Homework 4

Ασημάκης Κύδρος
ΑΕΜ: 3881
asimakis@csd.auth.gr

Μάρτιος 2023

1 Έστω οι boolean συναρτήσεις $f, g : \mathbb{F}_2^n \to \{0,1\}$. Ονομάζουμε *correlation coefficient* το

$$C(f,g) = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})}$$

Υπολογίστε το $C(f,g)$ αν $F, g : \mathbb{F}_2^3 \to \{0,1\}, f = x_1x_2 \oplus x_3, g = x_1 \oplus x_3$.

Αρχικά παρατηρούμε πως

$f(x) \oplus g(x) = x_1x_2 \oplus x_3 \oplus x_1 \oplus x_3 \Rightarrow f(x) \oplus g(x) = x_1x_2 \oplus x_1$

Επομένως μπορούμε να ξαναγράψουμε την σχέση ως:

$$C(f,g) = \frac{1}{8} \sum_{\mathbf{x} \in \mathbb{F}_2^3} (-1)^{x_1x_2 \oplus x_1}$$

Υπολογίζοντας το εκθετικό $(-1)^{x_1x_2 \oplus x_1}$ για κάθε δυνατή τιμή του $\mathbb{F}_2^3$ έχουμε:

$(x_1x_2x_3)$	$x_1x_2 \oplus x_1$	$(-1)^{x_1x_2 \oplus x_1}$
000	0	1
001	0	1
010	0	1
011	0	1
100	1	-1
101	1	-1
110	0	1
111	0	1

Η τελευταία στήλη δίνει άθροισμα 4. Επομένως

$$C(f, g) = \frac{1}{8} \cdot 4 = \frac{1}{2}$$

Υλοποιώντας την παραπάνω λύση σε python επιβεβαιώνουμε το αποτέλεσμα: task 1.py

2 Έστω το S-κιβώτιο $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ της σελίδας 46 των διαφανειών.

Ονομάζουμε *Differential Uniformity* το

$$Diff(S) = \max_{\mathbf{x}\in\mathbb{F}_2^n-\{0\},\mathbf{y}\in\mathbb{F}_2^m} |\{\mathbf{z} \in \mathbb{F}_2^n \ni S(\mathbf{z}\oplus\mathbf{x})\oplus S(\mathbf{z}) = \mathbf{y}\}|$$

Υπολογίστε το $Diff(S)$.

Η λύση δίνεται από το task 2.py. Ουσιαστικά τρέχουμε την σύγκριση $S(\mathbf{z}\oplus\mathbf{x})\oplus S(\mathbf{z}) = \mathbf{y}$ για όλα τα $\mathbf{z}$ του $\mathbb{F}_2^6$ για κάθε ζεύγος $(\mathbf{x}, \mathbf{y})$ του $\mathbb{F}_2^6 - \{0\} \times \mathbb{F}_2^4$ και κρατάμε σε μετρητή το πλήθος των $\mathbf{z}$ που την ικανοποιούν. Ο μέγιστος μεταξύ αυτών των μετρητών δίνει τη λύση, που στη προκειμένη περίπτωση βγαίνει

$$Diff(S) = 16$$

3 Extra: Έστω το παίγνιο - απόδειξη μη σημασιολογικής ασφάλειας του ECB με CPA της σελίδας 82 των διαφανειών. Γιατί αποτυγχάνει η επίθεση της Eve αν αντί του ECB χρησιμοποιηθεί CBC-mode?

Η επίθεση της Eve στηρίζεται στο ότι γνωρίζει την κρυπτογράφηση του M από πριν, καθώς το διαλέγει η ίδια και η Alice της στέλνει το αντίστοιχο C.
Επομένως, εφόσον ο ECB κάνει κρυπτογράφηση κάθε block ανεξάρτητα, βλέποντας το πρώτο block του C[b] μπορεί να καταλάβει αν αντιστοιχεί στο M και επομένως να αποφανθεί για το b.

Στον CBC-mode, πριν την κρυπτογράφηση κάθε αρχικού block γίνεται bit-wise xor του block-plaintext με ένα **τυχαίο** διάνυσμα IV. Επομένως η Eve **δεν** έχει πλέον την κρυπτογράφηση του M, και άρα δεν μπορεί να αποφανθεί για το b με τον προηγούμενο τρόπο.