

Moderne Kryptosysteme

GSM/GPRS

Gordon Kunkel

30. Juli 2006

Inhaltsverzeichnis

1	Global System for Mobile Communications	2
1.1	GSM-Netzarchitektur	3
1.2	Übertragung auf der Luftschnittstelle	5
1.2.1	GSM-Rahmenstruktur	6
2	Kryptographie	6
2.1	Authentifizierung	7
2.1.1	COMP128(A3/A8)	7
2.2	Gesprächsverschlüsselung(A5)	9
2.2.1	Der A5/1-Algorithmus	10
2.3	Andere bekannte Verfahren	11

1 Global System for Mobile Communications

Der GSM-Standard ist der Nachfolger der analogen Systeme (z.B. C-Netz¹ in Westdeutschland, NMT 450² in Nordeuropa/Benelux-Ländern, TACS³ in Großbritannien, Radiocom 2000 in Frankreich und RTMI/RTMS⁴ in Italien) der deren Nachteil, der untereinander fehlenden Kompatibilität, durch Einführung eines einheitlichen Standards löst. Außerdem sollte das GSM-Netz vollständig kompatibel zu herkömmlichen Telefonnetzen und ISDN⁵ sein. Nach dem Testbetrieb seit Mitte 1991 begann der offizielle Start in Deutschland 1992. Der GSM-Standard kommt heute in 670 Mobilfunknetzen in circa 200 Ländern zum Einsatz, das entspricht 78 Prozent aller Mobilfunkkunden. Die Anzahl der GSM-Nutzer betrug im März 2006 1,7 Milliarden, die zur Zeit aus etwa 1700 Handymodellen auswählen können. Täglich kommen eine Millionen Neukunden besonders aus Afrika, Indien, Lateinamerika und Asien dazu. 277 Milliarden US-Dollar betrug der Umsatz mit GSM-Technik im Jahr 2003.⁶

¹zellulares Mobilfunknetz der deutschen DeTeMobil (früher Deutsche Bundespost TELEKOM)

²Nordic Mobile Telephone

³Total Access Communication System

⁴Radio Telefono Mobile Integrato/repetitive TMS (Transcranial magnetic stimulation)

⁵Integrated Services Digital Network

⁶Umsatzangaben von der Deutschen Bank

1.1 GSM-Netzarchitektur

Das GSM-Netz gehört zu der Klasse der zellularen Mobilfunknetze, deren Bestandteile im folgenden näher erläutert werden und in Abbildung 1 zu sehen sind⁷:

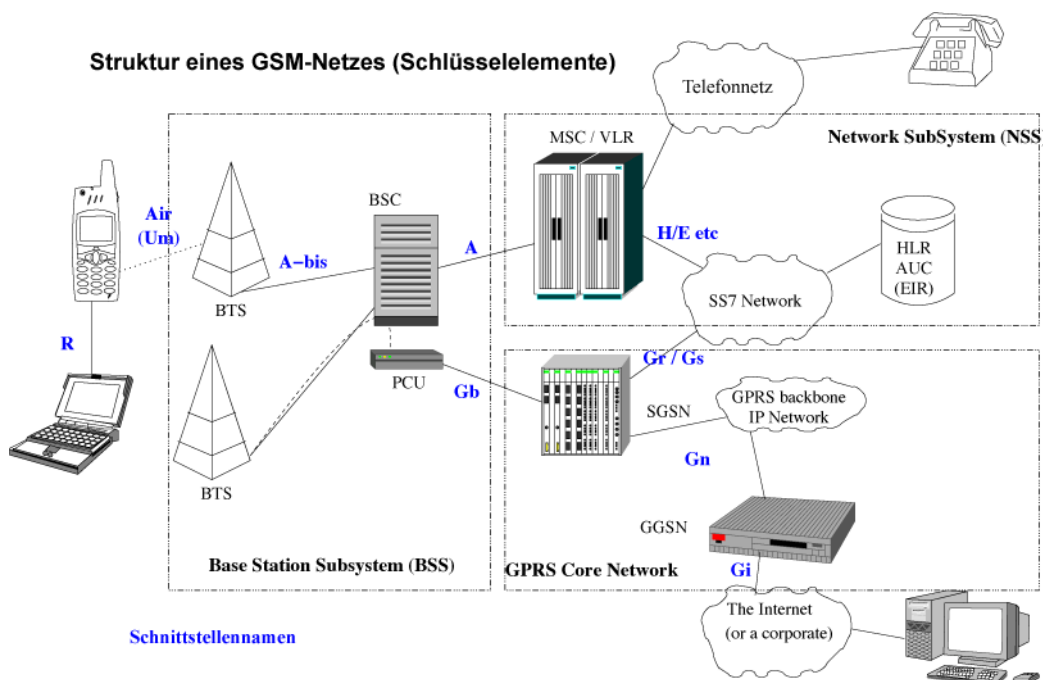


Abbildung 1: Aufbau eines GSM-Netzes

Mobile Station (MS): Das GSM-Mobiltelefon ist zweigeteilt, es besteht aus dem Mobilfunkgerät selbst und der Benutzeridentitätskarte, dem SIM⁸. Das Mobilfunkgerät besitzt eine internationale Geräteerkennung, die IMEI⁹. Die auf der SIM-Karte gespeicherte IMSI¹⁰ ist die Kundennummer und identifiziert den Nutzer. Die kryptographischen Algorithmen für Authentifizierung und Verschlüsselung der Nutzdaten befinden sich ebenfalls auf der SIM-Karte.

⁷Abbildung 1 unterliegt der GNU-Lizenz für freie Dokumentation http://upload.wikimedia.org/wikipedia/de/4/46/Gsm_netzwerk.png

⁸Subscriber Identity Module

⁹International Mobile Equipment Identity

¹⁰International Mobile Subscriber Identity

Base Tranceiver Station (BTS): Die Basisstation bedient eine oder mehrere Funkzellen und übernimmt die Ver- und Entschlüsselung der Funkdaten.

Base Station Controller (BSC): Der Base Station Controller überwacht die Funkverbindung. An ihm sind bis zu 100 Base Tranceiver Stations angeschlossen.

Mobile Switching Center (MSC): Das MSC ist die Vermittlungsstelle des Mobilfunknetzes und fungiert als Schnittstelle zwischen normalem Telefonnetz und Funknetz. Die Daten dazu bezieht es aus dem Home Location Register beziehungsweise aus dem Visitor Location Register. Zur Authentifizierung bedient es sich des Authentication Centers.

Home Location Register (HLR): Im HLR stehen alle wichtigen Teilnehmerdaten:

- IMSI - International Mobile Subscriber Identity
- MSISDN - Mobile Station ISDN-Number (Telefonnummer)
- aktuelle Adressen des Visitor Location Registers und des MSC
- gebuchtes Dienstprofil¹¹
- MSRN - Mobile Subscriber Roaming Number
- Authentication Set¹²
- Gebührendaten

Sie dienen zur Bestimmung des Aufenthaltsortes der Mobile Station (MS) um Gespräche weiterleiten zu können.

Visitor Location Register (VLR): Folgende Daten werden gespeichert:

- wie bei HLR: IMSI, MSISDN, MSRN, aktuelle MSC-Adresse, Daten des gebuchten Dienstprofils, Gebührendaten
- TMSI - Temporary Mobile Subscriber Identity
- LAI - Location Area Identification
- HLR-Adresse

¹¹z.B. Anrufweiterleitung, Dienstrestriktionen

¹²besteht aus mehreren Triples: ein Triple besteht aus Zufallszahl (*RAND*), Signed Response (*SRES*) und Sitzungsschlüssel (*K_c*)

Authentication Center (AUC): Erzeugen des Sitzungsschlüssels K_c aus Zufallszahl und geheimem Schlüssel K_i , sowie Rückgabe der Triple bestehend aus $RAND$, $SRES$ und K_c .

Equipment Identity Register (EIR): Enthält eine Datenbank mit allen bekannten und gültigen (weiße Liste) defekten oder gestohlenen (schwarze Liste) und zweifelhaften (graue Liste) IMEI-Nummern der Endgeräte. Den Endgeräten der schwarzen Liste wird die Teilnahme am Netzwerk untersagt. Trotzdem ist der EIR nicht sehr effektiv, da IMEI-Nummern des Mobilfunkgerätes geändert werden können, EIR nicht von jedem Netzbetreiber ausgewertet/angewendet wird, und der Austausch der Listen zwischen den Anbietern nicht erfolgt.

Serving GPRS Support Node (SGSN): Erfüllt die äquivalenten Funktionen für paketorientierte Dienste wie das MSC für die leistungsorientierten Dienste. Um Verbindung ins Internet zu erhalten, werden die Daten über das GGSN weitergeleitet.

Packet Control Unit (PCU): Die PCU konvertiert Datenpakete, die vom SGSN kommen, in den PCU-Rahmen zur Weiterübertragung über das BSC.

Gateway GPRS Support Node (GGSN): Verbindet das GPRS-Netz mit dem Internet oder dem ATM¹³-Netz.

1.2 Übertragung auf der Luftschnittstelle

Die Übertragung der digitalen Daten findet durch Mischung aus Frequenz- und Zeitmultiplexing statt. Hier in Abbildung 2¹⁴ ist das Frequenzband bei 900 MHz (GSM 900¹⁵) dargestellt, das in mehrere Kanäle unterteilt ist, die einen Abstand von 200 kHz besitzen. Die Senderichtung (Uplink: von MS zur Basisstation) befindet sich im Bereich 890 bis 915 MHz, die sich auf 124 Kanäle aufteilt. In Empfangsrichtung (Downlink: von Basisstation zur MS), die sich ebenfalls in 124 Kanäle aufsplittet, wird der Bereich von 935 bis 960 MHz benutzt.

¹³Asynchronous Transfer Mode

¹⁴Abbildung 2 unterliegt der GNU-Lizenz für freie Dokumentation <http://upload.wikimedia.org/wikipedia/de/4/41/Gsm-rahmenstruktur.png>

¹⁵Uplink: 880,0 - 915,0 Mhz; Downlink: 925,0 - 960,0 Mhz

1.2.1 GSM-Rahmenstruktur

Jede Trägerfrequenz transportiert acht Nutzkanäle zeitversetzt und stellt einen GSM-TDMA-Rahmen¹⁶ dar, der genau 4,615 ms andauert. Einer dieser acht Zeitschlitze (Timeslots) hat eine Sendelänge/einen Sendeimpuls (Burst) von 0,577 ms. Der GSM-Zeitschlitz kann Nutzdaten von 128bit Länge (2 x 57bit) transportieren. Der Rest entfällt auf Schutzzeit, zweimal Tail¹⁷ mit je 3 bit, zwei Daten/Kontrollbit und Training¹⁸ von 26 bit Länge.

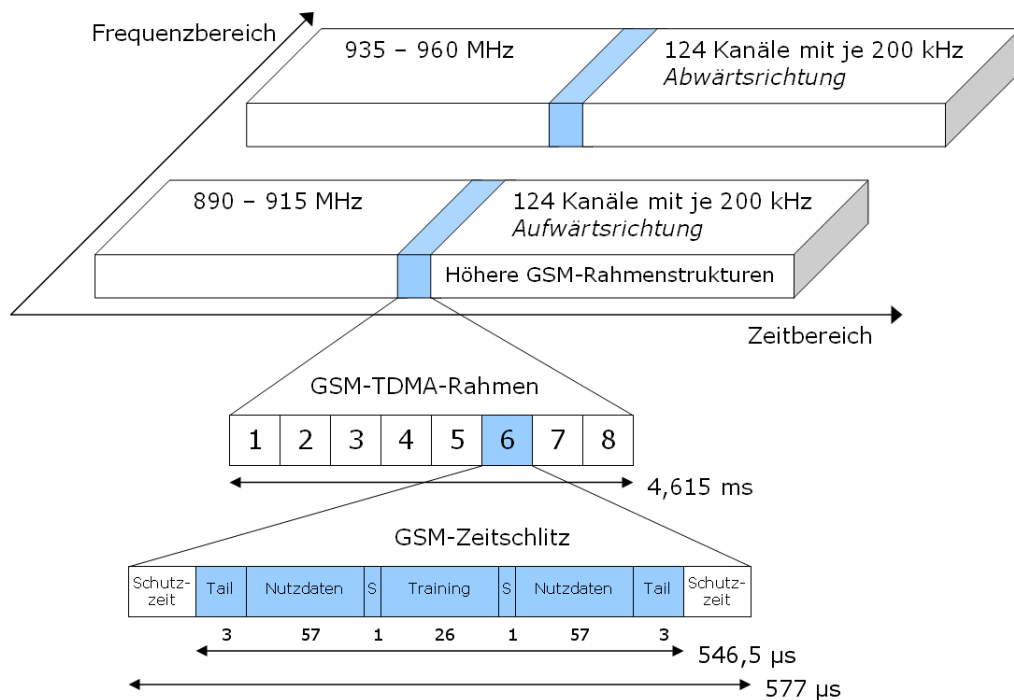


Abbildung 2: GSM-Rahmenstruktur

2 Kryptographie

Digitale Authentifikations- und Verschlüsselungsverfahren werden in der Mobilfunktelefonie verwendet, um genau zugeordnete Abrechnungen der Gespräche zu gewährleisten, sowie um unbefugtes Mithören und Telefonieren auf Kosten anderer zu verhindern.

¹⁶TDMA - Time Division Multiple Access

¹⁷auf Null gesetzt

¹⁸fest vorgegebenes Muster

2.1 Authentifizierung

Der A3-Algorithmus wird im GSM-Netz zur Authentifizierung genutzt. Die Algorithmen, die für A3 verwendet werden, sind nicht standardisiert und werden in der Regel von den Mobilfunkbetreibern geheimgehalten, nur die Schnittstellen unterliegen einem Standard. Die Eingabe setzt sich aus dem geheimen Schlüssel K_i und einer Zufallszahl $RAND$ zusammen, insgesamt ist sie 256 bit lang. Die Ausgabe besteht aus der Signed Response-Antwort ($SRES$) von 128 bit Länge. Der Algorithmus wird sowohl auf der Mobile Station, sowie beim Netzbetreiber angewendet; die jeweiligen Ergebnisse werden beim Betreiber verglichen (siehe Abbildung 3). Bei Übereinstimmung hat sich der Benutzer authentifiziert und ist für die Kommunikation freigeschaltet. Meistens werden vom AUC¹⁹ gleich mehrere Triplets ($RAND, SRES, K_c$) erzeugt. Wobei der Sitzungsschlüssel K_c ²⁰ im ebenfalls nicht standardisierten A8-Algorithmus gebildet wird (siehe auch 2.1.1).

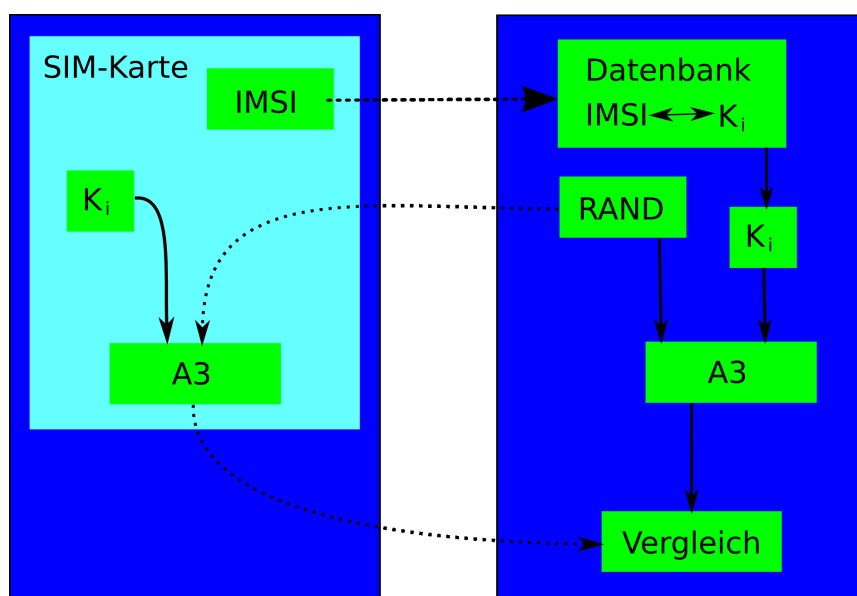


Abbildung 3: A3-Algorithmus

2.1.1 COMP128(A3/A8)

Der COMP128 war ursprünglich ebenfalls eine geheime Implementierung, der 1998 durch Reverse Engineering an die Öffentlichkeit gelangte. Eigentlich

¹⁹Authentication Center

²⁰wird für die Gesprächsverschlüsselung im A5-Algorithmus benötigt

war er nur als Beispielimplementierung geplant, findet aber in 190 Ländern der Welt Anwendung. Er fasst den A3-Algorithmus für die Authentifikation und den A8-Algorithmus für die Erzeugung des Sitzungsschlüssels K_c zusammen.

Algorithmus

Der COMP128 ist ein rundenbasierender Algorithmus (siehe Abbildung 4). Die 256 bit Eingabe, wie im A3-Algorithmus vorgegeben, besteht aus dem geheimen Schlüssel K_i (128 bit) und einer Zufallszahl $RAND$ (128 bit). Von der 128 bit langen Ausgabe werden die unteren 32 bit (0-31) für das *SRES*-Ergebnis von A3 verwendet. 54 bit, von 74 bis 127, bilden mit zehn angehängten 0-bits das Ergebnis von A8, also den Sitzungsschlüssel K_c . Die restlichen 42 bit verfallen ungenutzt. Die Hashing-Funktion läuft intern nochmals in fünf Runden, auch Level genannt, ab. Diese fünf Level stellen die Butterfly-Kompression dar. Nach Durchlauf hat sich der 256 bit Eingabewert auf 128 bit reduziert. Weitere Informationen zur Hashing-Funktion können in der Literatur (1) nachgelesen werden.

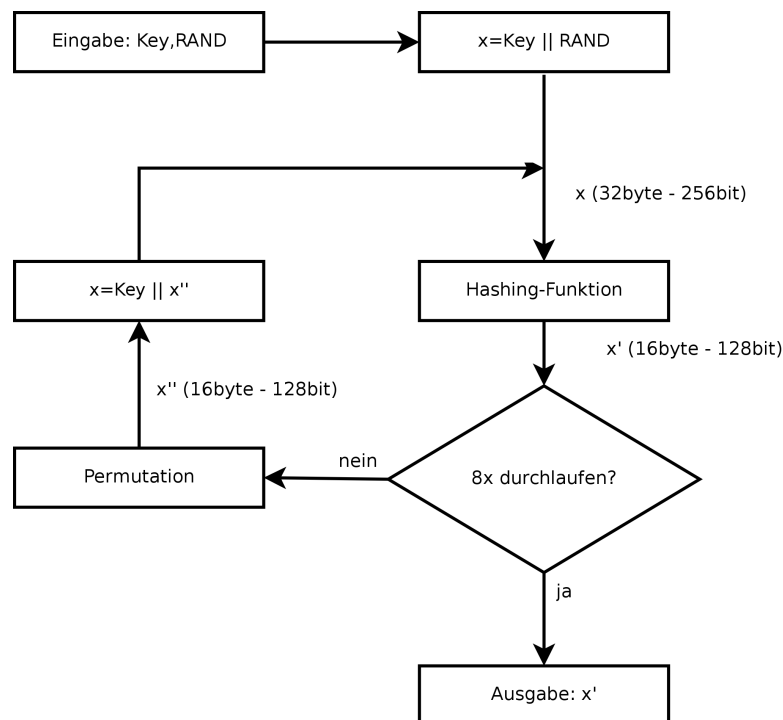


Abbildung 4: Rundenstruktur des COMP128

Sind die acht Runden des COMP128 noch nicht durchlaufen worden, folgt der Hashing-Funktion ein Permutationsblock, in dem das 128 bit lange Ergebnis

der Hashing-Funktion umgeordnet wird. Jede Bitposition k wird an die Position $(k \cdot 17) \bmod 128$ gesetzt. Diese Bitfolge liest man nun rückwärts ein und erhält mit dem vorangestellten geheimen Schlüssel K_i die neue Eingabe für den Hashing-Algorithmus. Nach acht Durchläufen erhalten wir die 128 bit-Ausgabe des COMP128-Algorithmus, die wie oben beschrieben verwendet wird.

Sicherheit des COMP128

1998 wurde durch Marc Briceno, Ian Goldberg und David Wagner an der Universität Berkley eine Kollisionsattacke²¹ auf den COMP128-Algorithmus durchgeführt. Sie rekonstruierten den geheimen Benutzerschlüssel K_i in sieben bis zwölf Stunden und benötigten dabei circa 165000 Anfragen an die SIM-Karte²². Mit dem Schlüssel K_i kann man auf Kosten anderer telefonieren und Gespräche desjenigen abhören. Andere alternative Methoden, um an den geheimen Benutzerschlüssel K_i zu kommen, sind zum einen die 2002 von Josyula R. Rao, Pankaj Rohatgi und Helmut Scherzer am IBM Watson Research Center präsentierte Analyse, die den Stromverbrauch und die EM-Strahlung auswertet²³, zum anderen eine Methode von A. Wiemers 2003 am BSI²⁴ gezeigt, die nur die Leistungsaufnahme vergleicht.²⁵

Der COMP128-Algorithmus kann also nicht als sicher bezeichnet werden, findet aber noch in vielen Ländern (nicht in Deutschland) Anwendung. Versuche die Sicherheit zu erhöhen, wie zum Beispiel die Einführung von COMP128-2 und Begrenzung der Anfrageversuche bei neuen SIM-Karten auf etwa 50000, verhindern eine komplette Kollisionsattacke. Für die *Partitioning Attack* oder die *Partial Collision Search by side Channel Analysis* greifen diese Maßnahmen allerdings nicht.

2.2 Gesprächsverschlüsselung(A5)

Für die Gesprächsverschlüsselung stehen drei, eigentlich vier Varianten zur Verfügung. Der A5/0-Algorithmus nutzt keine Verschlüsselung, der A5/1- und A5/2-Algorithmus verwenden eine Stromchiffre, dem A5/3-Algorithmus dient eine Blockchiffre zur Verschlüsselung. Im Folgenden soll ausschließlich

²¹Kollision tritt auf, wenn die Ergebnisse $SRES_1$ und $SRES_2$ für zwei verschiedene $RAND_1$ und $RAND_2$, identisch sind

²²circa 6,5 Anfragen pro Sekunde

²³*Partitioning Attack* - mit nur acht an die SIM-Karte gesendeten $RAND$ -Werten wird K_i ermittelt

²⁴Bundesamt für Sicherheit in der Informationstechnik

²⁵*Partial Collision Search by side Channel Analysis* - 2000 Versuche zur Ermittlung von K_i

der A5/1-Algorithmus erklärt werden, da der A5/2-Algorithmus diesem ähnlich und eine abgeschwächte Form des A5/1 ist²⁶ und der A5/3-Algorithmus bei UMTS²⁷ Anwendung findet. Dieser Standard wird in einem anderen Vortrag des Seminars näher erläutert.

2.2.1 Der A5/1-Algorithmus

Der Algorithmus besteht aus drei linear rückgekoppelten Schieberegistern (LFSR²⁸), deren Länge 19, 22 und 23 bit beträgt (siehe Abbildung 5). Es ergibt sich also eine Gesamtlänge von 64 bit. Der Sitzungsschlüssel K_c (64 bit) und die TDMA-Frame-Nummer (22 bit) werden in die Schieberegister geladen und stellen den ersten Initialwert dar. Die jeweils mittleren bits jedes einzelnen Registers sind die Taktkontrollbits. Steht höchstens ein Taktkontrollbit auf 1, werden alle Schieberegister mit Taktkontrollbit auf 0 weitergeschoben. Sind mehr als ein Taktkontrollbit auf 1, werden alle Register, die auf 1 stehen, weitergetaktet.

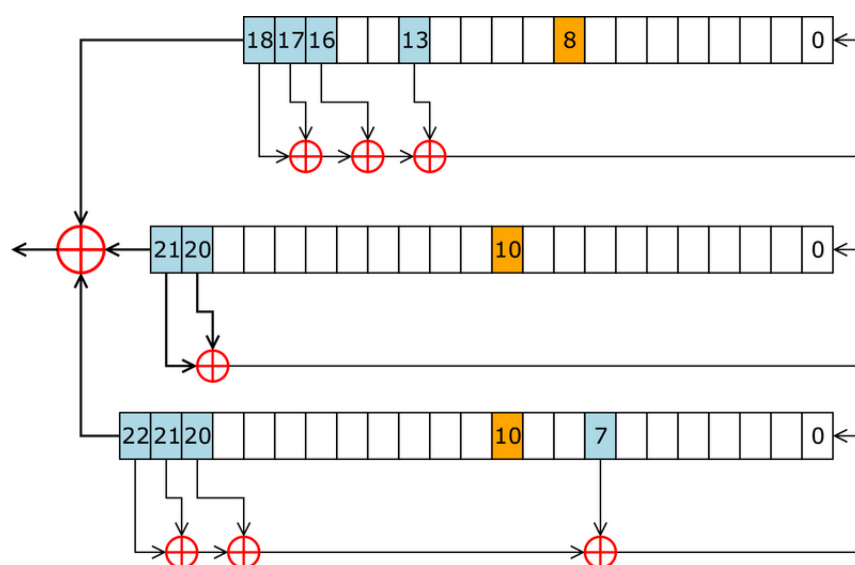


Abbildung 5: Schieberegister der A5/1

Auf diese Weise werden nun 328 bit pro TDMA-Rahmen erzeugt. Die ersten

²⁶Die Taktkontrollbits sind in ein viertes LFSR ausgelagert siehe 2.2.1 Seite 10

²⁷Universal Mobile Telecommunications System, Nachfolge-Mobilfunksystem der GSM-Systeme

²⁸Linear Feedback Shift Register

100 bit verfallen, die nächsten 114 bit werden für die Senderichtung und die restlichen 114 bit für die Empfangsrichtung verwendet. Für die Senderichtung werden nun die Nutzdaten (114 bit) und die erzeugten 114 bit des Bitstromes XOR-verknüpft. Das Ergebnis wird dann über die Luftschnittstelle gesendet und kann auf der Gegenseite mit der nachfolgenden XOR-Verknüpfung wieder entschüsselt werden. Die Schieberegister werden für jeden TDMA-Frame neu initialisiert. Die TDMA-Frame-Nummern wiederholen sich alle 209 Minuten²⁹, so also auch der Bitstrom, wenn der Sitzungsschlüssel K_c nicht vorher gewechselt wird.

2.3 Andere bekannte Verfahren

Da die kryptographischen Verfahren bei der GSM-Telefonie unzureichend oder gar nicht (wie bei A5/0) vorhanden sind, sowie die verwendeten Verfahren zum großen Teil geheim und nicht veröffentlicht sind, ist die Nutzung problematisch. Daher gibt es für die Übertragung sicherheitsrelevanter Informationen für das GSM-Netz andere Möglichkeiten. Zu nennen ist hier das Peer-to-Peer-Verfahren, bei dem die Verschlüsselung über zwei GSM-Kryptotelefone stattfindet. Zur Anwendung kommen symmetrische³⁰ oder asymmetrische³¹ Verfahren, oder deren Kombination³².

²⁹bedingt durch die darüberliegende GSM-Rahmenstruktur

³⁰Secret-key-Verfahren, zur Zeit 128 bit

³¹Public-key-Verfahren, zur Zeit 2048 bit

³²Authentifikation mit Public-key-Verfahren, dann erfolgt die Kommunikation über die symmetrische Verschlüsselung

Literatur

- [1] Marc Dingfelder: COMP128-Kollisionsattacke, Ruhr-Universität Bochum, Lehrstuhl Kommunikationssicherheit, Seminar IT-Sicherheit, Wintersemester 2002/2003
- [2] C. Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle, Oldenbourg Wissenschaftsverlag München, 2004, 3. Auflage
- [3] Thomas Wenckebach: GSM und UTM, Humboldt-Universität Berlin, Institut für Informatik, Seminar Mobile Computing, Wintersemester 2001/2002
- [4] Tobias Kipfelsberger: Sicherheit in GSM und UMTS, Universität Koblenz-Landau, Institut für Computer Visualistik, Seminar Net Security, Sommersemester 2004
- [5] Bundesamt für Sicherheit in der Informationstechnik: GSM-Mobilfunk, Gefährdung und Sicherheitsmaßnahmen, Stand: 2003
- [6] Dr. Stefan Lucks, Universität Mannheim, Theoretische Informatik, Vorlesung: Kryptographie (WS 1998/99), Kapitel 4: Schieberegister
- [7] Wikipedia: Global System for Mobile Communications - <http://de.wikipedia.org/wiki/GSM>, Stand 01.05.2006
- [8] Wikipedia: A5 (Algorithmus) - [http://de.wikipedia.org/wiki/A5_\(Algorithmus\)](http://de.wikipedia.org/wiki/A5_(Algorithmus)), Stand 01.05.2006
- [9] Erik Zenner, Rüdiger Weis, Stefan Lucks; Sicherheit des GSM-Verschlüsselungsstandards, DuD: Datenschutz und Datensicherheit 24, 2000