

Strengthening the E_0 Keystream Generator against Correlation Attacks and Algebraic Attacks

Frederik Armknecht and Matthias Krause and Dirk Stegemann

University of Mannheim
Germany

Stream ciphers are widely used for online-encryption of arbitrarily long data. An important class of stream ciphers are combiners with memory, with the E_0 generator from the Bluetooth standard for wireless communication [2] being their most prominent example.

E_0 consists of 4 driving devices, a finite state machine (FSM) \mathcal{C} with a 4 bit state, an output function f and a memory update function δ . At each clock, one keystream bit z_t is produced from the output $X_t \in \{0, 1\}^4$ of the driving devices and the current state $C_t \in \{0, 1\}^4$ of the FSM according to $z_t = f(C_t, X_t)$, and the state of the FSM is updated to $C_{t+1} := \delta(C_t, X_t)$.

So far, the best publicly known attacks against combiners with memory are correlation attacks [4] and algebraic attacks [1]. Correlation attacks exploit linear equations $L(X_t, \dots, X_{t+r-1}, z_t, \dots, z_{t+r-1}) = 0$ that are true with some probability $\frac{1}{2} + \lambda$ with $\lambda \neq 0$. Algebraic attacks use valid non-linear equations of preferably low degree to describe the secret key by a system of equations.

We show how to avert a special class of correlation attacks [3] that is currently the most effective against E_0 and introduce a general design principle which guarantees that all valid equations have a degree not smaller than a certain lower bound. Combining these results, we construct a slightly modified version of E_0 with significantly improved resistance against correlation attacks and algebraic attacks.

References

- [1] Armknecht, Krause: *Algebraic Attacks on Combiners with Memory*, Crypto 2003.
- [2] Bluetooth specification Version 1.1. <http://www.bluetooth.com>
- [3] Lu, Vaudenay: *Faster Correlation Attack on the Bluetooth Keystream Generator*, Crypto 2004.
- [4] Salmasizadeh, Golić, Dawson, Simpson: *A Systematic Procedure for Applying Fast Correlation Attacks to Combiners with Memory*, SAC 1997.