Kacper Zujko

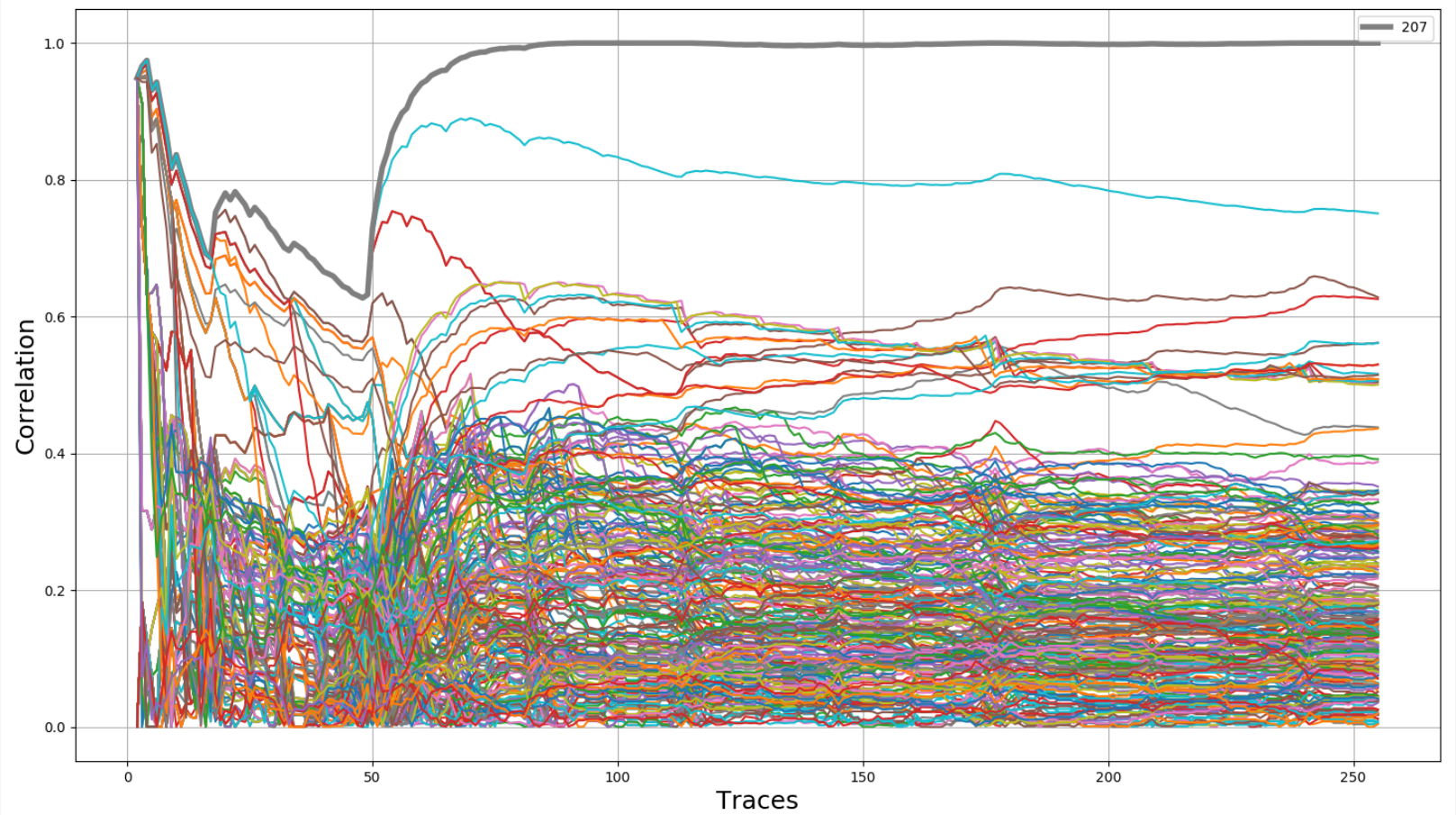
Military University of Technology

18 June 2019

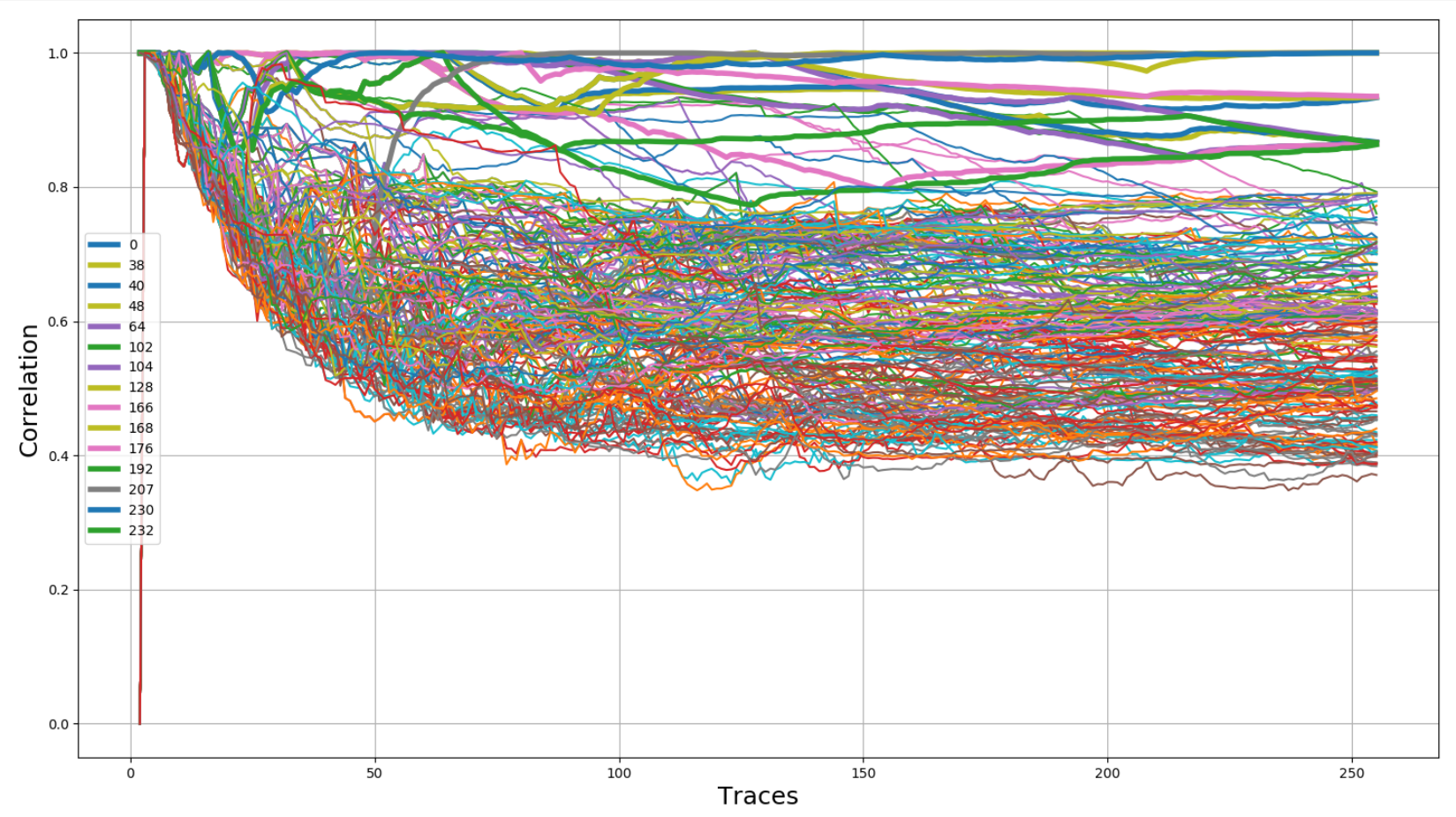
Some topics

- key distribution, PKI (centralized and decentralized)
- lattice-based crypto
- hash-based crypto
- side channel analysis (power, EM, cashe)
- other exploitation and protecting methods

Exact point, XMSS SHA-256 PRNG (addition)



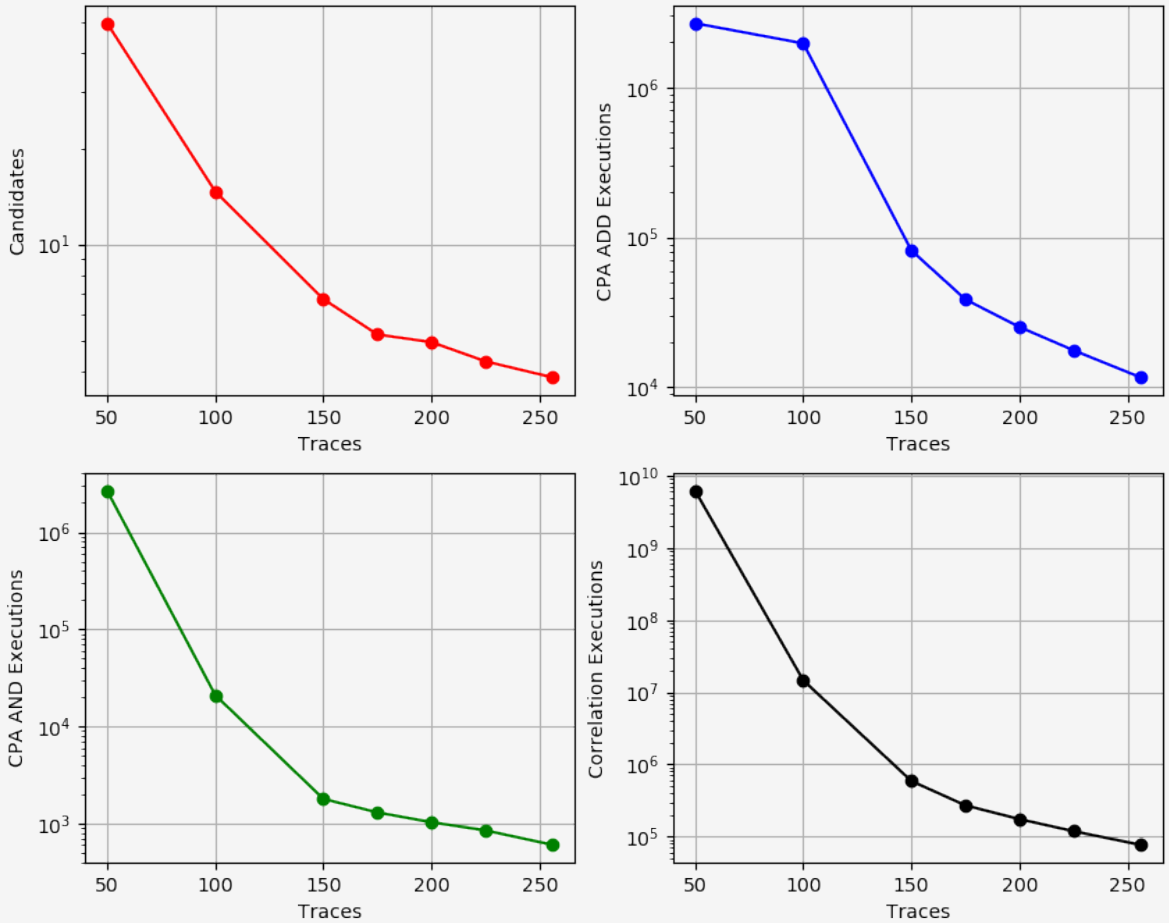
500 points, XMSS SHA-256 PRNG (addition)



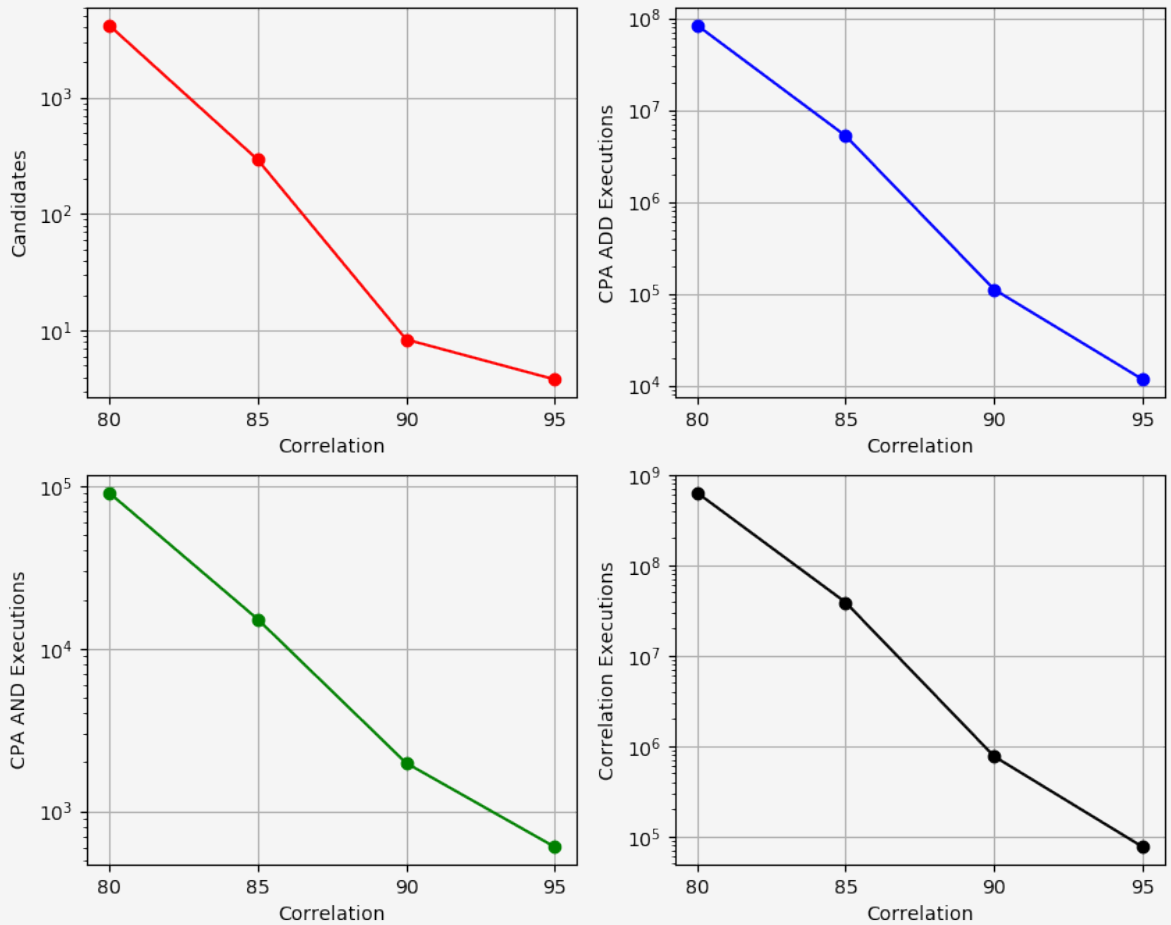
Small improving for sha256(i) $\longrightarrow$ i

1. Exploit Σ_0 and Σ_1.
2. Divide strategy (CH and MAJ).
3. Deal with no/small differences.

Exact point


Candidates
10^1
50
100
150
200
250
Traces
CPA ADD Executions
10^6
10^5
10^4
50
100
150
200
250
Traces
CPA AND Executions
10^6
10^5
10^4
10^3
50
100
150
200
250
Traces
Correlation Executions
10^{10}
10^9
10^8
10^7
10^6
10^5
50
100
150
200
250
Traces

Exact point


Candidates
10^3
10^2
10^1
80
85
90
95
Correlation
CPA ADD Executions
10^8
10^7
10^6
10^5
10^4
80
85
90
95
Correlation
CPA AND Executions
10^5
10^4
10^3
80
85
90
95
Correlation
Correlation Executions
10^9
10^8
10^7
10^6
10^5
80
85
90
95
Correlation

500 points, 256 traces

Candidates	CPA ADD	CPA AND	Correlation Verification
103,72	17 006 077	41 607	255 588 774