ПИСЬМО В РЕДАКЦИЮ

В моей статье «Оценка стойкости AE-криптосистем типа GCM», опубликованной в 2016 г. в № 2 (32) Вашего журнала, допущена ошибка. Она содержится в последнем абзаце доказательства утверждения 4: «Так как $q_1 + q_2 = q$, $q_1 \leqslant q - 1$ и функция $q_1(q_1 + 1)(1 - q_1)$ принимает максимальное значение при $q_1 = q - 1$, получаем отсюда, что вероятность успеха атаки не превосходит $\varepsilon q(q - 1)/2$, что и требуется доказать». Во-первых, вместо функции $q_1(q_1 + 1)(1 - q_1)$ в этом утверждении должна быть функция $q_1(q_1 + 1)(q - q_1)$. Во-вторых, оценка $\varepsilon q(q - 1)/2$ неверна и её следует заменить оценкой $\varepsilon(2q + 3)q^2/27$, которая достигается не при $q_1 = q - 1$, а при $q_1 = 2q/3$.

В связи с этим утверждение 4 и теорема 2 (которая использует это утверждение) должны быть сформулированы в следующем виде.

Утверждение 4. Пусть G — это εU-семейство функций. Тогда при использовании не более чем q запросов к оракулу проверки метки и к оракулу генерации метки система $FH[G]$ является $\varepsilon(2q + 3)q^2/27$-стойкой.

Теорема 2. Пусть $\mathcal{C}$ — противник, имеющий преимущество $\mathcal{C}_{\text{GCM'}}$ в атаке различения семейства функций, реализуемого GCM', или в активной атаке против GCM', при числе запросов к оракулам, не превосходящем q. Пусть для каждого запроса (iv, A, P) выполняются условия $l(A) + l(C) \leqslant l$ и $l(iv) = n - 32$. Тогда существует различитель $\mathcal{B}$ базового шифра E, имеющий преимущество $\mathcal{B}_E$, где

$$\mathcal{C}_{\text{GCM'}} \leqslant \mathcal{B}_E + \frac{1}{27}\left\lceil \frac{l}{n} + 1 \right\rceil q^2(2q + 3)/2^\tau + q(q + 1)/2^{n+1}.$$

Требует также исправления приведённый в конце статьи числовой пример. В нём следует заменить число 2^{32} на 2^{24} и число $1{,}1 \cdot 10^{-8}$ на $4{,}42 \cdot 10^{-8}$.

Приношу свои извинения читателям и редакции журнала.

А. Ю. Зубов