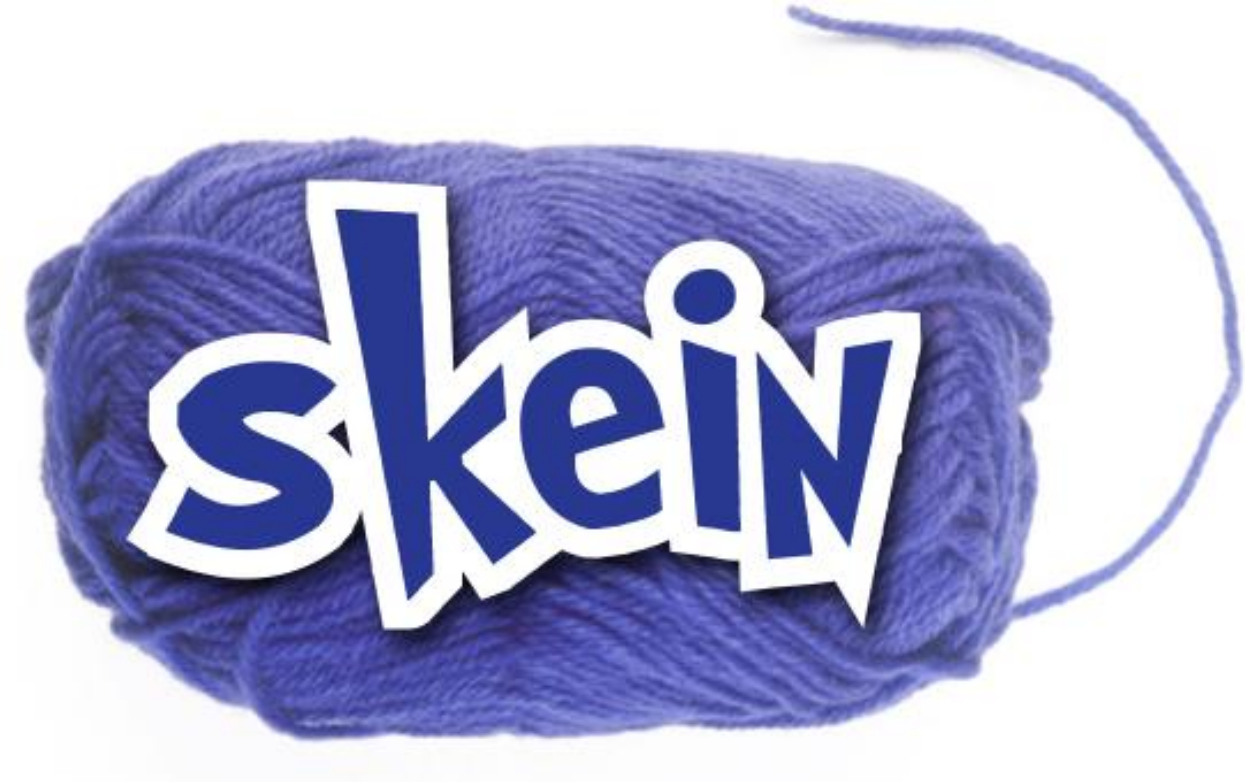
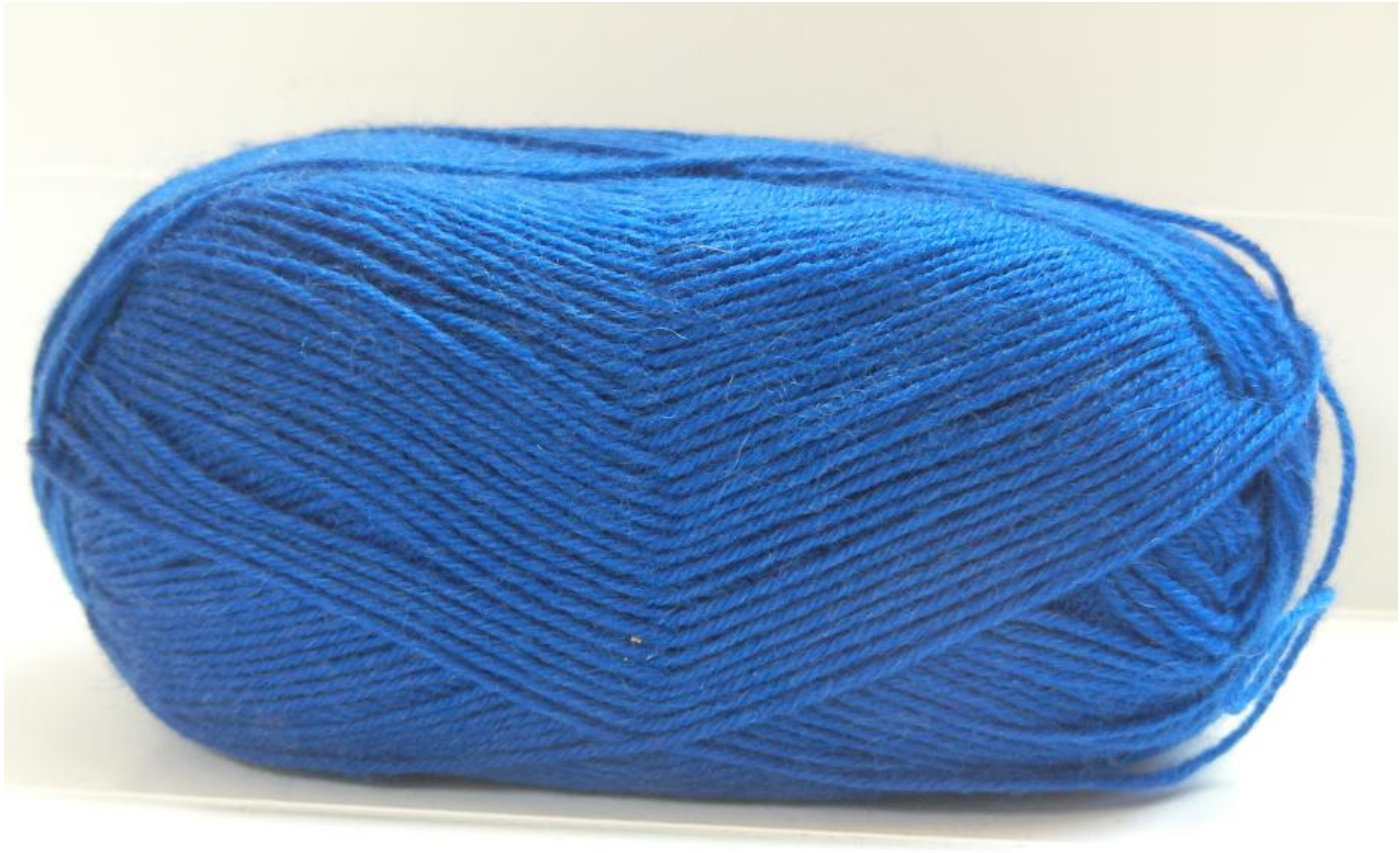
Cryptanalysis of



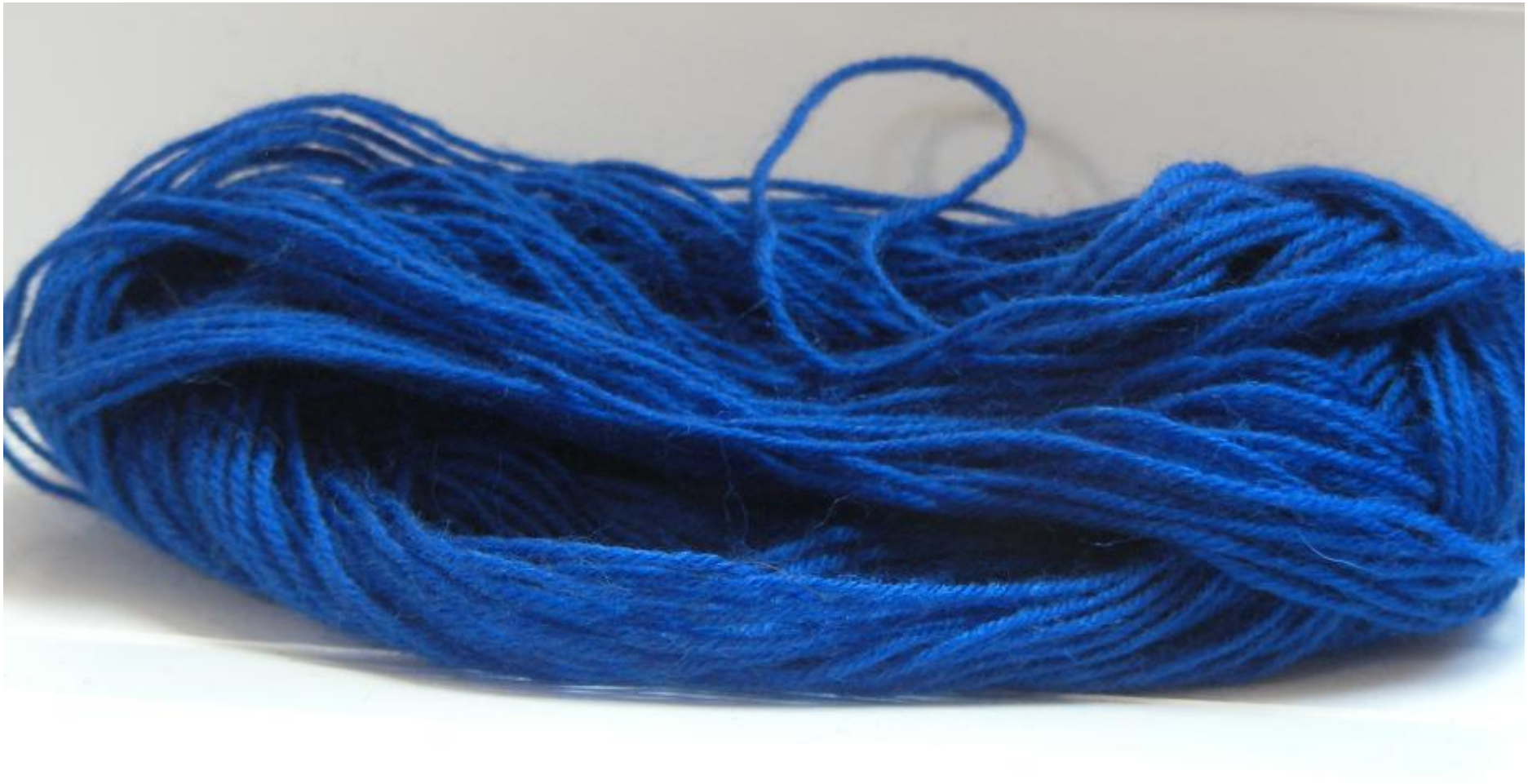
Daniel J. Bernstein and Tanja Lange

Skein with full 72 rounds



Self-similarity under rotational attack

Unravelling: Skein under brute-force attack

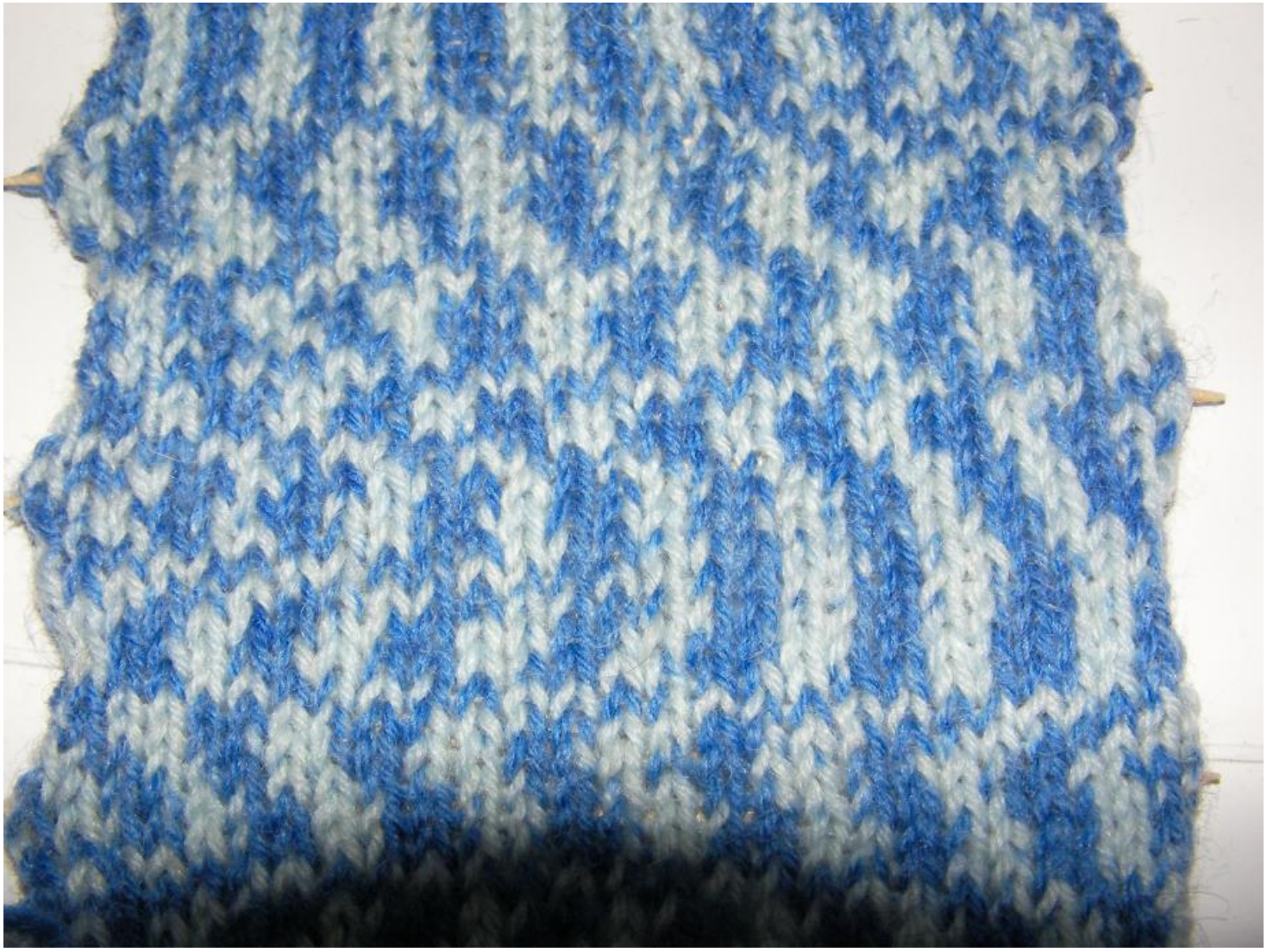


Linearization attack

- Introducing alternating bit patterns into Skein ...

Linearization attack

- . . . produces clear patterns in the output:



Methodology and tools: The attack in progress

The attack can be performed in real time. (Video on demand.)

Analyzing propagation of one-bit differentials

Conclusions

- Skein is soft and succumbs to brute force.
- Skein has been successfully linearized.
- Skein has clear output patterns.

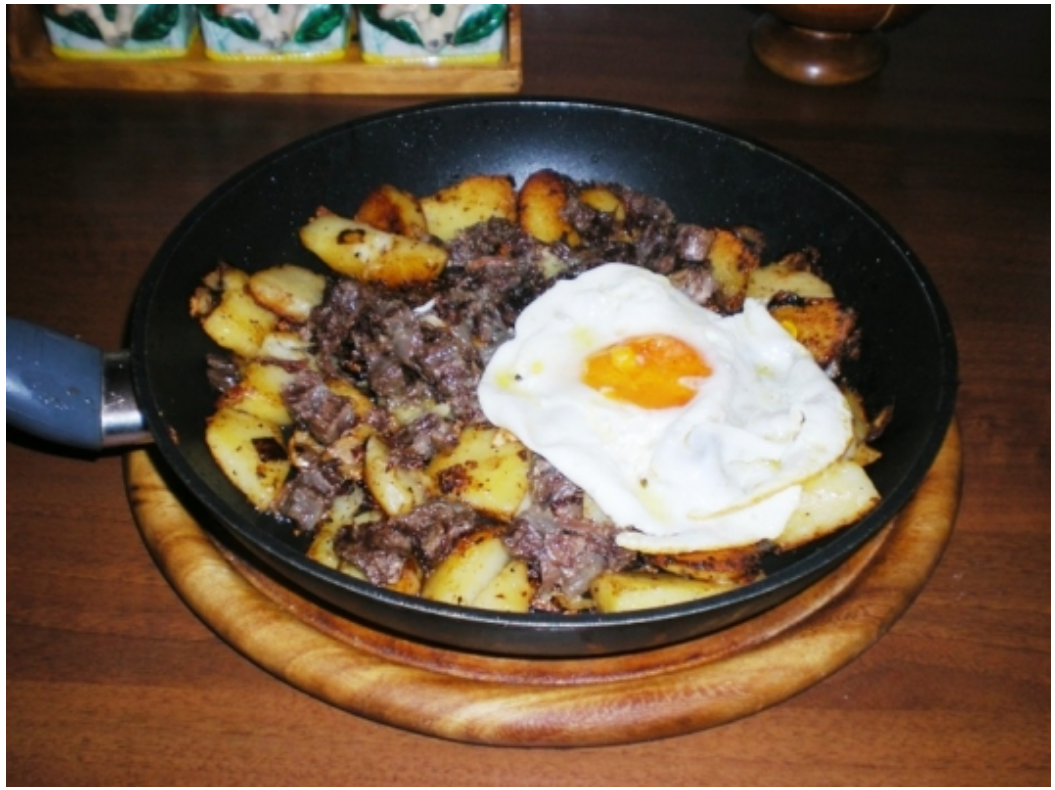
Conclusions

- Skein is soft and succumbs to brute force.
- Skein has been successfully linearized.
- Skein has clear output patterns.

- Skein is easily distinguishable from a random oracle.

Outlook

Outlook



Meat-in-the-middle attack on Grøstl