# Trapdoor one way functions associated with exponentiation

Virendra Sule
Department of Electrical Engineering
Indian Institute of Technology Bombay, Powai
Mumbai 400076, India
(vrs@ee.iitb.ac.in)

March 15, 2011

**Abstract**

This paper shows that if exponentiation $b = X^k$ in groups of finite field units or $B = [k]X$ in elliptic curves is considered as encryption of $X$ with exponent $k$ treated as symmetric key, then the decryption or the computation of $X$ from $b$ (respectively $B$) can be achieved in polynomial time with a high probability under random choice of $k$. Since given $X$ and $b$ or $B$ the problem of computing the discrete log $k$ is not known to have a polynomial time solution, the exponentiation has a trapdoor property associated with it. This paper makes this property precise. Further the decryption problem is a special case of a general problem of solving equations in groups. Such equations lead to more such trapdoor one way functions when solvable in polynomial time. The paper considers single and two variable equations on above groups and determines their solvability.

*Keywords*: Exponential function, elliptic curves, division polynomials.

## 1 Introduction

Trapdoor one way functions are foundations of symmetric and public key encryption algorithms. While the RSA scheme gives rise to such a trapdoor function, the function $a^x$ defined from $\mathbb{Z}_e$ to the cyclic group $< a >$ (of order $e$) used in the Diffie Hellman key exchange scheme by itself is not known to have an associated trapdoor one way function property [1, p. 47]. Nevertheless, since the inverse of the exponential function (or computing the discrete logarithm (DL) $x$) is believed to be a hard computational problem over groups of finite field units and elliptic curves, exponentiation does turn out to be a one way function. Consider the exponential function $a^x$ from $0 < x < q-1$ taking values in the group $\mathbb{F}_q^*$. Given a primitive element $a$ and $b = a^x$ the computation of the discrete log $x = \log_a b$ is believed to be a hard problem (for a random $x$, primitive $a$ and $q$ with reasonable properties) while exponentiation $a^x$ is computable in polynomial time (in the logarithm of the order of $\mathbb{F}_q^*$). So what about computation of $a$ in the group when $b$ and $x$ are given? If this is also achievable in polynomial time in the logarithm of the group order, then $a^k$ can be called a candidate as a (generalized) one way function with trapdoor $k$ over this group. The generalization meant here is made precise by the following definition.

**Definition 1** (Generalized Trapdoor One Way Function (GTOWF))**.** A function $F(k, x)$ from arguments $x, k$ represented each by $n$-bit strings and taking values in arguments $y$ represented by $n$-bit strings is called a GTOWF with trapdoor $k$ if

1. Given the $n$-bit string for $k$ the value $y = F(k, x)$ can be computed in polynomial time in $n$ for every $x$ in the function's domain.

2. Given a random $k$ and a value $y$ in the domain of values of $F$ for which $x$ exists, all possible $x$ can be computed with high probability in polynomial time in $n$ such that $y = F(k, x)$.

3. Given a pair $x, y$ corresponding to a randomly chosen $k$ such that $y = F(k, x)$ there is no known polynomial time in $n$ algorithm to compute $k$.

Note that in this definition we do not insist on unique inverse $x$ for any values $y$ of $F$ given $k$ and moreover computations of $x$ given $y$ are possible in polynomial time with high probability for randomly chosen $k$, justifying the adjective generalized. In this paper we shall first make an elementary observation that the exponential function is GTOWF with high probability over the group of units of finite fields and explore analogous questions of solving equations over elliptic curve groups over this field.

### 1.1 Equations over groups

Our problem is in fact a special case of the problem of solving equations over groups. Let $G$ be a finite Abelian group of order $n$. Given a positive integer $k < n$ and an element $b$ of $G$ the equation

$$b = X^k$$

is an example of an equation over $G$ in one variable. This is also called the *exponential function* $X^k$ in $G$. One of the important questions in computational sciences is to determine conditions for solvability of equations over groups and studying complexity of computation of their solutions [3]. We shall consider this question on groups of units of finite fields and elliptic curve over finite fields. In more than one variables, an example of such an equation (say in two variables) is,

$$b = X^k Y^l \tag{1}$$

in which $k, l$ are given positive integers $< n$ and $b$ is a given element of the group. Let the group be an elliptic curve $E(K)$ over a field $K$. An example of a two variable equation on this group is

$$Q = [k]X \oplus [l]Y \tag{2}$$

where $Q$ is a given point on $E$ and $k, l$ given integers. While it is well known that computation of solutions of solvable equations over Abelian groups is achievable in polynomial time [4] in the group order, this fact is not practically useful in cryptography since the group order is exponential in the input bit length (that of the size of the exponent). Hence it is important to determine when such equations are solvable in polynomial time in the logarithm of the group order.

## 2 Trapdoors associated with exponential function

We consider special cases of groups, the group of units of a finite field $\mathbb{F}_q^*$, the group of modular units $\mathbb{Z}_n^*$ where $n = pq$, $p, q$ prime, and an elliptic curve over a finite field $E(K)$. In all of these cases the exponentiation function $X^k$ (or $[k]X$ taking values in an elliptic curve), which we shall call the *encryption function*, is known to be computable in polynomial time in the logarithm of the group order. Hence the exponential function is of trapdoor one way class if the problem of computing solutions $X$ from given the inputs $k$ and value of $X^k$ (which we call the *decryption problem*) is solvable in polynomial time in the logarithm of the order. (Hereafter we shall use the term polynomial time to always mean in terms of the logarithm of the order). Analogously, in two variables $X$, $Y$ the decryption problem over finite field $K$ is one of computing solutions $X$, $Y$ in $K^*$ (respectively $E(K)$) from a value $b = X^k Y^l$ (respectively $B = [k]X \oplus [l]Y$) given $k, l$.

### 2.1 Decryption in the group $\mathbb{F}_q^*$

Consider the equation $b = X^k$. There are two cases. In first case let $k$ be coprime to the order $n = (q-1)$ of $\mathbb{F}_q^*$. Then $l = k^{-1} \mod n$ exists and $b^l$ is the unique solution. In the second case let $d = (k, n)$, $k = dk_1$, $l_1 = k_1^{-1} \mod n$. Compute $b_1 = b^{l_1}$. Then we have the equation

$$b_1 = X^d \tag{3}$$

If $a$ is a solution then any other solution $x$ satisfies $(xa^{-1})^d = 1$. Hence if one solution is found other solutions can be obtained from all $d^{\text{th}}$ roots of unity in $\mathbb{F}_q$. Since $d|(q-1)$ there exist $d$ such roots given by $d$ distinct powers of $g^{(q-1)/d}$ where $g$ is a primitive element of $\mathbb{F}_q^*$. These computations are polynomial time due to fast exponentiation. Hence it is necessary to examine computation of one solution of the above equation. This problem can be solved as an application of Berlekamp's algorithm for irreducible factorization of a polynomial in $\mathbb{F}_q^*$ [2] which has complexity $O(d^2 \log q)$. For random $k$ the gcd $d = (k, n)$ has with high probability only small divisors of $n$, alternatively with high probability has length of the order $\log n$. Hence with high probability the above equation can be solved in polynomial time. We state this as

**Proposition 1.** The exponential function $y = x^k$ where $x, y$ are in $\mathbb{F}_q^*$ and random exponent $k$ is a GTOWF.

### 2.2 Decryption in $\mathbb{Z}_n^*$

Consider the equation $b = X^k$. The order of the group is $\phi(n) = (p-1)(q-1)$, the Euler function evaluated at $n$. There are again two cases as above. Let $(k, \phi(n)) = 1$, then there is a unique $l < n$ such that $kl = 1 \mod \phi(n)$. Hence $X = b^l \mod n$ is a unique solution. In the next case $d = (k, \phi(n)) > 1$. Let $k = k_1 d$ where $k_1$ is coprime to $\phi(n)$ and $k_1 l_1 = 1 \mod \phi(n)$. Then the problem reduces to computing $d^{\text{th}}$ roots of $b_1 = b^l \mod n$. This problem is polynomial time by Chinese reminder theorem if prime factorization of $n$ are known. When these are known computation of $X$ is transferred to corresponding problems of computing $d^{\text{th}}$ rots modulo the prime factors hence the problem reduces to the field case above. This proves

**Corollary 1.** The exponentiation function $X^k$ on $\mathbb{Z}_n^*$ is a GTOWF if prime factors $p$, $q$ of $n$ are known.

### 2.3 Decryption on elliptic curve

Next we turn to the problem of solving the single variable equation

$$B = [k]X \tag{4}$$

where $B$ is a given point in of an elliptic curve $E(K)$ over a finite field $K$. First we assume that $\operatorname{char} K \neq 2$. Let $X = (x, y)$ be the unknown co-ordinates of $X$ a point on $E(K)$ to be solved. Let $n$ be the order of $E(K)$. We can thus assume $k < n$ or consider modulo $n$. If $K$ is coprime to $n$ then for $l = k^{-1} \mod n$, $X = [l]B$ is a solution. If $Y$ is another solution then $[k]([l]B \ominus Y) = \infty$. Hence all solutions can be obtained by listing $K$-rational points in $\ker k$ as an endomorphism of $E(K)$. Hence complexity of computation of $\ker k$ is the deciding factor in trapdoor one way-ness in this special case. Next consider the case when $(k, n) = d$. Let $k = dk_1$, $l_1 = k_1^{-1} \mod n$, $B_1 = [l]B$ then the equation reduces to $B_1 = [d]X$ where $d|n$. If $A$ is one solution then any other solution $Y$ satisfies $[d](X \ominus Y) = \infty$. Thus again this involves the problem of computation of $K$-rational points of $\ker d$ as an endomorphism of $E(K)$ to get all solutions of the equation (4). It is well known that the $x$-co-ordinates of points in $\ker d$ in $E(K)$ can be computed by computing $K$-rational roots of the $d^{\text{th}}$ division polynomial. We now examine how one solution $X$ can be computed. The theorem on representation of endomorphisms by division polynomials [5, Theorem 3.6] resolves this problem. (We refer to definition of division polynomials given in [5, Section, 3.2]. Following proposition directly follows from this theorem.

**Proposition 2.** For a positive integer $d$ There exist rational functions $r_1, r_2, r_3$ in $K(X)$ such that if $(x, y)$ denotes co-ordinates of a point on $E(K)$, then

$$[d](x, y) = (r_1(x), r_2(x) + y r_3(x)) \tag{5}$$

Further, the maximum of the degree of numerator and denominator of $r_i(x)$ is $d^2$.

Consider now the problem of solving for points $X$ in $E(K)$ from the equation

$$B = [d]X \tag{6}$$

where $B$ is a given point on $E(K)$ and $d$ a positive integer $< n$. Let $B = (x_b, y_b)$. Denote the rational functions $r_i(x)$ by relatively prime polynomial fractions over $K[x]$ as

$$r_i(x) = \frac{f_i(x)}{g_i(x)}$$

for $i = 1, 2, 3$. Denoting $B = (x_0, y_0)$ the above equation leads to equations in $x, y$, the co-ordinates of $X$, as follows.

$$\begin{aligned} g_1(x)x_0 &= f_1(x) \\ g_2(x)g_3(x)y_0 &= f_2(x)g_3(x) + y f_3(x)g_2(x) \end{aligned} \tag{7}$$

To this we need to add the equation defining the elliptic curve $E$. Hence the $x$ co-ordinates of solutions $X$ are $K$-roots of the first equation for which the elliptic curve equation is also satisfied for some $y$ in $K$. These $y$ co-ordinates can be computed by solving the second linear equation in $y$ for the roots $x$. The solution $y$ exists at all such points since $f_3(x)g_2(x) = 0$ would mean the point $X$ is $\infty$ and this is possible only when $B = \infty$.

Solution of $K$-roots of the first equation above is again achievable by Berlekamp's algorithm which will at most take time $O(d^4 \log q)$ since max degree of $f_1, g_1$ is $d^2$. Since (as we argued in the case of $\mathbb{F}_q^*$ above), for random $k$ the gcd $d = (k, n)$ is a small divisor of $n$ with high probability (or of length $\log n$). Hence the problem of computing the root of the first equation is polynomial time with high probability. If $R$ is a point on $E(K)$ obtained from solving the $K$-roots of the above polynomial equations, then all other associated solutions of (6) can be obtained as $R \ominus Z$ where $Z$ is a point in $\ker d$. Hence to get all solutions $X$ of the equation we need to compute the set of all points in $\ker d$ as an endomorphism of $E(K)$. Since all such points are solutions of the $d^{\text{th}}$ division polynomial which is of degree $d^2$ by the same arguments it can be observed that the complete set of solutions of (4) can be computed in polynomial time with high probability for a random choice of $k$. This proves

**Theorem 1.** The exponential function $[k]X$ on $E(K)$ is a GTOWF.

### 2.4 Case of char 2

The analysis of the decryption problem on $E(K)$ above assumes from the start that char $K \neq 2$. This is because the formulas for division polynomials in char 2 are different. This case is treated in this subsection. The elliptic curve $E$ in this case is assumed to be non-supersingular with defining equation

$$Y^2 + XY = X^3 + a_2X^2 + a_6$$

with $a_2$ in $\mathbb{F}_q$ and $a_6$ in $\mathbb{F}_q^*$, $q = 2^m$. Then as shown in [6, III.4.2] if $P = (x, y)$ and $[d]P \neq \infty$ then the division polynomials $f_r$ which are only functions of $x$ can be recursively computed such that

$$[d]P = (x + \frac{f_{d-1}f_{d+1}}{f_d^2},\ x + y + \frac{(x^2 + x + y)f_{d-1}f_df_{d+1} + f_{d-2}f_{d+1}^2}{xf_d^3})$$

with degree of $f_d$ of the order $O(d^2)$. However this expression is of the form (5)

$$[d]P = (r_1(x), r_2(x) + r_3(x))$$

with rational functions $r_i$ and hence leads to similar equations as (7). The degree of the polynomial to be solved for $x$ in $\mathbb{F}_{2^m}$ in the first of these can be observed to be same as $\deg f_d^2$. The $y$ co-ordinate can be solved from the second equation with the additional equation of the elliptic curve. This computation is equivalent to solving again a first order equation in $\mathbb{F}_{2^m}$ by squaring the second equation and substituting for $y^2$ from the elliptic curve equation. This shows that the equation (6) is solvable in polynomial time in $O((\deg f_d)^4 m)$. We thus have,

**Proposition 3.** The exponential function $[k]X$ on non-supersingular elliptic curves on $\mathbb{F}_{2^m}$ is a GTOWF.

## 3 Two variable equations

We shall now consider a system of two variable equations. Consider the system

$$\begin{aligned} b_1 &= X^a Y^b \\ b_2 &= X^c Y^d \end{aligned}$$

on $\mathbb{F}_q^*$. In this equation let $B_i$ be given elements of the group along with four integers $a, b, c, d$ less than order of the group. The problem is to solve for group elements $X, Y$. (Similar equation can be considered on $E(K)$). If $A, B$ is one solution then to get all solutions we need to solve the system of equations

$$\begin{aligned} I &= X^a Y^b \\ I &= X^c Y^d \end{aligned}$$

where $I$ is the group identity. Such a system can be solved by choosing $X$ a parameter and solving for $Y$ simultaneously from the resulting two equations. Hence existence of solution will depend on existence of a common root $Y$ to the two equations $x^{-a} = Y^b$ and $x^{-c} = Y^c$ where $x$ is a chosen parameter. This problem can be solved in polynomial time using above analysis of one variable equations by converting the problem to solving the resultant of the two polynomials over $\mathbb{F}_q^*$.

On elliptic curves $E(K)$ considered above, the two variables system of equations can be similarly converted to the form

$$\begin{aligned} -[a]P &= [b]Y \\ -[c]P &= [d]Y \end{aligned}$$

with arbitrary parameter point $P$. Then as in the one variable problem there will result two polynomials (computed from the systems of equations constructed from the division polynomials) whose common root in $K$ will give the $x$-co-ordinate of $Y$. Such common roots will require resultant computation of the two polynomials. These details are omitted. In conclusion it can be observed that existence and computation of two variable equations is achievable in polynomial time with high probability for randomly chosen $a, b, c, d$. This gives rise to possibilities of constructing additional GTOWFs.

## 4 Encryption schemes using exponentiation

As shown above the exponentiations in $K = \mathbb{F}_q^*$ and elliptic curves $E(K)$ are GTOWFs. Hence in principle they should be useful for encryption schemes. However their practical utility will depend on how fast can the encryption (exponentiation) $a^k$ or $[k]P$ and the decryption be computed. To recover the unique message $a$ or $P$ these will have to be recognized from the multiple solutions of the decryption problem. At a theoretical level this can be achieved by using another one way hash function $H(.)$ and sending the hash value $H(a)$ or $H(P)$ along with encryption and then check the hash value of solutions computed in the decryption problem. Computational details and analysis of security of such a scheme shall be developed elsewhere.

## 5 Conclusion

The exponential function on elliptic curve groups does have an associated trapdoor one way function of a generalized form defined in this article. However much further work on detailed computational analysis along with speeding up of the algorithm for irreducible factorization of polynomials in finite fields is necessary before this function can be utilized for cryptographic schemes.

Acknowledgement

The author is grateful to C. R. Rao Advanced Institute of Mathematics, Statistics and Computer science (CRRaoAIMSCS), Hyderabad, India, for supporting a visiting position in 2009-10 during which this work was initiated.

## References

[1] Hans Delfs, Helmut Knebl. Introduction to Cryptography, Principles and Applications. Springer 2002.

[2] J. v. z. Gathen, J. Gerhard. Modern computer algebra. Cambridge University Press, 2003.

[3] http://rjlipton.wordpress.com/2010/11/03/equations-over-groups-a-mess/

[4] M. Goldmann, A. Russell, The complexity of solving equations over finite groups. Information Computing, vol.178, no.1, pp.253-262, 2002.

[5] L. Washington, Elliptic curves, Number theory and Cryptography. Chapman & Hall/CRC press 2003.

[6] I. F. Blake, G. Seroussi, N. Smart, Elliptic curve cryptography. London Mathematical Society Lecture Note Series 265, Cambridge University Press 2002.