Analysis of Low Hamming Weight Products ⋆

Jung Hee Cheon *

ISaC and Dept. of Mathematics, Seoul National University, Seoul 151-737, Republic of Korea

HongTae Kim

Korea Air Force Academy, Republic of Korea

Abstract

Hoffstein and Silverman suggested a use of Low Hamming Weight Product (LHWP) to compute a random power in a group or a multiple of an element in a ring. It reduces the computation of powers in a group with fast endomorphisms such as the Galois field $\mathbb{F}_{2^n}$ and Koblitz elliptic curves. In this paper, we introduce a reduced representation of LHWP and apply them to attack the relevant cryptosystems.

Key words: low Hamming weight products, exponentiations, cryptanalysis, discrete logarithm problem

1 Introduction

Let G be an abelian group of order q with a generator g. Given an element $y \in G$, the discrete logarithm problem (DLP) on G asks to find $x \in \mathbb{Z}_p$ such that $y = g^x$. The exponentiations can be accelerated by using exponents with special structures [5,11,6,4], but most of them appeared to have less complexity than suggested [10,2], and so does not give any significant advantage over the ordinary exponents.

⋆ This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF-2006-0117).

* Corresponding author. This work was done while the first author was visiting UC Irvine.

Email addresses: jhcheon@snu.ac.kr (Jung Hee Cheon), kafa46@snu.ac.kr (HongTae Kim).

One exception is a method to use *Low Hamming Weight Products* (LHWPs) suggested by Hoffstein and Silverman in [6]. They introduced a product $x = x_1x_2x_3$ of integers as an exponent over $G = \mathbb{F}_{2^n}$, where each x_i has w_i nonzero digits in its binary representation. This type of exponents is called an exponent of weight (w_1, w_2, w_3) and accelerates the exponentiation g^x significantly. The computational advantage comes from the extensive use of the fast endomorphism *squaring* in the exponentiations. For example, only 17 multiplications are required for an exponentiation by an exponent of weight $(6, 7, 7)$ in a binary field if we use a normal basis. It can be also applied to scalar multiplications of a point in Koblitz curves, in which Frobenius map plays an role of a squaring in binary fields.

In this paper, we propose a new attack for the DLP with LHWP exponents. When the exponent is of form $x = x_1x_2x_3$ where x_1, x_2 and x_3 are drawn from the sets $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{X}_3$, respectively, the complexity of the DLP was assumed to be about $\max\{|\mathcal{X}_1|, |\mathcal{X}_2| \cdot |\mathcal{X}_3|\}$ if $|\mathcal{X}_1| \geq |\mathcal{X}_2|, |\mathcal{X}_3|$. We improve this attack by a factor of n for $G = \mathbb{F}_{2^n}$.

More precisely, we define a canonical representation of an element $z \in \mathbb{Z}/(2^n - 1)$ as $z = 2^k\bar{z}$ for integer k and maximum possible $\bar{z}$. Then we observe that $\bar{x} = 2^k\bar{x}_1\bar{x}_2\bar{x}_3$ for some k and the number of canonical elements of $\mathcal{X}$ is roughly $|\bar{\mathcal{X}}| \approx |\mathcal{X}|/n$. Using this we propose a variant of baby-step giant-step method [8], whose complexity can be as small as $\max\{|\mathcal{X}_1|, |\mathcal{X}_2| \cdot |\mathcal{X}_3|\}/n$. If $|\mathcal{X}_1| > |\mathcal{X}_2|, |\mathcal{X}_3|$, we can further improve the attack by splitting $\mathcal{X}_1$ into a sum of two elements, each of which belongs to a smaller set. For example, the complexity of the DLP with an exponent of weight (2,2,11) in a binary field was claimed to be more than 2^{80}, but our algorithm solves it in $2^{55.9}$ multiplications.

Similar attacks can be applied to a low Hamming weight product in τ-adic representation on Koblitz curves. For example, when using an exponent of weight $(6, 6, 6)$ on a Koblitz curve, the complexity of the DLP is reduced from 2^{80} to $2^{74.4}$.

The rest of papers are organized as follows: In Section 2, we introduce the notion of *rotation-free* elements for reduced representations. Using them, we analyze the DLP on binary fields and Koblitz curves in Section 3 and 4, respectively. We conclude in Section 5.

2 Rotation-free Elements

Let $\mathrm{wt}(x)$ denote the Hamming weight of $x \in \mathbb{Z}$, which is the number of nonzero coefficients in the binary representation of x. From now on, we use a

representative set $\{0, 1, 2, \ldots, 2^n - 2\}$ to express elements of $\mathbb{Z}/(2^n - 1)$. Thus $x \mod 2^n - 1$ is the integer in this representative set which is congruent to x modulo $2^n - 1$.

We define a relation $\sim$ on $\mathbb{Z}/(2^n - 1)$ as follows: Given two elements $a, b \in \mathbb{Z}/(2^n - 1)$, we define $a \sim b$ if and only if there exists a non-negative integer i such that $a = 2^i b$. Then $\sim$ is an equivalence relation on $\mathbb{Z}/(2^n - 1)$. We can simply check the followings:

(1) $a = 2^0 a$
(2) If $a = 2^i b$, then $a = 2^{n-i} b$ for a non-negative integer i.
(3) If $a = 2^i b$ and $b = 2^j c$ for non-negative integers i, j, then $a = 2^{i+j} c$.

Observe that a LHWP $x_1 x_2 x_3 \in \mathbb{Z}/(2^n - 1)$ is equal to $2^k \bar{x}_1 \bar{x}_2 \bar{x}_3$ where $0 \leq k < n$ and $\bar{x}_i$ is an element of the equivalence class of x_i. To reduce the redundancy of the representations of LHWPs, we need a subset of $\mathbb{Z}/(2^n - 1)$ which includes a set of representatives of the equivalence classes and is easily generated.

Definition 1 *An element $z \in \mathbb{Z}/(2^n - 1)$ is called* a rotation-free *element if there is a k-tuple $(a_1, a_2, \ldots, a_k)$ for a positive integer k satisfying*

(1) $a_i \geq a_1$ *for* $1 \leq i \leq k$
(2) $\sum_{i=1}^{k} a_i = n$
(3) $z = 2^{n-1} + 2^{n-1-a_1} + \cdots + 2^{n-1-(a_1+a_2+\cdots+a_{k-1})}$.

All the rotation-free elements of weight k can be easily generated by the following algorithm. Note that the corresponding k-tuple for a rotation-free element satisfies $ka_1 \leq a_1 + \cdots + a_k = n$.

Algorithm 1 (Generation of Rotation-free Elements)

(1) Input n and k
(2) Choose a positive integer $a_1 \leq n/k$
(3) For $i = 2$ up to $k - 1$, select an integer a_i such that

$$a_1 \leq a_i \leq n - (k - i)a_1 - \sum_{j=1}^{i-1} a_j$$

(4) Output $2^{n-1} + 2^{n-1-a_1} + \cdots + 2^{n-1-(a_1+a_2+\cdots+a_{k-1})}$

Note that the largest element of each equivalence class is a rotation-free element. Hence we can see that there is at least one rotation-free element in each equivalence class of $Z/(2^n - 1)$ with respect to the relation $\sim$.

Now we show that this number is not far from the number of equivalence classes.

Theorem 1 *Let n, k be positive integers with $k < n$ and $\mathrm{RF}(n,k)$ be the number of rotation-free elements of weight k in $\mathbb{Z}/(2^n-1)$. We have the followings:*

(1) $\mathrm{RF}(n,k) = \sum_{i=0}^{\lfloor \frac{n}{k} \rfloor - 1} \binom{n-2-ki}{k-2}$.

(2) There is at least one rotation-free element in each equivalence class.

(3) The difference $\mathcal{E}(n,k)$ between $\mathrm{RF}(n,k)$ and the number of equivalence classes on $\mathbb{Z}/(2^n-1)$ is at most

$$\binom{n-2}{k-2} - \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor - 1} \binom{n-2-ki}{k-1} + 1.$$

PROOF. We express an element z of weight k in $\mathbb{Z}/(2^n-1)$ uniquely as

$$2^{n-1-a_0} + 2^{n-1-(a_0+a_1)} + \cdots + 2^{n-1-(a_0+a_1+\cdots+a_{k-1})},$$

where $a_0, a_1, \ldots, a_k$ are positive integers such that $a_0 + a_1 + \cdots + a_k = n$.

Note that a rotation-free element z is the element of the form with $a_0 = 0$ and $a_i \geq a_1$. Hence $\mathrm{RF}(n,k)$ is the number of solutions $(a_1, \ldots, a_k)$ satisfying $a_1 + \cdots + a_k = n$ and $a_i \geq a_1$. Equivalently, it is the number of non-negative solutions $(a'_2, \ldots, a'_k)$ satisfying $a'_2 + \cdots + a'_k = n - ka_1$. Given a positive integer a_1, the number of such $(k-1)$-tuples is the number of multisets of cardinality $(k-1)$ with elements taken from a set of cardinality $(n-ka_1)$, that is $\binom{n-ka_1+k-2}{k-2}$. If we sum up $\binom{n-2-k(i-1)}{k-2}$ for all $1 \leq i \leq n/k$, we obtain $\mathrm{RF}(n,k)$.

Assume z is a maximal element in an equivalence class. Then a_0 must be zero. Otherwise, $2^{a_0}z$ is equivalent to and larger than z, which contradicts with the maximality of z. Moreover, a_1 must be the smallest one among $a_1, a_2, \ldots, a_k$. Otherwise, we have $i > 1$ such that $a_1 > a_i$, which implies $2^{a_0+a_1+\cdots+a_{i-1}}z \bmod (2^n-1) = 2^{n-1} + 2^{n-1-a_i} + \cdots + 2^{a_{i-1}}$ is equivalent to and larger than z. Therefore z is a rotation-free element.

Assume the set L of elements z satisfying $a_0 = 0$ and $a_i > a_1$ for all $i > 1$. Then any element z in L is the unique maximal element of the equivalence class containing z. Moreover, the cardinality of L is the number of solutions $(a_1, \ldots, a_k)$ satisfying $a_1 + \cdots + a_k = n$ and $a_i > a_1$. Or the number of non-negative solutions $(a'_2, \ldots, a'_k)$ satisfying $a'_2 + \cdots + a'_k = n - ka_1 - (k-1)$. Given a positive integer a_1, the number of such $(k-1)$-tuples is the number of multisets of cardinality $(k-1)$ with elements taken from a set of cardinality $(n - ka_1 -$

$k+1$), that is $\binom{n-ka_1-1}{k-2}$. If we sum up $\binom{n-ki-1}{k-2}$ for all $1 \le i \le (n+1)/k-1$, we obtain the cardinality L. Then the difference between $\mathrm{RF}(n,k)$ and the cardinality L is obtained using Pascal's identity. $\square$

3 Binary Fields

In order to speed up exponentiations in a binary field $\mathbb{F}_{2^n}$, Hoffstein and Silverman [6] proposed a use of exponent $x = x_1x_2x_3 \in \mathbb{Z}/(2^n-1)$ where x_1, x_2 and x_3 are integers of low weights in $\mathbb{Z}/(2^n-1)$ for $n \approx 1000$. We will call x a (w_1, w_2, w_3) exponent if $\mathrm{wt}(x_1) = w_1$, $\mathrm{wt}(x_2) = w_2$, $\mathrm{wt}(x_3) = w_3$. They proposed two types of exponents for 2^{80} security: $(6,7,7)$ exponents and $(2,2,11)$ exponents.

3.1 $(6,7,7)$ *Exponents*

Let $x = x_1x_2x_3$ be a $(6,7,7)$ exponent in F_{2^n}. The attack complexity to recover x from g and g^x with a $(6,7,7)$ exponent x was claimed to be

$$\binom{n}{6}\binom{n}{7} + \binom{n}{7} \approx 2^{107.7}, \quad n = 1000$$

by checking the equation

$$y^{x_3^{-1}} = g^{x_1x_2}.$$

For this exponent, only 5+6+6=17 multiplications are required for one exponentiation.

Now we propose another attack. We may rewrite x as $x = 2^k\bar{x}_1\bar{x}_2\bar{x}_3$ for rotation-free elements $\bar{x}_1, \bar{x}_2, \bar{x}_3$ of weight $(6,7,7)$ and $0 \le k < n$. Then we check the following equation by storing the left-hand side after sorting and comparing them with the right-hand side:

$$y^{2^{-k}\bar{x}_3^{-1}} = g^{\bar{x}_1\bar{x}_2}.$$

Then the complexity is

$$\begin{aligned} & n \cdot \mathrm{RF}(n,7) + \mathrm{RF}(n,6) \cdot \mathrm{RF}(n,7) \\ =& n \sum_{i=0}^{\lfloor \frac{n}{7} \rfloor - 1} \binom{n-2-7i}{5} + \sum_{i=0}^{\lfloor \frac{n}{6} \rfloor - 1} \binom{n-2-6i}{4} \cdot \sum_{i=0}^{\lfloor \frac{n}{7} \rfloor - 1} \binom{n-2-7i}{5}, \end{aligned}$$

which is about $2^{87.8}$ for $n = 1000$. If we pick up only one element from one equivalence class, the complexity becomes lower, but the difference is at most $\mathcal{E}(1000, 6)\mathcal{E}(1000, 5) \leq 2^{77.7}$.

3.2 $(2, 2, 11)$ *Exponents*

Let $x = x_1x_2x_3$ be a $(2, 2, 11)$ exponent in F_{2^n}. The attack complexity of the discrete logarithms with this type of exponents for $n = 1000$ was claimed to be $2^{84.3}$ by Baby-step Giant-step, which checks the equation:

$$y^{x_1^{-1}x_2^{-1}} = g^{x_3}.$$

Then the search space for the left-hand side is $\binom{n}{2}^2 = 2^{37.9}$ and the search space for the right-hand side is $\binom{n}{11} = 2^{84.3}$ for $n = 1000$. In this case, only 1+1+10=12 multiplications are required for one exponentiation.

We may rewrite x as $x = 2^k\bar{x}_1\bar{x}_2\bar{x}_3$ for $0 \leq k < n$ and rotation-free elements $\bar{x}_1, \bar{x}_2, \bar{x}_3$ with weight $(2, 2, 11)$. Then we check the following equation by storing the left-hand side after sorting and comparing them with the right-hand side:

$$y^{2^{-k}(\bar{x}_1\bar{x}_2)^{-1}} = g^{\bar{x}_3}.$$

Then the complexity is

$$n \cdot \mathrm{RF}(n, 2)^2 + \mathrm{RF}(n, 11) \approx 2^{74.4}.$$

However, we have more efficient attacks. We may rewrite $\bar{x}_3$ as $2^{k'}\bar{x}_3 = x'_3 + \bar{x}''_3$ for some k' where x'_3 is an element of weight 3 and $\bar{x}''_3$ is a rotation-free element of weight 8 in $\mathbb{Z}/(2^n - 1)$. Then we can write $x = 2^k\bar{x}_1\bar{x}_2(x'_3 + \bar{x}''_3)$ and check the following equation:

$$y^{2^{-k}(\bar{x}_1\bar{x}_2)^{-1}}g^{-x'_3} = g^{\bar{x}''_3}.$$

Then the complexity is

$$n \cdot \mathrm{RF}(n, 2)^2 \cdot \binom{n-1}{3} + \mathrm{RF}(n, 8) \approx 2^{55.2} + 2^{54.5} \approx 2^{55.9}, \quad n = 1000.$$

4 Koblitz Curves: τ-adic Exponents

Koblitz curve is an elliptic curve over $\mathbb{F}_{2^n}$ defined by

$$E: \quad y^2 + xy = x^3 + ax^2 + 1, \quad a \in \mathbb{F}_2.$$

Let τ be a Frobenius map on E:

$$\tau : \quad E(\mathbb{F}_{2^n} \to E(\mathbb{F}_{2^n}); \quad (x, y) \mapsto (x^2, x^2).$$

Then Frobenius map is efficiently computable on $E(\mathbb{F}_{2^n})$ and plays a similar role to squaring in binary fields. The secret exponent N is taken to be

$$N = N_1 N_2 N_3 = \left(1 + \sum_{u=1}^{6} \pm\tau^{i_u}\right)\left(1 + \sum_{u=1}^{6} \pm\tau^{j_u}\right)\left(1 + \sum_{u=1}^{6} \pm\tau^{k_u}\right).$$

A scalar multiplication of a point on the curve by N requires only $6 + 6 + 6$ elliptic additions when using normal basis, where the squaring and so τ operation is almost free. On the other hand, the attack complexity of the discrete logarithms with this type of exponents was claimed to be

$$\binom{n}{6}2^6 + \binom{n}{6}2^6 \cdot \binom{n}{6}2^6 \approx 2^{80.9}, \quad n = 163$$

by checking the equation

$$N_3^{-1}Q = N_1 N_2 P$$

for given P and $Q = NP$.

We say $N = \sum_{i=0}^{n} a_i\tau^i$ ($a_i \in \{-1, 0, 1\}$) is a *rotation-free* Frobenius expansion if $\sum_{i=0}^{n} |a_i|2^i$ is a rotation-free element in $\mathbb{Z}/(2^n - 1)$. The number of nonzero a_i's is called the weight of N. Since $\tau^n = 1$, we may rewrite N as $N = \tau^k \bar{N}_1 \bar{N}_2 \bar{N}_3$ where $0 \le k < 163$ and $\bar{N}_1, \bar{N}_2, \bar{N}_3$ are rotation free Frobenius expansions of weight 7. In this case, however, we allow -1 coefficients as well as 0 and 1, and so $2^6 \cdot \mathrm{RF}(n, 7)$ is the number of rotation-free Frobenius expansions. Then the complexity to check

$$\tau^{-k}\bar{N}_3^{-1}Q = \bar{N}_1\bar{N}_2 P$$

is

$$n \cdot 2^6 \cdot \mathrm{RF}(n, 7) + \left(2^6 \cdot \mathrm{RF}(n, 7)\right)^2 \approx 2^{75.5}, \quad n = 163.$$

If we consider only the pairs $(\bar{N}_1, \bar{N}_2)$ with $\bar{N}_1 \le \bar{N}_2$, then it becomes $2^{74.5}$.

We can reduce the complexity more by considering τ-adic Non-Adjacent Forms (τ-adic NAF) [9]. We can write N_i as a τ-adic NAF with weight at most $t = 7$, whose number is given by $\binom{n-t+1}{t}2^t$ [1]. Then the complexity is at most

$$n\sum_{i=0}^{7} 2^i \cdot \mathrm{RF}(n - i + 1, i) + \left(\sum_{i=0}^{7} 2^i \cdot \mathrm{RF}(n - i + 1, i)\right)^2 \approx 2^{75.4}, \quad n = 163.$$

Also by considering the case $\bar{N}_1 \le \bar{N}_2$ only, we have the final complexity $2^{74.4}$.

They proposed parameters with more security margin: $N = N_1 N_2 N_3$ with weights $(8, 9, 9)$ and $N = N_1 N_2 N_3 N_4$ with weights $(4, 5, 7, 8)$. The total search

spaces were claimed to be $2^{163.9}$ and $2^{160.5}$, but our methods a bit reduce them to $2^{157.4}$ and $2^{157.5}$. However, the attack complexities using proposed rotation-free Frobenius maps are still more than 2^{80}.

5 Conclusion

The use of LHWPs as exponents in the DLP, proposed by Hoffstein and Silverman, prevents efficient applications of meet-in-the-middle attacks, and so accelerates exponentiations significantly in a group with fast endomorphisms such as binary fields or Koblitz curves. In this paper, we proposed a reduced representation of LHWPs and exploited them to reduce the complexity of the relevant hard problems by a factor of 2^5 through 2^{25}. Our analysis shows that some of suggested parameters are not secure anymore. However, we remark that some other parameters (with more security margin) are still secure and give significant advantages in efficiency.

Since Erdös and Newman [3], there have been several studies to find a set of exponents whose Baby-step Giant-step complexity against the DLP is larger than the square root of the cardinality of the exponents set. (Refer to [7] for the survey of this problem and recent results.) A LHWP is a good candidate for this problem when the order of the base group is of special form. We note that our attack is generic on such a special group in the sense that it does not use any information about the representation of elements, but not applicable to general groups in which the relation $\sim$ may not form an equivalent relation. It would be interesting to investigate generic complexity of the DLP with LHWPs. The first step toward this direction would be to estimate the number of distinct LHWP exponents.

Acknowledgement:

The authors thanks to the anonymous reviewer for pointing out some mistakes in the preliminary version and providing an intuitional high level description.

References

[1] J. Cheon and J. Yi, *Fast Batch Verifications of Multiple Signatures*, Proc. PKC 2007, LNCS 4450, Springer-Verlag, 2007, pp. 442–457.

[2] J. Coron, D. Lefranc, and G. Poupard, *A New Baby-Step Giant-Step Algorithm and Some Applications to Crypanalysis*, Proc. CHES 2005, LNCS 3659, Springer-Verlag, 2005, pp. 47–60.

[3] P. Erdös and D. Newman, *Bases for Sets of Integers*, J. Number Theory, Vol. 9, No. 4, 1977, pp. 420–425.

[4] M. Girault and D. Lefranc, *Public Key Authetication with one Single (on-line) Addition*, Proc. CHES 2004, LNCS 3156, Springer-Verlag, 2004, pp. 413–427.

[5] R. Heiman, *A Note on Discrete Logarithms with Special Structures*, Proc. Eurocrypt '92, LNCS 0658, Springer-Verlag, 1992, pp. 454–457.

[6] J. Hoffstein and J. H. Silverman, *Random Small Hamming Weight Products with Applications to Cryptography*, Discrete Appl. Math., Vol. 130, No. 1, 2003, pp.37–49.

[7] Il Mironov, A. Mityagin, and K. Nissim, *Hard Instances of the Constrained Discrete Logarithm Problem*, Proc. ANTS 2006, LNCS 4076, Springer-Verlag, 2006, pp.582–598.

[8] D. Shanks, *Class Number, a Theory of Factorization, and Genera*, Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1971, pp. 415–440.

[9] J. Solinas, *An Improved Algorithm for Arithmetic on a Family of Elliptic Curves*, Proc. Crypto '97, LNCS 1294, Springer-Verlag, 1997, pp.357–371.

[10] D. Stinson, *Some Baby Step Giant Step Algorithms for the Low Hamming Weight Discrete Logarithm Problem*, Math. Comp., Vol. 71, No. 237, Amer. Math. Soc., Providence, RI, 2002, pp. 379–391.

[11] Y. Yacobi, *Discrete-Log With Compressible Exponents*, Proc. of Crypto '90, LNCS 0537, Springer-Verlag, 1990, pp. 639–643.