Cryptanalysis of KeeLoq with COPACOBANA

Martin Novotný[1,2], Timo Kasper[1]

[1]Horst Görtz Institute for IT-Security
Ruhr University Bochum

[2]Faculty of Information Technology
Czech Technical University in Prague

Case Study Access Control

Simple access controls: fixed code (“password”)

code

eavesdropper duplicates key (cloning)

but the industry learned…

Case Study Access Control

Horst Görtz Institute for IT-Security

advanced theft control: rolling code

$code = e_k(n_i)$

rolling code (or hopping code)

$code = e_k(n)$

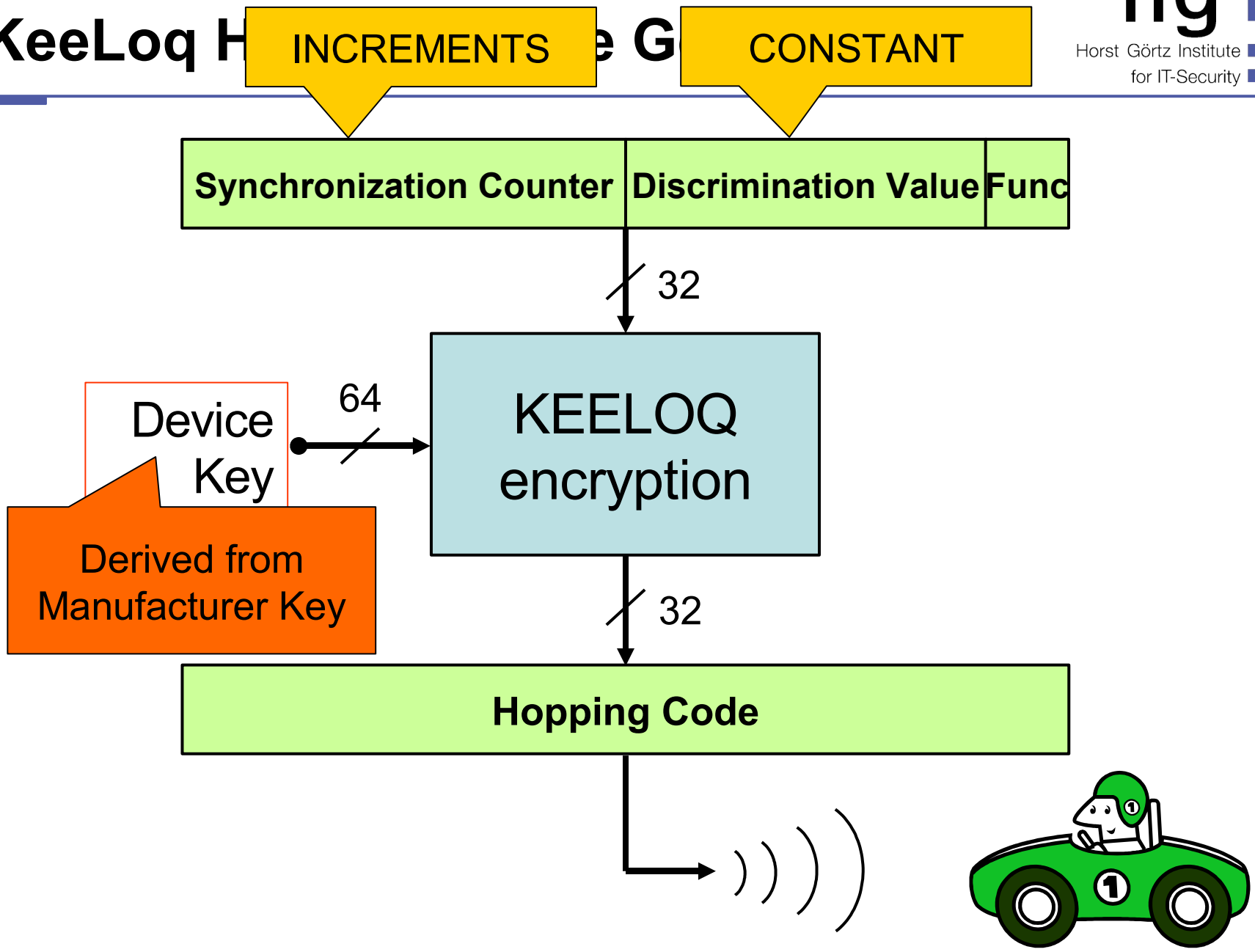
$code = e_k(n+1)$

$code = e_k(n+2)$

….

$e_k()$ is often a block cipher

KeeLoq H e G


INCREMENTS
CONSTANT
Synchronization Counter
Discrimination Value
Func
32
Device Key
64
KEELOQ encryption
Derived from Manufacturer Key
32
Hopping Code

So what can we do now?

Horst Görtz Institute for IT-Security

If we have ~~access~~ to a remote

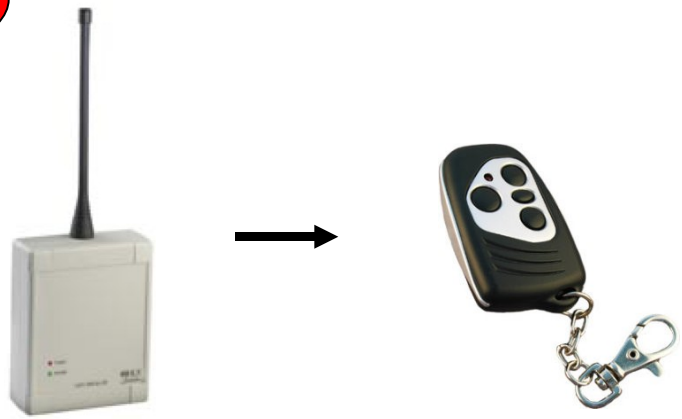
Recover **device key** and clone the device

People usually do not lend their keys to unknown people

In a shop

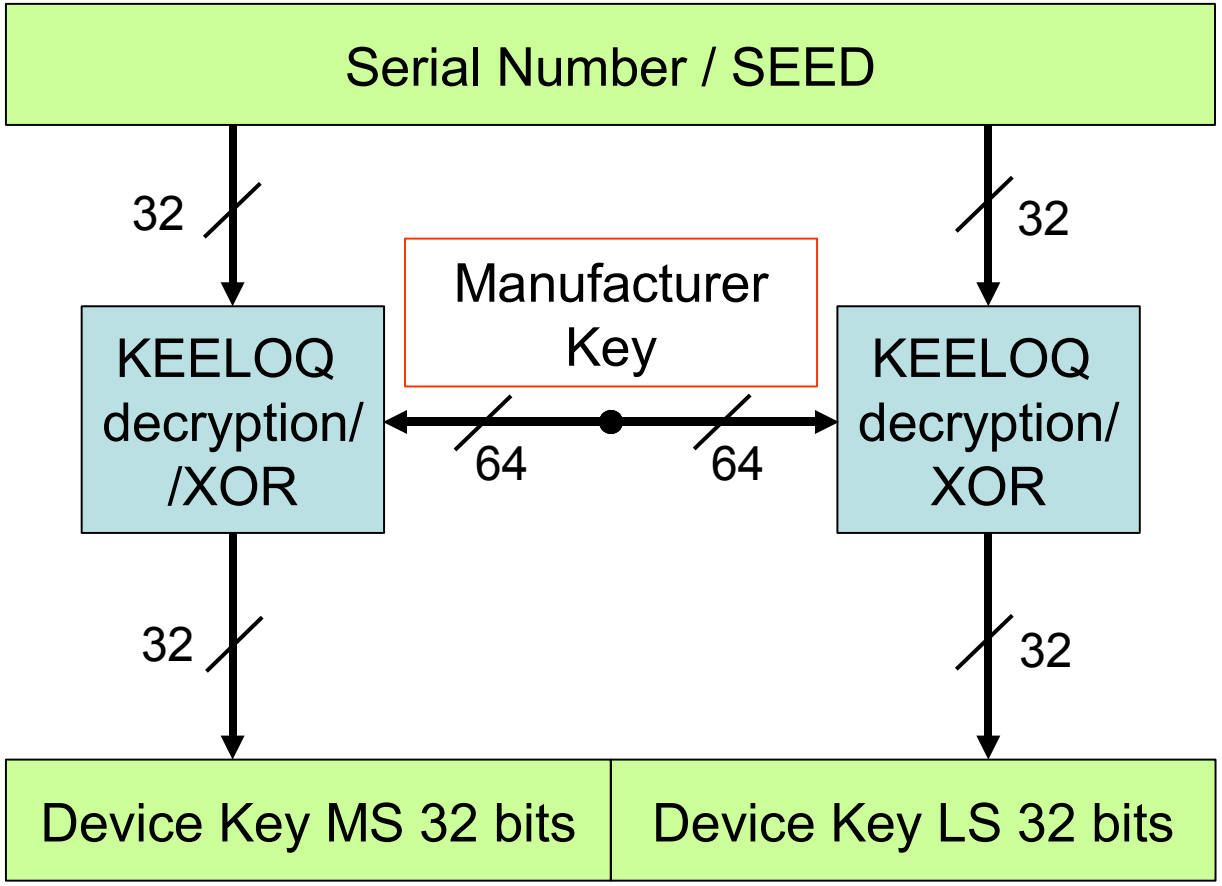
If we have access to a receiver

Recover **manufacturer key** and generate new remotes



Identical for all *GarageOpeners2000* and corresponding remotes

Device Key Derivation



So what can we do now?

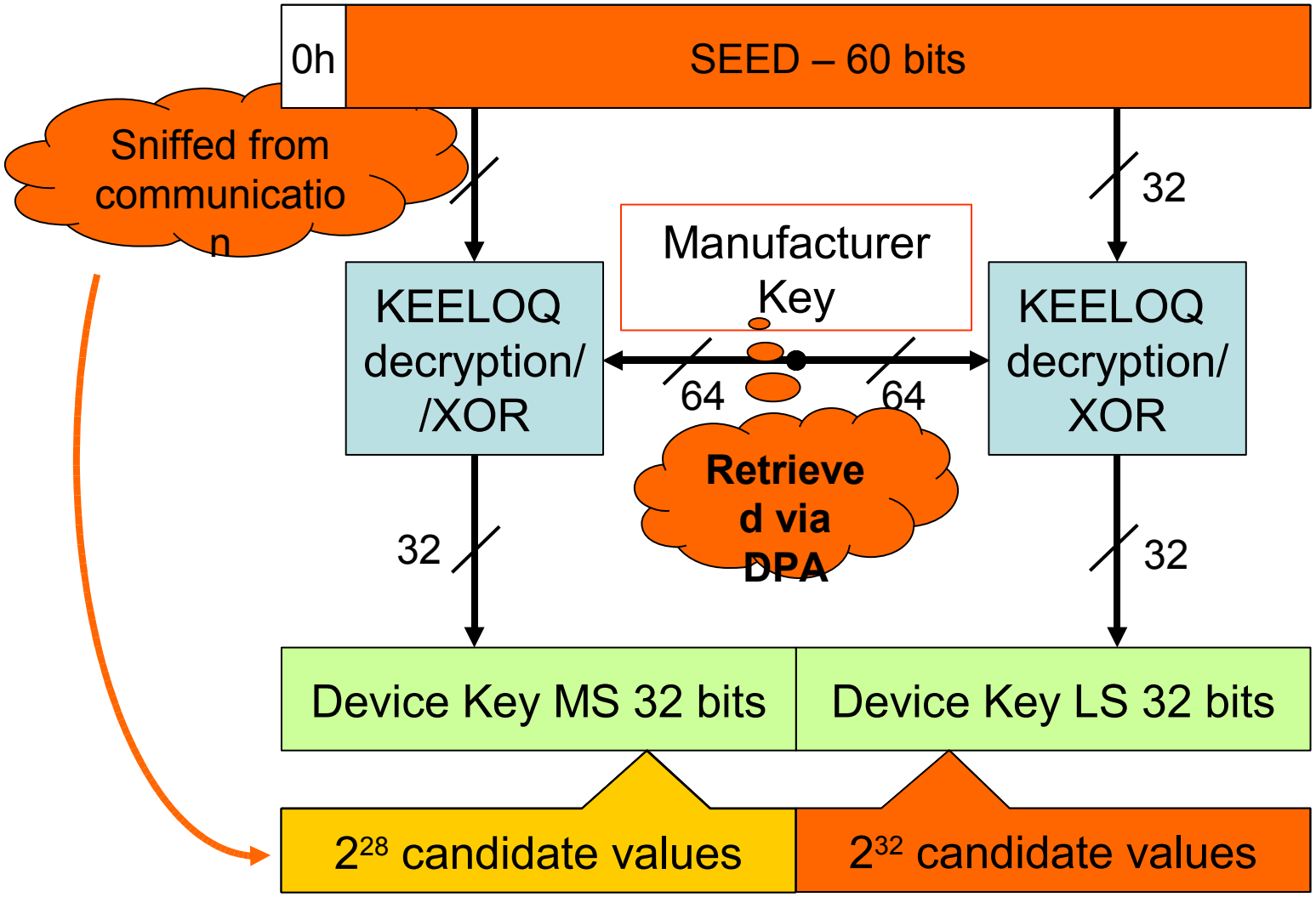
Horst Görtz Institute for IT-Security

After extracting of manufacturing key:

Remotely eavesdrop on 1-2 communications & clone key!

Serial Number,
KeeLoq(n+1)

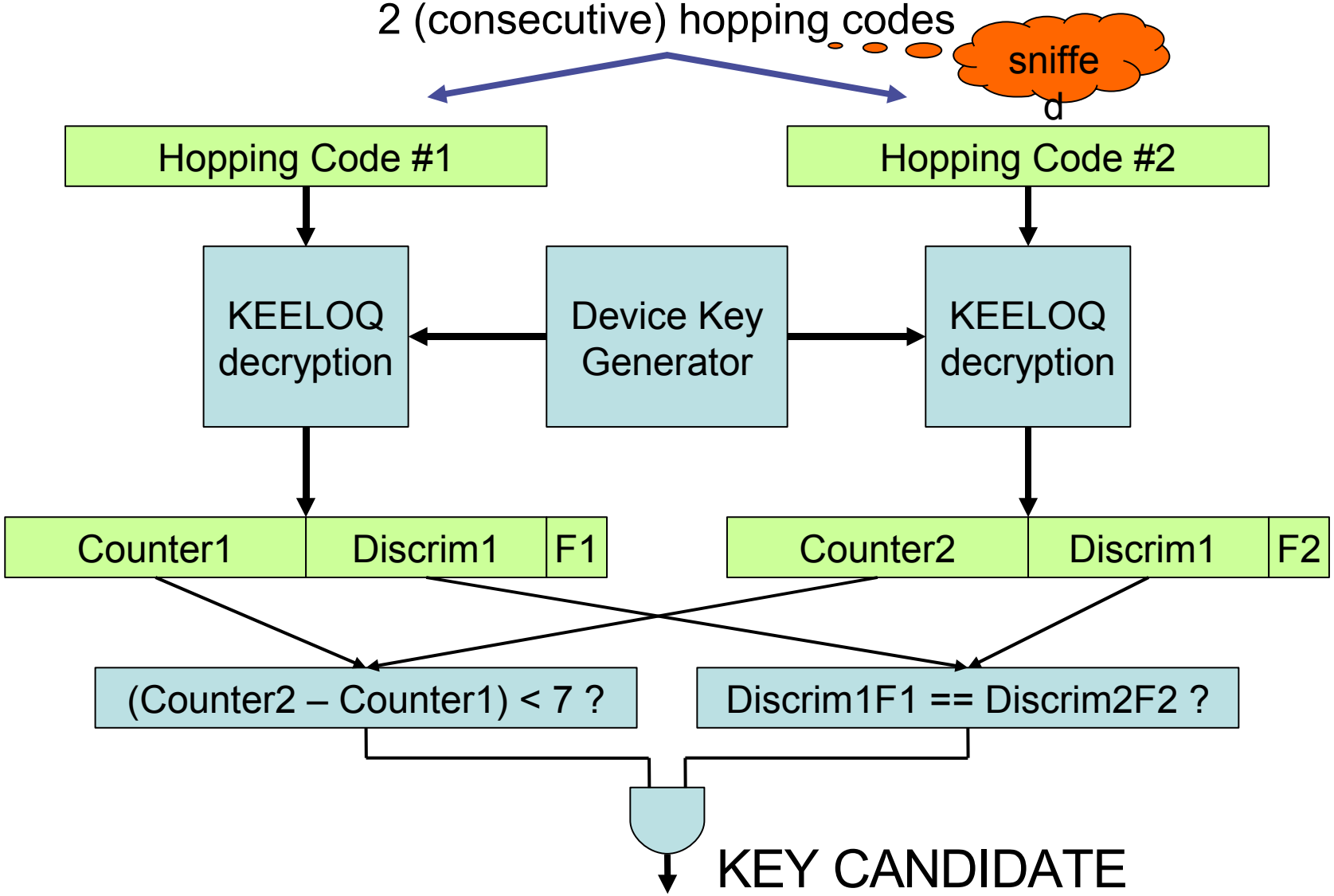
Device Key Derivation



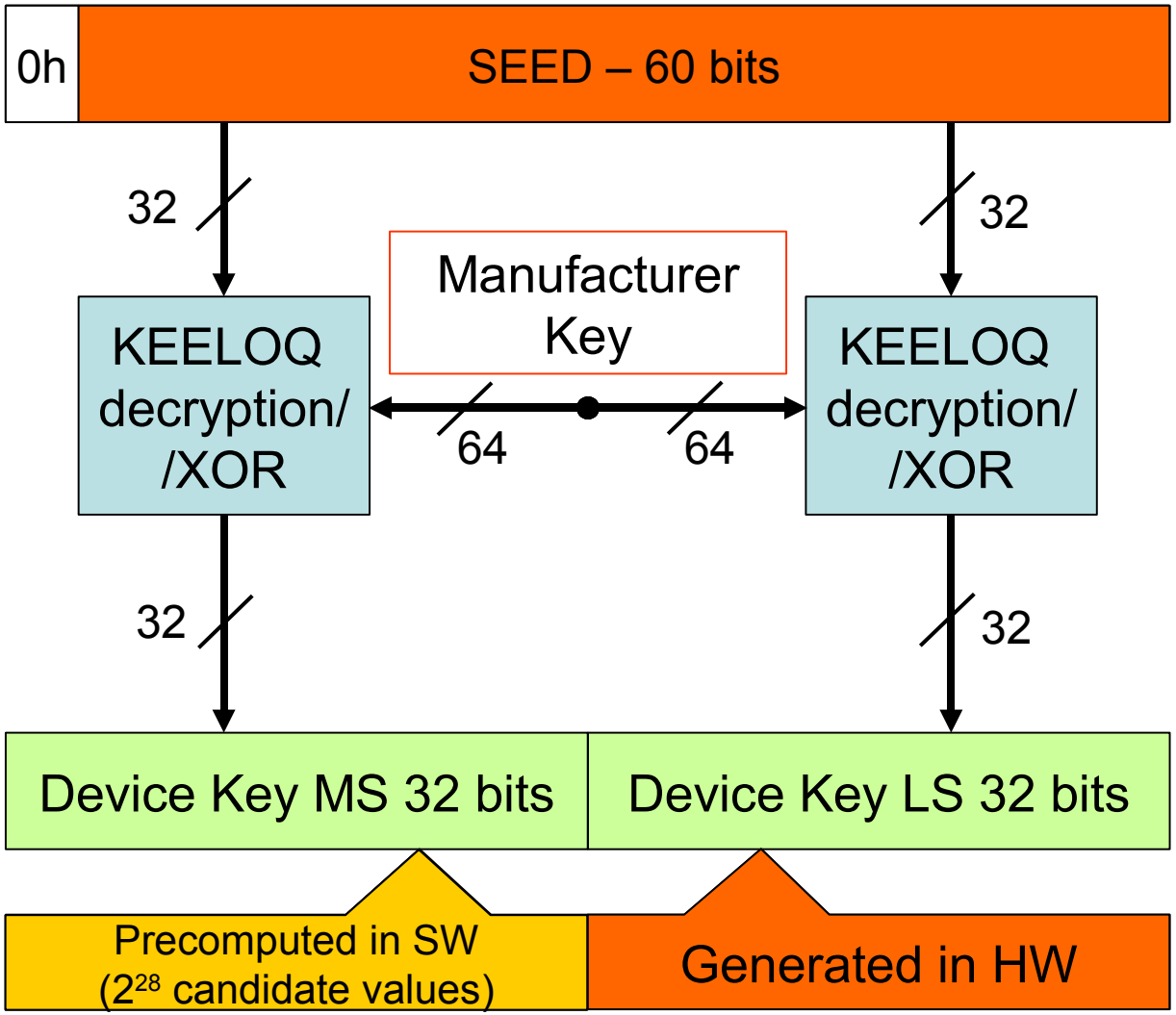
KeeLoq Cracker

KeeLoq Cracker

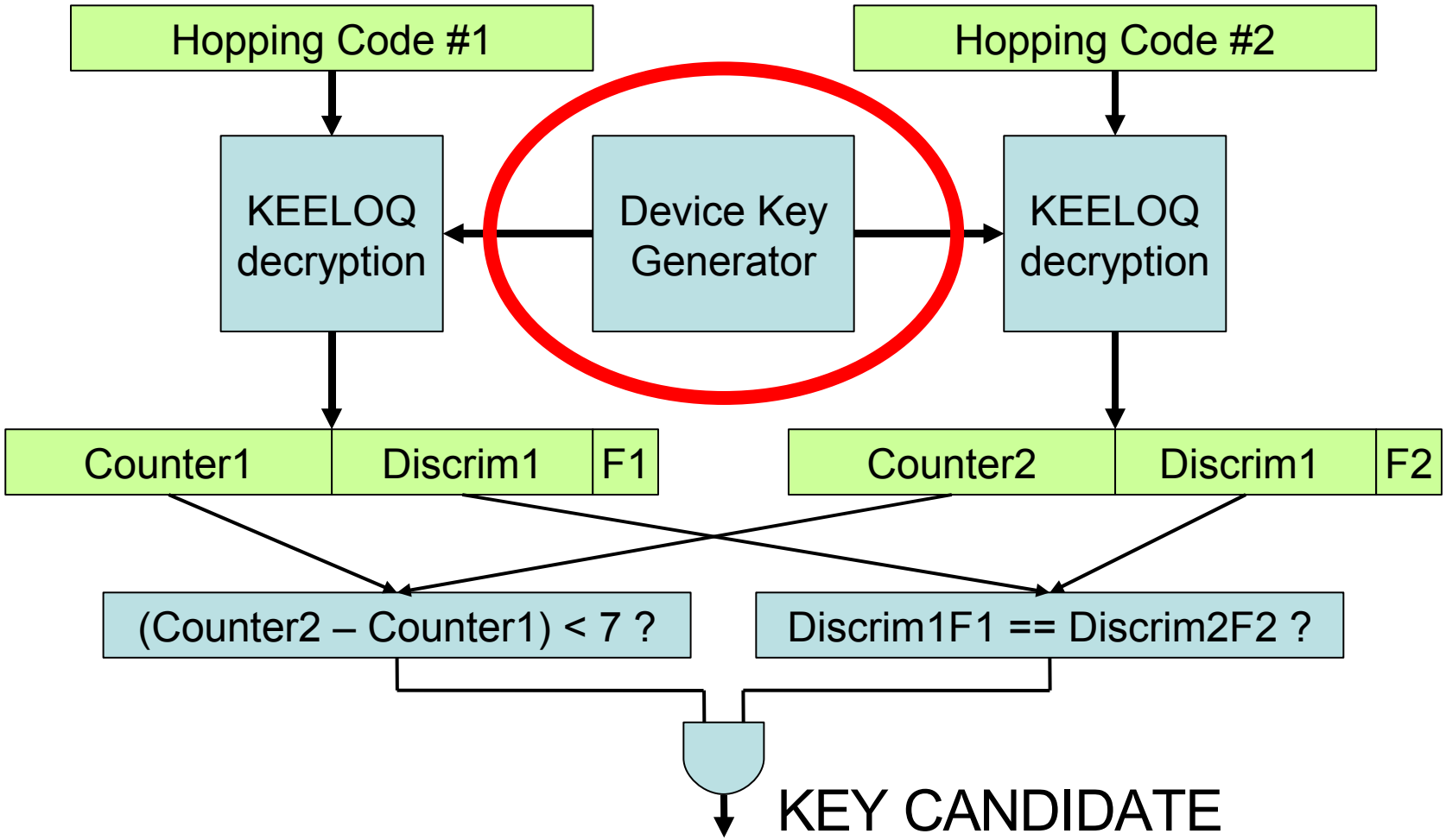
Horst Görtz Institute for IT-Security



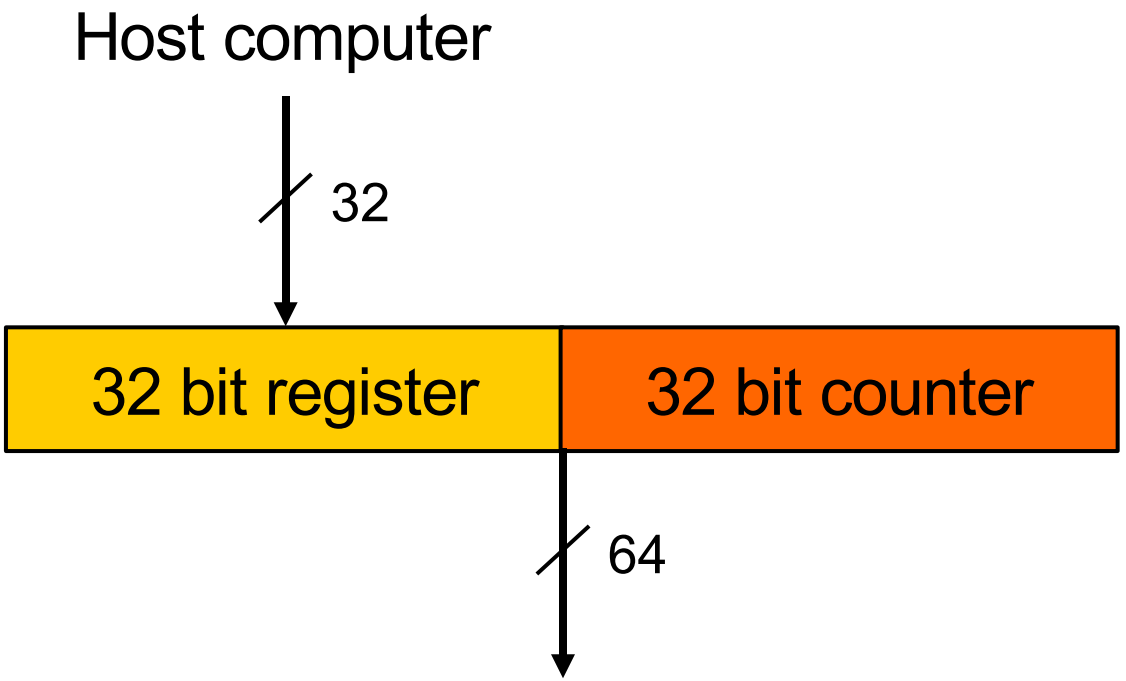
Device Key Derivation

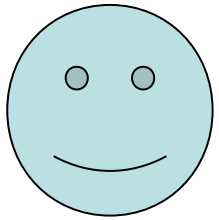


KeeLoq Cracker

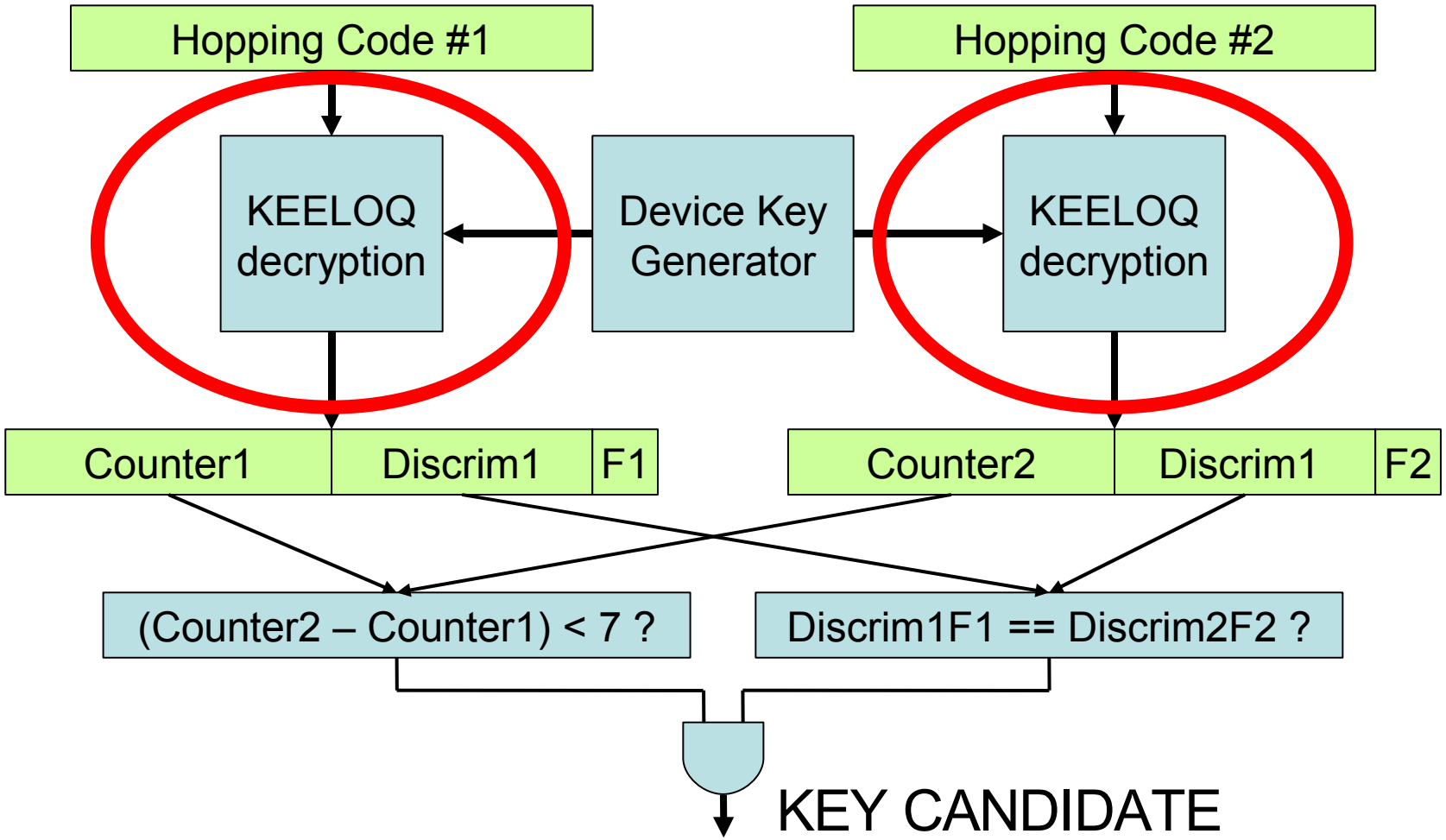


Device Key Generator



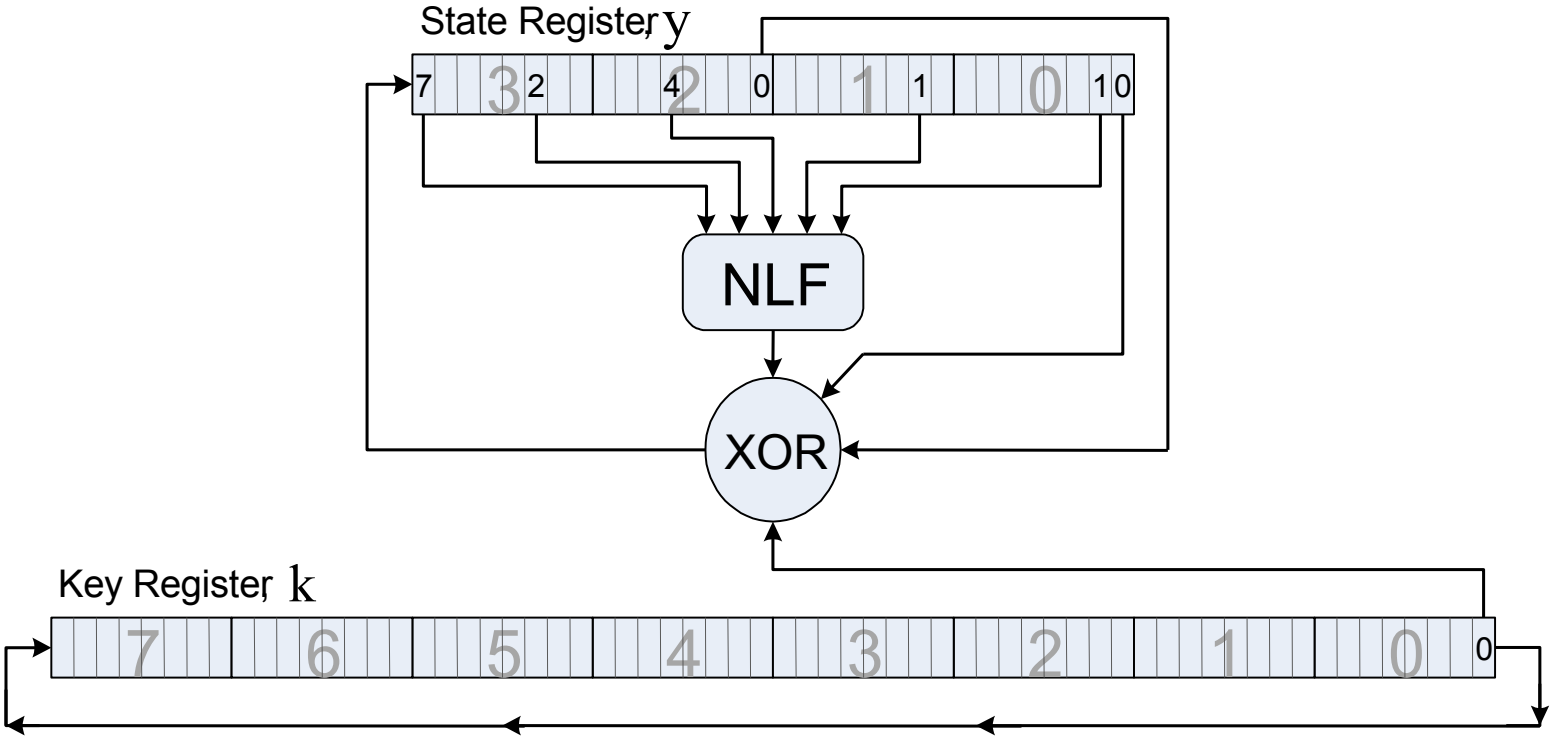


KeeLoq Cracker



KeeLoq – The Algorithm

Horst Görtz Institute
for IT-Security



64 bit key, 32 bit block length

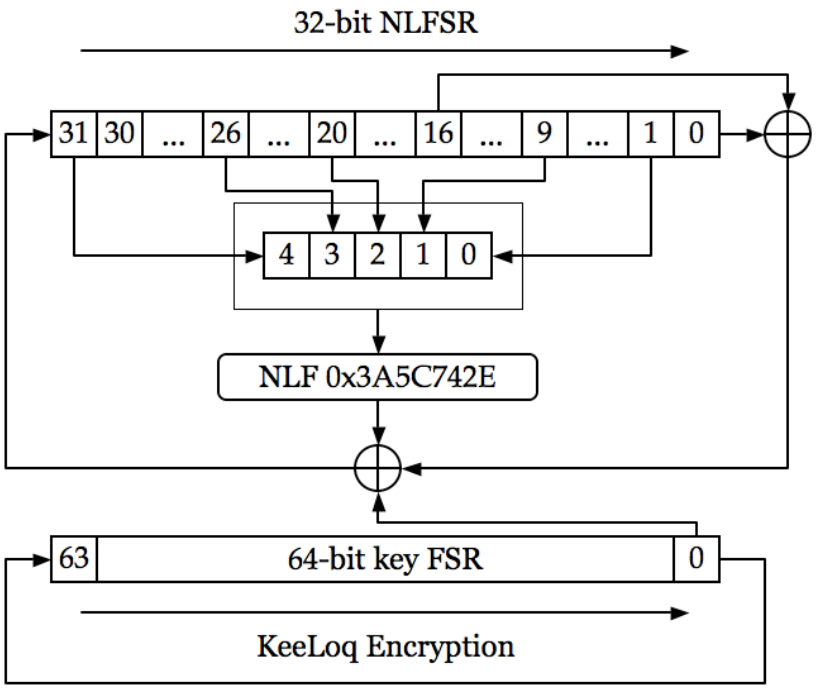
NLFSR comprising a 5x1 non-linear function

Simple key management: key is constantly rotated

528 rounds, each round one key bit is read

→ Lightweight cipher – cheap and efficient in hardware

KeeLoq Encryption

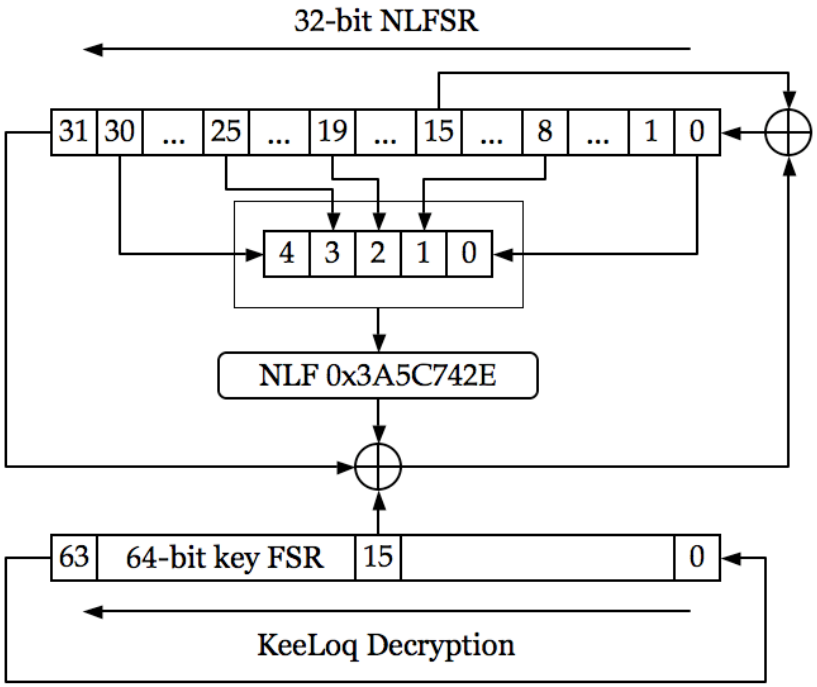


- 32 bit block length, 64 bit key
- NLFSR comprising a 5x1 non-linear function
- Simple key management: key is constantly rotated
- **528** rounds, each round one key bit is read

✂ → Lightweight cipher – cheap and efficient in hardware

source: Wikipedia

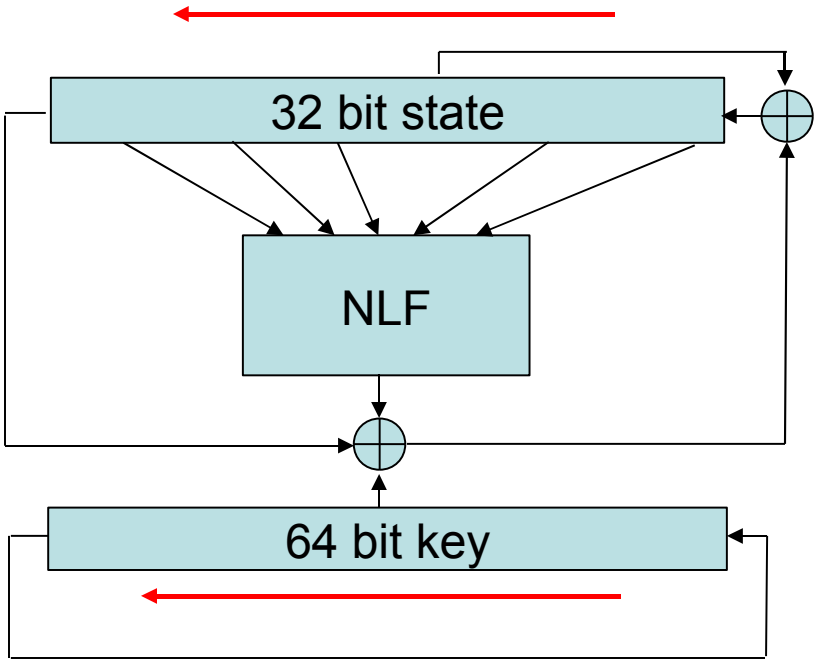
KeeLoq Decryption



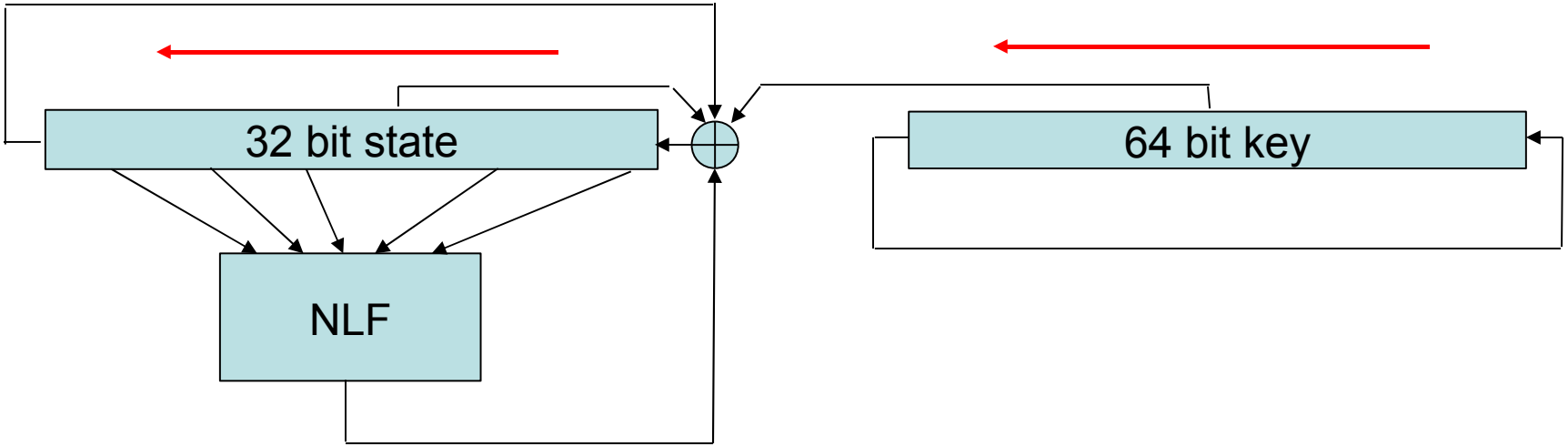
like encryption, but
in reverse order ☺

source: Wikipedia

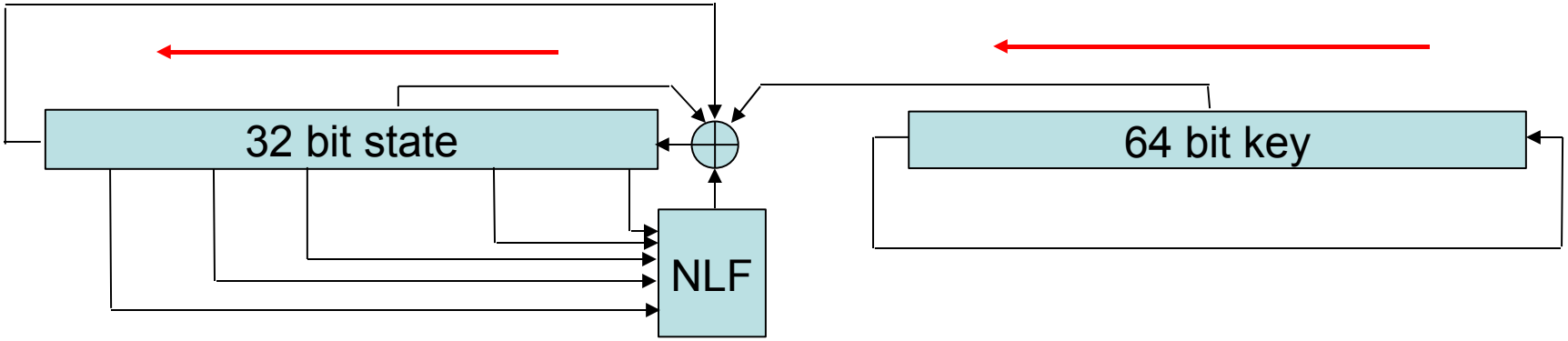
KeeLoq Decryption



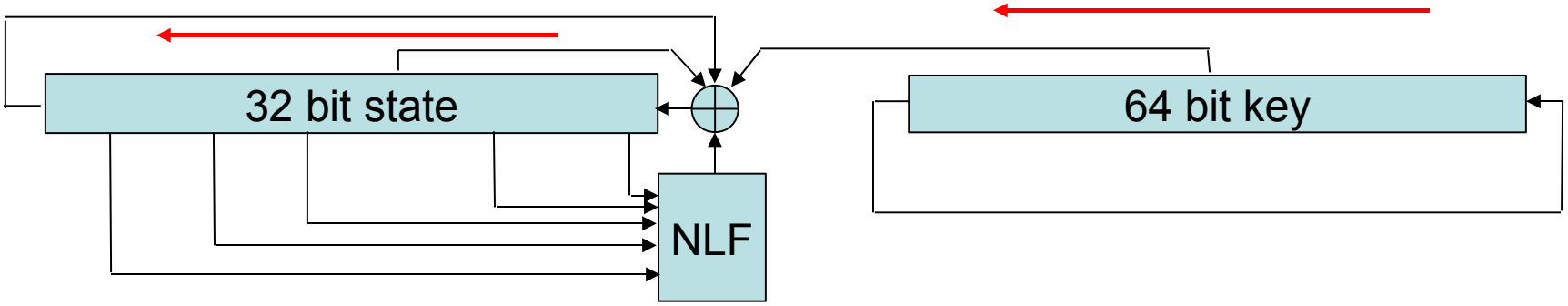
KeeLoq Decryption



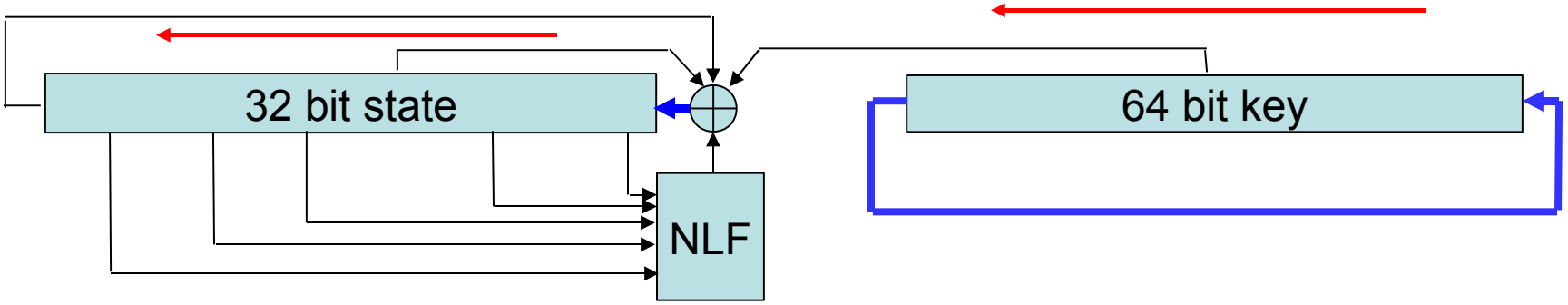
KeeLoq Decryption



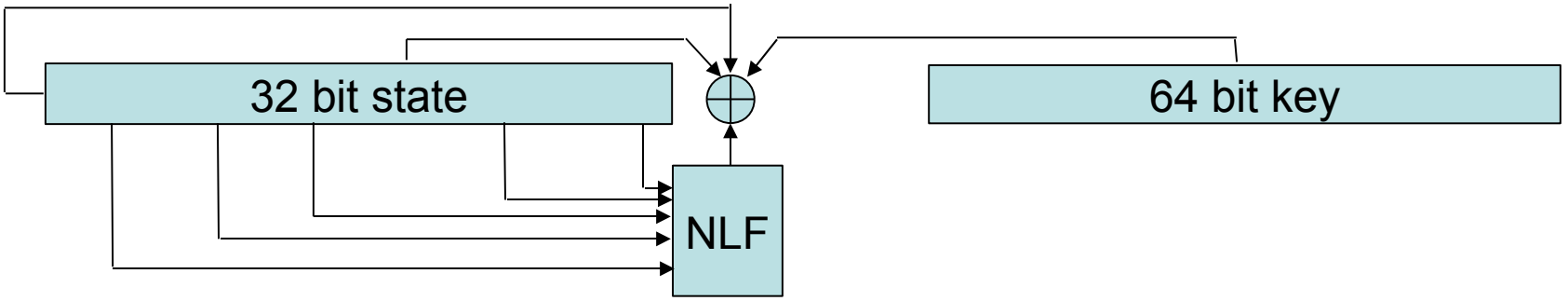
KeeLoq Decryption



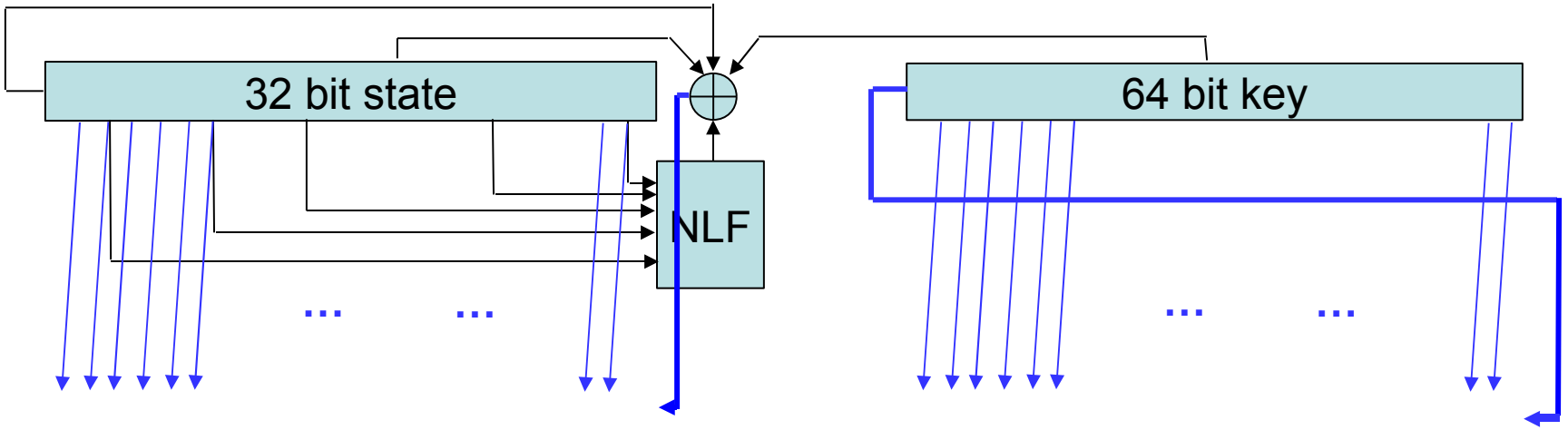
KeeLoq Decryption



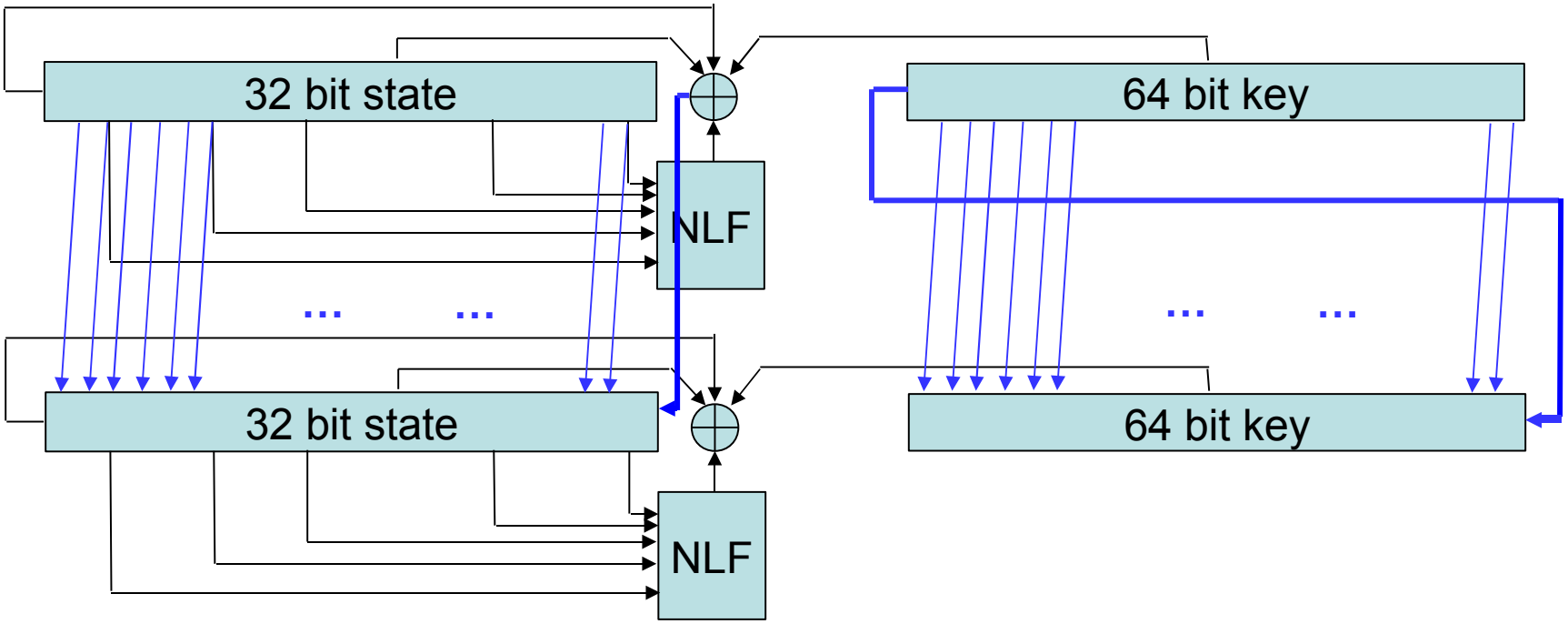
Unrolled KeeLoq Decryption



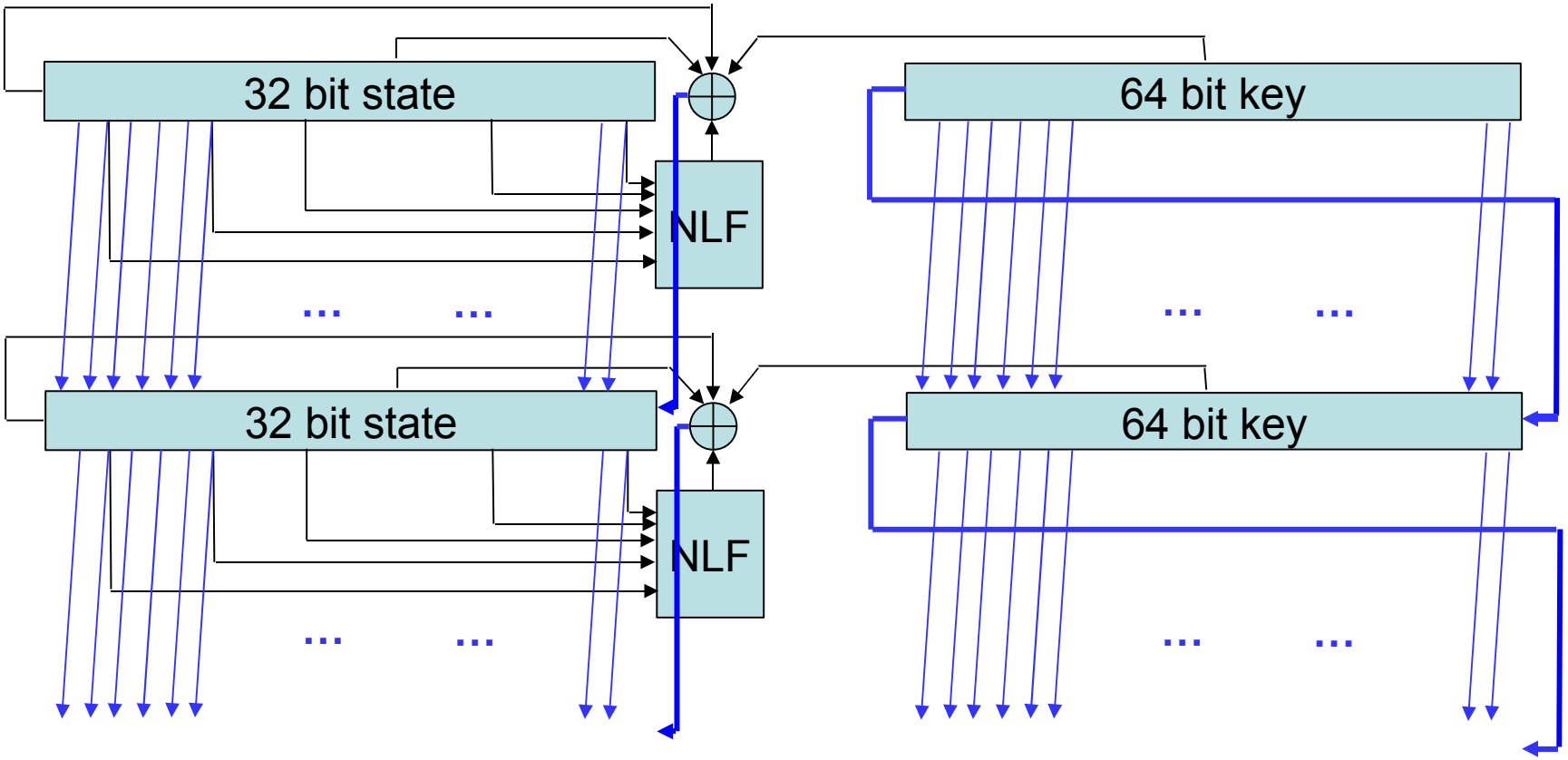
Unrolled KeeLoq Decryption



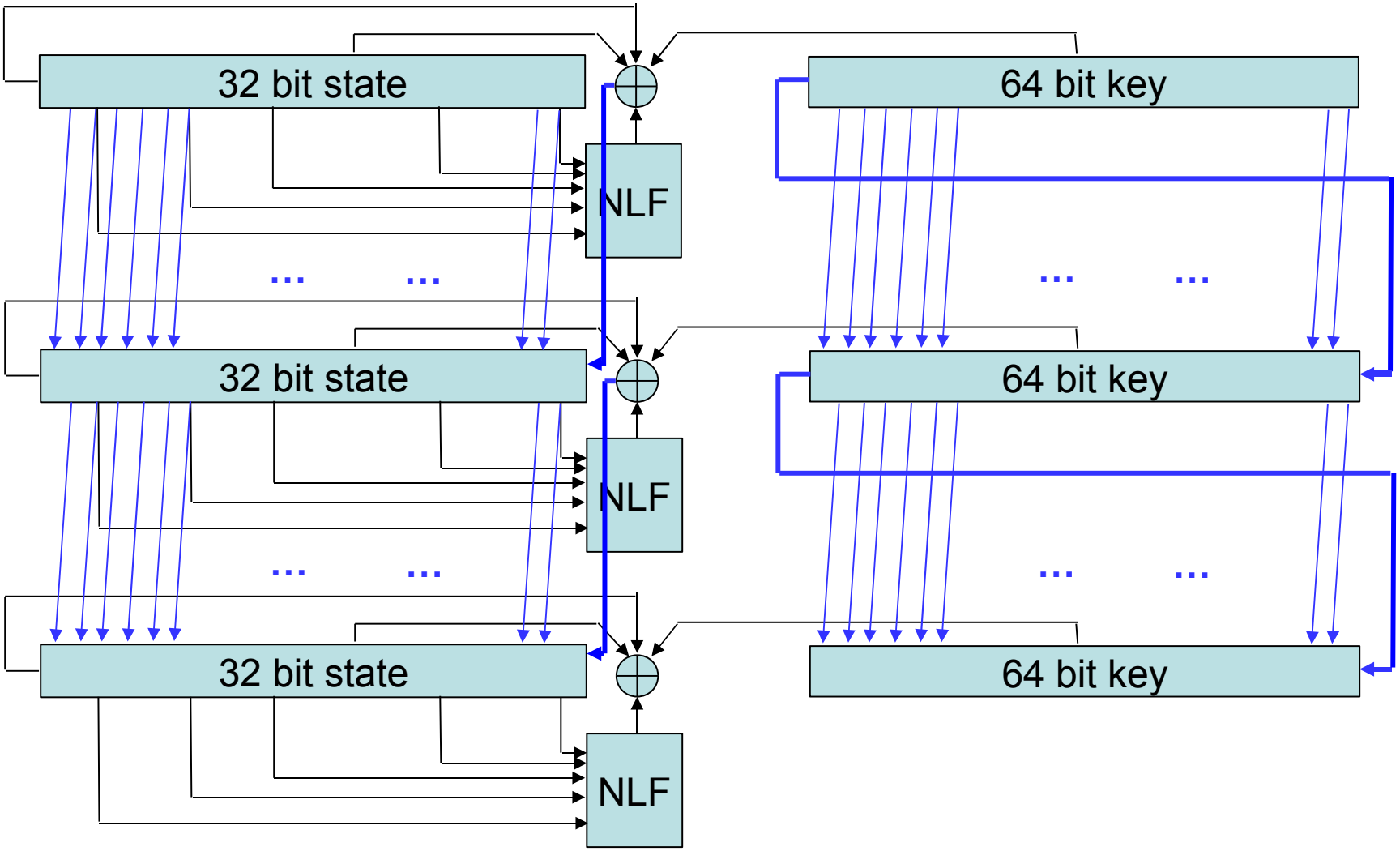
Unrolled KeeLoq Decryption



Unrolled KeeLoq Decryption

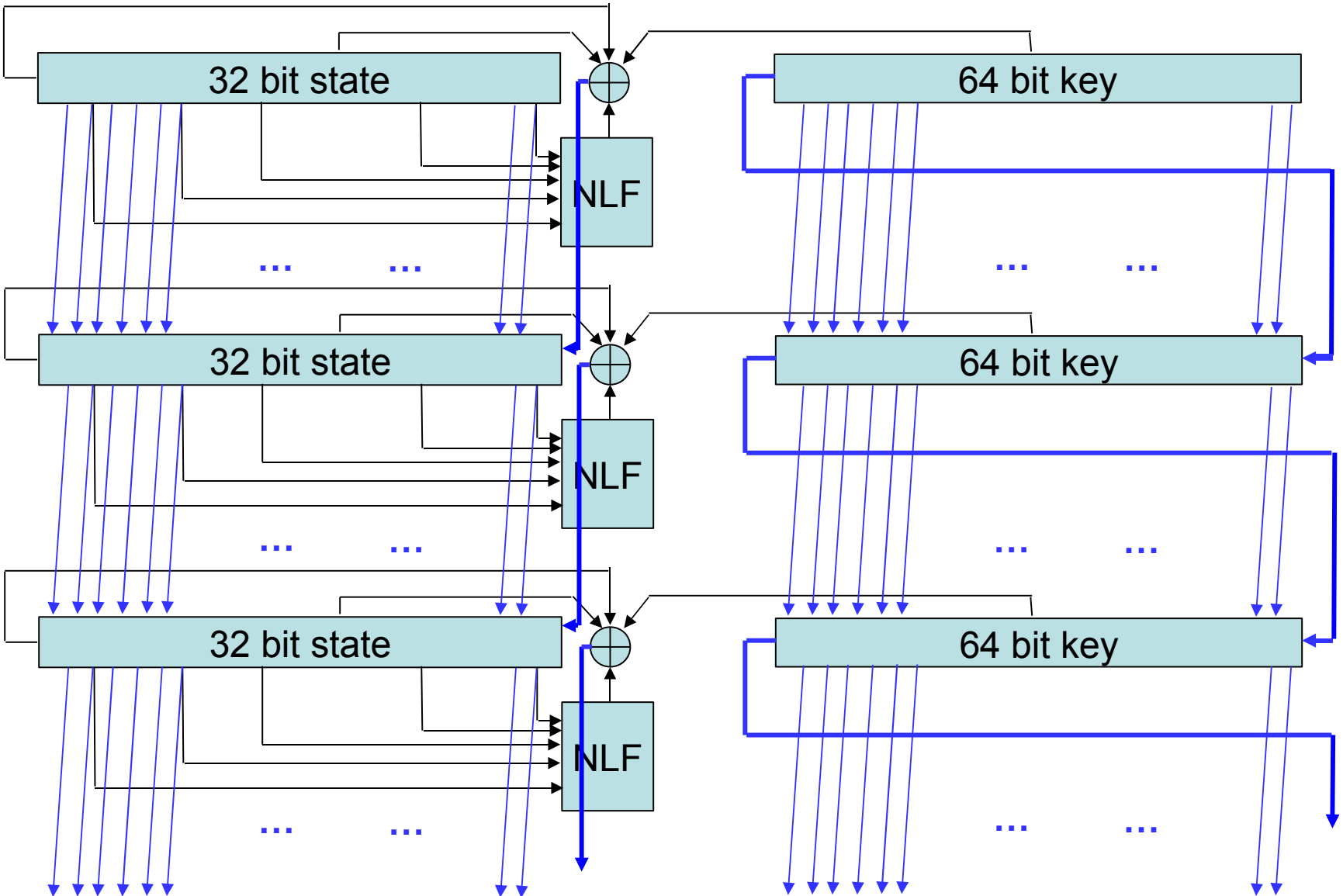


Unrolled KeeLoq Decryption



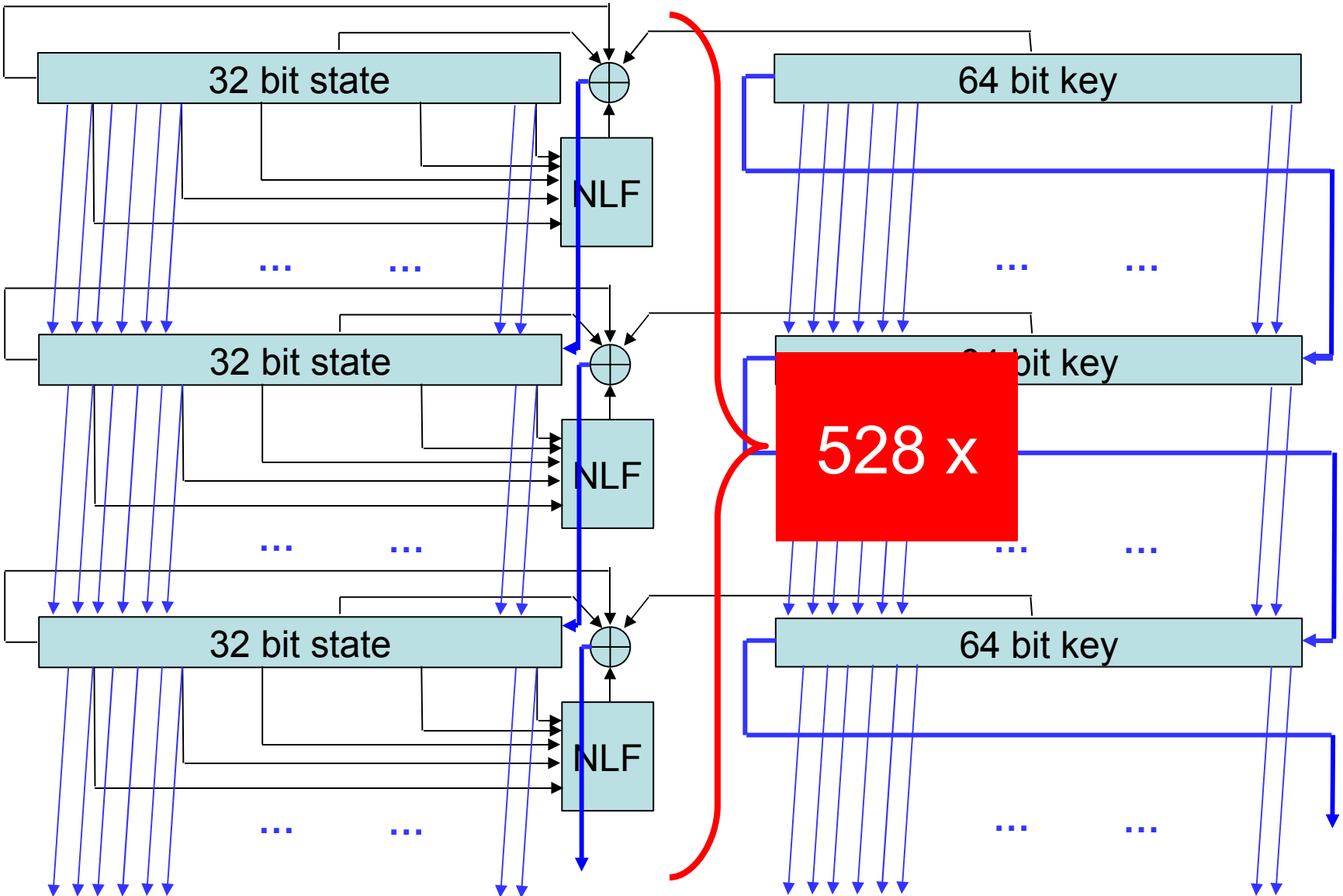
Unrolled KeeLoq Decryption

Horst Görtz Institute for IT-Security



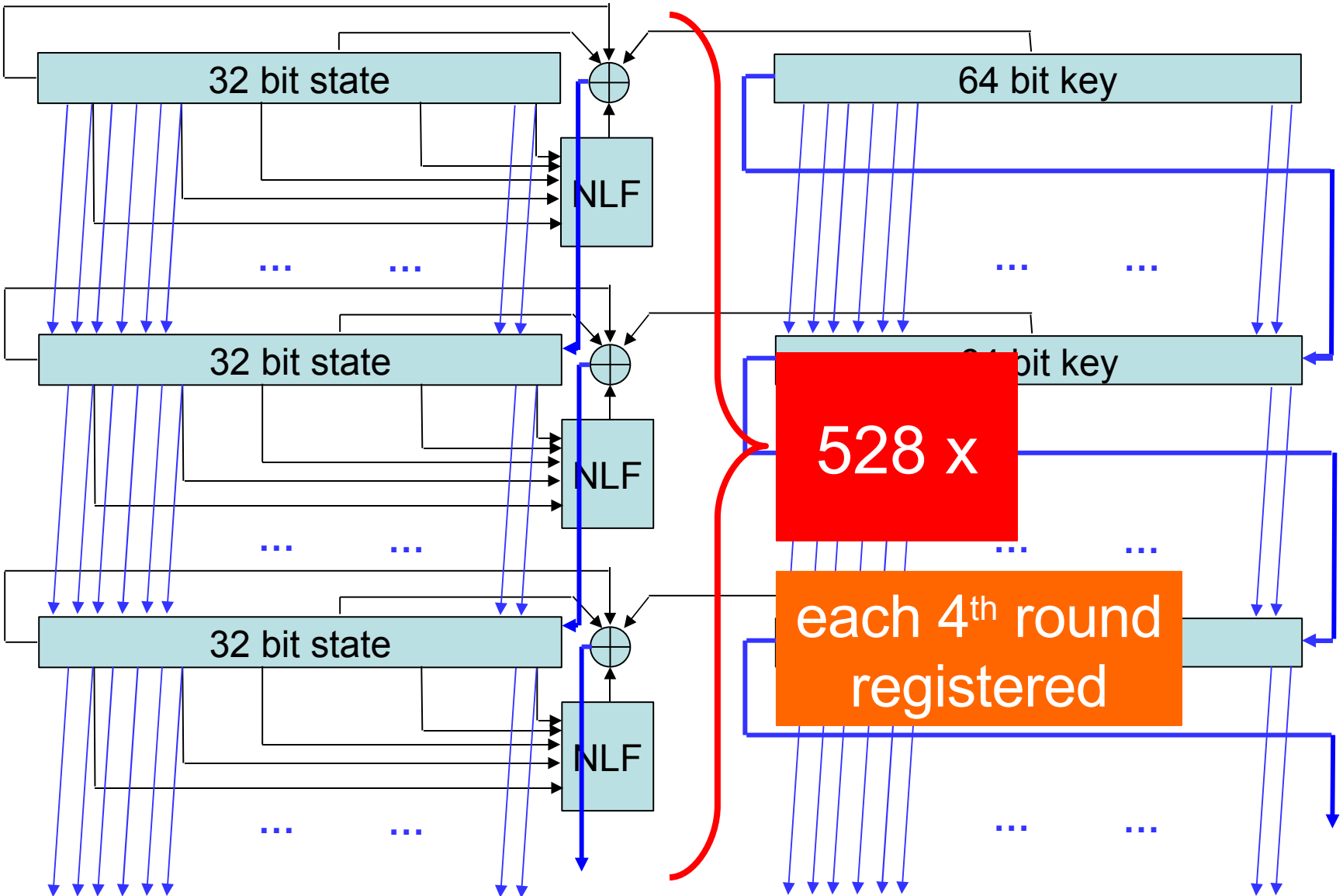
Unrolled KeeLoq Decryption

Horst Görtz Institute for IT-Security



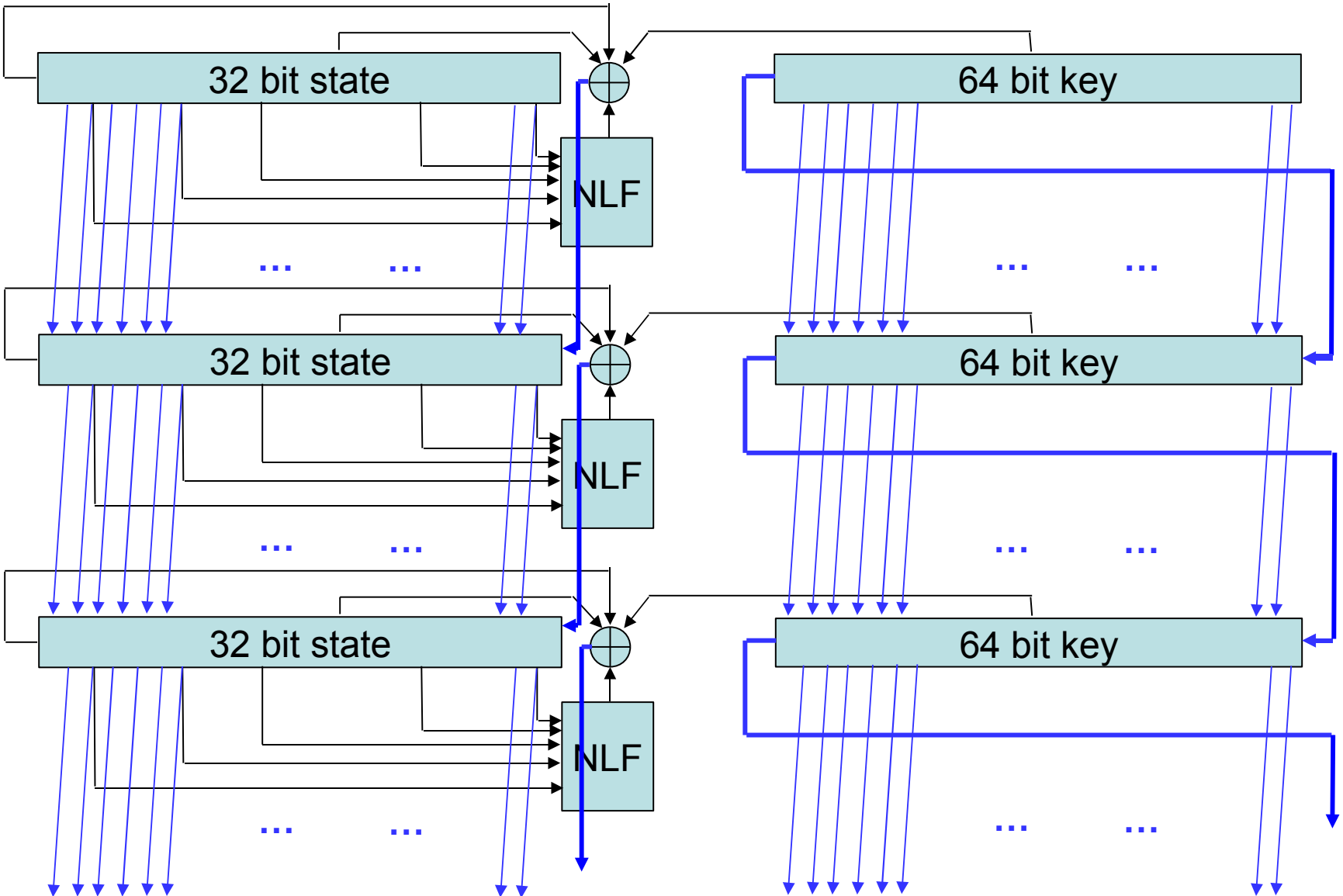
Unrolled KeeLoq Decryption

Horst Görtz Institute
for IT-Security



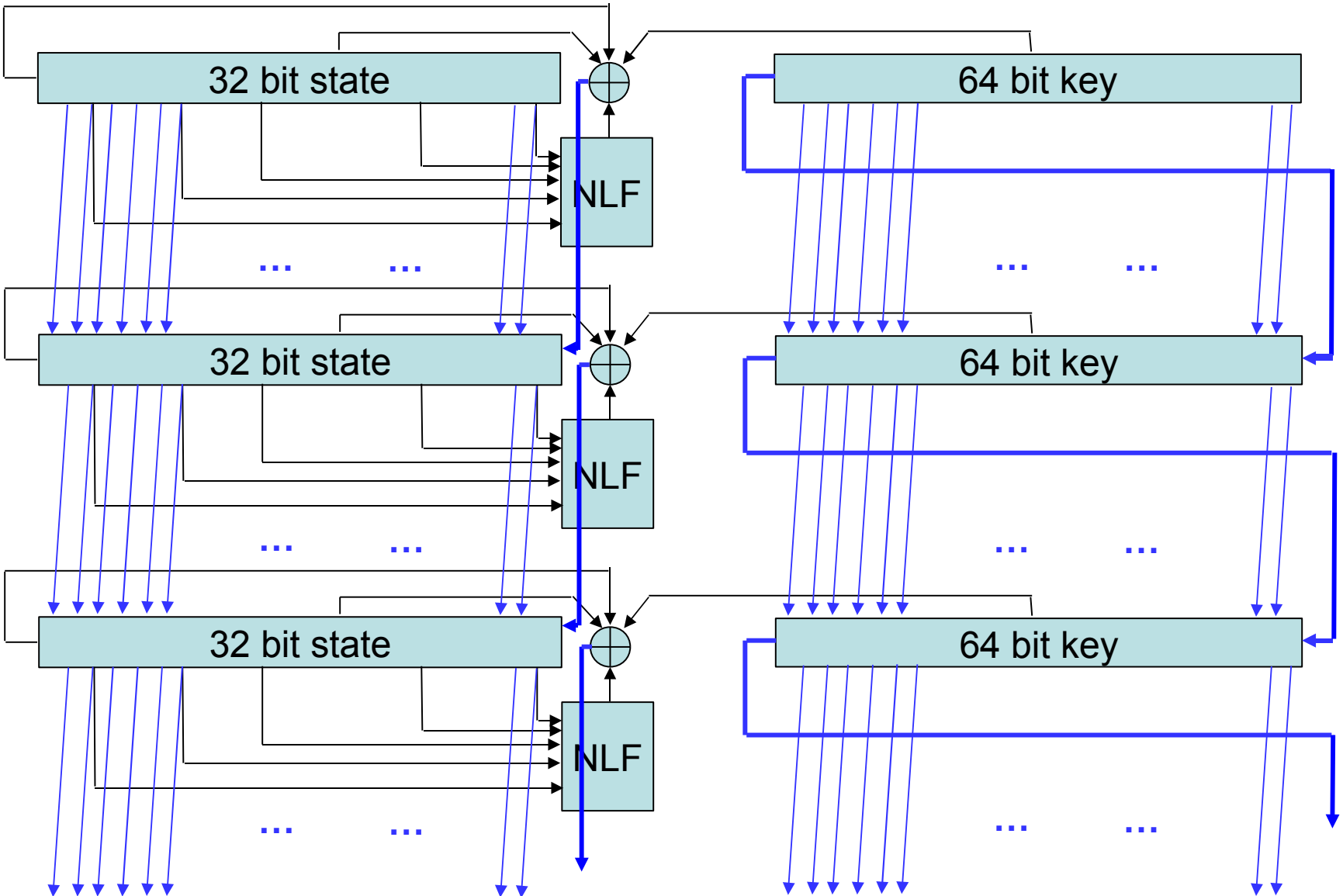
Unrolled KeeLoq Decryption

Horst Görtz Institute for IT-Security



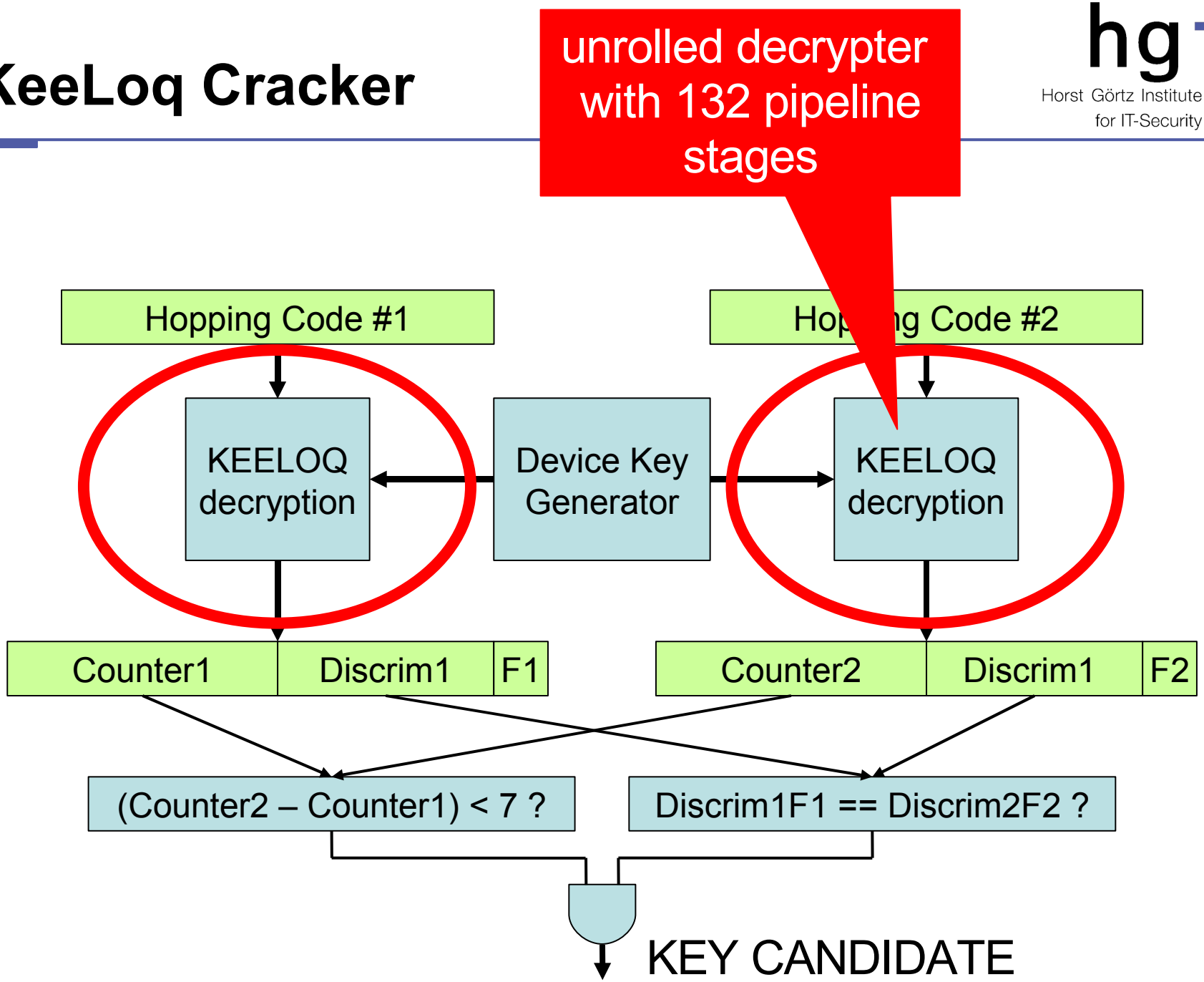
Unrolled KeeLoq Decryption

Horst Görtz Institute for IT-Security



KeeLoq Cracker

Horst Görtz Institute for IT-Security



Results

f_{max} = 110 MHz

110 million keys/s verified in 1 FPGA Spartan 3-1000

32 bit seed:	39 seconds / 1 FPGA
48 bit seed:	5.9 hours / 1 COPACOBANA
60 bit seed:	1011 days / 1 COPACOBANA