

# Appendix

Anonymous Submission

## 1 Second-order DOM-*indep* multiplier

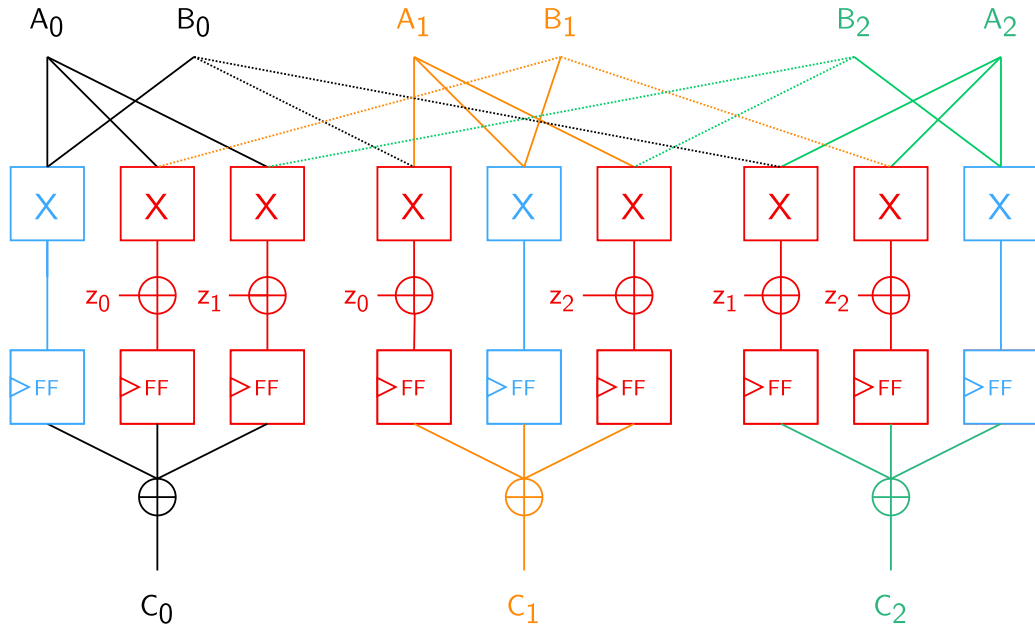


Figure A1: Second-order DOM-*indep* multiplier (Type A) as proposed by Gross et al. [GMK16].

The result  $C = C_0 \oplus C_1 \oplus C_2$  is the multiplication of the shared sensitive values  $A = A_0 \oplus A_1 \oplus A_2$  and  $B = B_0 \oplus B_1 \oplus B_2$ , using fresh randomness  $z_0, z_1$  and  $z_2$ . The three domains are drawn in black, orange and green. Cross-domain multiplications are drawn in red, while inner-domain multiplications are drawn in blue.

## 2 Second-order DOM-*dep* multiplier

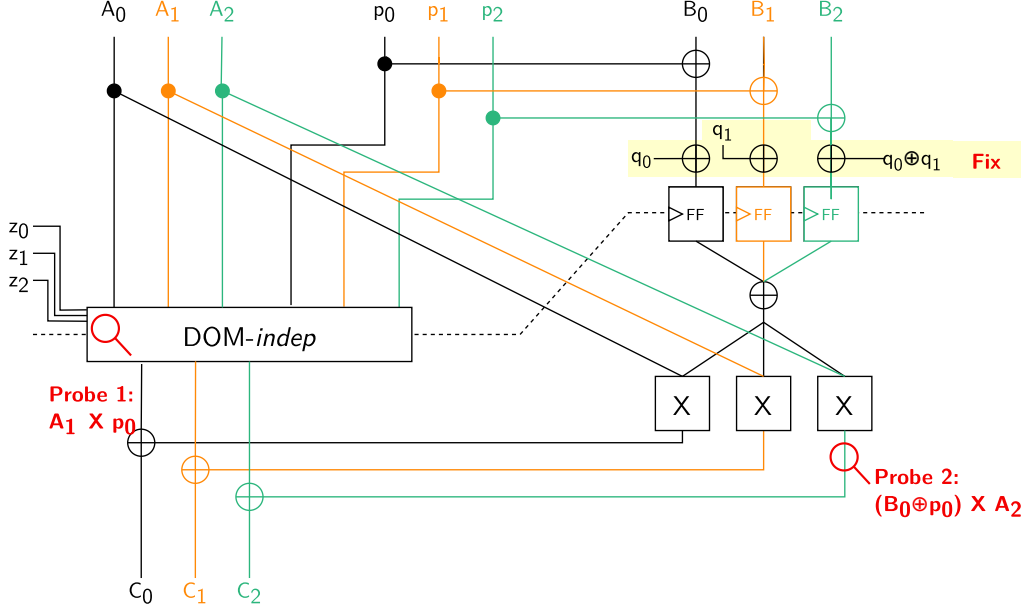


Figure A2: Second-order DOM-*dep* multiplier as initially proposed by Gross et al. [GMK16] in order to multiply the shared sensitive values  $A$  and  $B$  in case their sharing is not independent, e.g. if  $A = B$ .

In 2019, Moos et al. [MMSS19] pointed out that the construction is not second-order secure and an attacker could break the scheme using two probes (indicated by **Q**). Probe 1 is placed in the **DOM-indep** multiplier and allows to observe  $A_1 \times p_0$  after the computation phase. Probe 2 allows to observe  $(B_0 \oplus p_0) \times A_2$ , which leaks information about the sensitive value  $A$  in case  $B_0$  is not independent from  $A_0$ .

We fix this construction by re-freshing the shares of  $B$  with additional fresh randomness  $q_0$  and  $q_1$ , as highlighted in yellow.

### 3 Original second-order DOM AES S-box

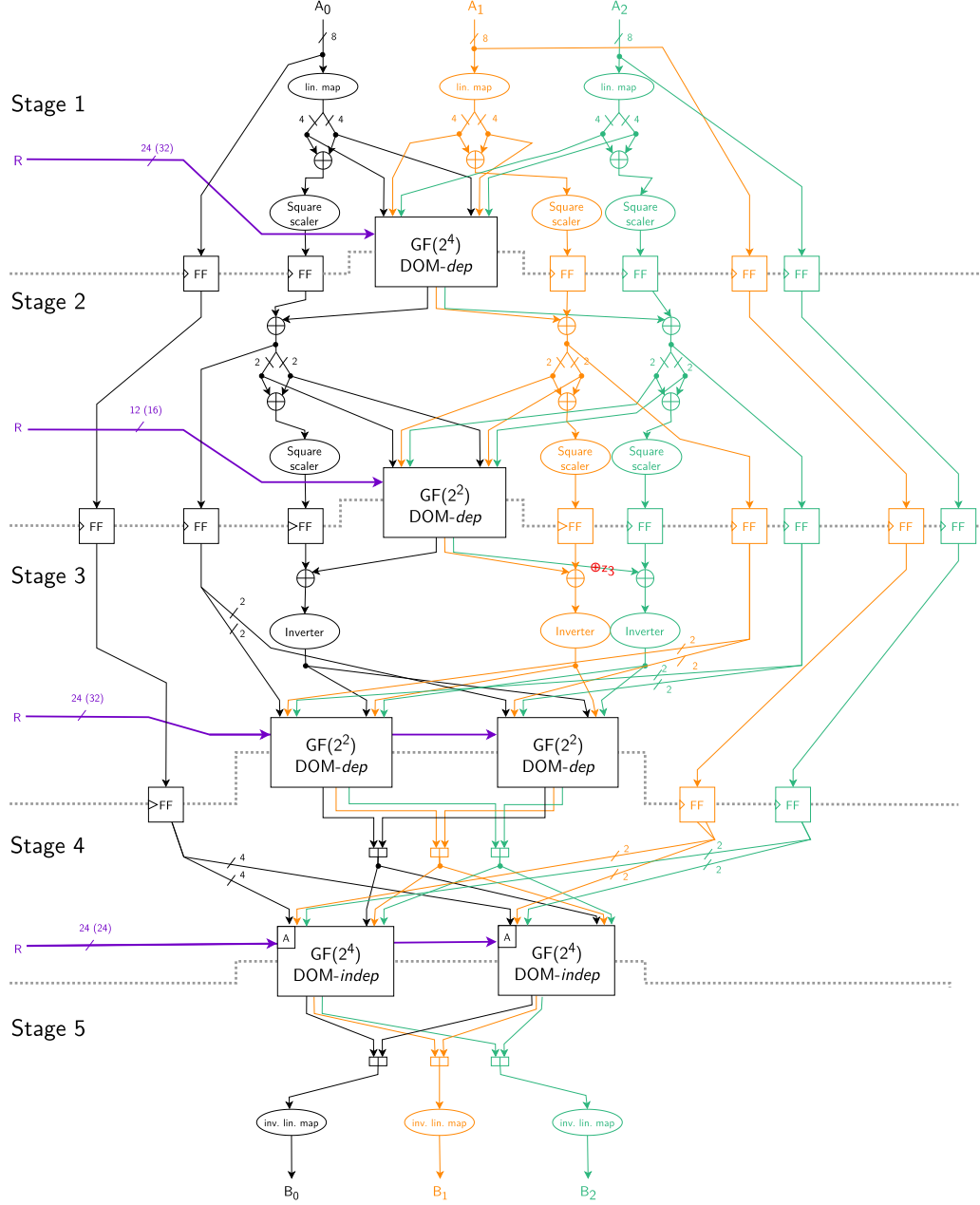


Figure A3: Second-order DOM AES S-box as proposed by [GMK16]. Fresh randomness required by the design is indicated in purple. All DOM-*indep* multipliers are Type A multipliers. The number in brackets indicates the increased amount of randomness required by the fixed version.

## 4 Optimized second-order DOM AES S-box

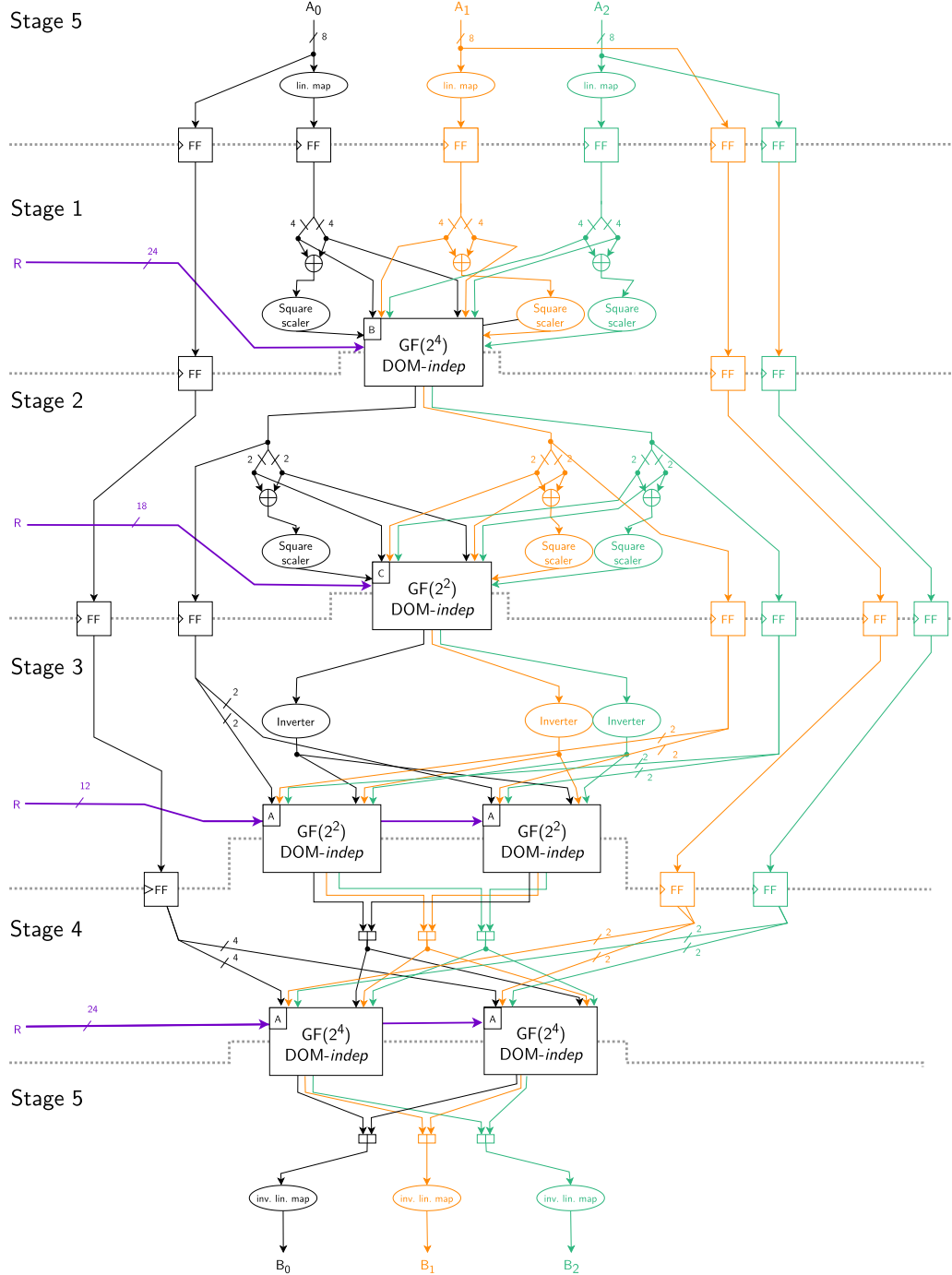


Figure A4: Our optimized second-order DOM AES S-box using only DOM-*indep* multipliers (Types A, B, C as indicated in the upper left corner) and precomputation of the linear map. Fresh randomness required by the design is indicated in purple.

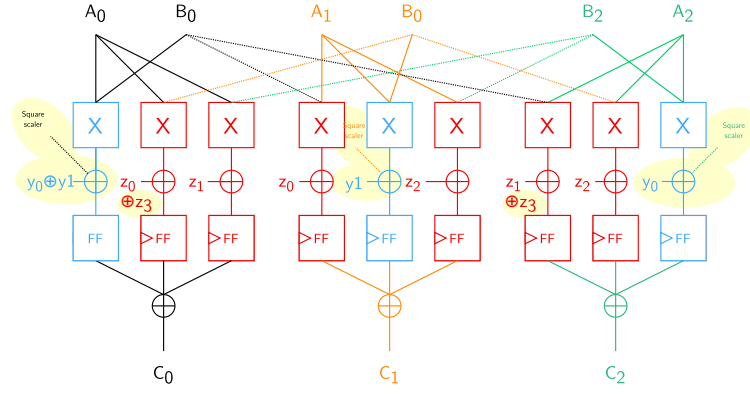


Figure A5: Adaptions made to the DOM-*indep* multiplier in Stage 1 (highlighted in yellow). This construction is referred to as the Type B DOM-*indep* multiplier.

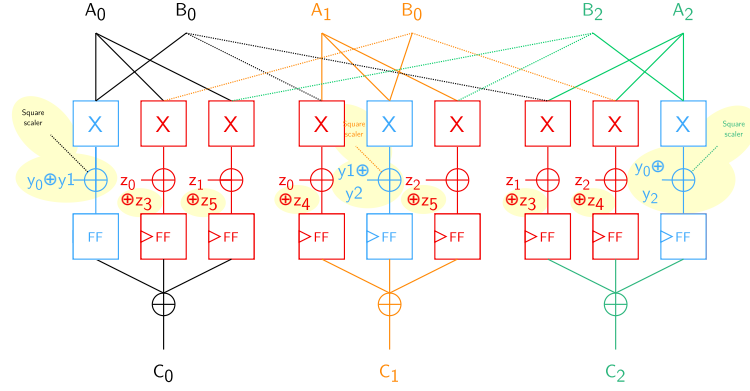


Figure A6: Adaptions made to the DOM-*indep* multiplier in Stage 2 (highlighted in yellow). This construction is referred to as the Type C DOM-*indep* multiplier.

## 7 5 Univariate T-test with RNG off/COTG on

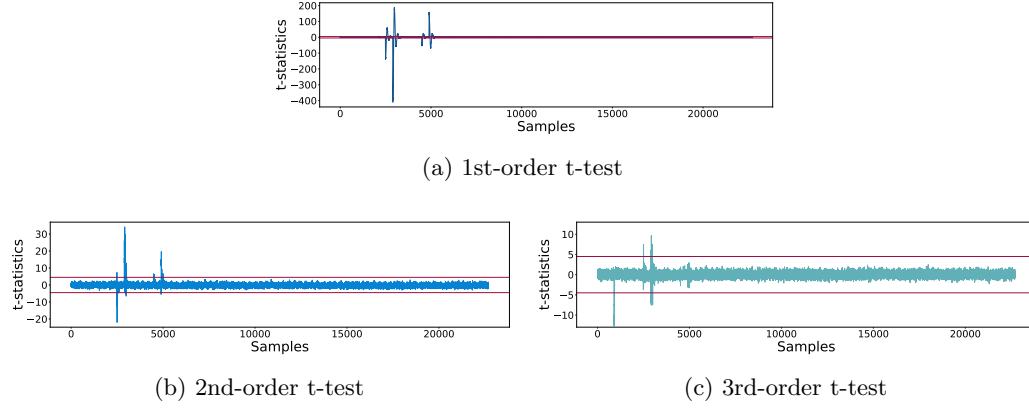


Figure A7: Non-specific leakage detection test of our second-order protected AES with 100 million traces, RNG turned off and COTG enabled.

## 8 6 Univariate T-test with RNG off/COTG off

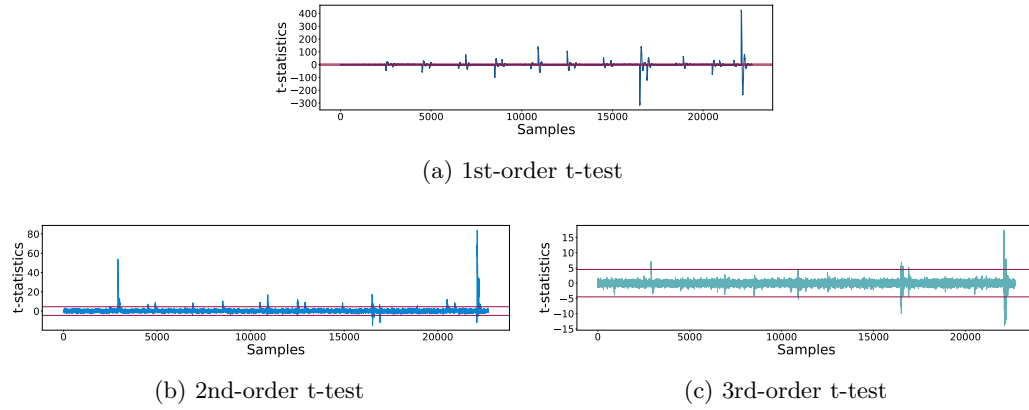
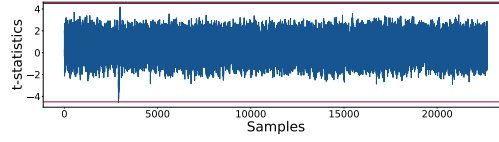
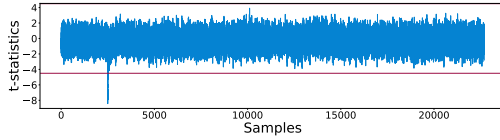


Figure A8: Non-specific leakage detection test of our second-order protected AES with 9 million traces, RNG turned off and COTG disabled.

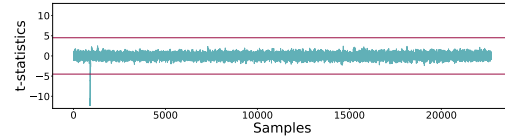
## 7 Univariate T-test with RNG on, constant key shares



(a) 1st-order t-test



(b) 2nd-order t-test



(c) 3rd-order t-test

Figure A9: Non-specific leakage detection test of our second-order protected AES with 100 million traces and RNG turned on. The three shares of the key are set to 0 such that no refreshing happens in AddRoundKey. The guards are instantiated correctly.

## 10 8 2nd-order bivariate T-test with RNG on

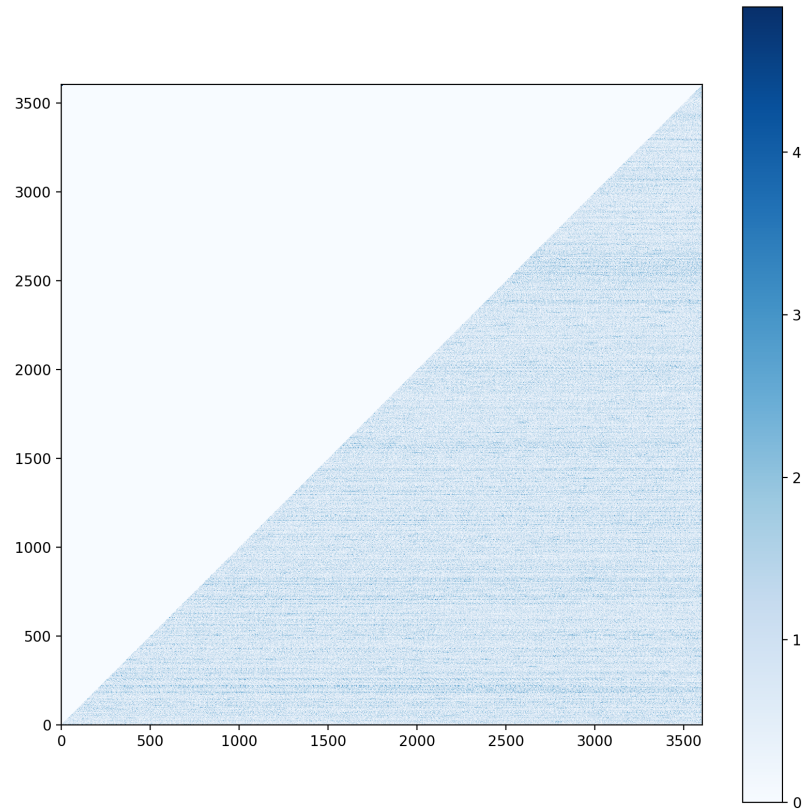


Figure A10: Non-specific bivariate leakage detection test on approx. the first two rounds of our second-order protected AES with 10 million traces and RNG turned on.



## 11 9 2nd-order bivariate T-test with RNG off/COTG off

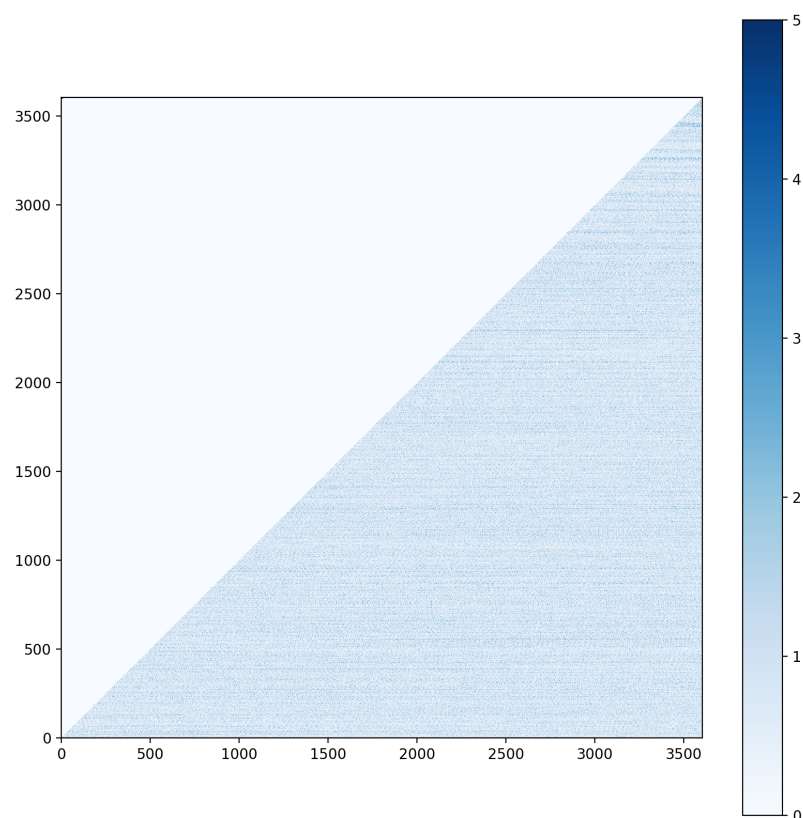


Figure A11: Non-specific bivariate leakage detection test on approx. the first two rounds of our second-order protected AES with 4 million traces, RNG turned off and COTG turned off.

## References

- [GMK16] Hannes Groß, Stefan Mangard, and Thomas Korak. Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. In *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*, page 3. ACM, 2016.
- [MMSS19] Thorben Moos, Amir Moradi, Tobias Schneider, and François-Xavier Standaert. Glitch-resistant masking revisited or why proofs in the robust probing model are needed. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(2):256–292, 2019.