free group of rank $|X|$ if we identify x_i with y_i for $i = 1, 2, \cdots, N$, then *f* is also an automorphism of F', because $|X| = |Y|$ and hence F' is isomorphic to *F*, see Theorem 12.

Alice needs a faithful representation of $\langle X \cup Y \mid \rangle$ into $\mathrm{SL}(2,\mathbb{Q})$ such that

$$g: \langle X \cup Y \mid \rangle \to \mathrm{SL}(2,\mathbb{Q})$$

$$x_i \mapsto M_i \quad \text{with } i = 1, 2, \cdots, N \text{ and } M_i \in \mathrm{SL}(2,\mathbb{Z}) \tag{29}$$

$$y_i \mapsto W_i \quad \text{with } i = 1, 2, \cdots, N \text{ and } W_i \in \mathrm{SL}(2,\mathbb{Q}) \text{ and } W_i \notin \mathrm{SL}(2,\mathbb{Z}) \tag{30}$$

Thus, each W_i has at least one entry which is an element in $\mathbb{Q} \setminus \mathbb{Z}$.

(a) The public element from Alice is as before $c = f^n(a) \in S^*$, with private key $n \in \mathbb{N}$.

(b) Bob chooses privately a message $m \in S^*$, a random $t \in \mathbb{N}$ and calculates $c_2 = f^t(a) \in S^*$ as before. After this he computes $f^t(c) = f^t\left(f^n(a)\right) = f^{t+n}(a) \in S^*$ and writes it as a word in *Y* whereby he used the assignment $x_i = y_i$ for $1 \le i \le N$. We denote $f^t(c)$ as $f_Y^t(c)$ when $f^t(c)$ is written as a word in *Y*. The element $f_Y^t(c)$ is a reduced word in *Y*. Bob's element $c_1 = m \cdot f_Y^t(c)$ is now a reduced word in $X \cup Y$. He applies the faithful representation *g* on this element. It is

$$g\left(m \cdot f_Y^t(c)\right) = \underbrace{g(m)}_{\in \mathrm{SL}(2,\mathbb{Z})} \cdot \underbrace{g\left(f_Y^t(c)\right)}_{\in \mathrm{SL}(2,\mathbb{Q})} =: c_1' \in \mathrm{SL}(2,\mathbb{Q}). \tag{31}$$

Instead of $(c_2, c_1) \in S^* \times S^*$ he sends $(c_2, c_1') \in S^* \times \mathrm{SL}(2,\mathbb{Q})$ to Alice.

(c) Firstly, Alice calculates $f^n(c_2)$ and hence gets the same element $f^t(c)$ as

Bob, because

$$f^n(c_2) = f^n\left(f^t(a)\right) = f^{n+t}(a) = f^{t+n}(a) = f^t\left(f^n(a)\right) = f^t(c). \tag{32}$$

Secondly, she writes $f^n(c_2)$ as a word in Y, thus she gets $f_Y^t(c)$. Thirdly, she uses the faithful representation g to calculate $g\left(f_Y^t(c)\right)$ and together with c_1' she gets

$$c_1' \cdot \left(g\left(f_Y^t(c)\right)\right)^{-1} = g(m) \cdot g\left(f_Y^t(c)\right)\left(g\left(f_Y^t(c)\right)\right)^{-1} = g(m) \in \mathrm{SL}(2,\mathbb{Z}). \tag{33}$$

She gets a matrix in $\mathrm{SL}(2,\mathbb{Z})$ and she knows that this matrix is a word in the letters of M_i, $1 \le i \le N$, hence there is an algorithm (see for instance [8]) to write $g(m)$ as a word in $g(X)$ and therefore as a word in X. Thus, she is able to recon-struct m.

An eavesdropper, Eve, gets a matrix $c_1' \in \mathrm{SL}(2,\mathbb{Q})$ and she is not able to write it as a word in the set $X \cup Y$ (because there is no algorithm known to solve the constructive membership problem in a (discrete) free subgroup of $\mathrm{SL}(2,\mathbb{Q})$ of rank greater than or equal to 2 (see [15]), which is not in $\mathrm{SL}(2,\mathbb{Z})$). Thus, she cannot get the situation as in the cryptosystem without the faithful representation g into $\mathrm{SL}(2,\mathbb{Q})$. There is no hint for the message m, instead of the system above in which it is possible that an initial segment of m is visible whereby Eve does not know how long this initial segment is and if it is relay visible. Thus, this variation extends the security certification to the constructive membership problem in the matrix group $\mathrm{SL}(2,\mathbb{Q})$.

We now end this section with an example.

Example 30. This example, is a very small one and it is just given for illustration purposes. The calculations were done with GAP, see Appendix B. Bob wants to send a message to Alice.

The **public parameters** are the free group F of rank 3 with free generating set $X = \{x, y, z\}$, the freely reduced word $a \in F$, with $a := x^2yz^{-2}y$ and the automorphism $f : F \to F$, which is given, for this example, by the regular Nielsen transformation: $\left[(N2)_{1.2}\right]^2 (N2)_{3.2} (N1)_3 (N2)_{2.3}$, thus, it is:

$$f : F \to F$$

$$x \mapsto xy^2,$$

$$y \mapsto z^{-1},$$

$$z \mapsto y^{-1}z^{-1}.$$

1) Alice's private key is $n = 7$. Thus, she gets the automorphism

$$f^7 : F \to F$$

$$x \mapsto xy^2z^{-1}y(yz)^2\left(zyz^2y\right)^2 zy$$

$$y \mapsto y^{-1}\left(\left(z^{-1}y^{-1}z^{-1}\right)^2 y^{-1}z^{-1}\right)^2 z^{-1}y^{-1}z^{-2}$$

$$z \mapsto \left(\left(\left(y^{-1}z^{-1}\right)^2 z^{-1}\right)^2 y^{-1}z^{-2}\right)^2 y^{-1}\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}.$$

Her public key is

$$c := f^7(a) = \left(xy^2z^{-1}y(yz)^2\left(zyz^2y\right)^2 zy\right)^2\left(z^2y\right)^2\left((zyz)^2\, yz\right)^2 zyz^2yz^{-1}.$$

2) Bob privately picks the ephemeral key $t = 5$ and gets the automorphism

$$f^5 : F \to F$$

$$x \mapsto xy^2z^{-1}y^2z(zy)^2$$

$$y \mapsto y^{-1}\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}$$

$$z \mapsto \left(\left(y^{-1}z^{-1}\right)^2 z^{-1}\right)^2 y^{-1}z^{-2}.$$

His message for Alice is $m = z^{-2}y^2zx^2y^{-1}x^{-1}$. He calculates

$$\begin{aligned}
c_1 &= m \cdot f^5(c) \\
&= z^{-2}y^2zx^2\left(yz^{-1}\right)^2\left(\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-2}y^{-1}\right)^2\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}y^{-1} \\
&\quad \left(\left(\left(\left(z^{-1}y^{-1}z^{-1}\right)^2 y^{-1}z^{-1}\right)^2 z^{-1}y^{-1}z^{-1}y^{-1}z^{-1}\right)^2\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-1}y^{-1}z^{-1}\right)^2 \\
&\quad \left(\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-2}y^{-1}\right)^2\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}xy^2z^{-1}y \\
&\quad \left(z^{-1}\left(\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-2}y^{-1}\right)^2\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}y^{-1}\right)^3\left(z^{-1}y^{-1}z^{-1}\right)^2 \\
&\quad y^{-1}z^{-1}\left(\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-2}y^{-1}\right)^2\left(z^{-1}y^{-1}z^{-1}\right)^2 y^{-1}\right)^3 z^{-1} \\
&\quad \left(\left(z^{-1}y^{-1}z^{-2}y^{-1}\right)^2 z^{-2}y^{-1}\right)^2\left(z^{-1}y^{-1}z^{-1}\right)^2 y^{-1}z^{-1}y
\end{aligned}$$

and

$$c_2 := f^5(a) = \left(xy^2z^{-1}y^2z(zy)^2\right)^2 z^2y(zyz)^2\, zyz^{-1}.$$

The ciphertext for Alice is the tuple (c_1, c_2).

3) Alice first computes

$$\begin{aligned}
\left(f^7(c_2)\right)^{-1} = y^{-1}&\left(\left(\left(\left((zy)^2 z\right)^2 zyz\right)^2 zy(zyz)^2\right)^2 zy\left((zyz)^2\, yz\right)^2 zyz\right)^2 \\
&\left(zy\left(\left((zyz)^2\, yz\right)^2 zyzyz\right)^2\left(zyz^2y\right)^2 z\right)^2 \\
&y\left(\left(\left(\left(z^2y\right)^2 zy\right)^2 z^2yzy\right)^2 z\left(zyz^2y\right)^2 zy\right)^2 z\left(zyz^2y\right)^2 z^2y \\
&\left(\left((zyz)^2\, yz\right)^2 zyzyz\right)^2\left(zyz^2y\right)^2 z\left(zy^{-1}\right)^2 y^{-1}x^{-1}\Big)^2
\end{aligned}$$

and gets m by

$$m = c_1 \cdot \left(f^7 \left(c_2 \right) \right)^{-1} = z^{-2} y^2 z x^2 y^{-1} x^{-1}.$$

8. Conclusions

A. Shamir's secret sharing protocol (see [6]) has become the standard method for solving the (n,t)-secret sharing problem. The introduced secret sharing schemes are of mathematical interest.

In contrast to other secret sharing schemes the part for the participants at the combinatorial secret sharing scheme, see Section 3, is very easy, they only have to add up m elements. The (time) expensive part is the part of the dealer, who has to generate the sets R_i for the participants. In contrast to Shamir's scheme, where the part of the dealer is the easier one and the participants have to do polynomial interpolation to reconstruct the secret.

The secret sharing scheme of Section 4 uses combinatorial group theory, especially Nielsen transformations and finitely generated free groups. It is mathematically a very interesting cryptographic protocol, which serves very good as a basis to develop other cryptographic protocol. In addition the secret sharing scheme of Section 5 is also a mathematically very interesting cryptographic protocol. Both secret sharing schemes are the basis for the newly developed cryptosystems.

In comparison to the standard cryptosystems which are mostly based on number theory we explained two cryptosystems which use combinatorial group theory. The first cryptosystem in Section 6 is a kind of a one-time pad, which choice of the random sequence for encryption is not number-theoretic. Especially the modifications with matrices are of interest for cryptography. If the symmetric key cryptosystem is used together with the second modification, which uses a faithful representation into $\mathrm{SL}(2,\mathbb{Q})$, then the system is secure and the security depends on the unknown solution of the (constructive) membership problem in the used matrix groups. If it is used together with the third modification, which uses matrices in $\mathrm{GL}(2,R)$, $R = \mathbb{Z}[y_1, y_2, \cdots, y_n]$, $n \geq 2$, then the system is secure and the security depends in addition on the negative solution of Hilbert's Tenth Problem. Moreover, we get also randomness to each ciphertext by the ephemeral matrices which the encrypter used for encryption. To generate these ephemeral matrices he only needs the common secret point $D \in \mathbb{Z}^n$, this improves also the security. Altogether, we get interesting new private key cryptosystems, which use non-commutative groups and are based on combinatorial group theory and not only on number theory. They provide other options for private key cryptosystems which are based on combinatorial group theory. The second cryptosystem in Section 7 is similar to the ElGamal cryptosystem (see [16]), which is easier to handle. The ElGamal cryptosystem is based on the discrete logarithm problem over a finite field. If this problem should eventually be solved we introduced here an alternative system, which is not based on number theory.

For further research one could search for other cryptographic protocols, which can be based on Nielsen transformations, for example a public key cryptosystem which is not ElGamal like or a key exchange protocol. There is no algorithm known to solve the

(constructive) membership problem for (discrete) free subgroups of rank equal or greater than 2 in $\mathrm{SL}(2,\mathbb{Q})$. Thus, the following questions appear: Are there quantum algorithms for solving the (constructive) membership problem in $\mathrm{SL}(2,\mathbb{Q})$? Are there quantum algorithms for solving other problems in combinatorial group theory, which are used in cryptography?

References

[1] Baumslag, G., Fine, B., Kreuzer, M. and Rosenberger, G. (2015) A Course in Mathematical Cryptography. De Gruyter, Berlin. http://dx.doi.org/10.1515/9783110372779

[2] Myasnikov, A., Shpilrain, V. and Ushakov, A. (2008) Group-Based Cryptography. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser, Basel.

[3] Chum, C., Fine, B. and Zhang, X. Shamir's Threshold Scheme and Its Enhancements. To Appear.

[4] Panagopoulos, D. (2010) A Secret Sharing Scheme Using Groups. Preprint. http://arxiv.org/abs/1009.0026 ,

[5] Moldenhauer, A.I.S. (2016) Cryptographic Protocols Based on Inner Product Spaces and Group Theory with a Special Focus on the Use of Nielsen Transformations. Ph.D. Thesis, University of Hamburg, Hamburg.

[6] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613.

[7] Atkinson, K. (1989) An Introduction to Numerical Analysis. 2nd Edition, John Wiley & Sons, Hoboken.

[8] Camps, T., Große Rebel, V. and Rosenberger, G. (2008) Einführung in die kombinatorische und die geometrische Gruppentheorie. Berliner Studienreihe zur Mathematik Band **19**. Heldermann Verlag, Berlin.

[9] Lyndon, R.C. and Schupp, P.E. (1977) Combinatorial Group Theory. Ergebnisse der Mathematik und ihre Grenzgebiete **89**, Springer-Verlag, New York.

[10] Magnus, W. Karrass, A. and Solitar, D. (1966) Combinatorial Group Theory. Pure and Applied Mathematics, a Series of Texts and Monographs Volume **XIII**. John Wiley & Sons, Hoboken.

[11] Ito, M., Saito, A. and Nishizeki, T. (1987) Secret Sharing Scheme Realizing General Access Structure. *Proceedings of IEEE Globecom* 87, 99-102.

[12] Benaloh, J. and Leichter, J. (1990) *Generalized Secret Sharing and Monotone Functions*. CRYPTO '88. Springer-Verlag, New York.

[13] Lehner, J. (1964) Discontinuous Groups and Automorphic Functions. Mathematical Surveys Number **VIII**. American Mathematical Society, Providence. http://dx.doi.org/10.1090/surv/008

[14] GAP (2015) Version 4.7.7 of 13-feb-2015 (Free Software, GPL). http://www.gap-system.org

[15] Eick, B., Kirschmer, M. and Leedham-Green, C. (2014) The Constructive Membership Problem for Discrete Free Subgroups of Rank 2 of $SL_2(\mathbb{R})$. *LMS Journal of Computation and Mathematics*, **17**, 345-359. http://dx.doi.org/10.1112/S1461157014000047

[16] ElGamal, T. (1985) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **IT-31**, 469-473. http://dx.doi.org/10.1109/TIT.1985.1057074

[17] Diekert, V., Kufleitner, M. and Rosenberger, G. (2013) Diskrete algebraische Methoden. De Gruyter, Berlin. http://dx.doi.org/10.1515/9783110312614

[18] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (1997) Handbook of Applied Cryptography. CRC Press LLC, Boca Raton.

Appendix

We now give the computer code in GAP[2] for Example 24 and Example 30. Therefore we use the FGA[3] package in GAP and also Nielsen transformations.

If there are Nielsen transformations of type $(N1)$ one after another we can do them in one step. For example if the Nielsen transformations $(N1)_5\,(N1)_3\,(N1)_2\,(N2)_{3.2}$ are applied to a set (a,b,c,d,e) we write instead of

$$\begin{aligned}(a,b,c,d,e) &\xrightarrow{(N1)_5}\left(a,b,c,d,e^{-1}\right)\\ &\xrightarrow{(N1)_3}\left(a,b^{-1},c,d,e^{-1}\right)\\ &\xrightarrow{(N1)_2}\left(a^{-1},b^{-1},c,d,e^{-1}\right)\\ &\xrightarrow{(N2)_{3.2}}\left(a^{-1},b^{-1},cb^{-1},d,e^{-1}\right)\end{aligned}$$

the following

$$\begin{aligned}(a,b,c,d,e) &\xrightarrow{(N1)_5(N1)_3(N1)_2}\left(a^{-1},b^{-1},c,d,e^{-1}\right)\\ &\xrightarrow{(N2)_{3.2}}\left(a^{-1},b^{-1},cb^{-1},d,e^{-1}\right).\end{aligned}$$

A. Calculations in GAP for Example 24

Alice and Bob use the free group $F=\langle X\mid\rangle$, with free generating set $X=\{x,y,z\}$, and the explicit free subgroup F_U of F with free generating set $U=\{u_1,u_2,\cdots,u_8\}$, u_i words in X, they choose

$$u_1:=xyz,\quad u_2:=yzy^{-1},\quad u_3:=x^{-1}zx^{-1},\quad u_4:=y^{-1}x^2,$$

$$u_5:=z^{-1}xyx,\quad u_6:=z^{-1}yx^{-1},\quad u_7:=x^3y,\quad u_8:=y^3z^{-2}.$$

In GAP they define

```
LoadPackage("FGA");;
F:=FreeGroup("x", "y", "z");;
AssignGeneratorVariables(F);;
u1:=x*y*z;;
u2:=y*z*y^-1;;
u3:=x^-1*z*x^-1;;
u4:=y^-1*x^2;;
u5:=z^-1*x*y*x;;
u6:=z^-1*y*x^-1;;
u7:=x^3*y;;
u8:=y^3*z^-2;;
FU:=Group(u1, u2, u3, u4, u5, u6, u7, u8);;
```

and prove that U is a Nielsen reduced set with the operation

```
▷ FreeGeneratorsOfGroup(FU)
```

[2]Groups, Algorithms and Programming [14].

[3]Free Group Algorithms. A GAP4 Package by Christian Sievers, TU Braunschweig.

which gives a Nielsen reduced generator set for the group *FU*:

```
gap> Free Generators Of Group (FU);
[x*y*z, y*z*y^-1, x^-1*z*x^-1, y^-1*x^2, z^-1*x*y*x,\
z^-1*y*x^-1, x^3*y, y^3*z^-2 ]
```

Alice knows the linear congruence generator h hence she can get the 4 required automorphisms of the set $\mathcal{H}_{Aut}$ to encrypt her message.

These automorphisms are describable with Nielsen transformations as follows:

- Automorphism f_{u_1} :

$$
\begin{aligned}
&(u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{1,7}}(u_1u_7,u_2,u_3,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{2,4}}(u_1u_7,u_2u_4,u_3,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N1)_5}(u_1u_7,u_2u_4,u_3,u_4,u_5^{-1},u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{7,8}}(u_1u_7,u_2u_4,u_3,u_4,u_5^{-1},u_6,u_7u_8,u_8)\\
&\xrightarrow{\left[(N2)_{3,4}\right]^2}(u_1u_7,u_2u_4,u_3u_4^2,u_4,u_5^{-1},u_6,u_7u_8,u_8)\\
&\xrightarrow{(N2)_{4,6}}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1},u_6,u_7u_8,u_8)\\
&\xrightarrow{(N2)_{5,1}}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6,u_7u_8,u_8)\\
&\xrightarrow{(N1)_7}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6,u_8^{-1}u_7^{-1},u_8)\\
&\xrightarrow{(N2)_{6,3}}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_8^{-1}u_7^{-1},u_8)\\
&\xrightarrow{(N2)_{8,1}}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_8^{-1}u_7^{-1},u_8u_1u_7)\\
&\xrightarrow{(N2)_{7,4}}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_8^{-1}u_7^{-1}u_4u_6,u_8u_1u_7)\\
&\xrightarrow{(N1)_7}(u_1u_7,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_6^{-1}u_4^{-1}u_7u_8,u_8u_1u_7)\\
&\xrightarrow{(N2)_{1,2}}(u_1u_7u_2u_4,u_2u_4,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_6^{-1}u_4^{-1}u_7u_8,u_8u_1u_7)\\
&\xrightarrow{(N2)_{2,3}}(u_1u_7u_2u_4,u_2u_4u_3u_4^2,u_3u_4^2,u_4u_6,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_6^{-1}u_4^{-1}u_7u_8,u_8u_1u_7)\\
&\xrightarrow{(N2)_{4,5}}(u_1u_7u_2u_4,u_2u_4u_3u_4^2,u_3u_4^2,u_4u_6u_5^{-1}u_1u_7,u_5^{-1}u_1u_7,u_6u_3u_4^2,u_6^{-1}u_4^{-1}u_7u_8,u_8u_1u_7)
\end{aligned}
$$

Hence, the automorphism is

$$
\begin{aligned}
f_{u_1}&:H\to H\\
u_1&\mapsto u_1u_7u_2u_4,\\
u_2&\mapsto u_2u_4u_3u_4^2,\\
u_3&\mapsto u_3u_4^2,\\
u_4&\mapsto u_4u_6u_5^{-1}u_1u_7,\\
u_5&\mapsto u_5^{-1}u_1u_7,\\
u_6&\mapsto u_6u_3u_4^2,\\
u_7&\mapsto u_6^{-1}u_4^{-1}u_7u_8,
\end{aligned}
$$

$$u_8 \mapsto u_8u_1u_7.$$

- Automorphism f_{u_2}:

$$\begin{aligned}
&(u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{1,3}}(u_1u_3,u_2,u_3,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{3,5}}(u_1u_3,u_2,u_3u_5,u_4,u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N1)_2(N1)_4}(u_1u_3,u_2^{-1},u_3u_5,u_4^{-1},u_5,u_6,u_7,u_8)\\
&\xrightarrow{(N2)_{6,5}}(u_1u_3,u_2^{-1},u_3u_5,u_4^{-1},u_5,u_6u_5,u_7,u_8)\\
&\xrightarrow{(N1)_1}(u_3^{-1}u_1^{-1},u_2^{-1},u_3u_5,u_4^{-1},u_5,u_6u_5,u_7,u_8)\\
&\xrightarrow{\left[(N2)_{3,4}\right]^2}(u_3^{-1}u_1^{-1},u_2^{-1},u_3u_5u_4^{-2},u_4^{-1},u_5,u_6u_5,u_7,u_8)\\
&\xrightarrow{(N2)_{5,2}}(u_3^{-1}u_1^{-1},u_2^{-1},u_3u_5u_4^{-2},u_4^{-1},u_5u_2^{-1},u_6u_5,u_7,u_8)\\
&\xrightarrow{(N2)_{7,6}}(u_3^{-1}u_1^{-1},u_2^{-1},u_3u_5u_4^{-2},u_4^{-1},u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8)\\
&\xrightarrow{(N2)_{4,2}}(u_3^{-1}u_1^{-1},u_2^{-1},u_3u_5u_4^{-2},u_4^{-1}u_2^{-1},u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8)\\
&\xrightarrow{(N2)_{2,8}}(u_3^{-1}u_1^{-1},u_2^{-1}u_8,u_3u_5u_4^{-2},u_4^{-1}u_2^{-1},u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8)\\
&\xrightarrow{(N2)_{8,4}}(u_3^{-1}u_1^{-1},u_2^{-1}u_8,u_3u_5u_4^{-2},u_4^{-1}u_2^{-1},u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N1)_4}(u_3^{-1}u_1^{-1},u_2^{-1}u_8,u_3u_5u_4^{-2},u_2u_4,u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N2)_{1,4}}(u_3^{-1}u_1^{-1}u_2u_4,u_2^{-1}u_8,u_3u_5u_4^{-2},u_2u_4,u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N2)_{2,6}}(u_3^{-1}u_1^{-1}u_2u_4,u_2^{-1}u_8u_6u_5,u_3u_5u_4^{-2},u_2u_4,u_5u_2^{-1},u_6u_5,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N2)_{5,6}}(u_3^{-1}u_1^{-1}u_2u_4,u_2^{-1}u_8u_6u_5,u_3u_5u_4^{-2},u_2u_4,u_5u_2^{-1}u_6u_5,u_6u_5,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N2)_{6,4}}(u_3^{-1}u_1^{-1}u_2u_4,u_2^{-1}u_8u_6u_5,u_3u_5u_4^{-2},u_2u_4,u_5u_2^{-1}u_6u_5,u_6u_5u_2u_4,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})\\
&\xrightarrow{(N2)_{4,7}}(u_3^{-1}u_1^{-1}u_2u_4,u_2^{-1}u_8u_6u_5,u_3u_5u_4^{-2},u_2u_4u_7u_6u_5,u_5u_2^{-1}u_6u_5,u_6u_5u_2u_4,u_7u_6u_5,u_8u_4^{-1}u_2^{-1})
\end{aligned}$$

Hence, the automorphism is

$$\begin{aligned}
&f_{u_2}: H \to H\\
&u_1 \mapsto u_3^{-1}u_1^{-1}u_2u_4,\\
&u_2 \mapsto u_2^{-1}u_8u_6u_5,\\
&u_3 \mapsto u_3u_5u_4^{-2},\\
&u_4 \mapsto u_2u_4u_7u_6u_5,\\
&u_5 \mapsto u_5u_2^{-1}u_6u_5,\\
&u_6 \mapsto u_6u_5u_2u_4,\\
&u_7 \mapsto u_7u_6u_5,\\
&u_8 \mapsto u_8u_4^{-1}u_2^{-1}.
\end{aligned}$$

- Automorphism f_{u_3}:

$$
\begin{aligned}
&\left(u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8\right)\\
&\xrightarrow{(N1)_2(N1)_5(N1)_8}\left(u_1,u_2^{-1},u_3,u_4,u_5^{-1},u_6,u_7,u_8^{-1}\right)\\
&\xrightarrow{(N2)_{6,3}}\left(u_1,u_2^{-1},u_3,u_4,u_5^{-1},u_6u_3,u_7,u_8^{-1}\right)\\
&\xrightarrow{(N2)_{3,7}}\left(u_1,u_2^{-1},u_3u_7,u_4,u_5^{-1},u_6u_3,u_7,u_8^{-1}\right)\\
&\xrightarrow{(N2)_{1,2}}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4,u_5^{-1},u_6u_3,u_7,u_8^{-1}\right)\\
&\xrightarrow{\left[(N2)_{4,8}\right]^2}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4u_8^{-2},u_5^{-1},u_6u_3,u_7,u_8^{-1}\right)\\
&\xrightarrow{(N2)_{5,6}}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3,u_7,u_8^{-1}\right)\\
&\xrightarrow{(N2)_{8,3}}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3,u_7,u_8^{-1}u_3u_7\right)\\
&\xrightarrow{(N2)_{6,3}}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7,u_8^{-1}u_3u_7\right)\\
&\xrightarrow{(N1)_8}\left(u_1u_2^{-1},u_2^{-1},u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7,u_7^{-1}u_3^{-1}u_8\right)\\
&\xrightarrow{(N2)_{2,3}}\left(u_1u_2^{-1},u_2^{-1}u_3u_7,u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7,u_7^{-1}u_3^{-1}u_8\right)\\
&\xrightarrow{(N2)_{7,4}}\left(u_1u_2^{-1},u_2^{-1}u_3u_7,u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7u_4u_8^{-2},u_7^{-1}u_3^{-1}u_8\right)\\
&\xrightarrow{(N2)_{1,8}}\left(u_1u_2^{-1}u_7^{-1}u_3^{-1}u_8,u_2^{-1}u_3u_7,u_3u_7,u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7u_4u_8^{-2},u_7^{-1}u_3^{-1}u_8\right)\\
&\xrightarrow{(N2)_{3,4}}\left(u_1u_2^{-1}u_7^{-1}u_3^{-1}u_8,u_2^{-1}u_3u_7,u_3u_7u_4u_8^{-2},u_4u_8^{-2},u_5^{-1}u_6u_3,u_6u_3^2u_7,u_7u_4u_8^{-2},u_7^{-1}u_3^{-1}u_8\right)
\end{aligned}
$$

Hence, the automorphism is

$$
\begin{aligned}
f_{u_3}&:H\to H\\
u_1&\mapsto u_1u_2^{-1}u_7^{-1}u_3^{-1}u_8,\\
u_2&\mapsto u_2^{-1}u_3u_7,\\
u_3&\mapsto u_3u_7u_4u_8^{-2},\\
u_4&\mapsto u_4u_8^{-2},\\
u_5&\mapsto u_5^{-1}u_6u_3,\\
u_6&\mapsto u_6u_3^2u_7,\\
u_7&\mapsto u_7u_4u_8^{-2},\\
u_8&\mapsto u_7^{-1}u_3^{-1}u_8.
\end{aligned}
$$

- Automorphism f_{u_4}:

$$
\begin{aligned}
&\left(u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8\right)\\
&\xrightarrow{(N1)_1(N1)_3(N1)_4}\left(u_1^{-1},u_2,u_3^{-1},u_4^{-1},u_5,u_6,u_7,u_8\right)\\
&\xrightarrow{(N2)_{6,2}}\left(u_1^{-1},u_2,u_3^{-1},u_4^{-1},u_5,u_6u_2,u_7,u_8\right)\\
&\xrightarrow{\left[(N2)_{8,2}\right]^3}\left(u_1^{-1},u_2,u_3^{-1},u_4^{-1},u_5,u_6u_2,u_7,u_8u_2^3\right)\\
&\xrightarrow{(N2)_{2,3}}\left(u_1^{-1},u_2u_3^{-1},u_3^{-1},u_4^{-1},u_5,u_6u_2,u_7,u_8u_2^3\right)\\
&\xrightarrow{(N2)_{3,4}}\left(u_1^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1},u_5,u_6u_2,u_7,u_8u_2^3\right)
\end{aligned}
$$

$$\xrightarrow{(N2)_{5.2}}\left(u_1^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1},u_5u_2u_3^{-1},u_6u_2,u_7,u_8u_2^3\right)$$

$$\xrightarrow{(N2)_{7.4}}\left(u_1^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1},u_8u_2^3\right)$$

$$\xrightarrow{(N2)_{1.3}}\left(u_1^{-1}u_3^{-1}u_4^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1},u_8u_2^3\right)$$

$$\xrightarrow{(N2)_{4.5}}\left(u_1^{-1}u_3^{-1}u_4^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1},u_8u_2^3\right)$$

$$\xrightarrow{(N2)_{8.3}}\left(u_1^{-1}u_3^{-1}u_4^{-1},u_2u_3^{-1},u_3^{-1}u_4^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N1)_1(N1)_2}\left(u_4u_3u_1,u_3u_2^{-1},u_3^{-1}u_4^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N2)_{7.2}}\left(u_4u_3u_1,u_3u_2^{-1},u_3^{-1}u_4^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1}u_3u_2^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N1)_3}\left(u_4u_3u_1,u_3u_2^{-1},u_4u_3,u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1}u_3u_2^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N2)_{2.3}}\left(u_4u_3u_1,u_3u_2^{-1}u_4u_3,u_4u_3,u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1}u_3u_2^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N2)_{3.5}}\left(u_4u_3u_1,u_3u_2^{-1}u_4u_3,u_4u_3u_5u_2u_3^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2,u_7u_4^{-1}u_3u_2^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

$$\xrightarrow{(N2)_{6.1}}\left(u_4u_3u_1,u_3u_2^{-1}u_4u_3,u_4u_3u_5u_2u_3^{-1},u_4^{-1}u_5u_2u_3^{-1},u_5u_2u_3^{-1},u_6u_2u_4u_3u_1,u_7u_4^{-1}u_3u_2^{-1},u_8u_2^3u_3^{-1}u_4^{-1}\right)$$

Hence, the automorphism is

$$f_{u_4}:H\to H$$

$$u_1\mapsto u_4u_3u_1,$$

$$u_2\mapsto u_3u_2^{-1}u_4u_3,$$

$$u_3\mapsto u_4u_3u_5u_2u_3^{-1},$$

$$u_4\mapsto u_4^{-1}u_5u_2u_3^{-1},$$

$$u_5\mapsto u_5u_2u_3^{-1},$$

$$u_6\mapsto u_6u_2u_4u_3u_1,$$

$$u_7\mapsto u_7u_4^{-1}u_3u_2^{-1},$$

$$u_8\mapsto u_8u_2^3u_3^{-1}u_4^{-1}.$$

In GAP she defines for the automorphisms:

```
#Automorphism f_{u_1}
u11:=u1*u7*u2*u4;;
u12:=u2*u4*u3*u4^2;;
u13:=u3*u4^2;;
u14:=u4*u6*u5^-1*u1*u7;;
u15:=u5^-1*u1*u7;;
u16:=u6*u3*u4^2;;
u17:=u6^-1*u4^-1*u7*u8;;
u18:=u8*u1*u7;;
#Automorphism f_{u_2}
u21:=u3^-1*u1^-1*u2*u4;;
```

```
u22:=u2^-1*u8*u6*u5;;
u23:=u3*u5*u4^-2;;
u24:=u2*u4*u7*u6*u5;;
u25:=u5*u2^-1*u6*u5;;
u26:=u6*u5*u2*u4;;
u27:=u7*u6*u5;;
u28:=u8*u4^-1*u2^-1;;
#Automorphism f_{u_3}
u31:=u1*u2^-1*u7^-1*u3^-1*u8;;
u32:=u2^-1*u3*u7;;
u33:=u3*u7*u4*u8^-2;;
u34:=u4*u8^-2;;
u35:=u5^-1*u6*u3;;
u36:=u6*u2^3*u7;;
u37:=u7*u4*u8^-2;;
u38:=u7^-1*u3^-1*u8;;
#Automorphism f_{u_4}
u41:=u4*u3*u1;;
u42:=u3*u2^-1*u4*u3;;
u43:=u4*u3*u5*u2*u3^-1;;
u44:=u4^-1*u5*u2*u3^-1;;
u45:=u5*u2*u3^-1;;
u46:=u6*u2*u4*u3*u1;;
u47:=u7*u4^-1*u3*u2^-1;;
u48:=u8*u2^3*u3^-1*u4^-1;;
```

Hence, to get the ciphertext

$$\begin{aligned} C &= f_{u_1}(\mathsf{L})\, f_{u_2}(\mathsf{O})\, f_{u_3}(\mathsf{V})\, f_{u_4}(\mathsf{E}) \\ &= f_{u_1}(u_1)\, f_{u_2}(u_4)\, f_{u_3}(u_7)\, f_{u_4}(u_2) \end{aligned}$$

as a word in X, she calculates in GAP:

```
gap > u11;
    x*y*z*x^3*y^2*z*y^-2*x^2
gap> u24;
    y*z*y^-2*x^5*y*z^-1*y*x^-1*z^-1*x*y*x
gap> u37;
    x^5*(z^2*y^-3)^2
gap> u42;
    x^-1*z*x^-1*y*z^-1*y^-2*x*z*x^-1
```

Thus, the ciphertext is

$$C = xyzx^3y^2zy^{-2}x^2 \wr yzy^{-2}x^5yz^{-1}yx^{-1}z^{-1}xyx \wr x^5\left(z^2y^{-3}\right)^2 \wr x^{-1}zx^{-1}yz^{-1}y^{-2}xzx^{-1}$$

and this is sent to Bob.

For decryption Bob calculates the tables Table 10 (page 86) and Table 11 (page 87). For this he chooses the automorphisms in $\mathcal{H}_{aut}$, which Alice also used. In GAP it is:

```
gap> u11; u12; u13; u14; u15; u16; u17; u18;
x*y*z*x^3*y^2*z*y^-2*x^2
y*z*y^-2*x*z*x^-1*(y^-1*x^2)^2
x^-1*z*x^-1*(y^-1*x^2)^2
y^-1*x^2*z^-1*y*x^-2*y^-1*x^-1*z*x*y*z*x^3*y
x^-1*y^-1*x^-1*z*x*y*z*x^3*y
z^-1*y*x^-2*z*x^-1*(y^-1*x^2)^2
x*y^-1*z*x^-2*y*x^3*y^4*z^-2 y^3*z^-2*x*y*z*x^3*y
gap> u21; u22; u23; u24; u25; u26; u27; u28;
(x*z^-1)^2*y^-1*x^-1*y*z*y^-2*x^2
y*z^-1*y^2*z^-3*y*x^-1*z^-1*x*y*x
x^-1*z*x^-1*z^-1*x*(y*x^-1)^2*x^-1*y
y*z*y^-2*x^5*y*z^-1*y*x^-1*z^-1*x*y*x
z^-1*(x*y)^2*z^-1*y^-1*z^-1*y*x^-1*z^-1*x*y*x
z^-1*y*x^-1*z^-1*(x*y)^2*z*y^-2*x^2
x^3*y*z^-1*y*x^-1*z^-1*x*y*x
y^3*z^-2*x^-2*y^2*z^-1*y^-1
gap> u31; u32; u33; u34; u35; u36; u37; u38;
x*y*z*y*z^-1*y^-2*x^-2*z^-1*x*y^3*z^-2
y*z^-1*y^-1*x^-1*z*x^2*y
x^-1*z*x^4*(z^2*y^-3)^2
y^-1*x^2*(z^2*y^-3)^2
x^-1*y^-1*x^-1*y*x^-2*z*x^-1
z^-1*y*x^-1*y*z^3*y^-1*x^3*y
x^5*(z^2*y^-3)^2
y^-1*x^-2*z^-1*x*y^3*z^-2
gap> u41; u42; u43; u44; u45; u46; u47; u48;
y^-1*x*z*y*z
x^-1*z*x^-1*y*z^-1*y^-2*x*z*x^-1
y^-1*x*z*x^-1*z^-1*(x*y)^2*z*y^-1*x*z^-1*x
x^-2*y*z^-1*(x*y)^2*z*y^-1*x*z^-1*x
z^-1*(x*y)^2*z*y^-1*x*z^-1*x
z^-1*y*x^-1*y*z*y^-2*x*z*y*z
x^3*y*x^-2*y*x^-1*z*x^-1*y*z^-1*y^-1
y^3*z^-2*y*z^3*y^-1*x*z^-1*x^-1*y
```

With this information Bob is able to reconstruct the message $S = \mathrm{LOVE}$.

B. Calculations in GAP for Example 30

Alice defines the public parameters.

Let $X=\{x,y,z\}$ be the free generating set for a free subgroup of rank 3:

```
LoadPackage("FGA");;
F:=FreeGroup("x", "y", "z");;
AssignGeneratorVariables(F);;
```

Additionally she defines the freely reduced word $a:=x^2yz^{-1}y$ and describes the automorphisms f with the following regular Nielsen transformation

$$\begin{aligned}(x,y,z) &\xrightarrow{\left[(N2)_{1,2}\right]^2}\left(xy^2,y,z\right)\\ &\xrightarrow{(N2)_{3,2}}\left(xy^2,y,zy\right)\\ &\xrightarrow{(N)_3}\left(xy^2,y,y^{-1}z^{-1}\right)\\ &\xrightarrow{(N2)_{2,3}}\left(xy^2,z^{-1},y^{-1}z^{-1}\right);\end{aligned}$$

hence the automorphism is

$$\begin{aligned}f&:F\to F\\ x&\mapsto xy^2,\\ y&\mapsto z^{-1},\\ z&\mapsto y^{-1}z^{-1},\end{aligned}$$

and she defines in GAP:

```
x1:=x*y^2;;
y1:=z^(-1);;
z1:=y^(-1)*z^(-1);;
```

Alice chooses as private key $n=7$, hence she must calculate the automorphism f^7. For this she calculates in GAP:

```
#Calculate automorphism f^2=f^1(f^1)
x2:=x1*y1^2;;
y2:=z1^(-1);;
z2:=y1^(-1)*z1^(-1);;
gap> x2; y2; z2;
x*y^2*z^-2
z*y
z^2*y
#Calculate automorphism f^3=f^1(f^2)
x3:=x2*y2^2;;
y3:=z2^(-1);;
z3:=y2^(-1)*z2^(-1);;
gap> x3; y3; z3;
x*y^2*z^-1*y*z*y
y^-1*z^-2
```

```
(y^-1*z^-1)^2*z^-1
#Calculate automorphism f^5=f^2(f^3)
x5:=x3*y3^2*z3^(-2);;
y5:=z3*y3;;
z5:=z3^2*y3;;
gap> x5; y5; z5;
x*y^2*z^-1*y^2*z*(z*y)^2
y^-1*(z^-1*y^-1*z^-1)^2*z^-1
((y^-1*z^-1)^2*z^-1)^2*y^-1*z^-2
#Calculate automorphism f^7=f^2(f^5)
x7:=x5*y5^(2)*z5^(-2);;
y7:=z5*y5;;
z7:=z5^2*y5;;
gap> x7; y7; z7;
x*y^2*z^-1*y*(y*z)^2*(z*y*z^2*y)^2*z*y
y^-1*((z^-1*y^-1*z^-1)^2*y^-1*z^-1)^2*z^-1*y^-1*z^-2
(((y^-1*z^-1)^2*z^-1)^2*y^-1*z^-2)^2*y^-1*(z^-1*y^-1*z^-1)^2*z^-1
```

Thus, the automorphism f^7 is

$$f^7 : F \mapsto F$$

$$x \mapsto xy^2z^{-1}y\left(yz\right)^2\left(zyz^2y\right)^2 zy,$$

$$y \mapsto y^{-1}\left(\left(z^{-1}y^{-1}z^{-1}\right)^2 y^{-1}z^{-1}\right)^2 z^{-1}y^{-1}z^{-2},$$

$$z \mapsto \left(\left(\left(y^{-1}z^{-1}\right)^2 z^{-1}\right)^2 y^{-1}z^{-2}\right)^2 y^{-1}\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1}.$$

Her public key is $c := f^7(a)$:

```
c:=x7^2*y7*z7^(-2)*y7;;
gap> c;
   (x*y^2*z^-1*y*(y*z)^2*(z*y*z^2*y)^2*z*y)^2*(z^2*y)^2*\
   ((z*y*z)^2*y*z)^2*z*y*z^2*y*z^-1
```

Bob is now able to send a message to Alice. Let $m = z^{-2}y^2zx^2y^{-1}x^{-1}$ be the message for Alice. He chooses the ephemeral key $t = 5$ and hence calculates the automorphism f^5 in GAP as follows:

```
m:=z^-2*y^2*z*x^2*y^-1*x^-1;;
#Calculate automorphism f^2=f^1(f^1)
x2:=x1*y1^2;;
y2:=z1^(-1);;
z2:=y1^(-1)*z1^(-1);;
gap> x2; y2; z2; x*y^2*z^-2 z*y z^2*y
#Calculate automorphism f^3=f^1(f^2)
```

```
x3:=x2*y2^2;;
y3:=z2^(-1);;
z3:=y2^(-1)*z2^(-1);;
gap> x3; y3; z3;
x*y^2*z^-1*y*z*y
y^-1*z^-2
(y^-1*z^-1)^2*z^-1
#Calculate automorphism f^5=f^2(f^3)
x5:=x3*y3^2*z3^(-2);;
y5:=z3*y3;;
z5:=z3^2*y3;;
gap> x5; y5; z5;
x*y^2*z^-1*y^2*z*(z*y)^2
y^-1*(z^-1*y^-1*z^-1)^2*z^-1
((y^-1*z^-1)^2*z^-1)^2*y^-1*z^-2
```

Hence, the automorphism f^5 is

$$f^5 : F \to F$$

$$x \mapsto xy^2z^{-1}y^2z\left(zy\right)^2,$$

$$y \mapsto y^{-1}\left(z^{-1}y^{-1}z^{-1}\right)^2 z^{-1},$$

$$z \mapsto \left(\left(y^{-1}z^{-1}\right)^2 z^{-1}\right)^2 y^{-1}z^{-2}.$$

He now calculates his ciphertext (c_1, c_2) for Alice with $c_1 = m \cdot f^5(c)$ and $c_2 = f^5(a)$ in GAP:

```
#c22:=f^5(c)
c22:=(x5*y5^2*z5^(-1)*y5*(y5*z5)^2*(z5*y5*z5^2*y5)^2*z5*y5)^2*\
(z5^2*y5)^2*((z5*y5*z5)^2*y5*z5)^2*z5*y5*z5^2*y5*z5^(-1);;
c1:=m*c22;;
gap> c1;
z^-2*y^2*z*x^2*(y*z^-1)^2*((z^-1*y^-1*z^-2*y^-1)^2\
*z^-2*y^-1)^2*(z^-1*y^-1*z^-1)^2*z^-1*y^-1*((((z^-\
1*y^-1*z^-1)^2*y^-1*z^-1)^2*z^-1*y^-1*z^-1*y^-1*z^\
-1)^2*(z^-1*y^-1*z^-2*y^-1)^2*z^-1*y^-1*z^-1)^2*((\
z^-1*y^-1*z^-2*y^-1)^2*z^-2*y^-1)^2*(z^-1*y^-1*z^-\
1)^2*z^-1*x*y^2*z^-1*y*(z^-1*(((z^-1*y^-1*z^-2*y^-\
1)^2*z^-2*y^-1)^2*(z^-1*y^-1*z^-1)^2*z^-1*y^-1)^3*\
(z^-1*y^-1*z^-1)^2*y^-1*z^-1*((z^-1*y^-1*z^-2*y^-1\
)^2*z^-2*y^-1)^2*(z^-1*y^-1*z^-1)^2*y^-1)^3*z^-1*(\
(z^-1*y^-1*z^-2*y^-1)^2*z^-2*y^-1)^2*(z^-1*y^-1*z^-1)^2*\
y^-1*z^-1*y
#c2:=f^5(a)
```

```
c2:=x5^2*y5*z5^(-2)*y5;;
gap> c2;
   (x*y^2*z^-1*y^2*z*(z*y)^2)^2*z^2*y*(z*y*z)^2*z*y*z^-1
```

Bob sends (c_1, c_2) to Alice. Alice gets the message m by calculating

$$m = c_1 \cdot \left(f^7 (c_2) \right)^{-1}.$$

In GAP she computes:

```
#dc:=f^7(c2)
dc:=(x7*y7^2*z7^(-1)*y7^2*z7*(z7*y7)^2)^2*z7^2*y7*\
(z7*y7*z7)^2*z7*y7*z7^(-1);;
gap> dc;
(x*y*(y*z^-1)^2*((z^-1*y^-1*z^-2*y^-1)^2*z^-2*y^-1\
)^2*(z^-1*y^-1*z^-1)^2*z^-1*y^-1*((((z^-1*y^-1*z^-\
1)^2*y^-1*z^-1)^2*z^-1*y^-1*z^-1*y^-1*z^-1)^2*(z^-\
1*y^-1*z^-2*y^-1)^2*z^-1*y^-1*z^-1)^2*((z^-1*y^-1*\
z^-2*y^-1)^2*z^-2*y^-1)^2*(z^-1*y^-1*z^-1)^2*z^-1)\
^2*y^-1*(((z^-1*y^-1*z^-1)^2*y^-1*z^-1)^2*z^-1*y^-\
1*z^-1*y^-1*z^-1)^2*(z^-1*y^-1*z^-2*y^-1)^2*z^-1*y\
^-1*z^-1*((((z^-1*y^-1*z^-2*y^-1)^2*z^-2*y^-1)^2*(\
z^-1*y^-1*z^-1)^2*z^-1*y^-1)^2*((z^-1*y^-1*z^-1)^2\
*y^-1*z^-1)^2*z^-1*y^-1*z^-2*y^-1)^2*(((z^-1*y^-1*\
z^-1)^2*y^-1*z^-1)^2*z^-1*y^-1*z^-1*y^-1*z^-1)^2*(\
z^-1*y^-1*z^-2*y^-1)^2*z^-1*y^-1*z^-1*y
gap> dc^-1;
y^-1*(((((z*y)^2*z)^2*z*y*z)^2*z*y*(z*y*z)^2)^2*z*\
y*((z*y*z)^2*y*z)^2*z*y*z)^2*(z*y*(((z*y*z)^2*y*z)\
^2*z*y*z*y*z)^2*(z*y*z^2*y)^2*z)^2*y*(((((z^2*y)^2\
*z*y)^2*z^2*y*z*y)^2*z*(z*y*z^2*y)^2*z*y)^2*z*(z*y\
*z^2*y)^2*z^2*y*(((z*y*z)^2*y*z)^2*z*y*z*y*z)^2*(z\
*y*z^2*y)^2*z*(z*y^-1)^2*y^-1*x^-1)^2
gap> c1*dc^-1;
   z^-2*y^2*z*x^2*y^-1*x^-1
```

Finally, she reconstructs the correct message

$$z^{-2} y^2 z x^2 y^{-1} x^{-1}.$$