A remark on the Independence Heuristic in the Dual Attack

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

August 16, 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 lead to new formulas that seem to describe the result in [1, Table 1] quite accurately.

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 $t = v + e$ with $v \in \Lambda$ for any dual vector $w \in \Lambda^\vee$ one has

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

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 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 $(\frac{k_1}{p}, \ldots, \frac{k_n}{p})$, 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 $\langle \alpha, \mu \rangle \bmod 1$ and $\langle \alpha, \tilde{\mu} \rangle \bmod 1$ 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 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

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

as a random variable in e. 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

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

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

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

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

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

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

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

can be interpreted as a computation of a mean. Therefore, we can expect that the expression (D) 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 (D)

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

For the total variance we therefore expect as approximation

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

[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

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

If the expectation value of the score is larger than its standard deviation, we can expect that we can in fact distinguish the cases "random targets vs. BDD targets" with good probability. However, this is only the case if

$$2(1-2\gamma_0)^{-n} - (1-4\gamma_0)^{-n/2} \geq 0$$

This condition can be reformulated as

$$|\gamma_0| \leq 2r + \sqrt{r + 4r^2} \approx \sqrt{r} \approx \sqrt{\frac{\ln(2)}{2n}} \text{ with } r = \frac{2^{2/n} - 1}{4} \qquad (E)$$

5 Conclusions and Interpretations

1. If γ_0 is small, concretly such as (E) is fulfilled, we can expect that the usual dual attack should work by just computing the score $f_W(t)$. We then distinguish between the cases "random targets vs. BDD targets" by checking if the score $f_W(t)$ lies above a certain bound.

2. If γ_0 is very small, we can approximate (D) by

$$\begin{aligned} & (1-4\gamma_0)^{-n/2} - (1-2\gamma_0)^{-n} \\ \approx \quad & e^{2n\gamma_0} - e^{2n\gamma_0} = 0 \end{aligned}$$

   Therefore, we can just neglect this term in the computation of the variance. In the end, the score behaves as if the independence heuristic is valid.

3. If (E) is not fulfilled, the expectation value lies well within the interval given by the standard deviation. In order to distinguish the cases "random targets vs. BDD targets" we should not look at the expectation values but rather we should consider the different standard deviations. The standard deviations are notably different if for example

$$\begin{aligned} & 2\frac{m_0}{2} \leq \frac{m_0}{2} + m_0^2[(1-4\gamma_0)^{-n/2} - (1-2\gamma_0)^{-n}] \\ \iff \quad & \frac{1}{2m_0} \leq (1-4\gamma_0)^{-n/2} - (1-2\gamma_0)^{-n} \end{aligned}$$

   Again, we have a simple conditions on m_0 for the success of distinguishing the cases. In practice, we just check if the absolute value of the score $|f_W(t)|$ lies above a certain bound.

4. We computed some numerical experiments where w was chosen from a gaussian distribution but not from the dual lattice $\Lambda^\vee$. We noticed that in general the score does not look like a gaussian distribution. The same observation is made in [1, 5.3] where the w were taken from the dual lattice.

5. By the technique described above (i.e. using the Poisson summation formula) it is certainly possible to compute approximations of higher moments of the distribution of the score. With a good approximation of the distribution one could choose a better distinguisher.

6. A natural question arises: What are good weights in the formula for the total score taking into account the covariances? We therefore consider weights β_w in

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

We have

$$E(f_\beta(t)) = \sum_{w \in W} \beta_w e^{-2\pi^2 \sigma_0^2 ||w||^2}$$
$$V(f_\beta(t)) = \frac{1}{2} \sum_{w \in W} \beta_w^2 + \sum_{w,\tilde{w} \in W, w \neq \tilde{w}} \beta_w \beta_{\tilde{w}} \operatorname{Cov}(f_w(t), f_{\tilde{w}}(t))$$

As in [2, 5.1] a natural choice for β_w are weights that maximize the quotient

$$\frac{E(f_\beta(t))^2}{V(f_\beta(t))}$$

Let M be the $m_0 \times m_0$-matrix with entries $\operatorname{Cov}(f_w(t), f_{\tilde{w}}(t))$ for $w \neq \tilde{w}$ and $\frac{1}{2}$ on the diagonal and γ the vector of length m_0 with components $e^{-2\pi^2 \sigma_0^2 ||w||^2}$ in w. Since $V(f_\beta(t))$ is a quadratic form in the weights β_w, we can use the Cauchy-Schwarz inequality for computing the maximizing weights. The maximizing weights are given by

$$M^{-1}\gamma$$

If however the maximum of $\frac{E(f_\beta(t))^2}{V(f_\beta(t))}$ is small compared to 1, we try to distinguish the cases "random targets vs. BDD targets" by looking at the different standard deviations. The quotient of the two standard deviation is maximal for the eigenvector of the largest eigenvalue of M. Again, we computed some numerical experiments, (where w was chosen from a gaussian distribution but not from the dual lattice $\Lambda^\vee$). We observed only slight improvements of the scores by using good weights. In the end, it seems to be a valid approach to use just the simple form of the score and to dispense with the computational effort for the optimal choice of the weights.

6 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