Addendum to the Article
“Transforming Out Timing Leaks, More or Less” — Experimental Results
Heiko Mantel and Artem Starostin
Computer Science Department, TU Darmstadt, Germany
<lastname>@mais.informatik.tu-darmstadt.de

This document contains plots of the experimental data obtained during our security evaluation of program transformation in the article “Transforming Out Timing Leaks, More or Less” [1]. This document should be printed in color.

1 Experimental Results for Modular Exponentiation

Figure 1: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for \texttt{modExp} in the baseline version.

Figure 2: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for \texttt{modExp} transformed with cross-copying.
2 Experimental Results for Share Value

Figure 3: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for modExp transformed with conditional assignment.

Figure 4: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for modExp transformed with transactional branching.

Figure 5: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for shareValue in the baseline version.
Figure 6: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for shareValue transformed with cross-copying.

Figure 7: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for shareValue transformed with conditional assignment.

Figure 8: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for shareValue transformed with transactional branching.
Experimental Results for Kruskal’s Algorithm

Figure 9: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for kruskal in the baseline version.

Figure 10: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for kruskal transformed with cross-copying.

Figure 11: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for kruskal transformed with conditional assignment.
Figure 12: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for \texttt{kruskal} transformed with transactional branching.

4 Experimental Results for Modular Multiplication

Figure 13: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for \texttt{mulMod16} in the baseline.

Figure 14: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for \texttt{mulMod16} transformed with cross-copying.
Figure 15: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for `mulMod16` transformed with conditional assignment.

Figure 16: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for `mulMod16` transformed with transactional branching.

Figure 17: Running time values (left) and frequency of their occurrence (right) in a distinguishing experiment for `mulMod16` transformed with unification.

References