Cryptology ePrint Archive: Report 2011/280

DDH-like Assumptions Based on Extension Rings

Ronald Cramer and Ivan Damgaard and Eike Kiltz and Sarah Zakarias and Angela Zottarel

Abstract: We introduce and study a new type of DDH-like assumptions based on groups of prime order q. Whereas standard DDH is based on encoding elements of F_{q} ``in the exponent" of elements in the group, we ask what happens if instead we put in the exponent elements of the extension ring R_f= \F_{q}[X]/(f) where f can be any degree-d polynomial. We show that solving the decision problem that follows naturally reduces to the case where f is irreducible. This variant is called the d-DDH problem, where 1-DDH is standard DDH. Essentially any known cryptographic construction based on DDH can be immediately generalized to use instead d-DDH, and we show in the generic group model that d-DDH is harder than DDH. This means that virtually any application of DDH can now be realized with the same (amortized) efficiency, but under a potentially weaker assumption. On the negative side, we also show that d-DDH, just like DDH, is easy in bilinear groups. This motivates our suggestion of a different type of assumption, the d-vector DDH problems (VDDH), which are based on f(X)= X^d, but with a twist to avoid the problems with reducible polynomials. We show in the generic group model that VDDH is hard in bilinear groups and that in fact the problems become harder with increasing d and hence form an infinite hierarchy. We show that hardness of VDDH implies CCA-secure encryption, efficient Naor-Reingold style pseudorandom functions, and auxiliary input secure encryption, a strong form of leakage resilience. This can be seen as an alternative to the known family of k-linear assumptions.

Category / Keywords: public-key cryptography / DDH, Public Key Encryption, PRF, Leakage Resilient Encryption

Date: received 30 May 2011

Contact author: angela at cs au dk