Polynomial Interpolation of the k-th root of the Discrete Logarithm

Gerasimos C. Meletiou

A.T.E.I. of Epirus, Arta, GREECE

Definition of the Discrete Logarithm Function

Let

G *be a cyclic group of order t,* $\left|\langle \mathrm{g} \rangle\right| = \left|\mathrm{G}\right| = \mathrm{t}$*,*

$Y \in \mathrm{G}$ *be an element of the group* G*.*

The Discrete Logarithm of Y *to the base* g *is the smallest positive integer* $\mathrm{x} : 0 \le \mathrm{x} < \mathrm{t}$ *such that* $Y = g^{x}$*.*

Definition of the k-th root of the Discrete Logarithm

Let

G *be a cyclic group of order t,* $\left|\langle g \rangle\right| = \left|G\right| = t$*,*

$Y \in G$ *be an element of the group* G*.*

A k-th root of the Discrete Logarithm of Y *to the base* g *is an integer* $x : 0 \le x < t$ *satisfying* $Y = g^{x^k}$ *if such a* x *exists.*

Remarks:

1) Existence and uniqueness of the k-th root of the discrete logarithm are not guaranteed.

In the case $\left|\left\{x : g^{x^k} = Y\right\}\right| \geq 2$ *branches of the k-th root of the discrete logarithm are defined.*

2) Group G *and parameters* g *and* t *can be chosen in such a way that computing discrete logarithms to the base* g *is infeasible. Also* t *can be chosen such that obtaining k-th roots modulo* t *is hard.*

The k-th root of the discrete logarithm is used as one-way function in cryptography:

- *Group signature schemes*
- *Publicly verifiable secret sharing schemes*
- *Electronic cash*
- *Offline electronic cash systems*
- *Anonymity control in multi-bank e-cash system*
- *History-based signatures*

Important references related to the definition of the k-th root of the discrete logarithm

Camenisch J L, Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem, Doctoral Dissertation, ZURICH, 1998.

Camenisch, J., Stadler, M.: Efficient group signature schemes for large groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997).

Lysyanskaya, A., Ramzan, Z.: Group blind digital signatures: A scalable solution to electronic cash. In: Hirschfeld, R. (ed.) FC 1998. LNCS, vol. 1465, pp. 184–197. Springer, Heidelberg (1998).

References related to cryptographic applications

Ateniese, G., Tsudik, G.: Some open issues and new directions in group signatures. In: Franklin, M. (ed.) FCT 1999. LNCS, vol. 1684, pp. 196–211. Springer,Heidelberg (1999).

Bresson E. and J. Stern, Efficient Revocation in Group Signatures, PKC 2001, LNCS 1992, pp. 190-206, 2001, Springer-Verlag Berlin Heidelberg 2001.

Bussard L., R. Molva, and Y. Roudier, History-Based Signature or How to Trust Anonymous Documents, iTrust 2004, LNCS 2995, pp. 78-92, 2004, Springer-Verlag Berlin Heidelberg 2004.

Stadler, M.: Publicly verifiable secret sharing. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 190–199. Springer, Heidelberg (1996).

Jeong I. R. and D. H. Lee : Anonymity Control in Multi-bank E-Cash System, INDOCRYPT 2000, LNCS 1977, pp. 104-116, 2000, Springer-Verlag Berlin Heidelberg 2000.

Pavlovski C. and Colin Boyd, Attacks Based on Small Factors in Various Group Structures, ACISP 2001, LNCS 2119, pp. 36-50, 2001, Springer-Verlag Berlin Heidelberg 2001.

Jacques Traore, Group Signatures and Their Relevance to Privacy-Protecting Offline Electronic Cash Systems, ACISP'99, LNCS 1587, pp. 228-243, 1999, Springer-Verlag Berlin Heidelberg 1999.

Remarks concerning the parameters in most of the applications:

- t *is an RSA modulus that, is* $t = p \cdot q$, p *and* q *are big primes and the factorization of* t *is unknown.*
- *In some applications* $t = p^2 \cdot q$, p *and* q *are primes.*
- *Concerning* k *it may be equal to two (square root), also* k *may be equal to* e, *the encryption exponent of the RSA (root of odd order).*

Polynomial representation of Cryptographic Functions

Functions from a finite field to itself can always be represented by polynomials (Lagrangian interpolation).

Interpolation and "approximation" techniques have been applied to address cryptographic problems.

Polynomial representation of Cryptographic Functions – The investigation of computing the function using Lagrangian Interpolation.

I. *Deduction of exact polynomial form for the cryptographic function over the finite field.*

II. *Interpolation of the cryptographic function over a set of given data, proper subset of the finite field.*

(I) Explicit formula for the Discrete Logarithm.

Let p *be a prime,* $g \in Z_p^*$, g *is a generator of the multiplicative group of the field* Z_p, *that is* $\langle g \rangle = Z_p^*$.

Then the polynomial formula:

$$-1 + \sum_{i=1}^{p-2} \left(g^{-i} - 1 \right)^{-1} \cdot x^i$$

represents the discrete logarithm of x *to the base* g, *for all* $x \in Z_p^*$.
Interpolation polynomial has largest possible degree $p-2$.
Surprisingly enough the functions for the coefficients are very simple.

(I) Explicit formula for the Discrete Logarithm - References

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

Meletiou, G.C., Mullen, G.L.: A note on discrete logarithms in finite fields. Appl. Algebra Engrg. Comm. Comput. 3(1), 75–78 (1992).

Mullen, G.L., White, D.: A polynomial representation for logarithms in GF(q). Acta Arith. 47(3), 255-261 (1986).

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

(I) Explicit formulas for other cryptographic functions

Aly, H., Winterhof, A.: Polynomial representations of the Lucas logarithm. Finite Fields Appl. 12(3), 413-424 (2006).

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

(II) Interpolation of the Discrete Logarithm over a set of given data – Lower bounds.

Let p *be a prime,* $g \in Z_p^*$. *Consider the subset:* $S \subseteq \{1, 2, \ldots, p-1\}$, *of order* $|S| = p - 1 - s$. *Let* $F(X) \in Z_p[X]$ *be a polynomial satisfying* $F(g^x) = x$ *for all* $x \in S$.

Then we have:

$$\deg(F) \geq p - 2 - 2s \quad \textit{(lower bound).}$$

Coppersmith, D., Shparlinski, I.: On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping. J. Cryptology 13(3), 339–360, (2000).

Niederreiter, H., Winterhof, A.: Incomplete character sums and polynomial interpolation of the discrete logarithm. Finite Fields Appl. 8(2), 184-192 (2002).

Shparlinski, I.E.: Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness. Progress in Computer Science and Applied Logic, vol. 22. Birkhauser Verlag, Basel (2003).

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

(II) Interpolation of other cryptographic functions over a set of given data – Lower bounds.

Adelmann, C., Winterhof, A.: Interpolation of functions related to the integer factoring problem. In: WCC 2005. LNCS, vol. 3969, pp. 144–154. Springer, Heidelberg (2006).

Aly, H., Winterhof, A.: Polynomial representations of the Lucas logarithm. Finite Fields Appl. 12(3), 413-424 (2006).

Coppersmith, D., Shparlinski, I.: On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping. J. Cryptology 13(3), 339–360, (2000).

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

Meidl, W., Winterhof, A.: A polynomial representation of the Diffie-Hellman mapping. Appl. Algebra Engrg. Comm. Comput. 13, 313–318 (2002).

Shparlinski, I.E.: Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness. Progress in Computer Science and Applied Logic, vol. 22. Birkhauser Verlag, Basel (2003).

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

Meletiou, G.C., Winterhof, A.: Interpolation of the Double Discrete Logarithm. In WAIFI 2008, LNCS vol. 5130, pp. 1–10, Springer, Heidelberg, 2008.

Definition of the Double Discrete Logarithm Function (Similar to the definition of the root of the Discrete Logarithm).

Let G *be a cyclic group of order t,* $\left|\langle g \rangle\right| = |G| = t$*,*

Let $h \in \mathbb{Z}_t^*$ *be an element of order* $\left|\langle h \rangle\right| = m$*.*

The Double Discrete Logarithm of an element $z = g^{h^x} \in G$ *to the bases* g *and* h *is the unique* $x : 0 \le x < m$*.*

Main results - Roots of odd order

Theorem 1. *Let* p *be a prime,* $g \in Z_p^*$, $\left|\langle g \rangle\right| = t$ *and let* $k \geq 1$ *be an integer s.t.* $\gcd\left(k, \phi(t)\right) = 1$. *Let* $S \subseteq Z_t^*$ *be a subset of order* $\left|S\right| = \phi(t) - s$. *We assume the existence of a polynomial* $F(X) \in Z_p[X]$ *s.t.* $F\left(g^{x^k}\right) = x$ *for all* $x \in S$.

Then we have $\deg(F) \geq \dfrac{\varphi(t) - 2s}{2}$ *(lower bound).*

Remarks

The exponent k is odd and relatively prime to $\phi(t)$ *and, of course, the k-th root function becomes a bijection.*

The main motivation stems from RSA. In this case k *is the encryption exponent* e*. In some applications message* m *is encrypted as* $c \equiv m^e \pmod{N}$ *and* g^{m^e} *becomes public. Recovering* m *from* g^{m^e}*, or verifying properties of* m *is the problem (Proofs of Knowledge of Roots of Discrete Logarithms-see Camenisch).*

Main results - Square Roots of Discrete Logarithms.

Theorem 2. *Let* p *be a prime,* $g \in Z_p^*$, $\left|\langle g \rangle\right| = t$ *and* t *be also a prime. Consider the subset:* $S \subseteq Z_t^*$, *of order* $|S| = \frac{t-1}{2} - s \leq \frac{t-1}{2}$. *Let* $F(X) \in Z_p[X]$ *be a polynomial satisfying* $F\left(g^{x^2}\right) = x$ *for all* $x \in S$.

Then we have:

$$\deg(F) \geq \frac{t-1-4s}{32}$$ *(lower bound).*

Main results - Square Roots of Discrete Logarithms – Remarks.

1) *By* QR_t *we denote the set of all quadratic residues modulo* t. QR_t *is a subgroup of* Z_t^*.
2) *The assumption* $t \equiv 3 \pmod 4$ *implies that for all* $x \in Z_t^*$, x *is a quadratic residue iff* $-x$ *is a quadratic non residue. Also that eacs element of* QR_t *has exactly two square roots: one in* QR_t *and one in* QNR_t.
3) *Under this assumption the square root function becomes a bijection from* QR_t *to* QR_t.

Main results - Square Roots of Discrete Logarithms.

Theorem 3. *Let* p *be a prime,* $g \in Z_p^*$, $\left|\langle g \rangle\right| = t$ *and* $t \equiv 3 \pmod 4$ *be also a prime. Consider the subset:* $S \subseteq QR_t \subseteq Z_t^*$, $\left|S\right| = \frac{t-1}{2} - s \le \frac{t-1}{2}$, *the elements of* S *are quadratic residues. Let* $F(X) \in Z_p[X]$ *be a polynomial satisfying* $F\left(g^{x^2}\right) = x$ *for all* $x \in S$.

Then we have:

$$\deg(F) \ge \max\left\{\frac{t-1-4s}{32}, \frac{t-1-4s}{2v^3}\right\}$$ *(lower bound),*

where v *is the smallest quadratic residue* $\bmod t$, $v \in \{2,3,4\}$.

Main results –Remark

The case of the RSA modulus is addressed. We assume that

1) $t = N = p \cdot q,\ p$ *and* q *are big primes.*

2) $p \equiv q \equiv 3 \pmod 4$.

The second assumption guarantees that each quadratic residue in Z_N^* *has exactly four square roots an that exactly one of them is a quadratic residue* $\pmod N$. *The square root function becomes a bijection. We generalize the previous theorem.*

Main results - Square Roots of Discrete Logarithms.

Theorem 4. *Let* r *be a prime,* $g \in Z_r^*$, $\left|\langle g \rangle\right| = N$, $N = p.q$ *an RSA modulus. In addition we assume that* $p \equiv q \equiv 3 \pmod 4$. *Consider the subset:*

$S \subseteq QR_N \subseteq Z_N^*$, $\left|S\right| = \frac{\phi(N)}{4} - s \leq \frac{\phi(N)}{4}$, *the elements of* S *are quadratic residues. Let* $F(X) \in Z_r[X]$ *be a polynomial satisfying* $F\left(g^{x^2}\right) = x$ *for all* $x \in S$.

Then we have:

$$\deg(F) \geq \frac{\phi(N) - 8s}{4v^3}$$ *(lower bound),*

where v *is the smallest quadratic residue* $\bmod N$, $v \in \{2,3,4\}$.

Thank you very much

for your kind attention