A Classical Introduction to Cryptography Exercise Book: Errata Page

Thomas Baignères, Pascal Junod, Yi Lu, Jean Monnerat, Serge Vaudenay
http://www.intro-to-crypto.info

October 26, 2007

If you find a mistake in the book, please report it to thomas.baigneres@epfl.ch.

1 Prehistory of Cryptography

p. 8, Solution 1. In question 4, diagrams (a) and (c) *do* represent a surjective function.

2 Conventional Cryptography

p. 37, Solution 5. In question 1(a), one should read 2^{112}2DES and 2^{111}2DES for the worst-case and the average case repspectively.

p. 38, Solution 6. In the second question, the probability that a given plaintext P is mapped on a given ciphertext C through the uniformly distributed random permutation C^* should be expanded as follows:

$$\begin{aligned}\Pr[\mathsf{C}^*(P) = C] &= \sum_{\mathsf{C}^*} \mathbf{1}_{\mathsf{c}(P)=C} \Pr[\mathsf{C}^* = \mathsf{c}] \\ &= \frac{1}{(2^{64})!} \sum_{\mathsf{c}} \mathbf{1}_{\mathsf{c}(P)=C}\end{aligned}$$

p. 41, Solution 7. The solution of question 7 is completely wrong, and solving it in a proper way is more complicated than we first thought it was. It is true that

$$u_4 = u'_4 \text{ and } v_4 = v'_4 \Rightarrow y_{\mathrm{L}} = y'_{\mathrm{L}}$$

but the converse is not necessarily true. We thus need to evaluate the probability that $u_4 = u'_4$ and $v_4 = v'_4$ when $y_{\mathrm{L}} = y'_{\mathrm{L}}$.

As a preliminary to the solution of this question, consider the building block shown on Figure 1. We consider a uniformly distributed random permutation $\mathsf{C}^* : \{0,1\}^\ell \to \{0,1\}^\ell$ and wonder about the

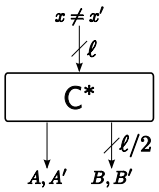

Figure 1: Computing the probability of a collision on half the output of a uniformly distributed random permutation.

probability that the right-most (or left-most) $\ell/2$ bits of $\mathsf{C}^*(x)$ and of $\mathsf{C}^*(x')$ collide when $x \neq x'$. Using

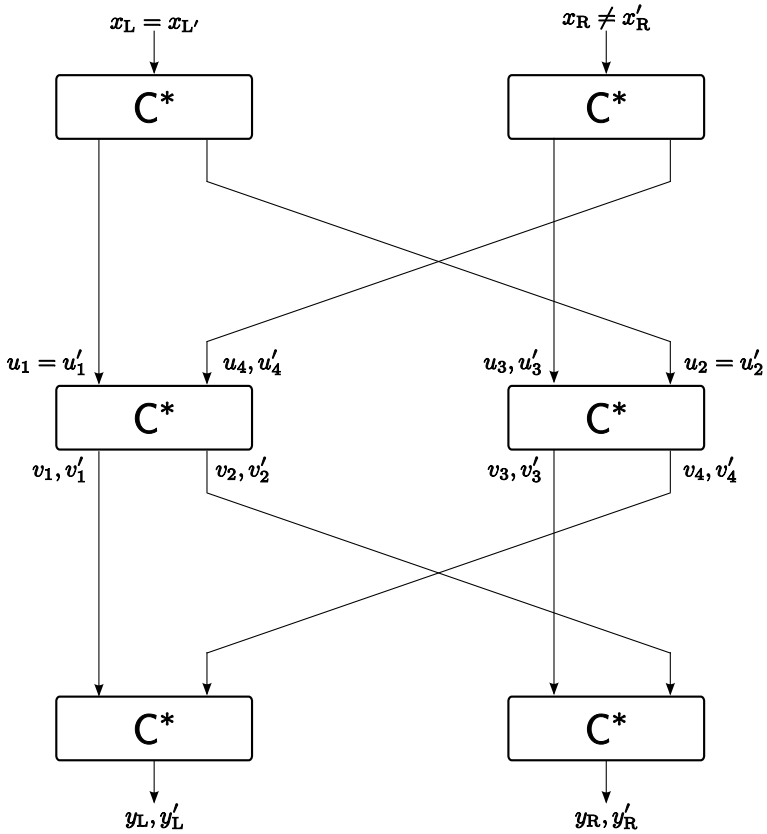

Figure 2: Computing $\Pr[\mathsf{icol}|y_L = y'_L]$

the notations of Figure 1 we have

$$\begin{aligned}\Pr[B = B'] &= \Pr[B = B'|A = A'] \cdot \Pr[A = A'] + \Pr[B = B'|A \neq A'] \cdot \Pr[A \neq A'] \\ &= 0 \cdot \Pr[A = A'] + 2^{-\ell/2} \cdot (1 - \Pr[A = A']).\end{aligned}$$

By symmetry, $\Pr[A = A'] = \Pr[B = B']$, so that the previous equation leads to

$$\Pr[A = A'] = \Pr[B = B'] = \frac{2^{-\ell/2}}{1 + 2^{-\ell/2}}. \tag{1}$$

In the following, we simply denote this probability by p.

We now consider the main problem, namely to compute $\Pr[u_4 = u'_4, v_4 = v'_4|y_L = y'_L]$ (see Figure 2). Denoting icol (for internal collision) the event $u_4 = u'_4, v_4 = v'_4$ we have

$$\Pr[\mathsf{icol}|y_L = y'_L] = \Pr[y_L = y'_L|\mathsf{icol}] \cdot \frac{\Pr[\mathsf{icol}]}{\Pr[y_L = y'_L]} = \frac{\Pr[\mathsf{icol}]}{\Pr[y_L = y'_L]}. \tag{2}$$

Using (1) we first have

$$\begin{aligned}\Pr[\mathsf{icol}] &= \Pr[\mathsf{icol}|u_3 = u'_3] \Pr[u_3 = u'_3] + \Pr[\mathsf{icol}|u_3 \neq u'_3] \Pr[u_3 \neq u'_3] \\ &= 0 \cdot p + \Pr[\mathsf{icol}|u_3 \neq u'_3] \cdot (1 - p).\end{aligned}$$

When $u_3 \neq u_3$, the two events $u_4 = u'_4$ and $v_4 = v'_4$ become independent (using the independence of the random permutations). Therefore, using (1) again,

$$\Pr[\mathsf{icol}] = \Pr[u_4 = u'_4|u_3 \neq u'_3] \cdot \Pr[v_4 = v'_4|u_3 \neq u'_3] \cdot (1 - p) = 2^{-\ell/2} \cdot p \cdot (1 - p). \tag{3}$$

We still need to compute $\Pr[y_{\mathrm{L}} = y'_{\mathrm{L}}]$. We have

$$\begin{aligned}
\Pr[y_{\mathrm{L}} = y'_{\mathrm{L}}] &= \Pr[v_1 = v'_1, v_4 = v'_4] \\
&= \Pr[v_1 = v'_1, v_4 = v'_4 | u_3 = u'_3, u_4 = u'_4] \cdot \Pr[u_3 = u'_3, u_4 = u'_4] + \\
&\quad \Pr[v_1 = v'_1, v_4 = v'_4 | u_3 = u'_3, u_4 \neq u'_4] \cdot \Pr[u_3 = u'_3, u_4 \neq u'_4] + \\
&\quad \Pr[v_1 = v'_1, v_4 = v'_4 | u_3 \neq u'_3, u_4 = u'_4] \cdot \Pr[u_3 \neq u'_3, u_4 = u'_4] + \\
&\quad \Pr[v_1 = v'_1, v_4 = v'_4 | u_3 \neq u'_3, u_4 \neq u'_4] \cdot \Pr[u_3 \neq u'_3, u_4 \neq u'_4] \\
&= 1 \cdot 0 + p \cdot p + p \cdot p + p2 \cdot (1 - 2 \cdot p) = 3 \cdot p2 - 2 \cdot p3.
\end{aligned}$$

From (2), (3) and the last equation, we finally obtain that

$$\Pr[\mathsf{icol} | y_{\mathrm{L}} = y'_{\mathrm{L}}] = \frac{1}{3 - 2 \cdot p}. \tag{4}$$

As $p \ll 1$, we conclude that $\Pr[\mathsf{icol} | y_{\mathrm{L}} = y'_{\mathrm{L}}] \approx \frac{1}{3}$, so that there is a non-negligible probability to have an internal collision when the event $y_{\mathrm{L}} = y'_{\mathrm{L}}$ is detected.

In the rest of solution given in the book it is assumed that $\Pr[\mathsf{icol} | y_{\mathrm{L}} = y'_{\mathrm{L}}] = 1$. This is wrong as we have just seen that this probability is close to $\frac{1}{3}$. Nevertheless, this just means that the attack suggested works with a probability $\frac{1}{3}$ (or, in other words, that running the attack 3 times in average should be enough to get one successful).

3 Dedicated Conventional Primitives

p. 71, Solution 4. In the third question, one should read "Clearly, they all produce [...]" instead of "Clearly, the all produce [...]".
p. 73, Solution 4. In the eighth question, one should read "with a probability $e^{-\lambda}$" instead of "with a probability e^{λ}".

4 Conventional Security Analysis

p. 86, Exercise 7. The second of the three boolean functions is not used in MD4İt is actually part of MD5 which also uses a fourth function.
p. 109, Solution 8. On Figure 4.9, ω^{-1} is wrong: the inputs should be swapped before the xor.

5 Security Protocols with Conventional Cryptography

Nothing yet.

6 Algorithmic Algebra

p. 147, Solution 5. In solution 3, one should read "the kernel is trivial, i.e., is equal to $\{1\}$".

7 Algorithmic Number Theory

p. 170, Solution 5. The number of prime numbers smaller than some integer n is $\Omega\left(\frac{n}{\log n}\right)$ and not $\Omega\left(\frac{\log n}{n}\right)$ as written in the solution.

8 Elements of Complexity Theory

Nothing yet.

9 Public Key Cryptography

Nothing yet.

10 Digital Signatures

Nothing yet.

11 Cryptographic Protocols

Nothing yet.

12 From Cryptography to Communication Security

p. 246, Solution 5. In the answer of the second question one should read $P' = M' \| Q'$ instead of $P' = M' \| Q$.

References

p. 250, Reference [17]. There is a typo in the name of the first author. The correct name is P. Flajolet.