Standardization Robustness

Distinguishers/Key recovery for FFX-3.1 and FEA

Orr Dunkelman[1], Abhishek Kumar[2], **Eran Lambooij**[1] and Somitra Kumar Sanadhya[2]

[1]University of Haifa, Israel

[2]IIT Ropar, India

ISO 3103

Figure: A broken tea cup

ISO 3591

Figure: A broken wine glass

FPE

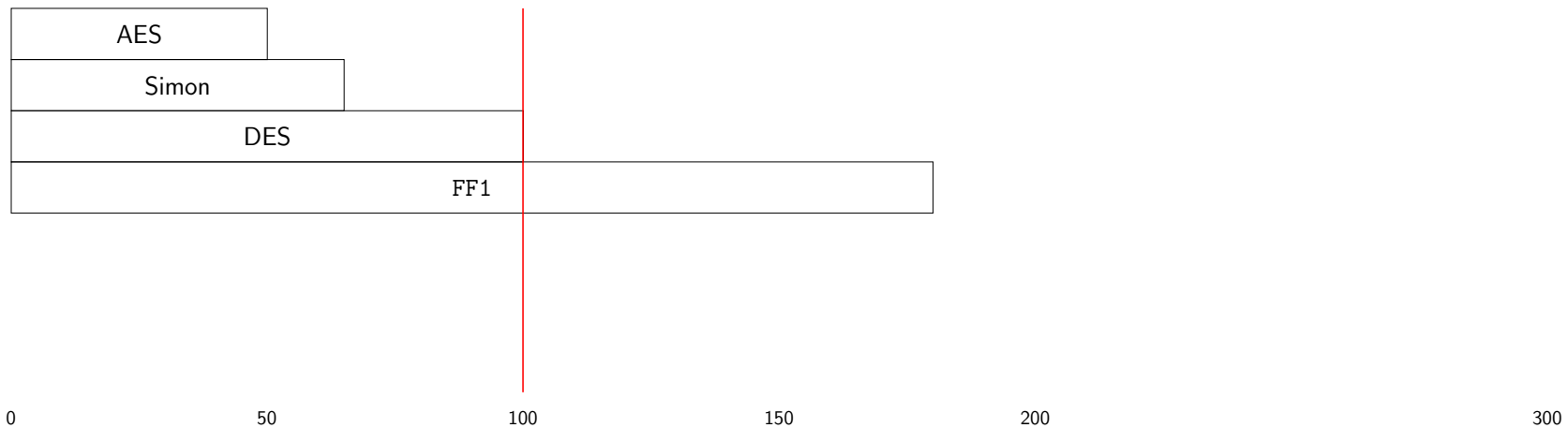
Figure: We protect your data!!!

FPE

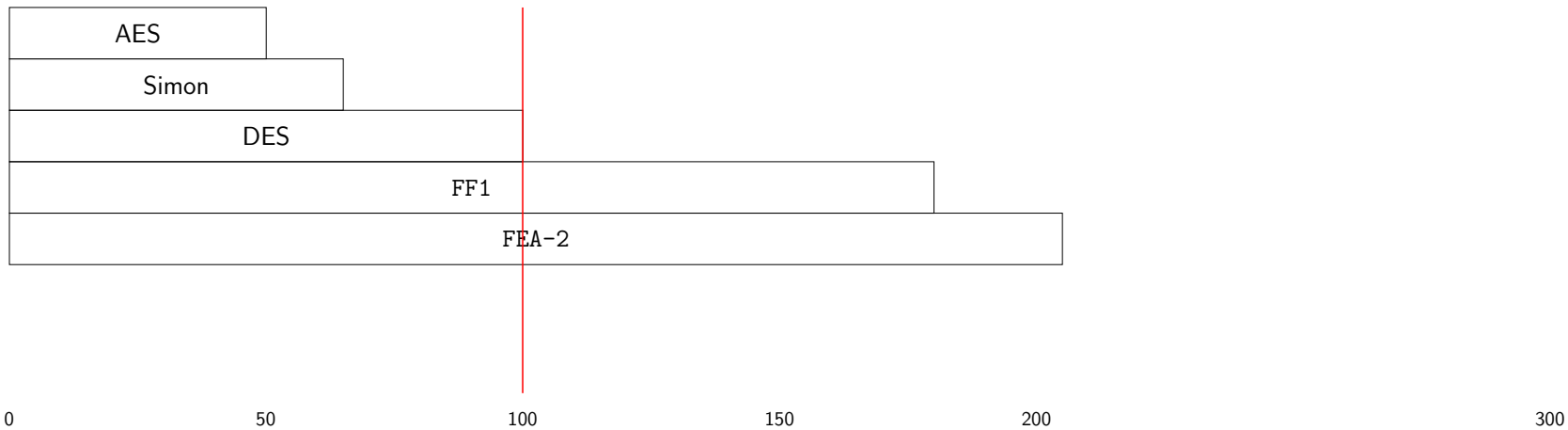
Figure: NIST SP-800-38G & TTAK.KO-12.0275

Distinguishers on FFX & FEA

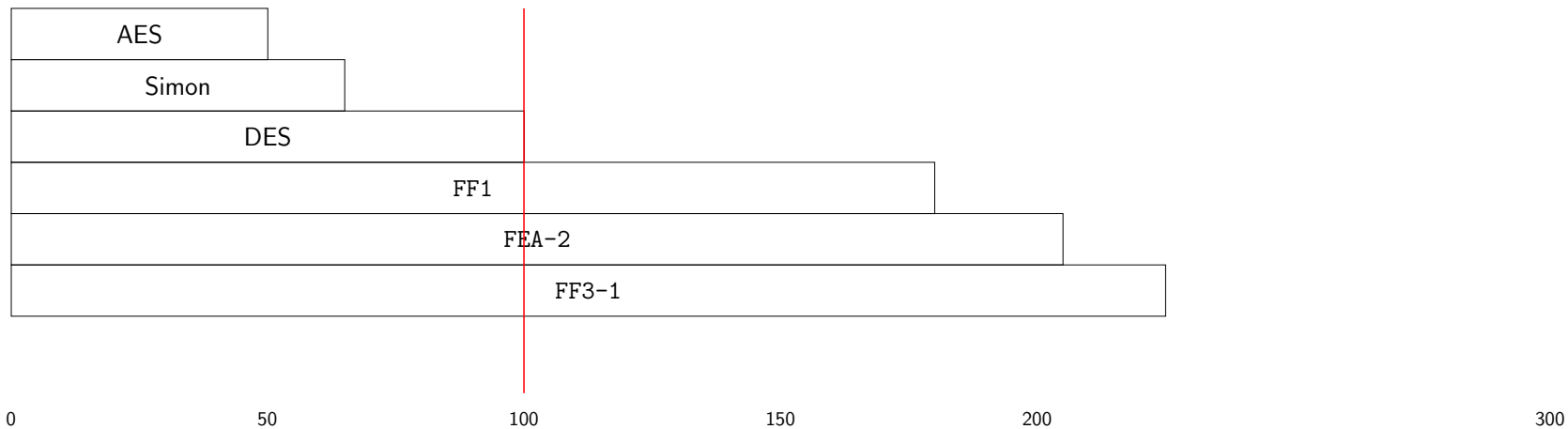
Distinguishers on FFX & FEA



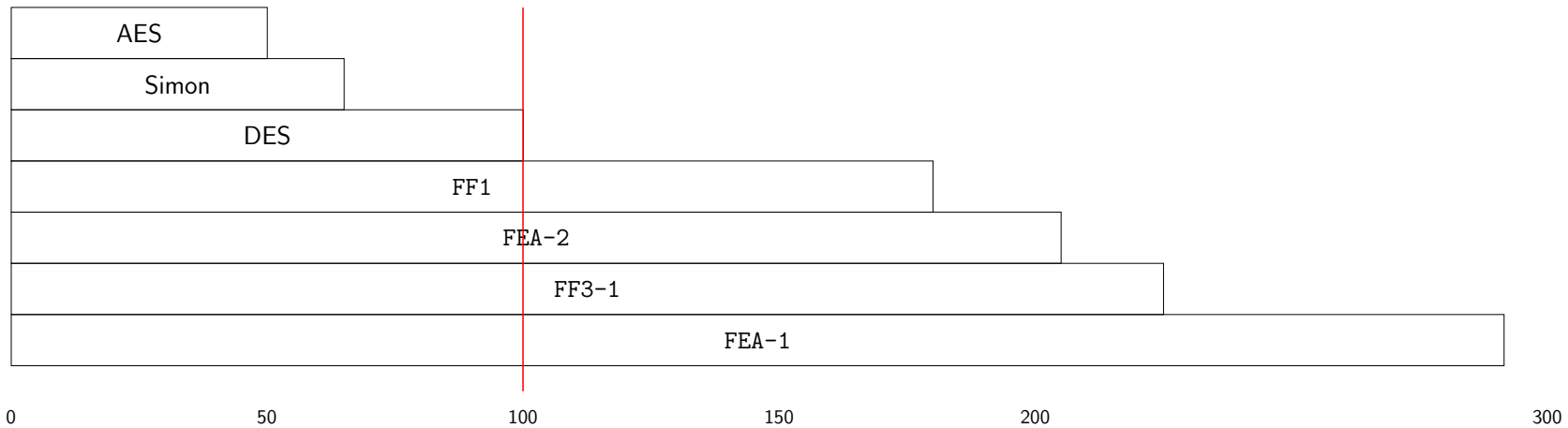
Distinguishers on FFX & FEA



Distinguishers on FFX & FEA



Distinguishers on FFX & FEA



Is it practical?

2^{36} time and 2^{32} data.[1].

[1] For the full round distinguisher on `FEA-1` with a 128 bit key

e-print coming soon!