

Hochsicherheits-Generalschlüssel Marke Eigenbau

Michael Weiner¹ RFguy^{1,2}

¹Chaos Computer Club München e.V.

²Sportsfreunde der Sperrtechnik – Deutschland e.V.

29.12.2016



Outline

- 1 Einführung
- 2 KESO 2000
- 3 EVVA 3KS
- 4 3KS-Schlüssel fräsen
- 5 Zusammenfassung

- Nichtkommerziell, z.B.

- Teleaufnahmen von Schlüsseln
- 3D-Modelle von TSA-Keys
- Erstellen von Rohlingen aus Fotos von Schlossern und 3D-Druck von Zackenschlüsseln
- Untersuchung von EVVA MCS

- Kommerziell, z.B.

- EasyEntry-Profilfräse (8000 € - 10000 €)
- Schlüsselfräsen (4000 € - 20000 €)
- InstaCode Schlüsseldatenbank und Ansteuerung von Schlüsselfräsen

Funktionsweise

Überblick



Codierung über Bohrmulden im Schlüssel

- zwei Reihen
- Kante

Funktionsweise

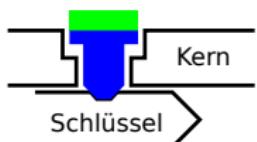
Abtastung der Bohrmulden

- ein Schließzylinder tastet pro Reihe fünf Bohrmulden in gleichem Abstand ab
- Schlüssel haben pro Reihe bis zu 10 Bohrmulden
- ein Schließzylinder kann nur jede zweite Bohrulde abtasten
- Stifte im Schließzylinder können aufgrund der geringen Bauhöhe **nur eine gültige Position** haben

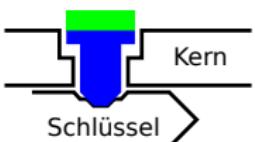


Funktionsweise

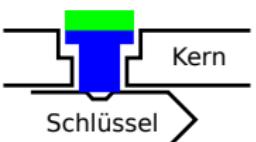
Stifttypen



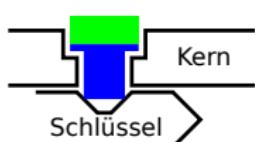
**Standardstift,
Standardbohrung**



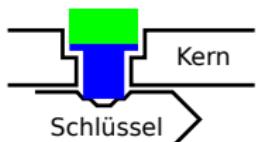
**Standardstift,
Stufenbohrung**



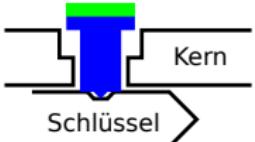
**Flachstift,
kleine Standard-
bohrung**



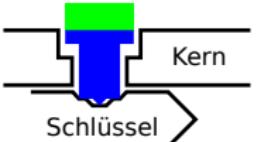
**Flachstift,
tiefe Standard-
bohrung**



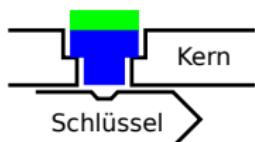
**Flachstift,
Stufenbohrung**



**Stufenstift,
Standard-
bohrung**



**Stufenstift,
Stufen-
bohrung**



Blindstift

Allgemeines

- Annahme: Zugang zu einigen verschiedenen Schlüsseln/Schließzylindern der gleichen Anlage ist vorhanden

Allgemeines

- Annahme: Zugang zu einigen verschiedenen Schlüsseln/Schließzylindern der gleichen Anlage ist vorhanden
- Ziel: Bestimmung eines Schließcodes, der alle zugänglichen Schließzylinder öffnet (und womöglich mehr)

Allgemeines

- Annahme: Zugang zu einigen verschiedenen Schlüsseln/Schließzylindern der gleichen Anlage ist vorhanden
- Ziel: Bestimmung eines Schließcodes, der alle zugänglichen Schließzylinder öffnet (und womöglich mehr)
- Frage: Wie kann man diesen Schließcode möglichst eindeutig und mit wenig Aufwand bestimmen?

Allgemeines

- Annahme: Zugang zu einigen verschiedenen Schlüsseln/Schließzylindern der gleichen Anlage ist vorhanden
- Ziel: Bestimmung eines Schließcodes, der alle zugänglichen Schließzylinder öffnet (und womöglich mehr)
- Frage: Wie kann man diesen Schließcode möglichst eindeutig und mit wenig Aufwand bestimmen?
- Grundsätzlich kann man als Informationsquelle nutzen
 - Schlüssel
 - Schließzylindern
- Was ist besser und wie geht man vor?

Allgemeines

- Annahme: Zugang zu einigen verschiedenen Schlüsseln/Schließzylindern der gleichen Anlage ist vorhanden
- Ziel: Bestimmung eines Schließcodes, der alle zugänglichen Schließzylinder öffnet (und womöglich mehr)
- Frage: Wie kann man diesen Schließcode möglichst eindeutig und mit wenig Aufwand bestimmen?
- Grundsätzlich kann man als Informationsquelle nutzen
 - Schlüssel
 - Schließzylindern
- Was ist besser und wie geht man vor?
 - hängt von der Bauart der Schließanlage ab

Schlüssel vs. Schloss

- Schlüssel als Informationsquelle
 - enthalten die Vereinigungsmenge der Bohrungen für alle Schließzylinder, für die sie berechtigt sind
- Schließzylinder als Informationsquelle
 - Informationsgewinn beschränkt sich auf untersuchten Schließzylinder

Dekodieren

Beispiel

Schlüssel 1**Gesamt**

Einführung



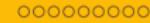
KESO 2000



EVVA 3KS



Fräsen



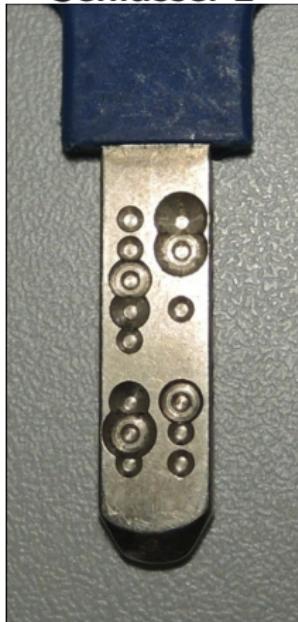
Zusammenfassung



Dekodieren

Beispiel

Schlüssel 2



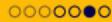
Gesamt



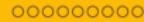
Einführung



KESO 2000



EVVA 3KS



Fräsen



Zusammenfassung



Dekodieren

Beispiel

Schlüssel 3



Gesamt



Beispiel - Seite

Gleiches Vorgehen für die Kante



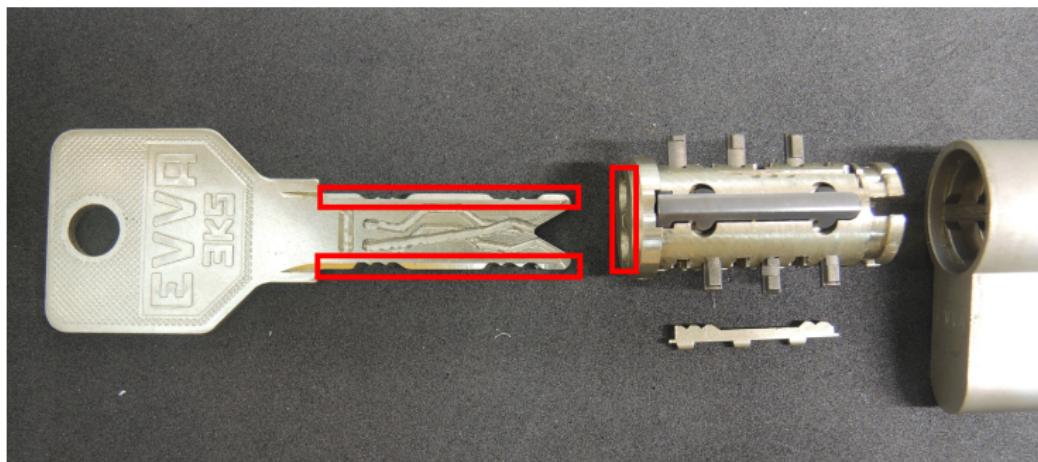
Funktionsweise

Übersicht



Funktionsweise

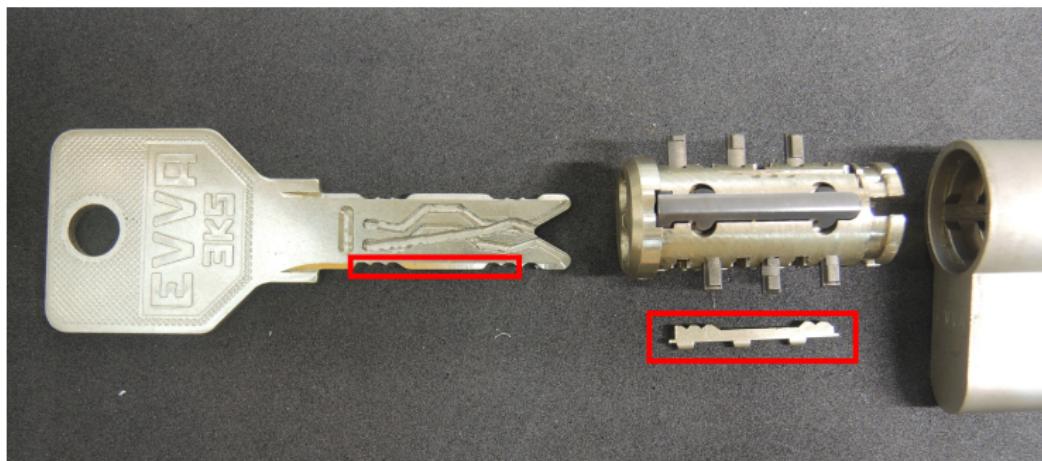
Übersicht



- Längskerben

Funktionsweise

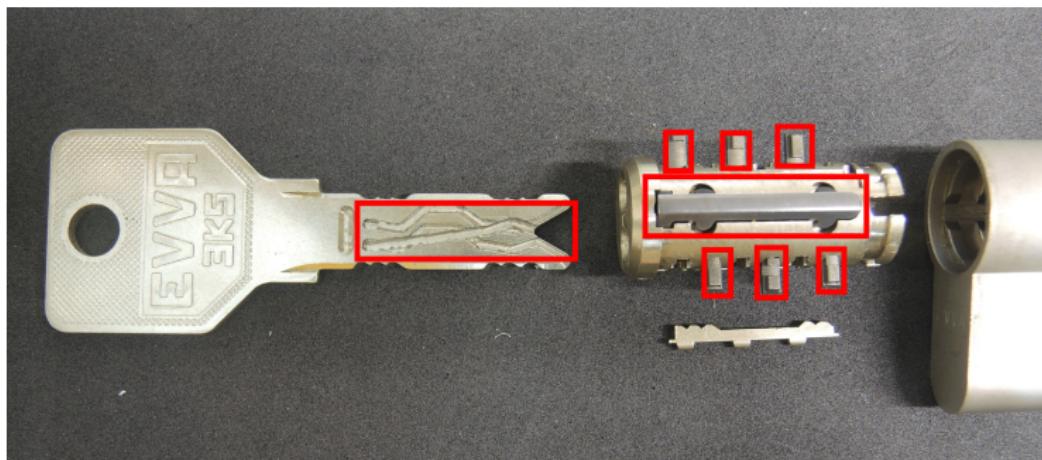
Übersicht



- Längskerben
- Sidebar-Code (passiv)

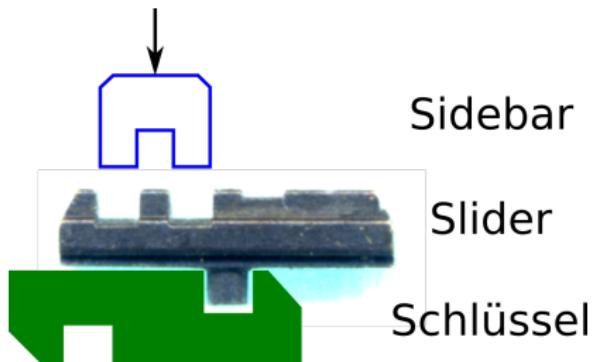
Funktionsweise

Übersicht



- Längskerben
- Sidebar-Code (passiv)
- Kurven (aktive Sidebar)

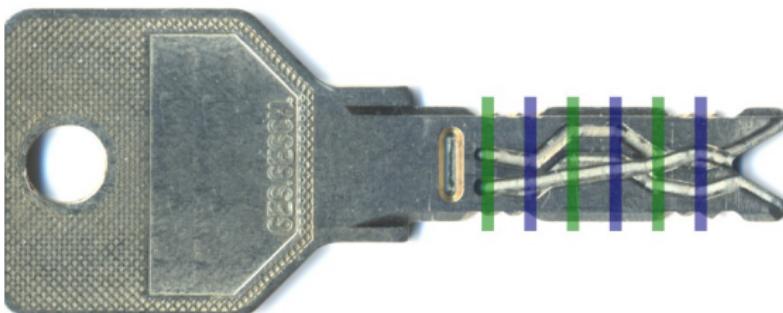
Kurven: Funktionsprinzip



- Slider wird durch Kurve im Schlüssel positioniert
- Beim Drehen wirkt eine Kraft auf die Sidebar, die diese nach unten drücken will
- Nur möglich, wenn der Slider an der richtigen Position eine Aussparung hat

Funktionsweise

Kurven: gemeinsame Eigenschaften



- sechs Abtastpositionen, Abstand 3.5mm
- Codeabstand 0.5mm
- Breite der Kurve 1.2mm
- abwechselnde Abtastung von Einzel- und Doppelkurve

Funktionsweise

Doppelkurve

- sieben mögliche Positionen
- Tiefe: 0.5mm
- “globale” Konfiguration
ändert sich nur bei großen Schließanlagen
bei hohen Hierarchieebenen
bzw. bei Eigenprofilen
- vorgeschlagene Notation:
 $d + v.o.n.u.$ $\{1, 2, \dots, 7\}$
- 3KS Plus:
Schieber an Position 6 dicker
und um halbe Position versetzt
- 4KS: Kurve beginnt erst an
Position 2



d327732

Funktionsweise

Einzelkurve

- neun mögliche Positionen
- Tiefe: 1.0mm
- "lokale" Konfiguration
- vorgeschlagene Notation:
 $s + v.o.n.u. \{1, 2, \dots, 9\}$
- 4KS: Kurve an Position 6 dicker
(und möglicherweise auch versetzt)

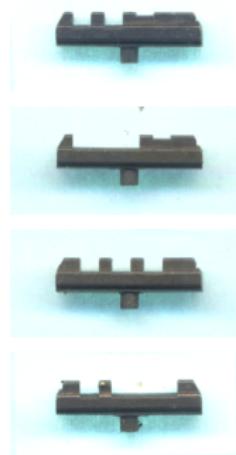


s123457

Funktionsweise

Slider-Zoo

Einzelkurve



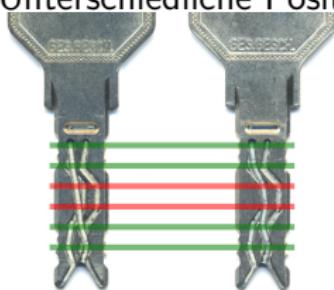
(spiegelverkehrt dargestellt)

Doppelkurve



• Schlüssel als Informationsquelle

- Überall gleiche Positionen liefern keine Information über die Generalschließebene
- Unterschiedliche Positionen schränken den Suchraum **nicht** ein



Vergleich der Einzelkurven: Mittlere beide Positionen stimmen nicht überein

• Schließzylinder als Informationsquelle

- jedes Schloss liefert alle gültigen Schließcodes
- deren Schnittmenge ergibt den General-Schließcode

Dekodieren

3KS: Beispiel

Zylinder 1



Dieser Zylinder:

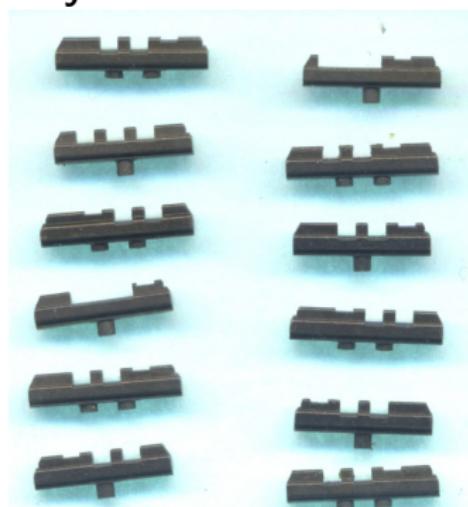
- d327732
- s [123] [2678] [345] [48] 57

Gesamt:

- d327732 (done!)
- s [123] [2678] [345] [48] 57
- ⇒ 72 verbleibende Kombinationen

3KS: Beispiel

Zylinder 2



Dieser Zylinder:

- d327732
- s [123] [26] 5 [456] 5 [37]

Gesamt:

- d327732
- s [123] [26~~78~~] [345] [4~~8~~] 57
- ⇒ 6 verbleibende Kombinationen

3KS: Beispiel

Zylinder 2



Dieser Zylinder:

- d327732
- s [123] [26] 5 [456] 5 [37]

Gesamt:

- d327732
- s [123] [26] 5457
- ⇒ 6 verbleibende Kombinationen

3KS: Beispiel

Zylinder 3



Dieser Zylinder:

- d327732
- s3[45678]5[456]5[37]

Gesamt:

- d327732
- s[123][26]5457
- sind wir...?

Dekodieren

3KS: Beispiel

Zylinder 3



Dieser Zylinder:

- d327732
- s3[45678]5[456]5[37]

Gesamt:

- d327732
- s365457
- **wir sind fertig!**

3KS: Beispiel – Vergleich mit Original-GHS



Hardware

CNC-Fräse/Graviermaschine



“China” CNC6040Z-S80 (ca. 1500 €)

- 50 µm Wiederholgenauigkeit
- benutzbarer Bereich 580mm x 400mm

CAD-Software

- OpenSCAD

- Eingabe: Textbasierte Beschreibung von 3D-Modellen
- Ausgabe: z.B. STL oder DXF (nur eine Ebene)
- quelloffen

- Inkscape

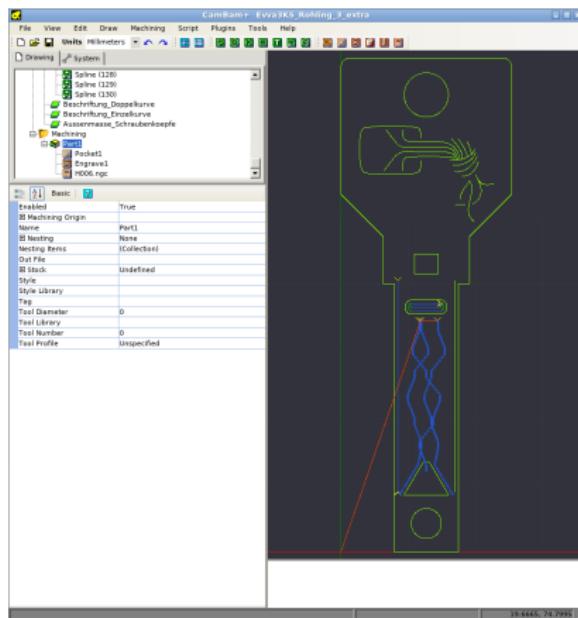
- Eingabe: 2D-Vektorzeichnung
- Ausgabe: z.B. DXF

CAM-Software

- CamBam

- Eingabeformat: DXF
- Ausgabe: G-Code
- closed source,
kommerziell,
aber kostenfreie Lizenzen
für Hackerspaces
auf Anfrage

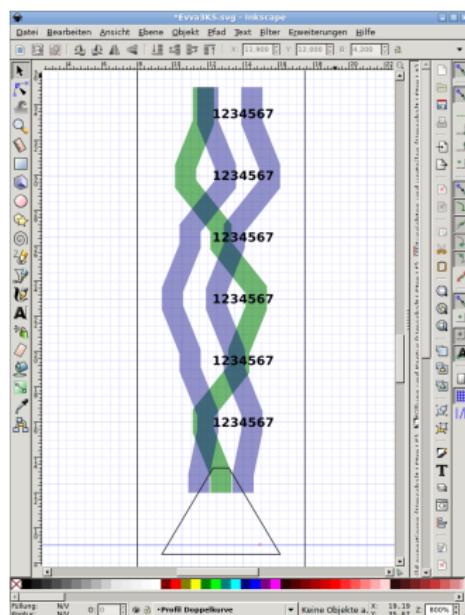
- Python



Software-Workflow

Software-Workflow 1.0

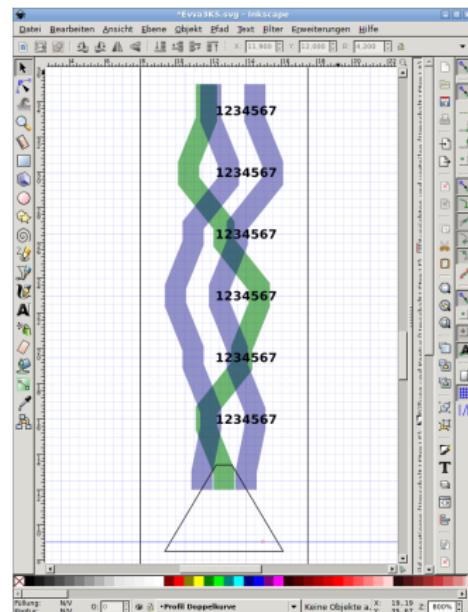
- ① Inkscape:
Vorlage-Kurven an Gitter ausrichten
- ② CamBam:
CNC-Parameter konfigurieren
- ③ LinuxCNC: kalibrieren, fräsen



Software-Workflow

Software-Workflow 1.0

- ① Inkscape:
Vorlage-Kurven an Gitter ausrichten
- ② CamBam:
CNC-Parameter konfigurieren
- ③ LinuxCNC: kalibrieren, fräsen
zeitaufwendig



Software-Workflow

Software-Workflow 2.0

Kann man die Erstellung des Werkzeugpfads für die Kurven automatisieren?

- Inkscape und CamBam skripten
- eigenen G-Code-Generator schreiben

Software-Workflow

Software-Workflow 2.0

Kann man die Erstellung des Werkzeugpfads für die Kurven automatisieren?

- Inkscape und CamBam skripten
- eigenen G-Code-Generator schreiben

DEMO

Anfangsfragen

- Wie kann man Schlüsselrohlinge genau genug positionieren?
- Wie kann man beidseitig fräsen?
- Welches Material verwendet man?
- Wie weit kann man das Fräsen automatisieren?

Hardware-Workflow

Positionierung der Rohlinge

- Freies Einspannen?
 - Erfordert Kalibrierung von X, Y, Z und Rotation
- Einspannvorrichtung
 - Schlüssel soll parallel zur Y-Achse ausgerichtet sein
 - Material: elektrisch nicht leitend, um antasten zu können
 - zwei unabhängige Fixierungen
 - Fräse <=> Einspannvorrichtung
 - Einspannvorrichtung <=> Rohling

Hardware-Workflow

Mit Halterung?

Anschlag_Wendeschlüssel.scad — OpenSCAD

```
79 L
80 //layer==2;
81
82 if(layer==1)
83 {
84     projection(cut=true) difference()
85     {
86         translate([0,0,-
87 hexagon_depth-delta]) anschlag(
88 plot_hexagon=true);
89         translate([0,0,-
90 hexagon_depth+delta]) anschlag(
91 plot_hexagon=true);
92     }
93 else if(layer==2)
94 {
95     projection(cut=true) difference()
96     {
97         translate([0,0,-
98 bottom_depth-delta]) anschlag(
99 plot_hexagon=false);
100        translate([0,0,delta])
101 anschlag(plot_hexagon=false);
102    }
103
104 translate([0,0,-hexagon_depth])
105 anschlag();
```

The screenshot shows the OpenSCAD software interface. On the left is the code editor with the script 'Anschlag_Wendeschlüssel.scad'. The main window displays a 3D rendering of a mechanical part, which is a rectangular block with two hexagonal holes on top and a central slot. A coordinate system (x, y, z) is shown at the bottom left. At the bottom of the screen, there is a toolbar with various icons for file operations, zooming, and selection.

Ansch: Verschiebung = [0.04 121.70 3.62], Rotation = [82.30 0.00 197.90], Abstand = 140.00

OpenSCAD 2015.03

Hardware-Workflow

Hardware-Workflow



- ① Rohlinge fräsen oder lasercutten
- ② Kurven, Seitenkerben und Längskerben fräsen
- ③ untere Halterung des Rohlings entfernen, entgraten

Nächste Schritte

Nächste Schritte

- Automatisierungsgrad erhöhen
 - Vierte Achse zum automatischen Wenden
 - Optimiertes Antasten, etc
- Weitere Schließsysteme fräsen
 - 3KS Plus, 4KS
 - Zackenschlüssel



Michael Weiner michi@muc.ccc.de
Jan Morawek RFguy@muc.ccc.de

Danke auch an Laura Eckardt und Maurice Massar