Distinguisher on reduced-round GIMLI

Mike Hamburg
Rambus Cryptography Research

What is Gimli?

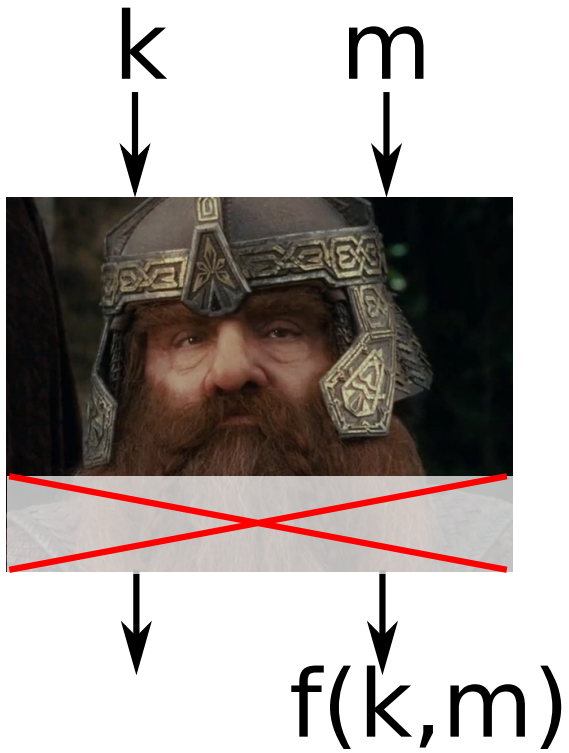
- Lightweight 384-bit permutation
- Designed for cross-platform performance
- Talk tomorrow

GIMLI

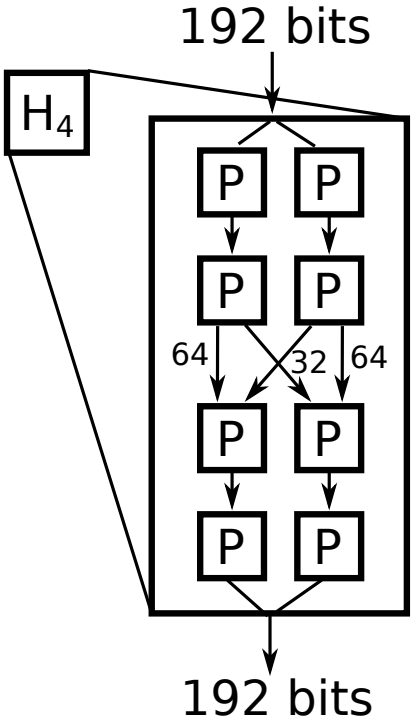
Distinguisher

(tested and works with reduced word size)

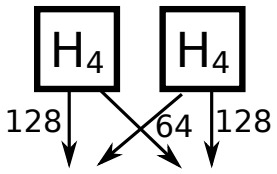
Breaks toy PRF with (15.5, 19.5, 22.5)-round GIMLI with data in sideways order with ~(2^{64}, 2^{128}, 2^{140}) effort



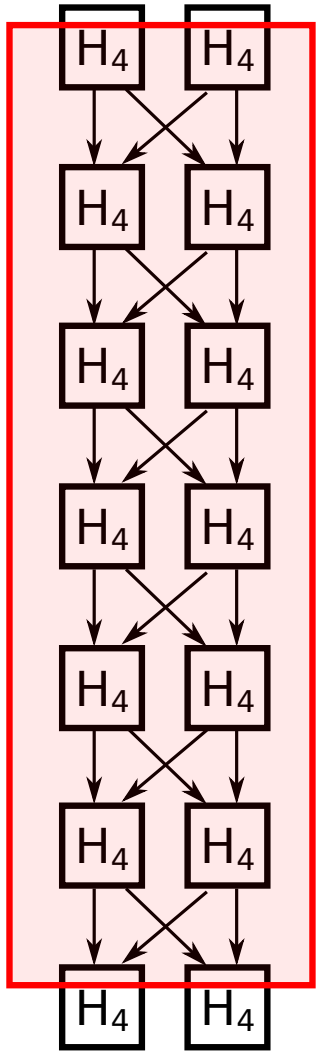
Structure of GIMLI



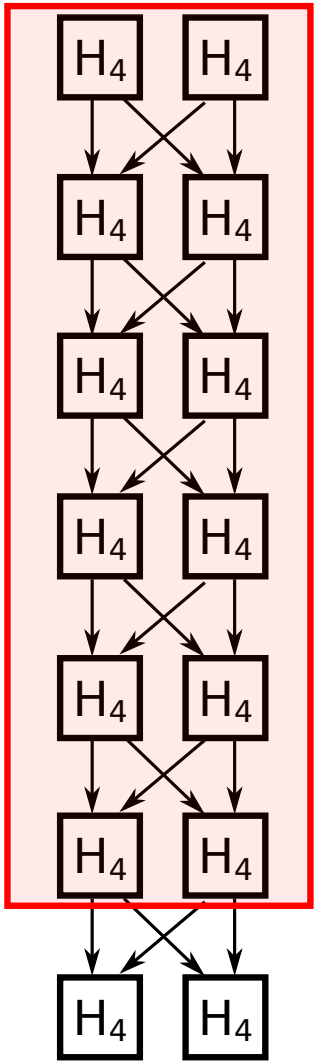
4 rounds:



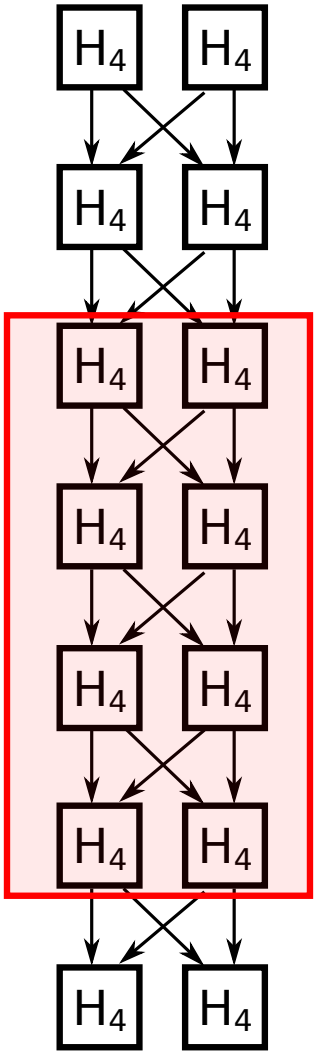
Full GIMLI:
24 rounds



~2^{140} work:
23.5 (22.5) rounds



~2^{64} work:
15.5 rounds



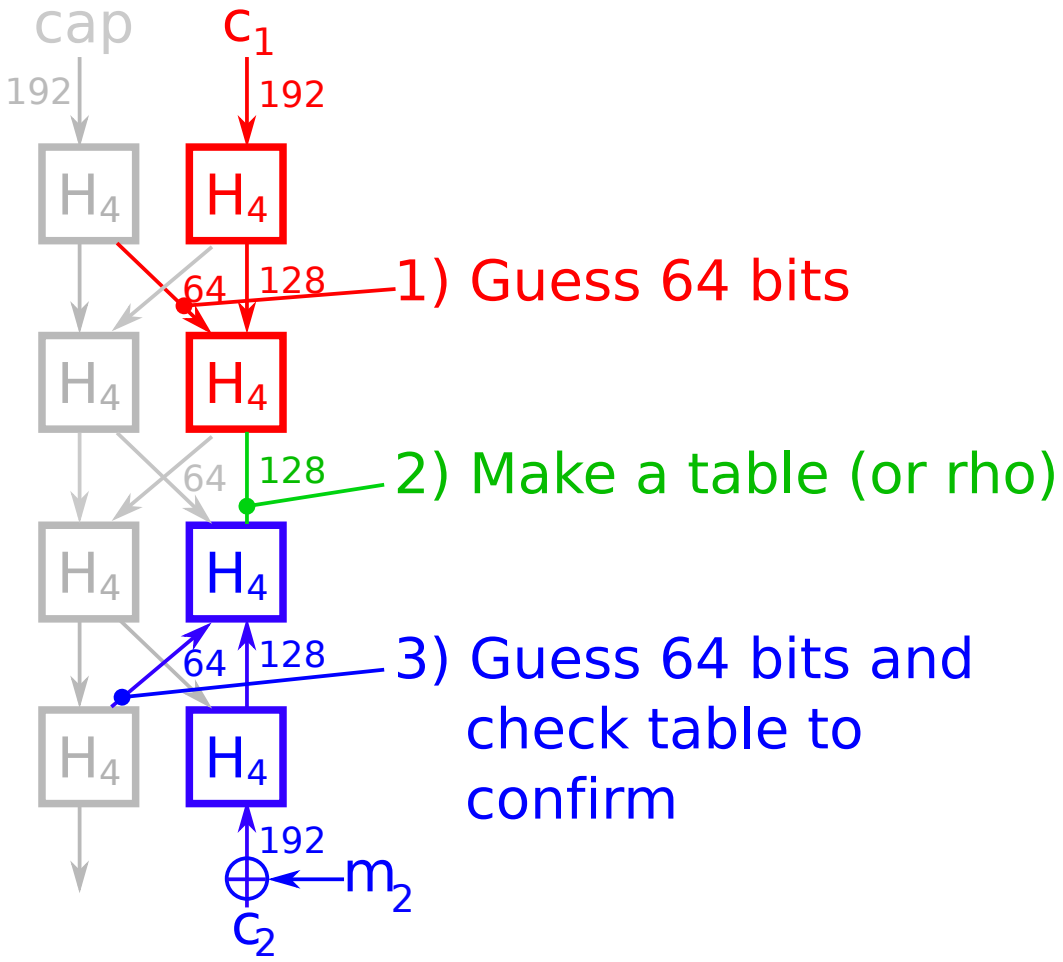
Attack on toy PRF

(15.5 round version)

Requires one known plaintext, ~2^{64} work, ~2^{72} bits memory

Or van Oorschot-Wiener: ~2^{101}/sqrt(memory)

Recovers part of key; whole key with a little more work?

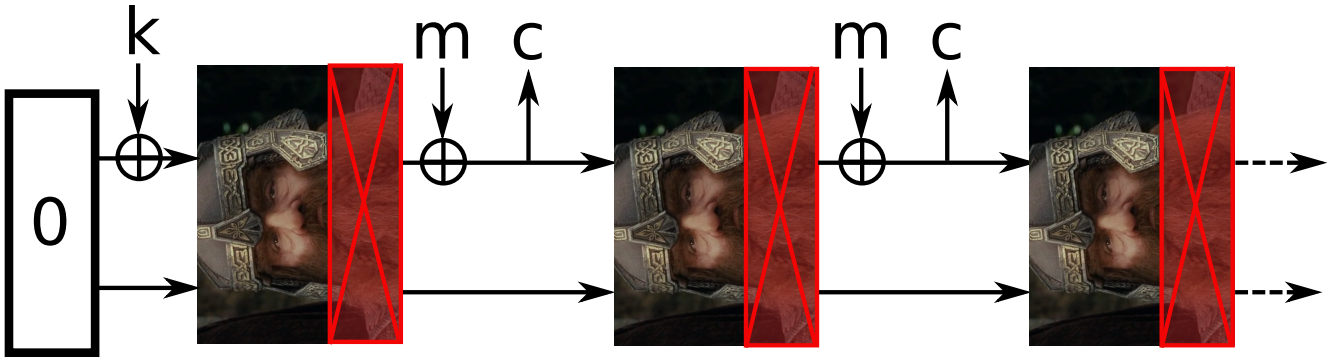


Conjectured extensions

(untested!)

Using about 2^{64} time, 2^{72} memory:

Key recovery on 15.5-round duplexing sponge (sideways)



Collision on 19.5-round hash (c=192, sideways)

Collision on 11.5-round hash (c=192, not sideways)

Conclusion

- Impractical attacks: no need to worry yet
  - But! Uses only high-level structure of GIMLI

    (also I don't really know what I'm doing)
  - Low-communication structure may be a liability
- Room for improvement??