Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

On the distribution of Low Hamming Weight products

Jianghua Li[1]* and Qiao Li[1]

*Correspondence:
249000809@qq.com
[1]College of Sciences, Xi'an University of Technology, Xi'an, China

Abstract

Jeffrey Hoffstein et al. (Discrete Appl. Math. 130:37–49, 2003) introduced the Low Hamming Weight products (LHWP) $X = x_1x_2x_3$ as random exponent of elements in a group or a ring to improve the operational efficiency, where each x_i has Hamming Weight Ham(x_i) in its binary representation. The random power or multiple be used in many cryptographic constructions, such as Diffie–Hellman key exchange, elliptic curve ElGamal variants, and NTRU public-key cryptosystem. But their randomness is just a conjecture, which lacks of the security proof. The main purpose of this paper is using the analytic method and the properties of the character sums to prove the distribution of the Hamming weight products, which is related to their pseudorandomness and unpredictability. It is important to research the application of LHWP in cryptographic constructions. Our theory shows that the LHWP are exponentially close to the uniform distribution, namely, an attack on algorithm (Hoffstein et al. in Discrete Appl. Math. 130:37–49, 2003) needs polynomial time to reach exponentially close probabilities of success.

Keywords: Character sums; Uniform distribution; Low Hamming weight

1 Background

Jeffrey Hoffstein and Joseph H. Silverman [1] proposed a new algorithm of fast exponentiation via Low Hamming Weight Products (LHWP), which is universally applied in cryptography. For example, Diffie–Hellman key exchange needs to output a random power of g^k in a finite field $\mathcal{F}$, if input an element g in $\mathcal{F}$. Divesh Aggarwal [2] introduced a new public-key cryptosystem whose security is based on the Mersenne Low Hamming Weight Ratio: there exist two Low Hamming Weight integers A and B such that $\frac{A}{B}$ is difficult to distinguish from a uniformly random string. NTRU algorithm [3–5] is suspected to be resistant to quantum attacks, their key generation requires a random polynomial product fg in the ring.

The products $X = x_1x_2x_3$ of integers in [1] acts as the exponent over $G = F_{2^n}$, where each x_i is a low Hamming weight number in its binary representation. It is a rapid method and has significant advantage of reducing the computation of powers in a group such as the Galois field $\mathcal{F}_{2^n}$. These kinds of questions also appear in [2, 6–9], where the representation of LHWP is applied to attack the relevant cryptosystems, and the Hamming weight model can be concentrated on the Differential Power Analysis.

Springer

The efficiency of the algorithm [1] is based on an assumption that a random multiplier is a product of factors, which is called the Low Hamming Product Assumption (see Definition 2). The security of the algorithm [2] is based on the assumption of Low Hamming Weight Ratio. They are all believed to be easily and rapidly computed, however, their randomness or pseudorandomness just is a conjecture, which is widely used, but lacks the solid foundation.

The main purpose of this paper is by using the analytic method and the bounds of the character sums to prove that the LHWP are exponentially close to the uniform distribution, which can imply their pseudorandomness. Furthermore, the theorem shows the unpredictability of LHWP. In addition, an attack on algorithm [1] needs polynomial time to reach exponentially close probabilities of success. The following are the definitions of low Hamming weight and some fundamental concepts required:

Denote by

$$\mathrm{Ham}(X) = \text{Hamming weight of } X$$

the number of 1s in the binary representation of X. In order to compute X faster, it is more advantageous to choose X such that $\mathrm{Ham}(X)$ is small. However, if $\mathrm{Ham}(X)$ is too small, then the algorithm can be exploited by an attacker who is trying to operate brutally.

Let $p > 2^n$ be a prime, and let $\mathcal{Z}_p$ be the residue integer ring modulo p. All elements $c \in \mathcal{Z}_p$ have the unique binary representation

$$c = \sum_{i=0}^{n-1} k_i \cdot 2^i, \quad k_i \in \{0, 1\}.$$

with a fixed specified binary Hamming weight $h = \sum k_i$. The Hamming weight number is equivalent to the Hamming distance from the all-zero string of the same length, which is widely used in several disciplines including information theory, coding theory, and cryptography. For example, the Hamming weight operation can be interpreted as a conversion from the unitary numeral system to binary numbers. Victor K Wei shows that a generalized Hamming weight is a natural generalization of the minimum distance. It is used to characterize the cryptographic performance of a linear code over the wire-tap channel (see [10]).

Definition 1 (Hamming weight inequalities; see [2], Lemma 2) Let p be a prime. For nonzero $A, B \in \mathcal{Z}_p$, denoting by $\mathrm{Ham}(A)$ the Hamming weight of the unique binary representation of A, we have

1. $\mathrm{Ham}(A + B) \leq \mathrm{Ham}(A) + \mathrm{Ham}(B)$.
2. $\mathrm{Ham}(A \cdot B) \leq \mathrm{Ham}(A) \cdot \mathrm{Ham}(B)$.
3. If a binary string $A \neq 0^n$, then $\mathrm{Ham}(-A) = n - \mathrm{Ham}(A)$.

Definition 2 (Low Hamming product assumption) Let h be an integer. Given n-bit strings A and B of low Hamming weight h are independent, it is difficult to distinguish between the product AB and a uniformly distributed random n-bit string.

The security proof in Sect. 3 also requires the regularity of the probability distributions. The variation distance of two distributions X and Y over a finite domain D is defined

as

$$\Delta(X,Y)=\frac{1}{2}\sum_{\alpha\in D}\big|\Pr[X=\alpha]-\Pr[Y=\alpha]\big|.$$

Recall that the definition of a statistical distance (sometimes it is called statistical closeness (see [11]) is: Let $n\in\mathcal{N}$ be an integer, for every positive polynomial $p(\cdot)$, and all sufficient large n, we say that two probability ensembles X_n and Y_n are statistically close if $\Delta(X_n,Y_n)$ is a negligible function of $\frac{1}{p(n)}$.

Similarly, δ-statistical closeness to uniform distribution (see [12, 13]) can be concluded based on the definition of statistical distance:

Definition 3 (δ-statistical closeness) For some constant $\delta>0$, a random variable X is δ-statistically close to a uniform random variable Y if

$$\Delta(X)=\frac{1}{2}\cdot\sum_{\alpha\in\mathcal{Z}}\left|\operatorname{pr}[X=\alpha]-\frac{1}{p-1}\right|\le\delta,$$

where we taking uniform probabilities of Y to equal $\frac{1}{p-1}$. More precisely, δ-statistically close means that the statistical distance $\Delta(X)$ is exponentially small.

2 Main results

Motivated by the universal use of Hamming weight in cryptography, studying the uniform distribution properties of LHWP is an important and interesting problem because it reveals some quality guarantee of their pseudorandomness. It is crucial for the security of the algorithms. We start with the following problem:

Let $p>2^n$ be a prime and denote by $\mathcal{Z}_p$ the residue ring modulo p. Given $h\in\mathcal{Z}_p$, find $x_1,x_2,x_3\in\mathcal{Z}_p$ of Hamming weight h, where x_i corresponds to an n-bit string of arbitrary Hamming weight, such that $X=x_1x_2x_3$ exists and is uniformly distributed in $\mathcal{Z}_p$. More specifically,

$$x_1x_2x_3 \bmod (p) \tag{1}$$

is uniformly distributed, where p is a prime.

Let $\mathcal{B}$ be the set of integers with Hamming weight less than h, that is, if $x_i\in\mathcal{B}$, and $\operatorname{Ham}(x_i)\le h$, where $i=1,2,3$, then the cardinality

$$|\mathcal{B}|=\sum_{0\le j\le h}\binom{n}{j}.$$

We consider the distribution of modular sums

$$X=x_1x_2x_3 \pmod p,\quad x_1,x_2,x_3\in\mathcal{B}.$$

To be more specific, given a fixed $c\in\mathcal{Z}_p$, denote by $N(\mathcal{B},c)$ the number of solutions of the congruence

$$x_1x_2x_3\equiv c \pmod p,\quad x_1,x_2,x_3\in\mathcal{B}. \tag{2}$$

For such integers $x_1, x_2, x_3 \in \mathcal{B}$, denote the probability by $P(\mathcal{B}, c)$, it is clearly

$$P(\mathcal{B}, c) = \frac{1}{|\mathcal{B}|^3} N(\mathcal{B}, c).$$

In Sect. 4, we shall use the classical bounds of character sums to give a uniform distribution proof for (2), which is related to the security of the algorithm [1]. That is, we shall prove the following

Theorem *Let $2^n < p < 2^{5n}$ be a prime. For some constants $\delta > 0, \epsilon > 0$, the LHWP $x = x_1x_2x_3$ is δ-statistically close to uniform distribution, namely*

$$\sum_{c \in \mathcal{Z}_p} \left| P(\mathcal{B}, c) - \frac{1}{p-1} \right| < p^{-\epsilon} < \delta.$$

3 Some lemmas

Let $\boldsymbol{\chi}_p$ be the set of multiplicative characters of the multiplicative group $\mathcal{Z}_p^*$. Denote by $\boldsymbol{\chi}_p^*$ the subset of nontrivial characters.

In this section, we shall give several necessary lemmas, which appear in the proof of our theorem. First, we have the following

Lemma 1 *For any $\epsilon > 0$, let χ be a nontrivial multiplicative character modulo $2^n < p < 2^{5n}$, while $\mathcal{B}$ is the set of integers with Hamming weight less than $h \le [\frac{n}{2}] + 1$ (here $[\frac{n}{2}]$ means the greatest integer $\le \frac{n}{2}$). Then there exists $\gamma > 0$ such that*

$$\max_{\chi \in \boldsymbol{\chi}_p^*} \left| \sum_{X \in \mathcal{B}} \chi(X) \right| \le |\mathcal{B}| p^{-\gamma},$$

where $p^{\frac{1}{5}+\epsilon} \le |\mathcal{B}| \le p$.

Proof By [14, Theorem 3], we know that if x is a number the Hamming Weight of which equals a fixed small j, then the following inequality holds:

$$\sum_x \chi\big(f(x)\big) \ll d^{\frac{1}{2}} \binom{n}{j}^{\frac{1}{2}} 2^{\frac{n}{4}} p^{\frac{1}{8}+o(1)},$$

where $d = \deg f$.

It is clear that $|\mathcal{B}| = \sum_{0 \le j \le h} \binom{n}{j} \le 2^{n-1}$, then for any $\epsilon > 0$, taking $f(x) = X$,

$$\begin{aligned} \sum_{x \in \mathcal{B}} \chi(X) &\ll \sum_{0 \le j \le h} \binom{n}{j}^{\frac{1}{2}} 2^{\frac{n}{4}} p^{\frac{1}{8}+o(1)} \\ &\ll |\mathcal{B}| \binom{n}{j}^{\frac{1}{2}} 2^{-\frac{3n}{4}} p^{\frac{1}{8}+o(1)} \\ &\ll |\mathcal{B}| 2^{-\frac{3n}{4}} p^{\frac{1}{8}+o(1)}. \end{aligned}$$

From $p < 2^{5n}$, we obtain $\sum_{x \in \mathcal{B}} \chi(X) \ll |\mathcal{B}| p^{-\frac{1}{40}+o(1)}$, thus taking $\gamma = \frac{1}{40} > 0$, the claim of Lemma 1 holds. □

Remark The most well known bound of $\max_{\chi\in\boldsymbol{\chi}_p^*}|\sum_{X\in\mathcal{B}}\chi(X)|$ is Polya–Vinogradov inequality (see [15, Theorem 2.2], [14, Lemma 1]):

$$\max_{\chi\in\boldsymbol{\chi}_p^*}\left|\sum_{X\in\mathcal{B}}\chi(X)\right|\le p^{\frac{1}{2}}\ln p,$$

which is nontrivial for $\mathcal{B}\ge p^{\frac{1}{2}+\epsilon}$. However, this bound related to $\mathcal{B}$ is too large to be used for our proof. In such cases we apply Lemma 1.

Lemma 2 *Let $X\in\mathcal{B}$ be an integer, its binary representation being an n-bit string of Hamming weight less than h, then $|\mathcal{B}|=\sum_{0\le j\le h}\binom{n}{j}$, therefore,*

$$|\mathcal{B}|\le 2^{nH(h/n)}<p^{H(h/n)},$$

where the entropy function is

$$H(\gamma)=-\gamma\log\gamma-(1-\gamma)\log(1-\gamma).$$

Proof See [16, Sect. 10.11]. □

4 Proof of the Theorem

Recall that (see [17, Chap. 5]) if G is a finite Abelian group (multiplicative) of order $|G|$, a character χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1, that is, a mapping from G into U with $\chi(g_1g_2)=\chi(g_1)\chi(g_2)$ for all $g_1,g_2\in G$. Then supposing g and h are elements of a finite Abelian group G, the following is the well-known property of character sums:

$$\frac{1}{|G|}\sum_{\chi\in\boldsymbol{\chi}_p}\chi(g)\overline{\chi(h)}=\begin{cases}0, & \text{for } g\ne h,\\ 1, & \text{for } g=h.\end{cases}$$

In this section, we shall complete the proof of our theorem. Note that

$$\begin{aligned}\sum_{c\in\mathcal{Z}_p}\left|P(\mathcal{B},c)-\frac{1}{p-1}\right|^2&=\sum_{c\in\mathcal{Z}_p}\left|\frac{N(\mathcal{B},c)}{|\mathcal{B}|^3}-\frac{1}{p-1}\right|^2\\&=\frac{1}{|\mathcal{B}|^6}\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|^2.\end{aligned}\tag{3}$$

Clearly, $N(\mathcal{B},c)$ is the number of solutions of the congruence (2), thus we have

$$N(\mathcal{B},c)=\frac{1}{p-1}\sum_{\chi\in\boldsymbol{\chi}_p}\sum_{x_1x_2x_3\in\mathcal{B}}\chi(x_1x_2x_3)\overline{\chi(c)}.$$

If $\chi=\chi_0$ is the trivial character, then the corresponding term of $N(\mathcal{B},c)$ is $|\mathcal{B}|^3/(p-1)$,

We know that $\chi(c^{-1}) = \overline{\chi(c)}$, and $z\overline{z} = |z|^2$, where $\overline{z}$ denotes the conjugate of a complex number z. Then c^{-1} runs through $\mathcal{Z}_p$ together with c, therefore

$$\begin{aligned}
&\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|^2\\
&\quad=\sum_{c\in\mathcal{Z}_p}\left(\frac{1}{p-1}\sum_{\chi\in\boldsymbol{\chi}_p^*}\overline{\chi(c)}\left|\sum_{x_1x_2x_3\in\mathcal{B}}\chi(x_1x_2x_3)\right|\right)^2\\
&\quad=\frac{1}{(p-1)^2}\sum_{c\in\mathcal{Z}_p}\sum_{\chi_1\chi_2\in\boldsymbol{\chi}_p^*}\chi_1(c)\chi_2(c)\left|\left(\sum_{X\in\mathcal{B}}\chi_1(X)\right)^3\right|\left|\left(\sum_{X\in\mathcal{B}}\chi_2(X)\right)^3\right|\\
&\quad=\frac{1}{(p-1)^2}\sum_{\chi_1\chi_2\in\boldsymbol{\chi}_p^*}\left|\left(\sum_{X\in\mathcal{B}}\chi_1(X)\right)^3\right|\left|\left(\sum_{X\in\mathcal{B}}\chi_2(X)\right)^3\right|\sum_{c\in\mathcal{Z}_p}\chi_1(c)\chi_2(c).
\end{aligned}$$

Recalling the identity of characters (see [18, Theorem 5.4]), for any $c\in\mathcal{Z}_p$

$$\sum_{\chi\in\boldsymbol{\chi}_p}\chi(c)=\begin{cases}p-1, & \text{if } \chi=\chi_0,\\ 0, & \text{otherwise,}\end{cases}$$

where χ_0 is the trivial character, the inner sum equals 0 unless

$$\chi_2(c)=\chi_1(c)^{-1}=\chi_1\left(c^{-1}\right)=\overline{\chi_1(c)},\quad c\in\mathcal{Z}_p,$$

Then,

$$\begin{aligned}
&\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|^2\\
&\quad=\frac{1}{(p-1)}\sum_{\chi_1\chi_2\in\boldsymbol{\chi}_p^*}\left|\left(\sum_{X\in\mathcal{B}}\chi_1(X)\right)^3\right|\left|\left(\sum_{X\in\mathcal{B}}\chi_2(X)\right)^3\right|\\
&\quad=\frac{1}{(p-1)}\sum_{\chi\in\boldsymbol{\chi}_p^*}\left|\sum_{X\in\mathcal{B}}\chi(X)\right|^6\\
&\quad<\frac{1}{(p-1)}\max_{\chi\in\boldsymbol{\chi}_p^*}\left|\sum_{X\in\mathcal{B}}\chi(X)\right|^4\sum_{\chi\in\boldsymbol{\chi}_p}\left|\sum_{X\in\mathcal{B}}\chi\left(X^{-1}\right)\right|^2\\
&\quad=\frac{1}{(p-1)}\max_{\chi\in\boldsymbol{\chi}_p^*}\left|\sum_{X\in\mathcal{B}}\chi(X)\right|^4\sum_{X\in\mathcal{B}}\sum_{\chi\in\boldsymbol{\chi}_p}\chi(X_1)\chi(X_2).
\end{aligned}$$

Note that

$$\frac{1}{(p-1)}\sum_{\chi\in\boldsymbol{\chi}_p}\left|\sum_{X\in\mathcal{B}}\chi(X_1)\chi(X_2)\right|=|\mathcal{B}|.$$

Therefore, from Lemma 1, we have

$$\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|^2=|\mathcal{B}|^5p^{-4\gamma}.$$

Denote

$$w(\mathcal{B},c)=\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|.$$

Using the Cauchy–Schwarz inequality, we obtain

$$w^2(\mathcal{B},c)\le p\sum_{c\in\mathcal{Z}_p}\left|N(\mathcal{B},c)-\frac{|\mathcal{B}|^3}{p-1}\right|^2=|\mathcal{B}|^5p^{1-4\gamma}. \tag{4}$$

Combining (3) and (4), we can easily get

$$\begin{aligned}\sum_{c\in\mathcal{Z}_p}\left|P(\mathcal{B},c)-\frac{1}{p-1}\right|&=\frac{1}{|\mathcal{B}|^3}w(\mathcal{B},c)\\&<|\mathcal{B}|^{-\frac{1}{2}}p^{\frac{1}{2}-2\gamma}.\end{aligned} \tag{5}$$

Recalling that $p>2^n$, for $0\le\gamma\le1$, $A>0$, from Lemmas 1 and 2, as well as (5), for some $\delta>0$, $\epsilon>0$, the following inequality holds:

$$\sum_{c\in\mathcal{Z}_p}\left|P(\mathcal{B},c)-\frac{1}{p-1}\right|<|\mathcal{B}|^{-\frac{1}{2}}p^{\frac{1}{2}-2\gamma}<p^{\frac{1}{4}-2\gamma}<p^{-\epsilon}<\delta.$$

That is, the statistical distance is exponentially small. We also can conclude that the LHWP are exponentially close to the uniform distribution, namely, and attack on algorithm [1] needs polynomial time to reach exponentially close probabilities of success. This proves the theorem.

5 Conclusion

Character sums are important and useful tools in the analytic number theory. In this paper we use character sums to prove the pseudorandomness of LHWP, which play a central role in cryptology, algorithms, and many other areas. It is important and meaningful to establish the uniform distribution of such products for giving the security assurance of cryptographic constructions. In addition, we need to emphasize that for our bounds to be nontrivial, the cardinality of the LHWP $\mathcal{B}$ should be sufficiently large, however, it also applies to sparse integers.

6 Notations

Throughout the paper the implied constants in symbols big "O" and "$\ll$" depend on the small real parameter "$\gamma>0$". Notations $A\ll B$ and $A=O(B)$ are equivalent to $|A|\le B$. The symbol small "o(1)" denotes the function tending to 0.

Acknowledgements
The authors would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper.

Funding
This work is supported by the N.S.F. (2017YFF0104401,413618022) of P.R. China and the N.S.F. of Shaanxi Province (2019JQ33).

Availability of data and materials
Data sharing not applicable to this article as no data sets were generated or analyzed during the current study.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
The authors contributed equally. All authors read and approved the final manuscript.

Publisher's Note

Received: 7 October 2019 Accepted: 19 February 2020 Published online: 28 February 2020

References

1. Hoffstein, J., Silverman, J.H.: Brca1 random small Hamming weight products with applications to cryptography. Discrete Appl. Math. **130**, 37–49 (2003)
2. Divesh, A., Antoine, J., Anupam, P., Miklos, S.: A new public-key cryptosystem via mersenne numbers. In: Advances in Cryptology CRYPTO 2018, pp. 459–482 (2018)
3. William, D.B., Shparlinski, I.E.: Brca1 avariant of ntru with non-invertible polynomials. In: Indocrypt'02 2551, pp. 62–70 (2002)
4. Yang, Y., Guangwu, X., Xiaoyun, W.: Brca1 provably secure ntru instances over prime cyclotomic rings. Public Key Cryptogr. **1**, 409–434 (2017)
5. Hoffstein, J., Pipher, J., Silverman, J.H.: Ntru: a new high speed public key cryptosystem. Presented at the rump session of crypto. In: Proceedings of the Algorithm Number Theory. ANTS III, vol. 1423, pp. 267–288 (1998)
6. Jung Hee, C., HongTae, K.: Brca1 analysis of low Hamming weight products. Discrete Appl. Math. **156**, 2264–2269 (2008)
7. Christian, E.: Brca1 almost all primes have a multiple of small Hamming weight. Bull. Aust. Math. Soc. **94**, 224–235 (2016)
8. ChinChen, C., YingTse, K., ChuHsing, L. (eds.): Fast Algorithms for Common-Multiplicand Multiplication and Exponentiation by Performing Complements IEEE Computer Society, Xi'an (2003)
9. Sarkar, S., Maitra, S., Chakraborty, K.: Differential power analysis in Hamming weight model: how to choose among (extended) affine equivalent s-boxes. In: Meier, W., Mukhopadhyay, D. (eds.) Progress in Cryptology. Indocrypt 2014, pp. 360–373 (2014)
10. Victor, K.W.: Generalized Hamming weights for linear codes. IEEE Trans. Inf. Theory **37**, 1412–1418 (1991)
11. Goldreich, O.: Foundations of Cryptography, Basic Tools. Cambridge University Press, Cambridge (2004)
12. Gilles, B., Francois, D., Pierre Alain, F., Benjamin, G., Mehdi, T., Jean Christophe, Z.: Making rsa-pss provably secure against non-random faults. Cryptogr. Hardware Embed. Syst. **8731**, 206–222 (2014)
13. Nguyen, P.Q., Shparlinski, I.E., Stern, J.: Distribution of modular sums and the security of the server aided exponentiation. Cryptogr. Comput. No. Theory **20**, 331–342 (2001)
14. Banks, W., Conflittia, A., Shparlinski, I.E.: Character sums over integers with restricted g-ary digits. Ill. J. Math. **46**, 819–836 (2002)
15. Narkiewicz, W.: Classical Problems in Number Theory. Polish Sci. Publ., Warszawa (1986)
16. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correctiong Codes. North-Holland Publishing Company, New York (1977)
17. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
18. Vinogradov, I.M.: Elements of Number Theory. Dover Publ., New York (1954)