Construction, Analysis, Modification and Security of 128-EIA3

Peng Wang
SKLOIS, China

*

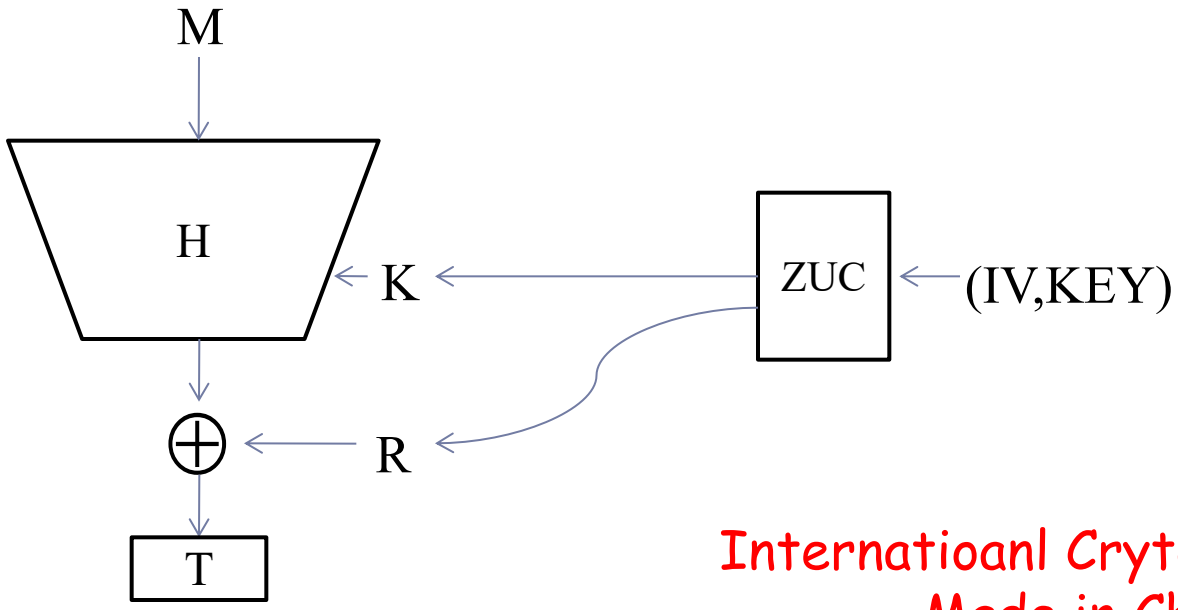
Outline

- 1) Introduction
- 2) Construction of 128-EIA3
- 3) Analysis of 128-EIA3
- 4) Modification of 128-EIA3
- 5) Security of 128-EIA3

1) Introduction

What is 128-EIA3?

- 128-EIA3 is a message authentication code based on stream cipher ZUC.
- 128-EIA3 has been adopted as the third integrity algorithm in the emerging 3GPP standard LTE.



Internatioanl Cryto Standard
Made in China

祖冲之密码算法成国际标准

祖冲之算法集

求助编辑　编辑词条

本
53次第三
被批准
首次走
据
别、完
运
件的人
法，对

祖冲之算法
28-EIA3，已经
究所信息安全国
年12月2至3在
开平评估范围，
意义。

据了解，在
带无线移动通信
学者自主设计的
28-EEA3和完整
馈移位寄存器(L

*

3GPP批准我国祖冲之密码算法成为国际标准

http://www.sina.com.cn 2011年09月27日 17:50 中华人民共和国工业和信息化部

9月19日-21日，在日本福岗召开的第53次第三代合作伙伴计划(3GPP)系统架构组(SA)会议上，我国祖冲之密
国商用密码算法首
祖冲之密码算
信研究院推荐给3GP
包括加密算法128-E

在工业和信息
多时间，得到了国
影响力，对我国移

祖冲之算法LTE国际标准产业化启动

2011年11月25日 14:30　来源：赛迪网　热点专题　手机看新闻

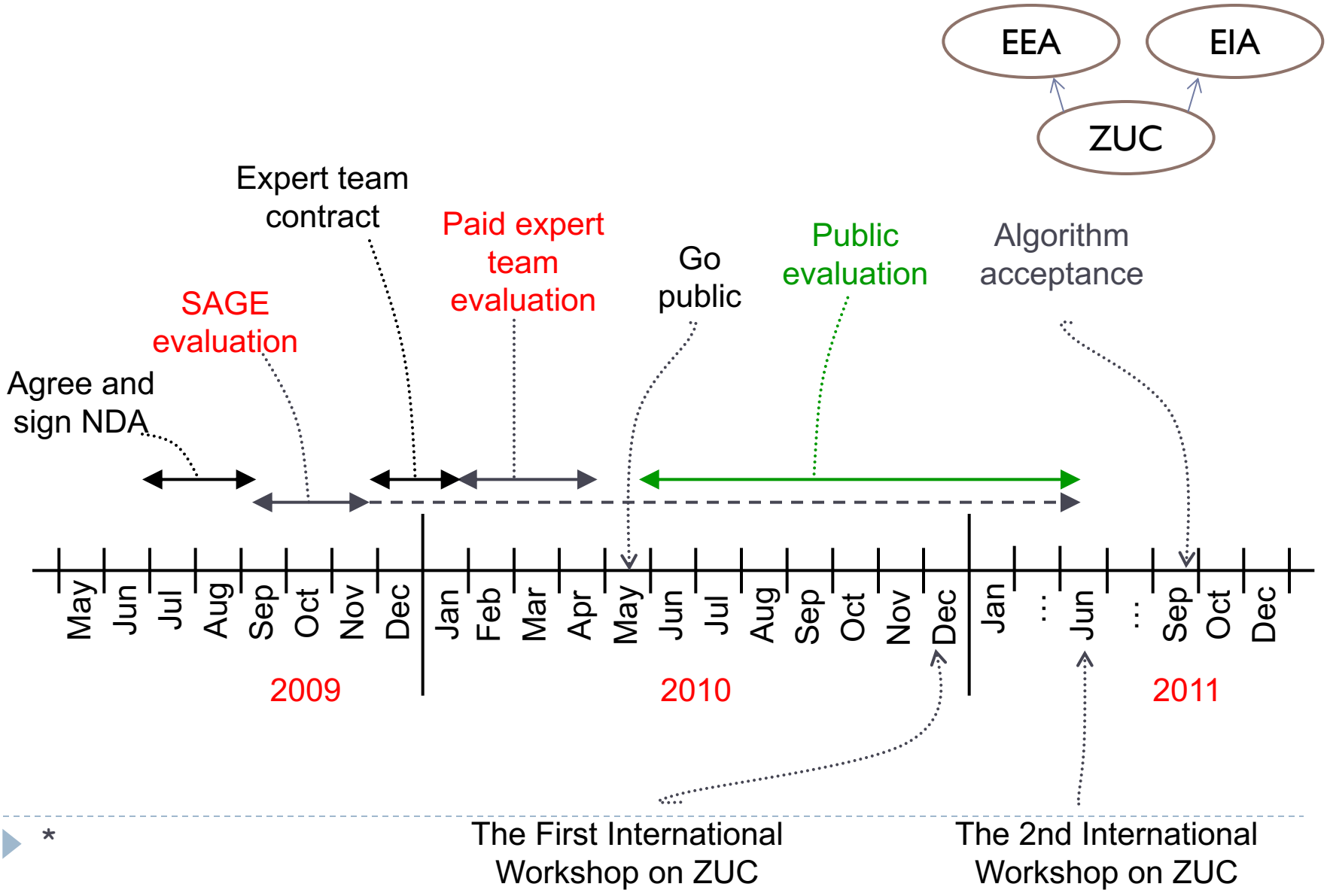
打印　网摘　纠错　商城　关注 71.1万　分享　推荐　微博　字号

科轩

本报讯 11月23日，工业和信息化部和国家密码管理局共同在北京举行祖冲之算法LTE国际标准研发和产业化启动会，研究部署祖冲之算法在移动通信领域的产业化推进工作。工业和信息化部杨学山副部长、国家密码管理局魏允韬局长出席会议并致辞。

杨学山指出，祖冲之算法成为LTE国际标准是通信行业和密码行业企事业单位共同努力、密切合作的成果，充分体现了我国商用密码应用的开放性和密码设计的水平，对保障移动通信网络信息安全和推动我国商用密码走向世界具有重要意义。杨学山要求，要提高认识，深刻领会在移动通信领域推广应用祖冲之算法的重要意义；要抓好落实，加快推进祖冲之算法产业化工作；要突出重点，着力加强标准制定、核心产品研制和试验验证等工作。

Standardization progress



*

Security Algorithms

A variety of security algorithms are used to provide authentication, cipher key generation, integrity and radio link privacy to users on mobile networks. Details of the various algorithms and how they can be obtained are provided below.

3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3

July 2011: ** NEW ** Prospective FINAL VERSIONS of the Algorithms 128-EEA3 & 128-EIA3 are now available for download. The algorithms themselves are identical to the ones published in January 2011, although some text in the documents has changed slightly. The documents have been submitted to the 3GPP Security Group, which will decide whether they can be recommended for inclusion in the LTE standards. The documents have not yet been through final 3GPP approval, hence they are still preliminary draft algorithm specifications, provided for evaluation purposes only, and potentially subject to change.

January 2011: ** NEW ** REVISED VERSIONS of the Algorithms 128-EEA3 & 128-EIA3 are available for download prior to approval and publication of a final version by 3GPP. These revised versions were published in January 2011. They are still preliminary draft algorithm specifications, provided for evaluation purposes only, and subject to change.

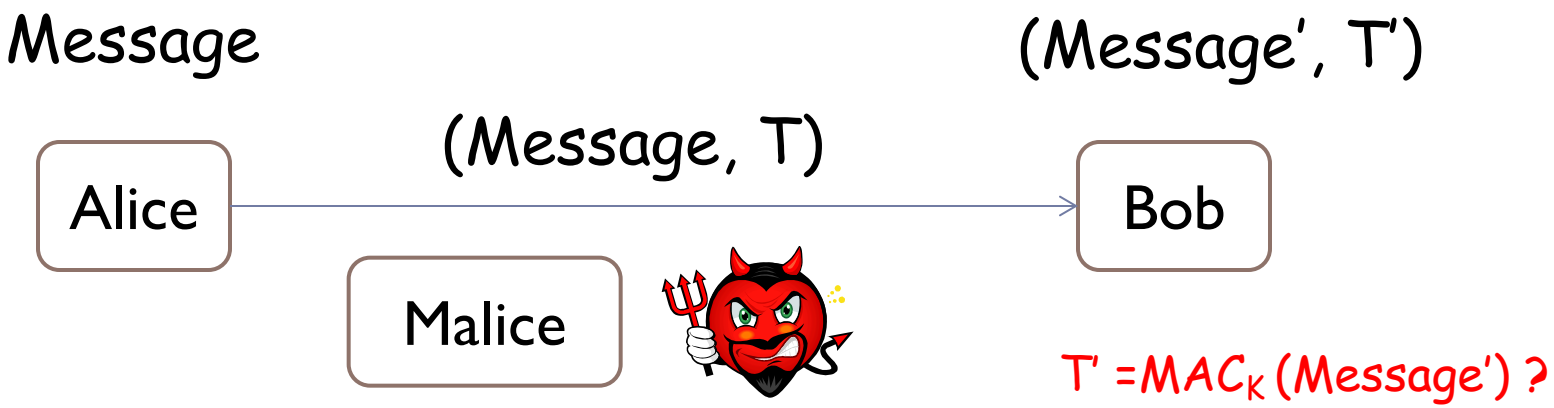
The draft specifications are as follows:

Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3 Revised versions published July 2011	**Document 1:** Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: 128-EEA3 & 128-EIA3 Specification	pdf doc
	Document 2: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: ZUC Specification	pdf doc
	Document 3: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: Implementor's Test Data	pdf doc
	Document 4: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: Design and Evaluation Report	pdf doc

*

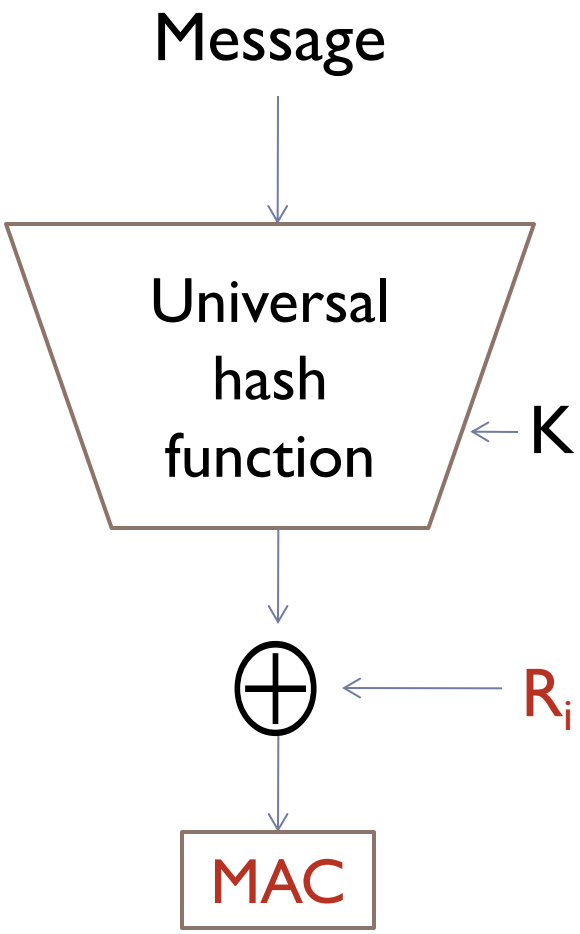
Message Authentication Code (MAC)

- ✓ Data integrity protection
- ✓ Data origin authentication



$T = MAC_K(Message)$

MACs based on Universal hash functions



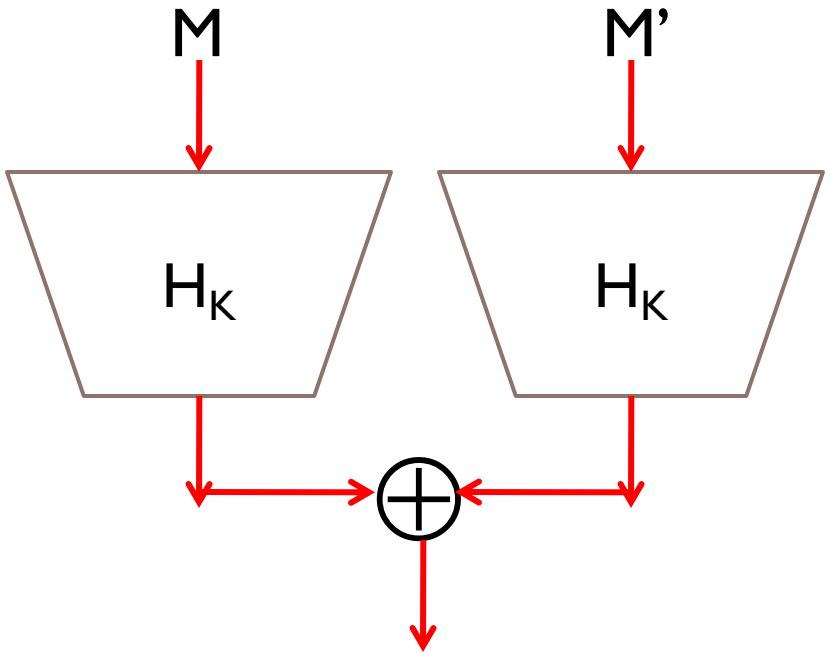
1) hash

2) mask

One Time Pad encryption

Wegman-Carter Scheme

Almost **X**or **U**niversal hash function [K94]



$H: \mathbf{K} \times \mathbf{D} \rightarrow \mathbf{R}$

$H_K(M) = C$

ε-AXU: $Pr_{K \in \mathbf{K}} [H_K(M) \oplus H_K(M') = C] \leq \varepsilon, \quad \forall \; M \neq M', C$

Why hash-then-mask works?

If we know (M, T) $\quad H_K(M) \oplus R = T$

We try to forge (M', T') $\quad H_K(M') \oplus R = T', M \neq M'$

$H_K(M') \oplus R = T' \iff H_K(M) \oplus H_K(M') = T \oplus T'$

Prob. $\leq \varepsilon$

Example of AXU functions (1)

- H: $\mathbf{\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n}$
- $H(K,M) = K \cdot M$
- $1/2^n$-AXU

Examples of AXU functions (2)

- Polynomial Evaluation Hash Function
- $H: \{0,1\}^n \times \{0,1\}^{nm} \rightarrow \{0,1\}^n$
- $H(K,M) = f(K)$
- $f(x) = M_1 x^m + M_2 x^{m-1} + \ldots + M_m x$
- $m/2^n$-AXU

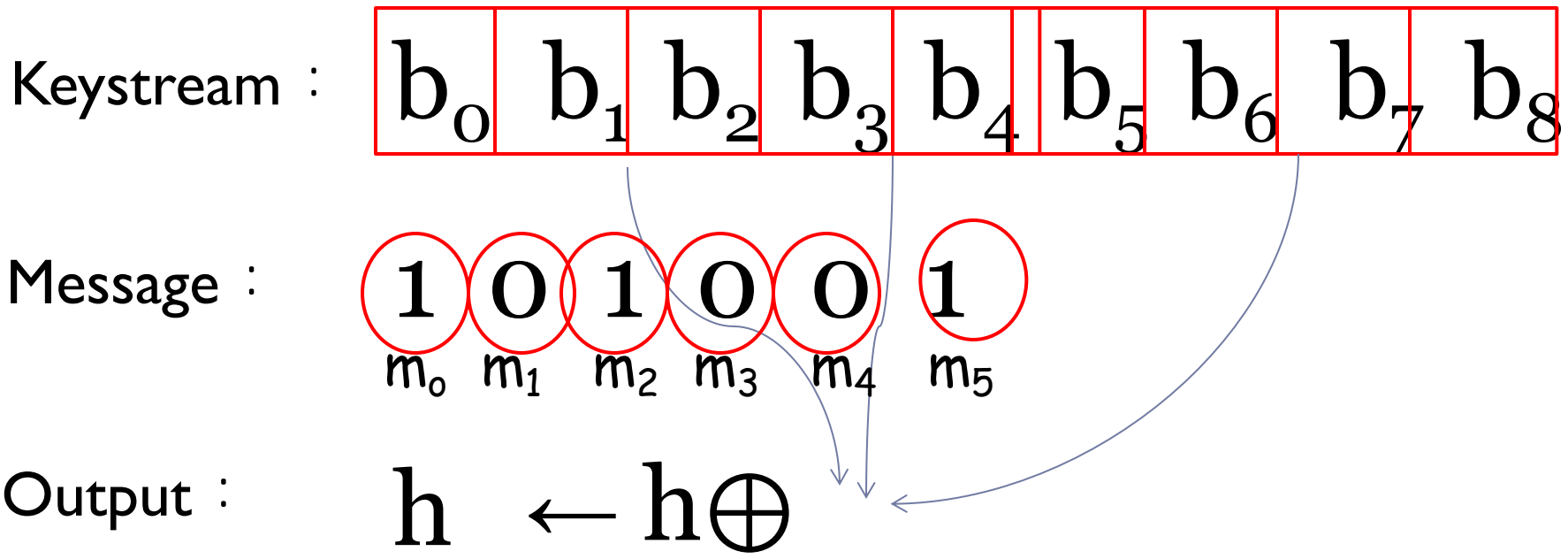
Universal hashing MAC

- Rogaway : Bucket hashing (1995)
- Halevi-Krawczyk : MMH (1997)
- Black-Halevi-Krawczyk-Krovertz-Rogaway : UMAC (1999)
- Bernstein: Poly1305(2005)
- ……

2) Construction of 128-EIA3

Toeplitz matrix based AXU function [K95]

|Output|=4, |Message|=6



in matrix form

b_0	b_1	b_2	b_3	b_4	b_5
b_1	b_2	b_3	b_4	b_5	b_6
b_2	b_3	b_4	b_5	b_6	b_7
b_3	b_4	b_5	b_6	b_7	b_8

$\cdot$

m_0
m_1
m_2
m_3
m_4
m_5

Toeplitz matrix

or

m_0	m_1	m_2	m_3	m_4	m_5	0	0	0
0	m_0	m_1	m_2	m_3	m_4	m_5	0	0
0	0	m_0	m_1	m_2	m_3	m_4	m_5	0
0	0	0	m_0	m_1	m_2	m_3	m_4	m_5

$\cdot$

b_0
b_1
b_2
b_3
b_4
b_5
b_6
b_7
b_8

Generally

For a l-bit message M= (m_0,m_1, …, m_{l-1})

We need (l+n-1)-bit keystream:

$$K = b_0, b_1, \underbrace{b_2, \ldots \ldots}_{W_i}, b_{l+n-2}$$

$$H'_K(M) = \bigoplus_{i=0}^{l-1} m_i W_i$$

H is **1/2^n-AXU**

But

- The above result only holds for fixed-length messages.
- How to treat variable-length messages？

We notice that

- $H'_K(M)=H'_K(M0\ldots0)$
- For different-length messages M and M', $|M|<|M'|$
- we can pad M with 0s， s.t.
- $|M0\ldots0|=|M'|$
- but we want differences after padding

How?

- We only need pad 1 after M.

$$M \rightarrow M\,1$$

$$H'_K(\mathbf{M}) = \bigoplus_{i=0}^{l-1} m_i W_i$$

$$H_K(M) = H'_K(\mathbf{M1}) = \left(\bigoplus_{i=0}^{l-1} m_i W_i\right) \oplus W_\ell$$

*

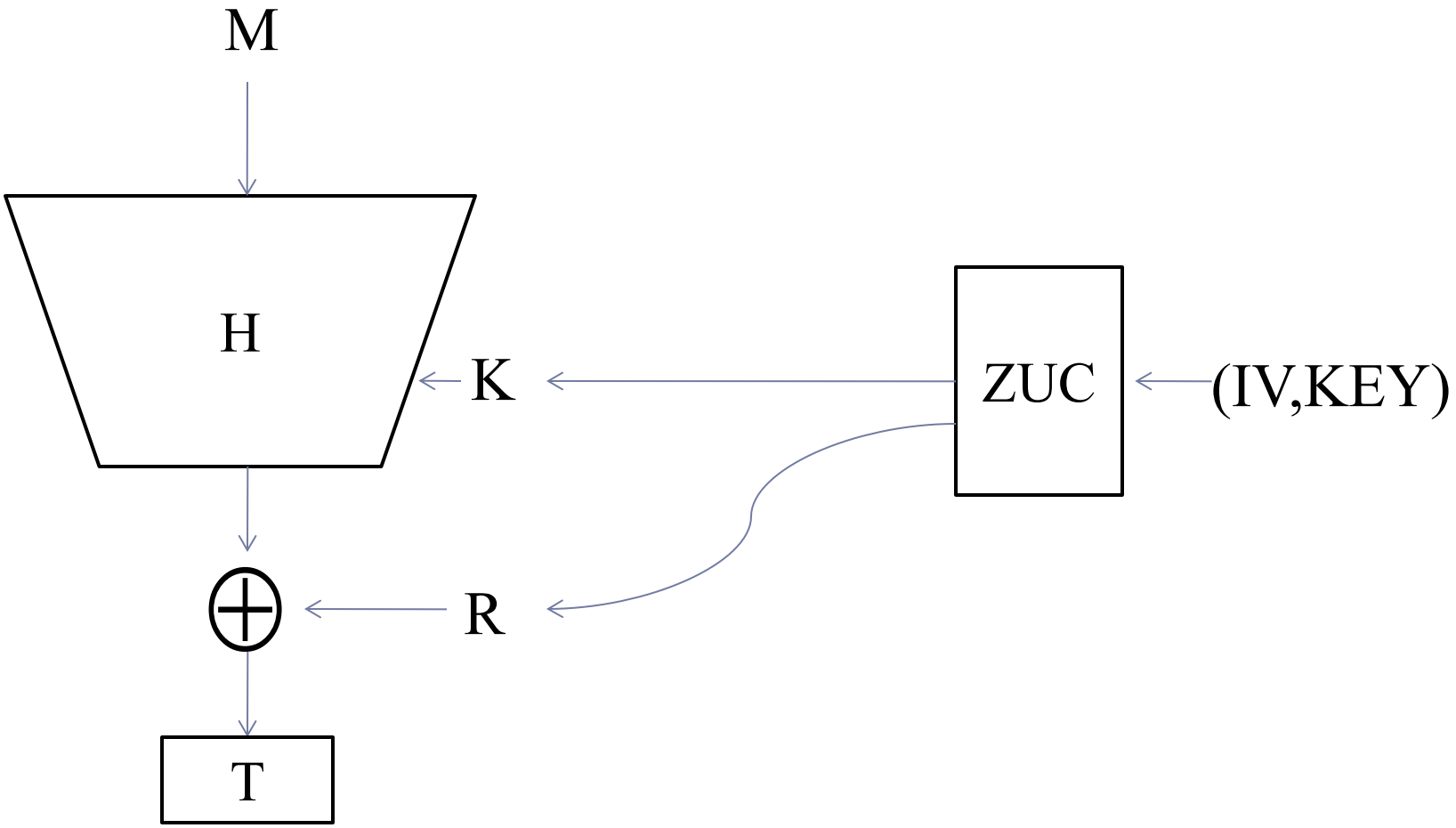
128-EIA3 v1.4

$b_0, b_1, \ldots b_{31}, \ldots, b_{l+31}, \ldots, b_{l+31}, b_{l+32} \ldots\ldots, b_{l+63}$

$$T = \left[\left(\bigoplus_{i=0}^{\ell} m_i W_i \right) \oplus W_\ell \right] \oplus W_{mask}$$

- Unfortunately, choose the mask value the wrong way

128-EIA3



$$128\text{-EIA3}(IV, KEY, M) = H(K,M) \oplus R$$

128-EIA3 v1.4

ZUC(IV,KEY)

$b_0, b_1, \ldots b_{31}, \ldots, b_{l+31}, \ldots, b_{l+31}$ $b_{l+32} \ldots\ldots, b_{l+63}$

W_0 W_1 W_{l-1} W_l W_{mask}

$$T = \left[\left(\bigoplus_{i=0}^{\ell-1} m_i W_i \right) \oplus W_\ell \right] \oplus W_{mask}$$

$$T = H(K, M) \oplus R$$

*

3) Analysis of 128-EIA3

T. Fuhr, H. Gilbert, J. Reinhard, and M. Videau. Analysis of the initial and modified version of the candidate 3GPP integrity algorithm 128-EIA3. SAC 2011.

Introduction to 128-EIA3

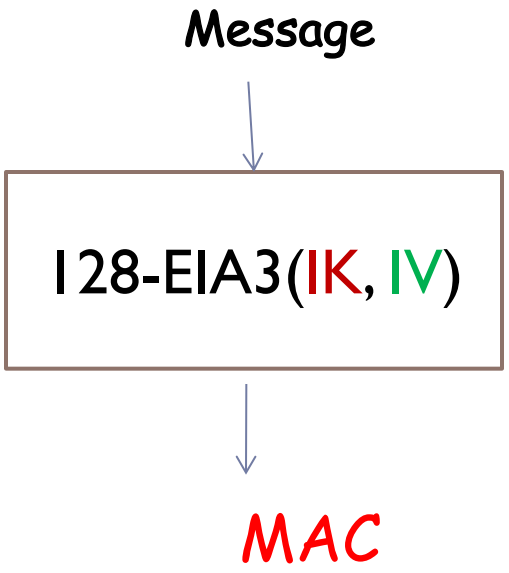
- IV-dependent MAC

  1) a 128-bit key

  2) 128-bit initial vector

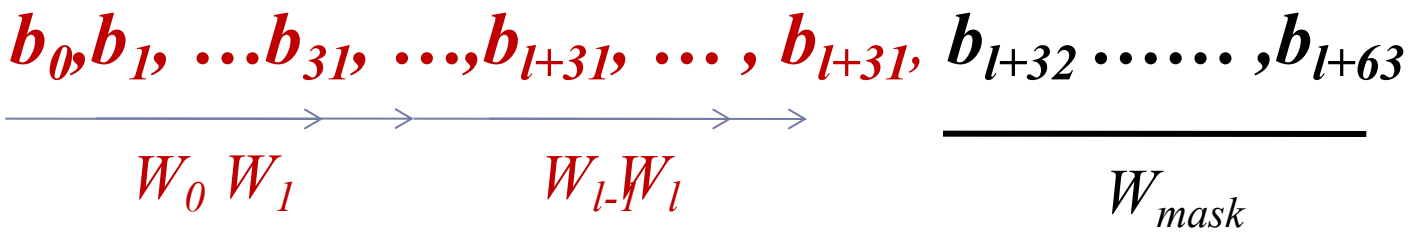
  3) a 1-20000 bits **message**

  4) 32-bit MAC value



- Security Goal: Unforgeability

  Infeasible to generate a new valid (IV, **Message**, MAC)



$$T = \left[\left(\bigoplus_{i=0}^{\ell} m_i W_i \right) \oplus W_\ell \right] \oplus W_{mask}$$

Some observations

- **W_i s are not independent**

$$W_{i+1} = ((W_i \ll 1), b_{i+32})$$

- **W_{mask}s are also related for the same IV**

$$W'_{mask} = ((W_{mask} \ll 1), b)$$

if $l' = l+1$

For two different messages and the same IV…

$$M = (m_0, \ldots, m_{\ell-1}) \xrightarrow{(IK,IV)} T$$

$$M' = (0, m_0, \ldots, m_{\ell-1}) \xrightarrow{(IK,IV)} T'$$

$$\begin{aligned} T' &= (\bigoplus_{i=0}^{\ell} m'_i W_i) \oplus W_{\ell+1} \oplus W'_{mask} \\ &= (\bigoplus_{i=0}^{\ell-1} m_i W_{i+1}) \oplus W_{\ell+1} \oplus W'_{mask} \end{aligned}$$

$$= (\bigoplus_{i=0}^{\ell-1} m_i((W_i \ll 1), b_{i+32})) \oplus (W_\ell \ll 1, b_{\ell+32}) \oplus ((W_{mask} \ll 1), b_{\ell+64})$$

$$\begin{aligned} &= (((\bigoplus_{i=0}^{\ell-1} m_i W_i) \oplus W_\ell \oplus W_{mask}) \ll 1, \beta) \\ &= (T \ll 1, \beta) \end{aligned}$$

*

For two different messages and the same IV…

$$M = (m_0, \ldots, m_{\ell-1}) \xrightarrow{(IK,IV)} T$$

$$M' = (0, m_0, \ldots, m_{\ell-1}) \xrightarrow{(IK,IV)} T'$$

$$T' = (T \ll 1, \beta)$$

*

An Existential Forgery

- When we get (IV, M, T)

$$M = (m_0,\ldots,m_{l-1})$$

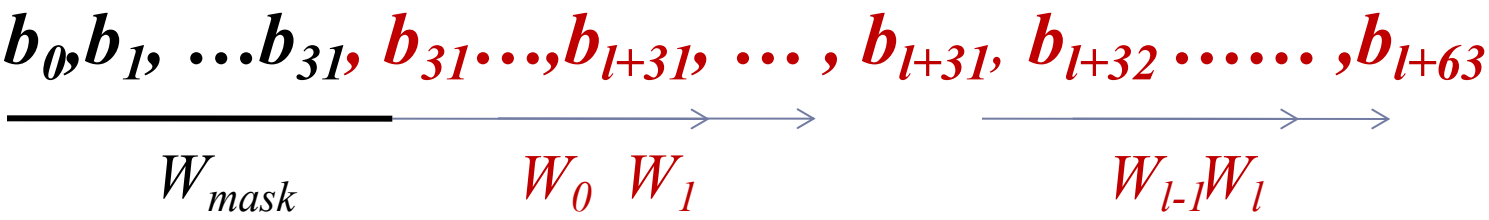
- We forge (IV, M', T')

$$M' = (0,m_0,\ldots,m_{l-1})$$

$$T' = (T<<1, \beta)$$

- The success probability is 1/2.

Modification: A slight variant of 128-EIA3



$$T = \left(\bigoplus_{i=0}^{\ell} m_i W_i \right) \oplus W_\ell \oplus W_{mask};$$

*

Conclusion

- 128-EIA3 v1.4 does not offer an adequate security.
- The identified weakness does neither relate to the core of 128-EIA3 v1.4,
- nor to the underlying stream cipher ZUC,
- But only to the way the mask values are derived from the keystream.

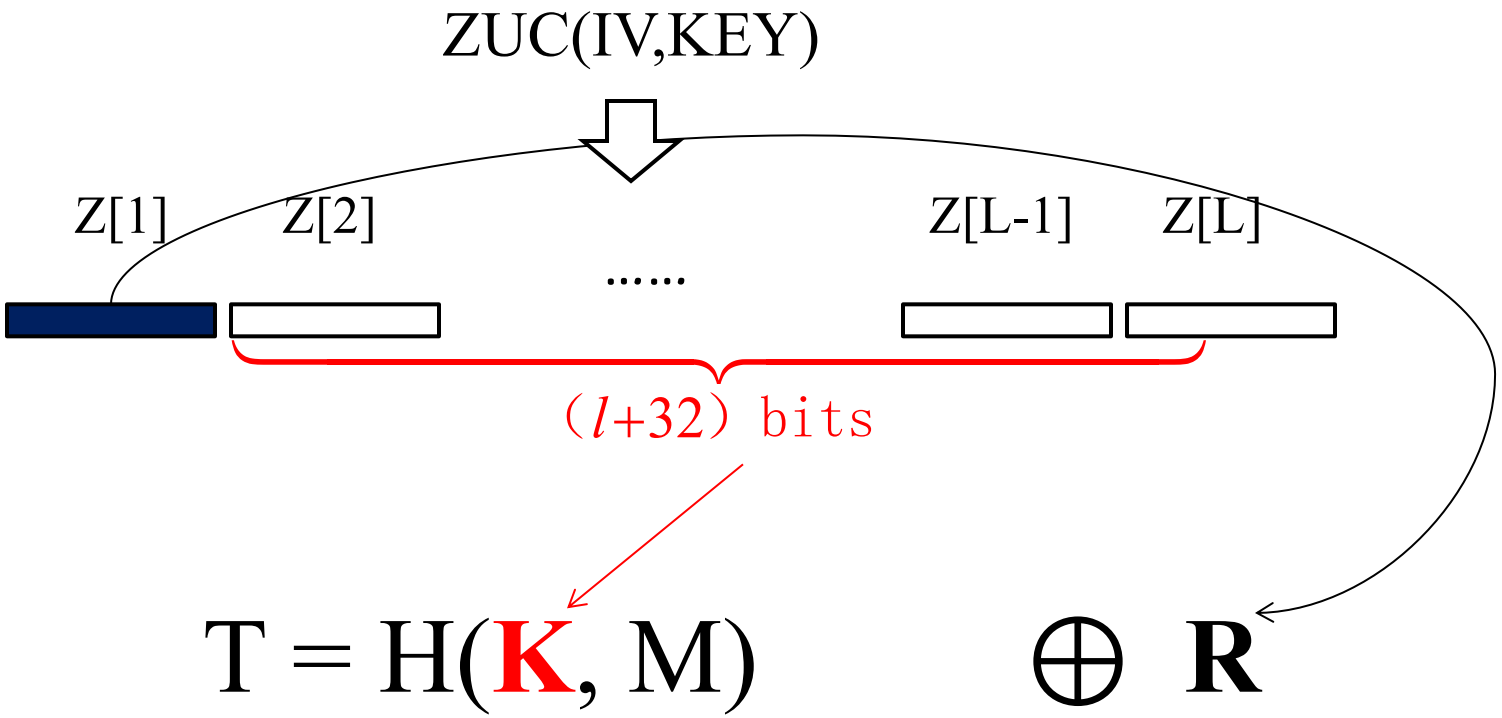
4) Modification of 128-EIA3

How to make modification?

- Big change?
  - ✓ New design
- Small tweak?
  - ✓ How to mask

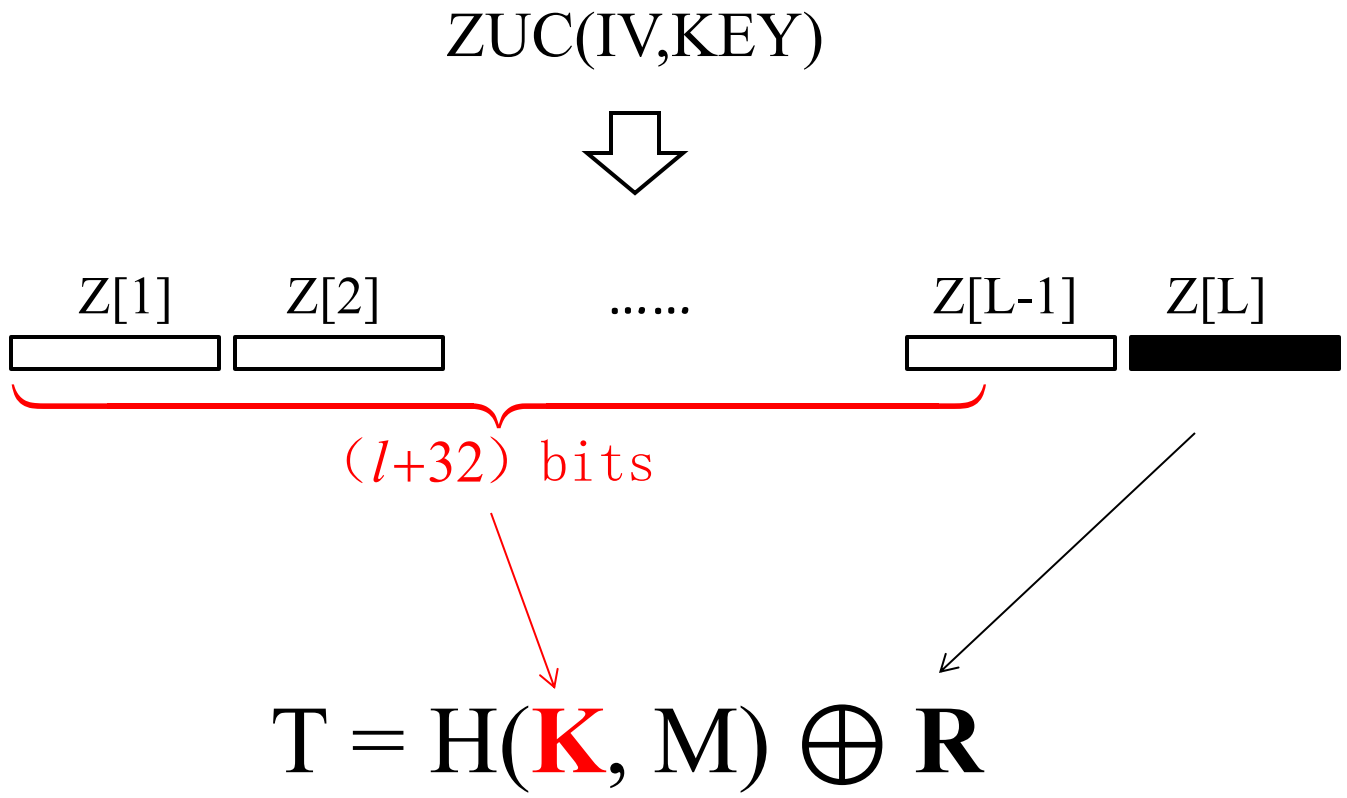
Tweak 1

Mask with first word [FGRV11]



Tweak 2

Mask with last word

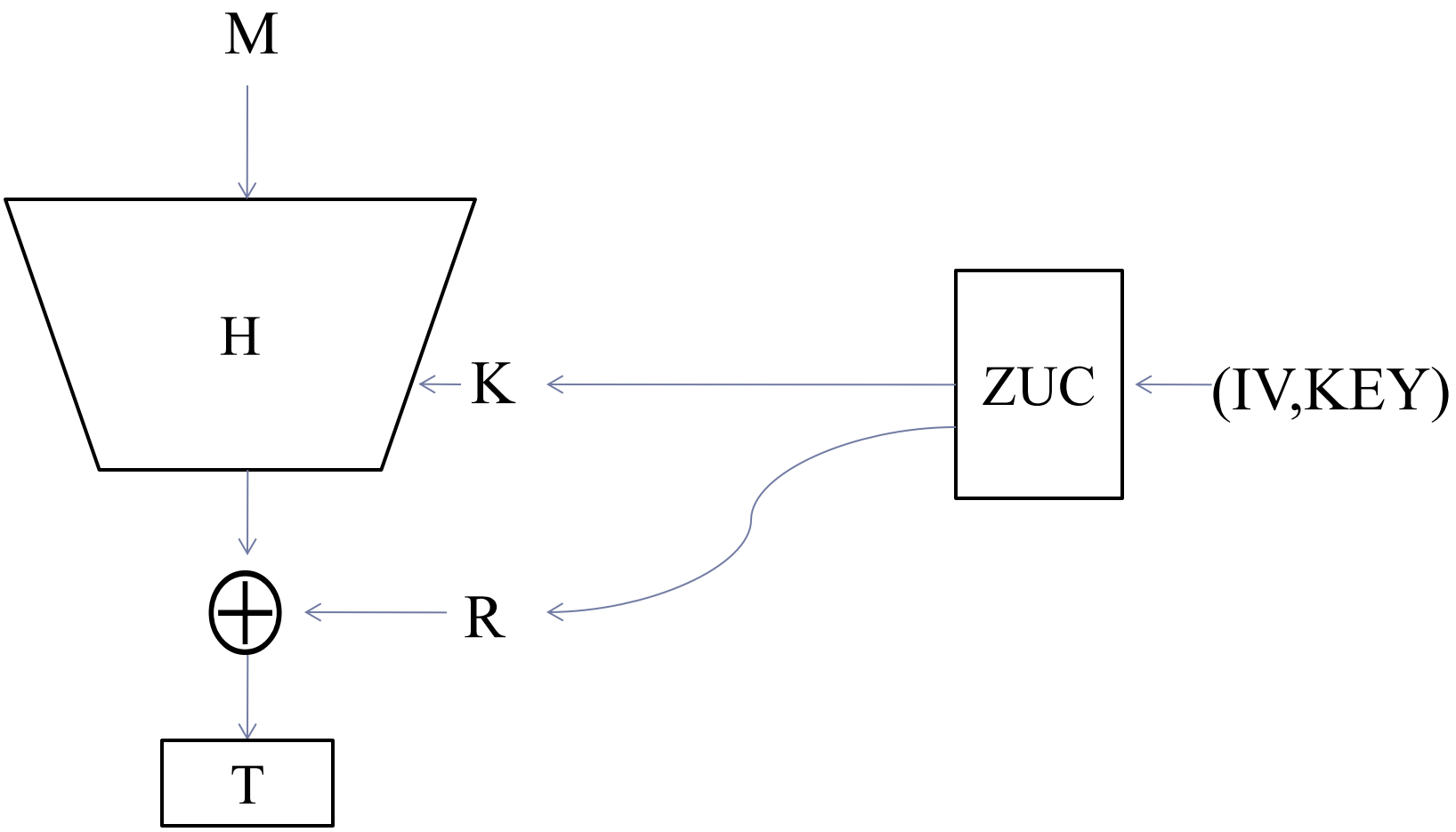


Comparison

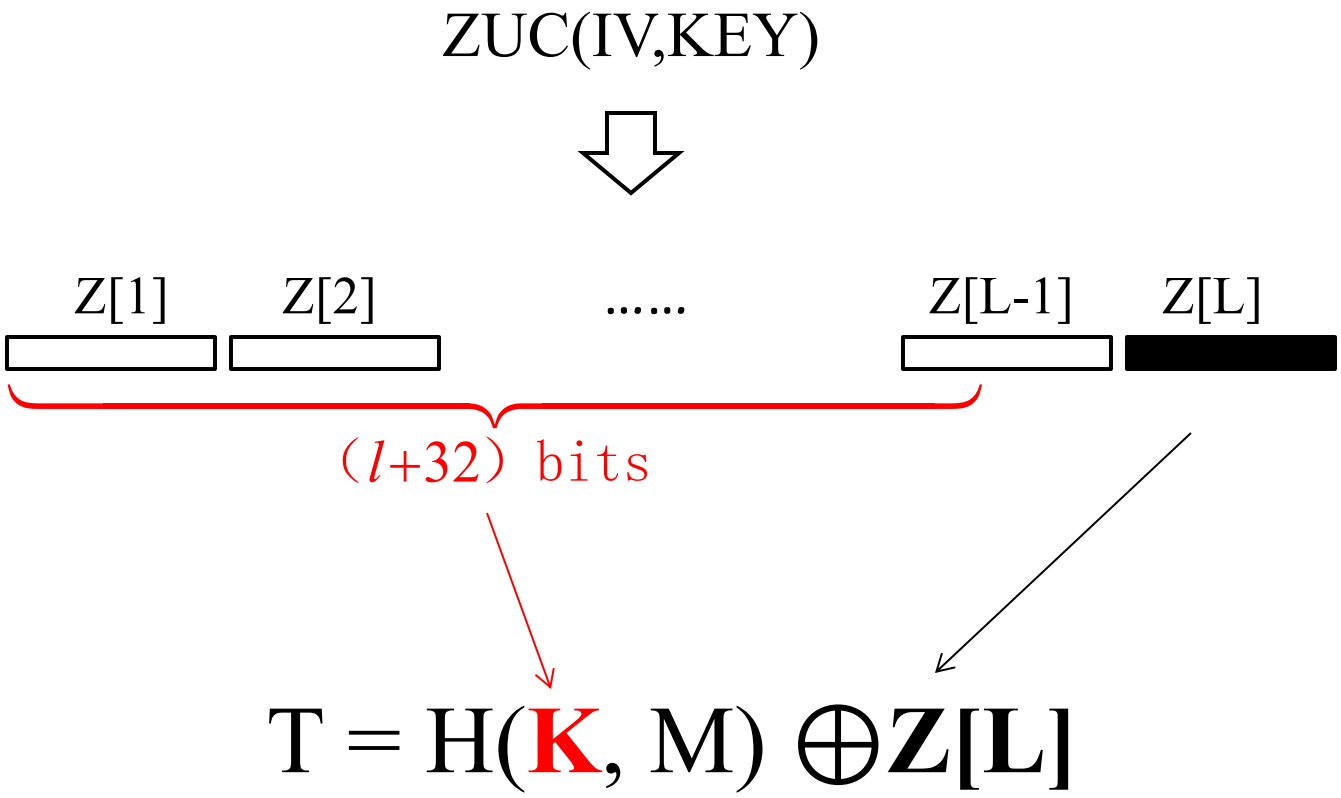
- Tweak 1: Bigger change to the previous scheme, but no change to the proof.
- Tweak 2: Smaller change to the previous scheme, but more complicated proof.

5) Security of 128-EIA3

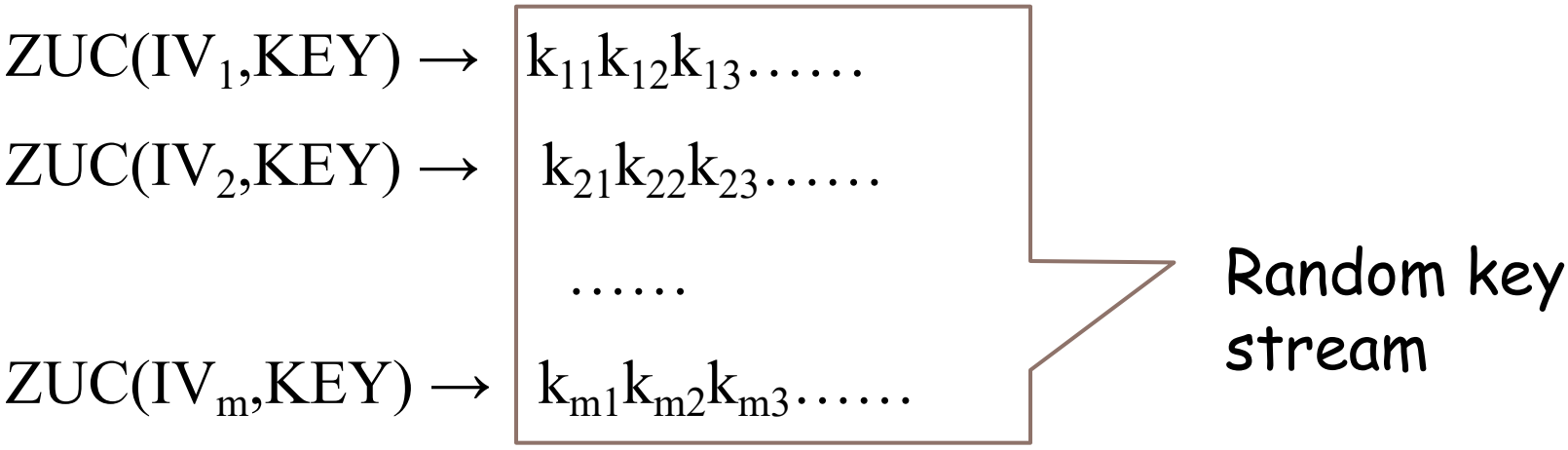
128-EIA3



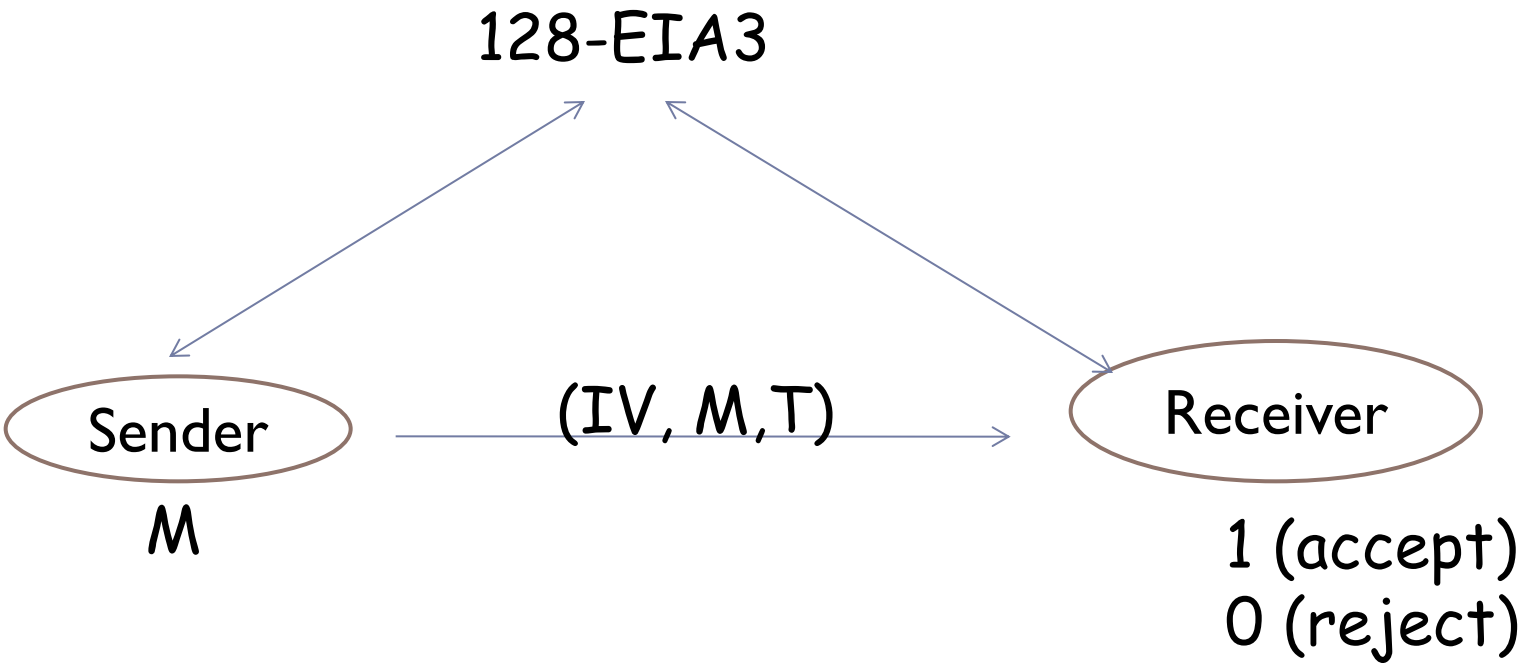
T= H(K,M) ⊕ Z[L]



Assumption: random key stream generated by ZUC



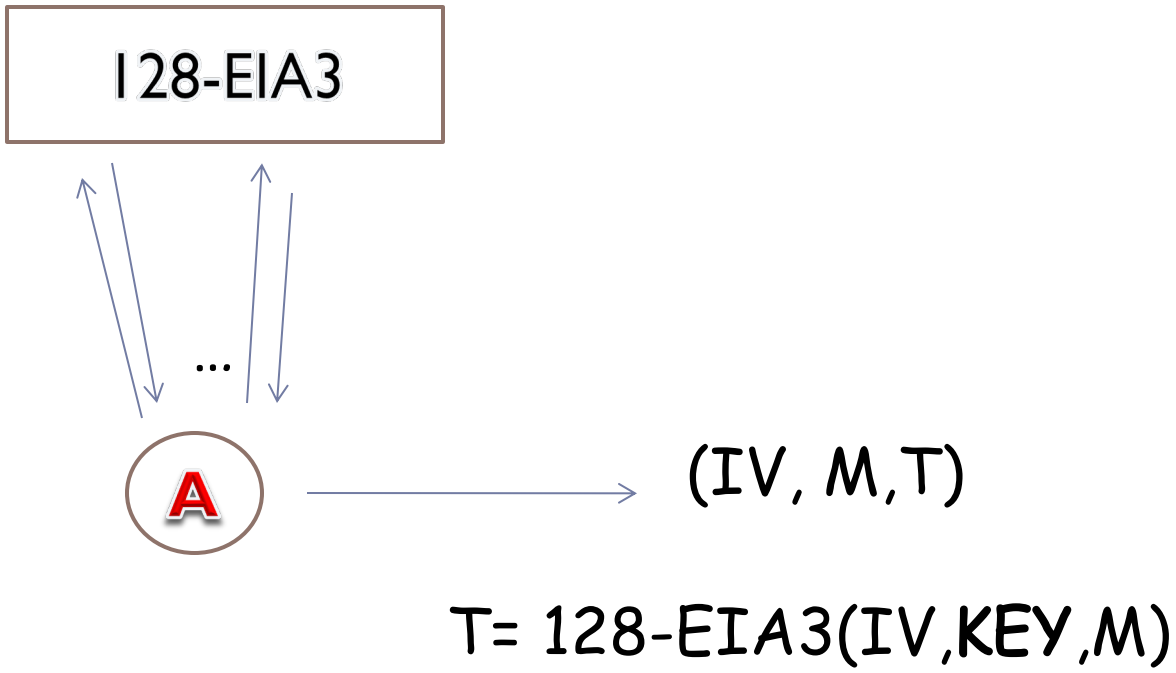
- IVs are not repeating



T= 128-EIA3(IV,KEY,M)

Security model

Unforgeability



Properties of the function H

- **1) H(K, M) is 1/2^32 AXU**
  - For x, x‘∈D, x≠x’ and y∈R, Pr[**H(k,x)⊕H(k,x')=y**]≤ 1/2^32
- **2) H(K, M) is uniform**
  - For any x∈D and y∈R, Pr[**H(k,x) =y**]=1/2^32

Security proof of 128-EIA3 v1.5

(IV_1, M_1, T_1)

(IV_2, M_2, T_2)

……

IVs are different

Adversary

(IV_s, M_s, T_s)

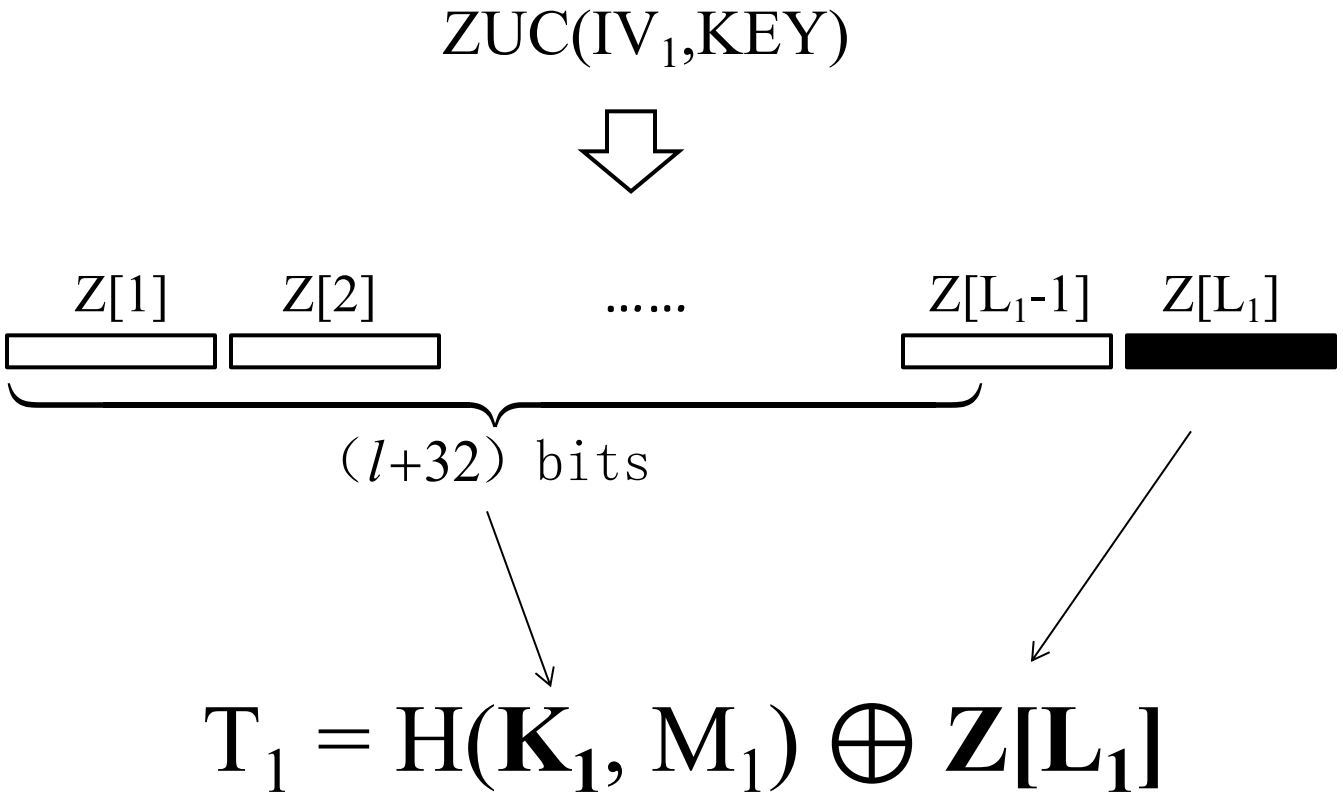
Output: (IV, M, T)

If IV is new,
then H(K,M) $\oplus$ Z[L] is random to the adversary

$p=2^{-32}$

Suppose: $IV = IV_1$

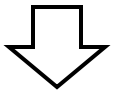
$IV=IV_1$



The success probability is:

Under the condition of known (IV_1,M_1,T_1), the probability of the valid (IV, M, T):

ZUC(IV,KEY)

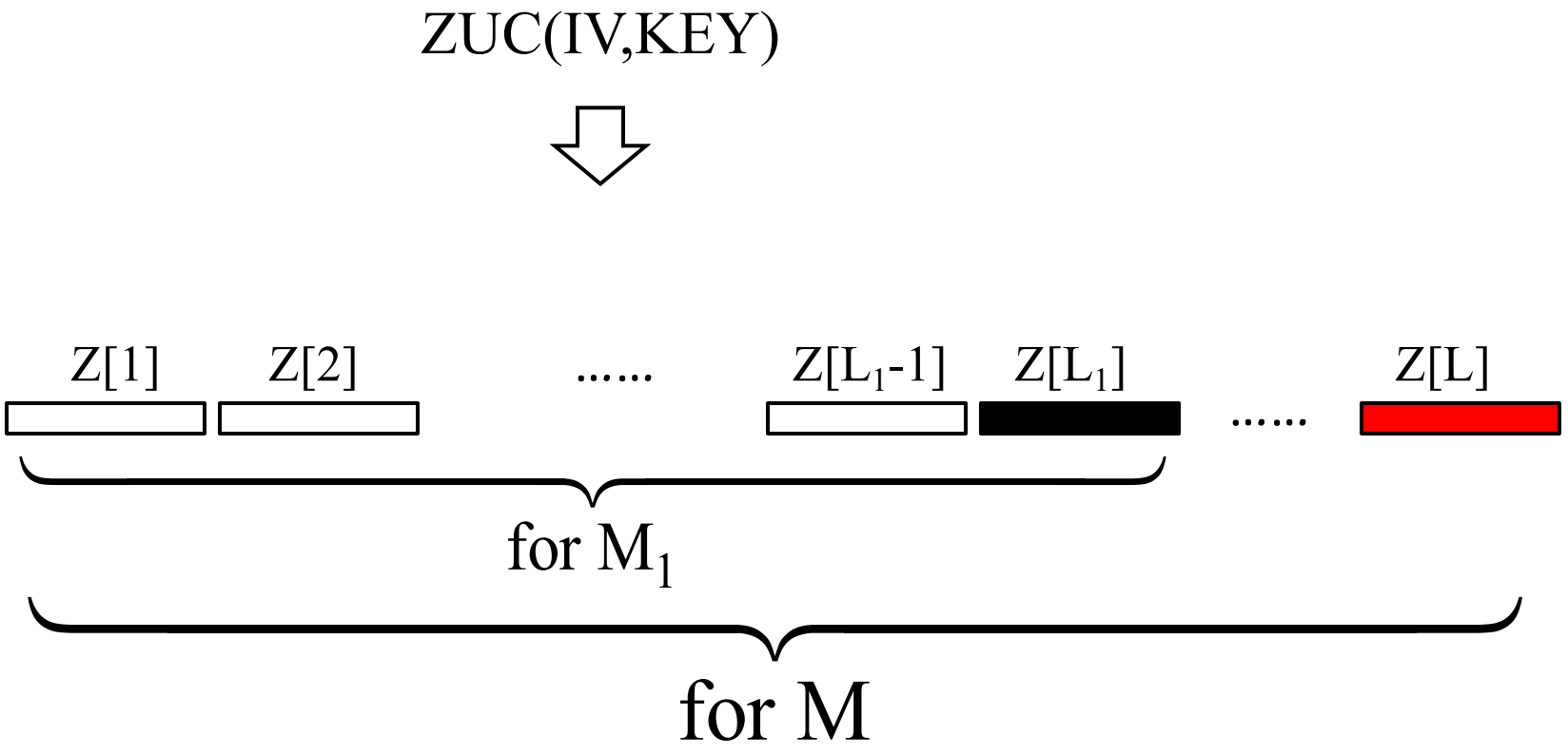


$$\mathbf{p}=Pr[T = H(\mathbf{K}, M) \oplus \mathbf{Z[L]} | T_1 = H(\mathbf{K_1}, M_1) \oplus \mathbf{Z[L_1]}]$$

Try to forge

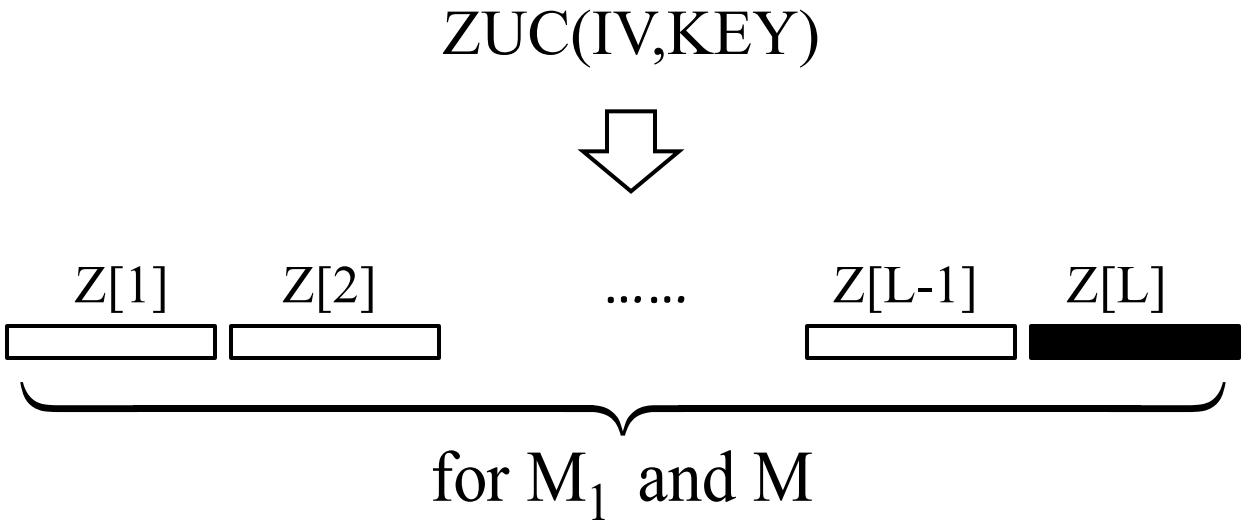
Known

1） $L>L_1$



$p=2^{-32}$

2） $L=L_1$



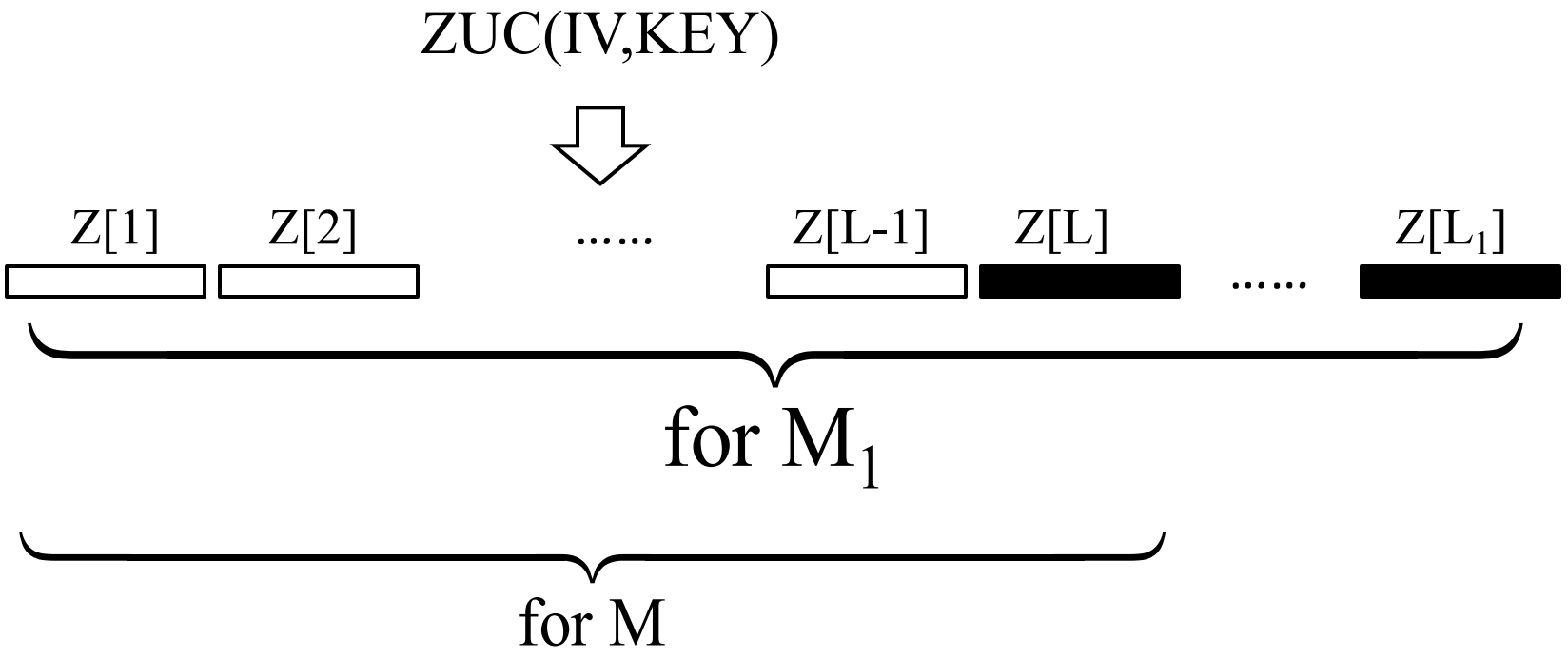
$$p=Pr[T = H(\mathbf{K}, M) \oplus \mathbf{Z[L]} | T_1 = H(\mathbf{K_1}, M_1) \oplus \mathbf{Z[L]}]$$

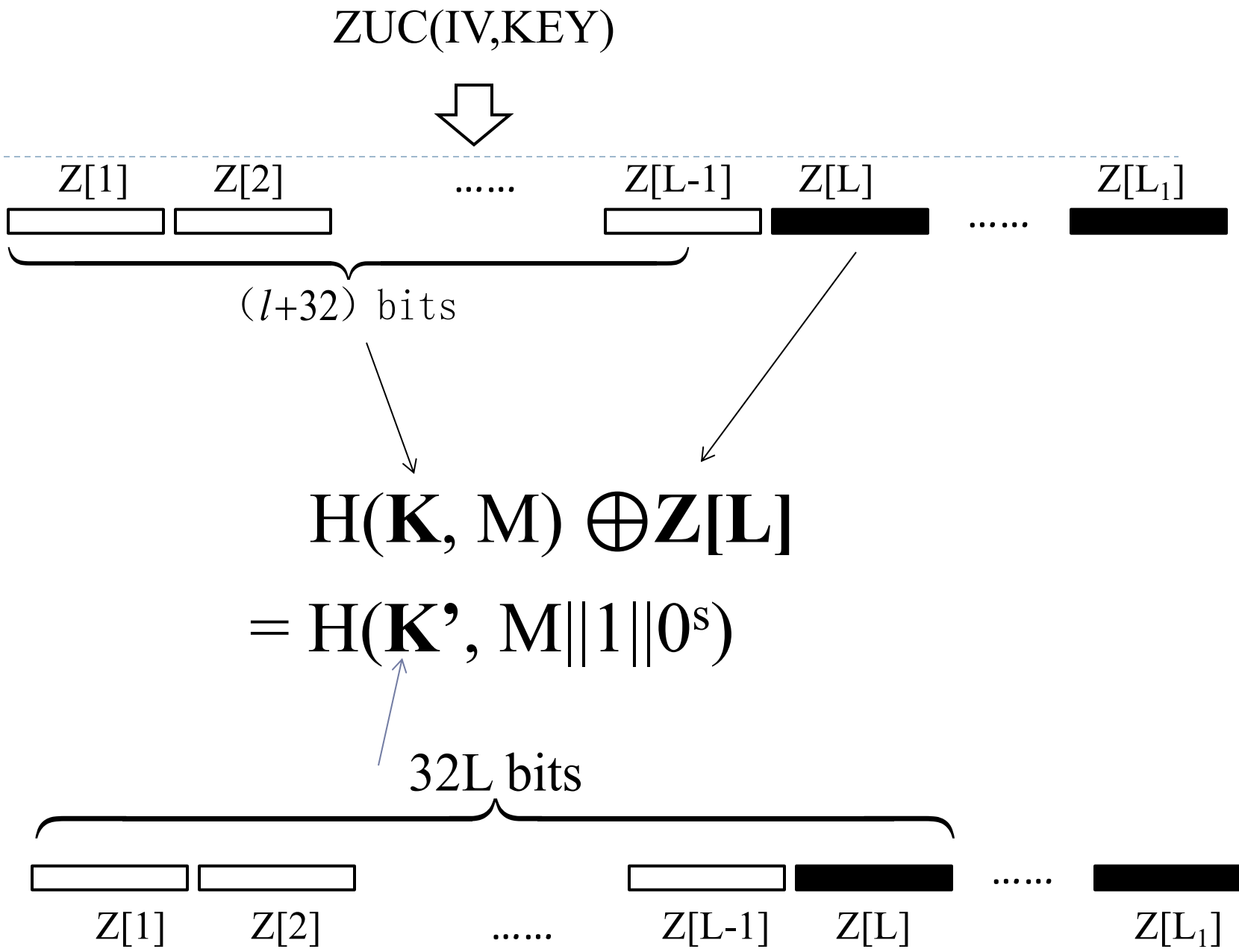
$$=Pr[H(\mathbf{K}, M) \oplus H(\mathbf{K_1}, M_1) = T \oplus T_1 | T_1 = H(\mathbf{K_1}, M_1) \oplus \mathbf{Z[L]}]$$

$$=Pr[H(\mathbf{K}, M) \oplus H(\mathbf{K_1}, M_1) = T \oplus T_1]=2^{-32}$$

*

3） $L<L_1$




ZUC(IV,KEY)
Z[1]
Z[2]
.....
Z[L-1]
Z[L]
.....
Z[L1]
(l+32) bits
H(K, M) ⊕Z[L]
= H(K', M||1||0s)
32L bits
Z[1]
Z[2]
.....
Z[L-1]
Z[L]
.....
Z[L1]

*

$$p=\Pr[T = H(\mathbf{K}, M) \oplus \mathbf{Z[L]} \mid T_1 = H(\mathbf{K_1}, M_1) \oplus \mathbf{Z[L_1]}]$$

$$=\Pr[T=H(\mathbf{K'}, M||1||0^s) \mid T_1 = H(\mathbf{K_1}, M_1) \oplus \mathbf{Z[L_1]}]$$

$$=\Pr[T=H(\mathbf{K'}, M||1||0^s] = 2^{-32}$$

Comments on 128-IEA3 V1.5

- 128-IEA3 v1.5 is still not a generic Wegman-Carter Scheme.
- Security of 128-EIA3 v1.5 is based on AXU and uniformity of the underlying universal hash function,
- or uniformity solely, because uniformity implies AXU in 128-EIA3 v1.5 .

Question at ZUC forum. http://zucalg.forumotion.net/

- Why not AES?
- Why not eStream?
- “Chinese algorithm” means China can break it?
- Is there something wrong with the other LTE algorithms?
- What happens now to the other LTE algorithms?
- Why does China get this special privilege?
- If every other country insists on a home-grown algorithm, will every LTE phone have to support 200 algorithms?
- Authenticated encryption?

References

- [WC81] Wegman and Carter, New hash functions and their use in authentication and set equality. 1981.
- [K94] Krawczyk. LFSR-based hashing and authentication. Crypto'94. Springer-Verlag, 1994, LNCS 839, 313-328.
- [K95] Krawczyk. New hash functions for message authentication. Crypto'95. Springer-Verlag, 1995, LNCS, 129-139.
- [S96] Shoup. On Fast and Provably Secure Message Authentication Based on Universal Hashing *Advances in Cryptology -- CRYPTO 1996, Springer-Verlag,* 1996*, LNCS 1109*, 313-328.
- [FGRV10] T. Fuhr, H. Gilbert, J. Reinhard, and M. Videau. A Forgery Attack on the Candidate LTE Integrity Algorithm 128-EIA3
- [FGRV11] T. Fuhr, H. Gilbert, J. Reinhard, and M. Videau. Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3

*

Thanks

Questions?

wpeng@iie.ac.cn