The CTR mode with encrypted nonces and its extension to AE

Sergey Agievich

Research Institute for Applied Problems
of Mathematics and Informatics

Belarusian State University

agievich@{bsu.by|gmail.com}

CTCrypt-2019

[Svetlogorsk, 2019.06.05]

1. CTR

A block cipher: $E = \{E_K : K \in \mathcal{K}\}$, $E_K \in \mathrm{Perm}(n)$
(Perm(n) is the set of all permutations over $\{0,1\}^n$)

An encryption mode: an extension of E from $\{0,1\}^n$ to $\{0,1\}^*$

The CTR mode ($\{0,1\}^* \ni X \mapsto Y \in \{0,1\}^{|X|}$):

- choose $\mathtt{next} \in \mathrm{Perm}(n)$;
- choose a nonce $S \in \{0,1\}^n$;
- build counters $C_1 = S, C_2 = \mathtt{next}(C_1), C_3 = \mathtt{next}(C_2), \ldots$;
- truncate $C_1 \parallel C_2 \parallel C_3 \parallel \ldots$ to $|X|$ bits and obtain $\Gamma \in \{0,1\}^{|X|}$;
- $Y \leftarrow X \oplus \Gamma$.

.su: “режим гаммирования”.

2. Gamma overlapping

Sequences of counters (gammas) in different encryption sessions **must not** overlap!

To avoid overlapping (NIST SP 800-38A, ISO 10116, GOST 34.13):
1) `next` is chosen to have long disjoint cycles in its cycle decomposition;
2a) the nonces S of different sessions are picked from different cycles
or
2b) a new nonce continues the cycle from the previous session.

Implementation: a safe monotonous timer, rewritable memory, ~~random generation~~.

3. . . . with encrypted nonces

GOST 28147 (1989): ~~$C_1 = S$~~ $C_1 = \mathtt{next}(E_K(S))$

CTR2 (Rogaway, 2004): $C_1 = E_K(S)$

Drawbacks of nonce encryption:
1) decreases effectiveness (the additional invocation of E_K);
2) only probabilistic guarantees of gamma non-overlapping.

Fortunately, these guarantees are strong enough ($\Downarrow$).

4. CPA-security (CPA = Chosen Plaintext Attack)

An adversary: a probabilistic algorithm A that gains access to an encryption oracle $O\colon (X, S) \mapsto Y$.

Contracts (A must follow one of them):

- $S \xleftarrow{\$} \{0,1\}^n$ (random nonces);
- the nonces S are arbitrary distinct (non-repeating nonces).

Implementations:

- $O(X, S) = \mathsf{CTR2}[E_K](X, S)$, $E_K \xleftarrow{\$} E$ (real);
- $O(X, S) = \mathsf{CTR2}[\pi](X, S)$, $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ (idealized real);
- $O(X, S) = \rho(S, X)$, where ρ is a random function (ideal).

A's advantage:

$$\mathbf{Adv}^{\texttt{ind-cpa}}_{\mathsf{CTR2}[\mathrm{Perm}(n)]}(A) = \left|\mathbf{P}\left\{A^{\mathsf{CTR2}[\pi]} = 1\right\} - \mathbf{P}\left\{A^{\rho} = 1\right\}\right|.$$

5. Security of CTR2

Theorem 1. Let M, the maximum cycle length of `next`, be at least $N-1$ ($N=2^n$). Let an adversary A make at most q queries (X,S) with either random or non-repeating S. Let r be the total number of X's blocks in these queries. Then

$$\mathbf{Adv}^{\texttt{ind-cpa}}_{\mathrm{CTR2[Perm}(n)]}(A) \le \frac{r(r-1)}{2N} + \varepsilon,$$

where

$$\varepsilon = \max\left(0, \frac{r(r+2q-1)(4qr-q^2-2r+3q+2)}{4N^2} - \frac{(r-q)^2+r-3q-2}{2N}\right).$$

Proof: Patarin's "coefficients H" technique, combinatorics ($\Downarrow$).

Corollary:

$$\mathbf{Adv}^{\texttt{ind-cpa}}_{\mathrm{CTR2[Perm}(n)]}(A) \le \frac{r^2+r+2}{2N} + \frac{r^2(9r^2+5)}{4N^2}.$$

6. Battleship on the cycle: the game

Players: Navy and an adversary.

Battlefield: a circle with M points (numbered from 0 to $M-1$).

Input: q (a number of ships) and r (their total displacement).

Rules:

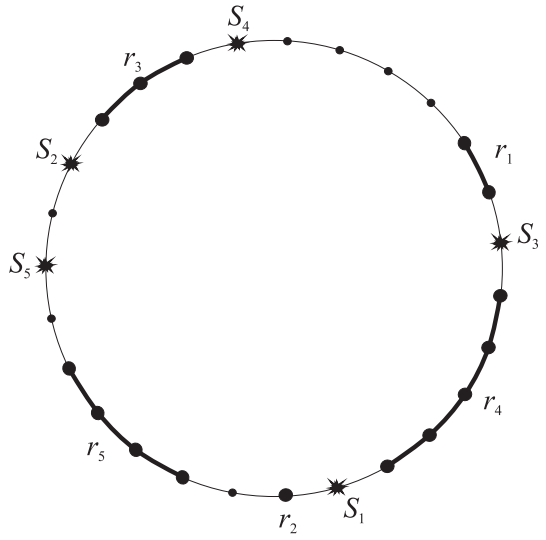
1. The adversary splits r into a sum $r_1+r_2+\ldots+r_q$ of positive integers and reports $r_1, r_2, \ldots, r_q$ to Navy.

2. Navy deploys ships at distinct random places on the circle. Navy loses in the case of collisions.

3. The adversary makes q shots at different points $S_1, \ldots, S_q$. If at least one shot hits a ship, then the adversary wins. If all the shots miss, then Navy wins.

Options: G_1 (S_i are random distinct), G_2 (S_i are arbitrary distinct).

7. Battleship on the cycle: odds to win



Lemma 1. In the games G_1 and G_2,

$$\mathbf{P}\{\text{Navy wins}\} \geq 1 - \frac{4qr - q^2 - 2r + q}{M}.$$

Proof: use a well-known estimate by V. Nosov (regarding the success of the ship deployment).

$\approx$ **the best** A**'s strategy in** G_2: choose $r_1 = r_2 = \ldots = r_{q-1} = \lceil r/q \rceil$ and shoot with step r_1 starting from a random point.

8. . . . and its extension to AE

AE (Authenticated Encryption): $(X, S) \mapsto (Y, T)$
(T is an authentication tag)

AEAD (AE with Additional Data): $(X, I, S) \mapsto (Y, T)$
(I is public data)

MAC-then-Encrypt: $T = T(I, X)$

Encrypt-then-MAC: $T = T(I, Y)$ (is preferable, see [Bellare and Namprepre, 2008])

Polynomial hashing:

1) interpret $\{0,1\}^n$ as $F = \mathbb{F}_{2^n}$;
2) $(I, Y) \overset{injective}{\mapsto} f(\lambda) \in F[\lambda]$;
3) choose a secret random point $H \in \{0,1\}^n$;
4) $T \leftarrow f(H) + \ldots$.

9. H: static or ephemeral?

The Wegman-Carter-Shoup scheme (the core of GCM, static H):

$H \leftarrow E_K(0)$, $T \leftarrow f(H) + E_K(S)$.

The math behind: if f and f' are distinct and $\deg f, \deg f' \leq d$, then

$$\mathbf{P}\left\{f(H) = f'(H)\right\} = \mathbf{P}\left\{H \text{ is a root of } f - f'\right\} \leq \frac{d}{N}.$$

The probability is small if $d \ll N$ (this is the case).

But: if S repeats, then H can be recovered as a root of $(f(\lambda) - T) - (f'(\lambda) - T')$.

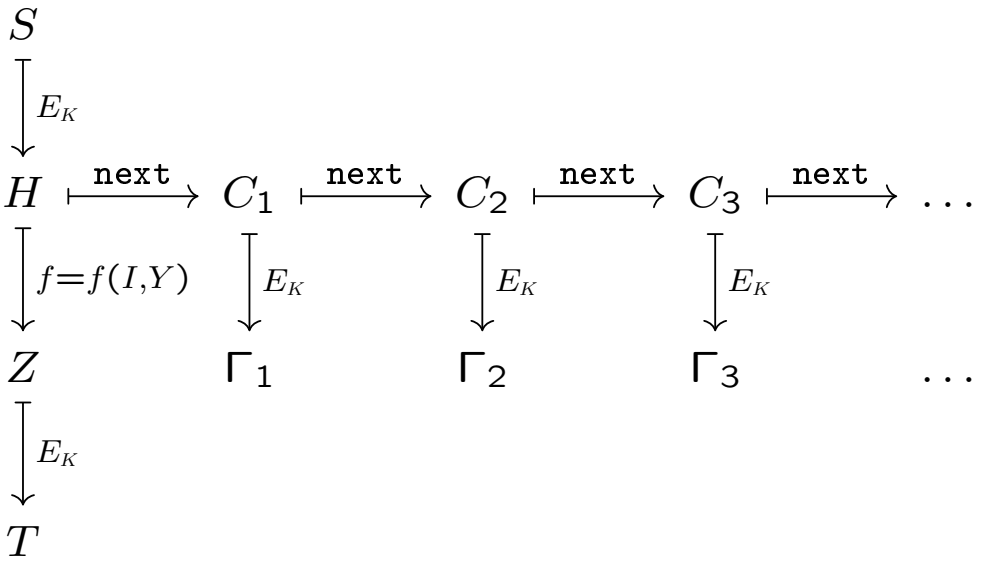
The EHE scheme (Encrypt-Hash-Encrypt, ephemeral H):

$H \leftarrow E_K(S)$, $T \leftarrow E_K(f(H))$.

The new math (due to Ore, 1922):

$$\mathbf{P}\left\{f(H) = f'(H')\right\} \leq \frac{d}{N}.$$

10. CHE = Counter+Hash+Encrypt



Problem: collisions $C_i = \texttt{next}^i(H) = f(H) = Z$

Solution:

1) $\texttt{next}(\lambda) = \alpha\lambda + \beta$, $\beta \neq 0$, α is primitive;
2) the free term of $f(\lambda)$ is always zero.

1) + 2) $\Rightarrow$ $(\texttt{next}^i - f)(\lambda)$ is nonzero $\Rightarrow$ $\mathbf{P}\left\{\texttt{next}^i(H) = f(H)\right\} \leq d/N$.

Another solution (`belt-datawrap`): $H \leftarrow E_K^2(S)$.

11. CHE: algorithms

Algorithm Wrap

Input: X, I, K, S.
Output: Y, T.
Steps:

1. $H \leftarrow E_K(S)$, $C \leftarrow H$, $T \leftarrow T_0$.
2. $(I_1, \ldots, I_{r'}) \xleftarrow{n} I$.
3. For $i = 1, 2, \ldots, r'$:
   (a) $T \leftarrow (T \oplus I_i) * H$.
4. $(X_1, \ldots, X_r) \xleftarrow{n} X$.
5. For $i = 1, 2, \ldots, r$:
   (a) $C \leftarrow \texttt{next}(C)$;
   (b) $Y_i \leftarrow X_i \oplus E_K(C)$;
   (c) $T \leftarrow (T \oplus Y_i) * H$.
6. $Y \xleftarrow[|X|]{} (Y_1, \ldots, Y_r)$.
7. Encode $|I|$ and $|X|$ by $W \in \{0,1\}^n$.
8. $T \leftarrow (T \oplus W) * H$.
9. $T \leftarrow E_K(T)$.
10. Return (Y, T).

Algorithm Unwrap

Input: Y, I, K, S, T.
Output: X or $\perp$ (authentication error).
Steps:

1. $H \leftarrow E_K(S)$, $C \leftarrow H$, $T' \leftarrow T_0$.
2. $(I_1, \ldots, I_{r'}) \xleftarrow{n} I$.
3. For $i = 1, 2, \ldots, r'$:
   (a) $T' \leftarrow (T' \oplus I_i) * H$.
4. $(Y_1, \ldots, Y_r) \xleftarrow{n} Y$.
5. For $i = 1, 2, \ldots, r$:
   (a) $T' \leftarrow (T' \oplus Y_i) * H$;
   (b) $C \leftarrow \texttt{next}(C)$;
   (c) $X_i \leftarrow Y_i \oplus E_K(C)$.
6. $X \xleftarrow[|Y|]{} (X_1, \ldots, X_r)$.
7. Encode $|I|$ and $|X|$ by $W \in \{0,1\}^n$.
8. $T' \leftarrow (T' \oplus W) * H$.
9. $T' \leftarrow E_K(T')$.
10. Return X if $T = T'$ and $\perp$ otherwise.

Complexity: $(r + 2)\mathsf{E} + (r + r')\mathsf{M}$ (under the proper choice of α in `next`)

12. Security of CHE

Theorem 2. Let an adversary A make at most q queries (X, I, S) with either random or non-repeating S. Let r be the total number of X's and I's blocks in these queries. Then*

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathsf{CHE}[\mathsf{Perm}(n)]}(A) \le \frac{(r+q)(r+q-1)}{2N} + \varepsilon,$$

where

$$\varepsilon = \frac{(2r^2+9qr+2q^2-3r+2q+2)(r+q)(r+3q-1)}{4N^2} + \frac{r^2+5qr-q^2-2r+3q+2}{2N}.$$

Corollary:

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathsf{CHE}[\mathsf{Perm}(n)]}(A) \le \frac{9r^2-r+2}{2N} + \frac{26r^4}{N^2}.$$

*`priv` is AE synonym for `ind-cpa`