Cryptographic Protocol Exercise 2

Deadline: 30.12.2010

1 Evaluate a Yao's circuit

- First, read the circuit below and tell what is the functionality of the circuit.
- All the encryption is used as 128 bits key AES. Evaluate the circuit and submit the output you got.
- The correct keys are always begin with 00000000_x.

1.1 Input Nodes Keys

In HEX format:

The key for the input node $x0$ is 00000000 9602D5D9 E6147984 2E742914
The key for the input node $x1$ is 00000000 E47628B1 4CAA7DB3 E2FAADE9
The key for the input node $y0$ is 00000000 098E8321 A057B69F 95B417E5
The key for the input node $y1$ is 00000000 72FE3D95 98DB9989 39E3ACAB

1.2 Output Nodes Keys

In HEX format:

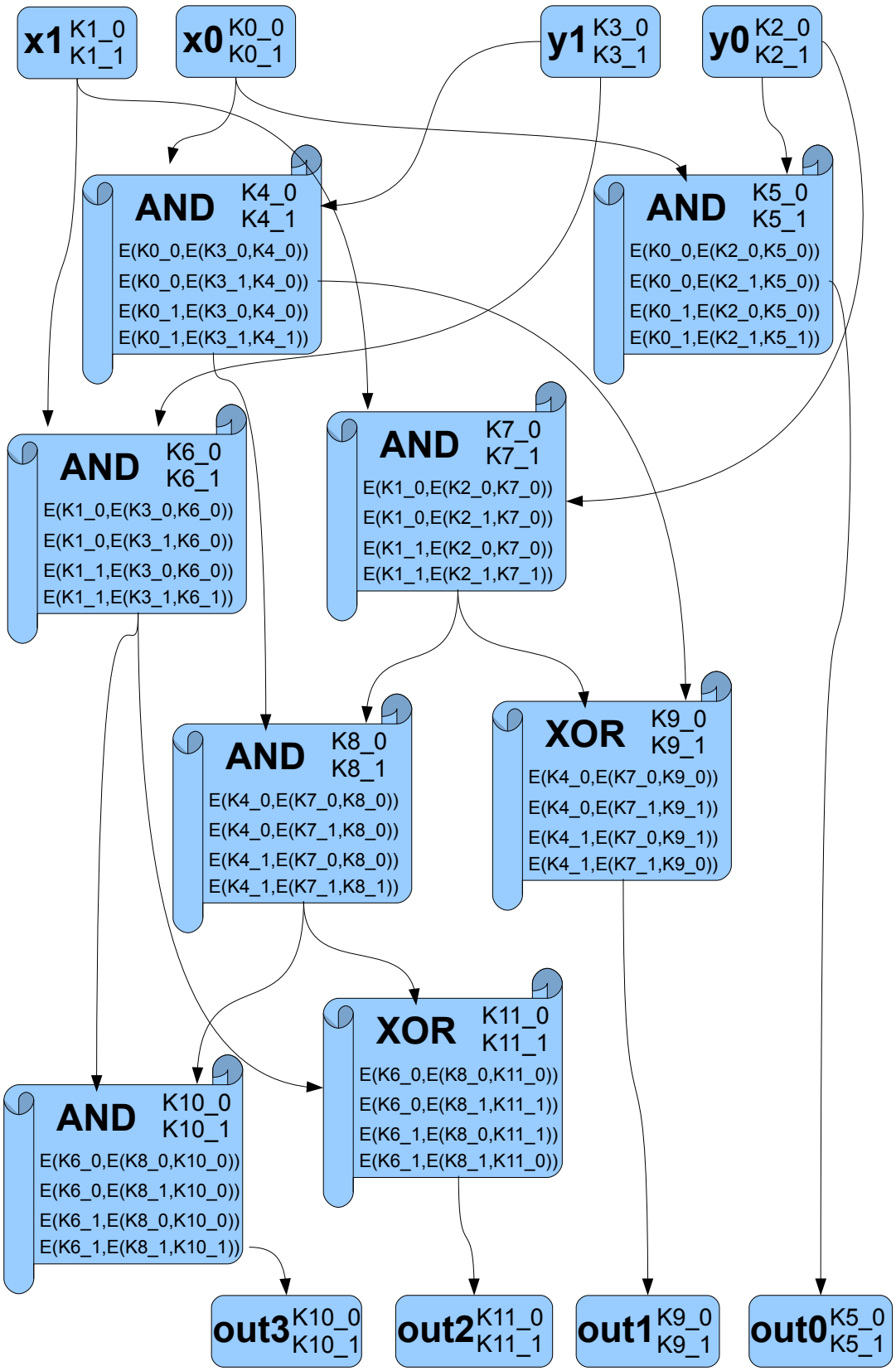
K5 that indicate 0: 00000000 A0234E43 BE043927 F6DCE2A0
K5 that indicate 1: 00000000 DE5E1E6C E34DA8F8 E4F74D1F
K9 that indicate 0: 00000000 19EBBCEC CD99209C 2F657572
K9 that indicate 1: 00000000 736BDE7F 8EE29E65 0836EE03
K10 that indicate 0: 00000000 4592BC38 A533F4A3 DD56A3CF
K10 that indicate 1: 00000000 0D0D4E96 97A0DFF1 3ABC9D04
K11 that indicate 0: 00000000 E79F51FB 5CFFB87D 36A9CD8F
K11 that indicate 1: 00000000 EAE139C5 D3E1A228 E3B86729

1.3 Internal Nodes

In HEX format:

- 4 Ciphertexts for Node of K4:
  - 632DEC83 A244FD87 1C1FFB6B 12649644
  - 06633B38 99487896 E1B026B4 9CF13276
  - 770798B9 D8328CA1 B2E70F9C 606F33D9
  - 520CD40E 5CF0BC2D 23FF4F5D CA6F3F85

- 4 Ciphertexts for Node of K5:
  - E24FA282 4D5CF62D 22012EC2 F37E58E4
  - 47677296 48BF68E1 782158BE 84D1407B
  - 63E5C714 61A7712F 7D330283 3C2AD873
  - 6BD80C3E DA072C5D FCE6A59A F42B7DDF
- 4 Ciphertexts for Node of K6:
  - 1052C258 6F4F8C71 779B5503 3678BF5D
  - 2E620151 DD2A526D A905D8A6 09808F26
  - 177DF36E C0627FEA D977B608 E593BDB8
  - 95449076 5E7E7C9D C1F00E47 C2265C65
- 4 Ciphertexts for Node of K7:
  - BA4FCF6B 0B73EC28 9C986FC5 13DD2DD5
  - 74F460A5 02D4E1E3 9F786576 493F2D14
  - 7EFA8636 E6FF3B5A A4A54C19 CE987364
  - 562D5E49 C692996E D5C14FDB 67DC079D
- 4 Ciphertexts for Node of K8:
  - 6259A9CD A5698402 B0C2D99A 85CC7B1D
  - AE0C4897 F5453DCD 373D074A DDCC2239
  - 457B6C39 E6553C95 6E78236C 2DEC3B15
  - 120F631B 7FCB35E5 CD414998 82B30BD0
- 4 Ciphertexts for Node of K9:
  - 9352FA0D 84A52B09 9D2C48E9 971404F3
  - 3969F25D 864B7AD5 5F585D89 5B5730BB
  - 7EC47474 FC526057 77B6676B 8E3BCD77
  - 4EAED16A F6750999 55A9A541 C3C2311B
- 4 Ciphertexts for Node of K10:
  - EB66BA6C 5A9394EB 9CC9FB89 A6BBE1B9
  - 4DA0C719 3762FD07 A87C21C0 45BFD5A4
  - 788127FE C8F52A4B 41DA32C5 43BE4D4E
  - 7DE769BA DF06FDE0 59AADFB6 96C12CB1
- 4 Ciphertexts for Node of K11:
  - 26FF462C AA6A6FA0 3F5DCAA4 1D537902
  - 084B3FBF 9F8662B4 B6ACB1A4 C98EA98C
  - C654662F 6A3D191F 6000DA3A 8C05F56C
  - D63A6B87 CC6799E4 4714A41C AEE0E103


x1 K1_0 K1_1
x0 K0_0 K0_1
y1 K3_0 K3_1
y0 K2_0 K2_1
AND K4_0 K4_1
E(K0_0,E(K3_0,K4_0))
E(K0_0,E(K3_1,K4_0))
E(K0_1,E(K3_0,K4_0))
E(K0_1,E(K3_1,K4_1))
AND K5_0 K5_1
E(K0_0,E(K2_0,K5_0))
E(K0_0,E(K2_1,K5_0))
E(K0_1,E(K2_0,K5_0))
E(K0_1,E(K2_1,K5_1))
AND K6_0 K6_1
E(K1_0,E(K3_0,K6_0))
E(K1_0,E(K3_1,K6_0))
E(K1_1,E(K3_0,K6_0))
E(K1_1,E(K3_1,K6_1))
AND K7_0 K7_1
E(K1_0,E(K2_0,K7_0))
E(K1_0,E(K2_1,K7_0))
E(K1_1,E(K2_0,K7_0))
E(K1_1,E(K2_1,K7_1))
AND K8_0 K8_1
E(K4_0,E(K7_0,K8_0))
E(K4_0,E(K7_1,K8_0))
E(K4_1,E(K7_0,K8_0))
E(K4_1,E(K7_1,K8_1))
XOR K9_0 K9_1
E(K4_0,E(K7_0,K9_0))
E(K4_0,E(K7_1,K9_1))
E(K4_1,E(K7_0,K9_1))
E(K4_1,E(K7_1,K9_0))
XOR K11_0 K11_1
E(K6_0,E(K8_0,K11_0))
E(K6_0,E(K8_1,K11_1))
E(K6_1,E(K8_0,K11_1))
E(K6_1,E(K8_1,K11_0))
AND K10_0 K10_1
E(K6_0,E(K8_0,K10_0))
E(K6_0,E(K8_1,K10_0))
E(K6_1,E(K8_0,K10_0))
E(K6_1,E(K8_1,K10_1))
out3 K10_0 K10_1
out2 K11_0 K11_1
out1 K9_0 K9_1
out0 K5_0 K5_1