CASA

Cyber Security in the Age of Large-Scale Adversaries

Cryptanalysis of HALFLOOP Block Ciphers: Destroying HALFLOOP-24

FSE 2024, Leuven, March 25

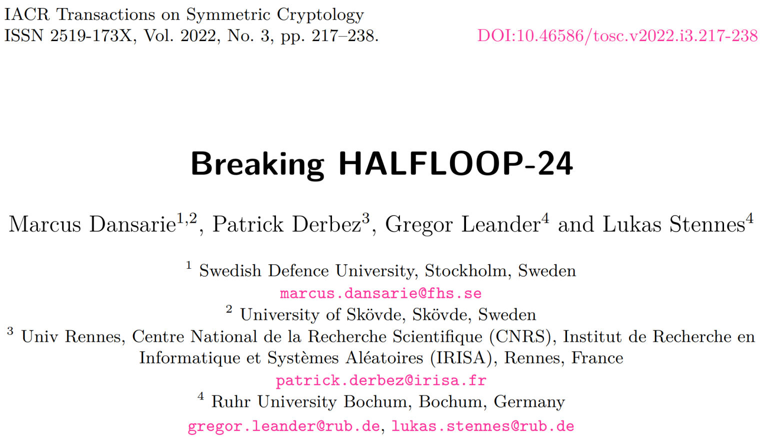
Gregor Leander, Shahram Rasoolzadeh and Lukas Stennes

RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HGI HORST GÖRTZ INSTITUT

CASA
Cyber Security in the Age of Large-Scale Adversaries



IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2022, No. 3, pp. 217–238.
DOI:10.46586/tosc.v2022.i3.217-238

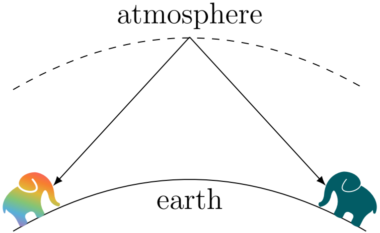
Breaking HALFLOOP-24

Marcus Dansarie[1,2], Patrick Derbez[3], Gregor Leander[4] and Lukas Stennes[4]

[1] Swedish Defence University, Stockholm, Sweden
marcus.dansarie@fhs.se
[2] University of Skövde, Skövde, Sweden
[3] Univ Rennes, Centre National de la Recherche Scientifique (CNRS), Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA), Rennes, France
patrick.derbez@irisa.fr
[4] Ruhr University Bochum, Bochum, Germany
gregor.leander@rub.de, lukas.stennes@rub.de

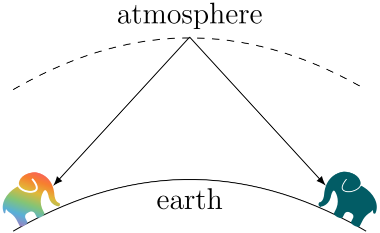
Why HALFLOOP: High Frequency Radio

- 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)



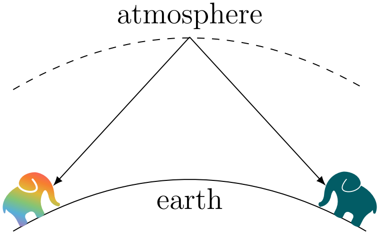
Why HALFLOOP: High Frequency Radio

- 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

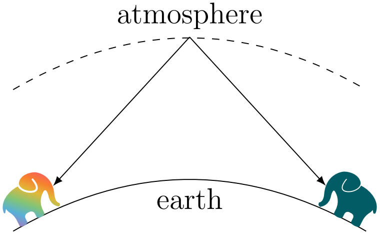
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for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



Why HALFLOOP: High Frequency Radio

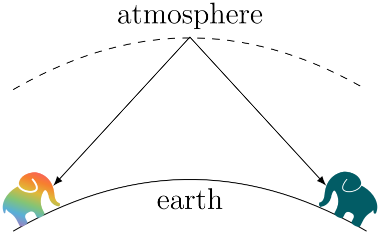
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- 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

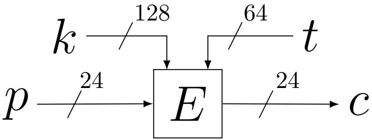
- Frequencies between 3MHz and 30MHz
- Skywave propagation: radio signals are reflected by upper atmosphere
- Enables communication across very large distances without any external infrastructure
- Users are the military, diplomatic services, disaster management agencies, etc.
- HALFLOOP is used for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



Description of HALFLOOP-24 (HALFLOOP-$\{48{,}96\}$ work similarly)

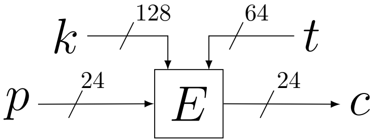
Description of HALFLOOP-24 – Big Picture

- 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**
- 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



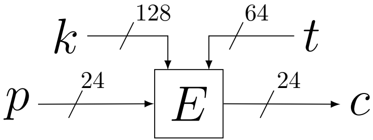
Description of HALFLOOP-24 – Big Picture

- 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**
- 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



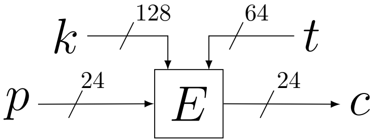
Description of HALFLOOP-24 – Big Picture

- 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**
- 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



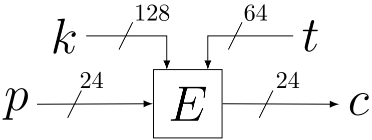
Description of HALFLOOP-24 – Big Picture

- 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**
- 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

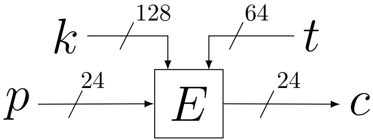
- HALFLOOP-24 is a tweakable block cipher E
  - Tweak consists of current time, a word counter and the used frequency
  - Supersedes SoDark cipher which used **56-bit** keys
  - Specified in MIL-STD-188-141 since **2017**
- HALFLOOP-24 is heavily inspired by AES
  - Uses the same SBox
  - Essentially the same key schedule
  - State is represented as 3×1 matrix over $\mathbb{F}_{2^8}$
  - 10 rounds



Description of HALFLOOP-24 – Big Picture

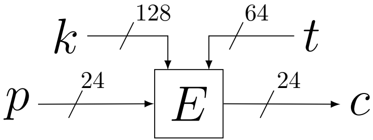
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- 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**
- 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



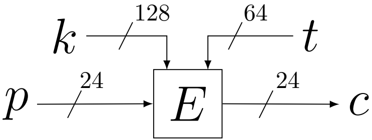
Description of HALFLOOP-24 – Big Picture

- 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**
- 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



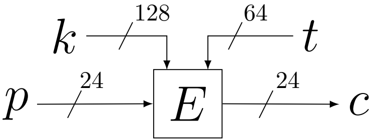
Description of HALFLOOP-24 – Big Picture

- 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**
- 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

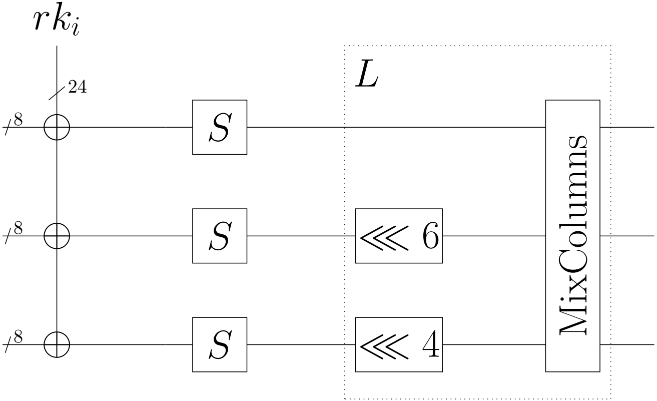


Description of HALFLOOP-24 – Big Picture

- 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**
- 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

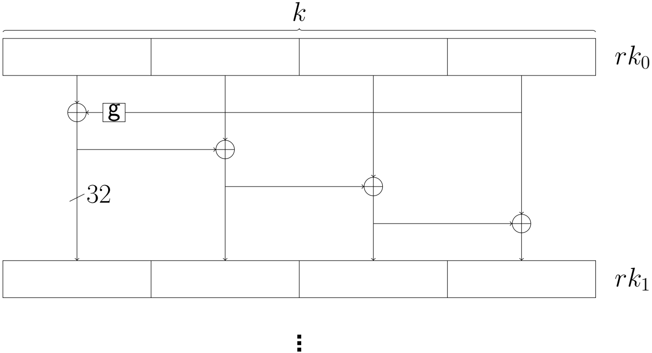


Description of HALFLOOP-24 – Round Function

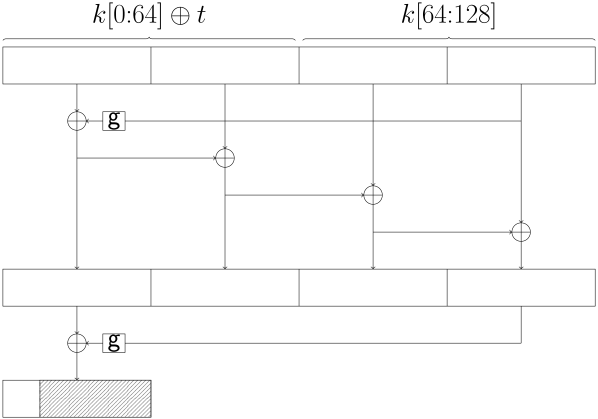


MC: multiply with $c(x) = x^2 + 2x + 9$ modulo $x^3 + 1$

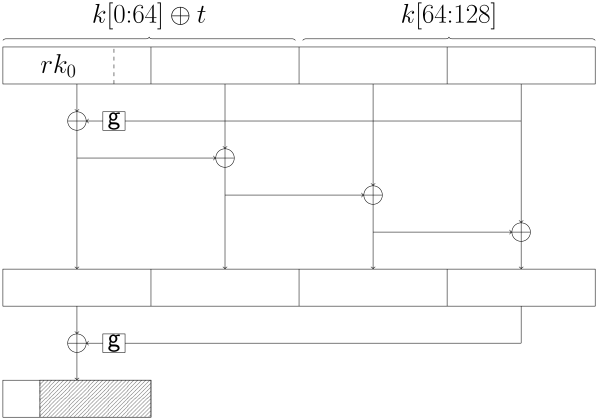
Description of HALFLOOP-24 – AES-128 Key Schedule



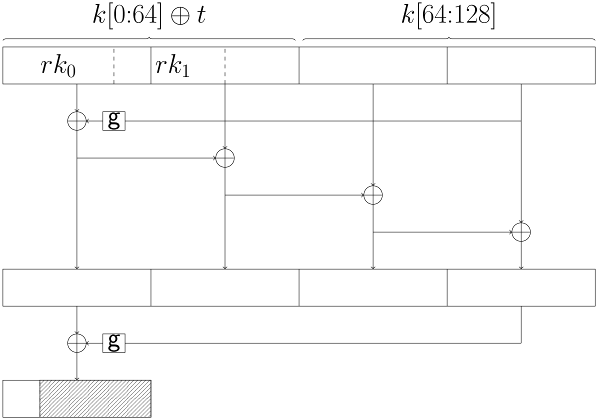
Description of HALFLOOP-24 – Key Schedule



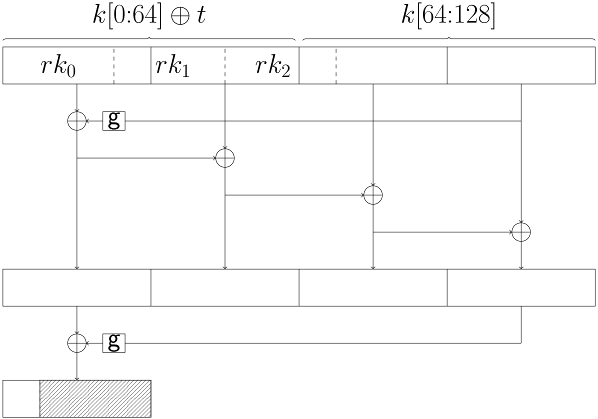
Description of HALFLOOP-24 – Key Schedule



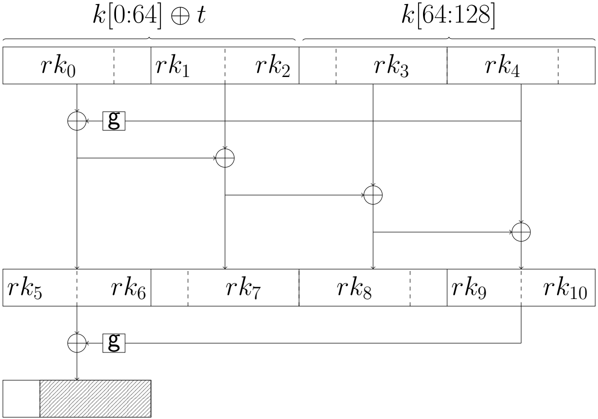
Description of HALFLOOP-24 – Key Schedule



Description of HALFLOOP-24 – Key Schedule

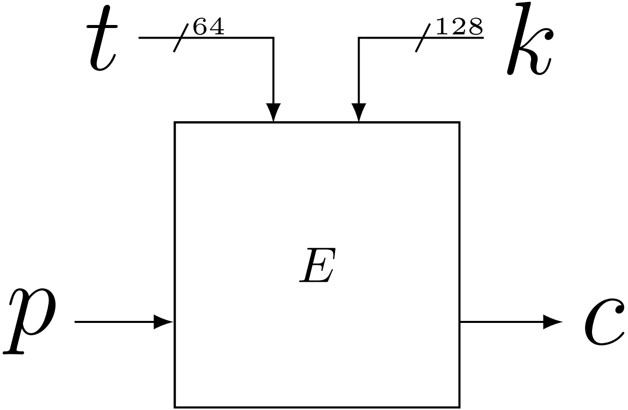


Description of HALFLOOP-24 – Key Schedule

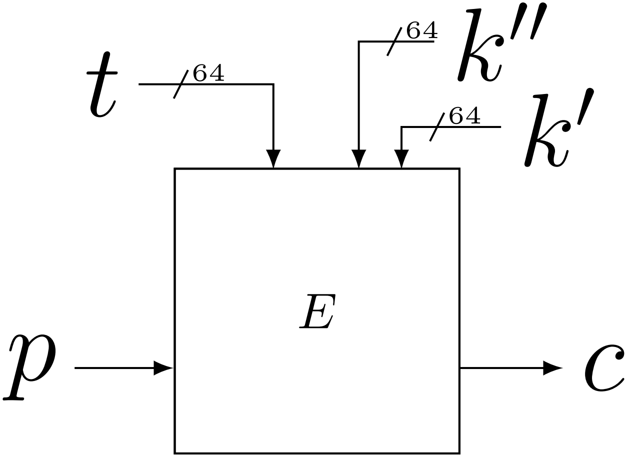


Generic Attack on HALFLOOP-{24,48,96}
(already pointed out by [LRW02, DDLS22])

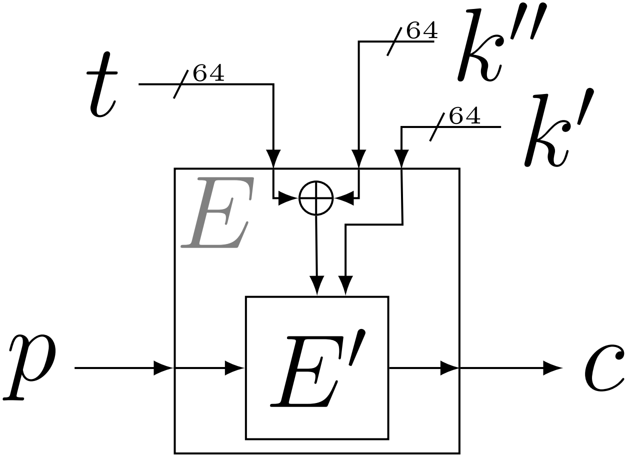
Generic Attack on HALFLOOP-{24,48,96}



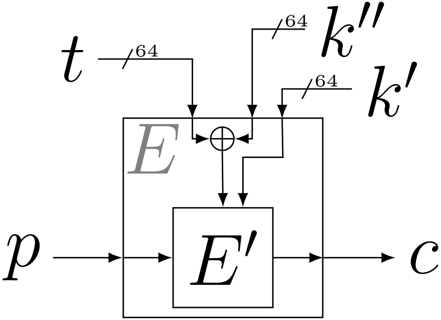
Generic Attack on HALFLOOP-{24,48,96}



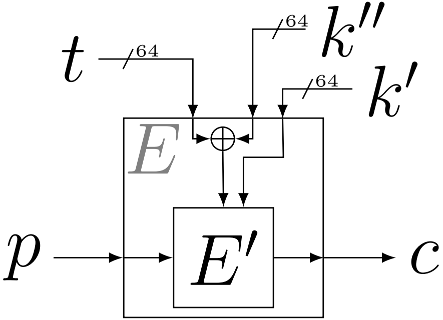
Generic Attack on HALFLOOP-{24,48,96}



Generic Attack on HALFLOOP-{24,48,96}



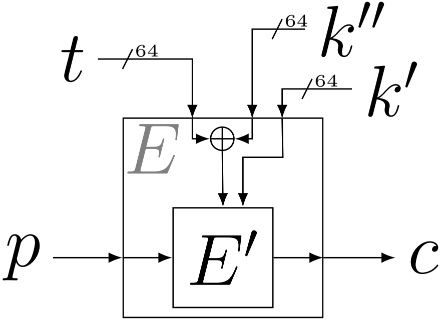
Generic Attack on HALFLOOP-{24,48,96}



Offline Phase:

```
$T = [\,]$
for all $k' \in \mathbb{F}_2^{64}$:
    $c = E'_{0||k'}(p)$
    append $(k', c)$ to $T$
```

Generic Attack on HALFLOOP-{24,48,96}



Offline Phase:

```
$T = [\,]$
for all $k' \in \mathbb{F}_2^{64}$:
    $c = E'_{0||k'}(p)$
    append $(k', c)$ to $T$
```

Online Phase:

```
for all $t \in \mathbb{F}_2^{64}$:
    $c = E(t, p)$
    if $\exists k' s.t. (k', c) \in T$:
        key candidate $t||k'$
```

Attacks on HALFLOOP-24 – So Far

Setting	Time	Data	Memory	Reference
CPA	2^{65}	2^{64}	2^{64}	[DDLS22]
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]

Attacks on HALFLOOP-24 – So Far

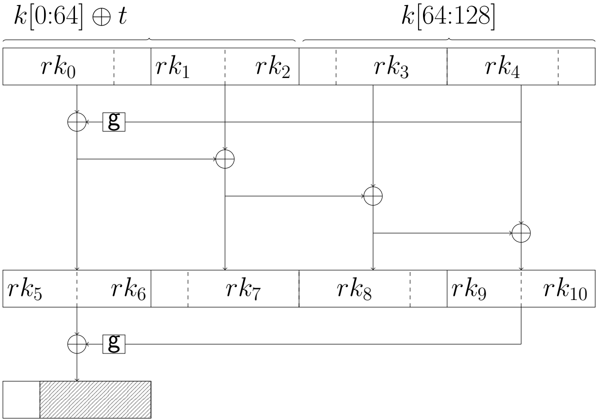
Setting	Time	Data	Memory	Reference
CPA	2^{65}	2^{64}	2^{64}	[DDLS22]
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]

Attacks on HALFLOOP-24 – So Far

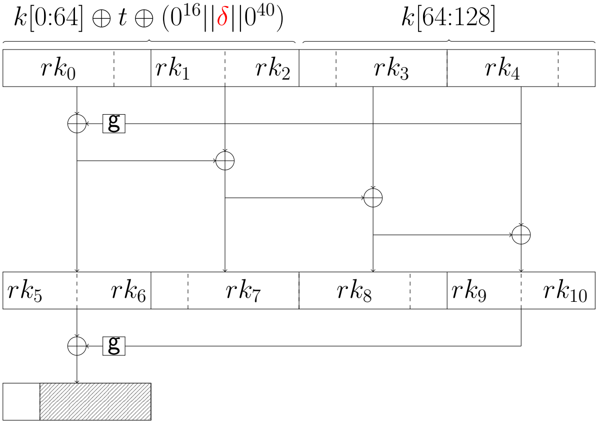
Setting	Time	Data	Memory	Reference
CPA	2^{65}	2^{64}	2^{64}	[DDLS22]
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]

New Attack on HALFLOOP-24
(with minimal data)

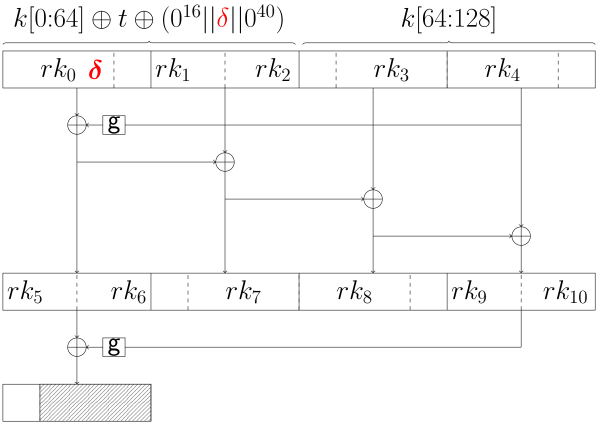
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



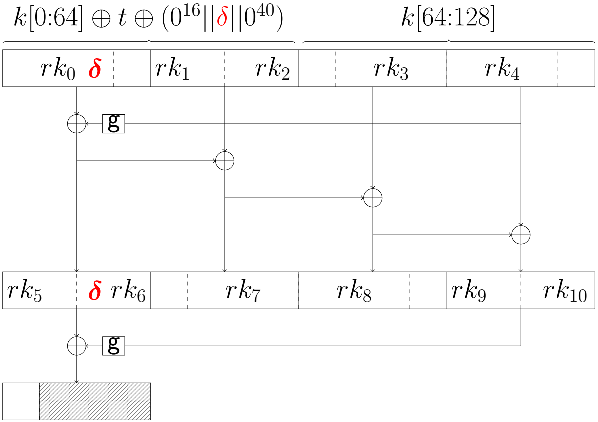
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



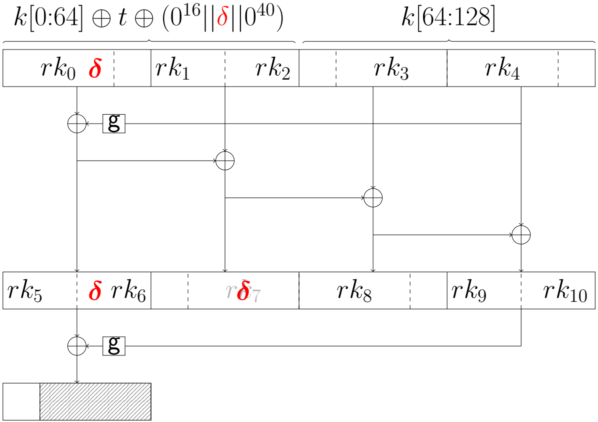
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



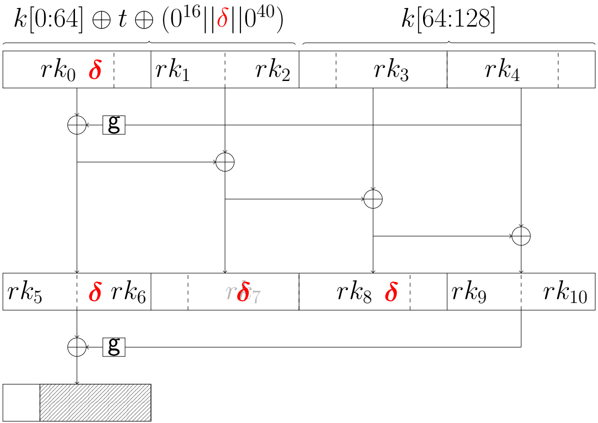
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



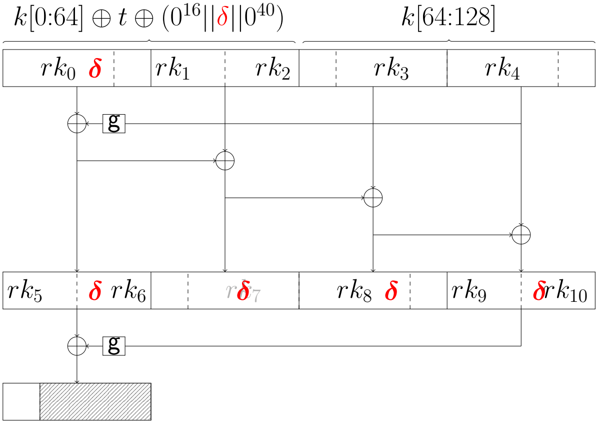
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



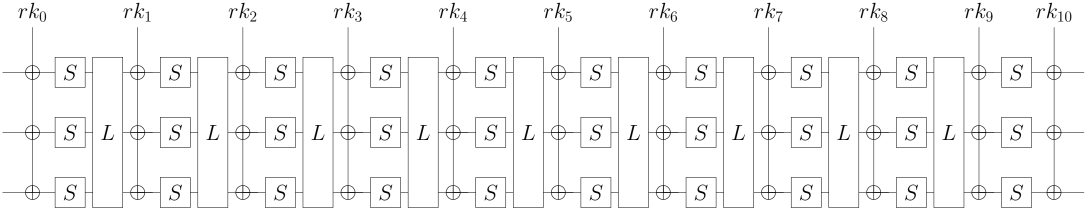
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule


$k[0{:}64] \oplus t \oplus (0^{16}||\delta||0^{40})$
$k[64{:}128]$
rk_0 $\boldsymbol{\delta}$
rk_1
rk_2
rk_3
rk_4
g
rk_5
$\boldsymbol{\delta}$ rk_6
rk_7 $\boldsymbol{\delta}$
rk_8 $\boldsymbol{\delta}$
rk_9
rk_{10}
g

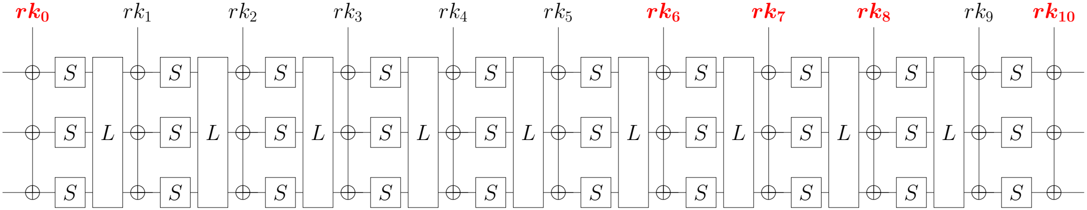
New Attack on HALFLOOP-24 – Old Related Tweak in Key Schedule



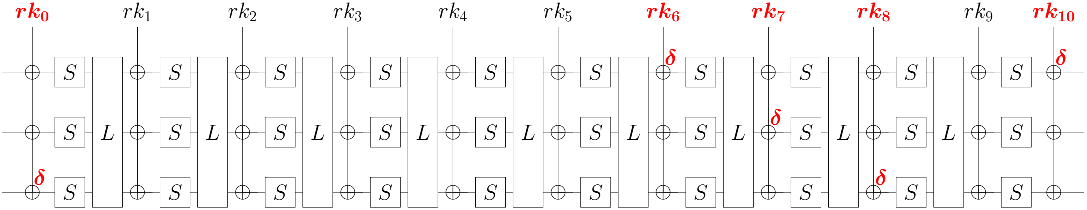
New Attack on HALFLOOP-24



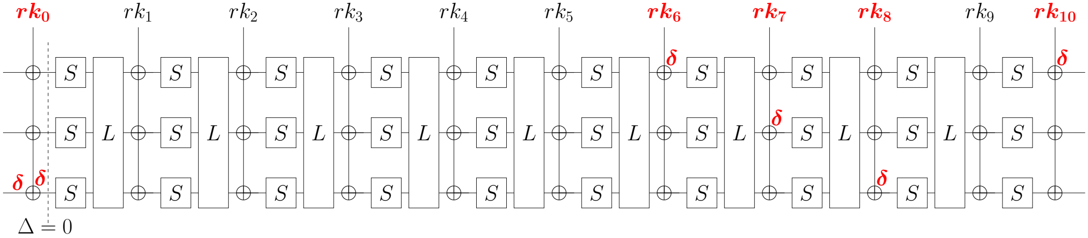
New Attack on HALFLOOP-24



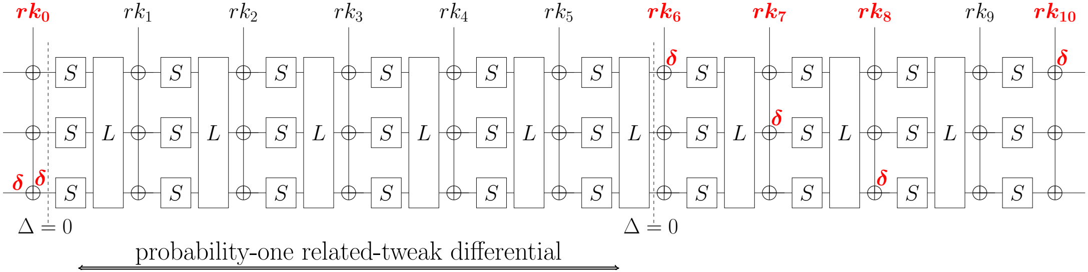
New Attack on HALFLOOP-24



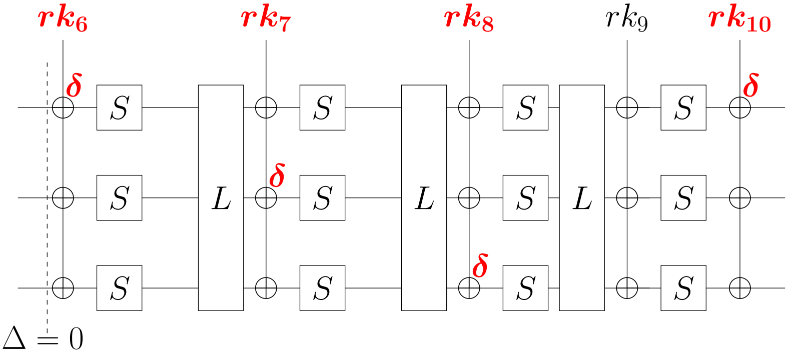
New Attack on HALFLOOP-24



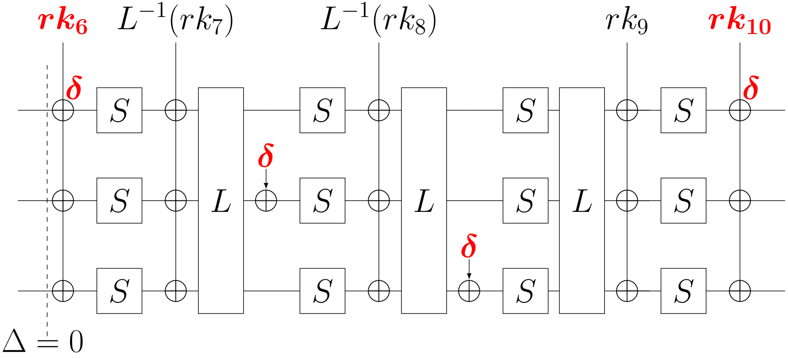
New Attack on HALFLOOP-24



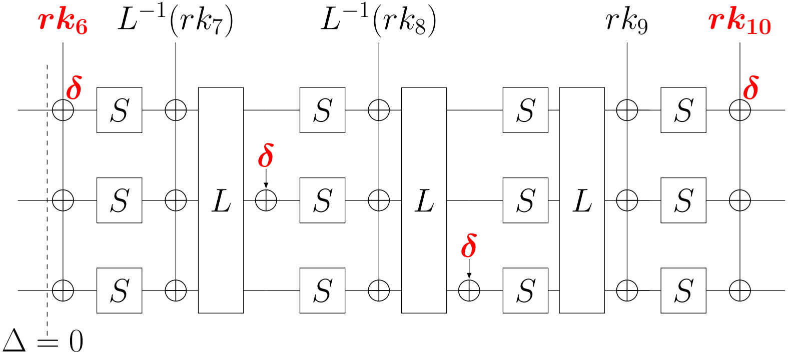
New Attack on HALFLOOP-24



New Attack on HALFLOOP-24

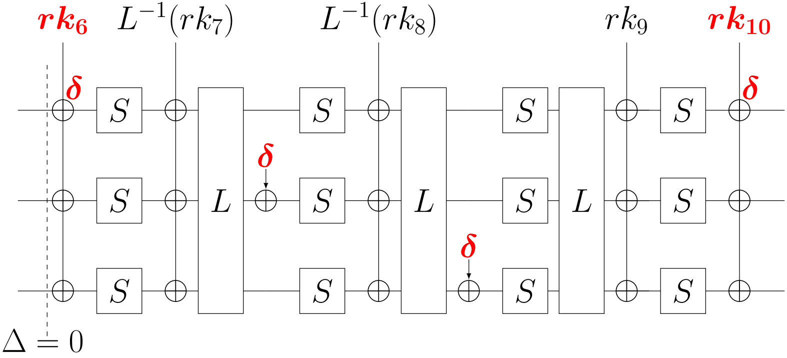


New Attack on HALFLOOP-24



$\Rightarrow$ trivial attack with $t = 2^{80}$ and $D = 6$ (CPA)

New Attack on HALFLOOP-24



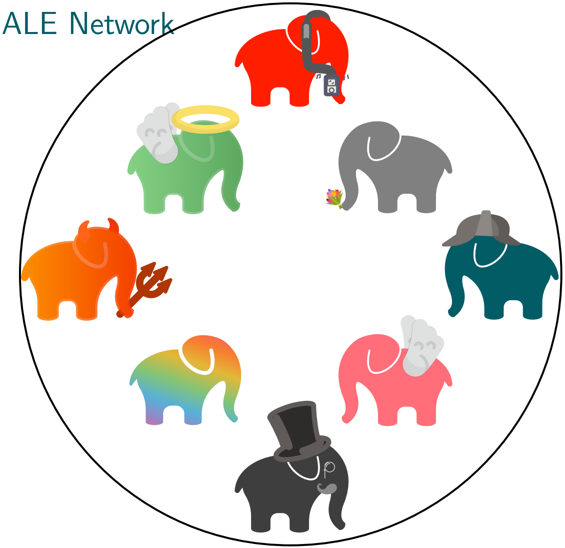
$\Rightarrow$ improved attack with $t = 2^{56}$ and $D = 6$ (CPA)

Attacks on HALFLOOP-24 – Overview

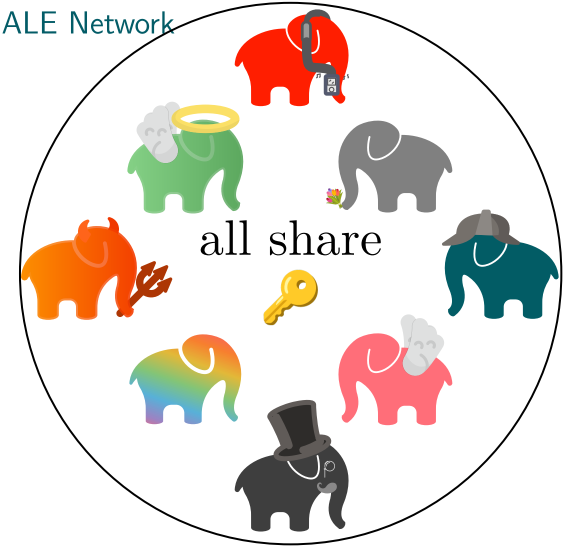
Setting	Time	Data	Memory	Reference
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]
CPA	2^{56}	6	5 GB	This Work
CPA	2^{48}	8	5 GB	This Work
ALE	2^{48}	**2 hours**	5 GB	This Work

Attack in Practice – **A**utomatic **L**ink **E**stablishment

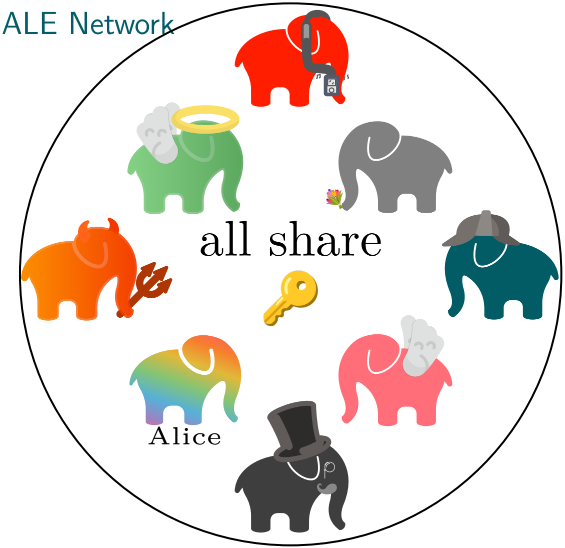
Attack in Practice – ALE Network



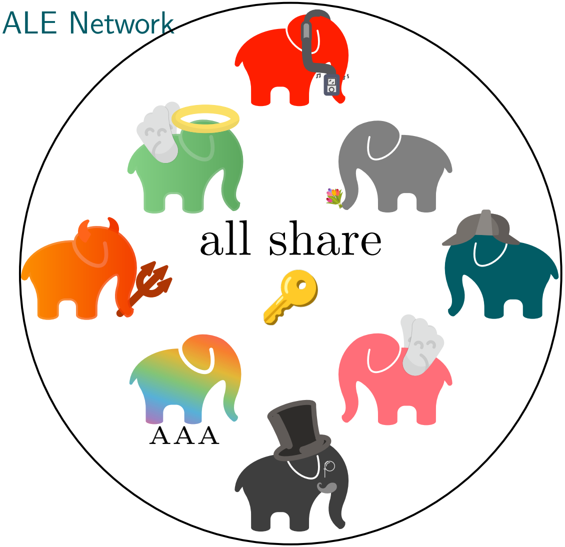
Attack in Practice – ALE Network



Attack in Practice – ALE Network

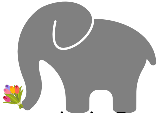


Attack in Practice – ALE Network



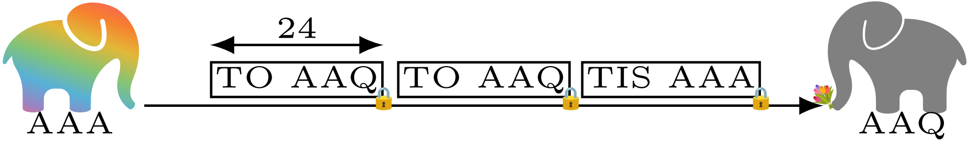
Attack in Practice – ALE Handshake

AAA

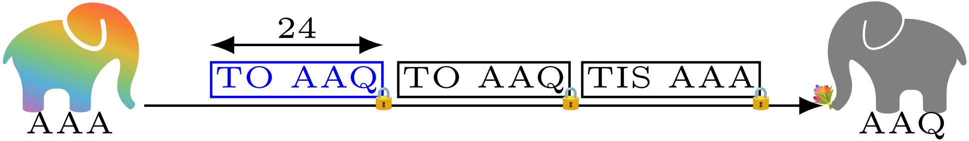


AAQ

Attack in Practice – ALE Handshake



Attack in Practice – ALE Handshake



24

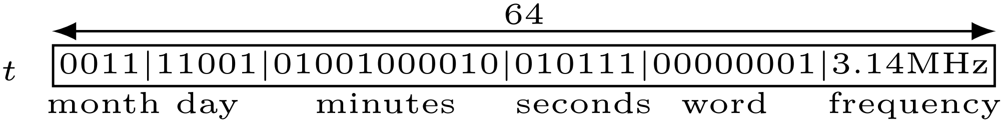
TO AAQ

TO AAQ

TIS AAA

AAA

AAQ



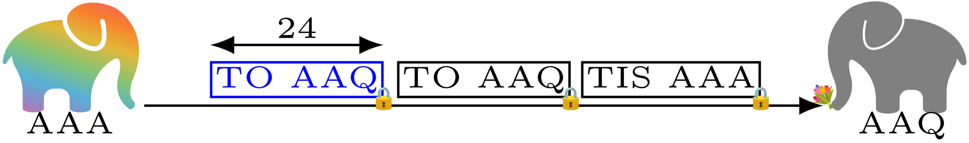
64

t

0011 | 11001 | 01001000010 | 010111 | 00000001 | 3.14MHz

month day minutes seconds word frequency

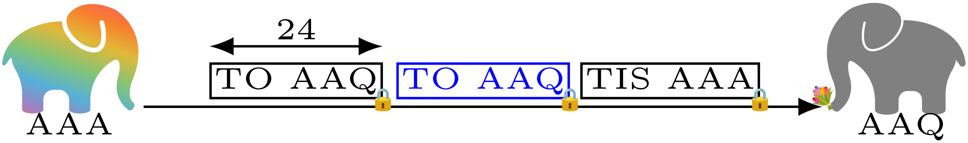
Attack in Practice – ALE Handshake



64

t	0011	11001	01001000010	010111	00000001	3.14MHz
	month	day	minutes	seconds	word	frequency

Attack in Practice – ALE Handshake



24

TO AAQ

TO AAQ

TIS AAA

AAA

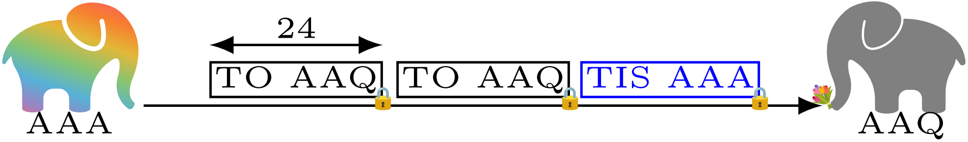
AAQ

64

t $\boxed{0011|11001|01001000010|010111|00000010|3.14\text{MHz}}$

month day minutes seconds word frequency

Attack in Practice – ALE Handshake

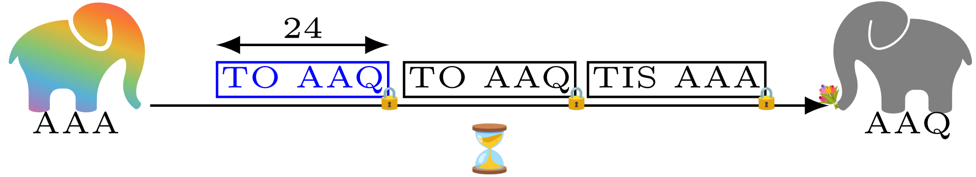


64

t

0011	11001	01001000010	010111	00000011	3.14MHz
month	day	minutes	seconds	word	frequency

Attack in Practice – ALE Handshake



24

TO AAQ

TO AAQ

TIS AAA

AAA

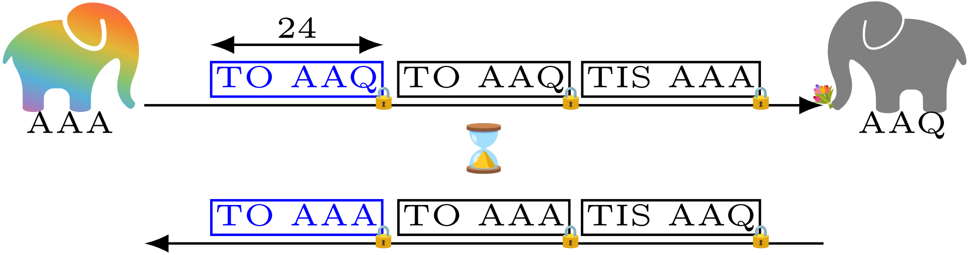
AAQ

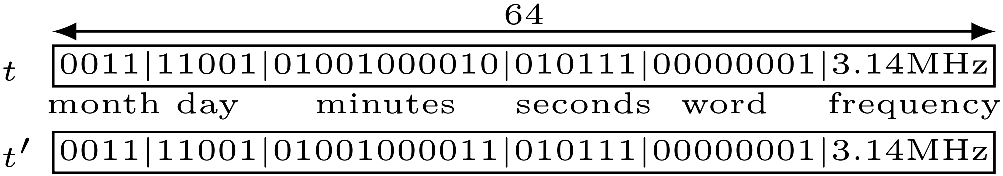
64

t 0011|11001|01001000010|010111|00000001|3.14MHz

month day minutes seconds word frequency

Attack in Practice – ALE Handshake



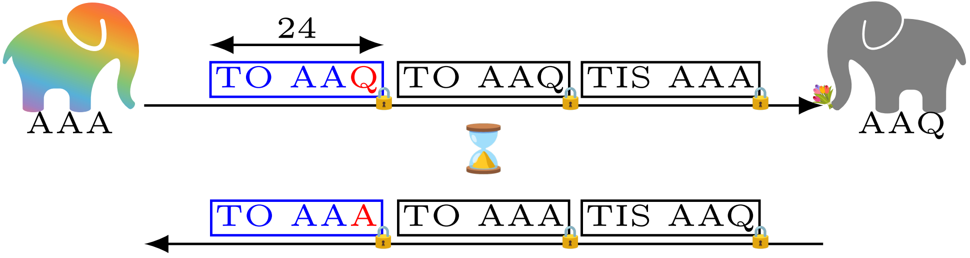


t: 0011|11001|0100100010|010111|00000001|3.14MHz

month day minutes seconds word frequency

t': 0011|11001|0100100011|010111|00000001|3.14MHz

Attack in Practice – ALE Handshake



24

AAA

TO AAQ | TO AAQ | TIS AAA

AAQ

TO AAA | TO AAA | TIS AAQ

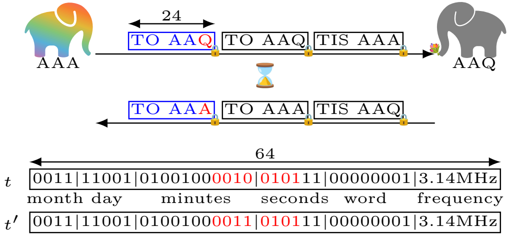
64

t 0011|11001|01001000010|010111|00000001|3.14MHz

month day minutes seconds word frequency

t' 0011|11001|01001000011|010111|00000001|3.14MHz

Attack in Practice – ALE Handshake

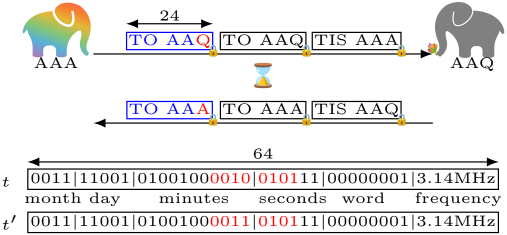


24
TO AAQ
TO AAQ
TIS AAA
AAA
AAQ
TO AAA
TO AAA
TIS AAQ
64
t
0011|11001|01001000010|010111|00000001|3.14MHz
month day
minutes
seconds
word
frequency
t′
0011|11001|01001000011|010111|00000001|3.14MHz

we get a good pair if

- frequencies are the same
- word counters are the same
- messages are sent in the same 16 minute bin
- seconds are the same modulo 4
- difference in remaining time matches difference in callsigns

Attack in Practice – ALE Handshake



AAA

24

TO AAQ | TO AAQ | TIS AAA

AAQ

TO AAA | TO AAA | TIS AAQ

64

t 0011|11001|01001000010|010111|00000001|3.14MHz

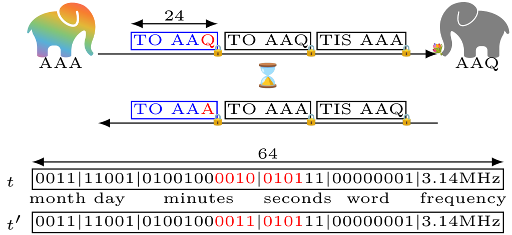
month day minutes seconds word frequency

t' 0011|11001|01001000011|010111|00000001|3.14MHz

we get a good pair if

- frequencies are the same
- word counters are the same
- messages are sent in the same 16 minute bin
- seconds are the same modulo 4
- difference in remaining time matches difference in callsigns

Attack in Practice – ALE Handshake



24

AAA — TO AAQ | TO AAQ | TIS AAA → AAQ

TO AAA | TO AAA | TIS AAQ ←

64

t 0011|11001|01001000010|010111|00000001|3.14MHz

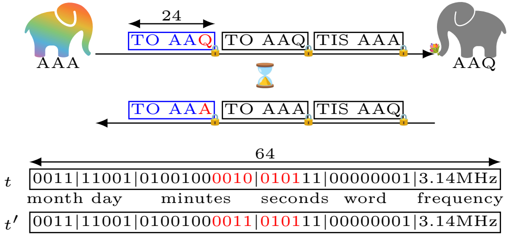
month day minutes seconds word frequency

t' 0011|11001|01001000011|010111|00000001|3.14MHz

we get a good pair if

- frequencies are the same
- word counters are the same
- messages are sent in the same 16 minute bin
- seconds are the same modulo 4
- difference in remaining time matches difference in callsigns

Attack in Practice – ALE Handshake

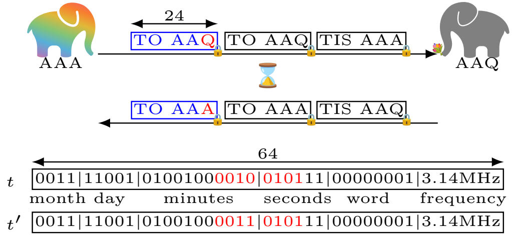


	month	day	minutes	seconds	word	frequency
t	0011	11001	01001000010	010111	00000001	3.14MHz
t'	0011	11001	01001000011	010111	00000001	3.14MHz

we get a good pair if

- frequencies are the same
- word counters are the same
- messages are sent in the same 16 minute bin
- seconds are the same modulo 4
- difference in remaining time matches difference in callsigns

Attack in Practice – ALE Handshake


24
TO AAQ
TO AAQ
TIS AAA
AAA
AAQ
TO AAA
TO AAA
TIS AAQ
64
t
0011|11001|01001000010|010111|00000001|3.14MHz
month day
minutes
seconds
word
frequency
t′
0011|11001|01001000011|010111|00000001|3.14MHz

we get a good pair if

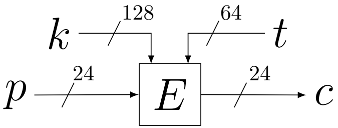
- frequencies are the same
- word counters are the same
- messages are sent in the same 16 minute bin
- seconds are the same modulo 4
- difference in remaining time matches difference in callsigns

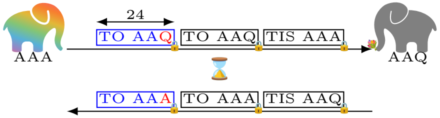
Attacks on HALFLOOP-$\{48{,}96\}$

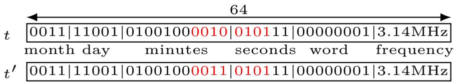
Attacks on HALFLOOP-{48,96} – Overview

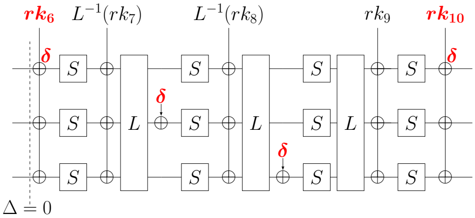
Variant	Attack	Time	Data	Memory
HALFLOOP-48	Generic	2^{65}	2^{64}	$3 \cdot 2^{29}$ TB
HALFLOOP-48	DS-MITM	2^{122}	13	2^{57} TB
HALFLOOP-96	Generic	2^{65}	2^{64}	$3 \cdot 2^{29}$ TB
HALFLOOP-96-7r	DS-MITM	2^{114}	15	2^{105}

Conclusion



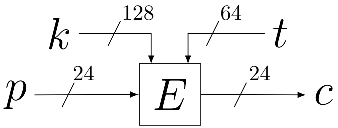


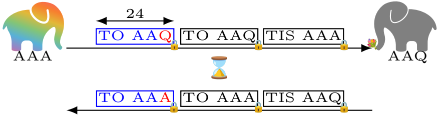

64
t
0011|11001|0100100010|010111|00000001|3.14MHz
month
day
minutes
seconds
word
frequency
t′
0011|11001|0100100011|010111|00000001|3.14MHz

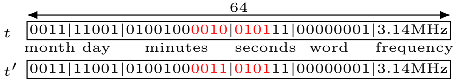


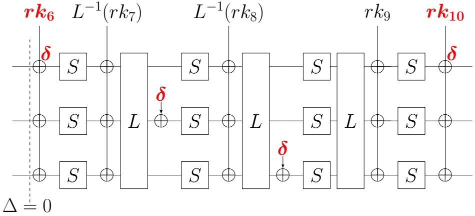
Setting	Time	Data	Memory	Reference
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]
CPA	2^{56}	6	5 GB	This Work
CPA	2^{48}	8	5 GB	This Work
ALE	2^{48}	**2 hours**	5 GB	This Work

Conclusion

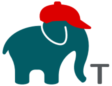





64
t 0011|11001|0100100010|010111|00000001|3.14MHz
month day minutes seconds word frequency
t' 0011|11001|0100100011|010111|00000001|3.14MHz



Setting	Time	Data	Memory	Reference
CCA	2^{10}	2^{10}	negligible	[DDLS22]
CPA	2^{56}	2^{18}	2 MB	[DDLS22]
ALE	2^{56}	**541 years**	2 MB	[DDLS22]
CPA	2^{56}	6	5 GB	This Work
CPA	2^{48}	8	5 GB	This Work
ALE	2^{48}	**2 hours**	5 GB	This Work



Thank You!