УДК 621.9.048.7

СПОСОБ ФОРМИРОВАНИЯ ОБЩЕГО КРИПТОГРАФИЧЕСКОГО КЛЮЧА ПУТЕМ СОГЛАСОВАНИЯ СЛАБО СОВПАДАЮЩИХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ЕГО УЯЗВИМОСТИ

Пивоваров В.Л., Голиков В.Ф.

БНТУ, Минск, Беларусь, vadim.pif@gmail.com

В работе [1] и патенте [2] предложен способ формирования идентичных бинарных последовательностей (БП) без использования односторонних функций, который может быть использован для решения задачи распределения ключей криптографической системы между двумя абонентами, имеющими незащищенный от прослушивания канал связи и не обладающими общим секретом.

Его алгоритм заключается в следующем:

1. Абонент *A* генерирует базовую бинарную последовательность (БП) X_0 длиной n и посылает ее абоненту *B*.

2. Затем абоненты *A* и *B* задаются количеством изменяемых битов r_A, r_B где $0 \le r_A \le n, 0 \le r_B \le n$ и генерируют независимо друг от друга случайные секретные последовательности чисел соответственно S_A и S_B, при этом $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}, S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$ где $S_i^a \in \{1,2,...,n\}$, $S_i^b \in \{1,2,...,n\}$, причем $s_i^a \neq s_j^a$, $i, j = 1,2, ..., r_A$ для S_A, $s_i^b \neq s_j^b$, $i, j = 1,2, ..., r_B$ для S_B.

3. Далее абоненты *A* и *B* в соответствии с полученными номерами бит S_i^a и S_i^b инвертируют эти биты в X_0 и получают последовательности X_A и X_B.

После того, как сформированы последовательности X_A и X_B абоненты *A* и *B* проделывают следующие операции:

4. Согласованно разбивают свои последовательности X_A и X_B на пары бит либо по порядку, либо случайным образом.

5. Вычисляют четности каждой пары бит и обмениваются ими.

6. Сравнивая четности пар своей БП с полученными четностями, находят пары с несовпадающими четностями и удаляют их из последовательностей.

7. В оставшихся парах удаляют по одному биту по договоренности.

8. Из оставшихся бит, количество которых n_1 ,образуют промежуточные последовательности X_{A1} и X_{B1} путем сдвига всех бит влево до полного заполнения образовавшихся после удаления пар и бит вакансий.

9. Повторяют п.4-8 назначенное число раз до получения X_{AN} и X_{BN}.

Полученные последовательности X_{AN} и X_{BN} и будут формировать криптографический ключ.

В работе [1] также проводится исследование для выбора оптимальных значений r_A и r_B для обеспечения доли несовпадающих битов близкой к 50%. Так, для n = 100000 оптимальными значениями будут r_A = 43800, r_B = 38700 либо r_A = 38700, r_B = 43800. Такие значения r_A, r_B обеспечат долю несовпадающих битов примерно 0,48. И поскольку вероятности, с которыми каждый бит итоговой последовательности равен или противоположен соответствующему биту исходной последовательности отличаются от 0,5, то это свойство может быть использовано для криптоанализа.

Будем считать, что все процедуры формирования итоговой последовательности известны криптоаналитику, также как известна вся информация, циркулирующая по открытому каналу связи.

На этапе формирования исходных БП криптоаналитику известна базовая последовательность X_0. На этапе удаления несовпадающих битов известны номера бит исходной последовательности, вошедших в ту или иную пару, четности пар бит абонентов *A* и *B*, номера

бит в парах, остающихся в БП после сравнения четностей, номера бит, удаленных из каждой не удаленной пары. Таким образом, криптоаналитику, пассивно наблюдающему процесс формирования идентичных БП, известны номера бит X_0, вошедших в итоговую БП, кроме того известны их новые позиции в этой последовательности. Однако значения этих бит криптоаналитику неизвестны, поскольку часть их подвергалась инвертированию. Доля инвертированных битов зависит от выбранных значений r_A и r_B. При значениях r_A и r_B, обеспечивающих долю несовпадающих битов примерно 0,48, доля инвертированных битов равна в среднем примерно 0,38 и является случайной величиной. Следовательно, в итоговой последовательности в каждой сотне битов содержится 38 бита, значения которых противоположны этим же битам в X_0, и 62 битов, значения которых равны значениям этих же биты в X_0. Однако позиции совпадающих и противоположных битов криптоаналитику неизвестны, в то время как абонентам A и B известны и позиции, поскольку каждый из абонентов знает номера бит в X_0, которые он инвертировал. Таким образом, для раскрытия итоговой последовательности криптоаналитику требуется определить какие биты в итоговой последовательности инвертированы, относительно исходной, а какие нет. Для этого как раз и предлагается использовать свойство, что вероятности, с которыми каждый бит итоговой последовательности равен или противоположен соответствующему биту исходной последовательности отличаются от 0,5.

Воспользуемся формулой условной вероятности Байеса.

$$P(\mathrm{H}_i \mid \mathrm{A}) = \frac{P(\mathrm{H}_i)\,\mathrm{P}(\mathrm{A} \mid \mathrm{H}_i)}{\sum_{i=1}^{N} P(\mathrm{H}_i) P(A \mid H_i)} \qquad (1)$$

Пусть X_0 – базовая БП длины n, X_A и X_B –сформированные БП на основе X_0, r_A, r_B – количество инвертируемых бит для X_A и X_B соответственно, C_i – значения четности пары бит для последовательности X_A (0 либо 1).

Тогда в формуле (1):

H_1 – событие, оба бита в первой паре последовательности X_A были инвертированы относительно базовой последовательности X_0.

H_2 – событие, первый бит в первой паре последовательности X_A был инвертирован, второй остался таким же относительно базовой последовательности X_0.

H_3 – событие, второй бит в первой паре последовательности X_A был инвертирован, первый остался таким же относительно базовой последовательности X_0.

H_4 – событие, оба бита в первой паре последовательности X_A остались такими же, относительно базовой последовательности X_0.

Получаем:

$P(H_1) = p * p;$

$P(H_2) = p * (1 – p);$

$P(H_3) = (1 – p) * p;$

$P(H_4) = (1 – p) * (1 - p),$

где $p = \frac{r_A}{n}$ – вероятность того, что какой-либо бит последовательности X_A был инвертирован.

$A_1|H_1$ – событие, четность пары бит равна 0, когда оба бита в первой паре последовательности X_A были инвертированы относительно базовой последовательности X_0.

$A_1|H_2$ – событие, четность пары бит равна 0, когда первый бит в первой паре последовательности X_A был инвертирован, второй остался таким же относительно базовой последовательности X_0.

$A_1|H_3$ – событие, четность пары бит равна 0, когда второй бит в первой паре последовательности X_A был инвертирован, первый остался таким же относительно базовой последовательности X_0.

$A_1|H_4$ – событие, четность пары бит равна 0, когда оба бита в первой паре последовательности X_A остались такими же, относительно базовой последовательности X_0.

$A_2|H_1$ – событие, четность пары бит равна 1, когда оба бита в первой паре последовательности X_A были инвертированы относительно базовой последовательности X_0.

$A_2|H_2$ – событие, четность пары бит равна 1, когда первый бит в первой паре последовательности X_A был инвертирован, второй остался таким же относительно базовой последовательности X_0.

$A_2|H_3$ – событие, четность пары бит равна 1, когда второй бит в первой паре последовательности X_A был инвертирован, первый остался таким же относительно базовой последовательности X_0.

$A_2|H_4$ – событие, четность пары бит равна 1, когда оба бита в первой паре последовательности X_A остались такими же, относительно базовой последовательности X_0.

Получаем:

для пары бит со значениями 00 либо 11 в исходной БП

$P(A_1|H_1) = 1$ $P(A_2|H_1) = 0$

$P(A_1|H_1) = 0$ $P(A_2|H_1) = 1$

$P(A_1|H_1) = 0$ $P(A_2|H_1) = 1$

$P(A_1|H_1) = 1$ $P(A_2|H_1) = 0$

для пары бит со значениями 01 либо 10 в исходной БП

$P(A_1|H_1) = 0$ $P(A_2|H_1) = 1$

$P(A_1|H_1) = 1$ $P(A_2|H_1) = 0$

$P(A_1|H_1) = 1$ $P(A_2|H_1) = 0$

$P(A_1|H_1) = 0$ $P(A_2|H_1) = 1$

Зная эти вероятности и значения C_i по формуле (1) можно вычислить для каждой пары бит значения $P(H_1|A)$ – более точную вероятность, с которой биты последовательности X_A были инвертированы относительно базовой последовательности X_0.

Проводя аналогичные вычисления на каждой итерации работы алгоритма формирования идентичных бинарных последовательностей (п.4-8), используя вместо C_i уже новые значения, полученные из последовательностей X_{A1}, X_{A2} и т.д. и вместо p, значение $P(H_1|A)$, полученное на предыдущем шаге, можно значительно уточнить вероятность, с которой биты в итоговой последовательности были инвертированы, относительно битов в исходной последовательности на тех же позициях, тем самым понизить конфиденциальность итоговой последовательности.

Рассмотрим этот метод на конкретном примере. Пусть абонент A сформировал последовательность

X_0 = [1(1) 1(2) 0(3) 0(4) 0(5) 0(6) 0(7) 0(8) 0(9) 1(10) 1(11) 0(12) 1(13) 0(14) 0(15) 0(16) 1(17) 1(18) 0(19) 1(20) 1(21) 0(22) 0(23) 0(24) 0(25) 1(26) 1(27) 1(28) 1(29) 1(30) 1(31) 1(32) 1(33) 1(34) 1(35) 1(36) 0(37) 0(38) 0(39) 1(40) 1(41) 1(42) 0(43) 1(44) 0(45) 1(46) 1(47) 0(48) 0(49) 0(50) 0(51) 0(52) 1(53) 1(54) 0(55) 0(56) 1(57) 1(58) 0(59) 1(60) 1(61) 1(62) 1(63) 1(64) 1(65) 1(66) 1(67) 0(68) 1(69) 1(70) 1(71) 0(72) 0(73) 0(74) 0(75) 0(76) 1(77) 1(78) 1(79) 0(80) 1(81) 0(82) 0(83) 1(84) 0(85) 1(86) 0(87) 1(88) 0(89) 1(90) 0(91) 0(92) 1(93) 0(94) 0(95) 1(96) 1(97) 1(98) 0(99) 0(100) 1(101) 1(102) 0(103) 0(104) 1(105) 1(106) 0(107) 1(108) 0(109) 0(110) 1(111) 1(112) 0(113) 0(114) 1(115) 0(116) 1(117) 0(118) 1(119) 0(120) 0(121) 0(122) 1(123) 0(124) 1(125) 0(126) 1(127) 1(128) 1(129) 0(130) 0(131) 0(132) 1(133) 0(134) 0(135) 1(136) 1(137) 1(138) 0(139) 0(140) 0(141) 0(142) 1(143) 1(144) 1(145) 1(146) 1(147) 0(148) 1(149) 0(150) 0(151) 0(152) 1(153) 1(154) 0(155) 1(156) 0(157) 1(158) 1(159) 0(160) 1(161) 1(162) 0(163) 0(164) 0(165) 1(166) 0(167) 1(168) 0(169) 0(170) 1(171) 1(172) 0(173) 1(174) 0(175) 0(176) 1(177) 0(178) 1(179) 0(180) 0(181) 1(182) 1(183) 1(184) 0(185) 1(186) 1(187) 1(188) 0(189) 0(190) 1(191) 1(192) 1(193) 1(194) 0(195) 1(196) 0(197) 0(198) 0(199) 0(200) 0(201) 1(202) 0(203) 0(204) 1(205) 1(206) 1(207) 0(208) 0(209) 0(210) 1(211) 0(212) 1(213) 1(214) 0(215) 0(216) 0(217) 0(218) 1(219) 1(220)] длиной 220 бит, r_A = 91, r_B = 84. После инвертирования бит абоненты получили следующие последовательности:

X_A = [0(1) 1(2) 0(3) 0(4) 0(5) 1(6) 0(7) 1(8) 0(9) 1(10) 1(11) 1(12) 1(13) 0(14) 1(15) 0(16) 1(17) 0(18) 0(19) 0(20) 0(21) 0(22) 1(23) 1(24) 1(25) 0(26) 1(27) 1(28) 0(29) 1(30) 0(31) 0(32) 1(33) 1(34) 1(35) 1(36) 0(37) 1(38) 0(39) 0(40) 0(41) 1(42) 0(43) 0(44) 0(45) 1(46) 0(47) 1(48) 0(49) 1(50) 1(51) 1(52) 1(53) 1(54) 1(55) 0(56) 1(57) 1(58) 0(59) 1(60) 1(61) 1(62) 1(63) 1(64) 1(65) 1(66) 1(67) 0(68) 0(69) 1(70) 0(71) 1(72) 0(73) 0(74) 1(75) 1(76) 1(77) 1(78) 1(79) 1(80) 1(81) 0(82) 0(83) 1(84) 0(85) 0(86) 0(87) 1(88) 0(89) 0(90) 0(91) 0(92) 1(93) 0(94) 0(95) 0(96) 1(97) 1(98) 0(99) 0(100) 1(101) 1(102) 0(103) 1(104) 0(105) 1(106) 1(107) 0(108) 0(109) 1(110) 1(111) 1(112) 1(113) 1(114) 1(115)

1(116) 1(117) 1(118) 0(119) 1(120) 0(121) 0(122) 0(123) 0(124) 0(125) 0(126) 1(127) 1(128) 1(129) 0(130) 1(131) 1(132) 1(133) 1(134) 0(135) 0(136) 1(137) 1(138) 0(139) 0(140) 1(141) 0(142) 1(143) 0(144) 1(145) 1(146) 0(147) 0(148) 1(149) 1(150) 1(151) 0(152) 0(153) 0(154) 0(155) 0(156) 1(157) 1(158) 1(159) 1(160) 0(161) 1(162) 0(163) 1(164) 0(165) 1(166) 0(167) 0(168) 1(169) 1(170) 0(171) 0(172) 0(173) 0(174) 0(175) 0(176) 0(177) 1(178) 0(179) 1(180) 1(181) 0(182) 1(183) 1(184) 0(185) 0(186) 0(187) 1(188) 0(189) 0(190) 0(191) 1(192) 0(193) 1(194) 1(195) 1(196) 0(197) 1(198) 0(199) 1(200) 0(201) 1(202) 1(203) 1(204) 1(205) 1(206) 0(207) 1(208) 0(209) 1(210) 1(211) 1(212) 0(213) 1(214) 0(215) 0(216) 0(217) 1(218) 0(219) 1(220)],

X_B = [0(1) 1(2) 0(3) 1(4) 1(5) 1(6) 0(7) 0(8) 1(9) 0(10) 1(11) 1(12) 1(13) 0(14) 1(15) 0(16) 1(17) 0(18) 0(19) 1(20) 1(21) 1(22) 1(23) 0(24) 0(25) 0(26) 1(27) 0(28) 1(29) 1(30) 1(31) 1(32) 1(33) 0(34) 1(35) 0(36) 0(37) 1(38) 0(39) 1(40) 1(41) 1(42) 0(43) 1(44) 1(45) 1(46) 1(47) 0(48) 0(49) 0(50) 1(51) 0(52) 1(53) 1(54) 1(55) 0(56) 0(57) 0(58) 1(59) 1(60) 0(61) 1(62) 0(63) 1(64) 0(65) 0(66) 1(67) 0(68) 0(69) 1(70) 0(71) 0(72) 0(73) 1(74) 0(75) 1(76) 0(77) 1(78) 0(79) 1(80) 0(81) 0(82) 1(83) 1(84) 1(85) 0(86) 0(87) 1(88) 0(89) 0(90) 1(91) 1(92) 1(93) 0(94) 0(95) 1(96) 1(97) 0(98) 1(99) 0(100) 1(101) 1(102) 0(103) 0(104) 1(105) 0(106) 1(107) 1(108) 1(109) 0(110) 0(111) 0(112) 1(113) 1(114) 1(115) 1(116) 0(117) 1(118) 1(119) 1(120) 0(121) 1(122) 0(123) 0(124) 1(125) 0(126) 0(127) 1(128) 0(129) 0(130) 1(131) 0(132) 1(133) 0(134) 0(135) 1(136) 0(137) 1(138) 0(139) 0(140) 1(141) 0(142) 1(143) 0(144) 1(145) 1(146) 1(147) 0(148) 1(149) 1(150) 1(151) 0(152) 1(153) 1(154) 1(155) 1(156) 0(157) 1(158) 1(159) 1(160) 1(161) 1(162) 0(163) 0(164) 1(165) 1(166) 0(167) 0(168) 0(169) 1(170) 1(171) 0(172) 1(173) 0(174) 0(175) 0(176) 1(177) 0(178) 1(179) 0(180) 0(181) 0(182) 0(183) 1(184) 1(185) 0(186) 0(187) 1(188) 1(189) 0(190) 1(191) 1(192) 1(193) 1(194) 0(195) 1(196) 0(197) 0(198) 0(199) 0(200) 0(201) 1(202) 1(203) 1(204) 1(205) 1(206) 0(207) 0(208) 0(209) 1(210) 1(211) 1(212) 1(213) 0(214) 0(215) 0(216) 0(217) 0(218) 0(219) 1(220)].

Для удобства каждый бит последовательностей X_0, X_A, X_B пронумеруем, биты в последовательностях будем разбивать на пары по порядку, а удалять из пары будем биты на первой позиции.

$$p = \frac{r_A}{n} = \frac{91}{220} = 0,41$$

Далее по формуле (1) вычислим значения $P(H_1|A)$, $P(H_2|A)$, $P(H_3|A)$, $P(H_4|A)$ для каждой пары бит последовательности X_A.

Зная значения p, C_i, $P(H_1|A)$, $P(H_2|A)$, $P(H_3|A)$, $P(H_4|A)$ легко можно получить вероятности того, что второй бит в каждой паре равен 1:

P = [0,5(2) 0,3322(4) 0,5(6) 0,5(8) 0,6677(10) 0,5(12) 0,3322(14) 0,5(16) 0,5(18) 0,5(20) 0,5(22) 0,3322(24) 0,6677(26) 0,6677(28) 0,5(30) 0,6677(32) 0,6677(34) 0,6677(36) 0,5(38) 0,5(40) 0,5(42) 0,5(44) 0,6677(46) 0,3322(48) 0,5(50) 0,3322(52) 0,6677(54) 0,5(56) 0,6677(58) 0,6677(60) 0,667723(62) 0,6677(64) 0,6677(66) 0,3322(68) 0,5(70) 0,3322(72) 0,3322(74) 0,3322(76) 0,6677(78) 0,5(80) 0,3322(82) 0,6677(84) 0,5(86) 0,6677(88) 0,5(90) 0,3322(92) 0,3322(94) 0,5(96) 0,6677(98) 0,3322(100) 0,6677(102) 0,5(104) 0,5(106) 0,6677(108) 0,5(110) 0,6677(112) 0,3322(114) 0,5(116) 0,5(118) 0,3322(120) 0,3322(122) 0,5(124) 0,5(126) 0,6677(128) 0,3322(130) 0,3322(132) 0,5(134) 0,5(136) 0,6677(138) 0,3322(140) 0,5(142) 0,5(144) 0,6677(146) 0,5(148) 0,5(150) 0,5(152) 0,6677(154) 0,5(156) 0,5(158) 0,5(160) 0,5(162) 0,5(164) 0,6677(166) 0,5(168) 0,3322(170) 0,6677(172) 0,5(174) 0,3322(176) 0,3322(178) 0,3322(180) 0,6677(182) 0,6677(184) 0,5(186) 0,5(188) 0,3322(190) 0,5(192) 0,5(194) 0,5(196) 0,5(198) 0,5(200) 0,6677(202) 0,3322(204) 0,6677(206) 0,3322(208) 0,5(210) 0,5(212) 0,5(214) 0,3322(216) 0,5(218) 0,5(220)]

Значения вычисляем только для вторых бит в каждой паре, т.к. первые биты на каждой итерации удаляются из последовательности.

Проделывая аналогичные вычисления на каждом шаге работы алгоритмы получаем следующие данные:

Шаг 1:

X_{A1} = [1(2) 1(10) 1(12) 0(14) 0(16) 0(18) 0(22) 0(32) 1(38) 1(48) 1(54) 0(56) 1(58) 1(66) 0(68) 1(70) 1(88) 0(90) 0(92) 0(94) 1(102) 1(106) 1(110) 1(112) 1(114) 1(116) 0(124) 0(140) 0(142) 0(144) 1(146) 1(150) 0(152) 0(154) 0(156) 1(160) 0(168) 0(176) 1(178) 1(180) 1(188) 1(202) 1(204) 1(206) 1(210) 1(212) 1(214) 0(216)]

X_{B1} = [1(2) 0(10) 1(12) 0(14) 0(16) 0(18) 1(22) 1(32) 1(38) 0(48) 1(54) 0(56) 0(58) 0(66) 0(68) 1(70) 1(88) 0(90) 1(92) 0(94) 1(102) 0(106) 0(110) 0(112) 1(114) 1(116) 0(124) 0(140) 0(142) 0(144) 1(146) 1(150) 0(152) 1(154) 1(156) 1(160) 0(168) 0(176) 0(178) 0(180) 1(188) 1(202) 1(204) 1(206) 1(210) 1(212) 0(214) 0(216)]

P_1 = [0,6677(10) 0,3322(14) 0,5(18) 0,6677(32) 0,3322(48) 0,3322(56) 0,8015(66) 0,6677(70) 0,3322(90) 0,1984(94) 0,6677(106) 0,6677(112) 0,3322(116) 0,3322(140) 0,5(144) 0,6677(150) 0,6677(154) 0,5(160) 0,3322(176) 0,1984(180) 0,6677(202) 0,5(206) 0,5(212) 0,3322(216)]

Шаг 2:

X_{A2} = [0(14) 0(18) 0(32) 0(56) 1(66) 1(70) 0(90) 1(112) 1(116) 0(140) 0(144) 1(150) 0(176) 1(180) 1(202) 1(206)]

X_{B2} = [0(14) 0(18) 1(32) 0(56) 0(66) 1(70) 0(90) 0(112) 1(116) 0(140) 0(144) 1(150) 0(176) 0(180) 1(202) 1(206)]

P_2 = [0,3322(18) 0,5(56) 0,8902(70) 0,8015(112) 0,5(140) 0,6677(150) 0,3322(180) 0,6677(206)]
Шаг 3:
X_{A3} = [0(18) 0(140) 1(150) 1(206)]
X_{B3} = [0(18) 0(140) 1(150) 1(206)]
P_3 = [0,1322(18) 0,5(140) 0,8677(150) 0,8015(206)]

Алгоритм произвел полную синхронизацию последовательностей за 3 такта. За эти 3 такта удалось сильно подкорректировать вероятности того, что какой-либо бит был инвертирован в итоговой последовательности. Таким образом, мы можем утверждать, что бит на позиции 1 в итоговой последовательности (бит 18 в базовой последовательности) с вероятностью 0,1322 равен 1, бит на позиции 2 в итоговой последовательности (бит 140 в базовой последовательности) с вероятностью 0,5 равен 1, бит на позиции 3 в итоговой последовательности (бит 150 в базовой последовательности) с вероятностью 0,8677 равен 1 и бит на позиции 4 в итоговой последовательности (бит 206 в базовой последовательности) с вероятностью 0,8015 равен 1. Для большинства бит удалось с высокой точностью определить их настоящее значение, однако есть биты, для которых вероятность того, что они равны 1 – 50%. Это происходит из-за того, что в случае, когда пара бит равна 00 или 11 и $C_i = 1$, вероятности $P(H_2|A)$ и $P(H_3|A)$ равны 0,5, а также когда пара бит равна 01 или 10 и $C_i = 0$, вероятности $P(H_2|A)$ и $P(H_3|A)$ равны 0,5.

Таким образом, можно сделать вывод, что предложенный алгоритм уточнения вероятностей итоговых значений позволяет с большой вероятностью раскрыть некоторые биты в итоговой последовательности, из-за чего способ формирования идентичных бинарных последовательностей без использования односторонних функций требует дополнительных условий для обеспечения конфиденциальности полученной секретной последовательности. Другой алгоритм формирования базовых последовательностей X_A и X_B, например, с использованием синхронизируемых нейронных сетей, является одним из способов решения данной проблемы.

ЛИТЕРАТУРА

1. Абдольванд Ф. Открытое формирование конфиденциальных идентичных бинарных последовательностей в задачах защиты информации. Кандидатская диссертация. Минск, 2012, 111с.

2. Голиков В.Ф. Способ распределения криптографического ключа между абонентами. Патент №17856, 2011.