Birthday Forgery Attack on 128-EIA3$_{(Version 1.5)}$

Raja Zeshan Haider
National University of Science and Technology,
Pakistan
zeshanjalip@hotmail.com

Abstract. 128-EIA3 is an integrity algorithm considered for adoption as a third integrity algorithm by European Telecommunication Standard Institute (ETSI) for 4th generation of GSM networks.128-EIA3 is vulnerable to birthday forgery attack. Birthday forgery attack requires minimum 2^{16} known message-MAC pairs for finding collision in 128-EIA3. 128-EIA3 is susceptible to internal collision of its universal hash function and external collision of its Xoring transformation. Birthday forgery attack on 128-EIA3 allows message forgery with success probability greater than $1/2^{32}$.

Keywords: Collision, Message Authentication Code (MAC), Message Forgery

1 Introduction

The evolution of third generation UMTS (Universal Mobile Telecommunication System) comprising of new radio access system named LTE (Long Term Evolution) and a new core network named SAE (System Architecture Evolution) introduced two standardized algorithms, namely 128-EEA3,Encryption algorithm and 128-EIA3,Integrity algorithm. This resulting algorithm set is based on a core stream cipher algorithm named ZUC, after Zu Chongzhi, the famous Chinese scientist. The algorithms were designed at the Data Assurance and Communication Security Research Center (DACAS) of the Chinese Academy of Sciences. Preliminary drafts of their specifications [1, 2] are currently open for public evaluation, after their preliminary evaluation by ETSI (European Telecommunication Standard Institute) task force and two funded teams of academic experts mandated by ETSI. After its adoption by 3GPP (3rd Generation Partnership Project), 128-EIA3 will represent the third LTE integrity algorithm.

The integrity algorithm 128-EIA3 is a universal hash function which is based on the Carter-Wegman family of universal hash functions [3].128-EIA3 is bit different to Carter-Wegman family of universal hash functions in terms of generation of it's masking value.In Carter-Wegman family of universal hash functions, masking value is generated independent of message whereas in 128-EIA3,it is dependent on the length of the message and it is generated from undelrying stream cipher ZUC. 128-EIA3 computes a 32-bit MAC of a given input message of length between 1 and 20000 bits using an integrity key(IK) and initialization vector (IV) of 128 bit each.

In this paper we show that 128-EIA3 is vulnerable to birthday forgery attack. The attack is based on the well known problem of birthday paradox and it requires minimum 2^{16} known message-MAC pairs for finding collision in 128-EIA3.Birthday forgery attack aims to find internal and external collision in 128-EIA3 for distinct messages of same length.

Outline of paper. In Section 2 short description of 128-EIA3 Integrity algorithm is provided.In section 3 birthday forgery attack on 128-EIA3 is described alongwith results and findings.In section 4 a variant of 128-EIA3 is suggested to thwart the birthday forgery attack.

2 Description of 128-EIA3 Algorithm

128-EIA3 is a universal a hash function which makes black box use of ZUC. 128-EIA3 takes input 128-bit key named integrity key IK and 128-bit initialization vector IV. IV is calculated from a set of parameters i.e.32-bit counter, 5-bit bearer identity, 1-bit direction which determines the direction of transmission; 0 for uplink and 1 for downlink.Counter variable of IV is incremented for each invocation of 128-EIA3 MAC generation oracle.IK and IV are input to the ZUC for generating key stream of length 64-bit more than the length of the message.128-EIA3 processes messages of length between 1 and 20000 bits and produces a 32-bit MAC value. Message is padded with a bit 1 before MAC calculation.Structure of 128-EIA3 is mentioned in following figure.

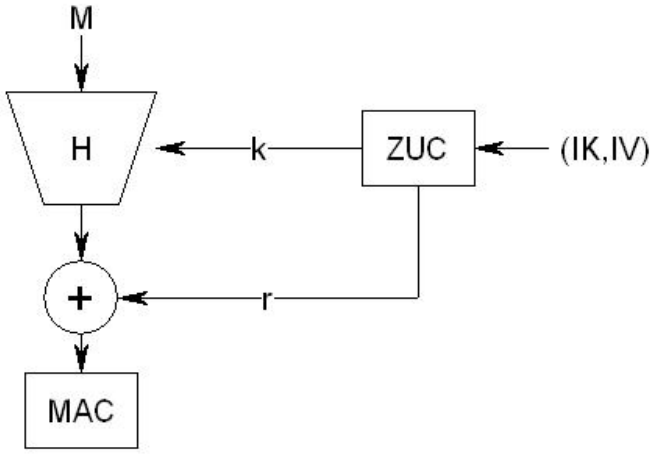

Fig. 1. Structure of 128-EIA3

128-EIA3 is based on universal hash function H and random stream generator ZUC ,IK and IV are input to the ZUC for random stream generation.128-EIA3

makes use of the following universal hash function $H{:}K\times\{0,1\}^*\rightarrow\ \{0,1\}^{32}$ as the message authentication code function.

$$H(k,x) = \begin{pmatrix} k_1 & k_2 & \cdots & k_{m+1} \\ k_2 & k_3 & \cdots & k_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ k_{32} & k_{33} & \cdots & k_{m+32} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \\ 1 \end{pmatrix}$$

The universal hash function above for 128-EIA3 is similar to the one based on Toeplitz matrix, with the exception that this universal hash function can handle variable-input-length messages.The output of universal hash function H is Xored with masking value derived from the ZUC generated keystream.Procedure for MAC calculation in 128-EIA3 algorithm is as follows.

Algorithm of 128-EIA3

Input: $IK \in \{0,1\}^{128}$, $IV \in \{0,1\}^{128}$ Where IV=IV(Count,Bearer,Direction)
Input: $M{=}(m_0,\ldots,m_{l-1}) \in\ \{0,1\}^l$

keystream:$(\mathrm{ks}_0,\ldots,\mathrm{ks}_{\mathrm{l}+63}) \leftarrow \mathrm{ZUC}(\mathrm{IK},\mathrm{IV})$
$T = 0$
for i=0 to *l-1* do
$\mathrm{W}_i \leftarrow (\mathrm{ks}_i,\ldots,\mathrm{ks}_{\mathrm{i}+31})$
if $\mathrm{m}_i = 1$ *then*
T$\leftarrow T\oplus \mathrm{W}_i$
end if
end for
$W_l \leftarrow (\mathrm{ks}_l,\ldots,\mathrm{ks}_{\mathrm{l}+31})$
$T \leftarrow T\oplus \mathrm{W}_l$
$W_{mask} \leftarrow (\mathrm{ks}_{l+32},\ldots,\mathrm{ks}_{\mathrm{l}+63})$
MAC=T $\oplus$ W_{mask}
Output:MAC

---

3 Birthday Forgery Attack on 128-EIA3 Algorithm

Birthday forgery attack is based on birthday paradox which pertains to the probability that in a set of randomly chosen people some pair of them will have the same birthday. In a group of at least 23 randomly chosen people, there is more than 50 % probability that some pair of them will both have been born on the same day and it reaches 100% when the number of people approaches 366.Birthday forgery attack is applicable to 128-EIA3 like other construction of MAC algorithms as mentioned in [4].

Considering 128-EIA3 it can be divided into two components ,one is universal hash function H whose universality is based on the length of the message and hamming weight of the message and other is Xoring of the hash result with the masking value.Consider the message pair $(x, x')$where x,x' are distinct messages of same length, with $h(x) = g(H_t)$ and $h(x') = g(H_t')$,where $h(x)$ relates to 128-EIA3 integrity algorithm,H_t is the hash result of universal hash function H and g is the output transformation that is the Xoring of the hash result with the masking value. Collision $h(x) = h(x')$ can be of two reasons ,if $H_t = H_t'$ it is said to be internal collision ,if $H_t \neq H_t'$ but $g(H_t) = g(H_t')$ it is said to be external collision.128-EIA3 is prone to both internal and external collision.Internal collision in context of 128-EIA3 refers as the collision found in universal hash function H whereas external collision refers as collision due to Xoring transformation of masking value with the hash result of the universal hash function H.

3.1 Internal Collision on 128-EIA3

128-EIA3 is susceptible to internal collision of its universal hash function H for distinct messages of same length under the same IK and IV.Internal collision of universal hash function H leads to external collision of 128-EIA3 under the same IK and IV.Internal collision on 128-EIA3 requires minimum 2^{16} known message-MAC pairs and one chosen message to launch a verifiable message forgery under the same IK and IV with success probability of 1.

As in case of internal collision of message pair (x, x'),128-EIA3 will generate the same MAC for $h(x\|y) = h(x'||y)$ for any single block y under the same IK and IV.The probability for finding internal collision in 128-EIA3 increases by increasing queries to MAC generation oracle.Although internal collision on 128-EIA3 under the same IK and IV is a trivial case but it exibits implications of reusage or repetition of IV under the same key.Occurrence of collided pairs in 128-EIA3 due to internal collision of universal hash function H under the same IK and IV for different known message-MAC pairs are as follows.

Sr.No	No of Known message-MAC Pairs	No of Collided Pairs Found
1	2^{16}	1
2	2^{18}	7
3	2^{20}	136
4	2^{22}	2010

Table 1: Internal Collision Statistics.

3.2 External Collision on 128-EIA3

Xoring of one-time masking value with output of universal hash function H results in external collision of 128-EIA3.128-EIA3 is susceptible to external collision of distinct messages of same length under different IK and IV.Following cases are considered for finding external collision in 128-EIA3.

– IK is fixed and COUNTER variable of IV is incremented for each invocation of 128-EIA3 MAC generation oracle.
– IK is randomly generated and COUNTER variable of IV is incremented for each invocation of 128-EIA3 MAC generation oracle.

Above mentioned cases require minimum 2^{16} known message-MAC pairs for finding external collision in 128-EIA3. Probability for finding external collision in 128-EIA3 increases by increasing queries to 128-EIA3 MAC generation oracle.Occurrence of collided pairs in 128-EIA3 due to external collision of Xoring tranformation under different IK and IV for different known message-MAC pairs are as follows.

Sr.No	No of Known message-MAC Pairs	No of Collided Pairs Found
1	2^{16}	1
2	2^{18}	8
3	2^{20}	140
4	2^{22}	2081

Table 2: External Collision Statistics.

The success probability of an opponent who wants to obtain a correct MAC value is equal to $max(2^{-ik}, 2^{-m})$, where ik is the key length of IK in bits and m is the length of the MAC result in bits.In case of 128-EIA3 success probability of an opponent to obtain a correct MAC is greater than 2^{-32} as collision is inevitable in 128-EIA3.A malicious attacker while observing communication in a GSM network and having access to MAC verification oracle can easily forge a message with success probability greater than $1/2^{32}$.This situation can be catastrophic when a centralized GSM authentication centre is autheticating subscribers and other elements of GSM network.The Design and Evaluation Report [5] erroneously invokes the security proofs of 128-EIA3 that no forgery of a new message can succeed with probability greater than $1/2^{32}$.

4 Variant of 128-EIA3

We have considered a slightly modified variant of 128-EIA3 algorithm to thwart the birthday forgery attack, that is quite similar to 128-EIA3 and requires the same number of key stream bits except that it makes the effective length of MAC to 64-bit.A 32-bit variable sequence number(*Seq-No*) intialized with 1 is introduced ,each invocation of 128-EIA3 MAC generation oracle requires unique *Seq-No*.Variable *Seq-No* is encrypted with first word of the ZUC generated keystream and then concatenated with the calculated MAC.If COUNTER variable of IV is being incremented for each invocation of 128-EIA3 MAC generation oracle,it will be more better option to use it instead of variable *Seq-No*.

Variant Algorithm of 128-EIA3

Input: $IK \in \{0,1\}^{128}$, $IV \in \{0,1\}^{128}$ Where IV=IV(Count,Bearer,Direction)
Input: $M = (m_0, \ldots, m_{l-1}) \in \{0,1\}^l$

keystream:$(\mathrm{ks}_0, \ldots, \mathrm{ks}_{l+63}) \leftarrow \mathrm{ZUC}(\mathrm{IK}, \mathrm{IV})$
$T = 0$
$Seq - No = 1$
for i=0 to *l-1* do
$\mathrm{W}_i \leftarrow (\mathrm{ks}_i, \ldots, \mathrm{ks}_{i+31})$
if $\mathrm{m}_i = 1$ *then*
T$\leftarrow T \oplus \mathrm{W}_i$
end if
end for
$W_l \leftarrow (\mathrm{ks}_l, \ldots, \mathrm{ks}_{l+31})$
$T \leftarrow T \oplus \mathrm{W}_l$
$W_{mask} \leftarrow (\mathrm{ks}_{l+32}, \ldots, \mathrm{ks}_{l+63})$
MAC=T $\oplus$ W_{mask}
MAC=MAC$\|ENC_ZUC(Seq - No)$
Output : MAC

Variant of 128-EIA3 is capable to thwart the birthday forgery attack but it requires in-depth analysis not only in terms of its cryptographic strength but also in context of its implementation perspective in GSM network,in realm of Long Term Evolution (LTE) security.

5 Conclusion and Direction for Future Work

128-EIA3 is not a ϵ-Almost Xor Universal hash function as it is susceptible to birthday forgery attack.Both internal collisions and external collisions are found in 128-EIA3.128-EIA3 if implemented in existing structure will have devastating effect on the integrity mechanisms of GSM as it has to be implemented in Subscriber Identity Module (SIM) cards and in GSM network authentication centres.Applicability of key/keystream recovery attacks based on collision should be considered for 128-EIA3.

References

[1] ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification. Version 1.5, 4th January 2011. http://www.gsmworld.com/documents/EEA3_EIA3_specification_v1_5.pdf.

[2] ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3. Document 2: ZUC Specification. Version 1.5, 4th January 2011. http://www.gsmworld.com/documents/EEA33ZUC1_5.pdf.

[3] J.L. Carter, M.N. Wegman, Universal classes of hash functions, Journal of Computer and System Sciences, Vol. 18, 1979, pp. 143154.

[4] B. Preneel, P.C. van Oorschot, "MDx-MAC and building fast MACs from hash functions," , Proc. Crypto'95, LNCS 963,Springer-Verlag, 1995, pp. 1-14.

[5] ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3. Document 4: Design and Evaluation Report. Version 1.3, 18th January 2011. http://www.gsmworld.com/documents/EEA3_EIA3_Design_Evaluation _v1_3.pdf.