Automatic Proofs of Correctness and Security for Masked Programs

François Dupressoir
IMDEA Software Institute, Madrid, Spain

Joint work with
Gilles Barthe Sonia Belaid Benjamin Grégoire
Pierre-Alain Fouque Pierre-Yves Strub

CHES 2014 Rump Session

A first solution and a challenge

- Security in t-threshold probing model is non-interference for any t intermediate values
  - Non-interference t intermediate values is a standard program verification model.
  - Easily handled by EasyCrypt.
- Non-interference for any t intermediate values is hard.
  - Size of programs grows with masking order
  - Number of sets to test explodes as masking order grows

Our Solution: Large observation sets

- Given a set of intermediate values known to be safe, efficiently extend it as much a possible.
- Recursively check t non-interference with variables not captured.
- Recursively check t non-interference for sets that straddle both subsets.
- Still exponential, but pretty good in practice.

Set of sets of observations to consider can be cut further by partial composition results.

Reference	Target	# tuples	Result	Complexity	
				# sets	time
First Order Masking					
RP-CHES10	multiplication	13	secure ✓	7	ε
CPRR-FSE13	Sbox (Algo 4)	63	secure ✓	17	ε
CPRR-FSE13	full AES (Algo 4)	17,206	secure ✓	77	16.560s
Second Order Masking					
SP-RSA06	Sbox	1M	secure ✓	215,430	3.068s
RP-CHES10	multiplication	435	secure ✓	92	0.001s
RP-CHES10	Sbox	7,140	2 flaws ($d = 1$)		
RP-CHES10	key sched. (CPRR13)	23M	secure ✓	771,263	340,745.292s
CPRR-FSE13	4 rounds of AES (Algo 4)	119M	secure ✓	215,762	3,152.904s
Third Order Masking					
RP-CHES10	multiplication	24,804	secure ✓	1,410	0.041s
CPRR-FSE13	Sbox (Algo 4)	4M	secure ✓	33,075	15.200s
CPRR-FSE13	Sbox (Algo 5)	4M	secure ✓	39,613	25.294s
Fourth Order Masking					
SP-RSA06	Sbox	4G	4* flaws ($d = 3$)	35,895,437	22,119.608
RP-CHES10	multiplication	2M	secure ✓	33,322	1.634s
CPRR-FSE13	Sbox (Algo 4)	2M	secure ✓	3,343,587	4368s
Fifth Order Masking					
RP-CHES10	multiplication	216M	secure ✓	856,147	69.572s
CPRR-FSE13	Sbox (Algo 4)	1,535G	secure ✓		