Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Applied Mathematics 154 (2006) 326–336
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Polynomial interpolation of cryptographic functions related to Diffie–Hellman and discrete logarithm problem

Eike Kiltz[a], Arne Winterhof[b]

[a]Lehrstuhl Mathematik & Informatik, Fakultät für Mathematik, Ruhr-Universität Bochum, 44780 Bochum, Germany
[b]Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, c/o Johannes Kepler University Linz, Altenbergerstraße 69, 4040 Linz, Austria

Received 20 June 2003; received in revised form 5 March 2004; accepted 21 March 2005
Available online 25 October 2005

Abstract

Recently, the first author introduced some cryptographic functions closely related to the Diffie–Hellman problem called *P*-Diffie–Hellman functions. We show that the existence of a low-degree polynomial representing a *P*-Diffie–Hellman function on a large set would lead to an efficient algorithm for solving the Diffie–Hellman problem. Motivated by this result we prove lower bounds on the degree of such interpolation polynomials. Analogously, we introduce a class of functions related to the discrete logarithm and show similar reduction and interpolation results.

Keywords: Diffie–Hellman; Discrete logarithm; Polynomial interpolation; Lower bounds

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of order q with a prime power q and let $0 \neq \gamma \in \mathbb{F}_q$ be an element of order t. The security of the Diffie–Hellman key exchange (see e.g. [13, Chapters 3.7 and 12.6]) for the group generated by γ depends on the intractability of the *Diffie–Hellman mapping* DH defined by

$$\mathrm{DH}(\gamma^x, \gamma^y) = \gamma^{xy}, \quad 0 \leqslant x, y \leqslant t-1.$$

For breaking the Diffie–Hellman cryptosystem it would be sufficient to have a low-degree polynomial that coincides with the mapping DH on a large subset of $\{0, 1, \ldots, t-1\}^2$. In [3,21] it was shown that such a polynomial does not exist for several types of subsets. Since

$$\gamma^{2xy} = \gamma^{(x+y)^2}\gamma^{-x^2}\gamma^{-y^2},$$

E-mail addresses: kiltz@lmi.ruhr-uni-bochum.de (E. Kiltz), arne.winterhof@oeaw.ac.at (A. Winterhof).

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.03.030

and square roots in finite fields can be efficiently calculated (see e.g. [1, Chapter 7]) we may consider the univariate mapping

$$\mathrm{dh}(\gamma^x) = \gamma^{x^2}, \quad 0 \leqslant x \leqslant t-1,$$

instead of the bivariate mapping DH. For lower bounds on the degree of interpolation polynomials of dh see [2,9,18,19].

Obviously, the Diffie–Hellman key exchange depends also on the hardness of the discrete logarithm ind defined by

$$\mathrm{ind}(\gamma^x) = x, \quad 0 \leqslant x \leqslant t-1.$$

For results on interpolation polynomials of ind see [2,11,12,14–16,18–20,22].

In the present paper we consider mappings of the form

$$P\text{-dh}(\gamma^x) = \gamma^{P(x)}, \quad 0 \leqslant x \leqslant t-1, \tag{1}$$

for a nonlinear polynomial $P(X) \in \mathbb{Z}_t[X]$ of small degree, with respect to t, say,

$$2 \leqslant \deg(P) \leqslant \log(t).$$

In [5] the first author suggested a toolbox of cryptographic functions called *P-Diffie–Hellman functions* including these mappings. In particular, he proved that computing P-dh is computationally equivalent to computing dh. Hence, a low-degree polynomial representation of P-dh would solve the Diffie–Hellman problem and an investigation of P-dh becomes very important.

Moreover, for the case when $q = p$ is a prime, we consider

$$Q\text{-ind}(\gamma^x) = Q(x), \quad 0 \leqslant x \leqslant t-1, \tag{2}$$

for a non-constant polynomial $Q(X) \in \mathbb{F}_p[X]$, where we assume that $\deg(Q)$ is small, say,

$$1 \leqslant \deg(Q) \leqslant \log(p).$$

After some preliminary results in Section 2 we prove that dh can be evaluated with an algorithm using $\mathrm{O}(\log^2(t) \log^2(q))$ bit operations and $\deg(P) - 1$ evaluations of P-dh in Section 3.1, which improves the result of [5]. We prove lower bounds on the degree and sparsity of interpolation polynomials of P-dh in Section 3.2.

The *sparsity* $\mathrm{spr}(f)$ (or *weight*) of a polynomial $f(X) \in \mathbb{F}_q[X]$ is the number of its non-zero coefficients.

In Section 4 we prove similar reduction and interpolation results for the mapping Q-ind. Finally, in Section 5 we mention some extensions of our work.

2. Preliminaries

The following result motivated by Newton's interpolation formula is essential for the reduction algorithms and the proofs of the interpolation results.

Lemma 1. *Let $\mathbb{D}$ be a commutative ring with identity 1. Let $B \geqslant 0$ be an integer and $P(X) \in \mathbb{D}[X]$ a polynomial of degree $D \geqslant B$ with leading coefficient a_D. Then we have*

$$\sum_{d=0}^{D-B} \binom{D-B}{d} (-1)^{D-B-d} P(X+d) = \frac{a_D D!}{B!} X^B + T_{B-1}(X),$$

where $T_{B-1}(X)$ is a polynomial of degree at most $B-1$ with the convention that the degree of the zero polynomial is -1.