Erratum for "Blind Unwrapping of Modulo Reduced Gaussian Vectors: Recovering MSBs from LSBs"

Elad Romanov and Or Ordentlich

The published version of our paper [1] contains several minor errors, that we list and correct in this document. All the items appearing here are minor, and do not impact the overall correctness of our results in any meaningful way.

1) The lower bound in Lemma 1 is incorrect. Eq. (63) should read:

$$\alpha(P;K)\mathbf{\Sigma} \preceq \mathbb{E}[\mathbf{X}\mathbf{X}^T \,|\, \mathbf{X} \in \mathcal{S}] \preceq \mathbf{\Sigma}\,.$$

We are grateful to Zhang Qi for kindly bringing this error to our attention.

2) The upper bound in Lemma 3 is incorrect. Eq. (73) should read:

$$P_{m+1} \leq K \cdot Q\left(\sqrt{\frac{1-\beta}{1+\beta}\cdot\alpha(P_m;K)}\cdot Q^{-1}\left(\frac{\epsilon}{2}\right)\right).$$

3) In the proof of Corollary 1, the following inequality, which appears on the second line:

$$\sqrt{\frac{1-\beta}{1+\beta}\frac{\alpha(P_m;K)}{1-P_m}} \geq \sqrt{\frac{0.9\cdot(1-\sqrt{1/10})}{1.1\cdot(1-1/30)}} \geq \frac{3}{4}$$

should be replaced by:

$$\sqrt{\frac{1-\beta}{1+\beta}\alpha(P_m;K)} \geq \sqrt{\frac{0.9\cdot(1-\sqrt{1/10})}{1.1}} \geq 0.74\,.$$

Accordingly, Eq. (78) should read:

$$P_{m+1} \leq K\cdot Q\left(6\cdot 0.74\sqrt{K}\right) \leq Q(4.44)\,.$$

Accordingly, Eq. (79) should read:

$$P_{m+2} \leq K\cdot Q\left(\sqrt{\frac{1-\beta}{1+\beta}}\cdot\sqrt{1-\sqrt{3Q(4.44)}}Q^{-1}\left(\frac{\epsilon}{2}\right)\right) \leq K\cdot Q\left(0.99\sqrt{\frac{1-\beta}{1+\beta}}Q^{-1}\left(\frac{\epsilon}{2}\right)\right).$$

4) The paragraph between Corollary 1 and Lemma 4 should read as follows (changes in bold):

"Corollary 1 leveraged Lemma 3 to show that once the probability of missing CUBE is not too large, it decreases very fast from iteration to iteration. Unfortunately, for large P_m, Lemma 3 does not imply **readily** that $P_{m+1} < P_m$, as $\alpha(P;K)$ is very **small** for P close to 1. To this end, we now develop another technique for upper bounding P_{m+1} in terms of P_m, which is effective for large P_m (but not for small P_m). "

5) In Theorem 2, the parameter $\overline{\beta}$ from Eq. (19) should read:

$$\overline{\beta} \triangleq \beta + \frac{2K \cdot \left(\frac{\Delta}{\tau_{\min}}\right)^2}{(1-P)\alpha(P;K) \cdot \sqrt{n}} .$$

The bound in Eq. (25) should be:

$$\Pr\left(\mathcal{E}_{\text{sample-est}}\right) \leq \exp\left[-\beta^2 \cdot \frac{(1-P)\alpha(P,K)}{C \cdot \frac{K}{2} \cdot \left(\frac{\Delta}{\tau_{\min}}\right)^2} \cdot n\right] + e^{-\frac{1}{2}(1-P)^2 n} . \tag{1}$$

6) In proof of Theorem 2, page 19: The upper bound on R^2 should be

$$R^2 = \frac{K\Delta^2}{4} \cdot \left\|\mathbf{\Sigma}_{\text{truc}}^{-1}\right\| \leq \frac{K\Delta^2}{4} \cdot \frac{1}{\alpha(P;K)} \left\|\mathbf{\Sigma}^{-1}\right\| = \frac{K}{4} \cdot \left(\frac{\Delta}{\tau_{\min}}\right)^2 \cdot \frac{1}{\alpha(P;K)} ,$$

and accordingly $\overline{\beta}$ should be bounded as

$$\overline{\beta} = \beta + \frac{|\mathcal{S}_0| - |\mathcal{T}|}{|\mathcal{S}_0|} \cdot 2R^2 \leq \beta + \frac{8}{(1-P)\sqrt{n}} R^2 \leq \beta + \frac{2K \cdot \left(\frac{\Delta}{\tau_{\min}}\right)^2}{(1-P)\alpha(P;K) \cdot \sqrt{n}} .$$

7) Lemma 15 and its proof: All mentions of $\alpha(P;K)$ should be replaced by $(1-P)\alpha(P;K)$.

REFERENCES

[1] E. Romanov and O. Ordentlich, "Blind unwrapping of modulo reduced gaussian vectors: Recovering msbs from lsbs," *IEEE Transactions on Information Theory*, vol. 67, no. 3, pp. 1897–1919, 2021.