A LINEAR TIME MATRIX KEY AGREEMENT PROTOCOL

by

Iris Anshel, Michael Anshel,
and Dorian Goldfeld

This Research supported by Arithmetica Inc.

PROTOCOL:

A multi–party algorithm, defined by a sequence of steps, specifying the actions required of two or more individuals in order to achieve a specified objective.

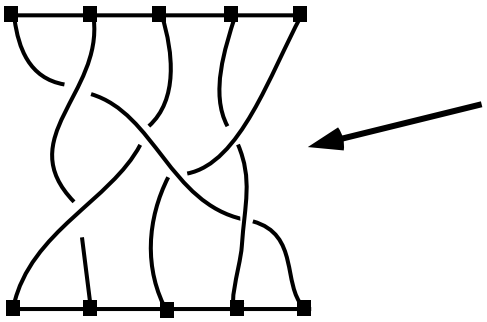
KEY ESTABLISHMENT PROTOCOL, (KAP):

A protocol whereby a shared secret becomes available to two or more individuals for further cryptographic applications.

We introduce BDH (Braid-Diffie–Hellman), a non–abelian KAP, for secret key establishment between two parties whose only means of communication is a public channel.

• BDH runs in linear time, providing a public key crypto system operating in linear time in the key length.

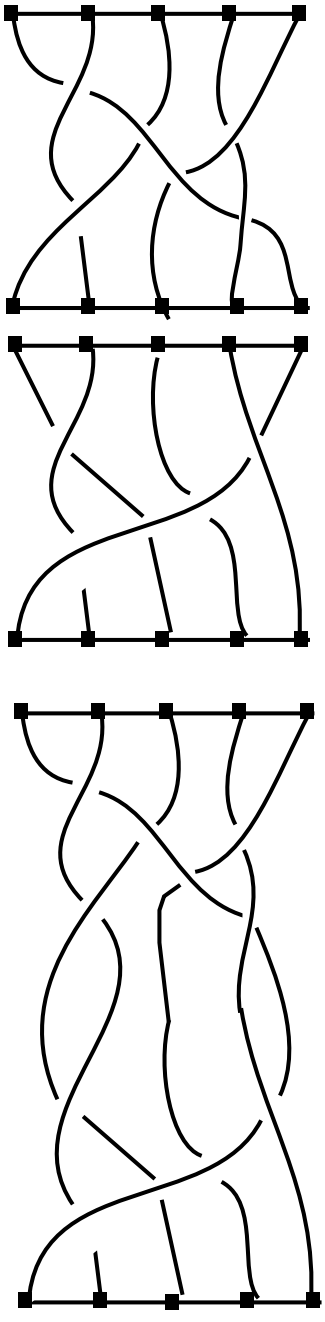
THE THEORY OF BRAIDS



A BRAID IS A WEAVING PATTERN BETWEEN 2 LINES. THE BRAID AT THE LEFT HAS 5 STRANDS AND 6 CROSSINGS.

Braids can be multiplied and divided, forming a mathematical group.

BRAID MULTIPLICATION



BRAID A

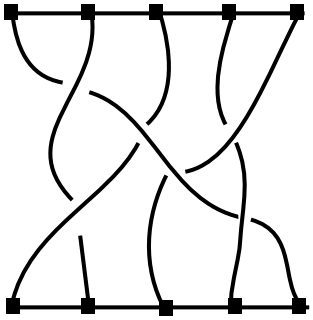
"times"

BRAID B

"equals"

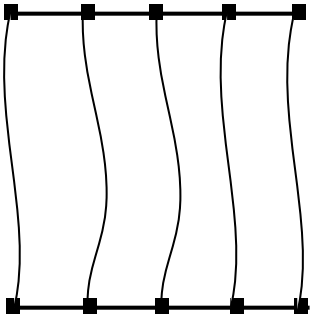
BRAID C

IDENTITY BRAID MULTIPLICATION



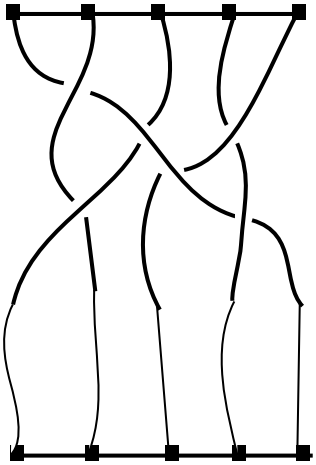
BRAID A

"times"



IDENTITY BRAID I

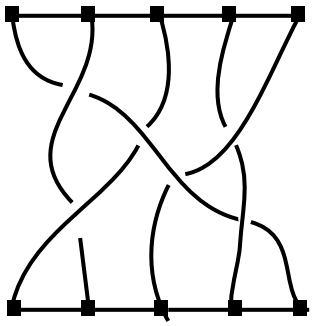
"equals"



BRAID A

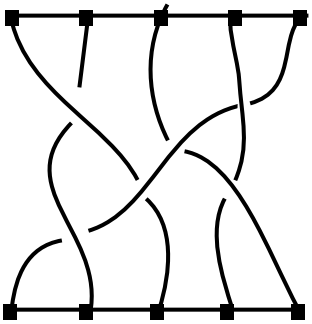
BRAID DIVISION

WE CAN ALSO PERFORM BRAID DIVISION WHICH IS THE INVERSE OF BRAID MULTIPLICATION. FOR EXAMPLE, THE INVERSE $\mathbf{A^{-1}}$ OF THE BRAID **A**



BRAID A

IS

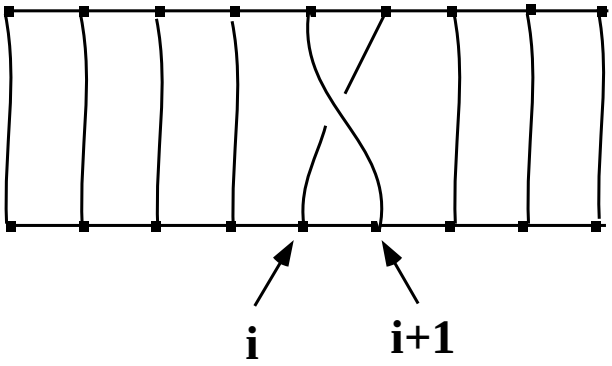


BRAID A^{-1}

$$\mathbf{A^* A^{-1} = I}$$

COMPUTER IMPLEMENTATION OF BRAID ARITHMETIC

LET $\mathbf{x_i}$ DENOTE THE BRAID BELOW:



THEN EVERY BRAID CAN BE EXPRESSED AS A PRODUCT OF THE $\mathbf{x_i}$'s.

IN THIS MANNER, THE ARITHMETIC OF BRAIDS CAN BE TRANSFORMED INTO THE MANIPULATION OF SYMBOLS SATISFYING CERTAIN RULES.

BACKROUND

Informally, a finitely presented group $\mathbf{G}$ is specified by a finite set of generators

$$g_1, g_2, \cdots, g_n$$

where every $g \in \mathbf{G}$ is a word in the generators and their inverses (product of g_i's and their inverses).

Further, there are finitely many words

$$r_1, r_2, \ldots, r_m$$

called relators and every r_i defines the identity element of $\mathbf{G}$. It is usual to suppress the trivial relations such as

$$g_i g_i^{-1} = g_i^{-1} g_i = e.$$

A presentation is written:

$$\langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m \rangle.$$

Braid Group Example:

Generators: $x_1, x_2, \ldots, x_N$.

Defining Relations:

$$x_i x_j = x_j x_i, \qquad \text{if } |j-i| \geq 2,$$

$$x_i x_j x_i = x_j x_i x_j, \quad \text{if } |i-j| = 1.$$

Colored Burau Matrix Group

B_N = braid group on N strands with $N-1$ Artin generators, $x_1, x_2, \ldots, x_{N-1}$.

Associated to each braid word $w \in B_N$ there is a unique

$(N-1) \times (N-1)$ matrix

depending on the variables $t_1, t_2, \ldots, t_{N-1}$.

Each Artin generator x_i maps to $(M_i(t_i), (i\ i+1))$ where

$$(i\ i+1)$$

denotes the transposition and

$$M_i(t_i) = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & t_i & -t_i & 1 \\ & & & & \\ & & & & 1 \end{pmatrix}$$

One checks that these elements obey the braid relations.

Definition: *The matrices*

$$M_1(t_1), \ldots, M_{N-1}(t_{N-1})$$

generate a group $\mathcal{M}_N$ *of matrices over* $\mathbb{Z}(t_1, \ldots, t_{N-1})$.

Definition: *We define*

$$\mathcal{C}_N = \mathcal{M}_N \rtimes S_N$$

(semi-direct product) to be the colored Burau matrix group.

Multiplication (denoted $*$) in $\mathcal{C}_N$ is defined as follows:

For $(M, \sigma),\ (M', \sigma') \in \mathcal{C}_N$,

$$(M,\, \sigma) * (M',\, \sigma') = \\ = (M \cdot \sigma(M'),\ \sigma\sigma').$$

Here $\sigma(M)$ is obtained from M by permuting the t_i in M via the permutation σ.

Let $w = x_{i_1} \cdot x_{i_2} \cdots x_{i_r}$ be a braid word in B_N. To compute the image of w in the colored Burau group one uses the following algorithm:

Initialization:

$$(m_1, \sigma_1) = \Big(M_{i_1}, (i_1\ i_1 + 1)\Big) * \Big(M_{i_2}, (i_2\ i_2 + 1)\Big)$$

Do Loop: $(j = 2, \ldots, r-1)$

$$(m_j, \sigma_j) = \Big(m_{j-1},\ \sigma_{j-1}\Big) * \Big(M_{i_{j+1}},\ (i_{j+1}\ \ i_{j+1}+1)\Big)$$

$$= \Bigg(m_{j-1} \cdot \sigma_{j-1}\Big(M_{i_{j+1}}\Big),\ \sigma_{j-1} \cdot (i_{j+1}\ \ i_{j+1}+1)\Bigg)$$

Remarks:

• The colored Burau algorithm can be speeded up further by reducing $\pmod{p}$ and letting $\{t_1, \ldots, t_{N-1}\}$ denote distinct and invertible integers $\pmod{p}$.

• This algorithm runs in linear time in the word length.

The most expensive operations in this algorithm are:

- *applying a permutation: i.e., replacing one element of a list by another,*

- *multiplying a matrix in $\mathbb{F}_p$ with a row vector of 3 entries.*

Theorem: *The running time to compute the image of a braid word* $w \in B_N$ *of length* ℓ *(in Artin generators) in the colored Burau group* $\mathcal{C}_N$ *reduced (mod* p*) is* $\mathcal{O}\big(N \log_2(p) \cdot \ell\big)$.

The Key Extractor E_p

A **keyspace** K of order k is a collection of bit strings (keys) each of length at most k.

We introduce the keyspace

$$\boxed{K_{N,p} = \big\{(M, \sigma)\big\}}$$

of order $\mathcal{O}\big(N^2 \log_2(p)\big)$ where $M = {}_{(N-1)\times(N-1)}$ matrix over $\mathbb{F}_p$ and $\sigma \in S_N$.

Definition: *A key extractor on a group G is a function $G \to K$, where K is a keyspace.*

Fix : $N \geq 6$, $p > N$ (a prime) and $\tau_1, \ldots, \tau_{N-1}$ distinct and invertible integers $\pmod{p}$.

Definition: *We define the key extractor* $E_{N,p} : \mathcal{C}_N \to K_{N,p}$ *given by setting* $t_1 = \tau_1, \ldots,$ $t_{N-1} = \tau_{N-1}$ *and reducing* (mod p).

Remarks: We believe $E_{N,p}$ to be a one–way function. It can be used to very efficiently extract keys in braid group cryptosystems.

The Left Multiplication $\bullet$

We shall introduce a left multiplication $\bullet$, which allows us to multiply an element in $K_{N,p}$ by an element in $\mathcal{C}_N$ where the element in $\mathcal{C}_N$ is on the right.

Set $\overrightarrow{\tau} = \{\tau_1, \ldots, \tau_{N-1}\}$.

Definition:

$$(M(\overrightarrow{\tau}) \pmod p, \sigma) \bullet (M', \sigma') = (M^*, \sigma\sigma')$$

where

$$M^* = \Big(M \cdot \sigma\,(M')\Big)(\overrightarrow{\tau}) \pmod p.$$

Remarks: The left multiplication $\bullet$ is associative and can be computed in linear time.

BDH (Braid–Diffie–Hellman)

PUBLIC INFORMATION:

- $N \geq 6,\ p > N.$
- $\tau_1, \ldots, \tau_{N-1} \pmod{p}.$
- $U, V \leq B_N$ (commuting subgroups).
- The keyspace $K_{N,p}$, a homomorphism $h : B_N \to \mathcal{C}_N$.
- $(M, \sigma) \in K_{N,p}.$

SECRET KEYS :

- Alice chooses $\alpha \in U$, Bob chooses $\beta \in V$, $(\alpha\beta = \beta\alpha)$.

PUBLIC KEYS :

Alice computes $(M, \sigma) \bullet h(\alpha)$.

Bob computes $(M, \sigma) \bullet h(\beta)$.

SHARED SECRET :

$\big((M, \sigma) \bullet h(\alpha)\big) \bullet h(\beta)$.

Choice of Commuting subgroups U, V

It is necessary that for $\alpha \in U$, $\beta \in V$ where

$$h(\alpha) = (M_\alpha, \sigma_\alpha),$$

$$h(\beta) = (M_\beta, \sigma_\beta),$$

that σ_β does not act trivially (or close to trivially) on M_α and σ_α does not act trivially on M_β.

Example of U, V

$$N \equiv 1 \pmod 2,\ m = \tfrac{N-1}{2}$$

$$B_N = \langle x_1, x_2, \ldots, x_{N-1} \rangle$$

$$H_L = \langle x_1, \ldots, x_{m-1} \rangle$$

$$H_R = \langle x_{m+1}, \ldots, x_{N-1} \rangle$$

$$\boxed{U = wH_Lw^{-1}}$$

$$\boxed{V = wH_Rw^{-1}}$$

Remark: If h is the natural homomorphism where each Artin generator x_i maps to:

$$\big(M_i(t_i),\ (i\ i+1)\big),$$

then the total running time for BDH is

$$\mathcal{O}(N \log_2(p) \cdot \ell)$$

where ℓ is the maximum word length of the secret keys α, β.

Security Issues

The security of BDH is tied to the difficulty of inverting the key extractor $E_{N,p}$. There are several reasons to believe that this is a one–way function.

- $E_{N,p}$ is not a homomorphism.

- The representation

$$B_N \to \mathcal{C}_N$$

induces a representation of rank $> N \cdot (N+1)!$. This rank is so large it appears infeasible to attack the system by methods of linear algebra.

There will be a class of weak keys arising from elements

$$w \in B_N$$

whose associated permutations are close to the identity. For these elements, the application of $E_{N,p}$ will not produce enough permutations to guarantee the security of the system.

It is important that the public key

$$(M, \sigma) \in K_{N,p}$$

be the image of a braid word w (under the map $E_{N,p}$) where the word w is sufficiently long and involves all of the Artin generators.