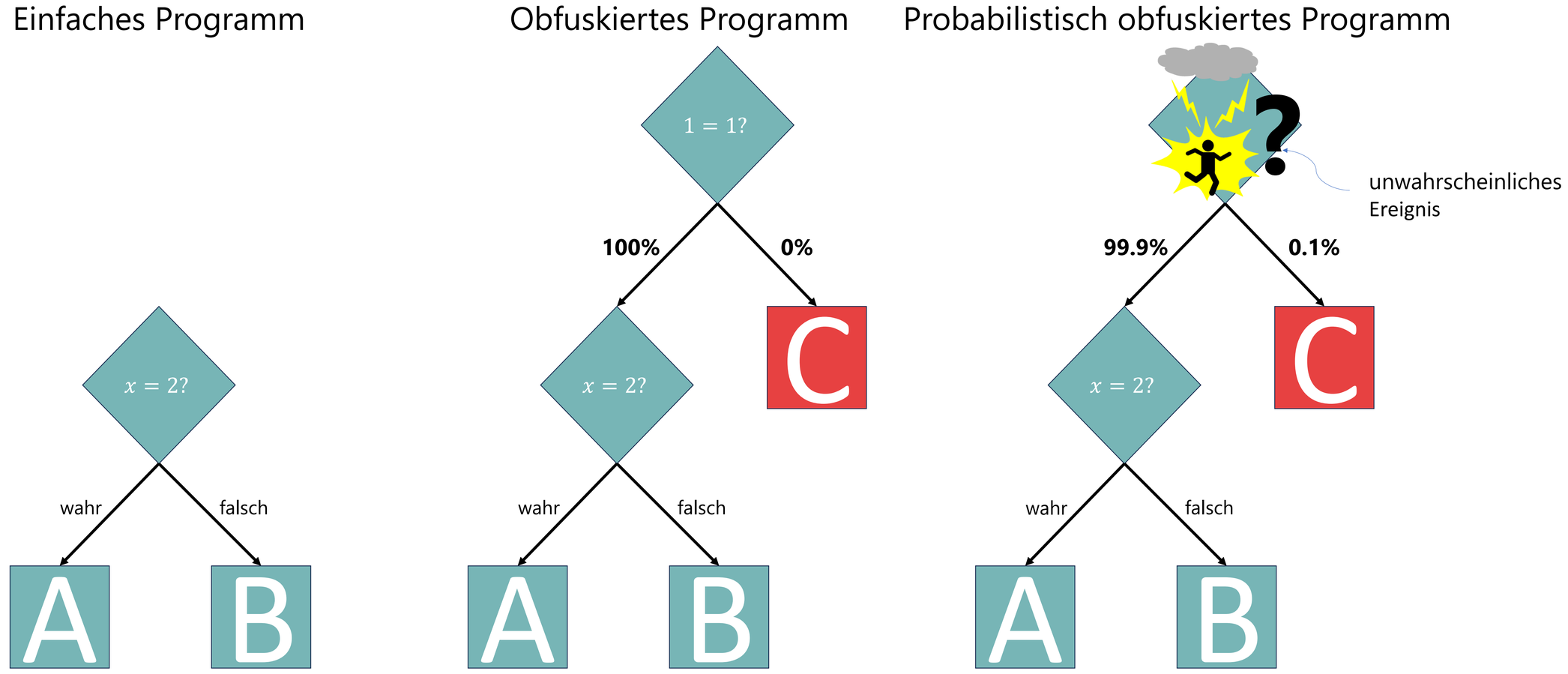
Wie sicher ist Ihre Software wirklich?

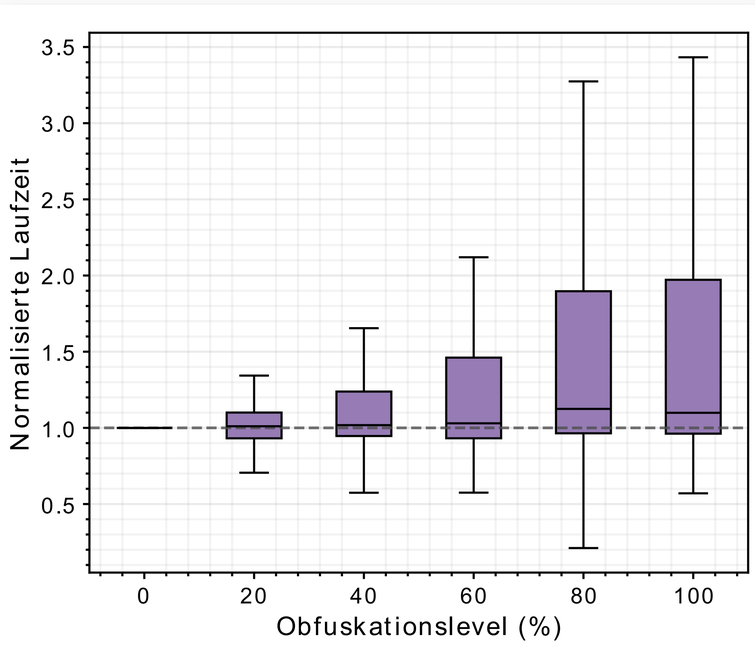
POP: Probabilistische opake Prädikate gegen symbolische Ausführung

Problem:

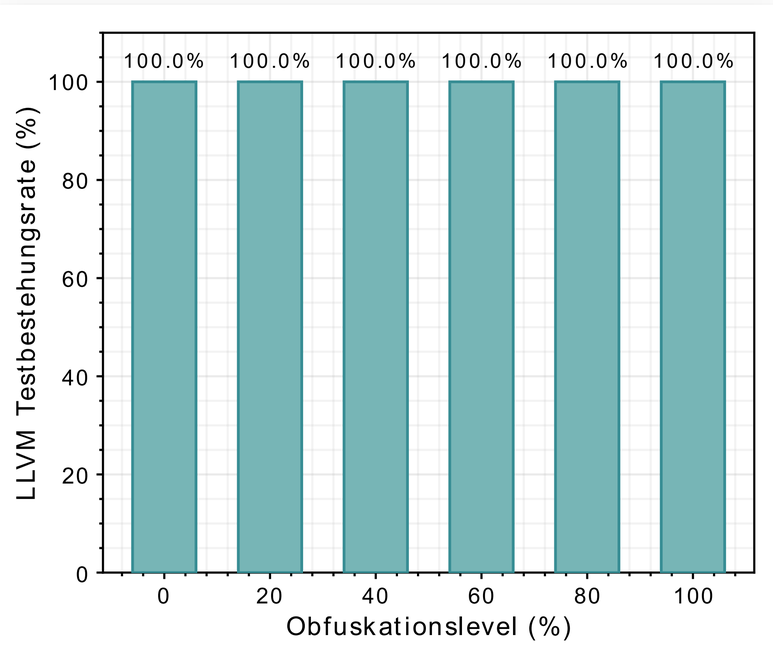
- Aktuelle Softwareverschleierungsmethoden (opake Prädikate) sind nicht resistent gegenüber manchen Angriffsmethoden (symbolischer Ausführung) → Möglichkeit, Software zu verstehen & zu rekonstruieren
- ~15 Mrd. Euro an Umsatz gehen jährlich in der EU durch Reverse Engineering/Cracking verloren [1]



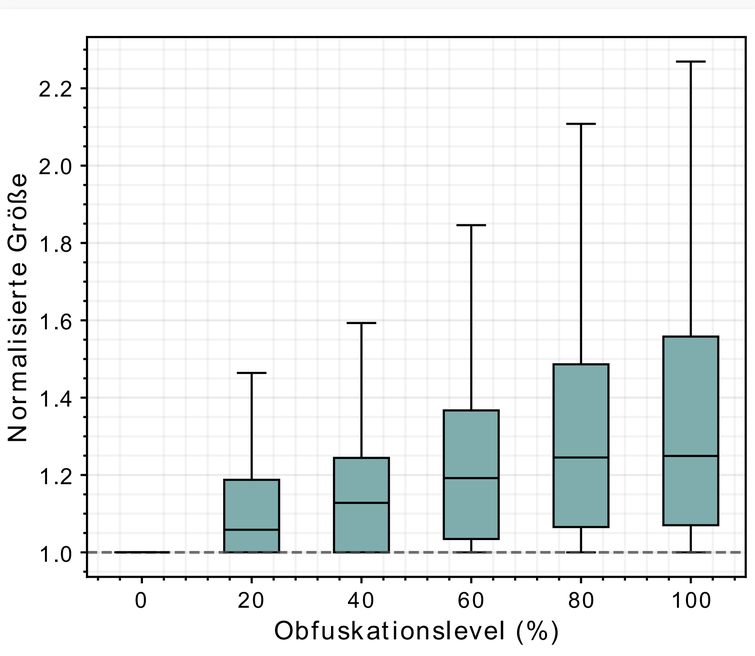
Ergebnis 1: Der **mediane Laufzeitimpakt** der neuen Obfuskation ist **gering**. Die Varianz ist allerdings groß.



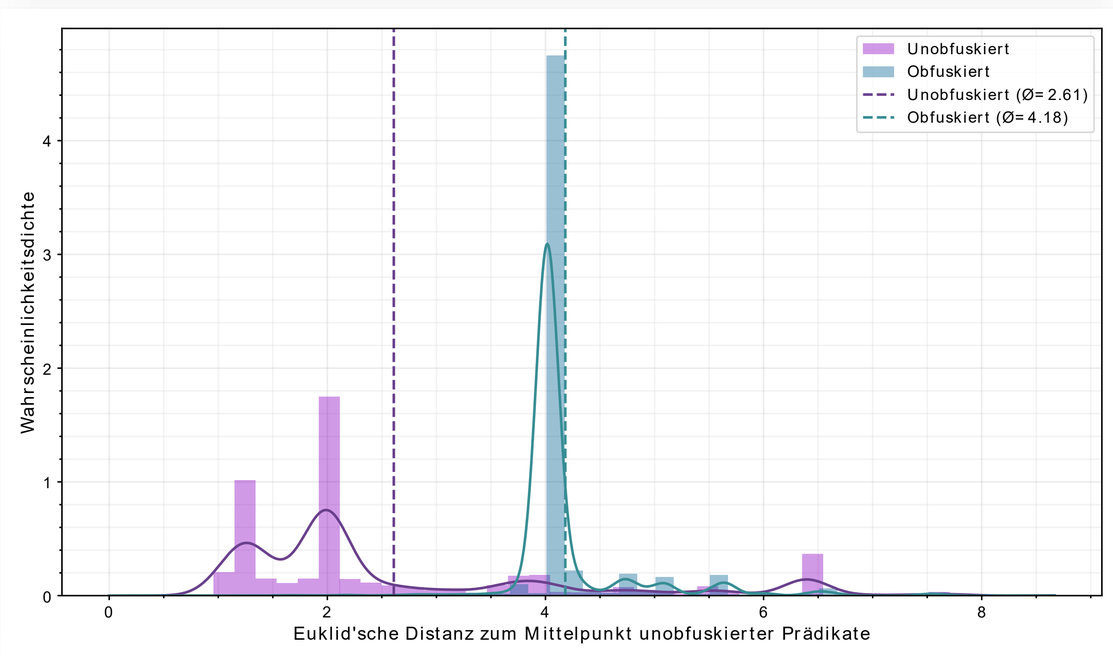
Ergebnis 2: Trotz der geringen Wahrscheinlichkeit, dass die POP-Prädikate den falschen Wert annehmen, **funktionieren alle Programme** .



Ergebnis 3: Der **mediane Speicherimpakt** der neuen Obfuskation ist **gering**. Die Varianz ist allerdings groß.



Ergebnis 4: Der **eingefügte Programmcode unterscheidet sich statistisch** von regulären Programmen.



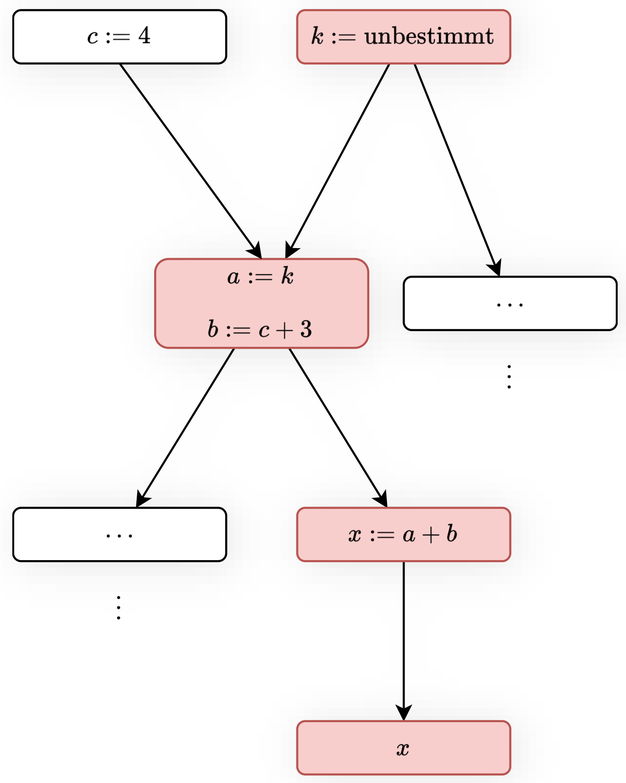
[1] BSA. „2018 Global Software Survey“. Mai 2018. url: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (besucht am 20.02.2026).

Wie sicher ist Ihre Software wirklich?

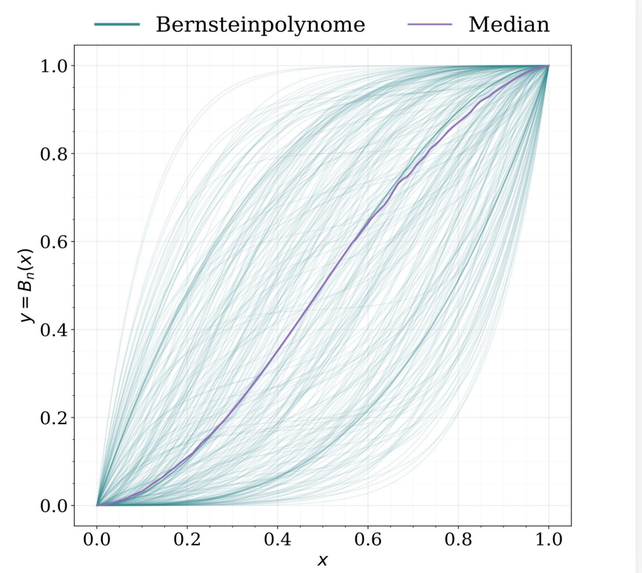
POP: Probabilistische opake Prädikate gegen symbolische Ausführung

Funktionsweise

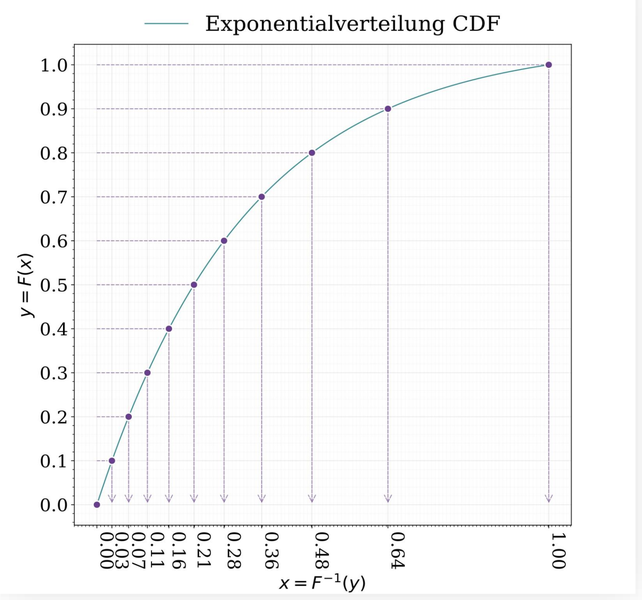
1. Parameter wählen, dessen Werte sich nicht statisch bestimmen lassen.



2. Kumulative Verteilungsfunktion generieren.



3. Über die Inversionsmethode Parameter gemäß der zugeordneten Wahrscheinlichkeitsdichtefunktion verteilen.



4. Da wir Kontrolle über die Verteilung der Zukunftsvariable haben, können wir festlegen, dass bestimmte Intervalle/Werte besonders wahrscheinlich sind.