Polynomial Interpolation of Cryptographic Functions Related to the Diffie-Hellman Problem

Eike Kiltz [1] and Arne Winterhof [2]

[1] Lehrstuhl Mathematik & Informatik, Fakultät für Mathematik,
Ruhr-Universität Bochum, 44780 Bochum, Germany.
E-Mail: kiltz@lmi.ruhr-uni-bochum.de

[2] Temasek Laboratories, National University of Singapore,
10 Kent Ridge Crescent, Singapore 119260, Republic of Singapore.
E-Mail: tslwa@nus.edu.sg

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.

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 prime order t. The security of the Diffie-Hellman key exchange (see e. g. [10, Chapters 3.7 and 12.6]) for the group generated by γ depends on the intractability of the *Diffie-Hellman mapping* DH defined by

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

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] and [16] it was shown that such a polynomial doesn't exist for several types of subsets. Since

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

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

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

instead of the bivariate mapping DH. For lower bounds on the degree of interpolation polynomials of dh see [2, 7].

In the present paper we consider mappings of the form

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

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

$$\deg(P) \le \log(q)^2.$$

In [4] 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.

After some preliminary results in Section 2 we prove that dh can be evaluated with an algorithm using $O(\log^2(t)\log^2(q))$ bit operations and $\deg(f)-1$ evaluations of P−dh in Section 3, which improves the result of [4]. We prove lower bounds on the degree of interpolation polynomials of P−dh in Section 4. 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 algorithm and the proof of the interpolation results.

Lemma 1 *Let $B \ge 0$ be an integer and $P(X) \in \mathbb{Z}[X]$ a polynomial of degree $D \ge B$ 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.

Proof. Fix $B \ge 0$. For $D = B$ the result is trivial. For $D \ge B+1$ with the convention $\binom{D-1-B}{-1} = 0$ we have

$$\begin{aligned}
S &:= \sum_{d=0}^{D-B} \binom{D-B}{d} (-1)^{D-B-d} P(X+d) \\
&= \sum_{d=0}^{D-B} \left(\binom{D-1-B}{d} + \binom{D-1-B}{d-1} \right) (-1)^{D-B-d} P(X+d) \\
&= \sum_{d=0}^{D-1-B} \binom{D-1-B}{d} (-1)^{D-1-B-d} (P(X+1+d) - P(X+d)) \\
&= \sum_{d=0}^{D-1-B} \binom{D-1-B}{d} (-1)^{D-1-B-d} Q(X+d),
\end{aligned}$$

where $Q(X) := P(X+1) - P(X)$ has degree $D-1$ and leading coefficient $a_D D$. By induction we get

$$S = \frac{a_D D(D-1)!}{B!} X^B + T_{B-1}(X),$$

where $T_{B-1}(X)$ is a polynomial of degree at most $B-1$. □

3 A Reduction Algorithm

In this section we present results emphasizing the importance of analyzing the interpolation polynomials of $P-$dh. More precisely, we show that a polynomial f that coincides with $P-$dh on some *fixed and known* points x can be used as an oracle to efficiently compute dh.

Theorem 1 *Let $0 \neq \gamma \in \mathbb{F}_q$ be an element of prime order t, $P(X) \in \mathbb{Z}_t[X]$ a polynomial of degree D with $2 \leq D \leq t-1$, and $f(X) \in \mathbb{F}_q[X]$ such that*

$$f(\gamma^x) = \gamma^{P(x)}, \quad x \in S,$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ of cardinality $|S| = H - s$ with $1 \leq H \leq t$. Then there exist a subset $R \subseteq S$ of cardinality $|R| \geq H - D + 2 - (D-1)s$ and an algorithm $\mathcal{A}$ that computes

$$\mathcal{A}(\gamma^x) = \gamma^{x^2}$$

for all $x \in R$ with $O(D \log(t) \max(D, \log(q)^2))$ bit operations and $D-1$ evaluations of $f(X)$.

Proof. Let R be the set of $x \in \{N+1, \ldots, N+H\}$ for which $x+i \in S$ for $0 \leq i \leq D-2$. Then obviously

$$|R| \geq H - D + 2 - (D-1)s.$$

Let γ^x be given for fixed $x \in R$. The algorithm $\mathcal{A}$ proceeds as follows. We evaluate $f(X)$ in γ^{x+d}, $0 \leq d \leq D-2$, and put

$$\eta_d = f(\gamma^{x+d}) = \gamma^{P(x+d)}, \quad 0 \leq d \leq D-2.$$

Then we get by Lemma 1 with $B = 2$

$$\zeta := \prod_{d=0}^{D-2} \eta_d^{\binom{D-2}{d}(-1)^{D-d}} = \gamma^{\sum_{d=0}^{D-2}\binom{D-2}{d}(-1)^{D-d}P(x+d)} = \gamma^{ex^2+c_1x+c_0}$$

with some constants c_1 and c_0 and $e := a_D D!/2$. This needs $O(D^2)$ additions in $\mathbb{Z}_t$ for determining recursively all binomial coefficients modulo t, $O(D)$ powers, inversions, and multiplications in $\mathbb{F}_q$, i. e.,

$$O(D \log(t) \max(D, \log(q)^2))$$

bit operations (cf. [1, Chapters 5 and 6]). Next we eliminate the linear term by computing

$$\xi := \zeta \cdot (\gamma^x)^{-c_1} \gamma^{-c_0} = \gamma^{ex^2}.$$

Finally, we determine the unique root of $X^e - \xi$, i. e., $\gamma^{x^2} = \xi^{e^{-1}}$, where e^{-1} denotes the inverse of e modulo t, in $O(\log(t)\log^2(q))$ bit operations (cf. [1, Theorem 7.3.1]). □

4 Interpolation

Theorem 2 *Let $0 \neq \gamma \in \mathbb{F}_q$ be an element of prime order t, $P(X) \in \mathbb{Z}_t[X]$ a polynomial of degree D with $2 \leq D \leq t-1$ and leading coefficient a_D, and $f(X) \in \mathbb{F}_q[X]$ such that*

$$f(\gamma^x) = \gamma^{P(x)}, \quad x \in S,$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ *of cardinality* $|S| = H - s$ *with* $1 \le H \le t$. *Then we have*

$$\deg(f) \ge \max\left(\frac{H-(D+1)(s+1)+1}{2^{D-1}}, \frac{H-D(s+1)+1-r}{2^{D-2}}\right),$$

where r *denotes the least residue of* $a_D D!$ *modulo* t.

Proof. Let R_1 be the set of $x \in \{N+1, \ldots, N+H\}$ for which $x+i \in S$ for $0 \le i \le D$. We see that

$$|R_1| \ge H - D - (D+1)s.$$

By Lemma 1 with $B = 0$ we have

$$\prod_{d=0}^{D} f(\gamma^{x+d})^{\binom{D}{d}(-1)^{D-d}} = \gamma^{\sum_{d=0}^{D}\binom{D}{d}(-1)^{D-d}P(x+d)} = \gamma^{a_D D!}, \quad x \in R_1,$$

and the polynomial

$$F_1(X) = \prod_{\substack{d=0 \\ D-d \text{ even}}}^{D} f(\gamma^d X)^{\binom{D}{d}} - \gamma^{a_D D!} \prod_{\substack{d=0 \\ D-d \text{ odd}}}^{D} f(\gamma^d X)^{\binom{D}{d}}$$

has at least $|R_1|$ zeros, namely γ^x with $x \in R_1$. Analogously to Lemma 1 we get

$$\sum_{\substack{d=0 \\ D-d \text{ even}}}^{D} d\binom{D}{d} = \sum_{\substack{d=0 \\ D-d \text{ odd}}}^{D} d\binom{D}{d}$$

and the leading coefficient of $F_1(X)$ is not zero. $F_1(X)$ is not identical to zero and thus $\deg(F_1) \ge |R_1|$. Now we have

$$\deg(F_1) = \sum_{\substack{d=0 \\ D-d \text{ odd}}}^{D} \binom{D}{d} \deg(f) = \frac{1}{2}\sum_{d=0}^{D}\binom{D}{d}\deg(f) = 2^{D-1}\deg(f)$$

and thus

$$\deg(f) \ge \frac{|R_1|}{2^{D-1}}.$$

Now let R_2 be the set of $x \in \{N+1, \ldots, N+H\}$ for which $x+i \in S$ for $0 \le i \le D-1$. We see that

$$|R_2| \ge H - D + 1 - Ds.$$

By Lemma 1 with $B = 1$ we have

$$\begin{aligned}\prod_{d=0}^{D-1} f(\gamma^{x+d})^{\binom{D-1}{d}(-1)^{D-1-d}} &= \gamma^{\sum_{d=0}^{D-1}\binom{D-1}{d}(-1)^{D-1-d}P(x+d)} \\ &= \gamma^{a_D D! x + b}, \quad x \in R_2,\end{aligned}$$

for some integer b and the nonzero polynomial

$$F_2(X) = \prod_{\substack{d=0 \\ D-1-d \text{ even}}}^{D-1} f(\gamma^d X)^{\binom{D-1}{d}} - \gamma^b X^r \prod_{\substack{d=0 \\ D-1-d \text{ odd}}}^{D-1} f(\gamma^d X)^{\binom{D-1}{d}}$$

has at least $|R_2|$ zeros, namely γ^x with $x \in R_2$. We have

$$\deg(F_2) = 2^{D-2}\deg(f) + r$$

and thus $\deg(f) \ge (|R_2| - r)/2^{D-2}$. ⊏|

5 Final Remarks

COMPOSITE t.
Put $e := a_D D!/2$. With the restriction $\gcd(e,t) = 1$ Theorem 1 is also valid for composite t. Without this restriction the solution of $X^e - \xi$ in the proof of Theorem 1 is not unique, but in many cases the right solution can be efficiently determined depending on the prime factorization of e. We quickly sketch how to compute the rth root of ξ for every prime factor r of e using ideas mentioned in [1, Chapter 7.3]. Note that since $x^{ab} = (x^a)^b$, taking the rth root for every prime factor r of e is sufficient to solve the problem of taking the eth root.
Now let r be a prime factor of t. If $\gcd(r,t) = 1$ then finding the rth root can be done as described in Theorem 1. Otherwise let $t = r^s u$ with $r \not| u$. For $m|t$, let C_m denote the unique subgroup of order m contained in G, where $G \subseteq \mathbb{F}_q^*$ is the subgroup of order t generated by γ. Then we have the isomorphism

$$G \cong C_{r^s} \times C_u.$$

Thus we can represent any element $x \in G$ as a pair $(x_r, x_u) \in C_{r^s} \times C_u$. The transformation is given by $x \mapsto (x^u, x^{r^s})$ and $(x_r, x_u) \mapsto x_r^\alpha x_u^\beta$, where $\alpha u + \beta r^s = 1$. The idea is to compute the rth root of ξ by computing it in each direct factor separately. The rth root of ξ in C_u is unique and can be efficiently computed as mentioned in the proof of Theorem 1. Instead of computing the rth root of ξ in C_{r^s} we compute γ^{x^2} in C_{r^s} directly from γ^x. This can be done by a "baby step-giant step" algorithm [14], see also [10]. For every prime factor r of e, the running time is $O(r \log^4(t))$ bit operations. The overall running time to compute the eth root is $O(T(e) \log^4(t))$ bit operations, where $T(e)$ denotes the sum of the prime factors of $\gcd(e,t)$.
With the restriction $t \not| a_D D!$ Theorem 2 is valid for composite t.

POLYNOMIALS OF HIGH DEGREE.
It seems to be not natural that the degree of the interpolation polynomial decreases if the degree of $P(X)$ increases in Theorem 2. Nontrivial results of this kind for $D \geq \log(t)$ are particularly interesting.

RELATION TO DISCRETE LOGARITHM.
Obviously, the Diffie-Hellman key exchange depends also on the hardness of the discrete logarithm ind_γ defined by

$$ind_\gamma(\gamma^x) = x, \quad 0 \leq x \leq t-1.$$

For results on interpolation polynomials of ind_γ see [2, 8, 9, 11, 12, 13, 15, 17].

BIVARIATE CASE.
With the method of [16] we can prove lower bounds on the degree of interpolation polynomials of the mappings P-DH$(\gamma^x, \gamma^y) = \gamma^{P(x)y}$ with an univariate polynomial P(X). Lemma 1 can be used to design a reduction algorithm to DH. It would be interesting to find similar results for the general case that P-DH$(\gamma^x, \gamma^y) = \gamma^{P(x,y)}$ with a nonlinear bivariate polynomial $P(X,Y)$.

COMPARISON WITH [4].
Note that in [4] similar results as given in Section 3 were proven though the presented results in this work are more efficient in terms of running time of the reduction algorithm and number of evaluations of the function f. The reason for the more efficient reduction is that in our

setting the points x for which the polynomial $f(\gamma^x)$ coincides with the function $\gamma^{P(x)}$ are *known*. In [4], the function f is viewed as an *oracle* that produces the correct answers $\gamma^{P(x)}$ for a certain fraction of all inputs, randomized over internal coin tosses. So, for a fixed x it is not known if $f(\gamma^x) = \gamma^{P(x)}$ does hold true or not.

Elliptic Curves.
The existence of subexponential algorithms for solving the discrete logarithm problem in finite fields motivates the consideration of other groups. An alternative used in practice is the group of points on an elliptic curve over a finite field. Lower bounds on the degree of interpolation polynomials of the Diffie-Hellman mapping were obtained in [6] and of the discrete logarithm in [5].

Acknowledgments.
Parts of this paper were written during a visit of the second author to the University of Bochum. He wishes to thank Prof. H. Dobbertin and the Institute of Information Security for hospitality and financial support.
The second author is supported by DSTA research grant R-394-000-011-422.

References

[1] E. Bach and J. O. Shallit, Algorithmic number theory, Vol.1: Efficient algorithms. MIT Press, Cambridge, 1996.

[2] D. Coppersmith and I. Shparlinski, On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping, J. Cryptology 13 (2000), 339–360.

[3] E. El Mahassni and I. Shparlinski, Polynomial representations of the Diffie-Hellman mapping, Bull. Austral. Math. Soc. 63 (2001), 467–473.

[4] E. Kiltz, A tool box of cryptographic functions related to the Diffie-Hellman function, Indocrypt'01, Lecture Notes Comp. Science 2247, 339–349.

[5] T. Lange and A. Winterhof, Polynomial Interpolation of the Elliptic Curve and XTR Discrete Logarithm, Proc. COCOON'02, Lecture Notes Comp. Science 2397, 137–143.

[6] T. Lange and A. Winterhof, Interpolation of the elliptic-curve Diffie-Hellman mapping, Proc. AAECC 15, Toulouse, 2003, to appear.

[7] W. Meidl and A. Winterhof, A polynomial representation of the Diffie-Hellman mapping, Appl. Algebra Engrg. Comm. Comput. 3 (2002), 313–318

[8] G. C. Meletiou, Explicit form for the discrete logarithm over the field GF(p, k), Arch. Math. (Brno) 29 (1993), 25–28.

[9] G. Meletiou and G. L. Mullen, A note on discrete logarithms in finite fields, Appl. Algebra Engrg. Comm. Comput. 3 (1992), 75–78.

[10] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of applied cryptography. CRC Press, Boca Raton 1997.

[11] G. L. Mullen and D. White, A polynomial representation for logarithms in GF(q), Acta Arith. 47 (1986), 255–261.

[12] H. Niederreiter, A short proof for explicit formulas for discrete logarithms in finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990), 55–57.

[13] H. Niederreiter and A. Winterhof, Incomplete character sums and polynomial interpolation of the discrete logarithm, Finite Fields Appl. 8 (2002), 184–192.

[14] D. Shanks, Class number, a theory of factorization and genera, in Proc. Symp. Pure Math. 20, pp. 415-440. AMS, Providence, R.I., 1971.

[15] A. L. Wells, Jr., A polynomial form for logarithms modulo a prime, IEEE Trans. Inform. Theory 30 (1984), 845–846.

[16] A. Winterhof, A note on the interpolation of the Diffie-Hellman mapping, Bull. Austral. Math. Soc. 64 (2001), 475–477.

[17] A. Winterhof, Polynomial interpolation of the discrete logarithm, Des. Codes Cryptogr. 25 (2002), 63–72.