# Proceedings of the
# 35th USENIX Security Symposium (USENIX Security '26)

# Errata Slip

In the paper "SING: Improving the Efficiency of MPC Protocol Assignment using Graph Neural Networks" by Jannis Blüml, Moritz Huppert, Nora Khayata, Joachim Schmidt, and Thomas Schneider, *Technical University of Darmstadt* (Thursday session, "Applications of Cryptography 3" pp. 2923–2942 of the Proceedings), the authors provide the following revisions to the content.

**Context:** During the thorough artifact review for the Artifacts Functional and Results Reproduced badges, the reviewers identified an issue with Experiment E2 (Section 8.5) that required us to revise the reported results. Specifically, our original implementation did not ensure that the MPC benchmarking circuits used to compare SING and Silph were excluded from SING's training pipeline. We therefore revised the experiment by retraining the SING models while explicitly excluding the corresponding benchmarking circuits from the respective datasets. Below, we report the updated experimental results.

**Original Figure 2 pp. 2934:**

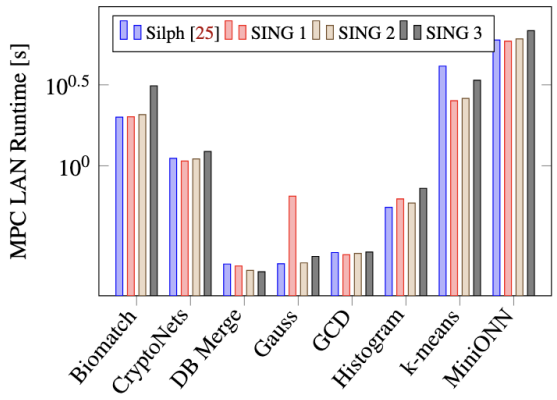



Figure 2: Comparison of resulting MPC LAN runtimes (s) for different share assignments. Detailed results in Table 6.

**Corrected Figure 2:**

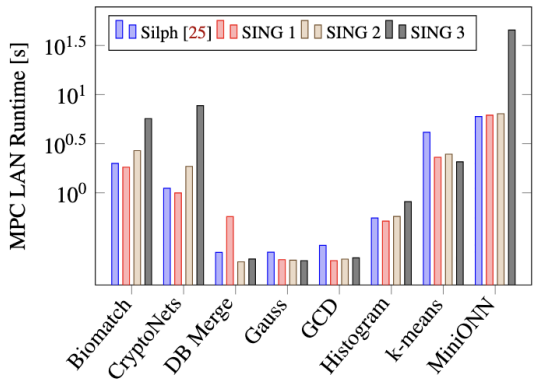



Figure 2: Comparison of resulting MPC LAN runtimes (s) for different share assignments. Detailed results in Table 6.

**Original Figure 3 pp. 2934:**

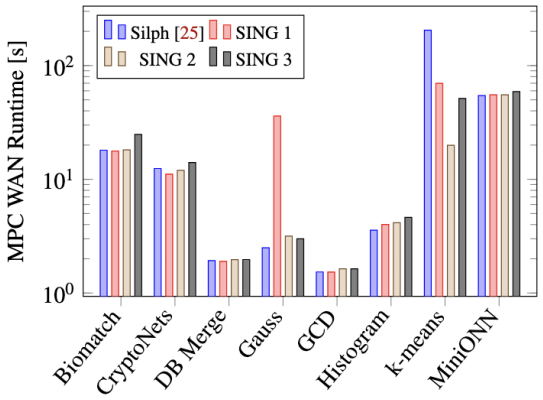



Figure 3: Comparison of resulting MPC WAN runtimes (s) for different share assignments. Detailed results in Table 7.

**Corrected Figure 3:**

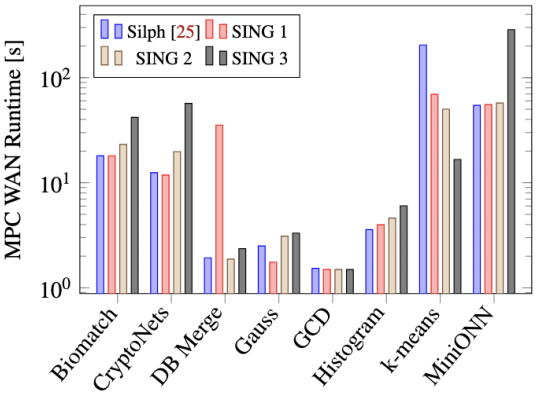



Figure 3: Comparison of resulting MPC WAN runtimes (s) for different share assignments. Detailed results in Table 7.

**Original Figure 4 pp. 2934:**

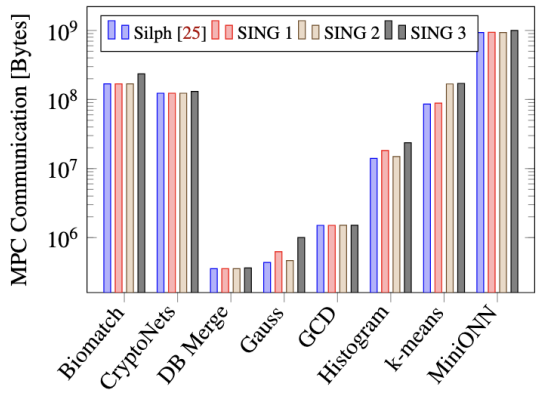



Figure 4: Resulting MPC communication (Bytes) for different share assignments; detailed results in Table 8.

**Corrected Figure 4:**

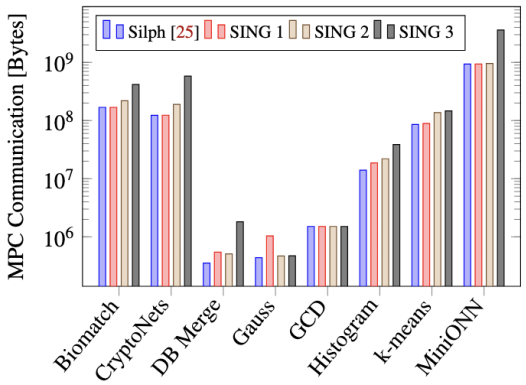



Figure 4: Resulting MPC communication (Bytes) for different share assignments; detailed results in Table 8.

**Original text pp. 2934, para. 2:**
For most benchmarks, the MPC runtime and communication achieved by share assignments generated by SING are very similar to Silph, excluding two outlier circuits.

**Corrected text:**
For most benchmarks, the MPC runtime and communication achieved by share assignments generated by SING 1 and SING 2 are similar to Silph, excluding two outlier circuits.

**Original text pp. 2934, para. 3:**
1) *Gauss* contains numerous MUX operations interleaved with arithmetic operations. SING 1 assigns a single division to bool instead of yao, increasing runtime by 161.23 %. This large impact is due to the circuit's small size.

**Corrected text:**
1) *DB Merge* contains a division operation, which SING 1 assigns to bool instead of yao, increasing runtime by 17.3× in WAN. This large impact is due to the circuit's small size.

**Original text pp. 2934, para. 5:**
It performs on par with our other models across all circuits. This highlights that $C^{SING}$ and $S^{SING}$ can capture how share assignments affect MPC performance *without external guidance*, despite $C^{SING}$ showing limited generalization on unseen circuits during training (cf. §8.2).

**Corrected text:**
Due to the high variance of MPC runtimes, this is a more complex task with higher requirements on the dataset quality. SING 3 performs on par with our other models for most circuits. Exceptions are Biomatch, CryptoNets, and MiniONN, where SING 3 assigns all additions to yao instead of arith leading to additional protocol conversion overhead. Our benchmarks show that $C^{SING}$ and $S^{SING}$ can partially capture how share assignments affect MPC performance *without external guidance*, despite $C^{SING}$ showing limited generalization on unseen circuits during training (cf. §8.2).

**Original Table 4 pp. 2941:**

Table 4: Hyperparameters of cost prediction model $C^{\text{SING}}$ and share assignment model $S^{\text{SING}}$.

| Hyperparameter | $C^{\text{SING}}$ | SING 1 | SING 2 | SING 3 |
|---|---|---|---|---|
| Epoch count | 150 | 200 | 200 | 200 |
| Batch size | 32 | 32 | 32 | 32 |
| Optimizer | Adam [57] | Adam | Adam | Adam |
| Dropout rate [48] | 0.5 | 0.5 | 0.5 | 0.5 |
| Learning rate | 0.001 | 0.01 | 0.001 | 0.01 |
| Weight decay | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ |
| Loss blending factor $\alpha$ | - | 0.9 | 0.1 | 0.9 |

**Corrected Table 4:**

Table 4: Hyperparameters of cost prediction model $C^{\text{SING}}$ and share assignment model $S^{\text{SING}}$.

| Hyperparameter | $C^{\text{SING}}$ | SING 1 | SING 2 | SING 3 |
|---|---|---|---|---|
| Epoch count | 150 | 200 | 200 | 200 |
| Batch size | 32 | 32 | 32 | 32 |
| Optimizer | Adam [57] | Adam | Adam | Adam |
| Dropout rate [48] | 0.5 | 0.5 | 0.5 | 0.5 |
| Learning rate | 0.001 | 0.01 | 0.001 | 0.001 |
| Weight decay | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ | $5 \times 10^{-4}$ |
| Loss blending factor $\alpha$ | - | 0.9 | 0.1 | 0.99 |

**Original Table 6 pp. 2942:**

Table 6: Comparison of MPC LAN runtimes in seconds with Silph [25]. $\Delta$ denotes the difference with respect to Silph. Aggregate differences are computed as geometric means over per-circuit runtime differences.

| Circuit | Silph [25] | SING 1 (supervised) | $\Delta$ [%] | SING 2 (minimize $C^{\text{Silph}}$) | $\Delta$ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | $\Delta$ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 2.00 | 2.01 | +0.65 | 2.07 | +3.69 | 3.12 | +56.25 |
| CryptoNets [38] | 1.11 | 1.07 | −3.87 | 1.10 | −0.85 | 1.23 | +10.15 |
| DB Merge | 0.25 | 0.24 | −2.68 | 0.23 | −8.69 | 0.22 | −10.30 |
| Gauss | 0.25 | 0.65 | +161.23 | 0.25 | +1.24 | 0.28 | +10.98 |
| GCD | 0.29 | 0.28 | −3.06 | 0.29 | −1.27 | 0.29 | +0.63 |
| Histogram | 0.55 | 0.62 | +12.78 | 0.59 | +6.22 | 0.73 | +31.12 |
| *k*-means | 4.13 | 2.53 | −38.85 | 2.61 | −36.77 | 3.38 | −18.14 |
| MiniONN [69] | 5.98 | 5.88 | −1.70 | 6.08 | +1.62 | 6.83 | +14.19 |
| Geometric mean | - | - | +6.19 | - | −5.42 | - | +9.80 |

**Corrected Table 6:**

Table 6: Comparison of MPC LAN runtimes in seconds with Silph [25]. $\Delta$ denotes the difference with respect to Silph. Aggregate differences are computed as geometric means over per-circuit runtime differences.

| Circuit | Silph [25] | SING 1 (supervised) | $\Delta$ [%] | SING 2 (minimize $C^{\text{Silph}}$) | $\Delta$ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | $\Delta$ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 2.00 | 1.83 | −8.59 | 2.69 | +34.56 | 5.70 | +185.64 |
| CryptoNets [38] | 1.11 | 1.00 | −10.39 | 1.86 | +66.90 | 7.72 | +594.19 |
| DB Merge | 0.25 | 0.57 | +131.26 | 0.20 | −19.72 | 0.21 | −14.39 |
| Gauss | 0.25 | 0.21 | −15.92 | 0.21 | −16.85 | 0.20 | −17.97 |
| GCD | 0.29 | 0.20 | −29.93 | 0.21 | −27.37 | 0.22 | −25.25 |
| Histogram | 0.55 | 0.51 | −7.05 | 0.58 | +3.84 | 0.81 | +46.61 |
| *k*-means | 4.13 | 2.30 | −44.22 | 2.47 | −40.10 | 2.07 | −49.87 |
| MiniONN [69] | 5.98 | 6.18 | +3.28 | 6.39 | +6.86 | 45.41 | +659.06 |
| Geometric mean | - | - | −6.23 | - | −3.96 | - | +66.15 |

**Original Table 7 pp. 2942:**

Table 7: Comparison of MPC WAN runtimes in seconds with Silph [25]. Δ denotes the difference with respect to Silph. Aggregate differences are computed as geometric means over per-circuit runtime differences.

| Circuit | Silph [25] | SING 1 (supervised) | Δ [%] | SING 2 (minimize $C^{\text{Silph}}$) | Δ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | Δ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 18.05 | 17.76 | −1.63 | 18.17 | +0.64 | 24.83 | +37.57 |
| CryptoNets [38] | 12.44 | 11.10 | −10.74 | 11.99 | −3.62 | 14.06 | +12.98 |
| DB Merge | 1.93 | 1.90 | −1.37 | 1.97 | +2.12 | 1.97 | +2.19 |
| Gauss | 2.50 | 35.97 | +1336.34 | 3.16 | +26.31 | 3.00 | +19.61 |
| GCD | 1.53 | 1.53 | −0.26 | 1.64 | +6.70 | 1.63 | +6.57 |
| Histogram | 3.57 | 4.00 | +12.08 | 4.15 | +16.21 | 4.63 | +29.56 |
| *k*-means | 204.55 | 69.89 | −65.83 | 19.92 | −90.26 | 51.45 | −74.85 |
| MiniONN [69] | 54.44 | 55.30 | +1.59 | 55.40 | +1.77 | 59.09 | +8.54 |
| Geometric mean | - | - | +21.74 | - | −20.87 | - | −4.09 |

**Corrected Table 7:**

Table 7: Comparison of MPC WAN runtimes in seconds with Silph [25]. Δ denotes the difference with respect to Silph. Aggregate differences are computed as geometric means over per-circuit runtime differences.

| Circuit | Silph [25] | SING 1 (supervised) | Δ [%] | SING 2 (minimize $C^{\text{Silph}}$) | Δ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | Δ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 18.05 | 18.07 | +0.08 | 23.18 | +28.41 | 41.87 | +131.95 |
| CryptoNets [38] | 12.44 | 11.82 | −4.95 | 19.78 | +59.03 | 56.90 | +357.40 |
| DB Merge | 1.93 | 35.38 | +1733.38 | 1.88 | −2.66 | 2.36 | +22.18 |
| Gauss | 2.50 | 1.76 | −29.88 | 3.11 | +24.11 | 3.32 | +32.52 |
| GCD | 1.53 | 1.49 | −2.67 | 1.49 | −2.66 | 1.50 | −2.43 |
| Histogram | 3.57 | 3.99 | +11.64 | 4.61 | +29.04 | 6.03 | +68.79 |
| *k*-means | 204.55 | 69.36 | −66.09 | 50.14 | −75.49 | 16.66 | −91.86 |
| MiniONN [69] | 54.44 | 55.36 | +1.69 | 57.43 | +5.49 | 286.09 | +425.52 |
| Geometric mean | - | - | +20.96 | - | −2.73 | - | +36.58 |

## Original Table 8 pp. 2942:

Table 8: Comparison of MPC communication amount in MBytes with Silph [25]. Δ denotes the overhead of SING over Silph.

| Circuit | Silph [25] | SING 1 (supervised) | Δ [%] | SING 2 (minimize $C^{\text{Silph}}$) | Δ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | Δ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 168.63 | 168.63 | +0.00 | 219.22 | +30.01 | 417.60 | +147.65 |
| CryptoNets [38] | 123.41 | 123.44 | +0.03 | 190.03 | +53.99 | 581.18 | +370.95 |
| DB Merge | 0.35 | 0.54 | +53.33 | 0.51 | +43.53 | 1.82 | +412.29 |
| Gauss | 0.44 | 1.04 | +136.45 | 0.47 | +6.85 | 0.47 | +7.68 |
| GCD | 1.51 | 1.51 | +0.00 | 1.51 | +0.00 | 1.51 | +0.10 |
| Histogram | 13.99 | 18.65 | +33.29 | 22.02 | +57.35 | 38.66 | +176.34 |
| *k*-means | 85.81 | 88.77 | +3.45 | 136.87 | +59.50 | 146.31 | +70.50 |
| MiniONN [69] | 934.40 | 938.54 | +0.44 | 956.16 | +2.33 | 3605.92 | +285.91 |

## Corrected Table 8:

Table 8: Comparison of MPC communication amount in MBytes with Silph [25]. Δ denotes the overhead of SING over Silph.

| Circuit | Silph [25] | SING 1 (supervised) | Δ [%] | SING 2 (minimize $C^{\text{Silph}}$) | Δ [%] | SING 3 (minimize $C^{\text{Runtime}}$) | Δ [%] |
|---|---|---|---|---|---|---|---|
| Biomatch | 168.63 | 168.63 | +0.00 | 219.22 | +30.01 | 417.60 | +147.65 |
| CryptoNets [38] | 123.41 | 123.44 | +0.03 | 190.03 | +53.99 | 581.18 | +370.95 |
| DB Merge | 0.35 | 0.54 | +53.33 | 0.51 | +43.53 | 1.82 | +412.29 |
| Gauss | 0.44 | 1.04 | +136.45 | 0.47 | +6.85 | 0.47 | +7.68 |
| GCD | 1.51 | 1.51 | +0.00 | 1.51 | +0.00 | 1.51 | +0.10 |
| Histogram | 13.99 | 18.65 | +33.29 | 22.02 | +57.35 | 38.66 | +176.34 |
| *k*-means | 85.81 | 88.77 | +3.45 | 136.87 | +59.50 | 146.31 | +70.50 |
| MiniONN [69] | 934.40 | 938.54 | +0.44 | 956.16 | +2.33 | 3605.92 | +285.91 |