Angewandte Kryptographie
SoSe 2016

Prof. Dr.-Ing. Kerstin Lemke-Rust
Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 3

C.1 In dieser Aufgabe wird eine weitere Variante eines künstlich abgeschwächten A5/1 eingeführt: Ein Geffe-Generator auf Basis der LFSRs des A5/1. Die Veränderungen des A5/1 sind wie folgt:

- Die irreguläre Taktung mit den Taktkontrollbits ist komplett deaktiviert.
- Die Kombinationsfunktion der drei Ausgangsbits x_1 von R1, x_2 von R2 und x_3 von R3 lautet jetzt $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$.

In dieser Aufgabe soll der "Divide-and-Conquer"-Korrelationsangriff auf einen Geffe-Generator praktisch durchgeführt werden. Hierzu liegt in LEA der Sourcecode a51_geffe.c, der den Geffe-Generator auf der Basis des A5/1 implementiert. (Gegenüber dem Orignal-Sourcecode a51.c von `http://www.scard.org/gsm/a51.html`, den Sie auch in LEA finden, sind alle Modifikationen durch "modified" gekennzeichnet). Mit demselben Sourcecode a51_geffe.c, aber mit einem anderen 64-bit Schlüssel (Variable key in der Funktion test()) sind die folgenden Ausgabewerte erzeugt worden (ebenfalls in Datei output.txt in LEA):

```
A->B: 0x0136BB69518021224FFD5EC4008340
B->A: 0x3E8286EB1C15AF1563172919CF91C0
```

Bestimmen Sie den internen Zustand der LFSR R1, R2 und R3 nach abgeschlossenem Key-Setup (Ende der Funktion keysetup()). Gehen Sie hierfür wie folgt vor.

(a) Bestimmen Sie den Inhalt des LFSR R1 durch eine Korrelationsattacke. (Hinweise: Anstelle der Berechnung des Korrelationskoeffizienten können Sie auch die Bits zählen, die bei der Ausgabe von R1 und den obigen Ausgabewerten übereinstimmen. Die oben gegebenen Ausgabewerte A->B:... und B->A:... können Sie für die Korrelationsattacke konkatenieren.)

(b) Bestimmen Sie den Inhalt des LFSR R3 analog wie bei R1 durch eine Korrelationsattacke.

(c) Im letzten Schritt bestimmen Sie den Inhalt des LFSR R2 durch Brute-Force.