Ein gruppentheoretischer Schlüsselaustausch

Tobias Gehroldt
17. 7. 2007

Voraussetzungen

Man benötigt eine Gruppe G, mit entweder zwei großen Untergruppen $A, B \leq G$, die elementweise kommutieren ($\forall\, a \in A\ \forall\, b \in B\ :\ ab = ba$), oder einer großen kommutativen Untergruppe $A \leq G$.

Groß genug soll hierbei heißen, dass man zufällig Elemente aus A (oder B) wählen kann.

Prinzip des Schlüssel-Transports

Alice	**öffentlich**	**Bob**
wählt $k \in G$ und $a_1, a_2 \in A$		wählt $b_1, b_2 \in B$
$p_1 := a_1 \cdot k \cdot a_2$	$\longrightarrow p_1$	
	$p_2 \longleftarrow$	$p_2 := b_1 \cdot p_1 \cdot b_2$
$p_3 := a_1^{-1} \cdot p_2 \cdot a_2^{-1}$	$\longrightarrow p_3$	
		$p_4 := b_1^{-1} \cdot p_3 \cdot b_2^{-1}$

Damit ist

$$p_4 = b_1^{-1} \cdot \underline{a_1^{-1} \cdot b_1} \cdot a_1 \cdot k \cdot a_2 \cdot \underline{b_2 \cdot a_2^{-1}} \cdot b_2^{-1} = \underline{b_1^{-1} \cdot b_1} \cdot \underline{a_1^{-1} \cdot a_1} \cdot k \cdot \underline{a_2 \cdot a_2^{-1}} \cdot \underline{b_2 \cdot b_2^{-1}} = k$$

Freie Gruppen

Definition: Eine Gruppe G heißt *freie Gruppe*, wenn sie eine Teilmenge S besitzt, so dass sich jedes Element von G eindeutig (bis auf Kürzen von benachbarten Paaren von Inversen) als Produkt von endlich vielen Elementen aus S und deren Inversen darstellen läßt. Man schreibt: $G = F(S)$.

Definition: Hat die Basis S gerade n Elemente, so heißt $F(S) =: F_n$ *freie Gruppe vom Rang n*.

Bemerkung: F_n ist bis auf Isomorphie eindeutig.

Beispiel: F_1 ist isomorph zu den ganzen Zahlen.

Vom Klartext zum Gruppenelement...

Sei $G = F(x_1, \ldots, x_n)$ und $U = F(W_1, W_2, W_3, \ldots) \leq G$ eine freie Untergruppe ($W_i \in G$). Die W_i können als Wörter (Produkte) aus den erzeugenden Elementen aufgefasst werden, also $W_i = W_i(x_1, \ldots, x_n)$. Dann kann man die einzelnen Zeichen eines Klartext-Alphabets $\{a, b, c, \ldots\}$ auf die W_i abbilden, etwa: $a \mapsto W_1,\ b \mapsto W_2,\ c \mapsto W_3, \ldots$

Mit dieser Abbildung erhält man aus einem Klartext-Wort durch Hintereinanderschreiben wiederum ein Wort aus den erzeugenden Elementen und damit ein Element aus G, zum Beispiel:
"abc" $\mapsto\ W(W_1, W_2, W_3) \in G$

...und zurück

Nach der Entschlüsselung muss man aus dem Element aus G wieder auf die Darstellung als Wort aus den Wörtern $W_1, W_2, W_3, \ldots$ schließen können (um daraus wieder auf die Klartext-Zeichen schließen zu können). Dies ist möglich, da jedes Element aus U eine eindeutige solche Darstellung besitzt, etwa mit Hilfe des Umschreibe-Algorithmus' nach Reidemeister-Schreier.

Beispiel: Automorphismengruppe der freien Gruppe vom Rang n

Sei $G := Aut(F_n)$, etwa mit $n \geq 5$.

Der Schlüssel ist dann eine Abbildung $k : F_n \to F_n$. Klartext und Chiffretext sind Elemente aus F_n. Es gibt eine große Auswahl an Untergruppen $A, B \leq Aut(F_n)$, die elementweise kommutieren. Beispiel für $F_n = F(x_1, \ldots, x_n)$: Sei A die Untergruppe, die x_1, x_2, x_3 fest lässt und B die Untergruppe, die $x_4, \ldots, x_n$ fest lässt.

Beispiel: Ganzzahlige invertierbare 4×4-Matrizen

Sei $G := SL_4(\mathbb{Z})$.

Der Schlüssel ist eine ganzzahlige invertierbare 4×4-Matrix. Als elementweise kommutierende Untergruppen benutzt man
$A := \begin{pmatrix} SL_2(\mathbb{Z}) & 0 \\ 0 & I_2 \end{pmatrix}$ und $B := \begin{pmatrix} I_2 & 0 \\ 0 & SL_2(\mathbb{Z}) \end{pmatrix}$, konjugiert mit einer (festen) Matrix $M \in SL_4(\mathbb{Z})$.

Freies Produkt

Definition: Seien G_1, G_2 (beliebige) Gruppen. Dann enthält $G := G_1 * G_2$, das *freie Produkt* von G_1 und G_2, genau die Wörter, in denen Elemente aus $G_1 \setminus \{e\}$ und Elemente aus $G_2 \setminus \{e\}$ alternieren. Die Operation auf G ist das Hintereinanderschreiben, wobei "gekürzt" wird, falls zwei Elemente aus der gleichen Gruppe hintereinander stehen. Neutrales Element ist das leere Wort.

Beispiel: Freies Produkt zweier freier Gruppen

Seien G_1, G_2 freie Gruppen und $U_1 \leq G_1$, $U_2 \leq G_2$ (beliebige, aber nicht zyklische) Untergruppen, die elementweise kommutieren. Sei nun $G := G_1 * G_2$.