Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption

CTCrypt 2017

Vladislav Nozdrunov

TC 26

05 June 2017

New scheme? Why it should be done?

New scheme? Why it should be done?

- lack in the National standards in these sphere;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;
  - not full parallelling MAC;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;
  - not full parallelling MAC;
  - not online;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;
  - not full parallelling MAC;
  - not online;
  - deep doubts about security;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;
  - not full parallelling MAC;
  - not online;
  - deep doubts about security;
- not only reporter's opinion – CAESAR competition prove it;

New scheme? Why it should be done?

- lack in the National standards in these sphere;
- NIST & ISO standards have different disadvantages:
  - patented;
  - not full parallelling MAC;
  - not online;
  - deep doubts about security;
- not only reporter's opinion – CAESAR competition prove it;
- many discussion on RusCrypto'2017 and other conference.

Tasks under construction

Tasks under construction

- full parallelization;

Tasks under construction

- full parallelization;
- support associated data;

Tasks under construction

- full parallelization;
- support associated data;
- online;

Tasks under construction

- full parallelization;
- support associated data;
- online;
- inverse free.

Description of PD–mode encryption

1. E_K – n-bit block cipher;
2. INPUT: $N \in V_{n-1}$, $K \in V_k$, $A, P \in V^*$;
3. OUTPUT: $C \in V^*$, $T \in V_n$;
4. Encryption – CTR_r mode:

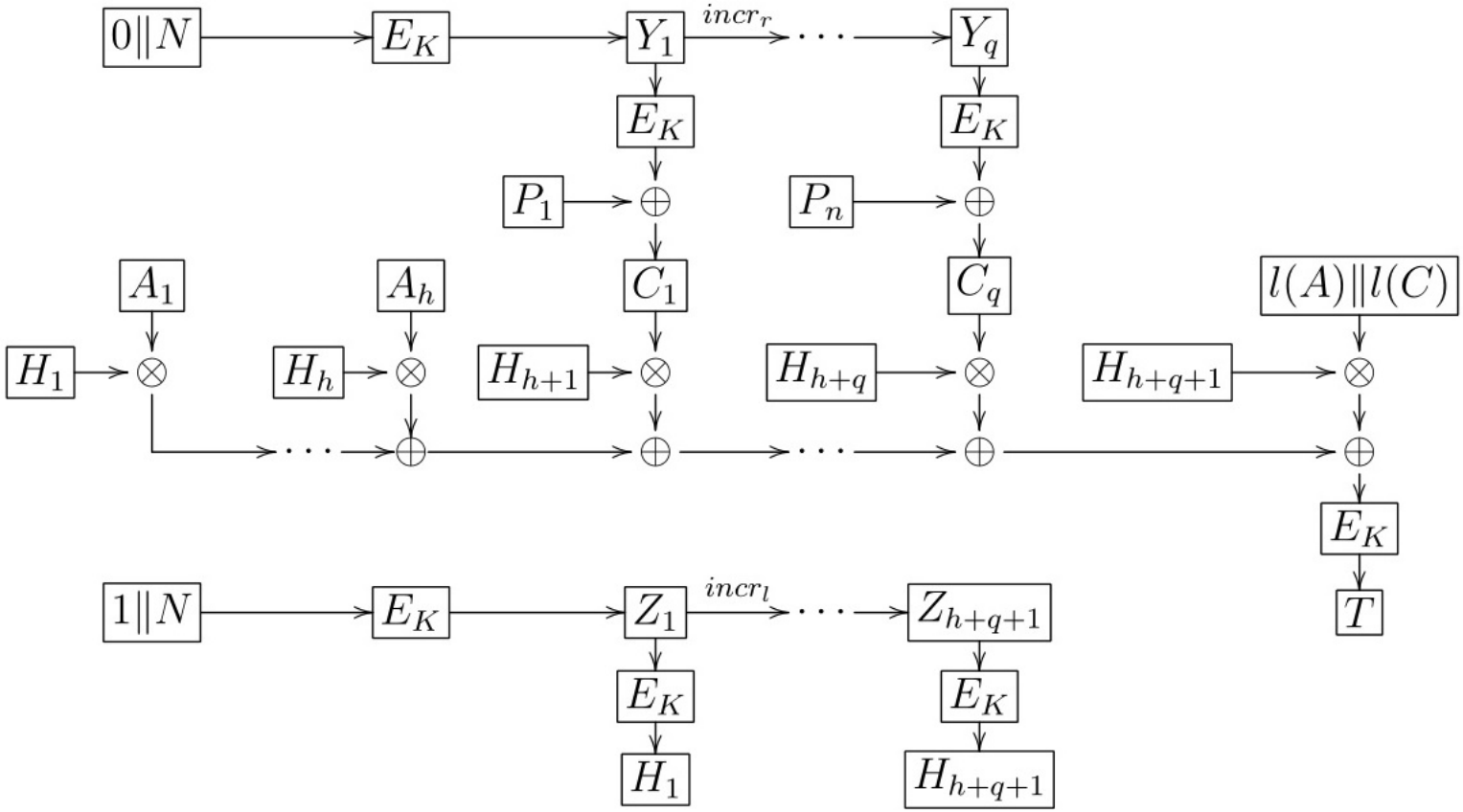
$$\begin{cases} Y_1 = E_K(0^1 \| N), \\ Y_i = incr_r(Y_{i-1}), & 2 \le i \le q, \\ C_i = P_i \oplus E_K(Y_i), & 1 \le i \le q-1, \\ C_q^* = P_q^* \oplus MSB_u(E_K(Y_q)), \\ incr_r(L \| R) = L \| (R \boxplus 1),\ L, R \in V_{n/2}. \end{cases}$$

Description of PD–mode authentication

1. E_K – n-bit block cipher;
2. INPUT: $N \in V_{n-1}$, $K \in V_k$, $A, P \in V^*$;
3. OUTPUT: $C \in V^*$, $T \in V_n$;
4. Authentication – $ML_K(A\|C, N) = T$:

$$\begin{cases} Z_1 = E_K(1^1\|N), \\ Z_i = incr_l(Z_{i-1}),\ 2 \le i \le h+q+1, \\ H_i = E_K(Z_i),\ incr_l(L\|R) = L \boxplus 1\|R,\ L, R \in V_{n/2}. \\ T = E_K\left(\sum_{i=1}^{h} H_i \otimes A_i \oplus \sum_{j=1}^{q} H_{h+j} \otimes C_j \oplus \right. \\ \qquad \left. \oplus\ H_{h+q+1} \otimes (l(A)\|l(C))\right) \end{cases}$$

PD-mode scheme



Security of encryption

Theorem 1

Let E_K be a block cipher, $K \in \mathcal{K}$, then, for any integers t, q and $\mu = q' \cdot n$

$$Adv^{lor-cpa}_{CTR_r}(q, \mu, t) \leq 2 \cdot Adv^{prp}_{E_K}(t, q') + \frac{(q-1)\mu}{n \cdot 2^{n-1}} - \frac{q(q-1)}{2^{n-1}}.$$

Security of authentication

Theorem 2

Let E_K be a block cipher, $ML = \{ML_K | K \in \mathcal{K}\}$ is the family of function defined above, then, for any integers $q_s, q_v, \mu_s, \mu_v, t$ we have

$$Adv^{auth}_{ML}(q_s, q_v, \mu_s, \mu_v, t) \leqslant \frac{\mu'(q'-1)}{n2^{n-1}} - \frac{q'(q'-1)}{2^{n-1}} + \\ + Adv^{prp}_{ML}(q'\mu', t') + + \frac{q'\mu'(q'\mu'-1)}{2^{n+1}} + \frac{q_v}{2^n}.$$

where $q' = (q_s + q_v)$, $\mu' = (\mu_s + \mu_v)$ and $t' = t + O(\mu' \cdot q')$.

The End

Thank you for your attention!
Any questions?

If you want something about provable security

Experiment $Exp^{lor-cpa-b}_{\Pi,A}$

- $K \longleftarrow \mathcal{K}$;
- $d = A^{\mathcal{E}_K(LR(\cdot,\cdot,b))}$;
- return d.

$$Adv^{lor-cpa}_{\Pi,A_{CPA}} = P\left[Exp^{lor-cpa-1}_{\Pi,A_{CPA}} = 1\right] - P\left[Exp^{lor-cpa-0}_{\Pi,A_{CPA}} = 1\right];$$

If you want something about provable security

For any integers t, q, μ

$$Adv_{\Pi}^{lor-cpa}(q, \mu, t) = \max_{A_{CPA}}\{Adv_{\Pi, CPA}^{lor-cpa}\};$$

where the maximum is over all A_{CPA} with "time complexity" t, each making at most q queries to the $\mathcal{E}_K(\mathcal{LR}(\cdot, \cdot; b))$ oracle, totalling at most μ bits.

If you want something about provable security

Experiment $Exp^{auth}_{MAC}(A)$

- $K \longleftarrow \mathcal{K}$;
- Run $A^{MAC_K(\cdot),VF_K(\cdot,\cdot)}$, where $VF_K(M,T)$ is 1 if $MAC_K(M) = T$ and 0 otherwise
- if A made VF_K query (M,T) such that
  - The oracle returned 1, and
  - A did not, prior to making verification query (M,T), make tag-generation query M

  then return 1 else return 0.

The auth advantage of A is defined as

$$Adv^{auth}_{MAC}(A) = P[Exp^{auth}_{MAC}(A) = 1].$$

If you want something about provable security

For any integers $q_s, q_v, \mu_s, \mu_v, t$ we define

$$Adv^{auth}_{MAC}(q_s, q_v, \mu_s, \mu_v, t) = \max_A \{Adv^{auth}_{MAC}(A)\}$$

where the maximum is over all A making q_s MAC-generation queries of total length μ_s, q_v MAC-verification queries of total length μ_v, and having running time t.