Grundlagen der Mobilfunk Sicherheit
5. IT-Sicherheitskonferenz

Paul Brüdgam (B.Sc.)

28. September 2016

Über mich

Paul Brüdgam (B.Sc.)

- Bachelor Angewandte Informatik – Informations- und Kommunikationstechnik an der FH Stralsund abgeschlossen
- Master Wirtschaftsinformatik – Softwareentwicklung an der FH Stralsund
- Neben dem Studium bei der bergwerk IT GmbH im Bereich Webentwicklung und Infrastruktur tätig gewesen
- Masterand bei Boreus Rechenzentrum GmbH mit dem Thema "Post-Quanten-Kryptographie"

Agenda

1. GSM
2. UMTS
3. LTE
4. Ausblick 5G

Wie alt ist Ihre SIM-Karte?

"Yeah - we used to call them cell phones."

Grundlegende Begriffe

Mobiltelefon

- **IMEI**. International Mobile Station Equipment Identity
  $\rightarrow$ Eindeutige Identifikation des Mobiltelefons

Subscription (Telefonanschluss)

- **SIM:** Subscriber Identifikation Module
- **IMSI:** International Mobile Subscriber Identity
  $\rightarrow$ Eindeutige Identifikation des Anschlusses
- **TMSI:** Temporary Mobile Subscriber Identity
  $\rightarrow$ Verschleierung der IMSI (Anonymität)

Das GSM-Protokoll

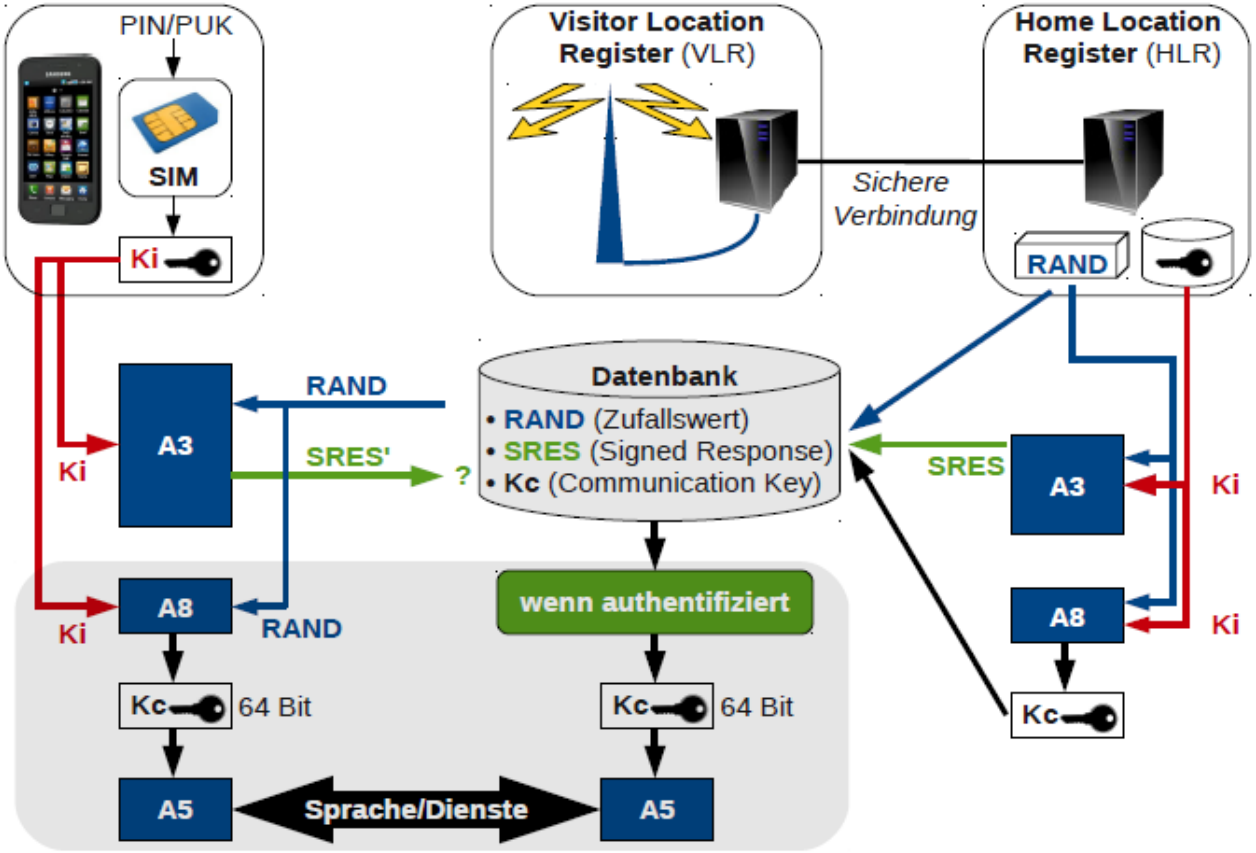

Abbildung: Sicherheitsarchitektur von GSM [Noa14]

Sicherheit von GSM

Sicherheitsrelevante Funktionen [Fed02]

- **SIM:** Zugangskontrolle und Kryptoalgorithmen
- **Authentisierung:** einseitiges Challenge-Response-Verfahren (Kryptoalgorithmus A3)
- **Anonymisierung** auf der Funkschnittstelle mittels TMSI
- **Verbindungsschlüssel** auf der Funkschnittstelle
  - A8 zur Generierung des Communication Key
  - A5 zur Verschlüsselung der Daten

Sicherheit von GSM

Die Sicherheit der GSM-Algorithmen A3/A8 [Bru04]

- Basieren auf dem COMP128-Algorithmus
- COMP128-1 kann in einer Minute gebrochen werden (Goldberg et al.'s Angriff [GB98])
- COMP128-2 und COMP128-3 bereinigen Fehler von COMP128-1 (geheim [3GP02])
- COMP128-4 für 3G Netzwerke basiert auf AES

Sicherheit von GSM

Die Sicherheit des GSM-Algorithmus A5 [Sch16]

- A5/1 und A5/2 sind Stromchiffren, A5/3 ist eine Blockchiffre (A5-Familie gilt als schwach)
- **A5/1:** effizienter Angriff von Biryukov, et al. [BSW00]
  Ermittlung durch die Software Kraken [g3g]
- **A5/2:** kann in Sekunden gebrochen werden
  Angriff von Barkan et. al [BBK03]
- **A5/3:** Angriff von Dunkelman et al. auf den Algorithmus auf Basis von KASUMI [DKS10]
- **A5/4:** ist wie A5/3 nur mit längerem Key [Sul12]

Sicherheit von GSM: IMSI-Catcher

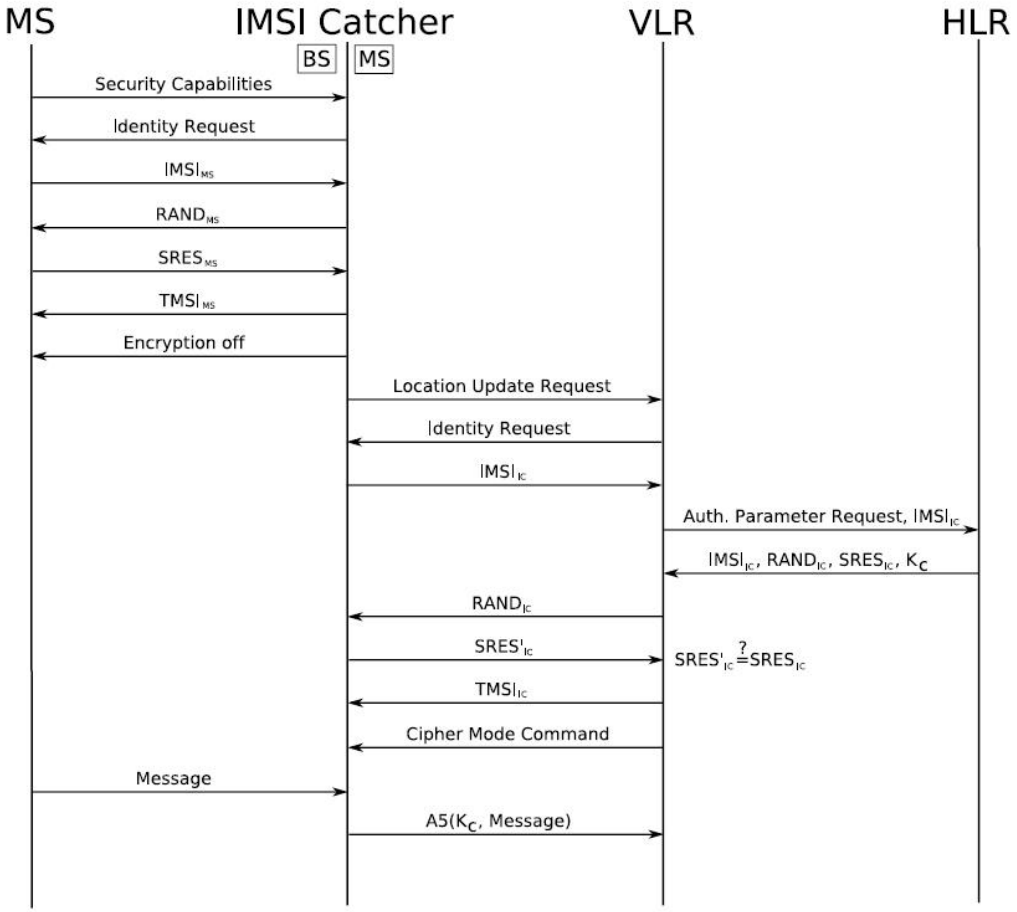

Abbildung: IMSI-Catcher Man-in-the-Middle [Str]

Das UMTS-Protokoll

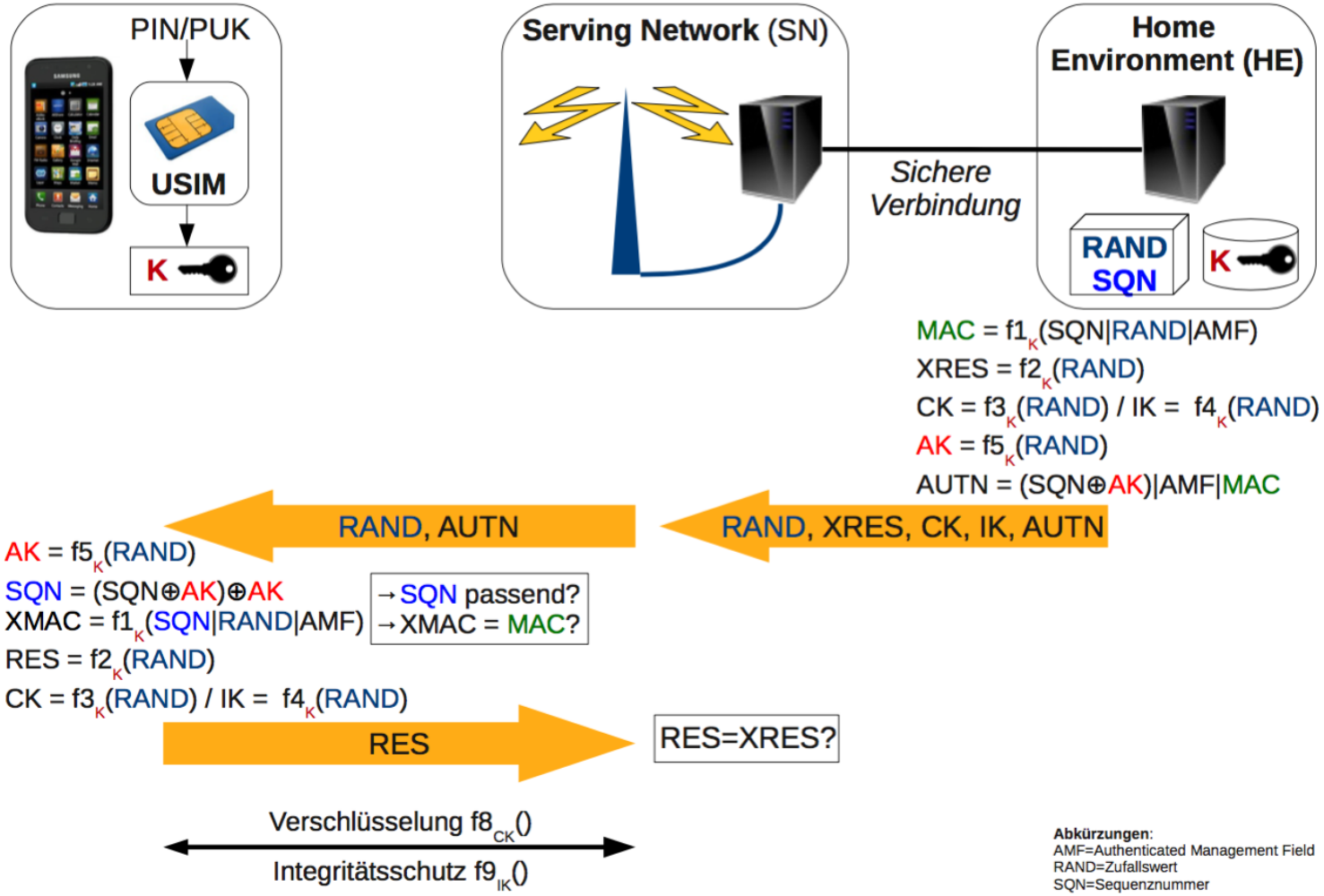

Abbildung: Sicherheitsarchitektur von UMTS [Noa14]

Sicherheit von UMTS

Sicherheitsfunktionen [Eck14, S.877ff]

- Beidseitige Authentifizierung
- Verwendung von Sequenznummern (Schutz vor Replay-Attacken)
- Service Netzwerk erneuert Schlüssel (128Bit) für beschränkte Nutzungsdauer
- $f_1 \ldots f_5$ durch Provider bestimmt (Empfehlung 3GPP: MILENAGE auf AES-Basis)
- f_8 Blockchiffre KASUMI wird mittels OFB zur Stromchiffre
- f_9 32-Bit CBC-MAC auf Basis von KASUMI

Sicherheit von UMTS

Angriffe auf UMTS

- IMSI-Catcher [MW04]
  - nutzt die Interoperabilität zu GSM aus
  - kennt UMTS-Schlüssel (CK, IK) nicht
    $\rightarrow$ Fallback auf A5/0 unverschlüsselt notwendig
- KASUMI (Bestandteil von A5/3 und A5/4) [Küh01] [BDK05]

Das LTE-Protokoll

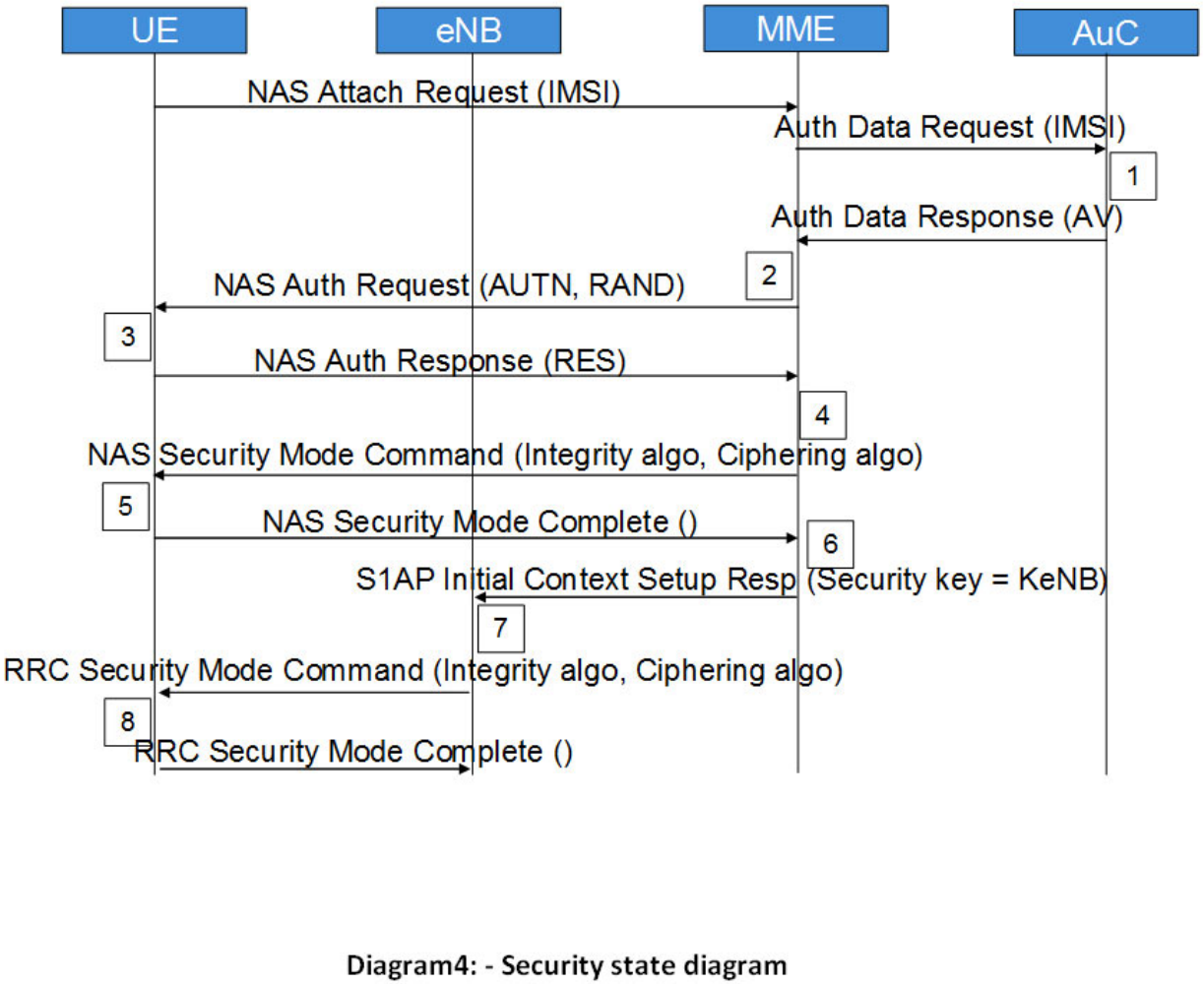

Abbildung: Security State Diagramm [Sah11]

Sicherheit von LTE

Überblick [ED13]

- Vier Security Domains (I – Network Access Security; II – Network Domain Security; III – User Domain Security; IV – Application Domain Security)
- beidseitige Authentifizierung und dynamische Schlüsselgenerierung
- Vertraulichkeits- und Integritätsschutz
- Komponenten des Providernetzes kommunizieren untereinander über unsichere Transportnetze

Sicherheit von LTE

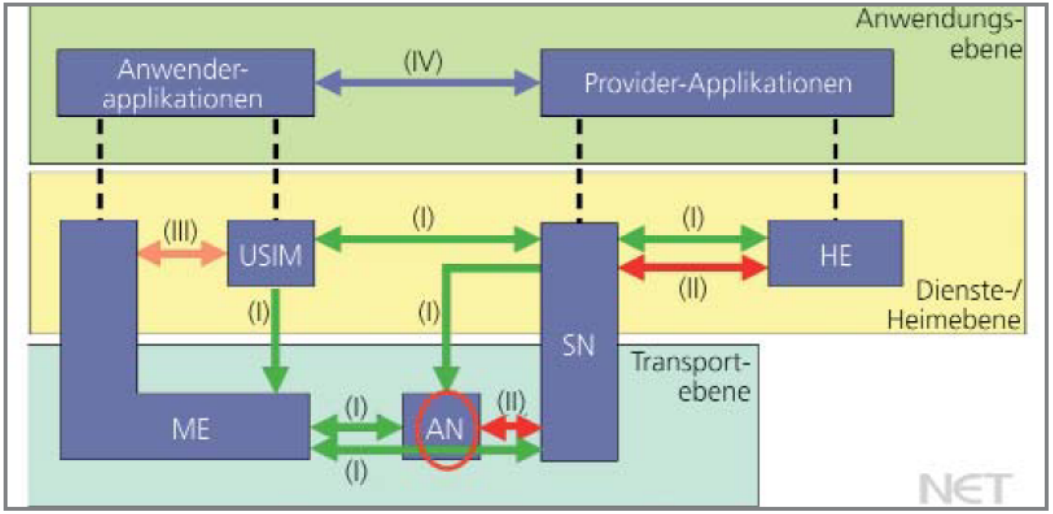

Bild 2: EPS Security-Domains
I – Network Access Security;
II – Network Domain Security;
III – User Domain Security;
IV – Application Domain Security;
V – Visibility and Configurability of Security

Abbildung: EPS Security-Domains [ED13]

Angriffe auf LTE

Angriffe [NIS16]

- "Böse" Basis-Stationen, z.B. Downgrade Attacken
- Attacken durch kompromittierte Femtozellen
- Radio Jamming Attacken

Ausblick 5G

Aktueller Stand [Zol16]

- Standard befindet sich aktuell noch in Entwicklung (ca. 2020)
- 1 Gbit/s bis 10 Gbit/s im Downlink
- Reaktionszeiten von einer Millisekunde

Spezifische Anwendungen [Zol16]

- Virtual- und Augmented-Realitiy-Anwendungen
- autonom fahrende Autos
- Internet der Dinge

Ausblick 5G

5G Manifest [Loh16] [Rud16]

- Chefs der 17 größten Telko-Konzerne Europas fordern Aufweichung der Gleichbehandlung der Daten im Netz (Netzneutralität)
- Telko-Konzerne drohen mit Investitionsstopp in die 5G-Mobilfunktechnik
- Wie wird sich ein solcher Stopp auswirken? Wer finanziert dann den 5G-Ausbau? Wird dies zu Lasten der Sicherheit ausgetragen?

Ausblick 5G

5 Schritte zu 5G [Wil16]

1. **Frequenzen bereitstellen:** Deutschland ist internationaler Treiber einer 5G-orientierten Frequenzpolitik. Darüber hinaus werden schon jetzt aus allen relevanten Frequenzbereichen Testfrequenzen für 5G bereitgestellt.
2. **Dialogforum 5G einrichten:** Das BMVI richtet ein "Dialogforum 5G" für die Telekommunikationswirtschaft und die Anwenderindustrien ein. Das Dialogforum organisiert die Vernetzung der Industriepartner - auch im Hinblick auf zukünftige Standards.
3. **5G-Forschung vorantreiben:** Mit gezielter 5G-Forschung erarbeitet sich Deutschland einen Technologievorsprung. Dadurch übernehmen wir eine Führungsrolle bei der internationalen Standardisierung von 5G.

Ausblick 5G

5 Schritte zu 5G [Wil16]

4. **Konkrete Anwendungsbeispiele schaffen:** Mit der Telekommunikationswirtschaft errichten wir eine 5G-Stadt in Deutschland. Sie bildet die gesamte Vielfalt der Anwendungen ab.
5. **5G-Rollout beschleunigen:** Dafür fördern wir den Infrastrukturausbau. Bis spätestens 2025 sollen alle Hauptverkehrswege und mindestens die 20 größten Städte in Deutschland mit 5G ausgestattet sein.

Literatur I

3GPP. *A3/A8 based on Milenage*. 2002. URL: ftp://www.3gpp.org/tsg_sa/WG3_Security/TSGS3_22_Bristol/Docs/PDF/S3-020063.pdf.

Elad Barkan, Eli Biham und Nathan Keller. *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*. 2003. URL: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf.

Eli Biham, Orr Dunkelman und Nathan Keller. *A Related-Key Rectangle Attack on the Full KASUMI*. 2005. URL: https://www.iacr.org/archive/asiacrypt2005/440/440.pdf.

Literatur II

Billy Brumley. *A3/A8 and COMP128*. 2004. URL: http://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-comp128.pdf.

Alex Biryukov, Adi Shamir und David Wagner. *Real Time Cryptanalysis of A5/1 on a PC*. 2000.

Orr Dunkelman, Nathan Keller und Adi Shamir. *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*. 2010. URL: http://eprint.iacr.org/2010/013.pdf.

Claudia Eckert. *IT-Sicherheit. Konzepte - Verfahren - Protokolle*. 9. Aufl. München: Oldenbourg Wissenschaftsverlag, 2014.

Literatur III

Evren Eren und Kai-Oliver Detken. *Evolutionsfrage - Ist LTE sicherer als seine Vorgänger?* Aug. 2013. URL: https://www.decoit.de/de/artikel.html?file=files/DECOIT/pdf/artikel/NET0913_LTE.pdf.

Hannes Federrath. *Sicherheitsfunktionen in GSM-Mobilfunknetzen*. Juni 2002. URL: http://svs.informatik.uni-hamburg.de/publications/2002/2002-06-20MannheimBvDMobil.pdf.

g3gg0de. URL: https://youtu.be/TbWLVLUguJw (besucht am 07. 09. 2016).

Ian Goldberg und Marc Briceno. *GSM Cloning*. Apr. 1998. URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

Literatur IV

Ulrich Kühn. *Cryptanalysis of Reduced-Round MISTY*. 2001. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.7609.

Thomas Lohninger. *„5G-Manifest“: Telekom-Industrie attackiert Netzneutralität, Günther Oettinger stellt sich auf ihre Seite*. Juli 2016. URL: https://netzpolitik.org/2016/5g-manifesto-telekom-industrie-attackiert-netzneutralitaet-guenther-oettinger-stellt-sich-auf-ihre-seite/.

Ulrike Meyer und Susanne Wetzel. *A Man-in-the-Middle Attack on UMTS*. 2004. URL: http://ece.wpi.edu/~dchasaki/papers/mitm_umts.pdf.

Literatur V

NIST. *LTE Architecture Overview and Security Analysis*. 2016. URL: http://csrc.nist.gov/publications/drafts/nistir-8071/nistir_8071_draft.pdf.

Andreas Noack. *Netzwerksicherheit II. Kapitel 5: Mobilfunk*. 2014.

Thomas Rudl. *Netzneutralität in der Zielgeraden: Morgen entscheidet sich die Zukunft des Internets in Europa (Update)*. Aug. 2016. URL: https://netzpolitik.org/2016/netzneutralitaet-in-der-zielgeraden-morgen-entscheidet-sich-die-zukunft-des-internets-in-europa/.

Prasanna Sahu. *LTE Security Architecture*. 2011. URL: https://www.iacr.org/archive/asiacrypt2005/440/440.pdf.

Literatur VI

Klaus Schmeh. *Kryptografie. Verfahren, Protokolle, Infrastrukturen*. 6. Aufl. Heidelberg: dpunkt.verlag, 2016.

Daehyun Strobel. URL: https://cyberwarfaremag.files.wordpress.com/2008/11/imsi-man-in-the-middle.jpg (besucht am 07. 09. 2016).

Alain Sultan. *Present and future Standards for mobile internet and smart phone information security*. 2012. URL: http://www.3gpp.org/ftp/information/presentations/presentations_2012/ETSI_visit_MiiT_10sept2012_Security.ppt.

Literatur VII

Andreas Wilkens. *http://www.heise.de/newsticker/meldung/Mobilfunk-Infrastrukturminister-Dobrindt-kuendigt-5-Schritte-zu-5G-an-3332918.html*. Sep. 2016.

Alexander Zollondz. *Nach 4G ist vor 5G: Auf der Suche nach dem LTE-Nachfolger*. Feb. 2016. URL: https://www.netzwelt.de/news/151495_2-4g-5g-suche-lte-nachfolger.html.