A remark on the Independence Heuristic in the Dual Attack

Andreas Wiemers, Stephan Ehlen, Kaveh Bashiri
Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

December 29, 2023

1 Introduction

In [1] the authors especially report on experiments they made comparing the distributions of scores for random targets and BDD targets. They discovered that the distribution of scores for BDD targets deviate from the predictions made under the independence heuristic. Here, we want to derive approximations for the distributions which take into account the dependency that occur in the scores. These approximations allow to find heuristic estimates for the success probability of distinguishing between the two distributions.

2 The Dual Distinguishing in [1]

We adopt the notation of [1] and repeat the approach described in [1, Section 2.3]. Given a BDD sample $t = v + e_0$ with $v \in \Lambda$ for any dual vector $w \in \Lambda^\vee$ one has

$$\langle t, w \rangle \equiv \langle e_0, w \rangle \bmod 1.$$

One naturally considers the total score over many dual vectors $W \subset \Lambda^\vee$ given by

$$f_W(t) = \sum_{w \in W} f_w(t) \text{ with } f_w(t) = \cos(2\pi \langle t, w \rangle).$$

In [1, Lemma 4] approximations of the expectation values and variances of a $\underline{\text{single}}$ $f_w(t)$ are given for the two cases "random targets vs. BDD targets". In general, we have for the variance of the score

$$V(f_W(t)) = \sum_{w \in W} V(f_w(t)) + \sum_{w, \tilde{w} \in W, w \neq \tilde{w}} \mathrm{Cov}(f_w(t), f_{\tilde{w}}(t))$$

If the [1, Heuristic 2 (Independence Heuristic)] is valid, the second sum over the single covariances is equal to 0. However, in the following we want to derive approximations of this second sum. In the end, this might explain that in the experiments in [1, Table 1] the measured variance is much larger as predicted.

3 Computing the covariances for random targets

We use the definition as in [2, Definition 1 (Random target distribution)]. Let Λ be a full-rank n-dimensional lattice, B is a basis of Λ. The random target distribution for Λ corresponds to the distribution obtained by sampling target vectors t uniformly at random from the fundamental parallelepiped generated by the basis B. (We write vectors as columns. The components of α with $t = B\alpha$, are uniform on $[-\frac{1}{2}, \frac{1}{2}]$.) We fix two dual vectors $w, \tilde{w} \in W, w \neq \tilde{w}$ and write explicitely

$$w = (B^{-1})^T \mu, \tilde{w} = (B^{-1})^T \tilde{\mu}$$

where the components of μ and $\tilde{\mu}$ are integers. We consider the 2-dimensional distribution of

$$\begin{pmatrix} \langle t, w \rangle \\ \langle t, \tilde{w} \rangle \end{pmatrix} = \begin{pmatrix} \langle \alpha, \mu \rangle \\ \langle \alpha, \tilde{\mu} \rangle \end{pmatrix}$$

and its reduction

$$\begin{pmatrix} \langle \alpha, \mu \rangle \bmod 1 \\ \langle \alpha, \tilde{\mu} \rangle \bmod 1 \end{pmatrix}$$

as a random variable in α. We want to compute the probabilities for $-1/2 \leq s, \tilde{s} \leq 1/2$

$$\begin{aligned} & P(\langle \alpha, \mu \rangle \bmod 1 \leq s, \langle \alpha, \tilde{\mu} \rangle \bmod 1 \leq \tilde{s}) \\ = \; & \mathrm{Vol}(\langle \alpha, \mu \rangle \bmod 1 \leq s, \langle \alpha, \tilde{\mu} \rangle \bmod 1 \leq \tilde{s}) \end{aligned}$$

We can compute this volume as as sub-volume of the n-dimensional cube by counting over the points $(\frac{k_1}{p}, \dots, \frac{k_n}{p})$, k_j integers with $-p/2 \leq k_j \leq p/2$, for very large prime p and going to the limit. As approximation we get the sum

$$\begin{aligned} & \sum_{\substack{r, \tilde{r}, \text{ with} \\ r/p \leq s, \tilde{r}/p \leq \tilde{s}}} \left[\sum_{\substack{k_j, \text{ with} \\ \sum_j \mu_j k_j/p \bmod 1 = r/p, \\ \sum_j \tilde{\mu}_j k_j/p \bmod 1 = \tilde{r}/p}} \frac{1}{p^n} \right] \\ = & \sum_{\substack{r, \tilde{r}, \text{ with} \\ r \leq sp, \tilde{r} \leq \tilde{s}p}} \left[\sum_{\substack{k_j, \text{ with} \\ \sum_j \mu_j k_j \bmod p = r, \\ \sum_j \tilde{\mu}_j k_j \bmod p = \tilde{r}}} \frac{1}{p^n} \right] \end{aligned}$$

where $r, \tilde{r}$ are integers in $[-p/2, p/2]$. We assume that μ and $\tilde{\mu}$ are linearly independent (over the rational numbers or the real numbers). Then the second sum has exactly p^{n-2} solutions. In the end, we derive as approximation

$$\sum_{\substack{r, \tilde{r}, \text{ with} \\ r \leq sp, \tilde{r} \leq \tilde{s}p}} \frac{1}{p^2} \approx (s + \frac{1}{2})(\tilde{s} + \frac{1}{2})$$

Therefore, the random variables $\langle \alpha, \mu \rangle$ mod 1 and $\langle \alpha, \tilde{\mu} \rangle$ mod 1 are independent and the covariances vanish.

4 Approximations for computing the covariances for BDD targets

We now assume that t is chosen as a BDD sample by sampling e_0 from an n-dimensional, continuous gaussion distribution with covariance matrix $\sigma_0^2 \cdot 1_n$. We fix two dual vectors $w, \tilde{w} \in W, w \neq \tilde{w}$ and consider the 2-dimensional distribution of

$$\begin{pmatrix} \langle e_0, w \rangle \\ \langle e_0, \tilde{w} \rangle \end{pmatrix}$$

as a random variable in e_0. This random variable is again gaussianly distributed with covariance matrix

$$\Sigma = \sigma_0^2 \begin{pmatrix} ||w||^2 & \langle w, \tilde{w} \rangle \\ \langle w, \tilde{w} \rangle & ||\tilde{w}||^2 \end{pmatrix}$$

Let us assume that w and $\tilde{w}$ are linear independent and hence define a 2-dimensional positive definite subspace of $\mathbb{R}^n$ and Σ is invertible. We set

$$\tilde{P}(z) = \frac{1}{2\pi\sqrt{\det(\Sigma)}} e^{-\frac{1}{2} z^T \Sigma^{-1} z}$$

The distribution of the reduced random variable

$$c = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \langle e_0, w \rangle \bmod 1 \\ \langle e_0, \tilde{w} \rangle \bmod 1 \end{pmatrix}$$

is equal to

$$P(c) = \sum_{\mu \in \mathbb{Z}^2} \tilde{P}(c + \mu).$$

We use the well known Poisson summation formula and get

$$P(c) = \sum_{\mu \in \mathbb{Z}^2} \tilde{P}(c + \mu) \quad = \quad \sum_{v \in \mathbb{Z}^2} e^{-2\pi i \langle v, c \rangle} e^{-2\pi^2 v^t \Sigma v}.$$

We now start the computation by

$$\begin{aligned} & E(f_w(t) \cdot f_{\tilde{w}}(t)) \\ = & \int_{c_1, c_2} \cos(2\pi c_1) \cdot \cos(2\pi i c_2) P(c_1, c_2) \mathrm{d}c_1 \mathrm{d}c_2 \\ = & \sum_{v \in \mathbb{Z}^2} e^{-2\pi^2 v^t \Sigma v} \int_{c_1} \cos(2\pi c_1) e^{-2\pi i v_1 c_1} \mathrm{d}c_1 \cdot \int_{c_2} \cos(2\pi c_2) e^{-2\pi i v_2 c_2} \mathrm{d}c_2 \end{aligned}$$

It is easily seen that each univariate integral (in c_1 or c_2, respectively) vanishes for all v_1, except for $v_1 = \pm 1$ and for $v_2 = \pm 1$, respectively. Namely, we have

$$2\int_0^1 \cos(2\pi nt)e^{-2\pi imt}dt = \int_0^1 e^{2\pi i(n-m)t}dt + \int_0^1 e^{2\pi i(-n-m)t}dt.$$

The first integral on the right-hand side vanishes except for $n = m$ and the second integral vanishes except for $n = -m$. Both integrals are equal to 1 if they do not vanish and the claim follows.

Therefore, we get

$$\begin{aligned} & E(f_w(t)\cdot f_{\tilde{w}}(t)) \\ = & \frac{1}{4}\sum_{v_1=\pm1, v_2\pm1} e^{-2\pi^2 v^t\Sigma v} \\ = & \frac{1}{2}\Delta_a + \frac{1}{2}\Delta_b \end{aligned}$$

where we set

$$\begin{aligned} \Delta_a &= e^{-2\pi^2||w+\tilde{w}||^2\sigma_0^2} \\ \Delta_b &= e^{-2\pi^2||w-\tilde{w}||^2\sigma_0^2} \\ \Delta_c &= e^{-2\pi^2||w||^2\sigma_0^2} \\ \Delta_d &= e^{-2\pi^2||\tilde{w}||^2\sigma_0^2} \end{aligned}$$

[1, Lemma 4] states the equality for the expectation value

$$E(f_w(t)) \quad = \quad e^{-2\pi^2\sigma_0^2||w||^2}$$

In the end, we derive for the covariance

$$\mathrm{Cov}(f_w(t), f_{\tilde{w}}(t)) \quad = \quad \frac{1}{2}\Delta_a + \frac{1}{2}\Delta_b - \Delta_c\cdot\Delta_d \qquad (B)$$

We look at the sum over all single covariances

$$\sum_{w,\tilde{w}\in W, w\neq\tilde{w}} \mathrm{Cov}(f_w(t), f_{\tilde{w}}(t)).$$

Instead of computing this sum via (B) directly we now want to find plausible approximations that give simple formulas. We set $m_0 = \#W$. Note that

$$\frac{1}{m_0^2}\sum_{w,\tilde{w}\in W, w\neq\tilde{w}} \mathrm{Cov}(f_w(t), f_{\tilde{w}}(t)). \qquad (C)$$

can be interpreted as a computation of a mean, (and using $m_0^2 - m_0 \approx m_0^2$). Therefore, we can expect that the expression (C) is near to the expectation value if we treat $w, \tilde{w} \in W, w \neq \tilde{w}$ as random variables. In the simplest approximation these random variables are gaussian distributed with covariance matrix $\tau_0^2 1_n$. The expectation value is of the form

$$E(e^{\gamma Y})$$

where Y is (standard)-χ-square distributed. For $\gamma < 0.5$ this is identical to

$$E(e^{\gamma Y}) = (1 - 2\gamma)^{-k/2},$$

where k denotes the degrees of freedom of Y. Δ_a (resp. Δ_b) depends on

$$||w + \tilde{w}||^2, \text{ resp. } ||w - \tilde{w}||^2$$

which has n degrees of freedom, whereas $\Delta_c \cdot \Delta_d$ depends on

$$||w||^2 + ||\tilde{w}||^2$$

which has $2n$ degrees of freedom. In the end, we derive as an approximation of (C)

$$\begin{array}{l} (1 - 4\gamma_0)^{-n/2} - (1 - 2\gamma_0)^{-n} \\ \text{where } \gamma_0 = -2\pi^2 \sigma_0^2 \tau_0^2 \end{array}$$

For the total variance we therefore expect as approximation

$$\begin{aligned} V(f_W(t)) &= \sum_{w \in W} V(f_w(t)) + \sum_{w, \tilde{w} \in W, w \neq \tilde{w}} \mathrm{Cov}(f_w(t), f_{\tilde{w}}(t)) \\ &\approx \frac{m_0}{2} + m_0^2[(1 - 4\gamma_0)^{-n/2} - (1 - 2\gamma_0)^{-n}] \qquad (D) \end{aligned}$$

[1, Lemma 4] states as approximation for the expectation value

$$E(f_W(t)) = \sum_{w \in W} e^{-2\pi^2 \sigma_0^2 ||w||^2}$$

Again, we further expect

$$E(f_W(t)) \approx m_0(1 - 2\gamma_0)^{-n/2}$$

5 Modelling the distribution of w in W

For any fixed e_0 we write

$$\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0,w\rangle)=F(e_0)+\delta_{W,e_0}$$

where $F(e_0)$ is the expectation value when w is treated as random variable. δ_{W,e_0} does depend on e_0 as well as on the whole set W. If we assume the elements w in the score as chosen independently, δ_{W,e_0} can be treated as a realization of an gaussian random variable, (central limit theorem), with expectation value 0 and a certain variance. Here, we want to assume that this variance is independent of e_0 and given by $\frac{1}{2m_0}$. In Chapter 4 we treat w as gaussian distributed with covariance matrix $\tau_0^2 1_n$ for computing the covariance terms. In a more accurate approach, we should assume that w is a realization of a random variable with values on the lattice $\Lambda^\vee$ where the distribution is induced by the gaussian distribution with covariance matrix $\tau_0^2 1_n$, i.e. the probability of w is

$$\frac{e^{-||w||^2/(2\tau_0^2)}}{\sum_{w\in\Lambda^\vee}e^{-||w||^2/(2\tau_0^2)}}$$

Thus, we compute

$$F(e_0)=\frac{\sum_{w\in\Lambda^\vee}\cos(2\pi\langle e_0,w\rangle)e^{-||w||^2/(2\tau_0^2)}}{\sum_{w\in\Lambda^\vee}e^{-||w||^2/(2\tau_0^2)}}\qquad (E)$$

The denominator and the numerator in the quotient (E) can be expressed as a sum over the lattice Λ by using the Poisson summation formula. Note that the Fourier transform of $e^{2\pi i\langle e_0,w\rangle}h(w)$ is just the Fourier transform of $h(w)$ with the shift $-e_0$. Therefore, we further derive

$$\begin{aligned}F(e_0) &= \frac{\sum_{z\in\Lambda}e^{-2\pi^2\tau_0^2||z-e_0||^2}}{\sum_{z\in\Lambda}e^{-2\pi^2\tau_0^2||z||^2}}\\ &= \frac{e^{-2\pi^2\tau_0^2||e_0||^2}+\sum_{0\neq z\in\Lambda}e^{-2\pi^2\tau_0^2||z-e_0||^2}}{1+\sum_{0\neq z\in\Lambda}e^{-2\pi^2\tau_0^2||z||^2}}\qquad (F)\end{aligned}$$

In typical cases, we can expect that the value of $\sum_{0\neq z\in\Lambda}e^{-2\pi^2\tau_0^2||z||^2}$ is very small: We want to assume that the Gauss heuristic is valid for both lattices $\Lambda,\Lambda^\vee$. Here we use the simple approximations $\frac{\sqrt{n}}{\sqrt{2\pi e}}\det(\Lambda)^{1/n}$, resp. $\frac{\sqrt{n}}{\sqrt{2\pi e}}\det(\Lambda)^{-1/n}$, for the shortest vectors in Λ, resp. $\Lambda^\vee$. Furthermore, we define λ_0 by the equation

$$\tau_0=\lambda_0\frac{1}{\sqrt{2\pi e}}\det(\Lambda)^{-1/n},\qquad (G)$$

so that $\tau_0\sqrt{n}$ is a λ_0-multiple of the shortest vector in $\Lambda^\vee$. Then, the smallest non-trivial vector of the stretched lattice $\sqrt{2\pi\tau_0^2}\Lambda$ is of length $\frac{\lambda_0}{\sqrt{2\pi e}}\sqrt{n}$. If $\lambda_0\geq e$, we can directly apply [3, Lemma (1.5, (i))] setting $c=\frac{\lambda_0}{\sqrt{2\pi e}}\geq\frac{1}{\sqrt{2\pi}}$ in this lemma in order to derive a bound on the sum $\sum_{0\neq z\in\Lambda}e^{-2\pi^2\tau_0^2||z||^2}$.

6 The distribution of $F(e_0)$ in the BDD case

We want to assume that the denominator of (F) can be set to 1. We assume that e_0 is chosen with length much smaller than the shortest vector in Λ. Therefore, we find a certain value μ with

$$||z - e_0||^2 \geq \mu^2 ||z||^2 \text{ for all } 0 \neq z \in \Lambda$$

Again, we can use [3, Lemma (1.5, (i))] for deriving an explicit bound for the sum $\sum_{0 \neq z \in \Lambda} e^{-2\pi^2 \tau_0^2 ||z-e_0||^2} \leq \sum_{0 \neq z \in \Lambda} e^{-2\pi^2 \tau_0^2 \mu^2 ||z||^2}$. In the end, we want to assume that the function

$$Z(e_0) = e^{-2\pi^2 \tau_0^2 ||e_0||^2}$$

is a valid approximation of $F(e_0)$. The distribution function of Z can be computed as

$$t \mapsto c_0(-\ln(t))^{n/2-1} t^{-1/(2\gamma_0)-1}$$

with a certain real number c_0 and $t \in [0, 1]$. If $|\gamma_0|$ is small, then the distribution function looks roughly like a gaussian function. If $|\gamma_0| > \frac{1}{2}$, the exponent of t is negative and the distribution function looks completely different.

Furthermore, we can compute the expectation value and the variance of $Z(e_0)$. We derive the values which we computed before in chapter 4, i.e. $(1 - 2\gamma_0)^{-n/2}$ for the expectation value and

$$(1 - 4\gamma_0)^{-n/2} - (1 - 2\gamma_0)^{-n}$$

for the variance.

7 The distribution of $F(e_0)$ in the case of uniform targets

We now consider the distribution of $F(e_0)$ in the case of targets uniformly chosen in $\mathbb{R}^n/\Lambda$. Again, we set the denominator of (F) to 1. Furthermore, the numerator in (F) should be well approximated by just the restricted sum over the $z \in \Lambda$, which are closest to e_0. However, it seems to be difficult to find a simple approximation of the distribution function of the score function in this case.

Since $\langle e_0, w \rangle \bmod 1$ is equally distributed on $[-\frac{1}{2}, \frac{1}{2}]$ for $w \neq 0$, see chapter 3, we can compute the expectation value of $F(e_0)$ as

$$\frac{1}{\sum_{w \in \Lambda^\vee} e^{-||w||^2/(2\tau_0^2)}}$$

We approximate the sum by an integral (alternatively using the Poisson summation formula and neglecting terms in $z \neq 0$) which gives

$$\frac{1}{\sum_{w \in \Lambda^\vee} e^{-||w||^2/(2\tau_0^2)}} \approx \frac{1}{\sqrt{2\pi\tau_0^2}^n \det(\Lambda)}$$

Note that

$$\sum_{w,w'\in\Lambda^\vee} \cos(2\pi\langle e_0, w\rangle)\cos(2\pi\langle e_0, w'\rangle) e^{-||w||^2/(2\tau_0^2)} e^{-||w'||^2/(2\tau_0^2)}$$
$$= \frac{1}{2}\sum_{w,w'\in\Lambda^\vee} [\cos(2\pi\langle e_0, w+w'\rangle) + \cos(2\pi\langle e_0, w-w'\rangle)] e^{-||w||^2/(2\tau_0^2)} e^{-||w'||^2/(2\tau_0^2)}$$

This property allows us to compute the second moment of $F(e_0)$ as

$$\frac{\sum_{w\in\Lambda^\vee} e^{-2||w||^2/(2\tau_0^2)}}{[\sum_{w\in\Lambda^\vee} e^{-||w||^2/(2\tau_0^2)}]^2}$$

We approximate the sums by integrals (alternatively using the Poisson summation formula and neglecting terms in $z \neq 0$) which gives

$$\frac{\sum_{w\in\Lambda^\vee} e^{-2||w||^2/(2\tau_0^2)}}{[\sum_{w\in\Lambda^\vee} e^{-||w||^2/(2\tau_0^2)}]^2} \approx \frac{1}{\sqrt{4\pi\tau_0^2}^n \det(\Lambda)}$$

In typical cases, we can expect that the distribution of $F(e_0)$ is extremely near to 0 since both the expectation value and the standard deviation are negligible: Again as in chapter 5, we want to assume that the Gauss heuristic is valid for both lattices $\Lambda, \Lambda^\vee$ and that $\tau_0\sqrt{n}$ is not too small a multiple λ_0 of the shortest vector in $\Lambda^\vee$ as in (G). Then, the expectation value of $F(e_0)$ is of size

$$\frac{1}{\sqrt{2\pi\tau_0^2}^n \det(\Lambda)} = [\frac{\lambda_0}{\sqrt{e}}]^{-n}$$

and the second moment is of size

$$\frac{1}{\sqrt{4\pi\tau_0^2}^n \det(\Lambda)} = [\frac{\lambda_0\sqrt{2}}{\sqrt{e}}]^{-n}$$

8 Conditions for getting notable success probabilities

Based on the assumption that a conditional version of the central limit theorem is valid, [4, Theorem 3.1], we suggest the following heuristic:

Heuristic: *The score function $\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0, w\rangle)$ can be treated as a realization of the sum $F(e_0) + X$ of two random variables $F(e_0)$ and X. X is a gaussian random variable with expectation value 0 and variance $\frac{1}{2m_0}$. $F(e_0)$ is the expectation value when w is treated as random variable and therefore does not depend on m_0.*

We want to distinguish the cases "random targets vs. BDD targets" with good probability by checking if the score is higher or lower than a certain value α. If we have good approximations for the distribution of $F(e_0)$, we can compute numerically a condition on m_0 based on the heuristic above. In the following, we want to derive a simple formular that gives us a plausible condition on m_0. To this end, we assume that the approximations in chapters 5 and 6 are valid. If e_0 is chosen uniformly in $\mathbb{R}^n/\Lambda$, we assume that $F(e_0)$ is extremely small compared to X. Therefore, we approximate

$$\begin{aligned} & P(\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0,w\rangle) \le \alpha|\text{case "random targets"}) \\ = \; & P(F(e_0)+X \le \alpha|\text{case "random targets"}) \approx P(X \le \alpha) \end{aligned}$$

We therefore choose for simplicity

$$\alpha = \frac{\mu_0}{\sqrt{2m_0}}$$

with a certain number $\mu_0 \geq 1$. On the other hand, we want that

$$P(\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0,w\rangle) \ge \alpha|\text{case "BDD targets"})$$

is notably larger than 0.5. We consider

$$\begin{aligned} & P(\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0,w\rangle) \ge \alpha|\text{case "BDD targets"}) \\ = \; & P(F(e_0)+X \ge \alpha|\text{case "BDD targets"}) \\ \approx \; & P(Z(e_0)+X \ge \alpha) \end{aligned}$$

Since we know the distribution function of Z and X, the probability $P(Z+X \geq \alpha)$ can be computed numerically by a two-dimensional integral, if we further assume that Z and X are independent. However, here we want to derive a rough estimate on m_0 that gives us a simple formula. Since the standard deviation of X is equal to $\frac{1}{\sqrt{2m_0}} = \frac{\alpha}{\mu_0}$, we can approximate $P(Z+X \geq \alpha)$ by $P(Z \geq \alpha)$ for moderate μ_0. We further compute

$$\begin{aligned} P(Z+X \ge \alpha) \approx P(Z \ge \alpha) \quad & = P(e^{\gamma_0||e_0||^2/\sigma_0^2} \ge \alpha) \\ & = P(||e_0||^2/\sigma_0^2 \le \frac{\ln(\alpha)}{\gamma_0}) \end{aligned}$$

$||e_0||^2/\sigma_0^2$ is χ^2-distributed. If we choose

$$n+\sqrt{2n} \le \frac{\ln(\alpha)}{\gamma_0} \iff \alpha \le e^{\gamma_0(n+\sqrt{2n})}$$

we get a "good" probability for $P(Z \geq \alpha)$. (For $n \geq 50$ this probability of the χ^2-distribution is very near to 0.84.) In the end, we derive the condition

$$e^{\gamma_0(n+\sqrt{2n})} \geq \frac{\mu_0}{\sqrt{2m_0}} \iff 2m_0 \geq \mu_0^2 e^{-2\gamma_0(n+\sqrt{2n})} \qquad (H)$$

Remark 1: The condition (H) is very similar to the usual condition on m_0 computed under the independence heuristic. The main difference - ignoring $\mu_0 \geq 1$ - is a slightly higher number for the number of vectors m_0 due to the new term $n + \sqrt{2n}$ instead of n, which results in an additional factor of the form $e^{-2\gamma_0\sqrt{2n}}$.

Remark 2: What happens in the asymptotic case, when m_0 is extremely large? In the derivation of (H) we assume that $F(e_0)$ is extremely small compared to X, if e_0 is chosen uniformly in $\mathbb{R}^n/\Lambda$. This is certainly not true, when m_0 is extremely large. Instead, we consider

$$\begin{aligned} & P(\frac{1}{m_0}\sum_{w\in W}\cos(2\pi\langle e_0, w\rangle) \leq \alpha|\text{case "random targets"}) \\ = \;& P(F(e_0) + X \leq \alpha|\text{case "random targets"}) \\ \approx \;& P(F(e_0) \leq \alpha|\text{case "random targets"}) \end{aligned}$$

If we assume that the approximations in chapters 5 and 6 are valid, we have different distributions for $F(e_0)$ in both cases. This allows to distinguish the cases "random targets vs. BDD targets" with certain fixed probabilities, that do not depend on m_0.

Remark 3: A natural question arises: What are good weights in the formula for the total score taking into account the approach above? We therefore consider weights β_w in

$$f_\beta(t) = \sum_{w\in W}\beta_w\cos(2\pi\langle t, w\rangle).$$

We can adapt the formulas above if we restrict ourselves by choosing

$$\beta_w = e^{-\zeta_0||w||^2}$$

In this way, one can find an optimal ζ_0 that gives a certain lower condition on m_0 compared to (H).

9 References

[1]: Ducas, Pulles: Does the Dual-Sieve Attack on Learning with Errors even Work?, https://eprint.iacr.org/2023/302
[2]: Laarhoven, Walter: Dual lattice attacks for closest vector problems (with preprocessing). CT-RSA 2021, volume 12704

[3] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen, 296(4):625–636, 1993.

[4]De-Mei Yuan, Li-Ran Wei, and Lan Lei, Conditional central limit theorems for a sequence of conditional independent random variables, J. Korean Math. Soc. 51 (2014), No. 1