On the Limitations of Logic Locking the Approximate Circuits

ASIANHOST 2022

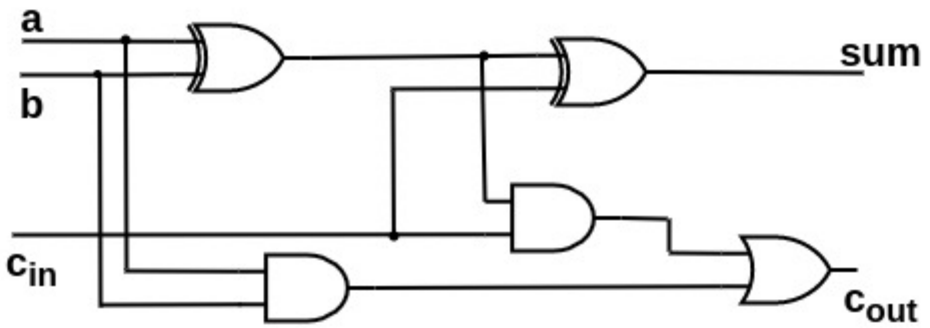
Motivation

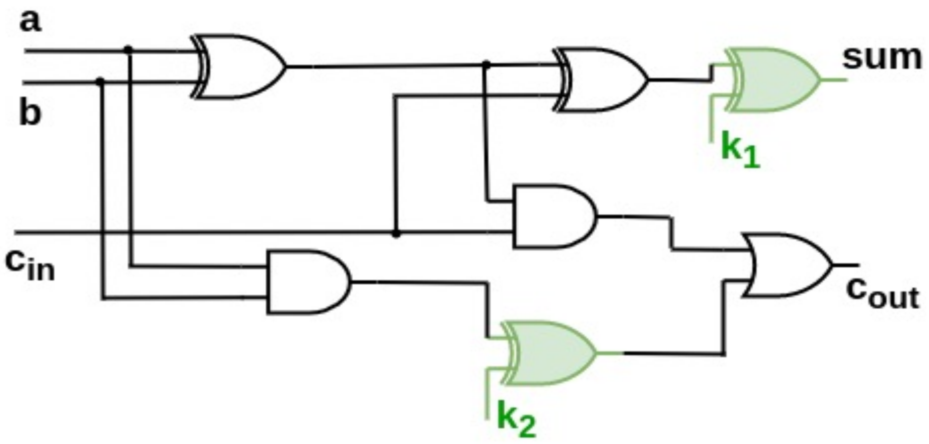
- An experiment in the direction of security of Approximate Computing (AxC).
- Benefits of AxC are discussed without considering security.
- AxC's relevance in security sensitive applications – unknown.

The security primitive under consideration is logic locking.

Logic Locking

- A gate level design obfuscation technique.
- Used as a countermeasure against supply chain attacks such as counterfeiting and overbuilding.
- Additional gates are inserted into the design, controlled by a secret key stored in tamper-proof memory.





Approximate Circuits

- AxC adds accuracy a new dimension into the design space.
- We opted for AxC arithmetic circuits for evaluation (from Prof.Han’s survey).
- The AxC arithmetic circuits can be divided into error rate and error magnitude category.

Adversarial Approach

For a circuit C, the Boolean expression C_f implements such that C= $C_{f.}$

AxC for a C will implement a circuit $\tilde{C}_f$ such that $\tilde{C}_f \approx C$.

If $\tilde{C}_k$ is the locked instance of AxC for a key k*, then for a partially correct key $\tilde{k}$, the circuit $\tilde{C}_{\tilde{k}} \approx \tilde{C}_f$?

If yes, what is the behavior of $\tilde{k}$?

SAT Attack

Boolean Satisfiability: Determining if there exists a solution for a Boolean function. SAT attack is based on this algorithm.

- A popular known attack against logic locking.
- Finds the key by eliminating the distinguishable input patterns (DIP).

- In recent years, logic locking is hardened by decreasing the DIPs for an incorrect key. This has led to low output corruption problem.

SAT-resilient locking on AxC

- Anti-SAT, SARLock, CAS Lock, SFLL are not suitable in approximate world.
- In an exhaustive simulation, for an incorrect key, the primitive circuits produced as good results as (fractionally lower) correctly deciphered circuits.
- On neural network inference, for an incorrect key, the results were identical to deciphered ones.

Random logic locking vs AxC

- Hence, we investigated random logic locking on AxC primitives.

- For investigation, we simulated the primitive AxC circuits exhaustively with different partially correct keys.
- We generated partially correct keys of various hamming distance to the secret key.
- For each hamming distance, many partially correct keys were generated.

AxC primitive circuits

- For adders, we used almost correct adder (ACA), error tolerant adder II (ETA) – these are approximations in the carry chain.
- Lower part OR, and XNOR based full-adders were used in accurate RCA and CLA adders to produce approximations in LSBs.
- We shall refer them as LOARCA/LOACLA and XRCA/XCLA.
- For approximations in multiplications, we used underdesigned multiplier (UDM) – approximation in partial product generation, and broken array multiplier (BAM) – approximation in the summation tree of array multiplier (AM).

AxC primitive circuits

- Critical path approximations produce fewer errors but significant ones. They are error rate (ER)-optimized.
- Lower bit approximations are normalized mean error distance (NMED)-optimized.
- Multipliers are complex structures to be easily categorized.

Observation concerning locking

- NMED-optimized adder is prone to adversarial model discussed earlier.
- UDM is more susceptible to the adversarial model in our experiment than BAM.
- The incorrect keys introduce higher magnitude errors for LSB approximations.
- We deduce that adversarial model is linked closely to NMED than ER.

Error characteristics

XOR/XNOR Locking (32 key-gates):

NMED	HD=0	HD=1	HD=2	HD=3	HD=4	HD=6
RCA	0	4.10E-2	7.83E-2	9.74E-2	1.18E-1	1.47E-1
LOARCA	2.20E-5	5.38E-2	8.51E-2	1.03E-1	1.12E-1	1.20E-1
ACA	3.96E-3	3.91E-2	7.10E-2	9.08E-2	1.10E-1	1.50E-1
ETA	1.68E-2	7.04E-2	1.22E-1	1.56E-1	1.81E-1	2.63E-1

AND/OR Locking (32 key-gates):

NMED	HD=0	HD=1	HD=2	HD=3	HD=4	HD=6
RCA	0	2.55E-2	5.56E-2	7.55E-2	7.55E-2	1.25E-1
LOARCA	2.20E-5	2.87E-2	5.48E-2	7.67E-2	1.20E-1	1.56E-1
ACA	3.96E-3	9.99E-3	1.59E-2	2.08E-2	2.61E-2	3.70E-2
ETA	1.68E-2	3.38E-2	4.85E-2	6.30E-2	7.60E-2	1.13E-1

>

Concerning

HD=0 represents the functional design.

Error characteristics

XOR/XNOR Locking (32 key-gates):

NMED	HD=0	HD=1	HD=2	HD=3	HD=4	HD=6
AM	0	2.24E-2	4.12E-2	6.04E-2	7.90E-2	1.05E-1
UDM	5.80E-2	9.53E-2	1.20E-1	1.33E-1	1.26E-1	1.56E-1
BAM	8.43E-3	2.93E-2	4.94E-2	6.83E-2	8.62E-2	1.20E-1

>

AND/OR Locking (32 key-gates):

NMED	HD=0	HD=1	HD=2	HD=3	HD=4	HD=6
AM	0	7.30E-3	1.09E-2	1.44E-2	1.79E-2	2.48E-2
UDM	5.80E-2	6.03E-2	6.22E-2	6.32E-2	6.57E-2	6.71E-2
BAM	8.43E-3	2.15E-2	3.17E-2	4.12E-2	4.98E-2	6.00E-2

Concerning

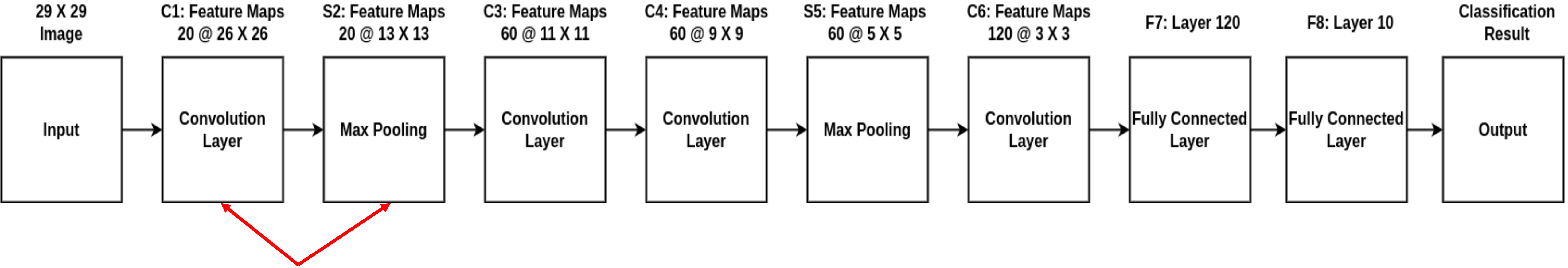
>

HD=0 represents the functional design.

Discussion

- We observed similar results for different lengths of key-gates and different configurations of adders/multipliers.
- When dissected to an individual incorrect key of low HD, for some keys, the circuits produced identical or better results.
- We term this as pathological behavior.
- To understand how this would translate to real-world application, we put the locked instances in neural network inference.

Locked instances in CNN



- The marked layers are implemented in Hardware. Rest in software.
- The network was trained for accurate adders and approximate ETA.
- We did not train the network for locked ETA to simulate the adversarial setting.

Results on CNN

- The validation accuracy of trained network for accurate adder is 92.6%.

XOR/XNOR Locking	**Partial key**	**HD**	**NMED**	**ER%**	**Class. Accurcy %**
-	-	0	2.47e-04	0.76	91.4
	0x8a90b5bd	1	2.50e-04	1.30	92.0
	0x8a90b5be	1	3.15e-04	6.91	91.0
	0x8a90b5b8	1	1.24e-01	49.81	8.6
	0x8a90b5ac	1	2.47e-04	61.62	91.4
	0x8a90b4bc	1	7.96e-03	12.99	45
	0x8a90b5bf	2	3.16e-04	7.20	91.2
	0x8a90b5ba	2	1.25e-01	53.09	8.6
	0x8a90b5ba	3	1.25e-01	53.21	8.6

Conclusion

- AxC circuits need protection against supply chain attacks such as counterfeiting and overbuilding.
- Known logic locking techniques are not a feasible solution in the approximate world.
- Noisy key obtained from side channel analysis may lead to correct deciphering of AxC circuits.

Acknowledgment

This work is partially supported by the European Union Horizon 2020 Program under the EVEREST project (grant agreement no 957269).