Lecture 9: Goldreich-Levin Hardcore Bit

Christopher Brzuska

March 11, 2024

Before moving on, let us quickly remind ourselves of the context of the theorems we prove. Namely, in the first half of the basic crypto course, we discussed (but did not prove) that one-way functions (OWFs) imply pseudorandom generators (PRGs), that PRGs imply pseudorandom functions (PRFs), that PRFs imply unforgeable message authentication codes (MAC) and confidential symmetric encryption schemes (ENC), and that MACs and confidential encryption schemes together can be used to build authenticated encryption. As all of the aforementioned cryptographic primitives imply one-way functions, they are all equivalent, i.e., one exists if and only if all of the other primitives exist:

$$\mathsf{OWF} \Leftrightarrow \mathsf{PRG} \Leftrightarrow \mathsf{PRF} \Leftrightarrow \mathsf{MAC} \Leftrightarrow \mathsf{ENC} \text{ (MiniCrypt)}$$

Since one-way function are a minimal assumption for (computationally secure) cryptography, if (computationally secure) cryptography exists at all, then all of these primitives must exist. Thus, Impagliazzo, in his essay on average-case complexity (see `https://www.karlin.mff.cuni.cz/~krajicek/ri5svetu.pdf`), names this world *MiniCrypt*.

In the basic cryptography course, we proved that PRFs imply MACs, ENC and AE, but we only stated (and did not prove) that OWFs imply PRGs and that PRGs imply PRFs. In the last two weeks, we proved

$$\mathsf{PRG} \Rightarrow \mathsf{PRF} \text{ (Lecture 7 \& Lecture 8)}$$

This week and next week, we prove

$$\mathsf{OWF} \Rightarrow \mathsf{PRG} \text{ (Lecture 9 \& Lecture 10).} \tag{1}$$

Namely, in the basic cryptography course, we showed that

$$\text{length-preserving, bijective } \mathsf{OWF} + \mathsf{HB} \Rightarrow \mathsf{PRG} \text{ (basic cryptography course).}$$

Now, if we can show that

$$\mathsf{OWF} \Rightarrow \text{ length-preserving, bijective } \mathsf{OWF} + \mathsf{HB},$$

then we have proven Implication (1). In this lecture, we show

$$\mathsf{OWF} \Rightarrow \ \mathsf{OWF} + \mathsf{HB}.$$

There is a small gap to prove Implication (1), because it is known that one-way functions do (most likely) not imply length-preserving, bijective one-way functions[1]. Thus, we only prove an easier statement than Implication (1), as we started from length-preserving, bijective one-way functions. We aim to cover (the essence of) the full proof of the Implication (1) in Lecture 10. It is not an easy proof and will be the hardest part of the course[2]. The original proof by Hastad, Impagliazzo, Leving and Luby is available here `https://www.nada.kth.se/~johanh/prgfromowf.pdf`, but we will present an easier proof due to Vadhan and Zheng `https://eccc.weizmann.ac.il/report/2011/141/`.

Existence of one-way functions with hardcore bits We now turn to proving that if one-way functions exist, then there exist one-way functions with hardcore bits. More precise, we show that if f_{base} is a one-way function, the Goldreich-Levin hardcore bit is a hardcore bit for

$$\begin{aligned} f :&\{0,1\}^{2*} \to \{0,1\}^* \\ &(x,r) \mapsto f_{\text{base}}(x)||r \end{aligned}$$

Recall the the Goldreich-Levin hardcore-bit was defined by flipping a random bit r^i for each index i and then taking the xor over all indices of x, where r^i is equal to 1:

$$\begin{aligned} b_{GL} :&\{0,1\}^{2*} \to \{0,1\} \\ &(x,r) \mapsto (x_1 \wedge r_1) \oplus ... \oplus (x_{|x|} \wedge r_{|x|}) \end{aligned}$$

Technical Tricks

Before we turn to the proof of the Goldreich-Levin hardcore bit, we introduce five technical ideas:

(1) Distinguishing vs. predicting

(2) Averaging arguments

(3) Chebychev: a Chernoff-type bound for pairwise independent random variables

(4) Constructing n pairwise independent bitstrings from $\log n$ uniformly random, independent bitstrings

(5) Linearity of the Goldreich-Levin hardcore bit b_{GL}

[1] see Chapter 9 of Rudich's PhD thesis `http://www2.eecs.berkeley.edu/Pubs/TechRpts/1988/CSD-88-468.pdf`, and also see one of the exercises on Exercise Sheet 3 that suggests to prove that length-preserving, bijective one-way functions imply hard problems in $\mathsf{NP} \cap \mathbf{co}\mathsf{NP}$, which we do not expect to be true for one-way functions generally, because it is not clear how to find a short witness that a value is not in the image of a one-way function.

[2] If you are unfamiliar with complexity theory, then Lecture 11 and Lecture 12 are difficult, too, but the proof techniques will be a little less advanced than the techniques used in Lecture 10, in my opinion.

Distinguishing vs. predicting We formulated the security experiments for the hardcore bit as *distinguishing* experiments. Once could also ask an adversary to *predict* a hardcore bit and demand that for all PPT adversaries $\mathcal{A}$, the following probability is negligible:

$$\begin{aligned}&\mathsf{Adv}(\mathcal{A};\mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(n)\\ :=\ &\Pr_{w\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n,f(w))=b(w)]-\tfrac{1}{2}\end{aligned}$$

where the probability is over the sampling of x and the randomness of $\mathcal{A}$ (kept implicit in the experiment). We know that $\mathsf{Adv}(\mathcal{A};\mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(n)$ is negligible for all PPT adversaries $\mathcal{A}$, if and only if

```
$\mathsf{Exp}^{\mathsf{HB},0}_{f,b,\mathcal{A}}(1^n)$
$w \leftarrow\$ \{0,1\}^n$
$y \leftarrow f(w)$
$z \leftarrow b(w)$
$d^* \leftarrow\$ \mathcal{A}(1^n,y,z)$
return $d^*$
```

```
$\mathsf{Exp}^{\mathsf{HB},1}_{f,b,\mathcal{A}}(1^n)$
$w \leftarrow\$ \{0,1\}^n$
$y \leftarrow f(x)$
$z \leftarrow\$ \{0,1\}$
$d^* \leftarrow\$ \mathcal{A}(1^n,y,z)$
return $d^*$
```

Figure 1: Distinguishing Security experiment for hardcore bits.

$$\left|\Pr\left[1=\mathsf{Exp}^{\mathsf{HB},0}_{f,b,\mathcal{A}}(1^n)\right]-\Pr\left[\mathsf{Exp}^{\mathsf{HB},1}_{f,b,\mathcal{A}}(1^n)\right]\right| \tag{2}$$

is negligible for all PPT adversaries $\mathcal{A}$. The reason is, intuitively, that if one has a prediction algorithm, then one can also build a distinguishing algorithm, since the distinguisher can simply compare its input with the prediction of the prediction algorithm. In the other direction, if one has a distinguisher, then one can build a prediction algorithm that feeds a random trial input bit to the distinguisher and makes its prediction based on whether the distinguisher sais that its input was "good" or not. If you want to explore the proof in greater depth, you can do so on Exercise Sheet 3.

Averaging Arguments A second trick we need is a so-called *averaging argument.* Namely, imagine we know that an algorithm $\mathcal{A}$ predicts the Goldreich-Levin hardcore bit with probability

$$\Pr_{x\leftarrow\$\{0,1\}^n,r\leftarrow\$\{0,1\}^n}\left[\mathcal{A}(1^{2n},f(x,r))=b_{GL}(x,r)\right]\geq\tfrac{3}{4}. \tag{3}$$

How many $x\in\{0,1\}^n$ have the property that

$$\Pr_{r\leftarrow\$\{0,1\}^n}\left[\mathcal{A}(1^{2n},f(x,r))=b_{GL}(x,r)\right]\geq\tfrac{3}{4}\ ?$$

It turns out that there might be only very, very few x, where this is the case, possibly even a single x only, see Appendix A for an example. However, there must quite some x such that

$$\Pr_{r\leftarrow\$\{0,1\}^n}\left[\mathcal{A}(1^{2n},f(x,r))=b_{GL}(x,r)\right]\geq\tfrac{5}{8}.$$

This is what the averaging argument states more generally.

Lemma 1 (Averaging Argument)**.** Let $\epsilon(n)\geq 0$, and assume that

$$\Pr_{x\leftarrow\$\{0,1\}^n,r\leftarrow\$\{0,1\}^n}\left[\mathcal{A}(1^{2n},f(x,r))=b_{GL}(x,r)\right]\geq\tfrac{1}{2}+\epsilon(n).$$

Then we have that for at least $\frac{\epsilon(n)}{2}2^n$ many $x\in\{0,1\}^n$ that

$$\Pr_{r\leftarrow\$\{0,1\}^n}\left[\mathcal{A}(1^{2n},f(x,r))=b_{GL}(x,r)\right]\geq\tfrac{1}{2}+\tfrac{\epsilon(n)}{2}.$$

We prove the general averaging lemma (stated in Lecture 2) on Exercise Sheet 2 and give the proof of Lemma 1 in Appendix B.

Chebychev The Chernoff bound tells us that if we repeat an experiment with 0-1-outcome, independently, many times, and each experiments has probability of, say, $\frac{1}{2}+\frac{\epsilon(n)}{2}$ of being 1 and probability $\frac{1}{2}-\frac{\epsilon(n)}{2}$ of being 0, then we are going to have roughly a fraction of $\frac{1}{2}+\frac{\epsilon(n)}{2}$ of our independent experiments that return 1. The Chebychev bound tells us that a similar statement is true even when not all experiments are independent, but rather, they are only *pairwise* independent, i.e., for each pair of experiments Exp_i and Exp_j with $i \neq j$, it holds that

$$\Pr\big[\mathsf{Exp}_i = 1 \ \wedge \ \mathsf{Exp}_j = 1\big] = \Pr[\mathsf{Exp}_i = 1] \cdot \Pr\big[\mathsf{Exp}_j = 1\big].$$

Lemma 2 (Chebychev)**.** Let $\frac{1}{2} \geq \epsilon \geq 0$, and assume that we have m *pairwise independent* experiments Exp_1,...,Exp_m such that for each of the experiments

$$\Pr[\mathsf{Exp}_i = 1] \geq \tfrac{1}{2} + \tfrac{\epsilon(n)}{2}.$$

Then, we have the following inequality:

$$\Pr\left[\sum_{i=1}^{m} \mathsf{Exp}_i < \tfrac{1}{2}m\right] < \frac{1-\epsilon^2}{\epsilon^2 \cdot m}$$

In particular, when $m = n^2 \cdot \frac{1}{\epsilon^2}$, we have that

$$\Pr\left[\sum_{i=1}^{m} \mathsf{Exp}_i < \tfrac{1}{2}m\right] < \frac{1-\epsilon^2}{n^2} < \frac{1}{n^2}$$

See *Foundations of Cryptography I*, Chapter 1.2.2 for the proof of Lemma 2.

Pairwise Independent Bitstrings For each pair of non-empty subsets $I, J \subseteq \{1,..,\log m\}$ such that $I \neq J$, we have that sampling $\log m$ uniformly random strings r^i and xoring the bitstrings with indices in I and J, respectively, yields two independent, uniform bitstrings

$$\bigoplus_{i\in I} r^i \text{ and } \bigoplus_{j\in J} r_j$$

The reason is that if I and J are non-empty and distinct, then one of them, say, J, contains an index, say, j_0 that is contained in J but not in I. If we first sample all bitstrings except for r_{j_0}, then (a) we know the value of $\bigoplus_{i\in I} r^i$ (since j_0 is not contained in I), and (b) when we now sample r_{j_0}, we get a uniformly random value for $\bigoplus_{j\in J} r_j$. In Appendix C, we express the same argument in terms of probability analysis.

The pairwise independent argument will be useful, since out of $\log m$ independent, uniformly random strings $r_1, .., r_{\log m}$, we can now build m pairwise independent, uniformly random strings r_I, one for each non-empty subset $I \subseteq \{1,..,\log m\}$.

Linearity of b_{GL} The Goldreich-Levin bin is *linear* in its second entry, i.e., for all $r, r' \in \{0,1\}^n$, it holds that

$$b_{GL}(x,r) \oplus b_{GL}(x,r') = b_{GL}(x, r \oplus r').$$

We can calculate that this is indeed true:

$$\begin{aligned}
&b_{GL}(x,r) \oplus b_{GL}(x,r') \\
=&((x_1 \wedge r_1) \oplus .. \oplus (x_n \wedge r_n)) \oplus ((x_1 \wedge r'_1) \oplus .. \oplus (x_n \wedge r'_n)) \\
=&(x_1 \wedge (r_1 \oplus r'_1)) \oplus .. \oplus (x_n \wedge (r_n \oplus r'_n)) \\
=&b_{GL}(x, r \oplus r'),
\end{aligned}$$

where the first and last equality follows by definition and the middle equality follows, since $(x_i \wedge r^i) \oplus (x_i \wedge r'_i)$ is equal to x_i when *exactly* one out of r^i and $r^{i'}$ is 0. Else, $(x_i \wedge r^i) \oplus (x_i \wedge r'_i)$ is equal to 0, regardless of the value x_i.

We will use this linearity for the string $e_1 = 10..0$ and $\bigoplus_{i \in I} r_i$ for some strings r_i to be defined later. Namely, we will use that

$$b_{GL}(x, e^1 \oplus \bigoplus_{i \in I} r^i) \oplus b_{GL}(x, \bigoplus_{i \in I} r^i) = b_{GL}(x, e^1),$$

since $\bigoplus_{i \in I} r^i$ cancels out.

Goldreich-Levin Proof

Theorem 1 (Goldreich-Levin). *Let f_{base} be a one-way function. Then, the predicate b_{GL} is a hardcore predicate for f.*

$$\begin{aligned}
b_{GL} :&\{0,1\}^{2*} \to \{0,1\} & f :&\{0,1\}^{2*} \to \{0,1\}^* \\
&(x,r) \mapsto (x_1 \wedge r_1) \oplus ... \oplus (x_{|x|} \wedge r_{|x|}) & &(x,r) \mapsto f_{base}(x)||r
\end{aligned}$$

By our discussion of predicting vs. decision, we need to show that if f_{base} is a one-way function, then for all PPT adversaries $\mathcal{A}$, it holds that

$$\mathsf{Adv}(\mathcal{A}; \mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n) = \Pr_{x \leftarrow \$ \{0,1\}^n, r \leftarrow \$ \{0,1\}^n}\left[\mathcal{A}(1^{2n}, f(x,r)) = b_{GL}(x,r)\right] - \tfrac{1}{2}$$

is negligible[3]. We proceed by contradiction. I.e., we assume towards contradiction that there exists a PPT adversary $\mathcal{A}$ and a constant $c \geq 1$ such that $\mathsf{Adv}(\mathcal{A}; \mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n) \geq n^{-c}$ for infinitely many n. Assuming this, we then construct a PPT adversary $\mathcal{R}_{\mathcal{A}}$ such that for these n, it holds that

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{ow}}_{f_{\text{base}}, \mathcal{R}_{\mathcal{A}}}(2n) \qquad (4) \\
&= \Pr_{x \leftarrow \$ \{0,1\}^n, y \leftarrow f_{\text{base}}(x)}\Big[\mathcal{R}_{\mathcal{A}}(y, 1^{2n}) \overset{\$}{\to} x' \in f^{-1}_{\text{base}}(y) \wedge |x| = n\Big] \geq \tfrac{1}{4} n^{-3c-2}.
\end{aligned}$$

If we are able to show Inequality 4, then we reached a contraction and thus, an adversary $\mathcal{A}$ such that $\mathsf{Adv}(\mathcal{A}; \mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n) \geq n^{-c}$ cannot exist.

[3] Let's ignore that these values are only defined for even numbers $2n$. We can fix this by always ignoring the last bit of the input when there is an odd number, so that for all n, we have $\mathsf{Adv}(\mathcal{A}; \mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n+1) = \mathsf{Adv}(\mathcal{A}; \mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n)$.

So, let us start with assuming that the advantage $\mathsf{Adv}(\mathcal{A};\mathsf{Exp}^{\mathsf{HBPRE}}_{f,b,\mathcal{A}})(2n) \geq n^{-c}$ and step-by-step build an algorithm $\mathcal{R}_{\mathcal{A}}$ such that Inequality 4 holds. The code of reduction $\mathcal{R}_{\mathcal{A}}$ is given in Figure 2 but requires some motivation to understand it and analyze its success probability.

Firstly, by our averaging argument, we know that there exist $\frac{1}{2n^c}2^n$ many $x \in \{0,1\}^n$ such that

$$\Pr_{r \leftarrow\$ \{0,1\}^n}\left[\mathcal{A}(1^{2n}, f(x,r)) = b_{GL}(x,r)\right] \\ \geq \tfrac{1}{2} + \tfrac{1}{2n^c}$$

Let us now focus on such values x. Our goal is to recover x bit by bit. Let us now focus on the first bit x_1 of x. If we could somehow obtain the value $b_{GL}(x,r)$ for $r = 10...0$, then we would be done, because this value is equal to $(x_1 \wedge 1) \oplus (x_2 \wedge 0) \oplus ... \oplus (x_n \wedge 0) = x_1$. Unfortunately, $\mathcal{A}$ is only good on a *random* r and might fail on $e^1 = 10..0$. However, if we pick uniformly random values $r_1, .., r_{\log m}$, then $r^{1,I} \leftarrow e^1 \oplus \bigoplus_{i\in I} r^i$ is a uniformly random value.

```
$\mathcal{B}(1^{2n}, y)$
$r^1, .., r^{\log m} \leftarrow\$ \{0,1\}^n$
$b^1, .., b^{\log m} \leftarrow\$ \{0,1\}$
for $\emptyset \neq I \subseteq \{1, .., \log m\}$
  $b^I \leftarrow \bigoplus_{i\in I} b^i;\ r^I \leftarrow \bigoplus_{i\in I} r^i$
for $j$ from $1$ to $n$
  for $\emptyset \neq I \subseteq \{1, .., \log m\}$
    $r^{j,I} \leftarrow e^j \oplus r^I$
    $d^* \leftarrow\$ \mathcal{A}(y, r^{j,I}, 1^n)$
    $s^{j,I} \leftarrow b^I \oplus d^*$
  $x^*_j \leftarrow \mathrm{MAJ}_{I\subseteq\{0,1\}^*} s^{j,I}$
return $x^*_1||..||x^*_n$
```

Figure 2: $m = n^2 \cdot p(n) \cdot q(n)$. e^i denotes an n-bitstring which is 1 at position i and 0, else. MAJ denotes the majority function.

(1) If we now run $d^* \leftarrow\$ \mathcal{A}(y, r^{1,I}, 1^n)$ and

(2) *if* $d^* = b_{GL}(x, r^{1,I})$ (recall that $r^{1,I} \leftarrow e^1 \oplus \bigoplus_{i\in I} r^i$) and

(3) *if* we somehow knew $b^1 = b_{GL}(x, \bigoplus_{i\in I} r^{i,I})$

(4) *then* we could compute x_1 as $d^* \oplus b^1$ by the linearity of b_{GL}.

In particular, we could perform this operation not only for $j = 1$, but also for all $1 \leq j \leq n$.

For (2), we know that $d^* = b_{GL}(x, 1^i_I)$ holds with probability at least $\frac{1}{2} + \frac{1}{2n^c}$. If we know *all* of the values b^i, we could simply run $\mathcal{A}(y, r^{1,I}, 1^n)$ for all subsets $I \subseteq \{1, .., \log m\}$ and obtain m pairwise independent guesses for x_1. By Chebychev inequality, we then obtain the correct value of x_1 with high probability, namely

$$\Pr\left[\sum_{i=1}^{m} \mathsf{Exp}_i < \tfrac{1}{2}m\right] < \frac{1-\epsilon^2}{n^2} < \frac{1}{n^2}$$

by Lemma 2, if we choose $m = n^2 \cdot n^{2c}$.

The key question, now, is how do we obtain the values b^i for all subsets $I \subseteq \{1, .., \log m\}$? The solution is that we simply guess the value for $b_{\{1\}}$,..,$b_{\{\log m\}}$. If these values are correct, then by linearity of the Goldreich-Levin predicate, we can compute b^i as $\bigoplus_{i\in I} b^i$. The probability that we guess all the $b_{\{1\}}$,..,$b_{\{\log m\}}$ correctly is $(\frac{1}{2})^{\log m}$.

In summary, the reduction $\mathcal{R}_{\mathcal{A}}$ recovers the first bit x_1 correctly if

(a) x is in the "good" set (probability greater than $\frac{1}{2n^c}$),

(b) we guess $b_{\{1\}}$,..,$b_{\{\log m\}}$ correctly (probability equal to $(\frac{1}{2})^{\log m} = n^{-2-2c}$)

(c) the small failure probability of Chebychev does not occur (probability $1 - \frac{1}{n^2}$)

Now, consider the code of $\mathcal{R}_\mathcal{A}$ in Figure 2, and let us determine the probability that $\mathcal{R}_\mathcal{A}$ recovers the entire string x correctly, not just the first bit. Firstly note that we lose the $\frac{1}{2n^c}$ factor for x being in the "good" set only once. Secondly, notice that $\mathcal{R}_\mathcal{A}$ guesses $b_{\{1\}}$,..,$b_{\{\log m\}}$ only once, and thus, we lose this probability only once. In turn, the Chebychev failure probability, we lose for each of the bits x_i. Thus, in summary we obtain the following inversion probability:

$$\mathsf{Adv}^{\mathsf{ow}}_{f_{\text{base}},\mathcal{R}_\mathcal{A}}(2n) \geq \tfrac{1}{2}n^{-c} \cdot n^{-2-2c} \cdot (1 - n \cdot \tfrac{1}{n^2}) \geq \tfrac{1}{4}n^{-2-3c},$$

since $(1-n\cdot\frac{1}{n^2})$ is lower bounded by $\frac{1}{2}$. This concludes the proof of Inequality 4.

Concluding Reflections The Goldreich-Levin hardcore bit proof is one an example of *amplification*. I.e., we take a very weak predication algorithm and run it many times on cleverly chosen inputs such that we learn not only a specific bit but actually n bits with some reasoneable probability. If you enjoyed this proof, you might enjoy classes by Parinya Chalermsook, Petteri Kaski, Jara Uitto and Jukko Suomela at the CS Department and Lasse Leskelä at the MS Department. This proof is central to understanding the equivalence between the hardness of inverting and building hard distinguishing problems (PRGs, PRFs, symmetric encryption) that most of our cryptographic applications rely on. Thus, one-wayness, a very weak version of hardness, implies pseudorandomness, a very strong version of hardness. The remaining proofs in this course will involve significantly less probability analysis than the proof of the Goldreich-Levin Hardcore bit proof.

A Example for averaging argument

There could be only a *single* x_{good} such that

$$\Pr_{r\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n, f(x_{\text{good}}, r)) = b_{GL}(x_{\text{good}}, r)] = 1,$$

while for all other $x_{\text{bad}} \in \{0,1\}^n \setminus \{x_{\text{good}}\}$, it holds that

$$\Pr_{r\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n, f(x_{\text{bad}}, r)) = b_{GL}(x_{\text{bad}}, r)] = \tfrac{3}{4} - 2^{-2n} < \tfrac{3}{4}.$$

Indeed, if this is the case, then Inequality 3 still holds, since

$$\begin{aligned}
&\Pr_{x\leftarrow\$,r\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)]\\
=&\sum_{x\in\{0,1\}^n} 2^{-n} \cdot \Pr_{r\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)]\\
=&2^{-n}\cdot 1 + \sum_{x_{\text{bad}}\in\{0,1\}^n\setminus\{x_{\text{good}}\}} 2^{-n}\Pr_{r\leftarrow\$\{0,1\}^n}[\mathcal{A}(1^n, f(x_{\text{bad}}, r)) = b_{GL}(x_{\text{bad}}, r)]\\
=&2^{-n} + (1-2^{-n})\cdot(\tfrac{3}{4} - 2^{-2n})\\
\geq&2^{-n} + \tfrac{3}{4} - 2^{-2n} - \tfrac{3}{4}2^{-n}\\
\geq&\tfrac{3}{4}
\end{aligned}$$

B Proof for averaging argument

Recall that we are given some $\epsilon(n) \geq 0$ such that

$$\Pr_{x \leftarrow\$ \{0,1\}^n, r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)] \geq \tfrac{1}{2} + \epsilon(n). \tag{5}$$

Let us denote by $p(x)$ the following probability:

$$p(x) := \Pr_{r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)].$$

Now, let us assume towards contradiction that there are *strictly less* than $\frac{\epsilon(n)}{2}2^n$ many $x \in \{0,1\}^n$ such that

$$\Pr_{r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)] \geq \tfrac{1}{2} + \tfrac{\epsilon(n)}{2}. \tag{6}$$

We will now derive from this a contradiction with Inequality 5 by showing that *if* there are less that $\frac{\epsilon(n)}{2}2^n$ many $x \in \{0,1\}^n$ for which Inequality 6 holds, then $\Pr_{x \leftarrow\$ \{0,1\}^n, r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)]$ is *strictly* smaller than $\frac{1}{2} + \epsilon(n)$ in contradiction to Inequality 5.

$$\begin{aligned}
&\Pr_{x \leftarrow\$ \{0,1\}^n, r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)] \\
=& \sum_{x \in \{0,1\}^n} 2^{-n} \Pr_{r \leftarrow\$ \{0,1\}^n}[\mathcal{A}(1^n, f(x,r)) = b_{GL}(x,r)] \\
=& \sum_{x \in \{0,1\}^n} 2^{-n} p(x) \\
=& \sum_{x \in \{0,1\}^n:\ p(x) < \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} p(x) + \sum_{x \in \{0,1\}^n:\ p(x) \geq \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} p(x) \\
\leq& \sum_{x \in \{0,1\}^n:\ p(x) < \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} p(x) + \sum_{x \in \{0,1\}^n:\ p(x) \geq \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} \cdot 1 \\
<& \sum_{x \in \{0,1\}^n:\ p(x) < \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} \left(\frac{1}{2} + \frac{\epsilon(n)}{2}\right) + \sum_{x \in \{0,1\}^n:\ p(x) \geq \frac{1}{2} + \frac{\epsilon(n)}{2}} 2^{-n} \cdot 1 \\
<& \left(2^n - \frac{\epsilon(n)}{2}2^n\right) \cdot 2^{-n} \left(\frac{1}{2} + \frac{\epsilon(n)}{2}\right) + \left(\frac{\epsilon(n)}{2}2^n\right) 2^{-n} \cdot 1 \\
=& \frac{1}{2} + \frac{\epsilon(n)}{2} - \frac{\epsilon(n)}{2} \cdot \left(\frac{1}{2} + \frac{\epsilon(n)}{2}\right) + \frac{\epsilon(n)}{2} \\
<& \frac{1}{2} + \epsilon(n)
\end{aligned}$$

The first equality follows by noticing that there are 2^n values $x \in \{0,1\}^n$, each of which is chosen with probability 2^{-n}. The second equality follows by applying the definition of $p(x)$. The third equality consists in splitting the sum in two disjoint sets, as for each $x \in \{0,1\}^n$, it must either hold that $p(x) < \frac{1}{2} + \frac{\epsilon(n)}{2}$ or that $p(x) \leq \frac{1}{2} + \frac{\epsilon(n)}{2}$. The next inequality follow from the $p(x) \geq \frac{1}{2} + \frac{\epsilon(n)}{2}$ below the second sum sign which implies that 1 is an upper bound for $p(x)$. Note that we do not know whether 1 is a strict upper bound, and thus, the inequality is not strict. The subsequent strict inequality follows from the strict inequality below the second sum sign. The subsequent strict inequality follows from assuming (towards contradiction) that there are *strictly less* than $\frac{\epsilon(n)}{2}2^n$ many $x \in \{0,1\}^n$ such that Inequality 6 holds. The next equality step is basic arithmetic, and the final strict inequality follows from removing the term $-\frac{\epsilon(n)}{2} \cdot \left(\frac{1}{2} + \frac{\epsilon(n)}{2}\right)$ which is a negative number since $\epsilon(n)$ is strictly positive.

C Probability Analysis for Pairwise Independence

Let $w_0, w_1 \in \{0,1\}^n$. To show pairwise independence of $\bigoplus_{i \in I} r^i$ and $\bigoplus_{j \in J} r_j$, we need to show that the probability that $\bigoplus_{i \in I} r^i = w_0$ and that $\bigoplus_{j \in J} r_j = w_1$ is equal to $2^{-n} \cdot 2^{-n}$. Let i_0 be a value contained in I, and let j_0 be a value contained in $J \setminus I$. We denote by S the set $\{1,..,\log m\} \setminus \{i_0, j_0\}$. Before the proof, for simplicity, we perform a variable renaming, and rename i_0 to 1 and j_0 to 2. Then, we have that $S = \{3,..,\log m\}$ which contains $\log m - 2$ elements. We have to make a case distinction whether 1 is contained in J or not. Let us start with the case that 2 is not contained in J:

$$\begin{aligned}
&\Pr_{r_1,..,r_{\log m} \leftarrow\$ \{0,1\}^n}\left[w_0 = \bigoplus_{i \in I} r^i \ \wedge\ w_1 = \bigoplus_{j \in J} r_j\right] \\
=& \sum_{r_3,..,r_{\log m} \in \{0,1\}^{(\log m - 2)n}} 2^{-(\log m - 2)n} \Pr_{r_1 \leftarrow\$ \{0,1\}^n, r_2 \leftarrow\$ \{0,1\}^n}\left[w_0 = \bigoplus_{i \in I} r^i \ \wedge\ w_1 = \bigoplus_{j \in J} r_j\right] \\
=& \sum_{r_3,..,r_{\log m} \in \{0,1\}^{(\log m - 2)n}} 2^{-(\log m - 2)n} \Pr_{r_1 \leftarrow\$ \{0,1\}^n, r_2 \leftarrow\$ \{0,1\}^n}\left[w_0 \oplus \bigoplus_{i \in I \setminus \{1\}} = r_1 \ \wedge\ w_1 \oplus \bigoplus_{j \in J \setminus \{2\}} = r_2\right] \\
=& \sum_{r_3,..,r_{\log m} \in \{0,1\}^{(\log m - 2)n}} 2^{-(\log m - 2)n} \Pr_{r_1 \leftarrow\$ \{0,1\}^n, r_2 \leftarrow\$ \{0,1\}^n}[w_0' = r_1 \ \wedge\ w_1' = r_2] \\
=& \sum_{r_3,..,r_{\log m} \in \{0,1\}^{(\log m - 2)n}} 2^{-(\log m - 2)n} 2^{-n} \cdot 2^{-n} \\
=& 2^{-n} \cdot 2^{-n} \cdot \sum_{r_3,..,r_{\log m} \in \{0,1\}^{(\log m - 2)n}} 2^{-(\log m - 2)n} 1 \\
=& 2^{-n} \cdot 2^{-n}
\end{aligned}$$

In the third inequality, we rename $w_0 \oplus \bigoplus_{i \in I \setminus \{1\}}$ to w_0', because it is a fixed value w.r.t. the probability, and we rename we rename $w_1 \oplus \bigoplus_{j \in J \setminus \{2\}}$ to w_1', because it is a fixed value w.r.t. the probability.

For the case that 1 is contained in J, the third equality will read

$$
\begin{aligned}
&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\,\Pr_{r_1\leftarrow\$\{0,1\}^n,r_2\leftarrow\$\{0,1\}^n}\left[w_0\oplus\bigoplus_{i\in I\setminus\{1\}}=r_1\ \wedge\ w_1\oplus\bigoplus_{j\in J\setminus\{2\}}=r_1\oplus r_2\right]\\
=&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\,\Pr_{r_1\leftarrow\$\{0,1\}^n,r_2\leftarrow\$\{0,1\}^n}[w_0'=r_1\ \wedge\ w_1'=r_1\oplus r_2]\\
=&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\sum_{r_1\in\{0,1\}^n}2^{-n}\,\Pr_{r_2\leftarrow\$\{0,1\}^n}[w_0'=r_1\ \wedge\ w_1'=r_1\oplus r_2]\\
=&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\sum_{r_1\in\{0,1\}^n}2^{-n}\,\Pr_{r_2\leftarrow\$\{0,1\}^n}[w_0'=r_1\ \wedge\ w_1'\oplus w_0'=r_2]\\
=&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\cdot 2^{-n}\,\Pr_{r_2\leftarrow\$\{0,1\}^n}[w_1'\oplus w_0'=r_2]\\
=&\sum_{r_3,..,r_{\log m}\in\{0,1\}^{(\log m-2)n}} 2^{-(\log m-2)n}\cdot 2^{-n}\cdot 2^{-n}
\end{aligned}
$$

where the second but last equality follows since there is only exactly one $r_1\in\{0,1\}^n$ that is equal to w_0'.