Proving the Security of the Extended Summation-Truncation Hybrid

Avijit Dutta[1,2] and Eik List[3]

[1] Institute for Advancing Intelligence, TCG-CREST, India
[2] Academy of Scientific and Innovative Research (AcSIR), India
avirocks.dutta13(at)gmail.com
[3] Independent researcher
firstnamefirstlettersecondname(at)posteo.de

Abstract. Since designing a dedicated secure symmetric PRF is difficult, various works studied optimally secure PRFs from the sum of independent permutations (SoP). At CRYPTO'20, Gunsing and Mennink proposed the Summation-Truncation Hybrid (STH). While based on SoP, STH releases additional $a \leq n$ bits of the permutation calls and sums $n - a$ bits of them. Thus, it produces $n + a$ bits at $O(n - a/2)$-bit PRF security. Both SoP or STH can be used directly in encryption schemes or MACs in place of permutation calls for higher security. However, simply replacing every call as in GCM-SIVr would demand more calls.
For encryption schemes, Iwata's XORP scheme is long known to provide a better trade-off between efficiency and security. It extends SoP to variable-length-outputs by using $r + 1$ calls to a block cipher where the output of one call is added to each of the other r outputs. A similar extension can be conducted for STH that we call XTH, the XORP-Truncation Hybrid. Such an extension was already suggested in the final discussion by Gunsing and Mennink, but left as an open problem.
This work fills the gap by formalizing and proving the security of XTH. For a rate of $r/(r + 1)$ as in XORP, we show $O(n - a/2 - 1.5 \log(r))$-bit security for XTH.

Keywords: Secret-key cryptography · provable security · encryption · sum of permutations

1 Introduction

Since dedicated symmetric-key pseudorandom functions (PRFs) are hard to construct, the cryptographic community has been devoting sophisticated efforts towards designing PRFs from block ciphers and permutations. Research on the design of more secure PRFs from permutations came from truncation and summation. Hall et al. [10] truncated the output of an n-bit permutation from n bits to a bits, which yielded security for up to $O(2^{n-a/2})$ queries [1, 8], i.e., $(n-a/2)$-bit security. On the other hand, Bellare et al. [2] studied the security of the sum of permutations SoP. Initially, they studied two domain-separated instances of

the same permutation Π. That is, they fed an $(n-1)$-bit value x, appended different domain bits and summed the outputs from $\Pi(x\|0) \oplus \Pi(x\|1)$. Alternatively, one could also consider the sum of two independent n-bit permutations, i.e. $\Pi_1(x) \oplus \Pi_2(x)$ (also called SoP2). After a long series of works, the PRF security of SoP and SoP2 is well-understood to be about $O(n)$ [3, 4, 6, 7, 15].

Summation-Truncation Hybrid. In [9], Gunsing and Mennink proposed a trade-off between output length and PRF security by reconsidering truncation. They introduced the *Summation-Truncation Hybrid* (STH), which filled the range between those extremes. STH outputs a bits of each permutation call and the sum of the remaining $(n-a)$-bit outputs from both permutations:

$$\mathsf{STH}[a](x) \triangleq \Pi_1(x)[n-1..n-a] \| \left(0^a \| \Pi_1(x)[n-a-1..0]\right) \oplus \Pi_2(x)\,.$$

They showed that STH provides PRF security for up to $O(2^{n-a/2})$ queries.
SoP has proven highly useful for a number of designs, e.g. as a finalization of MACs or authentication parts of authenticated encryption schemes, e.g. in PMAC$^+$ [17], 3kf9 [18], Lightmac$^+$ [16], DBHtS [5], or Deoxys [14]. It is still an interesting question of finding good applications for STH. Efficient extensions to variable output lengths (VOL) could be one avenue towards more applications. Simply plugging in SoP or STH as a replacement for a block cipher in encryption or authenticated encryption can already suffice to increase a scheme's security, e.g. in GCM-SIVr [13]. However, such in-place instantiations would double the number of primitive calls compared to a usual block-cipher-based construction. For SoP, a more efficient extension is long known. In [11], Iwata had extended SoP to a VOL-PRF XORP, which takes an m-bit input and produces a sequence of r n-bit outputs as

$$\mathsf{XORP}[r](x) \triangleq \|_{i=1}^{r} \Pi(x\|\langle 0\rangle_s) \oplus \Pi(x\|\langle i\rangle_s)\ ,$$

where $s = \lceil \log_2(r+1) \rceil$ and $\langle i \rangle_s$ denotes the s-bit binary representation of the integer i and $m + s = n$. XORP achieved $O(n - \log_2(r^2))$-bit PRF security at a rate of $r/(r+1)$ [12].

Extending STH. In the concluding thoughts of their work, Gunsing and Mennink [9] suggested an extension of STH to more outputs, but left it as an open problem. We formalize such an extension as XTH, the XORP-Truncation Hybrid, which takes n-bit inputs x and produces $(a+rn)$-bit outputs as

$$\mathsf{XTH}[a,r](x) \triangleq \Pi_0(x)[n-1..n-a] \| \left\| \right._{i=1}^{r} \left(0^a \| \Pi_0(x)[n-a-1..0]\right) \oplus \Pi_i(x)\,.$$

Thus, it uses the first permutation's $(n-a)$ bits to mask the other outputs, increasing the output size by a bits compared to that of XORP. Thus, XTH seems interesting, but has not a security proof yet.

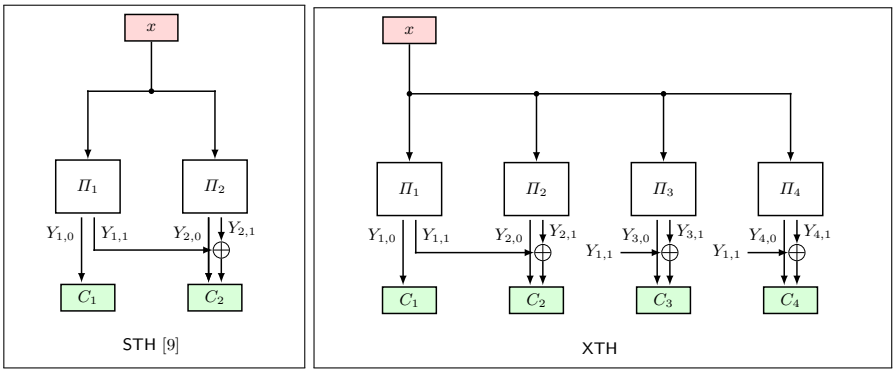

Fig. 1.1: Gunsing and Mennink's Summation-truncation hybrid and the XORP extension considered in this work.

Outline. In this work, we study the provable security of XTH and show that it achieves $O(n - a/2 - 1.5\log(r))$-bit PRF security. The remainder of this work is structured as follows. After preliminaries, Section 3 briefly recalls the definitions of STH and XTH before Sections 4 and 5 analyze the security of the latter. Section 6 concludes.

2 Preliminaries

For positive integers x, y, we write $[x] = \{1, \ldots, x\}$, $[0..x] = \{0, 1, \ldots, x\}$, and $[x..y] = \{x, x+1, \ldots, y\}$. We write $\{0,1\}^n$ for n-bit strings, and $X\|Y$ for the concatenation of two bitstrings X and Y. By $\langle i \rangle_s$, we denote the s-bit binary representation of a non-negative integer i. For a bitstring X, $|X|$ denotes the length of the bitstring X in terms of the number of bits. For integers x, n and bitstring $X \in \{0,1\}^n$, we use $X_1, \ldots, X_m \xleftarrow{x} X$ for the splitting of X into segments of $\leq x$ bits s. t. $|X_1| = \cdots = |X_{m-1}| = x$ and $|X_m| \leq x$. $(X_1, X_2) \xleftarrow{x,n-x} X$ indicates that $|X_1| = x$, $|X_2| = n - x$ and $X_1\|X_2 = X$. We write $X_1, X_2, \ldots \leftarrow_{\$} \mathcal{X}$ for the uniform and pairwise independent sampling with replacement of $X_1, X_2, \ldots$ from $\mathcal{X}$. Thus, $X_i \leftarrow_{\$} \mathcal{X}$, independent of the values X_j for $i \neq j$. For non-empty sets or spaces $\mathcal{T}$ and $\mathcal{X}$, $\mathsf{Perm}(\mathcal{X})$ is the set of permutations over $\mathcal{X}$ and $\widetilde{\mathsf{Perm}}(\mathcal{T}, \mathcal{X})$ the set of tweakable permutations over $\mathcal{X}$ with tweak space $\mathcal{T}$, that is, the functions $\widetilde{\Pi}(T, \cdot)$ that, for each tweak $T \in \mathcal{T}$, $\widetilde{\Pi}(T, \cdot)$, is a bijection over $\mathcal{X}$.

Distinguishers. A distinguisher **D** is an algorithm that interacts with one of several worlds that it shall distinguish between. Prior, the challenger samples a random bit $b \leftarrow_{\$} \{0,1\}$ and presents **D** with one of two sets of oracles depending on the value of b. We use $b = 1$ for the real world. Moreover, the challenger uses internal secrets. **D** interacts with the individual oracles and collects the

responses. At the end, $\mathbf{D}$ outputs a guess b' and wins iff $b = b'$. We write

$$\Delta_{\mathbf{D}}(\mathcal{R}_K; \mathcal{I}) \triangleq \left| \Pr_K \left[\mathbf{D}^{\mathcal{R}_K} = 1\right] - \Pr\left[\mathbf{D}^{\mathcal{I}} = 1\right] \right|$$

for the advantage of $\mathbf{D}$ in distinguishing a real keyed construction $\mathcal{R}_K$ from an ideal construction $\mathcal{I}$, where the probability is over the key K, the randomness of $\mathcal{I}$, the coins of $\mathbf{D}$ and that of the challenger, if any.

PRF Security. Given two non-empty sets or spaces $\mathcal{X}, \mathcal{Y}$, let $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, $\rho \leftarrow\!\!\$\, \mathsf{Func}(\mathcal{X}, \mathcal{Y})$, and let $K \leftarrow\!\!\$\, \mathcal{K}$ be a secret key. The PRF advantage of a distinguisher $\mathbf{D}$ on F_K is defined as $\mathbf{Adv}^{\mathsf{PRF}}_{F_K}(\mathbf{D}) \triangleq \Delta_{\mathbf{D}}(F_K; \rho)$.

The χ^2 Method. We will employ the χ-square method by Dai et al. [4]. For this purpose, we briefly recall its main theorem. For each $i \in [q]$ and each vector $\mathbf{W}^{i-1} = (W_2^{i-1}, \ldots, W_r^{i-1})$ with $\mathbf{W}_j^{i-1} = (W_j^1, W_j^2, \ldots, W_j^{i-1})$, define

$$\chi^2(\mathbf{W}^{i-1}) \stackrel{\text{def}}{=} \sum_{W \in (\mathbb{F}_2^b)^{r-1}} \frac{\left(\Pr_{\mathcal{O}_{\text{real}}}[\mathbf{W}^i = W | \mathbf{W}^{i-1}] - \Pr_{\mathcal{O}_{\text{ideal}}}[\mathbf{W}^i = W | \mathbf{W}^{i-1}]\right)^2}{\Pr_{\mathcal{O}_{\text{ideal}}}[\mathbf{W}^i = W | \mathbf{W}^{i-1}]} .$$

Theorem 1 (χ^2 Method [4]). Consider two systems $\mathcal{O}_{\text{real}}$ and $\mathcal{O}_{\text{ideal}}$. Suppose that for any vector $\mathbf{W}$, it holds that $\Pr_{\mathcal{O}_{\text{ideal}}}[\mathbf{W}^i] > 0$ whenever $\Pr_{\mathcal{O}_{\text{real}}}[\mathbf{W}^i] > 0$. Then

$$\left| \Pr_{\mathcal{O}_{\text{real}}} \left[\mathbf{W}^i\right] - \Pr_{\mathcal{O}_{\text{ideal}}} \left[\mathbf{W}^i\right] \right| \leq \sqrt{\frac{1}{2} \sum_{i=1}^{q} \mathbb{E}_{\mathcal{O}_{\text{real}}}[\chi^2(\mathbf{W}^{i-1})]} .$$

3 XTH

STH. We note that two versions of the Summation-Truncation-Hybrid [9] exist: based on a single n-bit secret full-round permutation Π, and based on a pair of independent permutations Π_1 and Π_2. Here, we focus on the second version and refer to it as STH.
It feeds the n-bit input x into two independent full round n-bit secret permutations Π_1 and Π_2, and splits each of their outputs Y_i, where $Y_i = \Pi_i(x)$, into an a-bit part $Y_{i,0}$ and an $(n-a)$-bit part $Y_{i,1}$, for $i \in \{1, 2\}$, i.e., $(Y_{i,0}, Y_{i,1}) \xleftarrow{a, n-a} Y_i$, for $i \in \{1, 2\}$. The a-bit parts $Y_{1,0}$ and $Y_{2,0}$ are output in plain; the $(n-a)$-bit parts are summed and output as $Y_{1,1} \oplus Y_{2,1}$. Gunsing and Mennink have shown that STH achieves roughly $(n - a/2)$-bit security.

XTH. We define the XORP-based Summation-Truncation Hybrid (XTH) as follows. For $a, r \in \mathbb{N}$ with $a \leq n$, $\mathsf{XTH}[a, r]$ feeds an n-bit input x into r independent n-bit secret permutations $\Pi_1, \ldots, \Pi_r$. Thereupon, it partitions each permutation output $Y_i = \Pi_i(x)$ into an a-bit part $Y_{i,0}$ and an $(n-a)$-bit part $Y_{i,1}$, for

Algorithm 1 Definition of $\mathsf{XTH}[a,r]_{\Pi_0,\ldots,\Pi_r}$.

11: **function** $\mathsf{STH}[a]_{\Pi_1,\Pi_2}(x)$	21: **function** $\mathsf{XTH}[a,r]_{\Pi_1,\Pi_2,\ldots,\Pi_r}(x)$
12: $(Y_{1,0}, Y_{1,1}) \xleftarrow{a,n-a} \Pi_1(x)$	22: **for** $i \leftarrow 1 \,..\, r$ **do**
13: $(Y_{2,0}, Y_{2,1}) \xleftarrow{a,n-a} \Pi_2(x)$	23: $(Y_{i,0}, Y_{i,1}) \xleftarrow{a,n-a} \Pi_i(x)$
14: **return** $Y_{1,0} \| Y_{2,0} \oplus Y_{2,1}$	24: **return** $Y_{1,0} \Big\| \Big(\|_{i=2}^{r} Y_{i,0} \| Y_{1,1} \oplus Y_{i,1} \Big)$

$i \in \{1,\ldots,r\}$. The a-bit parts $Y_{1,0}, Y_{2,0}, \ldots, Y_{r,0}$ are then returned as outputs. The $(n-a)$-bit parts $Y_{2,1}$, $Y_{3,1}$ etc., in contrast, are XORed to the $(n-a)$-bit output of the first permutation call, and the sum is returned for each block: $Y_{1,1} \oplus Y_{2,1}, Y_{1,1} \oplus Y_{3,1}, \ldots, Y_{1,1} \oplus Y_{r,1}$. Algorithm 1 lists formal definitions for both STH and XTH.

4 Security Analysis of XTH

In this section, we state and prove the following main security result of XTH.

Theorem 2. Let r, n, a, b and q be positive integers with $r \geq 2$, $a + b = n$, and $q < 2^{b-2}$ and $q \leq 2^n/(2r)$. Let $\Pi_1, \ldots, \Pi_r \leftarrow\!\!\$\, \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let $\mathbf{D}$ be a PRF distinguisher on the construction $\mathsf{XTH}[a,r]_{\Pi_1,\Pi_2,\ldots,\Pi_r}$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{XTH}[a,r]}(\mathbf{D}) \leq \left(\frac{4}{3}\right)^r \left(\frac{rq}{2^{n-a/3}}\right)^{3/2} + 2^{a-1} \cdot \left(\frac{16rq}{2^n}\right)^{2^{b-2}} + \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{trunc}_a}(rq)\,.$$

By substituting $r = 2$ into Theorem 2, we recover the PRF advantage of STH using a pair of independent permutations as follows:

Corollary 1. Let n, a, b and q be positive integers such that $a + b = n$, and $q < 2^{b-2}$ and $q \leq 2^n/4$. Let $\Pi_1, \Pi_2 \leftarrow\!\!\$\, \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let $\mathbf{D}$ be a PRF distinguisher on $\mathsf{STH}[a]_{\Pi_1,\Pi_2}$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{STH}[a]}(\mathbf{D}) \leq 8 \cdot \left(\frac{q}{2^{n-a/3}}\right)^{3/2} + 2^{a-1} \cdot \left(\frac{32q}{2^n}\right)^{2^{b-2}} + \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{trunc}_a}(2q)\,.$$

Proof (Proof of Theorem 2). The general proof strategy will follow that by [9]. Let $\Pi_1, \ldots, \Pi_r \leftarrow\!\!\$\, \mathsf{Perm}(\mathbb{F}_2^n)$ such that all permutations Π_j are pairwise independent. We consider two oracles, $\mathcal{O}_{\text{ideal}}$ and $\mathcal{O}_{\text{real}}$. Let $\mathbf{D}$ be a distinguisher that is given access to one of them, chosen uniformly at random. $\mathbf{D}$ shall distinguish between both worlds, given the transcript τ of queries of $\mathbf{D}$ to the oracle, the corresponding responses, and intermediate variables. We define by $\mathbf{I}_n$ the identity permutation over $\mathbb{F}_2^n$. For integers $n = a + b$ and $X \in \mathbb{F}_2^n$ with $X = V \| Y$ and $V \in \mathbb{F}_2^a$, $Y \in \mathbb{F}_2^b$, we define $\mathsf{msb}_a(X) = V$ to always return the leftmost a bits of X and $\mathsf{lsb}_b(X) = Y$ to return the b least significant b bits of X, and $(V, Y) \xleftarrow{a,n-a} X$ splits X into an a-bit part V and an $(n-a)$-bit part Y.

Algorithm 2 Real-world oracles from the analysis of $\mathsf{XTH}[a,r]_{\Pi_1,\ldots,\Pi_r}$.

```
11: function O_1(M)
12:     Π_1, Π_2, ... Π_r ←$ Perm(F_2^n)
13:     M^1, ..., M^q ← M
14:     for i ← 1 to q do
15:         for j ← 1 to r do
16:             (V_j^i, Y_j^i) ←^{a,b} Π_j(M^i)
17:             if j ≥ 2 then
18:                 W_j^i ← Y_1^i ⊕ Y_j^i
19:         V^i ← (V_1^i, V_2^i, ..., V_j^i)
20:         W^i ← (W_2^i, ..., W_j^i)
21:     V ← (V^1, ..., V^q)
22:     W ← (W^1, ..., W^q)
23:     τ ← (V, W)
24:     return τ

31: function O_2(M)
32:     V ← PTrunc[r](M)
33:     W ← PSoP[r](M, V)
34:     return τ = (V, W)

41: function PTRUNC[r](M)
42:     for i ← 1 to q do
43:         for j ← 1 to r do
44:             V_j^i ←$ F_2^a
45:         V^i ← (V_1^i, ..., V_r^i)
46:     return V = (V^1, ..., V^q)

51: function PSoP[r](M, V)
52:     for j ← 1 to r do
53:         if Perm_comp(V_j) = ∅ then
54:             Π_j ←$ I_n
55:         else
56:             Π_j ←$ Perm_comp(V_j)
57:     for i ← 1 to q do
58:         for j ← 1 to r do
59:             Y_j^i ← lsb_b(Π_j(⟨i⟩))
60:             if j ≥ 2 then
61:                 W_j^i ← Y_1^i ⊕ Y_j^i
62:         W^i ← (W_2^i, ..., W_r^i)
63:     return W = (W^1, ..., W^q)
```

On message input M^i, the real world $\mathcal{O}_{\text{real}}$ uses $\mathsf{XTH}[a,r]_{\Pi_1,\ldots,\Pi_r}(M^i)$ and produces and outputs $V_1^i, V_2^i, W_2^i, \ldots, V_r^i, W_r^i$, where for each $j \in [r]$, $(V_j^i, Y_j^i) \xleftarrow{a,b} \Pi_j(M^i)$ and $W_j^i = Y_1^i \oplus Y_j^i$ for all $j \in [2..r]$. The values are collected in vectors $\mathbf{V} = (\mathbf{V}^1, \ldots, \mathbf{V}^q), \mathbf{Y} = (\mathbf{Y}^1, \ldots, \mathbf{Y}^q)$, and $\mathbf{W} = (\mathbf{W}^1, \ldots, \mathbf{W}^q)$ with $\mathbf{V}^i = (V_1^i, \ldots, V_r^i), \mathbf{Y}^i = (Y_1^i, \ldots, Y_r^i)$, and $\mathbf{W}^i = (W_2^i, \ldots, W_r^i)$ for all $i \in [q]$. Let $\tau = (\mathbf{V}, \mathbf{W})$ be the transcript. Over all queries, we define the short-hand notation $\mathbf{V}_j = (V_j^1, \ldots, V_j^q)$ for some $j \in [r]$.

The ideal world $\mathcal{O}_{\text{ideal}}$ samples all outputs $V_j^i \leftarrow_{\$} \mathbb{F}_2^a$, for all $i \in [q]$ and $j \in [r]$ and samples $W_2^i, \ldots, W_r^i \leftarrow_{\$} \mathbb{F}_2^b$, for all $i \in [q]$. We denote the real-world oracle as $\mathcal{O}_1$ since we will modify it stepwise in the following. It holds that

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{XTH}[a,r]}(\mathcal{A}) \leq \left|\Pr\left[\mathcal{O}_{\text{ideal}}\right] - \Pr\left[\mathcal{O}_{\text{real}}\right]\right| .$$

Next, we separate the a-bit values, $(V_1^i, \ldots, V_r^i)$, given out in clear from the results of the sums, $(W_2^i, \ldots, W_r^i)$. This yields the modified real world $\mathcal{O}_2$. Internally, $\mathcal{O}_2$ uses a function $\mathsf{PTrunc}[r]$ that samples the values $\mathbf{V} = (V_1, \ldots, V_r)$ as a-bit values sampled independently uniformly at random from $\mathbb{F}_2^a$ each. This is given in Algorithm 2. Moreover, we define $\mathsf{PSoP}[r]$, which takes $(V_1, \ldots, V_r)$ and samples $r-1$ permutations compatible to it (if they exist) and computes the vector of sum values, $\mathbf{W} = (W_2^i, \ldots, W_r^i)$, from it. For all $j \in [r]$ and given vectors of a-bit strings $\mathbf{V}_j = (V_j^1, \ldots, V_j^q) \in (\mathbb{F}_2^a)^q$, we define $\mathsf{Perm}_{\mathsf{comp}}(\mathbf{V}_j) \subseteq \mathsf{Perm}(\mathbb{F}_2^{n-a})$ as the set of all n-bit permutations that would produce $\mathbf{V}_j$ in their most significant a-bit outputs for the inputs in $\mathbf{V}_j$. The difference between both worlds is upper bounded by

$$\left|\Pr[\mathcal{O}_2] - \Pr[\mathcal{O}_{\text{real}}]\right| \leq \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{trunc}_a}(rq) .$$

From the triangle inequality, the difference in the setting is at most

$$\left|\Pr[\mathcal{O}_{\text{ideal}}] - \Pr[\mathcal{O}_{\text{real}}]\right| \leq \left|\Pr[\mathcal{O}_{\text{ideal}}] - \Pr[\mathcal{O}_2]\right| + \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{trunc}_a}(rq) .$$

We want to upper bound the distance between the multi-sum of pairwise independent permutations and the function that produces random bits. For the

values V_1, V_2, ..., V_r, we define counters

$$C_{\mathbf{V},j}(i) \stackrel{\text{def}}{=} \left|\left\{V_j^{i'} : V_j^{i'} = V_j^i\right\}\right| , \text{ for all } j \in [r] .$$

Those counters will later have to remain below 2^{b-2}. For the case that one of them exceeds this amount, we define a set bad of vectors $\mathbf{V}$ such that there exists $k \in [r]$ with $C_{\mathbf{V},k}(i) \geq 2^{b-2}$, which we denote as bad. Given a transcript τ that contains $\mathbf{V}$, we see that

$$\mathbb{E}_\tau[\Pr[\mathcal{O}_{\text{ideal}} = \tau] - \Pr[\mathcal{O}_2 = \tau]] \leq \mathbb{E}_\tau[\Pr[\mathcal{O}_{\text{ideal}} = \tau] - \Pr[\mathcal{O}_2 = \tau|\overline{\mathsf{bad}}]] + \Pr[\mathsf{bad}] .$$

Multi-Collision. We can upper bound $\Pr[\mathsf{bad}]$ first, which requires a (2^{b-2})-collision of values $V_j^{i_1} = \cdots = V_j^{i_{2^{b-2}}}$ inside any one of r vectors $\mathbf{V}_j$ in $\mathbf{V}$. Since the values V_j^i are chosen independently and uniformly at random each, the probability for a t-collision is upper bounded by

$$\frac{(rq)^t}{2^{a(t-1)} \cdot t!}$$

By using Stirling's approximation and substituting $t = 2^{b-2}$

$$\begin{aligned}\Pr[\mathsf{bad}] &\leq \frac{1}{\sqrt{2\pi}} \cdot \frac{(rq)^t}{2^{a(t-1)}} \cdot \left(\frac{1}{2^{3/2} \cdot t}\right)^t \leq \frac{2^a}{\sqrt{2\pi}} \cdot \left(\frac{rq}{2^{a-3/2} \cdot t}\right)^t \\ &\leq \frac{2^a}{\sqrt{2\pi}} \cdot \left(\frac{rq}{2^{a-2} \cdot 2^{b-2}}\right)^{2^{b-2}} \leq 2^{a-1} \cdot \left(\frac{16rq}{2^n}\right)^{2^{b-2}} .\end{aligned}$$

We have to upper bound the expectation of the difference of the probabilities of the realized good transcripts in world $\mathcal{O}_2$ and $\mathcal{O}_{\text{ideal}}$. Since for good transcripts, the vectors $\mathbf{V}$ are sampled equally in both worlds, we can focus on the vectors $\mathbf{W}$. We obtain the following.

Theorem 3. Let a, b, q, r be positive integers and $\tau = (\mathbf{V}, \mathbf{W})$ be a good transcript such that $C_{\mathbf{V},j}(i) < 2^{b-2}$ holds for all $i \in [q]$ and $j \in [r]$ and $q \leq 2^n/(3r)$. Then, for $r \geq 2$

$$\mathbb{E}_\tau \left[\left|\Pr\left[\mathcal{O}_2 = \tau\right] - \Pr\left[\mathcal{O}_{\text{ideal}} = \tau\right]\right|\right] \leq \left(\frac{4}{3}\right)^r \cdot \left(\frac{rq}{2^{n-a/3}}\right)^{3/2} .$$

5 Proof of Theorem 3

We can easily see that $\Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W|\mathbf{W}^{i-1}] = 2^{-(r-1)b}$. Though, it remains to determine the probability in the real world. We denote the outputs $(Y_1^i, Y_2^i, \ldots, Y_r^i)$ also as $(y_1^i, y_2^i, \ldots, y_r^i)$ and the fixed sum values at the i-th step $(W_2^i, \ldots, W_r^i)$ also as $(w_2^i, \ldots, w_r^i)$. We consider r independent permutations π_1, $\ldots \pi_r$. We have to determine the probability

$$\Pr_{\mathcal{O}_{\text{real}}}\left[\mathbf{W}^i = (w_2^i, \ldots, w_r^i)|\mathbf{Y}^{i-1}\right] ,$$

where $\mathbf{Y}^{i-1} = (Y_1^1, \ldots, Y_r^1, \ldots, Y_1^{i-1}, \ldots, Y_r^{i-1})$. Fix a tuple $\mathbf{W}^i = (w_2^i, \ldots, w_r^i) \in (\mathbb{F}_2^b)^{r-1}$. We define $q \times r$ sets $\mathcal{S}_j^i = \{y_j^1, \ldots, y_j^{i-1}\}$ for all $i \in [q]$ and $j \in [r]$. Furthermore, we propose sets of translated values $\mathcal{S}_{y_j \to w_j}^i = \mathcal{S}_j^i \oplus w_j \triangleq \{Y_j \in \mathcal{S}_j^i : Y_j \oplus w_j\}$ to denote the elementwise translation of $\mathcal{S}_j^i$ for the fixed scalar $w_j \in \mathbb{F}_2^b$ for all $j \in \{2, \ldots, r\}$. For consistency, we introduce $w_1^i = 0^b$ for all $i \in [q]$ so we can define $\mathcal{S}_{y_1 \to w_1}^i = \mathcal{S}_1^i$. We define cardinalities $s_j^{i,w_j} = |\mathcal{S}_{y_j \to w_j}^i| = |\mathcal{S}_j^i|$ for all $j \in [r]$, and will use the short form $s_j^i = s_j^{i,w_j}$ hereafter. We have to find the number of possible solutions $Y^i = (Y_1^i, \ldots, Y_r^i)$ for the next fixed tuple $W^i = (w_2^i, \ldots, w_r^i)$. For $Y_1^i \oplus Y_2^i = w_2^i$, $Y_1^i \oplus Y_3^i = w_3^i$, ..., it must hold that

$$Y_1^i \in \mathbb{F}_2^b \setminus \left(\mathcal{S}_1^i \cup \bigcup_{j=2}^{r} (\mathcal{S}_{y_j \to w_j}^i) \right) .$$

Let n^i denote the number of choices for Y_1^i. From the inclusion-exclusion principle

$$\begin{aligned}
n^i &= 2^b - \left(|\mathcal{S}_{y_1 \to w_1}^i| + |\mathcal{S}_{y_2 \to w_2}^i| + \cdots + |\mathcal{S}_{y_r \to w_r}^i|\right) \\
&\quad + \left(|\mathcal{S}_{y_1 \to w_1}^i \cap \mathcal{S}_{y_2 \to w_2}^i| + |\mathcal{S}_{y_1 \to w_1}^i \cap \mathcal{S}_{y_3 \to w_3}^i| + \cdots + |\mathcal{S}_{y_{r-1} \to w_{r-1}}^i \cap \mathcal{S}_{y_r \to w_r}^i|\right) \\
&\quad - \left(|\mathcal{S}_{y_1 \to w_1}^i \cap \mathcal{S}_{y_2 \to w_2}^i \cap \mathcal{S}_{y_3 \to w_3}^i|\right) + \cdots \Big) + \cdots \\
&= 2^b - \left(\sum_{j=1}^{r} |\mathcal{S}_{y_j \to w_j}^i| \right) + \left(\sum_{j_1 < j_2} |\mathcal{S}_{y_{j_1} \to w_{j_1}}^i \cap \mathcal{S}_{y_{j_2} \to w_{j_2}}^i| \right) \\
&\quad - \left(\sum_{1 \le j_1 < j_2 < j_3 \le r} |\mathcal{S}_{y_{j_1} \to w_{j_1}}^i \cap \mathcal{S}_{y_{j_2} \to w_{j_2}}^i \cap \mathcal{S}_{y_{j_3} \to w_{j_3}}^i| \right) + \cdots \\
&= 2^b - \left(\sum_{j=1}^{r} s_j^i \right) + \left(\sum_{1 \le j_1 < j_2 \le r} s_{j_1,j_2}^{i,w_{j_1},w_{j_2}} \right) - \left(\sum_{1 \le j_1 < j_2 < j_3 \le r} s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}} \right) \\
&\quad + \cdots + (-1)^r \left(\sum_{1 \le j_1 < \cdots < j_r \le r} s_{j_1,\ldots,j_r}^{i,w_{j_1},w_{j_2},\ldots,w_{j_r}} \right) , \qquad (1)
\end{aligned}$$

where we define $s_{1,2}^{i,w_1,w_2}$, $s_{1,2,3}^{i,w_1,w_2,w_3}$, ... for the cardinalities of the corresponding intersection sets in a natural manner. We call the terms $s_{1,2}^{i,w_1,w_2}$ 2-tuple-related, $s_{1,2,3}^{i,w_1,w_2,w_3}$ 3-tuple-related, and so on. For each, we have to upper bound its expectation and variance.

Expectation and Variance of 2-tuple-related Terms. We can use the knowledge about $s_{1,2}^{i,w_1,w_2} = s_{1,2}^{i,0,w_2} = D_{i,w}$ from [4, 9]. Thus, the expectation and variance of all cardinalities of two-component intersections can be taken from Equations (34), (35) in [9] as

$$\mathbb{E}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] = \frac{s_{j_1}^i s_{j_2}^i}{2^b} \quad \text{and} \quad \mathbf{Var}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] \le \frac{2 s_{j_1}^i s_{j_2}^i}{2^b} . \qquad (2)$$

For independent permutations $\pi_1, \ldots, \pi_r$, and independent Binomial variables, we can derive them more precisely.

Lemma 1. For distinct $j_1, j_2 \in [r]$, it holds that

$$\mathbb{E}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] = \frac{s_{j_1}^i s_{j_2}^i}{2^b} \quad \text{and} \quad \mathbf{Var}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] = \frac{s_{j_1}^i s_{j_2}^i}{2^b} - \frac{(s_{j_1}^i s_{j_2}^i)^2}{2^{3b}}\,.$$

Expectation and Variance of 3-tuple-related Terms. Next, we consider the expectation and variance of $s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}$.

Lemma 2. For distinct $j_1, j_2, j_3 \in [r]$, it holds that

$$\mathbb{E}\left[s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}\right] = \frac{s_{j_1}^i s_{j_2}^i s_{j_3}^i}{2^{2b}}, \quad \mathbf{Var}\left[s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}\right] = \frac{s_{j_1}^i s_{j_2}^i s_{j_3}^i}{2^{2b}} - \frac{(s_{j_1}^i s_{j_2}^i s_{j_3}^i)^2}{2^{5b}}\,.$$

Expectation and Variance of Terms for General Tuples.

Lemma 3. Let $t \leq r$ and $\mathcal{I} = \{j_1, \ldots, j_t\} \subseteq \{1, \ldots, r\}$. Then, it holds for the expectation and variance that

$$\mathbb{E}\left[s_{j_1,j_2,\ldots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \frac{\prod_{j\in\mathcal{I}} s_j^i}{2^{(t-1)b}}, \quad \mathbf{Var}\left[s_{j_1,j_2,\ldots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \frac{\prod_{j\in\mathcal{I}} s_j^i}{2^{(t-1)b}} - \frac{\left(\prod_{j\in\mathcal{I}} s_j^i\right)^2}{2^{(2t-1)b}}\,.$$

We defer the proof of Lemmas 1, 2, and 3 to Appendix A.1, Appendix A.2, and Appendix A.3 respectively.

Determining the Ratio. In the real and ideal worlds, it holds that

$$\Pr_{\mathcal{O}_{\text{real}}}\left[W^i = (w_2^i, \ldots, w_r^i) | \mathbf{Y}^{i-1}\right] = \mathbb{E}\left[\frac{n^i}{d^i}\right] \text{ and}$$
$$\Pr_{\mathcal{O}_{\text{ideal}}}\left[W^i = (w_2^i, \ldots, w_r^i) | \mathbf{W}^{i-1}\right] = \frac{1}{2^{(r-1)b}}\,,$$

respectively, with n^i given in Equation (1). The number of all choices of Y^i, that represents the denominator d^i, is given by

$$\begin{aligned} d^i &= (2^b - s_1^i) \cdot (2^b - s_2^i) \cdot \cdots \cdot (2^b - s_r^i) = \prod_{j=1}^{r} (2^b - s_j^i) \\ &= 2^{rb} - 2^{(r-1)b}\left(\sum_{j=1}^{r} s_j^i\right) + 2^{(r-2)b}\left(\sum_{1\leq j_1<j_2\leq r} s_{j_1}^i s_{j_2}^i\right) - \\ &\quad 2^{(r-3)b}\left(\sum_{1\leq j_1<j_2<j_3\leq r} s_{j_1}^i s_{j_2}^i s_{j_3}^i\right) + \cdots + (-1)^r\left(\sum_{1\leq j_1<\cdots<j_r\leq r} s_{j_1}^i \cdots s_{j_r}^i\right), \end{aligned} \tag{3}$$

which yields

$$\begin{aligned}
&\mathbb{E}\left[\left(\Pr_{\mathcal{O}_{\text{real}}}[W^i = (w_2^i, \ldots, w_r^i)|\mathbf{Y}^{i-1}] - \Pr_{\mathcal{O}_{\text{ideal}}}[W^i = (w_2^i, \ldots, w_r^i)|\mathbf{W}^{i-1}]\right)^2\right] \\
&= \mathbb{E}\left[\left(\frac{n^i}{d^i} - \frac{1}{2^{(r-1)b}}\right)^2\right] = \mathbb{E}\left[\left(\frac{2^{(r-1)b}\cdot n^i - d^i}{2^{(r-1)b}\cdot d^i}\right)^2\right] \\
&\leq \left(\frac{4}{3}\right)^{2r} \cdot \frac{1}{2^{(4r-2)b}} \cdot \mathbb{E}\left[\left(2^{(r-1)b}\cdot n^i - d^i\right)^2\right], \qquad (4)
\end{aligned}$$

where we used the assumption of $s_j^i < 2^{b-2}$, for all $j \in [r]$, to upper bound $d^i \geq \left(\frac{3}{4}\cdot 2^b\right)^r$. In the following, we focus on the rightmost term of Equation (4), i.e., the expectation of the squared difference. We observe that the two leftmost terms of $2^{(r-1)b}\cdot n^i$, that we call $\underline{n}^i$ for short,

$$\underline{n}^i = 2^{(r-1)b}\cdot\left(2^b - \sum_{j=1}^{r} s_j^i\right) = 2^{rb} - 2^{(r-1)b}\left(\sum_{j=1}^{r} s_j^i\right),$$

are identical to the two leftmost terms in d^i as in Equation (3) and cancel in the difference. We define

$$\begin{aligned}
\overline{n}^i = n^i - \left(2^b - \sum_{j=1}^{r} s_j^i\right) &= \left(\sum_{1\leq j_1<j_2\leq r} s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right) \\
&- \left(\sum_{1\leq j_1<j_2<j_3\leq r} s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}\right) + \cdots + (-1)^r\left(s_{1,\ldots,r}^{i,w_1,w_2,\ldots,w_r}\right). \qquad (5)
\end{aligned}$$

We define $\overline{d}^i = d^i - \underline{n}^i$. We substitute the extended formulation of d^i from Equation (3) into Equation (5) and factor out $(2^{(r-1)b})^2$:

$$\begin{aligned}
\mathbb{E}\left[\left(2^{(r-1)b}\cdot n^i - d^i\right)^2\right] &= \mathbb{E}\left[2^{2(r-1)b}\cdot\left(n^i - \frac{d^i}{2^{(r-1)b}}\right)^2\right] \\
&= 2^{2(r-1)b}\cdot\mathbb{E}\left[\left(\overline{n}^i - \frac{\overline{d}^i}{2^{(r-1)b}}\right)^2\right]. \qquad (6)
\end{aligned}$$

We can write the rightmost term as

$$\begin{aligned}
\frac{\overline{d}^i}{2^{(r-1)b}} &= \left(\sum_{1\leq j_1<j_2\leq r} \frac{s_{j_1}^i s_{j_2}^i}{2^b}\right) - \left(\sum_{1\leq j_1<j_2<j_3\leq r} \frac{s_{j_1}^i s_{j_2}^i s_{j_3}^i}{2^{2b}}\right) \\
&+ \cdots + (-1)^r\cdot\frac{s_1^i\cdots s_r^i}{2^{(r-1)b}}. \qquad (7)
\end{aligned}$$

From Equation (1) for n^i, we can observe that for the sum of terms x in $\overline{n}^i$, Equation (7) consists of exactly the sum of terms $\mathbb{E}[\mathsf{x}]$.

$$(6) = 2^{(2r-2)b} \cdot \mathbb{E}\left[\left(\overline{n}^i - \mathbb{E}\left[\overline{n}^i\right]\right)^2\right] = 2^{(2r-2)b} \cdot \mathbf{Var}[\overline{n}^i]\,.$$

Inserting it into Equation (4) yields

$$\left(\frac{4}{3}\right)^{2r} \cdot \frac{1}{2^{(4r-2)b}} \cdot \mathbb{E}\left[\left(2^{(r-1)b} \cdot n^i - d^i\right)^2\right] \leq \left(\frac{4}{3}\right)^{2r} \cdot \frac{1}{2^{2rb}} \cdot \mathbf{Var}[\overline{n}^i]\,.$$

For the sum of random variables x_i, it holds that

$$\mathbf{Var}[\overline{n}^i] = \sum_i \sum_j \mathbf{Cov}[\mathsf{x}_i, \mathsf{x}_j] = c^i\,,$$

where c^i is the sum of the pairwise covariances of all combinations of two addends in $\mathbf{Var}[\overline{n}^i]$, which includes the (always positive) variance terms:

$$\begin{aligned}
c^i = \Bigg[& \left(\sum_{1 \leq j_1 < j_2 \leq r} \sum_{1 \leq j'_1 < j'_2 \leq r} \mathbf{Cov}[s^{i,w_{j_1},w_{j_2}}_{j_1,j_2}, s^{i,w_{j'_1},w_{j'_2}}_{j'_1,j'_2}] \right) \\
& - \left(\sum_{1 \leq j_1 < j_2 \leq r} \sum_{1 \leq j'_1 < j'_2 < j'_3 \leq r} \mathbf{Cov}[s^{i,w_{j_1},w_{j_2}}_{j_1,j_2}, s^{i,w_{j'_1},w_{j'_2},w_{j'_3}}_{j'_1,j'_2,j'_3}] \right) + \cdots \\
& + (-1)^r \left(\sum_{j_1,j_2} \sum_{j'_1,\ldots j'_r} \mathbf{Cov}[s^{i,w_{j_1},w_{j_2}}_{j_1,j_2}, s^{i,w_{j'_1},w_{j'_2},\ldots,w_{j'_r}}_{j'_1,\ldots,j'_r}] \right) \Bigg] \\
& - \Bigg[\left(\sum_{1 \leq j_1 < j_2 < j_3 \leq r} \sum_{1 \leq j'_1 < j'_2 < j'_3 \leq r} \mathbf{Cov}[s^{i,w_{j_1},w_{j_2},w_{j_3}}_{j_1,j_2,j_3}, s^{i,w_{j'_1},w_{j'_2},w_{j'_3}}_{j'_1,j'_2,j'_3}] \right) - \cdots \\
& + (-1)^r \left(\sum_{j_1,j_2,j_3} \sum_{j'_1,\ldots j'_r} \mathbf{Cov}[s^{i,w_{j_1},w_{j_2},w_{j_3}}_{j_1,j_2,j_3}, s^{i,w_{j'_1},w_{j'_2},\ldots,w_{j'_r}}_{j'_1,\ldots,j'_r}] \right) \Bigg] + \cdots\,.
\end{aligned}$$

Covariance. Recall that the covariance of a term with itself equals its variance and is always positive: $\mathbf{Cov}[\mathsf{x}_i, \mathsf{x}_i] = \mathbf{Var}[\mathsf{x}_i]$. Thus, we need to compute the covariance for all pairs of different variables. From the definition of the covariance,

$$\mathbf{Cov}[\mathsf{x}_i, \mathsf{x}_j] = \mathbb{E}[\mathsf{x}_i \cdot \mathsf{x}_j] - \mathbb{E}[\mathsf{x}_i] \cdot \mathbb{E}[\mathsf{x}_j]\,, \tag{8}$$

we can compute the products of expectations, but have to find the expectations of the products $\mathbb{E}[\mathsf{x}_i \cdot \mathsf{x}_j]$, with dependent variables x_i and x_j.
Lemma 4 considers the expectation of products. We use $\mathcal{I}, \mathcal{J} \subseteq \{j_1, \ldots, j_r\}$ as distinct index sets and overload the notations so that for each set $\mathcal{I} = \{j'_1, \ldots, j'_t\} \subseteq \{j_1, \ldots, j_r\}$, we define $s^i_{\mathcal{I}} = s^i_{j'_1,\ldots,j'_t}$. Moreover, we define $p_{\mathcal{I}} = \prod_{j \in \mathcal{I}} p_j$. Note that

$$\mathbb{E}[s^i_{\mathcal{I}}] \cdot \mathbb{E}[s^i_{\mathcal{J}}] = np_{\mathcal{I}} \cdot np_{\mathcal{J}}, \quad \mathbb{E}[s^i_{\mathcal{I}} \cdot s^i_{\mathcal{J}}] = \mathbb{E}[s^i_{\mathcal{I}}] \cdot \mathbb{E}[s^i_{\mathcal{J}}] + \mathbf{Cov}[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}]\,.$$

If $\mathcal{I} \cap \mathcal{J} = \emptyset$, it follows that $p_{\mathcal{I}\cup\mathcal{J}} = p_{\mathcal{I}} \cdot p_{\mathcal{J}}$; thus, $\mathbf{Cov}[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}] = 0$ and

$$\mathbb{E}[s^i_{\mathcal{I}} \cdot s^i_{\mathcal{J}}] = \mathbb{E}[s^i_{\mathcal{I}}] \cdot \mathbb{E}[s^i_{\mathcal{J}}]\,.$$

Though, for the cases when $\mathcal{I} \cap \mathcal{J} \neq \emptyset$, we have to find $\mathbf{Cov}[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}]$ in Lemma 4. We defer its proof to Appendix A.4.

Lemma 4. It holds that $\mathbf{Cov}\left[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}\right] = np_{\mathcal{I}\cup\mathcal{J}} - np_{\mathcal{I}} \cdot p_{\mathcal{J}}$.

We show that we are allowed to apply Lemma 4. Since the permutations are independent from each other and the values are sampled independently at random, we can say that each value in $\mathcal{S}_u$, $\mathcal{S}_v$, $\mathcal{S}_w$ is chosen independently from the others. The size of all three lists is $n = 2^b$; moreover, we can instantiate the probabilities p_j, for $j \in [r]$ as $p_j = \frac{s^i_j}{2^b}$. In our case, this means

$$\mathbb{E}\left[s^i_{\mathcal{I}} \cdot s^i_{\mathcal{J}}\right] = 2^{2b} \cdot \prod_{i\in\mathcal{I}} p_j \cdot \prod_{j\in\mathcal{J}} p_j + \mathbf{Cov}\left[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}\right]\,, \quad \text{where}$$
$$\mathbf{Cov}\left[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}\right] = 2^b \cdot \prod_{i\in\mathcal{I}\cup\mathcal{J}} p_i - 2^b \cdot \prod_{i\in\mathcal{I}} p_i \cdot \prod_{j\in\mathcal{J}} p_j\,.$$

For example, let $\mathcal{I} = \{1, 2\}$ and $\mathcal{J} = \{1, 3, 4\}$. Then,

$$\mathbf{Cov}\left[s^i_{1,2}, s^i_{1,3,4}\right] = 2^b \cdot \left(\frac{s^i_1 s^i_2 s^i_3 s^i_4}{2^{4b}} - \frac{(s^i_1)^2 s^i_2 s^i_3 s^i_4}{2^{5b}}\right)\,.$$

Decomposing c^i. Given the covariance, we can rewrite c^i. We define $\mathcal{C}_{t,r}$ for the set of t-out-of-r element combinations, e.g. $\mathcal{C}_{2,3} = \{(1,2), (1,3), (2,3)\}$.

$$c^i = \sum_{t_1=2}^{r}\sum_{t_2=2}^{r}(-1)^{t_1+t_2} \cdot c^i_{t_1,t_2,r}, \text{ where } c^i_{t_1,t_2,r} = \sum_{\mathcal{I}\in\mathcal{C}_{t_1,r}}\sum_{\mathcal{J}\in\mathcal{C}_{t_2,r}} \mathbf{Cov}[s^{i,w_{\mathcal{I}}}_{\mathcal{I}}, s^{i,w_{\mathcal{J}}}_{\mathcal{J}}]\,. \tag{9}$$

Lemma 4 yields

$$c^i_{t_1,t_2,r} = \sum_{\mathcal{I}\in\mathcal{C}_{t_1,r}}\sum_{\mathcal{J}\in\mathcal{C}_{t_2,r}} 2^b \cdot (p_{\mathcal{I}\cup\mathcal{J}} - p_{\mathcal{I}}p_{\mathcal{J}}) \tag{10}$$
$$= 2^b \cdot \underbrace{\left(\sum_{\mathcal{I}\in\mathcal{C}_{t_1,r}}\sum_{\mathcal{J}\in\mathcal{C}_{t_2,r}}\prod_{j\in\mathcal{I}\cup\mathcal{J}} p_j\right)}_{\overline{c}^i_{t_1,t_2,r}} - 2^b \cdot \underbrace{\left(\sum_{\mathcal{I}\in\mathcal{C}_{t_1,r}}\sum_{\mathcal{J}\in\mathcal{C}_{t_2,r}}\prod_{i\in\mathcal{I}} p_i \prod_{j\in\mathcal{J}} p_j\right)}_{\underline{c}^i_{t_1,t_2,r}}\,. \tag{11}$$

Later, we will consider the case that $p_1 = p_2 = \cdots = p_r = p$. Then, we can write $c^i_{t_1,t_2,r}$ as

$$2^b \cdot \left(\overline{c}^i_{t_1,t_2,r} - \underline{c}^i_{t_1,t_2,r}\right) = 2^b \cdot \left(\sum_{j=0}^{u}\left(\overline{k}^i_{t_1,t_2,r,j} \cdot p^{\overline{\ell}^i_{t_1,t_2,r,j}}\right) - \underline{k}^i_{t_1,t_2,r} \cdot p^{\underline{\ell}^i_{t_1,t_2,r}}\right)$$

with $u =^{\text{def}} \min(r - t_2, t_1)$ and j denotes the number of elements in $\mathcal{I}$ that are not contained in $\mathcal{J}$. Thus, we can reduce the task to that of finding the multiples

$$\overline{k}^i_{t_1,t_2,r,j} = |\{(\mathcal{I},\mathcal{J}) \in \mathcal{C}_{t_1,r}, \times\mathcal{C}_{t_2,r} : |\mathcal{I} \cup \mathcal{J}| = t_2 + j\}| \quad \text{and} \quad \overline{\ell}^i_{t_1,t_2,r,j} = |\mathcal{I} \cup \mathcal{J}|\,. \tag{12}$$

and

$$\underline{k}^i_{t_1,t_2,r} = |\{(\mathcal{I},\mathcal{J}) \in \mathcal{C}_{t_1,r}, \times\mathcal{C}_{t_2,r}\}| = |\mathcal{C}_{t_1,r}| \cdot |\mathcal{C}_{t_2,r}| = \binom{r}{t_1} \cdot \binom{r}{t_2} \quad \text{and} \tag{13}$$

$$\underline{\ell}^i_{t_1,t_2,r} = |\mathcal{I}| + |\mathcal{J}| = t_1 + t_2\,. \tag{14}$$

The exponent $\overline{\ell}^i_{t_1,t_2,r,j}$ is derived from the size of the union set $\mathcal{I} \cup \mathcal{J}$ when j elements of $\mathcal{I}$ are not in $\mathcal{J}$. Thus $\overline{\ell}^i_{t_1,t_2,r,j} = \max(t_1,t_2) + j$ for all $j \in [0..u]$ where $u =^{\text{def}} \min(r - t_2, t_1)$. It remains to determine $\overline{k}^i_{t_1,t_2,r,j}$. For this purpose, we can use the simple combinatorial Lemma 5.

Lemma 5. Let t_1, t_2, r, j be fixed integers with $t_1 \le t_2 \le r$ and $j \in [t_2..r]$. Let $\mathcal{I}, \mathcal{J} \subseteq [r]$ be non-identical subsets of $[r]$ with $|\mathcal{I}| = t_1$ and $|\mathcal{J}| = t_2$. Then, the number of combinations of distributing $\mathcal{I}$ and $\mathcal{J}$ so that

$$|\{(\mathcal{I},\mathcal{J}) \in \mathcal{C}_{t_1,r}, \times\mathcal{C}_{t_2,r} : |\mathcal{I} \cup \mathcal{J}| = t_2 + j\}| = \binom{r}{t_2} \cdot \binom{t_2}{t_1 - j} \cdot \binom{r - t_2}{j}\,.$$

Proof. W.l.o.g., we had fixed that $|\mathcal{I}| \le |\mathcal{J}|$ and therefore $t_1 \le t_2$. There are $\binom{r}{t_2}$ sets $\mathcal{J}$ among r elements. We defined that j elements of $\mathcal{I}$ are not in $\mathcal{J}$. For a fixed $\mathcal{J}$ and fixed j, there are $\binom{t_2}{t_1-j}$ combinations of the $t_1 - j$ values in $\mathcal{I} \cap \mathcal{J}$ and $\binom{r-t_2}{j}$ combinations of distributing j values from $\mathcal{I} \setminus \mathcal{J}$ outside of $\mathcal{J}$. □

We can rewrite Lemma 5 as Lemma 6, which will serve useful.

Lemma 6. Let t_1, t_2, r, ℓ be fixed integers with $t_1, t_2 \le r$. Let $\mathcal{I}, \mathcal{J} \subseteq [r]$ such that $|\mathcal{I}| = t_1$, $|\mathcal{J}| = t_2$, and $j = \ell - t_1$. Then, the number of combinations of distributing $\mathcal{I}$ and $\mathcal{J}$ so that $|\mathcal{I} \cup \mathcal{J}| = \ell$ is

$$|\{(\mathcal{I},\mathcal{J}) \in \mathcal{C}_{t_1,r}, \times\mathcal{C}_{t_2,r} : |\mathcal{I} \cup \mathcal{J}| = \ell\}| = \binom{r}{t_1}\binom{t_1}{t_1 + t_2 - \ell}\binom{r - t_1}{\ell - t_1}(-1)^{t_1+t_2}\,.$$

Proof. There are $\binom{r}{t_1}$ sets $\mathcal{I}$ among r elements. The overlap, i.e., the number of shared elements in the intersection $|\mathcal{I} \cap \mathcal{J}| = t_1 + t_2 - \ell$. Among the t_1 elements of $\mathcal{I}$, there are $\binom{t_1}{t_1+t_2-\ell}$ combinations what elements of $\mathcal{I}$ and $\mathcal{J}$ could be in the intersection. Then, the remaining $\ell - t_1$ elements in $\mathcal{J} \setminus \mathcal{I}$ can be distributed by $\binom{r-t_1}{\ell-t_1}$ combinations over the remaining $r - t_1$ elements not in $\mathcal{I}$. □

Upper Bounding c^i for General r. We aim at having a simplified upper bound for c^i for general r. The terms in c^i consist of multiples of powers of p from exponents 2 to $2r$. Now, we can find non-negative integer coefficients k^i_j, for all $j \in [2..r]$, so that

$$c^i = k^i_2 \cdot p^2 + k^i_3 \cdot p^3 + \sum_{j=2}^{r} \left(k^i_{2j} \cdot p^{2j}\right) . \tag{15}$$

We show that there the indices $j \in [2..2r]$ are the only potential positive coefficients k^i_j. For $k^i_\ell \cdot p^\ell$ with $k_\ell < 2$, there must exist $\overline{\ell}^i_{t_1,t_2,r,j} < 2$ or $\underline{\ell}^i_{t_1,t_2,r} < 2$ for some $t_1, t_2 \in [2..r]$ and $j \leq r$. Though, our sets always have $|\mathcal{I}|, |\mathcal{J}| \in [2..r]$. Hence,

$$\begin{aligned} \overline{\ell}^i_{t_1,t_2,r,j} = |\mathcal{I} \cup \mathcal{J}| \implies \overline{\ell}^i_{t_1,t_2,r,j} \in [2..2r] \quad \text{and} \\ \underline{\ell}^i_{t_1,t_2,r} = |\mathcal{I}| + |\mathcal{J}| \implies \underline{\ell}^i_{t_1,t_2,r} \in [4..2r] . \end{aligned}$$

Thus, $k^i_\ell = 0$ for all $\ell \notin [2..2r]$. We want to reduce the bound to the terms with the few lowest exponents and show that we can upper bound the tail. In particular, we want a bound so that we can reduce Equation (15) to

$$c^i \leq 2^b \cdot (k^i_2 \cdot p^2 + k^i_3 \cdot p^3) .$$

We show the following lemma. Later, we also show that $p \leq 1/3r$ always holds.

Lemma 7. Let $r \geq 2$ be integer. For all even $\ell = 2j$ for some $j \in [2..r-1]$,

$$\frac{|k^i_{\ell+1}|}{|k^i_\ell|} \leq 3r , \quad k^i_{\ell+1} \geq 0 , \quad k^i_\ell \leq 0 \quad \text{and} \quad k^i_{2r} \leq 0 .$$

We defer the proof of Lemma 7 to Appendix A.5. Combined with our assumption that $p \leq 1/3r$, it follows for all $\ell = 2j$ for some $j \in [2..r-1]$, that

$$k^i_{\ell+1} \cdot p^{\ell+1} \leq \left(3r \cdot k^i_\ell\right) \cdot \left(p^\ell \cdot \frac{1}{3r}\right) = k^i_\ell \cdot p^\ell ,$$

and therefore

$$c^i = 2^b \cdot (k^i_2 p^2 + k^i_3 p^3 + \sum_{j=2}^{r-1} \underbrace{\left(-k^i_{2j} p^{2j} + k^i_{2j+1} p^{2j+1}\right)}_{\leq 0} - k^i_{2r} p^{2r}) \leq 2^b \cdot (k^i_2 p^2 + k^i_3 p^3) .$$

The factors k^i_2 and k^i_3 result from only few terms in c^i. In particular, they stem from $c^i_{2,2,r}$, $c^i_{2,3,r} = c^i_{3,2,r}$, and $c^i_{3,3,r}$. Given $r \geq 3$, they result from

$$\begin{aligned} k^i_2 &= \overline{k}^i_{2,2,r,0} = \binom{r}{2}\binom{2}{2}\binom{2}{0} = \binom{r}{2} \\ k^i_3 &= \overline{k}^i_{2,2,r,1} - \overline{k}^i_{2,3,r,0} - \overline{k}^i_{3,2,r,0} + \overline{k}^i_{3,3,r,0} = \binom{r}{3} . \end{aligned}$$

Note that the statement also holds for $r = 2$, where $k_2^i = 1$, $k_4^i = 1$, and $k_j^i = 0$ for all positive integers $j \notin \{2, 4\}$. We obtain

$$c^i \leq 2^b \cdot \left(\binom{r}{2} \cdot p^2 + \binom{r}{3} \cdot p^3 \right) . \tag{16}$$

Equal Probabilities p_i. It remains to show that $p_1 = \cdots = p_r$. The values of the a most significant bits of the permutation outputs, $\mathbf{V}_j^i = V_j^1, \ldots, V_j^i$, for all $j \in [r]$, are sampled uniformly and independently at random, also in the modified real world $\mathcal{O}_{\text{real}}$ since we replace their sampling with that from a truncated permutation. Thus, every V_j^i has probability 2^{-a} to be equal to a specific a-bit value. Therefore

$$\mathbb{E}_{\mathbf{V}^{i-1}}[s_1^i] = \cdots = \mathbb{E}_{\mathbf{V}^{i-1}}[s_r^i] = \frac{i-1}{2^a} .$$

Thus, for all $j \in [r]$, we can use

$$p_j = \mathbb{E}\left[\frac{s_j^i}{2^b}\right] = \frac{\mathbb{E}[s_j^i]}{2^b} = \frac{i-1}{2^n} .$$

We have to show that the expectations of the quantities $s_1^i, \ldots, s_r^i$ are independent. We can adopt the argument from [9] here: it holds since they stem from pairwise independent permutations and hence

$$\mathbb{E}_{\mathbf{V}^{i-1}}[s_2^i | s_1^i] = \mathbb{E}_{\mathbf{V}^{i-1}}[s_2^i]$$

and similar statements can be derived for all other combinations. We can use

$$\mathbb{E}_{\mathbf{V}^{i-1}}[s_1^i s_2^i] = \mathbb{E}_{\mathbf{V}^{i-1}}[s_1^i] \cdot \mathbb{E}_{\mathbf{V}^{i-1}}[s_2^i]$$

and the other product combinations can be decomposed similarly.

Finalizing with the χ^2 Approach. We have that

$$\mathbb{E}\left[\left(\Pr_{\mathcal{O}_{\text{real}}}[W^i = W | \mathbf{W}^{i-1}] - \Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W | \mathbf{W}^{i-1}] \right)^2 \right] \leq \left(\frac{4}{3}\right)^{2r} \cdot \frac{1}{2^{2rb}} \cdot \mathbf{Var}[\overline{n}^i] .$$

Using the χ^2 approach and inserting $\Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W|\mathbf{W}^{i-1}] = 2^{-(r-1)b}$, we obtain

$$
\begin{aligned}
&\left(|\Pr[\mathcal{O}_{\text{real}} = \tau] - \Pr[\mathcal{O}_{\text{ideal}} = \tau]|\right)^2 \\
&\leq \frac{1}{2}\sum_{i=1}^{q} \mathbb{E}_{\mathcal{O}_{\text{real}}}[\chi^2(\mathbf{W}^{i-1})] \\
&\leq \frac{1}{2}\sum_{i=1}^{q} \sum_{W\in(\mathbb{F}_2^b)^{r-1}} \mathbb{E}_{\mathcal{O}_{\text{real}}}\left[\frac{\left(\Pr_{\mathcal{O}_{\text{real}}}[W^i = W|\mathbf{W}^{i-1}] - \Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W|\mathbf{W}^{i-1}]\right)^2}{\Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W|\mathbf{W}^{i-1}]}\right] \\
&\leq \frac{1}{2}\cdot 2^{(r-1)b}\cdot\sum_{i=1}^{q} \sum_{W\in(\mathbb{F}_2^b)^{r-1}} \mathbb{E}\left[\left(\Pr_{\mathcal{O}_{\text{real}}}[W^i = W|\mathbf{W}^{i-1}] - \Pr_{\mathcal{O}_{\text{ideal}}}[W^i = W|\mathbf{W}^{i-1}]\right)^2\right] \\
&\leq \frac{1}{2}\cdot 2^{(r-1)b}\cdot\sum_{i=1}^{q} \sum_{W\in(\mathbb{F}_2^b)^{r-1}} \left(\left(\frac{4}{3}\right)^{2r}\cdot\frac{1}{2^{2rb}}\cdot c^i\right) \\
&\leq \frac{1}{2^{2b+1}}\cdot\left(\frac{4}{3}\right)^{2r}\cdot\sum_{i=1}^{q} c^i\,. \qquad (17)
\end{aligned}
$$

From Equation (16)

$$c^i \leq 2^b\left(\binom{r}{2}p^2 + \binom{r}{3}p^3\right)$$

and $p = (i-1)/2^n$, we obtain that

$$
\begin{aligned}
(17) &= \sqrt{\frac{1}{2^{2b+1}}\cdot\left(\frac{4}{3}\right)^{2r}\cdot\sum_{i=1}^{q} 2^b\cdot\left(\binom{r}{2}\frac{(i-1)^2}{2^{2n}} + \binom{r}{3}\frac{(i-1)^3}{2^{3n}}\right)} \\
&= \sqrt{\frac{1}{2^{2b+1}}\cdot\left(\frac{4}{3}\right)^{2r}\cdot\frac{1}{2^a}\cdot\sum_{i=1}^{q}\left(\binom{r}{2}\frac{(i-1)^2}{2^n} + \binom{r}{3}\frac{(i-1)^3}{2^{3n}}\right)} \\
&\leq \sqrt{\frac{1}{2^{2n-a}}\cdot\left(\frac{4}{3}\right)^{2r}\cdot\frac{1}{2}\cdot\left(\frac{r^2q^3}{2^n} + \frac{r^3q^4}{2^{2n}}\right)} \\
&\leq \left(\frac{4}{3}\right)^{r}\cdot\frac{1}{2}\cdot\sqrt{\frac{r^2q^3}{2^{3n-a}} + \frac{r^3q^4}{2^{4n-a}}} \\
&\leq \left(\frac{4}{3}\right)^{r}\cdot\left(\frac{rq}{2^{n-a/3}}\right)^{3/2},
\end{aligned}
$$

where we used $q \leq 2^n/3r$ to upper bound

$$\frac{r^2q^3}{2^{3n-a}} + \frac{r^3q^4}{2^{4n-a}} \leq \frac{2r^3q^3}{2^{3n-a}}\,.$$

This yields the bound in Theorem 3. □

We can obtain tighter constant factors for concrete values of r. We give the results for $r = 3, 4$ in Corollary 2 to aid the reader.

Corollary 2. Let a, b, q be positive integers and $\tau = (\mathbf{V}, \mathbf{W})$ be a good transcript such that $C_{\mathbf{V},j}(i) < 2^{b-2}$ holds for all $i \in [q]$ and $j \in [r]$ and $q \leq 2^n/9$. Then, it holds

$$\mathbb{E}_\tau[\Pr[\mathcal{O}_2 = \tau] - \Pr[\mathcal{O}_{\text{ideal}} = \tau]] \leq \begin{cases} 4 \cdot \left(\frac{q}{2^{n-a/3}}\right)^{3/2} & \text{for } r = 3 \\ 8 \cdot \left(\frac{q}{2^{n-a/3}}\right)^{3/2} & \text{for } r = 4\,. \end{cases}$$

6 Conclusion

We have shown that XTH, the XORP-like extension of STH achieves a level of $O(n - a/2 - 1.5\log(r))$-bit PRF security. This is similar to the logarithmic loss in r of XORP compared to the sum of permutations, providing a trade-off between releasing more bits from each permutation call and from summation. Note that this work has considered the version with independent permutations. Future work can investigate variants that feed domain-separated inputs into the same permutation.

References

1. M. Bellare and R. Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to prp to prf conversion. Cryptology ePrint Archive, Report 1999/024, 1999. http://eprint.iacr.org/1999/024.
2. Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In Kaisa Nyberg, editor, *EUROCRYPT*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.
3. Srimanta Bhattacharya and Mridul Nandi. Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the \chi ˆ2 Method. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT I*, volume 10820 of *LNCS*, pages 387–412. Springer, 2018.
4. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017. Full version at http://eprint.iacr.org/2017/537, version 20170616:190106.
5. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. *IACR Trans. Symmetric Cryptol.*, 2018(3):36–92, 2018.
6. Itai Dinur. Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis. In Marc Joye and Gregor Leander, editors, *EUROCRYPT I*, volume 14651 of *Lecture Notes in Computer Science*, pages 33–62. Springer, 2024.
7. Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of mirror theory for $\xi_{\max} = 2$. *IEEE Trans. Inf. Theory*, 68(9):6218–6232, 2022.

8. Shoni Gilboa and Shay Gueron. The advantage of truncated permutations. *Discret. Appl. Math.*, 294:214–223, 2021.
9. Aldo Gunsing and Bart Mennink. The Summation-Truncation Hybrid: Reusing Discarded Bits for Free. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO I*, volume 12170 of *LNCS*, pages 187–217. Springer, 2020.
10. Chris Hall, David A. Wagner, John Kelsey, and Bruce Schneier. Building prfs from prps. In *CRYPTO 1998, Proceedings*, pages 370–389, 1998.
11. Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *LNCS*, pages 310–327. Springer, 2006.
12. Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is Optimally Secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.
13. Tetsu Iwata and Kazuhiko Minematsu. Stronger Security Variants of GCM-SIV. *IACR Transactions on Symmetric Cryptology*, 2016(1):134–157, 2016.
14. Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. The Deoxys AEAD Family. *J. Cryptol.*, 34(3):31, 2021.
15. Stefan Lucks. The Sum of PRPs Is a Secure PRF. In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *LNCS*, pages 470–484. Springer, 2000.
16. Yusuke Naito. Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT III*, volume 10626 of *Lecture Notes in Computer Science*, pages 446–470. Springer, 2017.
17. Kan Yasuda. A New Variant of PMAC: Beyond the Birthday Bound. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *LNCS*, pages 596–609. Springer, 2011.
18. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *LNCS*, pages 296–312. Springer, 2012.

A Proof of the Leftover Lemmas for Theorem 3

A.1 Proof of Lemma 1

Lemma 1. For distinct $j_1, j_2 \in [r]$, it holds that

$$\mathbb{E}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] = \frac{s_{j_1}^i s_{j_2}^i}{2^b} \quad \text{and} \quad \mathbf{Var}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] = \frac{s_{j_1}^i s_{j_2}^i}{2^b} - \frac{(s_{j_1}^i s_{j_2}^i)^2}{2^{3b}}\,.$$

Proof. Let us focus on $s_{1,2}^{i,w_1,w_2}$; the remaining 2-tuple-related terms $s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}$ behave similarly, for all $j_1 \neq j_2$, $j_1, j_2 \in [r]$. Given fixed $w_2 \in \mathbb{F}_2^b$, for each $y_1 \in \mathbb{F}_2^b$, we define Bernoulli variables I_{y_1} as

$$I_{y_1} \triangleq \begin{cases} 1 & y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \\ 0 & \text{otherwise.} \end{cases}$$

Then, we derive

$$\mathbb{E}\left[s_{1,2}^{i,w_1,w_2}\right] = \sum_{y_1 \in \mathbb{F}_2^b} \Pr[I_{y_1}]\,.$$

To obtain

$$\mathbf{Var}\left[\mathsf{x}\right] = \mathbb{E}\left[\mathsf{x}^2\right] - \left(\mathbb{E}[\mathsf{x}]\right)^2 ,$$

we have to determine $\mathbb{E}\left[\mathsf{x}^2\right]$. For a sum of n independent Bernoulli variables I_{y_1}, with $\Pr[I_{y_1} = 1] = p$ for all y_1,

$$\mathsf{x} = \sum_{y_1} \Pr[I_{y_1} = 1] ,$$

it holds that

$$\mathbb{E}\left[\mathsf{x}^2\right] = \mathbb{E}\left[\left(\sum_{j=1}^{n} I_j\right)^2\right] = n(n-1)p^2 + np .$$

In our case, $n = 2^b$ and $p = s_1^i s_2^i \cdot 2^{-2b}$, for all $y_1 \in \mathbb{F}_2^b$. Given that $\left(\mathbb{E}[\mathsf{x}]\right)^2 = (2^b p)^2$, we obtain

$$\begin{aligned} \mathbf{Var}\left[s_{1,2}^{i,0,w_2}\right] &\leq \frac{s_1^i s_2^i}{2^b} - \frac{(s_1^i s_2^i)^2}{2^{3b}} \quad \text{and in general} \\ \mathbf{Var}\left[s_{j_1,j_2}^{i,w_{j_1},w_{j_2}}\right] &\leq \frac{s_{j_1}^i s_{j_2}^i}{2^b} - \frac{(s_{j_1}^i s_{j_2}^i)^2}{2^{3b}} . \end{aligned}$$

A.2 Proof of Lemma 2

Lemma 2. For distinct $j_1, j_2, j_3 \in [r]$, it holds that

$$\mathbb{E}\left[s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}\right] = \frac{s_{j_1}^i s_{j_2}^i s_{j_3}^i}{2^{2b}}, \quad \mathbf{Var}\left[s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}\right] = \frac{s_{j_1}^i s_{j_2}^i s_{j_3}^i}{2^{2b}} - \frac{(s_{j_1}^i s_{j_2}^i s_{j_3}^i)^2}{2^{5b}} .$$

Proof. Again, the remaining 3-tuple-related terms $s_{j_1,j_2,j_3}^{i,w_{j_1},w_{j_2},w_{j_3}}$ behave similarly, for all distinct $j_1, j_2, j_3 \in [r]$. Given fixed $w_1 = 0^b$ and $w_2, w_3 \in \mathbb{F}_2^b$, for each $y_1 \in \mathbb{F}_2^b$, we define Bernoulli variables I_{y_1} as

$$I_{y_1} \triangleq \begin{cases} 1 & y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_3 \in \mathcal{S}_3^i \\ 0 & \text{otherwise.} \end{cases}$$

Then, it holds that

$$\mathbb{E}\left[s_{1,2,3}^{i,w_1,w_2,w_3}\right] = \mathbb{E}\left[\sum_{y_1 \in \mathbb{F}_2^b} I_{y_1}\right] = \sum_{y_1 \in \mathbb{F}_2^b} \mathbb{E}[I_{y_1}] .$$

Since the expectations for a fixed value $y_1 \in \mathbb{F}_2^b$ and its translations to be in the list of all three permutations are mutually independent, the probability is 2^{-3b}.

Over all elements of the sets $|\mathcal{S}^i_{y_1 \to w_1}| = |\mathcal{S}^i_1|$, $|\mathcal{S}^i_{y_2 \to w_2}|$, and $|\mathcal{S}^i_{y_3 \to w_3}|$, it holds that

$$\mathbb{E}[I_{y_1}] = \frac{s^i_1 s^i_2 s^i_3}{2^{3b}} \quad \text{and therefore} \quad \mathbb{E}\left[s^{i,w_1,w_2,w_3}_{y_1,y_2,y_3}\right] = \frac{s^i_1 s^i_2 s^i_3}{2^{2b}}\,. \tag{18}$$

It remains to determine its variance

$$\begin{aligned}\mathbf{Var}\left[s^{i,w_1,w_2,w_3}_{y_1,y_2,y_3}\right] &= \mathbb{E}\left[\left(s^{i,w_1,w_2,w_3}_{y_1,y_2,y_3}\right)^2\right] - \left(\mathbb{E}\left[s^{i,w_1,w_2,w_3}_{y_1,y_2,y_3}\right]\right)^2 \\ &= \mathbf{Var}\left[\sum_{y_1 \in \mathbb{F}_2^b} I_{y_1}\right] = \sum_{y_1 \in \mathbb{F}_2^b} \mathbf{Var}\left[I_{y_1}\right] + \sum_{y_1 \neq y_1'} \mathbf{Cov}\left[I_{y_1}, I_{y_1'}\right]\,,\end{aligned}$$

with the covariance

$$\begin{aligned}\mathbf{Cov}\left[I_{y_1}, I_{y_1'}\right] &= \mathbb{E}\left[I_{y_1} \cdot I_{y_1'}\right] - \mathbb{E}[I_{y_1}]\,\mathbb{E}\left[I_{y_1'}\right] \\ &= \mathbb{E}[I_{y_1}] \cdot \Pr[I_{y_1'} = 1 | I_{y_1} = 1] - \mathbb{E}[I_{y_1}]\,\mathbb{E}\left[I_{y_1'}\right]\,.\end{aligned}$$

For the variance of the Bernoulli variables, it holds that

$$\mathbf{Var}\left[I_{y_1}\right] = \mathbb{E}\left[(I_{y_1})^2\right] - (\mathbb{E}[I_{y_1}])^2 = \mathbb{E}[I_{y_1}] - (\mathbb{E}[I_{y_1}])^2 = \frac{s^i_u s^i_v s^i_w}{2^{3b}} - \left(\frac{s^i_u s^i_v s^i_w}{2^{3b}}\right)^2\,.$$

For their covariance, we need to determine the conditional probability. We consider the case that $y_1' \notin \{y_1 \oplus w_2, y_1 \oplus w_3\}$. Since $y_1' \neq y_1$, it holds that all values differ mutually

$$\begin{aligned}\Pr[I_{y_1'} = 1 | I_{y_1} = 1] &= \Pr[(y_1' \in \mathcal{S}^i_1) \wedge (y_1' \oplus w_2 \in \mathcal{S}^i_2) \wedge (y_1' \oplus w_3 \in \mathcal{S}^i_3) | \\ &\qquad (y_1 \in \mathcal{S}^i_1) \wedge (y_1 \oplus w_2 \in \mathcal{S}^i_2) \wedge (y_1 \oplus w_3 \in \mathcal{S}^i_3)] \\ &\leq \frac{(s^i_1 - 1)(s^i_2 - 1)(s^i_3 - 1)}{(2^b - 1)^3}\,.\end{aligned}$$

We conduct it for $y_1' = y_1 \oplus w_2$ exemplarily. From the requirement of the covariance that $y_1' \neq y_1$, we must exclude $w_2 = 0$.

$$\begin{aligned}&\Pr[I_{y_1 \oplus w_2} = 1 | I_{y_1} = 1] \\ &\leq \Pr[(y_1 \oplus w_2 \in \mathcal{S}^i_1) \wedge (y_1 \in \mathcal{S}^i_2) \wedge (y_1 \oplus w_2 \oplus w_3 \in \mathcal{S}^i_3) | I_{y_1} = 1] \\ &\leq \frac{(s^i_u - 1)(s^i_v - 1)(s^i_w - 1)}{(2^b - 1)^3}\,.\end{aligned}$$

From $s^i_1, s^i_2, s^i_3 < 2^b$, it follows that

$$\Pr[I_{y_1 \oplus w_2} = 1 | I_{y_1} = 1] \leq \mathbb{E}[I_{y_1 \oplus w_2}]\,,$$

and therefore $\mathbf{Cov}\left[I_{y_1}, I_{y_1 \oplus w_2}\right] \leq 0$ in this case. A similar argument holds for $y_1' = y_1 \oplus w_3$, $w_2 \neq w_3$. It remains to consider $y_1' = y_1 \oplus w_2$ with $w_2 = w_3$.

$$\begin{aligned}&\Pr[I_{y_1 \oplus w_2} = 1 | I_{y_1} = 1, w_2 = w_3] \\ &\leq \Pr[(y_1 \oplus w_2 \in \mathcal{S}^i_1) \wedge (y_1 \in \mathcal{S}^i_2) \wedge (y_1 \in \mathcal{S}^i_3) | I_{y_1} = 1] \\ &\leq \frac{(s^i_1 - 1)(s^i_2 - 1)(s^i_3 - 1)}{(2^b - 1)^3}\,.\end{aligned}$$

Again, $s_1^i, s_2^i, s_3^i < 2^b$ implies

$$\Pr[I_{y_1 \oplus w_2} = 1 | I_{y_1} = 1] \leq \mathbb{E}[I_{y_1 + w_2}] \,,$$

and therefore, $\mathbf{Cov}\left[I_{y_1}, I_{y_1 \oplus w_2}\right] \leq 0$. Thus, it holds that $\mathbf{Cov}\left[I_{y_1}, I_{y_1'}\right] \leq 0$ over all cases of y_1', and it follows that

$$\begin{aligned}\mathbf{Var}\left[s_{1,2,3}^{i,w_1,w_2,w_3}\right] &\leq \sum_{y_1 \in \mathbb{F}_2^b} \mathbf{Var}\left[I_{y_1}\right] \\ &= 2^b \cdot \left(\frac{s_1^i s_2^i s_3^i}{2^{3b}} - \left(\frac{s_1^i s_2^i s_3^i}{2^{3b}}\right)^2\right) = \frac{s_1^i s_2^i s_3^i}{2^{2b}} - \frac{(s_1^i s_2^i s_3^i)^2}{2^{5b}} \,.\end{aligned}$$

A.3 Proof of Lemma 3

Lemma 3. Let $t \leq r$ and $\mathcal{I} = \{j_1, \ldots, j_t\} \subseteq \{1, \ldots, r\}$. Then, it holds for the expectation and variance that

$$\mathbb{E}\left[s_{j_1,j_2,\ldots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \frac{\prod_{j \in \mathcal{I}} s_j^i}{2^{(t-1)b}}, \quad \mathbf{Var}\left[s_{j_1,j_2,\ldots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \frac{\prod_{j \in \mathcal{I}} s_j^i}{2^{(t-1)b}} - \frac{\left(\prod_{j \in \mathcal{I}} s_j^i\right)^2}{2^{(2t-1)b}} \,.$$

Proof. Given fixed $w_{j_2}, \ldots w_{j_t} \in \mathbb{F}_2^b$, for each $y_1 \in \mathbb{F}_2^b$, we define Bernoulli variables I_{y_1} as

$$I_{y_1} \triangleq \begin{cases} 1 & y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_{j_2} \in \mathcal{S}_{j_2}^i \wedge \ldots \wedge y_1 \oplus w_{j_t} \in \mathcal{S}_{j_t}^i \\ 0 & \text{otherwise.} \end{cases}$$

Then, it holds that

$$\mathbb{E}\left[s_{j_1,j_2,\cdots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \mathbb{E}\left[\sum_{y_1 \in \mathbb{F}_2^b} I_{y_1}\right] = \sum_{y_1 \in \mathbb{F}_2^b} \mathbb{E}[I_{y_1}] \,.$$

Since the expectations for a fixed value $y_1 \in \mathbb{F}_2^b$ and its translations to be in the list of all three permutations are mutually independent, the probability is 2^{-tb}. Over all elements of the sets, it holds that

$$\mathbb{E}[I_{y_1}] = \frac{\prod_{j \in \mathcal{I}} s_j^i}{2^{tb}} \quad \text{and therefore} \quad \mathbb{E}\left[s_{j_1,j_2,\cdots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] = \frac{\prod_{j \in \mathcal{I}} s_j^i}{2^{(t-1)b}} \,.$$

For $\mathsf{x} = \sum_{y_1} \Pr[I_{y_1} = 1]$, as a sum of n independent Bernoulli variables I_{y_1}, with $\Pr[I_{y_1} = 1] = p$ for all y_1, it holds that

$$\mathbb{E}\left[\mathsf{x}^2\right] = \mathbb{E}\left[\left(\sum_{j=1}^{n} I_j\right)^2\right] = n(n-1)p^2 + np \,.$$

In our case, $n = 2^b$ and $p = \prod_{j\in\mathcal{I}} s_j^i \cdot 2^{-tb}$, for all $y_1 \in \mathbb{F}_2^b$. Given that $(\mathbb{E}[\mathsf{x}])^2 = (2^b p)^2$, we obtain

$$\mathbf{Var}\left[s_{j_1,j_2,\cdots,j_t}^{i,w_{j_1},w_{j_2},\ldots,w_{j_t}}\right] \leq \frac{\prod_{j\in\mathcal{I}} s_j^i}{2^{(t-1)b}} - \frac{\left(\prod_{j\in\mathcal{I}} s_j^i\right)^2}{2^{(2t-1)b}}\,.$$

A.4 Proof of Lemma 4

Lemma 4. It holds that $\mathbf{Cov}\left[s_{\mathcal{I}}^i, s_{\mathcal{J}}^i\right] = np_{\mathcal{I}\cup\mathcal{J}} - np_{\mathcal{I}} \cdot p_{\mathcal{J}}$.

Proof. Let us focus examplarily on $\mathcal{I} = \{1,2,3\}$ and $\mathcal{J} = \{1,2,4\}$. Thus, we consider $s_{1,2,3}^{i,w_1,w_2,w_3}$ and $s_{1,2,4}^{i,w_1,w_2,w_4}$. The remaining tuples behave similarly, for all $\mathcal{I} \neq \mathcal{J}$. Given fixed $w_1 = 0^b$ and $w_2, w_3, w_4 \in \mathbb{F}_2^b$, for each $y_1 \in \mathbb{F}_2^b$, we define Bernoulli variables I_{y_1} as

$$I_{y_1} \triangleq \begin{cases} 1 & y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_3 \in \mathcal{S}_3^i \\ 0 & \text{otherwise} \end{cases}$$

and

$$J_{y_1} \triangleq \begin{cases} 1 & y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_4 \in \mathcal{S}_4^i \\ 0 & \text{otherwise.} \end{cases}$$

Then, we derive

$$\mathbb{E}\left[s_{\mathcal{I}}^{i,w_1,w_2,w_3}\right] = \sum_{y_1\in\mathbb{F}_2^b} \Pr[I_{y_1}]$$
$$\mathbb{E}\left[s_{\mathcal{J}}^{i,w_1,w_2,w_4}\right] = \sum_{y_1\in\mathbb{F}_2^b} \Pr[J_{y_1}]$$

We want to bound

$$\mathbf{Cov}\left[s_{\mathcal{I}}^i, s_{\mathcal{J}}^i\right] = \mathbb{E}\left[s_{\mathcal{I}}^i \cdot s_{\mathcal{J}}^i\right] - \mathbb{E}\left[s_{\mathcal{I}}^i\right] \cdot \mathbb{E}\left[s_{\mathcal{J}}^i\right]\,. \tag{19}$$

We know the latter expectations from the proof of Lemma 3 to be bounded by

$$\mathbb{E}\left[s_{\mathcal{I}}^i\right] = 2^b \cdot \prod_{j\in\mathcal{I}} \frac{s_j^i}{2^b} \quad \text{and} \quad \mathbb{E}\left[s_{\mathcal{J}}^i\right] = 2^b \cdot \prod_{j\in\mathcal{J}} \frac{s_j^i}{2^b}\,.$$

Thus, it remains to bound the expectation of the product. It holds that

$$\begin{aligned}\mathbb{E}\left[s_{\mathcal{I}}^i \cdot s_{\mathcal{J}}^i\right] &= \mathbb{E}\left[\left(\sum_{y_1\in\mathbb{F}_2^b} I_{y_1}\right) \cdot \left(\sum_{y_1\in\mathbb{F}_2^b} J_{y_1}\right)\right] \\ &= \rho_{I_{y_1},J_{y_1}} \cdot \sqrt{2^b \cdot 2^b \cdot \mathbf{Var}\left[I_{y_1}\right] \cdot \mathbf{Var}\left[J_{y_1}\right]} \\ &\quad + \left(\sum_{y_1\in\mathbb{F}_2^b} \mathbb{E}[I_{y_1}]\right) \cdot \left(\sum_{y_1\in\mathbb{F}_2^b} \mathbb{E}[J_{y_1}]\right)\,. \end{aligned} \tag{20}$$

where

$$\rho_{I_{y_1},J_{y_1}} = \frac{\mathbb{E}[I_{y_1} \cdot J_{y_1}] - \mathbb{E}[I_{y_1}] \cdot \mathbb{E}[J_{y_1}]}{\sqrt{\mathbf{Var}[I_{y_1}] \cdot \mathbf{Var}[J_{y_1}]}} \,. \tag{21}$$

We know

$$\mathbb{E}[I_{y_1}] = \prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b} \quad \text{and} \quad \mathbb{E}\left[s_{\mathcal{J}}^i\right] = \prod_{j \in \mathcal{J}} \frac{s_j^i}{2^b} \,.$$

and need

$$\mathbb{E}[I_{y_1} \cdot J_{y_1}] = \mathbb{E}[I_{y_1}] \cdot \Pr[J_{y_1} | I_{y_1}] \,.$$

We know that

$$\begin{aligned}
\Pr[J_{y_1} | I_{y_1}] &= \Pr\big[y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_4 \in \mathcal{S}_4^i \,\big|\, \\
&\qquad y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_3 \in \mathcal{S}_3^i\big] \\
&= \Pr\left[y_1 \oplus w_4 \in \mathcal{S}_4^i \,|\, y_1 \in \mathcal{S}_1^i \wedge y_1 \oplus w_2 \in \mathcal{S}_2^i \wedge y_1 \oplus w_3 \in \mathcal{S}_3^i\right] \\
&= \frac{s_4^i}{2^b}
\end{aligned}$$

since the individual terms w_i are independent from each other and $\prod_{j \in \mathcal{J} \setminus \mathcal{I}} \frac{s_j^i}{2^b}$ in general. Thus, it holds that

$$\mathbb{E}[I_{y_1} \cdot J_{y_1}] = \prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b} \cdot \prod_{j \in \mathcal{I} \setminus \mathcal{J}} \frac{s_j^i}{2^b} = \frac{1}{2^b} \cdot \prod_{j \in \mathcal{I} \cup \mathcal{J}} s_j^i \,.$$

Thus,

$$(21) = \frac{\prod_{j \in \mathcal{I} \cup \mathcal{J}} \frac{s_j^i}{2^b} - \prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b} \cdot \prod_{j \in \mathcal{J}} \frac{s_j^i}{2^b}}{\sqrt{\mathbf{Var}[I_{y_1}] \cdot \mathbf{Var}[J_{y_1}]}}$$

Inserting into Equation (20),

$$\begin{aligned}
\mathbb{E}\left[s_{\mathcal{I}}^i \cdot s_{\mathcal{J}}^i\right] = {} & \frac{\left(\prod_{j \in \mathcal{I} \cup \mathcal{J}} \frac{s_j^i}{2^b}\right) - \left(\prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b} \cdot \prod_{j \in \mathcal{J}} \frac{s_j^i}{2^b}\right)}{\sqrt{\mathbf{Var}[I_{y_1}] \cdot \mathbf{Var}[J_{y_1}]}} \cdot \sqrt{2^b \cdot 2^b \cdot \mathbf{Var}[I_{y_1}] \cdot \mathbf{Var}[J_{y_1}]} + \\
& \left(\sum_{y_1 \in \mathbb{F}_2^b} \mathbb{E}[I_{y_1}]\right) \cdot \left(\sum_{y_1 \in \mathbb{F}_2^b} \mathbb{E}[J_{y_1}]\right) \\
= {} & 2^b \cdot \underbrace{\left(\prod_{j \in \mathcal{I} \cup \mathcal{J}} \frac{s_j^i}{2^b}\right)}_{p_{\mathcal{I} \cup \mathcal{J}}} - 2^b \cdot \underbrace{\left(\prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b}\right)}_{p_{\mathcal{I}}} \cdot \underbrace{\left(\prod_{j \in \mathcal{J}} \frac{s_j^i}{2^b}\right)}_{p_{\mathcal{J}}} \\
& + 2^b \cdot \underbrace{\left(\prod_{j \in \mathcal{I}} \frac{s_j^i}{2^b}\right)}_{p_{\mathcal{I}}} \cdot 2^b \cdot \underbrace{\left(\prod_{j \in \mathcal{J}} \frac{s_j^i}{2^b}\right)}_{p_{\mathcal{J}}}
\end{aligned}$$

substituting $n = 2^b$ and inserting into Equation produces

$$\begin{aligned}(19) = \mathbf{Cov}\left[s^i_{\mathcal{I}}, s^i_{\mathcal{J}}\right] &= \mathbb{E}\left[s^i_{\mathcal{I}} \cdot s^i_{\mathcal{J}}\right] - \mathbb{E}\left[s^i_{\mathcal{I}}\right] \cdot \mathbb{E}\left[s^i_{\mathcal{J}}\right] \\ &= n \cdot p_{\mathcal{I}\cup\mathcal{J}} - n \cdot p_{\mathcal{I}} \cdot p_{\mathcal{J}} + n \cdot p_{\mathcal{I}} \cdot n \cdot p_{\mathcal{J}} - n \cdot p_{\mathcal{I}} \cdot n \cdot p_{\mathcal{J}} \\ &= n \cdot p_{\mathcal{I}\cup\mathcal{J}} - n \cdot p_{\mathcal{I}} \cdot p_{\mathcal{J}}\,,\end{aligned}$$

which gives our claim in Lemma 4.

A.5 Proof of Lemma 7

Lemma 7. Let $r \geq 2$ be integer. For all even $\ell = 2j$ for some $j \in [2..r-1]$,

$$\frac{|k^i_{\ell+1}|}{|k^i_\ell|} \leq 3r\,, \quad k^i_{\ell+1} \geq 0\,, \quad k^i_\ell \leq 0 \quad \text{and} \quad k^i_{2r} \leq 0\,.$$

Proof. First, we note that k^i_ℓ will be negative whereas $k^i_{\ell+1}$ will be positive, given that $\ell \geq 4$. We can write $k^i_\ell = \underline{k}^i_\ell + \overline{k}^i_\ell$. We consider $\underline{k}^i_\ell$ first. To isolate those terms that contribute to the fixed ℓ, we can see from Equation 11 and 14 that $t_1 + t_2 = \ell$ must hold. Since we consider an even exponent $\ell = t_1 + t_2 = 2j$, those summands add to

$$\begin{aligned}\underline{k}^i_\ell &= -(-1)^{t_1+t_2}\binom{r}{2}\binom{r}{\ell-2} - \binom{r}{3}\binom{r}{\ell-3} - \cdots - \binom{r}{\ell-2}\binom{r}{2} \\ &= -\left(\sum_{t_1=2}^{\ell-2}\binom{r}{t_1}\binom{r}{\ell-t_1}\right).\end{aligned}$$

For odd $\ell + 1$, the inverse holds, i.e., all terms in $\underline{k}^i_{\ell+1}$ will be positive:

$$\underline{k}^i_\ell = \left(\sum_{t_1=2}^{\ell-1}\binom{r}{t_1}\binom{r}{\ell+1-t_2}\right).$$

Next, we consider the summands that contribute to $\overline{k}^i_\ell$. From Lemma 6, we know that the factors for fixed t_1, t_2, r, and ℓ for $\overline{k}^i_\ell$ are

$$\overline{k}^i_{t_1,t_2,r} = \binom{r}{t_1}\binom{r}{t_1+t_2-\ell}\binom{r-t_1}{\ell-t_1}(-1)^{t_1+t_2}\,.$$

Over all $t_1, t_2 \in \{2, \ldots, \ell\}$ in Equation 9 and considering the correct signs,

$$\overline{k}^i_\ell = \sum_{t_1=2}^{\ell}\sum_{t_2=2}^{\ell}\left(\binom{r}{t_1}\binom{t_1}{t_1+t_2-\ell}\binom{r-t_1}{\ell-t_1}(-1)^{t_1+t_2}\right).$$

Note that values of $t_1, t_2 > \ell$ do not contribute since they have no terms in c^i that produce powers p^ℓ. We observe that $\overline{k}^i_\ell$ consists of summands of different

sign. To gain clarity, we decompose and group those first according to $\binom{r}{t_1}$ and second to their sign.

$$\overline{k}^i_\ell = \sum_{t_1=2}^{\ell} \binom{r}{t_1}\binom{r-t_1}{\ell-t_1}(-1)^{t_1+t_2} \left(\sum_{t_2=2,4,\ldots,\ell} \binom{t_1}{t_1+t_2-\ell} - \sum_{t_2=3,5,\ldots,\underline{\ell+1}} \binom{t_1}{t_1+t_2-\ell} \right) \tag{22}$$

$$\overline{k}^i_{\ell+1} = \sum_{t_1=2}^{\ell+1} \binom{r}{t_1}\binom{r-t_1}{\ell+1-t_1}(-1)^{t_1+t_2+1} \left(\sum_{t_2=2,4,\ldots,\ell+1} \binom{t_1}{t_1+t_2-(\ell+1)} - \sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1+t_2-(\ell+1)} \right). \tag{23}$$

Note that for odd $\ell+1$, the cardinalities of $|\{2,4,\ldots,\ell+1\}| = |\{3,5,\ldots,\ell+1\}| = \ell/2$. Though, while $|\{2,4,\ldots,\ell\}| = \ell/2$, $|\{3,5,\ldots,\ell\}| = \ell/2-1$. Since the term $\binom{t_1}{t_1+t_2-\ell} = \binom{t_1}{-1} = 0$ for $t_2 = \ell+1$, we were allowed to extend the underlined index in the rightmost sum in Equation (22) from ℓ to $\ell+1$ without changing the result. Then, we have $\ell/2$ terms in each difference and will be able to use another helping lemma.

For some set $\mathcal{I} \subseteq \mathbf{N}_0$, let $\mathcal{I}_e = \{i \in \mathcal{I} : i \text{ is even}\}$ and $\mathcal{I}_o = \{i \in \mathcal{I} : i \text{ is odd}\}$ denote the sets of even and odd non-negative numbers in $\mathcal{I}$. The following result is well-known.

Lemma 8. Let n be a positive integer. Then

$$\sum_{k\in[0..n]_e} \binom{n}{k} = \sum_{k\in[0..n]_o} \binom{n}{k} = \frac{2^n}{2}\,.$$

It follows that

$$\begin{aligned}
\sum_{k\in[0..n]_o} \binom{n}{k} - \sum_{k\in[0..n]_e} \binom{n}{k} &= 0\\
\sum_{k\in[1..n]_o} \binom{n}{k} - \sum_{k\in[1..n]_e} \binom{n}{k} &= \binom{n}{0} = 1\\
\sum_{k\in[2..n]_o} \binom{n}{k} - \sum_{k\in[2..n]_e} \binom{n}{k} &= \binom{n}{0} - \binom{n}{1} = 1-n\,.
\end{aligned}$$

First, we consider $\overline{k}^i_{\ell+1}$ with three cases.

Case $t_1 \leq \ell - 1$: From Equation (23), we see that for all even $t_1 \leq \ell - 1$

$$\sum_{t_2=2,4,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_o} \binom{t_1}{k}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_e} \binom{t_1}{k}$$

and from Lemma 8

$$\sum_{t_2=2,4,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} - \sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = 0\,.$$

A similar statement can be derived for all odd $t_1 \leq \ell - 1$.

Case $t_1 = \ell$: For $t_1 = \ell$, we have

$$\sum_{t_2=2,4,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_o} \binom{t_1}{k}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_e} \binom{t_1}{k} - \binom{t_1}{0}\,.$$

Case $t_1 = \ell$: For $t_1 = \ell + 1$, it holds that

$$\sum_{t_2=2,4,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_e} \binom{t_1}{k} - \binom{t_1}{0}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - (\ell+1)} = \sum_{k \in [0..\ell+1]_o} \binom{t_1}{k} - \binom{t_1}{1}$$

We obtain that

$$\begin{aligned}\overline{k}^i_{\ell+1} &= \binom{r}{\ell}\binom{r-\ell}{\ell+1-\ell}\binom{\ell}{0} - \binom{r}{\ell+1}\binom{r-(\ell+1)}{\ell+1-(\ell+1)}\left(\binom{\ell+1}{1} - \binom{\ell+1}{0}\right) \\ &= \binom{r}{\ell+1}\,.\end{aligned}$$

Next, we consider $\overline{k}^i_\ell$ with three similar cases.

Case $t_1 \leq \ell - 2$: From Equation (23), we see that for all even $t_1 \leq \ell - 2$

$$\sum_{t_2=2,4,\ldots,\ell} \binom{t_1}{t_1 + t_2 - \ell} = \sum_{k \in [0..\ell+1]_e} \binom{t_1}{k}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1 + t_2 - \ell} = \sum_{k \in [0..\ell+1]_o} \binom{t_1}{k}$$

and from Lemma 8

$$\sum_{t_2=2,4,\ldots,\ell} \binom{t_1}{t_1+t_2-\ell} - \sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1+t_2-\ell} = 0\,.$$

A similar statement can be derived for all odd $t_1 \leq \ell - 2$.

Case $t_1 = \ell - 1$: For $t_1 = \ell - 1$, we have

$$\sum_{t_2=2,4,\ldots,\ell} \binom{t_1}{t_1+t_2-\ell} = \sum_{k\in[0..\ell]_o} \binom{t_1}{k}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1+t_2-\ell} = \sum_{k\in[0..\ell]_e} \binom{t_1}{k} - \binom{t_1}{0}\,.$$

Case $t_1 = \ell$: For $t_1 = \ell$, it holds that

$$\sum_{t_2=2,4,\ldots,\ell} \binom{t_1}{t_1+t_2-\ell} = \sum_{k\in[0..\ell]_e} \binom{t_1}{k} - \binom{t_1}{0}$$
$$\sum_{t_2=3,5,\ldots,\ell+1} \binom{t_1}{t_1+t_2-\ell} = \sum_{k\in[0..\ell]_o} \binom{t_1}{k} - \binom{t_1}{1}$$

We obtain that

$$\overline{k}^i_\ell = \binom{r}{\ell-1}\binom{r-(\ell-1)}{\ell-(\ell-1)}\binom{\ell-1}{0} - \binom{r}{\ell}\binom{r-\ell}{\ell-\ell}\left(\binom{\ell}{1} - \binom{\ell}{0}\right) = \binom{r}{\ell}\,.$$

Now, we can insert our terms to bound our desired ratio

$$\frac{k^i_{\ell+1}}{k^i_\ell} = \frac{\underline{k}^i_{\ell+1} + \overline{k}^i_{\ell+1}}{\underline{k}^i_\ell + \overline{k}^i_\ell} = \frac{\left(\sum_{t_1=2}^{\ell-1}\binom{r}{t_1}\binom{r}{\ell+1-t_1}\right) + \binom{r}{\ell+1}}{-\left(\sum_{t_1=2}^{\ell-2}\binom{r}{t_1}\binom{r}{\ell-t_1}\right) - \binom{r}{\ell}}$$
$$= \frac{\overbrace{\left(\sum_{t_1=2}^{\ell-2}\binom{r}{t_1}\binom{r}{\ell+1-t_1}\right)}^{a} + \overbrace{\binom{r}{\ell-1}\binom{r}{2}}^{b} + \overbrace{\binom{r}{\ell+1}}^{c}}{-\underbrace{\left(\sum_{t_1=2}^{\ell-2}\binom{r}{t_1}\binom{r}{\ell-t_1}\right)}_{d} - \underbrace{\binom{r}{\ell}}_{e}}\,.$$

Thus, we have shown the positivity and negativity statements from Lemma 7:

$$k^i_{\ell+1} \geq 0, \quad k^i_\ell \leq 0, \quad \text{and} \quad k^i_{2r} \leq 0\,.$$

It remains to obtain upper bound the ratio of their absolutes. We can use

$$\frac{a+b+c}{d+e} \leq \frac{a}{d+e} + \frac{b}{d+e} + \frac{c}{d+e} \leq \frac{a}{d} + \frac{b}{d} + \frac{c}{e}\,.$$

We can see that

$$\frac{a}{d} = \frac{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell+1-t_1}}{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}} = \frac{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}\frac{r-(\ell-t_1)}{\ell-t_1+1}}{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}} \leq \frac{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}\frac{r-2}{3}}{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}} \leq \frac{r}{3}\,.$$

Similarly, for all $\ell \geq 4$:

$$\frac{b}{d} = \frac{\binom{r}{\ell-1}\binom{r}{2}}{\sum_{t_1=2}^{\ell-2} \binom{r}{t_1}\binom{r}{\ell-t_1}} \leq \frac{\binom{r}{2}\binom{r}{\ell-1}}{\binom{r}{2}\binom{r}{\ell-2}} \leq \frac{\binom{r}{2}\binom{r}{\ell-2}\frac{r-(\ell-2)}{\ell-1}}{\binom{r}{2}\binom{r}{\ell-2}} \leq \frac{r}{3}\,.$$

Finally, for all $\ell \geq 4$, it holds

$$\frac{c}{e} = \frac{\binom{r}{\ell+1}}{\binom{r}{\ell}} \leq \frac{\binom{r}{\ell}\frac{r-\ell}{\ell+1}}{\binom{r}{\ell}} \leq \frac{r}{\ell+1} \leq \frac{r}{5}\,.$$

The sum of the three bounds yields that for all $\ell = 2j$ and $j \in [2..r-1]$:

$$\frac{|k^i_{\ell+1}|}{|k^i_\ell|} \leq 3r\,.$$