Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Monday, 30 January 2012, 23:59:59.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 11.1 (crypto-GPS). (10 points)

In the lecture we have encountered zero-knowledge proofs for the discrete logarithm problem. The protocol crypto-GPS presented in the lecture is not exactly the same one as the one from the original article "On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order" by Girault, Poupard and Stern.

(i) Describe detailed the differences between the protocol from the lecture and the one from the paper. [4]

(ii) In the paper a security-proof for the proposed protocol is given. Explain detailed why you believe (or not believe) that crypto-GPS from the lecture is secure. [6]

Exercise 11.2 (Stream cipher design principles). (10 points)

In the lecture we have seen a nice construction for stream ciphers from block ciphers. In particular, we defined for input stream $x = x_0, x_1, \ldots$ values [10]

$$u_\tau = x_\tau + g_1 u_{\tau-1} + g_2 u_{\tau-2} + g_3 u_{\tau-3} + g_4 u_{\tau-4},$$
$$y_\tau = u_{\tau-4} + f_1 u_{\tau-3} + f_2 u_{\tau-2} + f_3 u_{\tau-1} + f_4 u_\tau,$$

where $u_{-1}, u_{-2}, u_{-3}, u_{-4}$ are some initial values and (f, g) form the linear filter in the specification of the cipher. Abbreviate $s^0 = D^4 u^0$ and

$$f = D^4(1 + f_1 D^{-1} + f_2 D^{-2} + f_3 D^{-3} + f_4 D^{-4}),$$
$$g = 1 - g_1 D - g_2 D^2 - g_3 D^3 - g_4 D^4.$$

Further let

$$x^0 = D^{-4}((s^0 g) \bmod D^4),$$
$$y^0 = D^{-4}((s^0 f) \bmod D^4).$$

Show that

$$y = \frac{f}{g}(x + x^0) - y^0.$$

Exercise 11.3 (Branch number). (5 points)

5 Compute the branch number of the linear layer in PRESENT-80. Is it good?

Exercise 11.4 (Reality). (10 points)

10 We have now studied plenty of primitives that can (or cannot) be used in ultra-lightweight scenarios. Find out which kind of primitives are *really* used in practice. Discuss the technology and put it into context to the results from the lecture.