Near Birthday Attack on «8 bits» AEAD Mode

Liliya R. Ahmetzyanova,
Grigory A. Karpunin,
Grigory K. Sedov

CryptoPro LLC

CTCrypt 2018
Suzdal, Russia, May 28–30, 2018

AEAD mode standardization in Russia

Now there is no AEAD mode standard in Russia.

Development of AEAD mode specification (for standardization in Russia) has been planned for 2018 in TC 26 (Technical committee for standardization "Cryptography and security mechanisms") in the "Cryptographic protocols and additional mechanisms" working group (chairs: S.V. Smyshlyaev, V.A. Shishkin).

According to the decision of the XX meeting of TC 26, the series of seminars was started on the base of the Lomonosov Moscow State University scientific seminar "Mathematical methods of cryptanalysis" led by E.K. Alekseev, A.A. Chilikov, S.V. Smyshlyaev, O.A. Logachev

Two modes were heavily discussed as the main candidates for standardization: the MGM mode (see IETF draft-smyshlyaev-mgm) and the «8 bits» mode.

AEAD mode standardization in Russia

Now there is no AEAD mode standard in Russia.

Development of AEAD mode specification (for standardization in Russia) has been planned for 2018 in TC 26 (Technical committee for standardization "Cryptography and security mechanisms") in the "Cryptographic protocols and additional mechanisms" working group (chairs: S.V. Smyshlyaev, V.A. Shishkin).

According to the decision of the XX meeting of TC 26, the series of seminars was started on the base of the Lomonosov Moscow State University scientific seminar "Mathematical methods of cryptanalysis" led by E.K. Alekseev, A.A. Chilikov, S.V. Smyshlyaev, O.A. Logachev

Two modes were heavily discussed as the main candidates for standardization: the MGM mode (see IETF draft-smyshlyaev-mgm) and the «8 bits» mode.

AEAD mode standardization in Russia

Now there is no AEAD mode standard in Russia.

Development of AEAD mode specification (for standardization in Russia) has been planned for 2018 in TC 26 (Technical committee for standardization "Cryptography and security mechanisms") in the "Cryptographic protocols and additional mechanisms" working group (chairs: S.V. Smyshlyaev, V.A. Shishkin).

According to the decision of the XX meeting of TC 26, the series of seminars was started on the base of the Lomonosov Moscow State University scientific seminar "Mathematical methods of cryptanalysis" led by E.K. Alekseev, A.A. Chilikov, S.V. Smyshlyaev, O.A. Logachev

Two modes were heavily discussed as the main candidates for standardization: the MGM mode (see IETF draft-smyshlyaev-mgm) and the «8 bits» mode.

AEAD mode standardization in Russia

Now there is no AEAD mode standard in Russia.

Development of AEAD mode specification (for standardization in Russia) has been planned for 2018 in TC 26 (Technical committee for standardization "Cryptography and security mechanisms") in the "Cryptographic protocols and additional mechanisms" working group (chairs: S.V. Smyshlyaev, V.A. Shishkin).

According to the decision of the XX meeting of TC 26, the series of seminars was started on the base of the Lomonosov Moscow State University scientific seminar "Mathematical methods of cryptanalysis" led by E.K. Alekseev, A.A. Chilikov, S.V. Smyshlyaev, O.A. Logachev

Two modes were heavily discussed as the main candidates for standardization: the MGM mode (see IETF draft-smyshlyaev-mgm) and the «8 bits» mode.

AEAD mode standardization in Russia

29.01.2018, the seminar “Mathematical methods of cryptanalysis” at the Lomonosov Moscow State University, V.I. Nozdrunov gave a talk “On standardization perspectives of AEAD cipher mode in Russia”.

In this talk V.I. Nozdrunov presented two proposals for Russian AEAD cipher mode: the MGM mode and the “8 bits” mode.

At the present moment this talk is the only public source of information on the «8 bits» mode.

CryptoPro actively participates in the work of TC 26 and, in particular, in the process of standardizing the Russian AEAD mode. As part of this process, we studied the cryptographic properties of the «8 bits» mode. The results of our research we present at the conference CTCrypt 2018.

AEAD mode standardization in Russia

29.01.2018, the seminar “Mathematical methods of cryptanalysis” at the Lomonosov Moscow State University, V.I. Nozdrunov gave a talk “On standardization perspectives of AEAD cipher mode in Russia”.

In this talk V.I. Nozdrunov presented two proposals for Russian AEAD cipher mode: the MGM mode and the “8 bits” mode.

At the present moment this talk is the only public source of information on the «8 bits» mode.

CryptoPro actively participates in the work of TC 26 and, in particular, in the process of standardizing the Russian AEAD mode. As part of this process, we studied the cryptographic properties of the «8 bits» mode. The results of our research we present at the conference CTCrypt 2018.

AEAD mode standardization in Russia

29.01.2018, the seminar “Mathematical methods of cryptanalysis” at the Lomonosov Moscow State University, V.I. Nozdrunov gave a talk “On standardization perspectives of AEAD cipher mode in Russia”.

In this talk V.I. Nozdrunov presented two proposals for Russian AEAD cipher mode: the MGM mode and the “8 bits” mode.

At the present moment this talk is the only public source of information on the «8 bits» mode.

CryptoPro actively participates in the work of TC 26 and, in particular, in the process of standardizing the Russian AEAD mode. As part of this process, we studied the cryptographic properties of the «8 bits» mode. The results of our research we present at the conference CTCrypt 2018.

«8 bits» AEAD mode at a glance

«8 bits» is a modification of the AEAD mode CCM. The purpose of the modification is to eliminate the known efficiency shortcomings of the CCM mode.

«8 bits» is based on the two standardized cipher modes described in GOST R 34.13-2015:

- the CTR mode — to provide confidentiality;
- the OMAC1 mode — to provide authenticity.

«8 bits» uses the block cipher Kuznyechik as a base block cipher for the CTR and OMAC1 modes.
Kuznyechik has the key length $k = 256$ and the block length $n = 128$.

«8 bits» security estimations: confidentiality

In the talk V.I. Nozdrunov presented two theorems which give security estimations of the «8 bits» AEAD mode:

Theorem («8 bits» conf.) [Nosdrunov's talk, 2018]

Let $E\colon \mathsf{Key} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $CTR[E]$ be a CTR mode based on E. Then for all t, q_e and $\mu_e = \min(q_E n, n2^n)$ the following inequality holds

$$\mathrm{Adv}^{ind\text{-}cpa}_{CTR[E]}(\cdot, t, q_e, \mu_e) \leq 2\mathrm{Adv}^{prp}_{E}(t, q_E) + q_E^2 2^{-n}.$$

Informally

Let the cipher E (Kuznyechik) be secure in the PRP model. Then any adversary $\mathcal{A}$, making queries of total length $q_E \ll 2^{n/2}$ blocks, can not break the «8bits» mode without MAC tag in the IND-CPA model.

«8 bits» security estimations: confidentiality

In the talk V.I. Nozdrunov presented two theorems which give security estimations of the «8 bits» AEAD mode:

Theorem («8 bits» conf.) [Nosdrunov's talk, 2018]

Let $E\colon \mathsf{Key} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $CTR[E]$ be a CTR mode based on E. Then for all t, q_e and $\mu_e = \min(q_E n, n2^n)$ the following inequality holds

$$\mathrm{Adv}^{ind\text{-}cpa}_{CTR[E]}(\cdot, t, q_e, \mu_e) \leq 2\mathrm{Adv}^{prp}_{E}(t, q_E) + q_E^2 2^{-n}.$$

Informally

Let the cipher E (Kuznyechik) be secure in the PRP model. Then any adversary $\mathcal{A}$, making queries of total length $q_E \ll 2^{n/2}$ blocks, can not break the «8bits» mode without MAC tag in the IND-CPA model.

«8 bits» security estimations: authenticity

Theorem («8 bits» auth.) [Nosdrunov's talk, 2018]

Let $E\colon \mathsf{Key} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $OMAC1[E]$ be the OMAC1 mode based on E. Let $m \leq 2^n/4$. Then the following inequality holds

$$\mathrm{Adv}^{suf\text{-}cma}_{OMAC1[E]}(\cdot, q_u, q_v, nm) \leq \frac{(5m^2+1)(q_u+q_v)^2+1}{2^n} + \mathrm{Adv}^{prp}_{E}(t', q'),$$

where $t' = t + O(m(q_u+q_v))$ and $q' = m(q_u+q_v)+1$.

Informally

Let the cipher E (Kuznyechik) be secure in the PRP model. Then any adversary $\mathcal{A}$, making queries of total maximum length $m(q_u+q_v) \ll 2^{n/2}$ in blocks, can not break the «8 bits» mode without ciphertext in the SUF-CMA model.

«8 bits» security estimations: authenticity

Theorem («8 bits» auth.) [Nosdrunov's talk, 2018]

Let $E\colon \mathsf{Key} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $OMAC1[E]$ be the OMAC1 mode based on E. Let $m \leq 2^n/4$. Then the following inequality holds

$$\mathrm{Adv}^{\textit{suf-cma}}_{OMAC1[E]}(\cdot, q_u, q_v, nm) \leq \frac{(5m^2+1)(q_u+q_v)^2+1}{2^n} + \mathrm{Adv}^{prp}_{E}(t', q'),$$

where $t' = t + O(m(q_u+q_v))$ and $q' = m(q_u+q_v)+1$.

Informally

Let the cipher E (Kuznyechik) be secure in the PRP model. Then any adversary $\mathcal{A}$, making queries of total maximum length $m(q_u+q_v) \ll 2^{n/2}$ in blocks, can not break the «8 bits» mode without ciphertext in the SUF-CMA model.

CCM security estimations: confidentiality

For the CCM mode security estimations were obtained by J. Jonsson in 2002.

Theorem (CCM conf.) [J. Jonsson, SAC 2002]

Let $\mathcal{A}$ be an adversary against the confidentiality of CCM. Let q_u be the number of encryption queries and let $Q_1, Q_2, \ldots, Q_{q_u}$ denote the queries. Let q_v be the number of forgery attempts and let $Q_1^*, Q_2^*, \ldots, Q_{q_v}^*$ denote the attempts. Put $l_u = \sum_i l_{Q_i}$ and $l_v = \sum_i l_{Q_i^*}$. Then there is a PRP distinguisher $\mathcal{B}$ such that

$$\mathrm{Adv}^{conf}_{CCM}(\mathcal{A}) \leq \mathrm{Adv}^{prp}_{E}(\mathcal{B}) + l_u^2 \cdot 2^{-n}.$$

The distinguisher $\mathcal{B}$ has an additional running time equal to the time needed to process the queries from $\mathcal{A}$. This includes making l_u oracle queries and xoring $l_u - q_u$ pairs of blocks of size n.

CCM security estimations: authenticity

Theorem (CCM auth.) [J. Jonsson, SAC 2002]

Let $\mathcal{A}$ be an adversary against the authenticity of CCM. Let q_u, q_v, l_u, l_v be as in Theorem (CCM conf.) Then there is a PRP distinguisher $\mathcal{B}$ such that

$$\mathrm{Adv}^{auth}_{CCM}(\mathcal{A}) \leq \mathrm{Adv}^{prp}_{E}(\mathcal{B}) + q_v 2^{-s} + (l_u + l_v)^2 \cdot 2^{-n}.$$

The distinguisher $\mathcal{B}$ has an additional running time equal to the time needed to process the queries from $\mathcal{A}$. This includes making $l_u + l_v$ oracle queries and xoring $l_u - q_u + l_v - q_v$ pairs of blocks of size n.

Problem of improving estimations for CCM

Problem (CCM auth.) [J. Jonsson, SAC 2002]

Let notations be as in previous Theorems with $\mathcal{A}$ being an adversary against the authenticity of CCM, and assume that E is a block cipher. Is there a PRP distinguisher $\mathcal{B}$ with approximately the same running time as $\mathcal{A}$ such that

$$Adv^{auth}_{CCM}(\mathcal{A}) \leq Adv^{prp}_{E}(\mathcal{B}) + q_v^{1+o(1)} \cdot 2^{-s} + (l_u + l_v)^{1+o(1)} \cdot 2^{-n}?$$

Problem of improving estimations for CCM

Let the cipher E be secure in the PRP model. Then we can transform the above question to the following one

Problem (CCM auth.)

Is there an adversary $\mathcal{A}$, making queries of total length $2^{n/2} \lesssim l_u + l_v \ll 2^n$ in blocks, that can break the authenticity of CCM?

Until now, as far as we know, this question is open.

Problem of improving estimations for «8 bits»

The similar question can be formulated for «8 bits» mode.

Let the cipher E (Kuznyechik) be secure in the PRP model.

Problem («8 bits» auth.)

Is there an adversary $\mathcal{A}$, making queries of total length $2^{n/2} \lesssim l_u + l_v \ll 2^n$ in blocks, that can break the authenticity of «8 bits»?

In the paper we show that the answer for this question for «8 bits» is YES.

We construct an attack to break the «8 bits» authenticity with near birthday bound complexity.

Notations

- E — Kuznyechik, $n = 128$, $k = 256$ (GOST R 34.12-2015)
- $|x|$ — the length of x in bits
- $\mathrm{str}_q(i)$ — representation of the number i as an q-bits string from $\{0,1\}^q$ (the most significant bit — the first)

GOST R 34.13-2015. CTR mode

«8 bits» uses the simple variant of the GOST R 34.13-2015 CTR mode — without truncation:

$\underline{CTR^N(K, M)}$

1: $t = \lceil |M|/n \rceil$
2: $\Gamma = E_K(N) \| E_K(N+1) \| \ldots \| E_K(N+t-1)$
3: $C = M \oplus \Gamma[\text{first } |M| \text{ bits}]$
4: return C

GOST R 34.13-2015. MAC mode

Key derivation procedure:

$R = E_K(0^{128})$, $B_{128} = 0^{120} \| 10000111$

$$K_1 = \begin{cases} R \ll 1, & \text{if } R[\text{first bit}] = 0, \\ (R \ll 1) \oplus B_{128}, & \text{otherwise} \end{cases}$$

$$K_2 = \begin{cases} K_1 \ll 1, & \text{if } R[\text{first bit}] = 0, \\ (K_1 \ll 1) \oplus B_{128}, & \text{otherwise} \end{cases}$$

$\underline{OMAC1^{(s)}(K, M = M[1] \| \ldots \| M[t])}$

1: $C[0] = 0^n$

2: $C[i] = E_K(C[i-1] \oplus M[i]), i = 1, \ldots, t-1$

3: $(K^*, M^*) = \begin{cases} (K_1, M[t]), & \text{if } |M[t]| = n \\ (K_2, M[t] \| 1 \| 0^{n-|M[t]|-1}), & \text{otherwise} \end{cases}$

4: $T = E_K(C[t-1] \oplus M^* \oplus K^*)[\text{first } s \text{ bits}]$

5: return T

«8 bits» scheme

$IV \in \{0,1\}^{56}$, $s \leq 128$, $0 < |P| < 2^{64}$, $0 \leq |A| < 2^{64}$

$\underline{8\text{bits}^{(s)}.\mathsf{Enc}(K, IV, P, A)}$

1: $N = 0^8 \| IV \| \text{str}_{64}(1)$

2: $C = CTR^N(K, P)$

3: $F = \begin{cases} 1^7 \| 0 & \text{if } |A| = 0, \\ 1^7 \| 1 & \text{if } |A| > 0 \end{cases}$

4: $B = \underbrace{F \| \text{str}_8(s) \| IV \| A \| C \| 0^{128d - |C| - |A| - 72}}_{128d} \| \text{str}_{64}(|A|) \| \text{str}_{64}(|C|)$

5: $T = OMAC1^{(s)}(K, B)$

6: return $C \| T$

We assume that for i-th processed message IV is calculated as a counter by the following way: $IV = \text{str}_{56}(i-1)$.

«8 bits» scheme

$IV \in \{0,1\}^{56}$, $s \leq 128$, $0 < |P| < 2^{64}$, $0 \leq |A| < 2^{64}$

$\underline{8\text{bits}^{(s)}.\mathsf{Enc}(K, IV, P, A)}$

1: $N = 0^8 \| IV \| \text{str}_{64}(1)$
2: $C = CTR^N(K, P)$
3: $F = \begin{cases} 1^7 \| 0 & \text{if } |A| = 0, \\ 1^7 \| 1 & \text{if } |A| > 0 \end{cases}$
4: $B = \underbrace{F \| \text{str}_8(s) \| IV \| A \| C \| 0^{128d - |C| - |A| - 72}}_{128d} \| \text{str}_{64}(|A|) \| \text{str}_{64}(|C|)$
5: $T = OMAC1^{(s)}(K, B)$
6: return $C \| T$

We assume that for i-th processed message IV is calculated as a counter by the following way: $IV = \text{str}_{56}(i-1)$.

Our attack

Stage 1: Getting information from encryption part

The goal of our attack is to make a forgery for $s = 128$.

Let $l \in \{6, \ldots, 55\}$ be a parameter of the attack.
Take no associated data $A = \varnothing$ and arbitrary plaintexts P_1, P_2, $\ldots$, P_{2^l} such that $|P_i| = 2^{64} - 128$, $i = 1, \ldots, 2^l$.

For all $i = 1, \ldots, 2^l$ we make the query $(IV_i, P_i, \varnothing)$ with $IV_i = \mathrm{str}_{64}(i-1)$ to $8\mathrm{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C_i, T_i).

$P_i = P_i[1] \| P_i[2] \| \ldots \| P_i[t]$, $t = 2^{57} - 1$
$C_i = C_i[1] \| C_i[2] \| \ldots \| C_i[t]$
$C_i[j] = P_i[j] \oplus E_K(S_i[j])$, $S_i[j] = 0^8 \| IV_i \| \mathrm{str}_{64}(j)$
Now we know all $\Gamma_i[j] = E_K(S_i[j])$, $i = 1, \ldots, 2^l$, $j = 1, \ldots, 2^{57} - 1$.
Denote by
$\mathcal{S} = \{S_i[j]\}$ — the set of all strings $S_i[j]$.
$\mathcal{G} = \{\Gamma_i[j]\}$ — the corresponding set of the cipher outcomes.

Our attack

Stage 1: Getting information from encryption part

The goal of our attack is to make a forgery for $s = 128$.

Let $l \in \{6, \ldots, 55\}$ be a parameter of the attack.
Take no associated data $A = \varnothing$ and arbitrary plaintexts P_1, P_2, $\ldots$, P_{2^l} such that $|P_i| = 2^{64} - 128$, $i = 1, \ldots, 2^l$.

For all $i = 1, \ldots, 2^l$ we make the query $(IV_i, P_i, \varnothing)$ with $IV_i = \mathrm{str}_{64}(i-1)$ to $8\mathrm{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C_i, T_i).

$P_i = P_i[1] \| P_i[2] \| \ldots \| P_i[t]$, $t = 2^{57} - 1$
$C_i = C_i[1] \| C_i[2] \| \ldots \| C_i[t]$
$C_i[j] = P_i[j] \oplus E_K(S_i[j])$, $S_i[j] = 0^8 \| IV_i \| \mathrm{str}_{64}(j)$
Now we know all $\Gamma_i[j] = E_K(S_i[j])$, $i = 1, \ldots, 2^l$, $j = 1, \ldots, 2^{57} - 1$.
Denote by
$\mathcal{S} = \{S_i[j]\}$ — the set of all strings $S_i[j]$.
$\mathcal{G} = \{\Gamma_i[j]\}$ — the corresponding set of the cipher outcomes.

Our attack

Stage 1: Getting information from encryption part

The goal of our attack is to make a forgery for $s = 128$.

Let $l \in \{6, \ldots, 55\}$ be a parameter of the attack.
Take no associated data $A = \varnothing$ and arbitrary plaintexts P_1, P_2, $\ldots$, P_{2^l} such that $|P_i| = 2^{64} - 128$, $i = 1, \ldots, 2^l$.

For all $i = 1, \ldots, 2^l$ we make the query $(IV_i, P_i, \varnothing)$ with $IV_i = \mathrm{str}_{64}(i-1)$ to $8\mathsf{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C_i, T_i).

$P_i = P_i[1] \| P_i[2] \| \ldots \| P_i[t]$, $t = 2^{57} - 1$
$C_i = C_i[1] \| C_i[2] \| \ldots \| C_i[t]$
$C_i[j] = P_i[j] \oplus E_K(S_i[j])$, $S_i[j] = 0^8 \| IV_i \| \mathrm{str}_{64}(j)$
Now we know all $\Gamma_i[j] = E_K(S_i[j])$, $i = 1, \ldots, 2^l$, $j = 1, \ldots, 2^{57} - 1$.

Denote by
$\mathcal{S} = \{S_i[j]\}$ — the set of all strings $S_i[j]$.
$\mathcal{G} = \{\Gamma_i[j]\}$ — the corresponding set of the cipher outcomes.

Our attack

Stage 1: Getting information from encryption part

The goal of our attack is to make a forgery for $s = 128$.

Let $l \in \{6, \ldots, 55\}$ be a parameter of the attack.
Take no associated data $A = \varnothing$ and arbitrary plaintexts P_1, P_2, $\ldots$, P_{2^l} such that $|P_i| = 2^{64} - 128$, $i = 1, \ldots, 2^l$.

For all $i = 1, \ldots, 2^l$ we make the query $(IV_i, P_i, \varnothing)$ with $IV_i = \mathrm{str}_{64}(i-1)$ to $8\mathsf{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C_i, T_i).

$P_i = P_i[1] \| P_i[2] \| \ldots \| P_i[t]$, $t = 2^{57} - 1$
$C_i = C_i[1] \| C_i[2] \| \ldots \| C_i[t]$
$C_i[j] = P_i[j] \oplus E_K(S_i[j])$, $S_i[j] = 0^8 \| IV_i \| \mathrm{str}_{64}(j)$
Now we know all $\Gamma_i[j] = E_K(S_i[j])$, $i = 1, \ldots, 2^l$, $j = 1, \ldots, 2^{57} - 1$.
Denote by
$\mathcal{S} = \{S_i[j]\}$ — the set of all strings $S_i[j]$.
$\mathcal{G} = \{\Gamma_i[j]\}$ — the corresponding set of the cipher outcomes.

Our attack

Stage 2: Getting information from authentication part

$\mathcal{IV}' = \{IV_i \mid i = 1, \ldots, 2^l\}$, $\mathcal{IV}'' = \{0,1\}^{56} \setminus \mathcal{IV}'$.
For all $IV \in \mathcal{IV}''$ we set $P = 0^1 \in V_1$, $A = 0^1 \in V_1$, make the query (IV, P, A) to $8\text{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C, T).
Consider the tag $T = OMAC1^{(128)}(K, B)$, where

$$B = \underbrace{F \| \mathrm{str}_8(128) \| IV \| A \| C \| 0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)}_{B_1},$$

$$T = E_K(E_K(B_0) \oplus K_1 \oplus B_1).$$

Note that for any new IV the string B_0 is new and $B_1 = \mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)$. By $\mathcal{B} = \{(F \| \mathrm{str}_8(128) \| IV \| A \| C \| 0^{54}) \mid IV \in \mathcal{IV}''\}$ we denote the set of all such blocks B_0.
Thus at the end of this stage we have OMAC1 tags $\mathcal{T} = \{E_K(E_K(B_0) \oplus K_1 \oplus B_1) \mid B_0 \in \mathcal{B}\}$.

Our attack

Stage 2: Getting information from authentication part

$\mathcal{IV}' = \{IV_i \mid i = 1, \ldots, 2^l\}$, $\mathcal{IV}'' = \{0,1\}^{56} \setminus \mathcal{IV}'$.
For all $IV \in \mathcal{IV}''$ we set $P = 0^1 \in V_1$, $A = 0^1 \in V_1$, make the query (IV, P, A) to $8\text{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C, T).
Consider the tag $T = OMAC1^{(128)}(K, B)$, where

$$B = \underbrace{F\|\mathrm{str}_8(128)\|IV\|A\|C\|0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)}_{B_1},$$

$$T = E_K(E_K(B_0) \oplus K_1 \oplus B_1).$$

Note that for any new IV the string B_0 is new and $B_1 = \mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)$. By $\mathcal{B} = \{(F\|\mathrm{str}_8(128)\|IV\|A\|C\|0^{54}) \mid IV \in \mathcal{IV}''\}$ we denote the set of all such blocks B_0.
Thus at the end of this stage we have OMAC1 tags $\mathcal{T} = \{E_K(E_K(B_0) \oplus K_1 \oplus B_1) \mid B_0 \in \mathcal{B}\}$.

Our attack

Stage 2: Getting information from authentication part

$\mathcal{IV}' = \{IV_i \mid i = 1, \ldots, 2^l\}$, $\mathcal{IV}'' = \{0,1\}^{56} \setminus \mathcal{IV}'$.
For all $IV \in \mathcal{IV}''$ we set $P = 0^1 \in V_1$, $A = 0^1 \in V_1$, make the query (IV, P, A) to $8\text{bits}^{(s)}.\mathsf{Enc}$ and get the answer (C, T).
Consider the tag $T = OMAC1^{(128)}(K, B)$, where

$$B = \underbrace{F\|\mathrm{str}_8(128)\|IV\|A\|C\|0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)}_{B_1},$$

$$T = E_K(E_K(B_0) \oplus K_1 \oplus B_1).$$

Note that for any new IV the string B_0 is new and $B_1 = \mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)$. By $\mathcal{B} = \{(F\|\mathrm{str}_8(128)\|IV\|A\|C\|0^{54}) \mid IV \in \mathcal{IV}''\}$ we denote the set of all such blocks B_0.
Thus at the end of this stage we have OMAC1 tags $\mathcal{T} = \{E_K(E_K(B_0) \oplus K_1 \oplus B_1) \mid B_0 \in \mathcal{B}\}$.

Our attack

Stage 3: Finding collision

Now we find a collision — an element in $\mathcal{G} \cap \mathcal{T}$.
It is needed to estimate the collision probability

$$p = \Pr_K \left[\underbrace{\{E_K(S)_{S \in \mathcal{S}}\}}_{\mathcal{G}} \cap \underbrace{\{E_K(E_K(B_0) \oplus K_1 \oplus B_1)\}_{B_0 \in \mathcal{B}}}_{\mathcal{T}} \neq \varnothing \right]$$

under the following conditions : $\mathcal{S} \cap \mathcal{B} = \varnothing$, $0^{128} \notin \mathcal{S}$, $0^{128} \notin \mathcal{B}$, $|\mathcal{S}| = 2^l(2^{57} - 1)$, $|\mathcal{B}| = 2^{56} - 2^l$, $K_1 = K_1(E_K(0^{128}))$.
In the ideal cipher model we obtain the following estimation

$$p \geqslant 1 - e^{-2^{l-15}\left(1-\frac{1}{2^{56-l}}\right)\left(1-\frac{1}{2^{57}}-\frac{1}{2^{57+l}}\right)} \underbrace{\approx}_{\text{fix } l=15} 1 - e^{-1} \approx 0.63.$$

Our attack

Stage 3: Finding collision

Now we find a collision — an element in $\mathcal{G} \cap \mathcal{T}$.
It is needed to estimate the collision probability

$$p = \mathrm{Pr}_K \left[\underbrace{\{E_K(S)_{S \in \mathcal{S}}\}}_{\mathcal{G}} \cap \underbrace{\{E_K(E_K(B_0) \oplus K_1 \oplus B_1)\}_{B_0 \in \mathcal{B}}}_{\mathcal{T}} \neq \varnothing \right]$$

under the following conditions : $\mathcal{S} \cap \mathcal{B} = \varnothing$, $0^{128} \notin \mathcal{S}$, $0^{128} \notin \mathcal{B}$, $|\mathcal{S}| = 2^l(2^{57} - 1)$, $|\mathcal{B}| = 2^{56} - 2^l$, $K_1 = K_1(E_K(0^{128}))$.
In the ideal cipher model we obtain the following estimation

$$p \geqslant 1 - e^{-2^{l-15}\left(1-\frac{1}{2^{56-l}}\right)\left(1-\frac{1}{2^{57}}-\frac{1}{2^{57+l}}\right)} \underbrace{\approx}_{\text{fix } l=15} 1 - e^{-1} \approx 0.63.$$

Our attack

Stage 4: Forging tag

Suppose that we have collision and $OMAC1^{(128)}(K, B) = \Gamma_i[j] = E_K(0^8 \| IV_i \| \mathrm{str}_{64}(j))$, where

$$B = \underbrace{F \| \mathrm{str}_8(128) \| IV \| A \| C \| 0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)}_{B_1}.$$

Consider pairs (C', A'): $C' = 0^1 \in V_1$ and $A' = 0 \| C \| 0^u$, $u = 0, \ldots, 53$. Note that the OMAC input for such pairs is equal to

$$B' = \underbrace{F \| \mathrm{str}_8(128) \| IV \| A' \| C' \| 0^{55-(u+2)}}_{B'_0} \| \underbrace{\mathrm{str}_{64}(u+2) \| \mathrm{str}_{64}(1)}_{B'_1}.$$

Note that $B'_0 = B_0$ and thus OMAC value $OMAC1^{(128)}(K, B')$ is equal to $E_K(E_K(B'_0) \oplus K_1 \oplus B'_1) = E_K(E_K(B_0) \oplus K_1 \oplus B'_1)$

Let us consider the set of strings
$\hat{\mathcal{B}} = \{\hat{B} \in V_{128} | \hat{B} = \mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1), r = 2, \ldots, 55$. This set describes all possible values of B'_1 for pairs (C', A'). Note that for all $\hat{B} \in \hat{\mathcal{B}}$ holds

$$E_K(B_0) \oplus K_1 \oplus \hat{B} = E_K(B_0) \oplus K_1 \oplus B_1 \oplus (B_1 \oplus \hat{B}) =$$
$$= 0^8 \| IV_i \| \mathrm{str}_{64}(j) \oplus ((\mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)) \oplus (\mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1))) =$$
$$= 0^8 \| IV_i \| \mathrm{str}_{64}(j) \oplus ((\mathrm{str}_{64}(1) \oplus \mathrm{str}_{64}(r)) \| \mathrm{str}_{64}(0)) = 0^8 \| IV_t \| \mathrm{str}_{64}(j),$$

where IV_t can differ from IV_i only in the 6 least significant bits. Hence $0^8 \| IV_t \| \mathrm{str}_{64}(j) \in \mathcal{S}$, and we know the corresponding ciphertext $E_K(0^8 \| IV_t \| \mathrm{str}_{64}(j))$ from the first stage.
Therefore we can forge the tag value for the pair (C', A') that corresponds $\hat{B}$ as follows

$$E_K(E_K(B_0) \oplus K_1 \oplus \hat{B}) = E_K(0^8 \| IV_t \| \mathrm{str}_{64}(i)),$$

where $\hat{B} = \mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1)$. Therefore we get 54 forged tags with the probability $p > 0.63$.

Summary of the attack

Our attack on «8 bits» mode has the followng characteristics:

- Threat: forging tags for 54 ciphered messages with associated data
- Success probability: 0.63
- Number of queries: 2^{56}
- Total length of queries: 2^{72} blocks
- Total complexity: 2^{79} elementary operations over 128-bits words

Countermeasures

The described attack is based on the adversary's possibility to obtain clear tag values and then to compare them with keystream blocks used for encryption.

One of the ways to resist the above attack is to use design principals of the CCM — to cipher the MAC output.

$8\text{bits}^{(s)}.\mathsf{Enc}(K, IV, P, A)$

1: $N = 0^8 \| IV \| \text{str}_{64}(1)$

2: $(\underbrace{\gamma}_{128} \| C) = CTR^N(K, 0^{128} \| P)$

3: $F = \begin{cases} 1^7 \| 0 & \text{if } |A| = 0, \\ 1^7 \| 1 & \text{if } |A| > 0 \end{cases}$

4: $B = \underbrace{F \| \text{str}_8(s) \| IV \| A \| C \| 0^{128d - |C| - |A| - 72}}_{128d} \| \text{str}_{64}(|A|) \| \text{str}_{64}(|C|)$

5: $T = OMAC1^{(s)}(K, B) \oplus \gamma[\text{first } s \text{ bits}]$

6: return $C \| T$

Countermeasures

The described attack is based on the adversary's possibility to obtain clear tag values and then to compare them with keystream blocks used for encryption.

One of the ways to resist the above attack is to use design principals of the CCM — to cipher the MAC output.

$\underline{8\text{bits}^{(s)}.\mathsf{Enc}(K, IV, P, A)}$

1: $N = 0^8 \| IV \| \mathrm{str}_{64}(1)$

2: $(\underbrace{\gamma}_{128} \| C) = CTR^N(K, 0^{128} \| P)$

3: $F = \begin{cases} 1^7 \| 0 & \text{if } |A| = 0, \\ 1^7 \| 1 & \text{if } |A| > 0 \end{cases}$

4: $B = \underbrace{F \| \mathrm{str}_8(s) \| IV \| A \| C \| 0^{128d - |C| - |A| - 72}}_{128d} \| \mathrm{str}_{64}(|A|) \| \mathrm{str}_{64}(|C|)$

5: $T = OMAC1^{(s)}(K, B) \oplus \gamma[\text{first } s \text{ bits}]$

6: return $C \| T$

Conclusion

- the near birthday attack for the «8 bits» mode is proposed
- the minor modification of the «8 bits» mode to resist the attack is proposed

Thank you for your attention!

Questions?

Questions, comments:

- lah@cryptopro.ru
- karpunin@cryptopro.ru
- sedovgk@cryptopro.ru