Walsh Spectrum Analysis on Sampling Distributions

Fast Software Encryption - FSE 2017 (Rump Session)

Speaker: Yi LU (EPFL, Ph.D.)

Selmer Center for Secure and Reliable Communications,

Department of Informatics,

University of Bergen (UiB),

Norway

Dr.Yi.Lu@ieee.org

Walsh Spectrum Analysis on Sampling Distributions

- In this talk, we formulate and introduce the problem to be studied in crypto community, after more than a decade's joint academia collaborations among EPFL, NTU, UCL, Chinese Academy of Sciences, UiB, just to name a few.
- Part of results is considered suitable for submission to the nature journal to benefit both scientific and engineering communities broadly.

Walsh Spectrum Analysis on Sampling Distributions

- Currently, we are seeking industrial partnerships, esp. in computing and communication industries.
- The problem is called “Walsh spectrum analysis on sampling distributions”. It initiates the study of finding the largest and/or significantly large Walsh coefficients and the index positions of an unknown distribution by sampling.

Walsh Spectrum Analysis on Sampling Distributions

- We have uploaded our first dataset as the experimental analysis subject to IEEE data port (http://ieee-dataport.org).
- We hope and are trying to make it publicly available on IACR's website.

Walsh Spectrum Analysis on Sampling Distributions

- The uploaded dataset stores a random sampling distribution with cardinality of support 2^32.
- Specifically, the source generator is fixed as a symmetric-key cryptographic function with 64-bit input and 32-bit output. A total of 2^34 randomly chosen inputs are used to produce the sampling distribution as the dataset.

Walsh Spectrum Analysis on Sampling Distributions

- The integer-valued sampling distribution is formatted as 2^32 entries, and each entry occupies one byte in storage.
- For details, see ieee-dataport.org/documents/walsh-spectrum-analysis-sampling-distributions

Walsh Spectrum Analysis on Sampling Distributions

References:

- doi.org/10.1109/isit.2015.7282921
- arxiv:1504.07648v1
- arxiv:1508.06336
- eprint.iacr.org/2016/419
- ieeexplore.ieee.org/document/7821757

Thank you for your attention!