CASA

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Breaking HALFLOOP-24

Kobe, Japan, Thursday, March 23

Marcus Dansarie, Patrick Derbez, Gregor Leander and Lukas Stennes

Swedish Defence University

Université de Rennes

RUHR UNIVERSITÄT BOCHUM

RUB

What is HALFLOOP

CASA
Cyber Security in the Age of Large-Scale Adversaries

« HALFLOOP is a parody of AES that can be summarized as "What if we take AES-128, add a tweak in the key and reduce the block size?". This paper focuses on HALFLOOP-24, which has a 24-bit block size. As one can expect it is completely broken. »

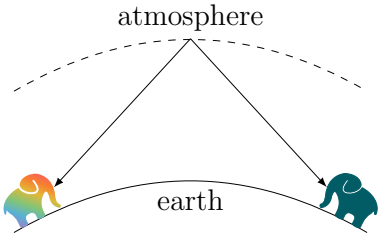
Reviewer B

Why HALFLOOP

Why HALFLOOP: High Frequency Radio

CASA
Cyber Security in the Age of Large-Scale Adversaries

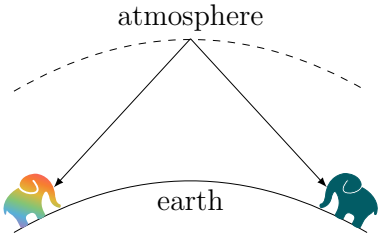
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for encrypting handshake messages (confidentiality and authentication)



Why HALFLOOP: High Frequency Radio

CASA
Cyber Security in the Age of Large-Scale Adversaries

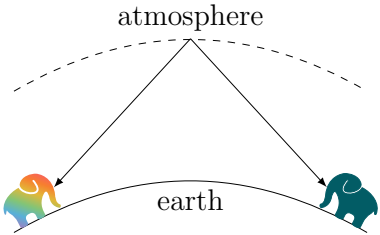
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for encrypting handshake messages (confidentiality and authentication)



Why HALFLOOP: High Frequency Radio

CASA
Cyber Security in the Age of Large-Scale Adversaries

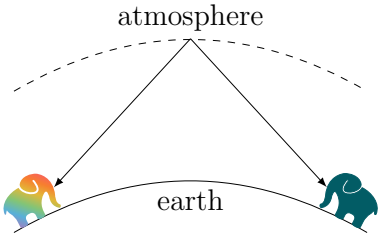
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for encrypting handshake messages (confidentiality and authentication)



Why HALFLOOP: High Frequency Radio

CASA
Cyber Security in the Age of Large-Scale Adversaries

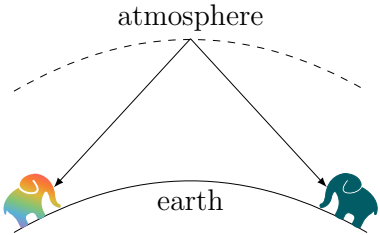
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for encrypting handshake messages (confidentiality and authentication)



Why HALFLOOP: High Frequency Radio

CASA
Cyber Security in the Age of Large-Scale Adversaries

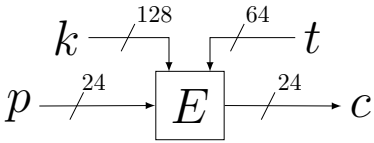
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for encrypting handshake messages (confidentiality and authentication)



Description of HALFLOOP-24

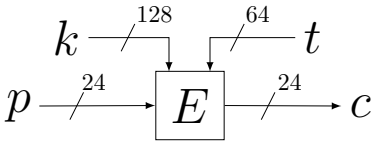
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



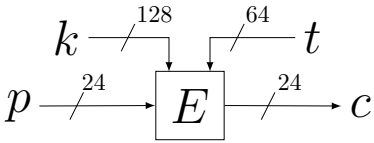
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



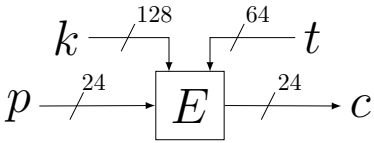
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



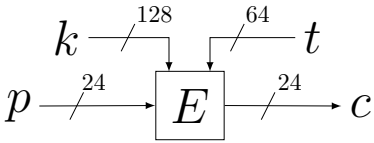
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



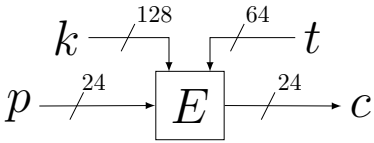
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



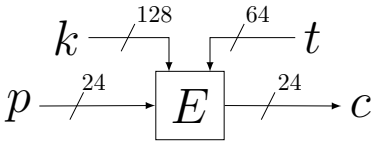
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



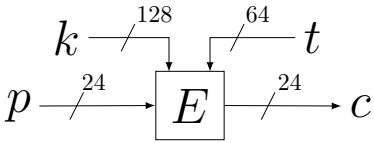
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



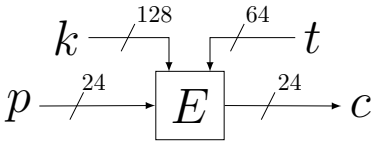
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



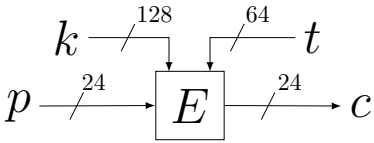
Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds

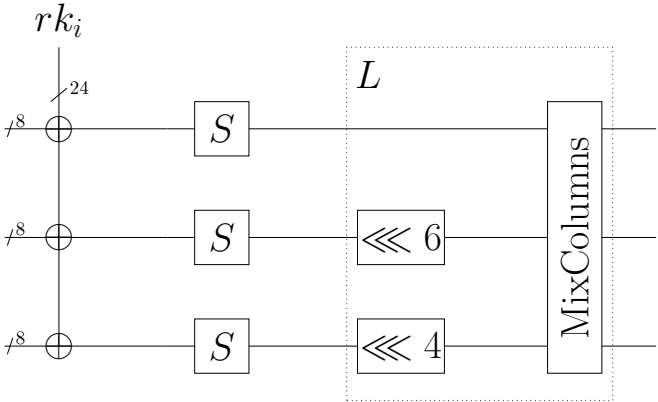


Description of HALFLOOP-24 – Big Picture

- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
  - No public cryptanalysis before
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds

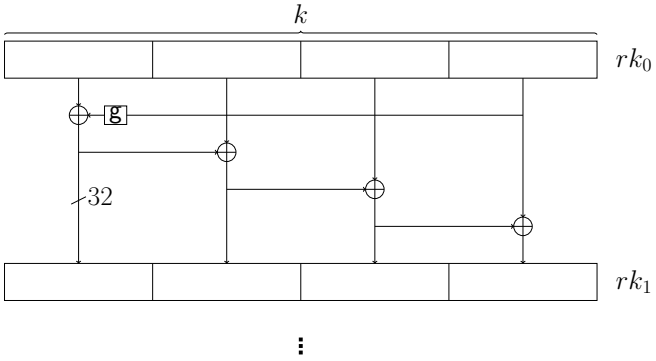


Description of HALFLOOP-24 – Round Function

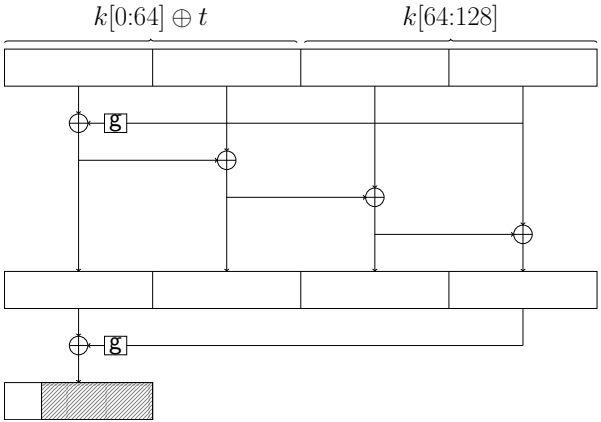


MC: multiply with $c(x) = x^2 + 2x + 9$ modulo $x^3 + 1$

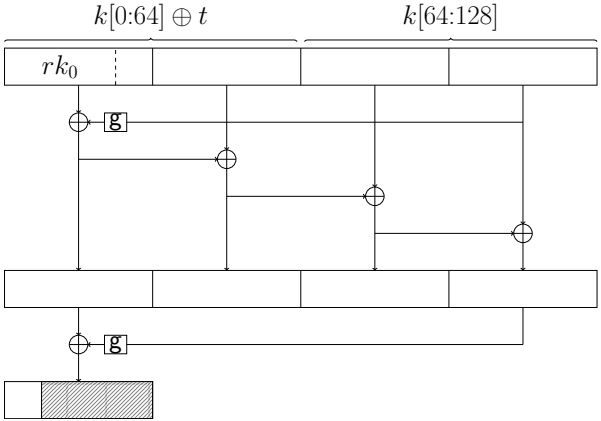
Description of HALFLOOP-24 – AES-128 Key Schedule



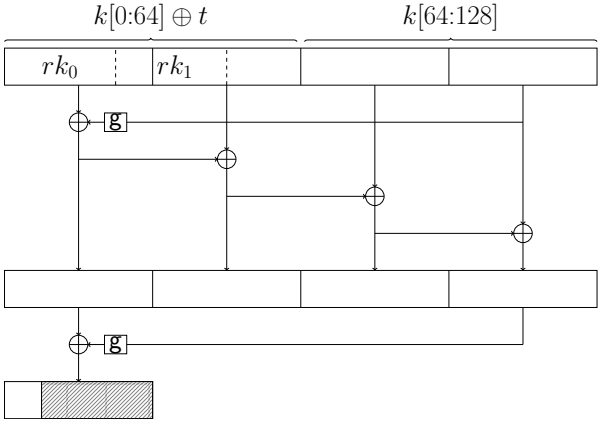
Description of HALFLOOP-24 – Key Schedule



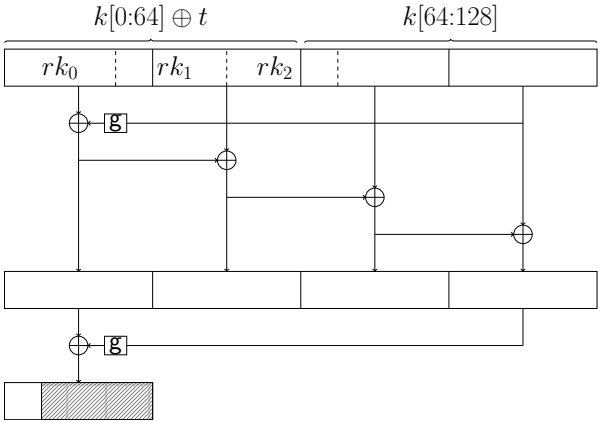
Description of HALFLOOP-24 – Key Schedule



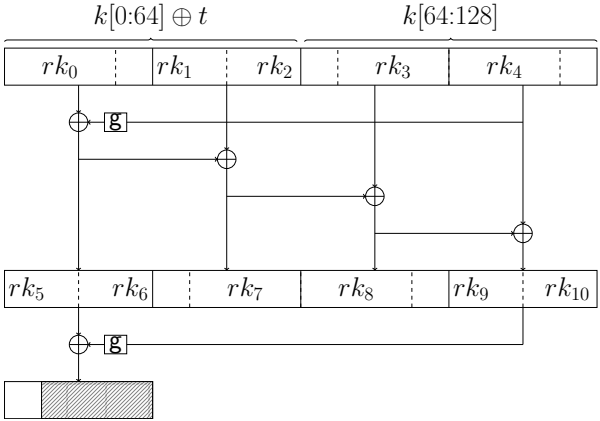
Description of HALFLOOP-24 – Key Schedule



Description of HALFLOOP-24 – Key Schedule

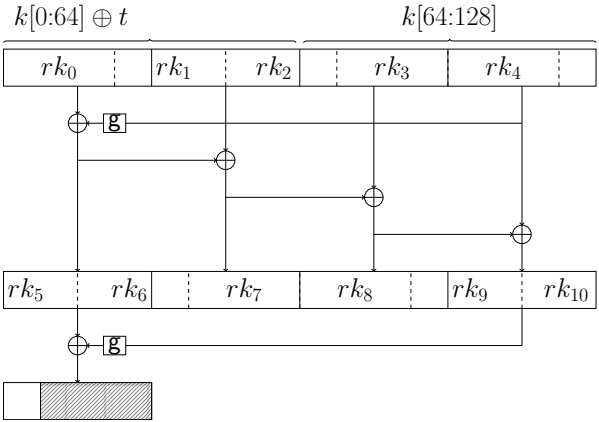


Description of HALFLOOP-24 – Key Schedule

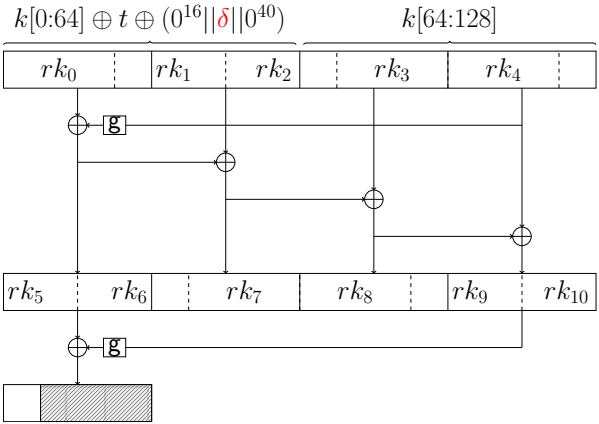


Our Attacks on HALFLOOP-24

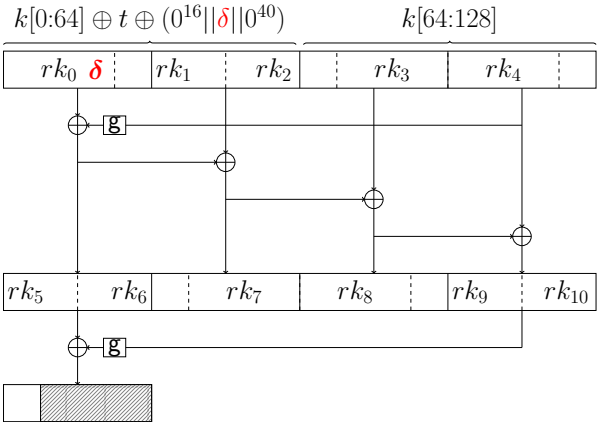
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



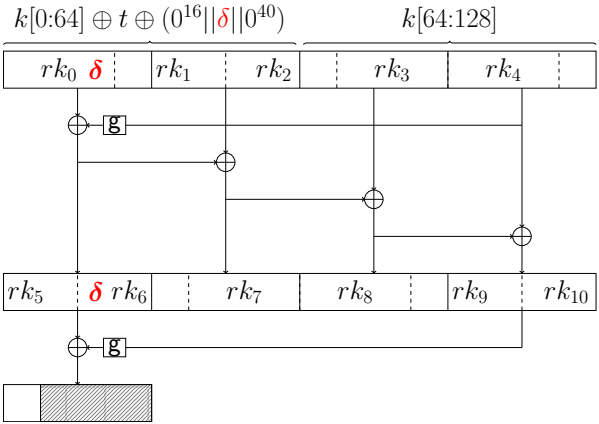
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



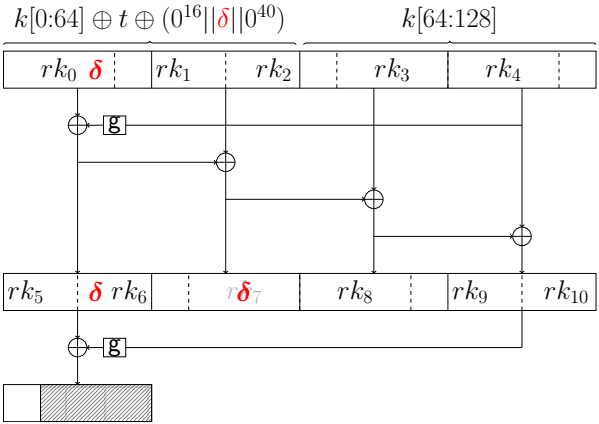
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



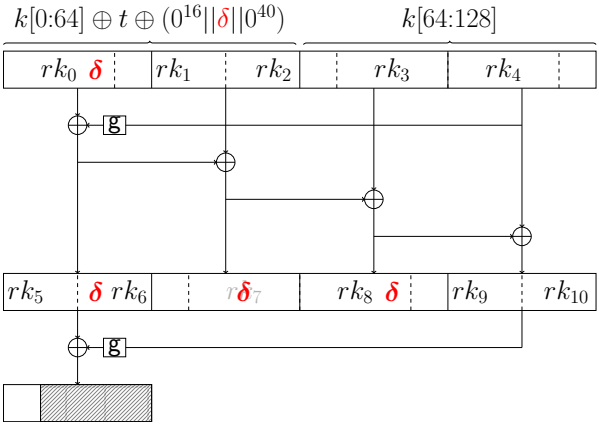
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



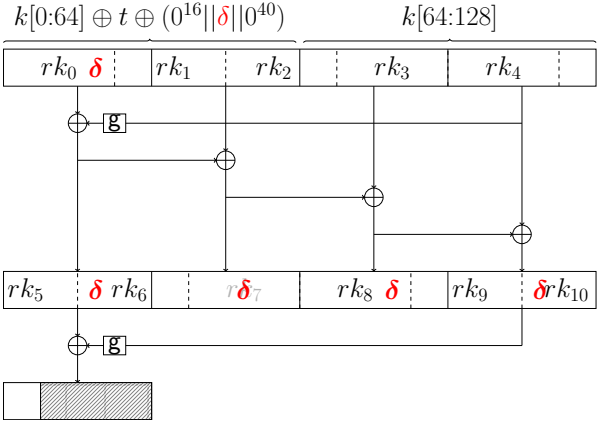
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



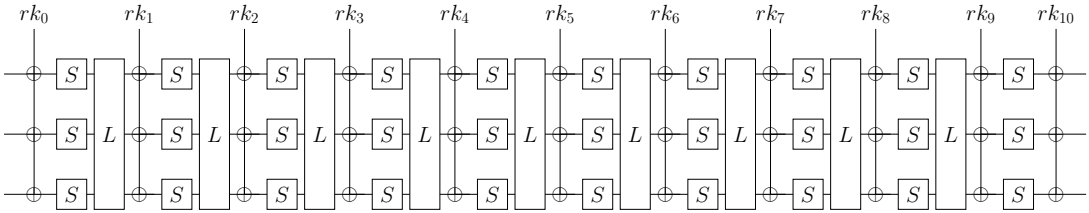
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



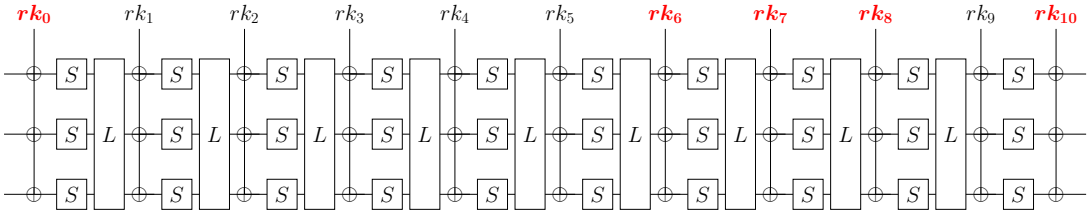
Our Attacks on HALFLOOP-24 – Related Tweak in Key Schedule



Our Attacks on HALFLOOP-24 – Related Tweak Attack

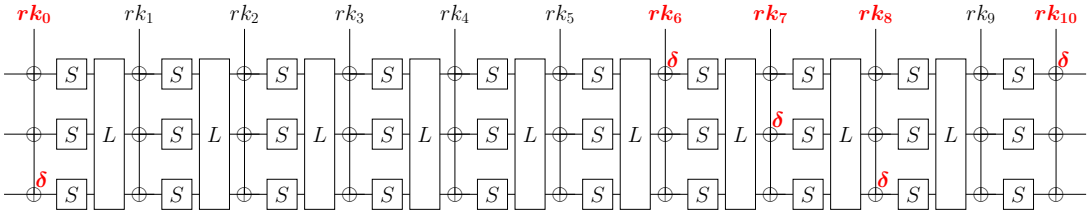


Our Attacks on HALFLOOP-24 – Related Tweak Attack

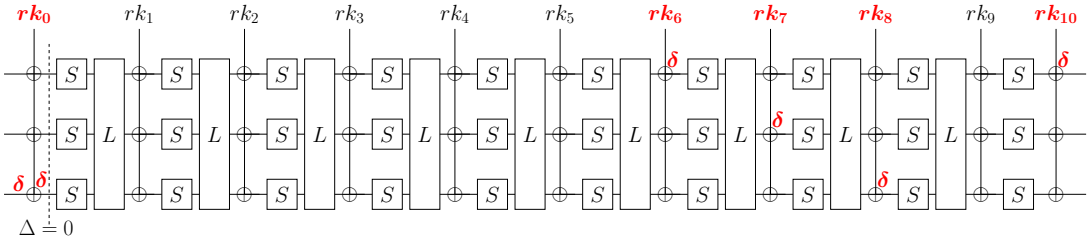


Our Attacks on HALFLOOP-24 – Related Tweak Attack

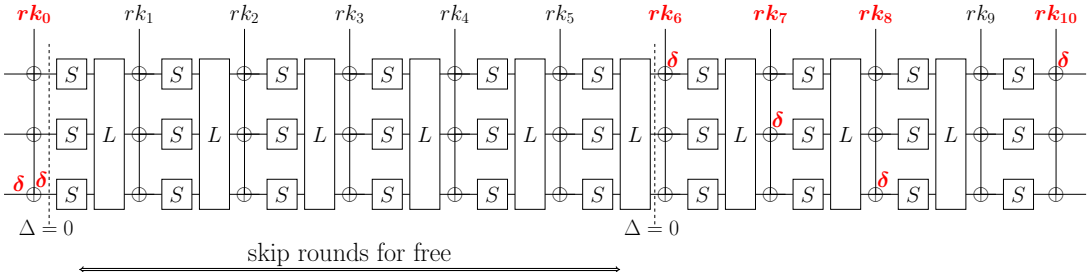
CASA
Cyber Security in the Age of Large-Scale Adversaries



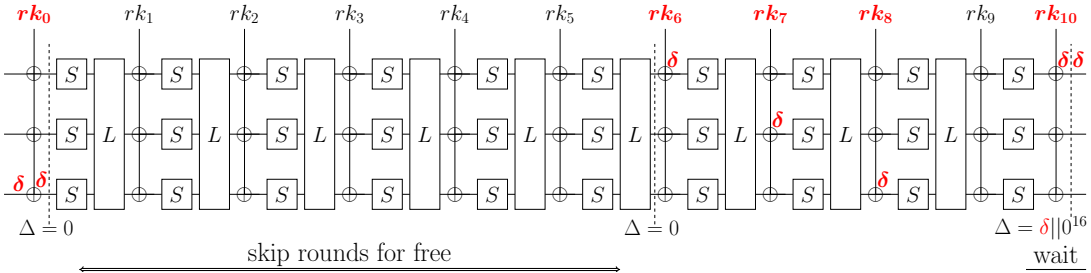
Our Attacks on HALFLOOP-24 – Related Tweak Attack



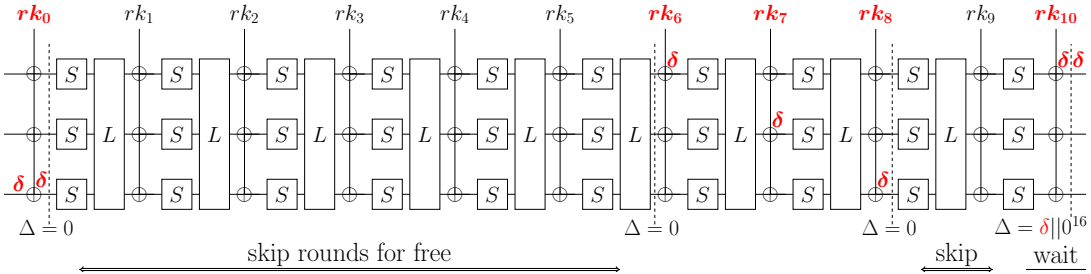
Our Attacks on HALFLOOP-24 – Related Tweak Attack



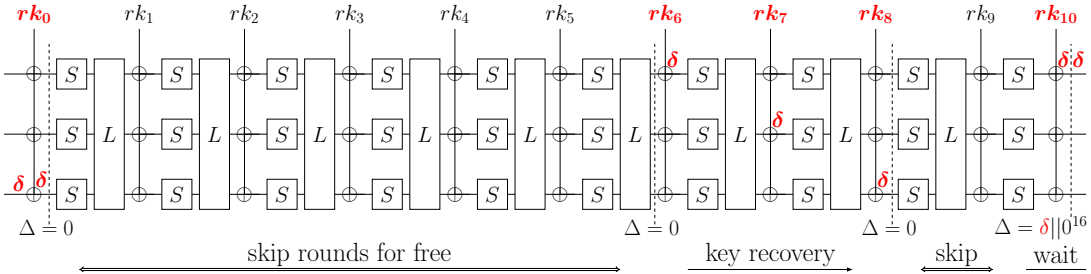
Our Attacks on HALFLOOP-24 – Related Tweak Attack



Our Attacks on HALFLOOP-24 – Related Tweak Attack



Our Attacks on HALFLOOP-24 – Related Tweak Attack

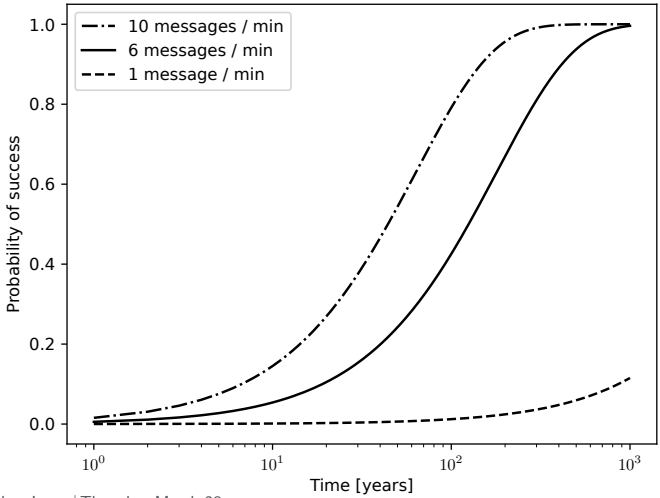


Our Attacks on HALFLOOP-24 – Overview

CASA
Cyber Security in the Age of Large-Scale Adversaries

Setting	Time	Data	Memory
Ciphertext only	2^{87}	2^{38}	2^{63}
Known-plaintext	2^{56}	2^{37}	2^{16}
Chosen-plaintext	2^{56}	2^{18}	2^{16}
Chosen-ciphertext	2^{10}	2^{10}	1

Our Attacks on HALFLOOP-24 – Practicality



Conclusion and Future Work

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

Conclusion and Future Work

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Conclusion
  - HALFLOOP-24 is far from providing 128 bits of security
  - We advice against the usage of *any* HALFLOOP variant
- Possible future work
  - Study HALFLOOP-48 and HALFLOOP-96
  - Reduce data complexity of our attacks

CASA
Cyber Security in the Age of Large-Scale Adversaries

Paper

Code

Thank You!