Das DDR-Chiffriergerät T-310

Winfried Stephan Wolfgang Killmann

32th Crypto Day, 15 January 2021

Der Vortrag präsentiert die Ergebnisse der Sicherheitsanalyse des Fernschreibchiffriergeräts T-310, das in der DDR für Staatsgeheimnisse zugelassen war, bewertet die Analyse aus heutiger Sicht und gibt inhaltliche und methodische Anregungen für aktuelle kryptologische Analysen.

Das Chiffriergerät T-310 war das am weitesten verbreitete Fernschreibchiffriergerät in der DDR. Der Chiffrieralgorithmus des Geräts wurde 2006 in der Fachzeitschrift Cryptologia veröffentlicht (Schmeh, 2006). Es erschien eine Reihe von bisher neun Publikationen über Eigenschaften des Chiffrieralgorithmus T-310 von einer internationalen Gruppe von Kryptologen um Nicolas T. Courtois z. B. (Courtois, Schmeh, Drobick, Patarin, Oprisanu, Scarlata & Bhallamudi, 2018; Courtois & Georgiou, 2020). Killmann und Stephan(2021)beschreiben die Entwicklung, die Analyse und die Geschichte der T-310 aus Sicht der damaligen Entwickler.

Im Vortrag soll nach einem Überblick über die Geschichte der T-310 ihr Chiffrieralgorithmus (CA) vorgestellt. Die Einführung sogenannter Langzeitschlüssel (LZS) als Parameter des CA führte dazu, dass eigentlich eine Algorithmenklasse definiert wurde. Die wichtigsten Ergebnisse der mathematisch-kryptologischen Analyse zu dieser Algorithmenklasse während der Einsatzzeit der T-310 werden danach präsentiert. Eine sorgfältige Auswahl des strukturbestimmenden Langzeitschlüssels ermöglichte den Nachweis wichtiger Sicherheitseigenschaften des CA, wie z. B. zu Gruppeneigenschaften in der Chiffrierabbildung, der Periodizität und Schlüsseläquivalenz. Neuere Untersuchungen konzentrieren sich auf die (uns bereits bekannte) Existenz kryptologisch schwacher LZS.

Ebenso wird herausgearbeitet, dass die konsequente Anwendung von Methoden der Gruppen- und Automatentheorie für unsere Analyse (11, 1980) eine zentrale Rolle spielte. Ein aktueller Bezug zu diesen Arbeiten findet sich in den Analyseergebnissen zu Gruppeneigenschafen des RIJNDAEL (AES), seines Vorläufers DES, des IDEA und des SAFER++ siehe z. B. (Wernsdorf, 1994). Die im Design festgelegten Eigenschaften sind nach unserer Meinung die Ursache dafür, dass inzwischen entwickelte Analysemethoden, wie die differentiale und lineare Cryptanalysis oder algebraisch basierte Attacken keine erfolgreichen Angriffe liefern.

Wir konzentrieren uns auf die Diskussion des CA, da dieser hauptsächlich in den aktuellen Veröffentlichungen untersucht wird. Es wird aber auch die Wechselwirkung der Analyse des Chiffrieralgorithmus, des Chiffriergeräts, des Chiffrierverfahrens und ihrer Anwendung betont. Hardwareimplementierung und Algorithmuseigenschaften beeinflussen sich gegenseitig.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-11

Für den CA T-310 mit den für den operativen Einsatz vorgesehenen LZS-Varianten sind aus unserer Sicht auch heute noch keine erfolgreichen Dekryptieransätze erkennbar.

References

Referat 11 (1980). Kryptologische Analyse des Chiffriergeräts T-310/50. Technical Report GVS ZCO Nr. 402/80, ZCO. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. AR3 594.

Nicolas T. Courtois & Marios Georgiou (2020). Variable elimination strategies and construction of nonlinear polinomial invariant attacks on T-310. *Cryptologia* **44**(1), 20 – 38.

Nicolas T. Courtois, Klaus Schmeh, Jörg Drobick, Jacques Patarin, Maria-Bristena Oprisanu, Matteo Scarlata & Om Bhallamudi (2018). Cryptographic Security Analysis of T-310. URL `https://eprint.iacr.org/2017/440.pdf`.

Wolfgang Killmann & Winfried Stephan (2021). *Das DDR-Chiffriergerät T-310, Kryptographie und Geschichte*. Springer Spektrum. ISBN 978-3-662-61896-7.

Klaus Schmeh (2006). The East German Encryption Machine T-310 and the Algorithm It Used. *Cryptologia* **30**(3), 251–257.

Ralph Wernsdorf (1994). The Round Functions of RIJNDAEL Generate the Alternating Group. In *EUROCRYPT '93*, LNCS 658, 99 – 112. Springer, Berlin.