Corrections and Clarifications for Thesis

Yang, Jing

2021

Corrections and Clarifications for Thesis

Jing Yang

Department of Electrical and Information Theory, Lund University

The document presents the list of corrections and clarifications of Jing Yang's thesis "Contributions to confidentiality and Integrity Algorithms for 5G", which is accessible at https://portal.research.lu.se/en/publications/contributions-to-confidentiality-and-integrity-algorithms-for-5g

- **P101**, the first line: ".. that **u** and **z**.." ⇒ "..that **u** and **y**..".
- **P105**, line 6: "Here (E, E') can be regarded as following the 4-tuple 16-bit distribution...".
- **P104**, 16-bit correlation attack. To collect the correct codeword, we actually need to update the equivalent LFSR over $\mathbb{F}_{2^8}$ four times between $y^{(t)}$ and $y^{(t+1)}$. Therefore, the samples $(\oplus_{j=1}^{4}(y^{(t_j)}, \oplus_{j=1}^{4} y^{(t_j+1)}))$ involve the first $l'+4$ 8-bit states of the LFSR instead of $l'+1$. However, as the complexity of a correlation attack is mainly determined by the bias (squared Euclidean imbalance) of the linear approximation (e.g., the required number of parity checks is computed as $\approx 2l'n \ln 2/\epsilon$ where $n = 8$, ϵ is the bias, and $l' = 19$ in our attack), the complexity is generally in the same order.
- **P130**: the linear mask M (above Section 4.5) is missing, it should be:

```
uint32_t M[32] ={
        0x26dad00b, 0x5de94454, 0x3bdfdb0d, 0x1423c42f, 0xc4f35585, 0x1f22e504,
        0xeb07cc1e, 0x3633b301, 0x11b4bca3, 0x6f23b103, 0x912adb7d, 0x6a058e9e,
        0x67d4ef5a, 0xdd0830b6, 0xee579099, 0x9af30192, 0x455d8a7b, 0x22133144,
        0x7fb935a8, 0x4d923b96, 0xc0c9967e, 0x99db94fc, 0x442f1154, 0x17994e1f,
        0x08d2662e, 0xccc8fe9c, 0x994d8fb8, 0xfba4f0dc, 0x462d2a69, 0x373306ed,
        0x91282e11, 0x9b82d788};
```

- **P150**, the last paragraph: "It is now...since z^t depends only on $\hat{R}1$ and $\hat{R}2$, and $z^{(t+1)}$ depends on $\hat{R}1$, $\hat{R}2$ and $\hat{R}3$, there...".
- **P184**, the second paragraph: "..in Appendix 6.2.." ⇒ "..in Equation 13..".
- **P165**, the proof of primitivity: note that we used left matrix multiplication (with a 16-bit state vector) to illustrate the effect of multiplying with α. When deriving the big transition matrix in P166, the transpose form of M_α is used (because the right matrix multiplication is used).
- **P185**, Table 6: 356 Gpbs and 356+ Gpbs for the first two implementations of SNOW-V.
- **P269**, the last paragraph: the Euler-Mascheroni constant γ (some other notation should have been used for it) should be distinguished from the notation γ for the number of fixed variables throughout the paper.