

USING THE INHOMOGENEOUS SIMULTANEOUS APPROXIMATION PROBLEM FOR CRYPTOGRAPHIC DESIGN

Frederik Armknecht, Carsten Elsner and Martin Schmidt

Progress in Cryptology - Africacrypt 2011, 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011, A.Nitaj, D.Pointcheval (Eds.), Springer Verlag, 2011, LNCS 6737, 242-259

We introduce the Inhomogeneous Simultaneous Approximation Problem (ISAP), an old problem from the field of analytic number theory. Although the Simultaneous Approximation Problem (SAP) is already known in cryptography, it has mainly been considered in its *homogeneous* instantiation for *attacking* schemes. We take a look at the hardness and applicability of ISAP, i.e., the *inhomogeneous* variant, for *designing* schemes.

More precisely, we define a decisional problem related to ISAP, called DISAP, and show that it is NP-complete. With respect to its hardness, we review existing approaches for solving related problems and give suggestions for the efficient generation of hard instances. Regarding the applicability, we describe as a proof of concept a bit commitment scheme where the hiding property is directly reducible to DISAP. An implementation confirms its usability in principle (e.g., size of one commitment is 6273 bits and execution time is in the milliseconds).