Koopman interpretation and analysis of public-key cryptosystems

Sebastian Schlor[1], Robin Strässer[1], Frank Allgöwer[1]

[1]) Institute for Systems Theory and Automatic Control,
University of Stuttgart, 70550 Stuttgart, Germany
{schlor,straesser,allgower}@ist.uni-stuttgart.de

The security of public-key cryptosystems relies on computationally hard problems such as the discrete logarithm problem stated on the left-hand side of Table 1. The hardness of these problems is classically analyzed by number theoretic methods. On our poster, we present a new perspective on cryptosystems from a systems theoretic point of view. We demonstrate how the Diffie-Hellman key exchange cryptosystem depicted in Figure 1 and the underlying problem can be reformulated as a nonlinear dynamical system as on the right-hand side of Table 1 [2].

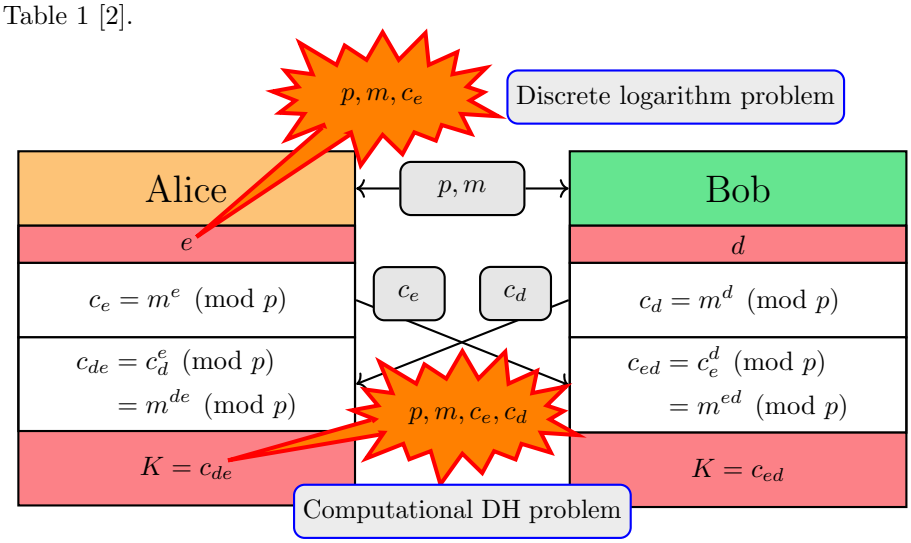

Figure 1: In the Diffie-Hellman key exchange, Alice and Bob create a common secret K based on their own secrets e and d by publicly communicating p, m, c_e and c_d. The discrete logarithm problem and the computational Diffie-Hellman problem prevent adversaries from learning e, d and K.

Employing Koopman theory, we transfer this dynamical system into a higher-dimensional space to analytically derive a purely linear system that equivalently describes the cryptosystem. In this form, analytic tools for linear systems allow us in principle to reconstruct the secret integers of the key exchange by simple manipulations. Moreover, we prove that the linear system has to be at least of dimension

$$n = \frac{p-1}{2} + 1$$

Table 1: Comparison of the classical discrete logarithm problem and the interpretation using a dynamical system.

Classic	Dynamic
Given c_e, m and p, find e s.t. $c_e = m^e \pmod p$.	Given m and p, the initial condition $x_0 = 1$ and the end-point $x_e = c_e$, find the length e of the trajectory of the dynamical system $x_{k+1} = mx_k \pmod p$ that connects the two points.

to guarantee perfect accuracy for our choice of lifting coordinates. We relate the obtained state dimension as a notion of complexity to the classical concept of linear complexity. Finally, we transfer this approach to a data-driven setting where the Koopman representation is learned from data samples of the cryptosystem. Here, our result on the minimal required state dimension translates into conditions on the minimal number of data samples that have to be collected. Further details on the results can be found in [1].

References

[1] Schlor, S. and Strässer, R. and Allgöwer, F. 2022. Koopman interpretation and analysis of a public-key cryptosystem: Diffie-Hellman key exchange. *Preprint arXiv:2211.11290.*

[2] Schmitz, R. 2008. Public key cryptography: A dynamical systems perspective. In: *Proc. Second International Conf. on Emerging Security Information, Systems and Technologies,* IEEE. pp. 209-212.