УДК 621.391.25 (075.8)

ЭФФЕКТИВНОСТЬ УСТРАНЕНИЯ ОШИБОК В БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ПРИ РАЗНЕСЕННОМ ФОРМИРОВАНИИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

В.Ф. ГОЛИКОВ, Ф. АБДОЛЬВАНД

Белорусский национальный технический университет,
пр. Независимости, 65, Минск, 220013, Беларусь

Поступила в редакцию 29 июня 2010

Излагается процедура устранения несовпадений (ошибок) в разнесенных бинарных последовательностях при конфиденциальном формировании общего ключа для симметричных криптосистем.

Ключевые слова: бинарная последовательность, криптографический ключ, устранение ошибок, сохранение конфиденциальности.

Введение

Важной задачей, которую необходимо решать для обеспечения надежной работы симметричной криптосистемы, является задача формирования абонентами системы общего секретного ключа. Для ее решения уже длительное время с успехом используется алгоритм открытого распределения ключей Диффи–Хеллмана или аналогичные процедуры, базирующиеся на использовании односторонних функций. Однако развитие физики, электроники, математики и информатики сделало вполне реальным появление в ближайшем будущем квантового компьютера, одним из возможных применений которого является "взлом" традиционных односторонних функций с последующим вычислением общего ключа, формируемого по схеме Диффи–Хеллмана. В [1, 2] рассматриваются альтернативные способы формирования общего ключа без использования классических однонаправленных функций. Суть этих методов сводится к формированию у абонентов криптосистемы бинарных последовательностей, идентичность которых обеспечивается тем или иным способом. Независимо от способа обеспечения идентичности при этом возникает необходимость устранения различий (ошибок) последовательностей, процент которых зависит от выбранного способа формирования общего ключа.

Постановка задачи

Пусть стороны A и B формируют общую ключевую последовательность X_{AB} из своих предварительно сгенерированных последовательностей X_A и X_B ($X_A = \{0,1\}^n$, $X_B = \{0,1\}^n$, $X_{AB} = \{0,1\}^n$), где $n-$ длина последовательности в битах. Последовательности X_A и X_B имеют d несовпадающих бит (ошибок), $0 \le d \le n$. Процесс формирования X_{AB} сводится к обнаружению ошибок и их устранению. Для обнаружения ошибок стороны вынуждены обмениваться некоторой информацией о своих последовательностях по открытому каналу связи, потенциально прослушиваемому криптоаналитиком E, который перехватывая информацию о X_A и X_B, конструирует свою последовательность X_E, пытаясь приблизить ее мак-

симально к X_{AB}. Если обозначить информацию о X_A и X_B через $I(X_A)$ и $I(X_B)$, то процесс формирования X_{AB} можно представить как вычисление

$$X_{AB} = \Phi_i\{I(X_A), I(X_B)\} \quad \text{при} \quad H(X_{AB}) \geq H_{\min},$$

где Φ_i — итерационная процедура устранения ошибок; i — номер итерации; $H(X_{AB})$ — энтропия X_{AB}; $H_{\min}$ — минимально допустимая энтропия. Получить общее решение (1) не представляется возможным вследствие сложности и неформализуемости задачи. Целесообразно получить частные решения и оценить их эффективность.

Процедура устранения ошибок

Рассмотрим процесс обнаружения ошибочных бит. Пусть в последовательностях X_A и X_B имеется одно несовпадение $d = 1$. Для обнаружения ошибки в [3] предлагается метод половинного разбиения. A и B разбивают свои последовательности пополам и вычисляют четности каждой половины:

$$C_{A_l}^{(1)} = \sum_{j=1}^{\frac{n}{2}} a_j \pmod 2,\ C_{A_r}^{(1)} = \sum_{j=\frac{n}{2}+1}^{n} a_j \pmod 2,$$

$$C_{B_l}^{(1)} = \sum_{j=1}^{\frac{n}{2}} b_j \pmod 2,\ C_{B_r}^{(1)} = \sum_{j=\frac{n}{2}+1}^{n} b_j \pmod 2,$$

где $C_{A_l}^{(1)}, C_{A_r}^{(1)}, C_{B_l}^{(1)}, C_{B_r}^{(1)}$ — четности левой (правой) половин последовательностей $X_A(X_B)$ при первой итерации, равные $\{0,1\}$[1]. Сторона A высылает $C_{A_l}^{(1)}$ стороне B, которая сравнивает $C_{A_l}^{(1)}$ с $C_{B_l}^{(1)}$ и информирует A о результате сравнения. Если $C_{A_l}^{(1)} = C_{B_l}^{(1)}$, то делается вывод об отсутствии ошибки в l-половинах, в противном случае ошибка находится в l-половинах. Половины, в которых содержится ошибка, вновь разбиваются пополам и вновь вычисляются четности фрагментов:

$$C_{A_l}^{(2)} = \sum_{j \in Q_{A_l}^{(2)}} a_j \pmod 2,\ C_{A_r}^{(2)} = \sum_{j \in Q_{A_r}^{(2)}} a_j \pmod 2,$$

$$C_{B_l}^{(2)} = \sum_{j \in Q_{B_l}^{(2)}} b_j \pmod 2,\ C_{B_r}^{(2)} = \sum_{j \in Q_{B_r}^{(2)}} b_j \pmod 2,$$

где $Q_{A_l(r)}^{(2)}, Q_{B_l(r)}^{(2)}$ — множество номеров элементов, входящих во фрагмент последовательностей $X_A(X_B)$, четность которого вычисляется.

Сравнивая четности фрагментов, устанавливают, в каком из них содержится ошибка. Процедура разбиения и сравнения четностей продолжается до тех пор, пока длина фрагмента не станет равной двум битам. Дальнейшее разбиение бессмысленно, так как это приводит к оглашению каждого бита найденной пары и они становятся известными E.

Проанализируем потери конфиденциальности за счет оглашения четностей. Поскольку место нахождения ошибки случайно и заранее неизвестно, то потери конфиденциальности — величина случайная. Найдем оценки для минимальных и максимальных потерь. Минимальные потери имеют место при минимальном числе итераций, что соответствует процессу, когда сразу угадывается фрагмент, содержащий ошибку. Подсчитаем число необходимых итераций, обеспечивающих изменение длины фрагментов от n до 2. Пусть $n = 2(s+1)$, где $s = 2,3,4,\ldots,k$, тогда: $L^{(1)} = n/2,\ L^{(2)} = n/4,\ \ldots L^{(i)} = n/2^i,\ \ldots,\ L^{(k)} = n/2^k$. Так как должно быть

$L^{(k)}=2$, то $\frac{n}{2^k}=2$, откуда $k=\log(n,2)-1$. Например, если $n=16$, то $L^{(1)}=8, L^{(2)}=4,$ $L^{(3)}=2, k=3$. Таким образом, чтобы локализовать пару бит, содержащую ошибку, необходимо сделать 3 разбиения. Каждое разбиение сопровождается оглашением четностей двух фрагментов:

$C_{A_l}^{(1)}=(a_1+a_2+...+a_8) \bmod 2,\ C_{A_r}^{(1)}=(a_9+a_{10}+...+a_{16}) \bmod 2,$

$C_{B_l}^{(1)}=(b_1+b_2+...+b_8) \bmod 2,\ C_{B_r}^{(1)}=(b_9+b_{10}+...+b_{16}) \bmod 2,$

$C_{A_l}^{(2)}=(a_1+a_2+...+a_4) \bmod 2,\ C_{A_r}^{(2)}=(a_5+a_6+...+a_8) \bmod 2,$

$C_{B_l}^{(2)}=(b_1+b_2+...+b_4) \bmod 2,\ C_{B_r}^{(2)}=(b_5+b_6+...+b_8) \bmod 2,$

$C_{A_l}^{(3)}=(a_1+a_2) \bmod 2,\ C_{A_r}^{(3)}=(a_3+a_4) \bmod 2,$

$C_{B_l}^{(3)}=(b_1+b_2) \bmod 2,\ C_{B_r}^{(3)}=(b_3+b_4) \bmod 2.$

Оглашение четности фрагмента приводит к потере одного бита (один бит выражается через остальные входящие во фрагмент), поэтому общие потери конфиденциальности, включая пару, содержащую ошибку, равны $3+2=5$, а в общем случае $n_p=k+2=\log(n,2)-1+2=1+\log(n,2)$. С ростом длины последовательности потери конфиденциальности возрастают, однако их относительная величина уменьшается. Зависимость относительных потерь $w(n)=\frac{n_p}{n}=\frac{1+\log(n,2)}{n}$ от n приведена на рис. 1.

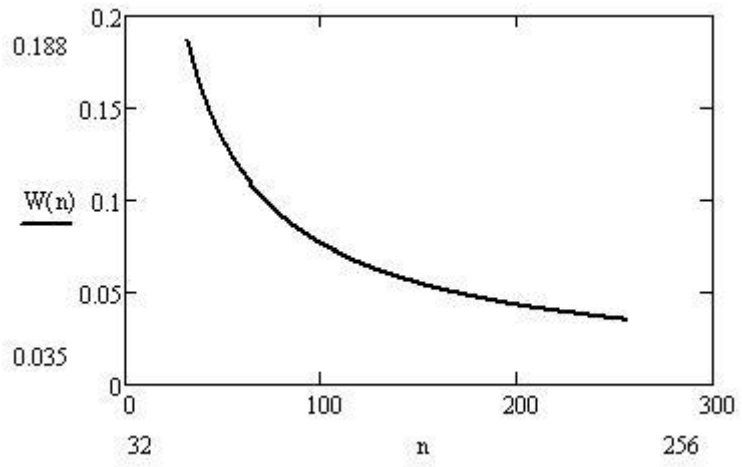

Рис. 1. Относительные потери энтропии

При количестве ошибок $d\rangle 1$ и неизвестном их количестве в [3] метод половинного разбиения дополняется согласованным перемешиванием битов в X_A и X_B. Суть такого поиска ошибочных пар заключается в следующем.

Стороны A и B разбивают свои последовательности пополам и вычисляют четности фрагментов: $C_{A_l}^{(1)}, C_{A_r}^{(1)}, C_{B_l}^{(1)}, C_{B_r}^{(1)}$. Сравнивая четности, делают следующие выводы. Если четности совпадают, то количество ошибок в данном фрагменте четное число $d_l^{(1)}=0,2,4,...$, или $d_r^{(1)}=0,2,4,...$, если не совпадают, то $d_l^{(1)}=1,3,5,...$, или $d_r^{(1)}=1,3,5,...$, (нечетное число). Фрагмент с нечетным числом ошибок, снова разбивается пополам и вновь сравниваются четности. Если полученные половины содержат четное число ошибок, то биты целого фрагмента в

X_A и X_B подвергаются согласованной случайной перестановке и вновь подвергаются разбиению. Таким образом, локализуются фрагменты, содержащие нечетное число ошибок, это продолжается, пока размер фрагмента не станет равным 2. Фрагменты, в которых несколько перестановок и последующих разбиений не выявляют нечетное число ошибок, вероятнее всего, не содержат ошибок и исключаются из разбиения.

Аналитический анализ описанной процедуры весьма затруднителен в силу сложности формализации используемого итерационного процесса. Однако упрощенно можно сделать следующие предположения, если число ошибок невелико, т.е. $d \langle\langle n$, то вероятно их равномерное распределение по номерам последовательности. Поэтому, сделав несколько предварительных разбиений k_0, удается локализовать ошибки в пределах различных фрагментов, т.е. в каждом фрагменте одна ошибка. Далее, затратив k разбиений каждого фрагмента, локализуется пара бит, содержащая одну ошибку. Однако поскольку точное число ошибок к началу процедуры неизвестно, то необходимо каждую пару фрагментов, сравнение четностей которых показало отсутствие одиночной ошибки, подвергнуть перестановкам p раз, чтобы убедиться в отсутствии кратных ошибок. Таким образом, число потерянных бит будет, как минимум, определяться выражением $n_p = k_0 + dk + p$, где $k_0 = d$, $p \approx d$, тогда окончательно получим $n_p \approx d + \ 2 + log\ \ n,2\ \ d = ns\ 1 + \ 2 + log\ \ n,2\ \ $, где $s = d/n$ — доля ошибок в последовательности. Зависимость $n_p(s)$ для $n = 100$ изображена на рис. 2

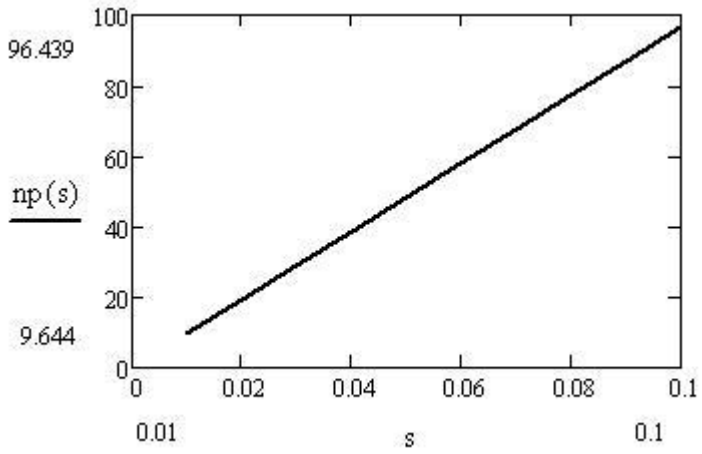

Рис. 2. Зависимость числа потерянных бит от доли ошибок

Лучшие результаты можно получить, если при разбиении последовательности на фрагменты учитывать вероятности попадания некоторого количества ошибок во фрагмент определенной длины. Однако для этого необходимо априорно знать количество (процент) ошибок в исходных последовательностях. Эти сведения могут быть получены, если известен метод, которым формировались исходные последовательности X_A и X_B Например, если для формирования ключевых последовательностей используется квантовый канал без прослушивания, то величина ошибок составляет несколько процентов [4], если метод аномальных эффектов [1], то — до 30%, если метод синхронизированных нейронных сетей [5], то процент ошибок зависит от количества несогласованных весовых коэффициентов при досрочной остановке процесса синхронизации.

Таким образом, если известно примерное количество ошибок, можно рассчитать величину первого фрагмента разбиения из условия наиболее вероятного попадания в него одной ошибки. Сформулированная задача может быть решена приближенно с использованием биномиальной модели описания процесса. Будем считать, что длина исходных последовательностей n велика, вероятность того, что любой бит является ошибочным, одна и та же и равна P_0,

причем $P_0 = \frac{d}{n}$. Обозначим длину искомого фрагмента в битах L, число ошибочных бит в нем d.

Тогда вероятность того, что фрагмент содержит i ошибок, где $i = 0,1,2,...,L$, равна

$$B(i) = \binom{L}{i} P_0^i (1 - P_0)^{L-i}. \quad (1)$$

Эта функция изображена на рис. 3. при $n = 120$, $P_0 = 0{,}3$ для $L = 2$ и $L = 4$.

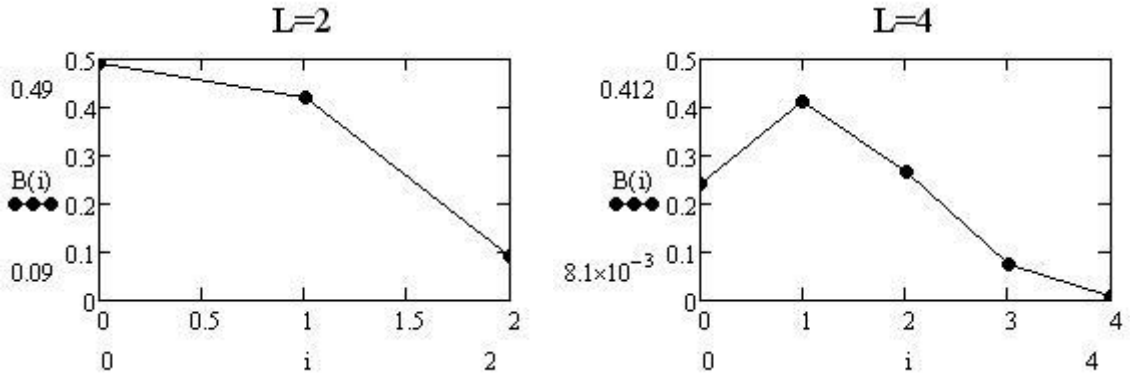

Рис. 3 Закон распределения вероятности ошибок

Будем рассчитывать длину фрагмента в битах L, исходя из условия обеспечения максимальной вероятности того, что данный фрагмент содержит только одну ошибку, т.е. $i = 1$.

Зависимость $B(L) = \binom{L}{1} P_0^1 (1 - P_0)^{L-1}$ для различных значений d изображена на рис. 4, где $B4(L), B10(L), B40(L)$ — зависимость $B(L)$ при $d = 4, d = 10, d = 40$.

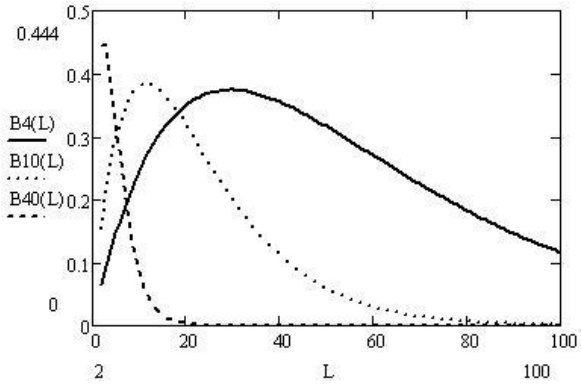

Рис. 4. Зависимость вероятностей распределения ошибок от длины фрагментов разбиения

Из рис. 4 видно, что исследуемая функция имеет максимум по L, зависящий от значения d/n. Найдем его, дифференцируя $B(L)$ по L и приравнивая производную к 0.

$$\frac{d}{dL}[L P_0^1 (1 - P_0)^{L-1}] = 0,$$

$$\frac{P_0}{1 - P_0}(1 - P_0)^L [1 + L \ln(1 - P_0)] = 0.$$

Откуда

$$L_{opt} = -\frac{1}{\ln(1-P_0)}.$$

Искомая длина фрагмента убывает с ростом числа ошибочных бит в последовательности (с увеличением процента ошибок), так при $d = 4$ имеем $L_{opt} \approx 30$, при $d = 10$ имеем $L_{opt} \approx 11$ при $d = 40$ имеем $L_{opt} \approx 2$.

Поскольку мы имеем дело с конечной совокупностью, то для второго и последующих фрагментов формула (1) будет неточна (изменяются величины n и d). Однако, как показывает моделирование, изложенный подход к расчету L дает приемлемые для практического применения результаты. В то же время, очевидно, что при оптимальной длине фрагмента, равной 2 битам, дальнейшее разбиение не имеет смысла и возникает задача разработки нового метода удаления ошибок.

Заключение

Таким образом, проведенное исследование показало, что известные методы устранения ошибок, разработанные применительно для формирования общего ключа с использованием квантового канала, эффективны при малом проценте ошибок. При большом количестве ошибок (более 20%) необходима разработка новых методов.

ELIMINATION OF ERRORS IN BINARY KEY SEQUENCES IN CASE OF DIVERSE KEY GENERATION

V.F. GOLIKOV, F. ABDOLVAND

Abstract

We describe how to troubleshoot inconsistencies (errors) in case of diverse key generation in the confidential formation of a general key for symmetric cryptosystems.

Литература

1. *Голиков В.Ф., Абдольванд Ф.* // Материалы 14-й Международной конференции "Комплексная защита информации". Могилев. 2009. С. 77–79.
2. *Голиков В.Ф., Абдольванд Ф.* // Вестник Белорусского национального технического университета. 2010. № 2. С. 29–32.
3. *Боумейстер Д., Экерт А., Цайлингер А.* // Физика квантовой информации. М., 2002. С. 59–60.
4. *Bennet C.H., Brassard G.* // Quantum cryptography: quantum key distribution and coin tossing. Int. conf. on computers systems ans signal processing. Bangalore. India. 1984. P. 175–179.
5. *Kinzel W., Kanter I.* // Advances in Solid State Physics; ed. B. Kramer. Springer Verlag, 2002. Vol. 42. P. 1–9.