

Защита от side channel attack на основе случайных изоморфизмов

Александр Ростовцев

28 сентября 2004 г.

1 Введение

Стойкость шифраторов и устройств электронной цифровой подписи (ЭЦП) традиционно определяется методами криптоанализа соответствующих алгоритмов. Недавно описан новый вид атак — “side channel attacks”, которые используют особенности программно-аппаратной реализации шифратора или устройства ЭЦП [?], [?]. Если устройство криптографической защиты обрабатывает информацию, вычислимым образом связанную с ключом, то измерение физических сигналов, сопровождающих работу устройства, может дать дополнительную информацию о ключе.

Под термином “side channel attacks” понимают совокупность атак на основе анализа длительности выполнения операций, мгновенной потребляемой мощности, электромагнитных и акустических полей и т.п. [?]. На практике сигналы, несущие информацию о ключе, значительно меньше шума, поэтому для их измерения требуется значительное число повторов.

Часто такие атаки значительно более эффективны, чем дифференциальный [?] или линейный [?] методы анализа шифров или метод Полларда [?] для ЭЦП на эллиптической кривой. Например, такая атака на мобильный телефон позволяет легко вычислить секретный ключ [?].

Целью данной статьи является описание общего подхода к защите устройств ЭЦП и шифров от side channel attacks на основе случайных изоморфизмов криптографических алгоритмов.

2 Изоморфизмы криптографических алгоритмов

Назовем два алгоритма изоморфными, если они для одинаковых входов дают одинаковые выходы. В общем случае изоморфизмы алгоритма могут базироваться на автоморфизмах алгебраической структуры, в терминах которой описывается алгоритм. Рассмотрим типовые алгебраические структуры, используемые в криптографических алгоритмах, и их автоморфизмы.

Стандарт ЭЦП ГОСТ Р 34.10–2001 [?] использует эллиптическую кривую $E(\mathbf{F}_p)$ над простым полем \mathbf{F}_p , имеющую подгруппу простого порядка r . Параметрами схемы подписи является кривая $E(\mathbf{F}_p)$, образующая точка Q порядка r и хэш-функция h . Конфиденциальным ключом является показатель l . Для формирования подписи вырабатывается случайный показатель k , вычисляется точка $(x_R, y_R) = kQ$, вычисляется хэш-функция $e = h(m)$ для сообщения m и показатель

$$s \equiv lx_R + ke \pmod{r}. \quad (1)$$

Группа автоморфизмов модуля \mathbf{F}_r изоморфна группе \mathbf{F}_r^* .

Симметричные шифры обычно описываются в терминах кольца полиномов Жегалкина

$$\mathbf{G}_n \cong \mathbf{F}_2[x_1, \dots, x_n] / (x_1^2 - x_1, \dots, x_n^2 - x_n).$$

Каждая булева функция $f(x_1, \dots, x_n)$ может быть однозначно представлена как 2^n -мерным вектором \mathbf{f} значений, так и полиномом Жегалкина

$$f = a_0 + \sum_i a_i x_i + \sum_{i>j} a_{ij} x_i x_j + \dots + a_{1\dots n} x_1 \dots x_n,$$

то есть 2^n -мерным вектором коэффициентов \mathbf{a} , при этом $\mathbf{a} = L_n \mathbf{f}$, где L_n определяется рекурсивно как блочная матрица: $L_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $L_{i+1} =$

$$\begin{pmatrix} L_i & 0 \\ L_i & L_i \end{pmatrix}.$$

Кольцо \mathbf{G}_n имеет единственный обратимый элемент — константу 1. Назовем разложения $f = 1 \cdot f$ и $f = f \cdot f$ тривиальными, а элементы, допускающие только тривиальные разложения, — неразложимыми.

В кольце \mathbf{G}_n существует 2^n неразложимых элементов, для них вектор значений имеет единственную нулевую координату. Произведению элементов кольца \mathbf{G}_n соответствует объединение множеств их нулей. Поскольку булева функция однозначно определяется списком своих нулей, кольцо \mathbf{G}_n обладает однозначным разложением на неразложимые элементы. Однозначность разложения позволяют описать автоморфизмы кольца \mathbf{G}_n .

Лемма 1. Каждый автоморфизм кольца \mathbf{G}_n переводит неразложимый элемент в неразложимый элемент.

Доказательство. Пусть φ — автоморфизм. Из равенства $1 \cdot f = f$ получаем $\varphi(1) = 1$, при этом непостоянный полином отображается в непостоянный полином. Пусть элемент f неразложимый. Предположим, что $\varphi(f) = gh$, где $g \neq h$. Тогда отображение φ не может быть обратимым.

Следствие 2. Группа автоморфизмов кольца \mathbf{G}_n изоморфна группе перестановок из 2^n элементов.

Доказательство следует из того, что перестановка двух неразложимых элементов является автоморфизмом кольца \mathbf{G}_n .

Таким образом, при больших n почти все автоморфизмы кольца \mathbf{G}_n являются трудновычислимыми.

Механизм защиты ключа на основе случайных изоморфизмов основан на том, что изоморфные алгоритмы при одинаковых входах дают одинаковые выходы, при этом промежуточные значения данных могут различаться случайным образом. Действительно, side channel attack использует вычислимую зависимость между ключом и кодом текущей обрабатываемой информации, но для не известных нарушителю изменяющихся изоморфизмов эта зависимость не является вычислимой.

3 Защита ключа подписи

Для защиты ключа автоморфизмы модуля $\mathbf{Z}/r\mathbf{Z}$ должны быть случайными и периодически изменяться. На первой реализации электронной цифровой подписи вместо постоянного ключа l используется замаскированное значение $k_1^{-1}l$, где k_1 — случайное число. Преобразуем уравнение формирования подписи (??) с учетом наложения и снятия маски. Получим

$$s \equiv k_1((k_1^{-1}l)x_R + e) \pmod{r}. \quad (2)$$

Для формирования первой подписи отправитель вырабатывает случайный показатель k_1 , полагает $u_1 = k_1$, вычисляет значение $u_1^{-1}l \pmod{r}$, точку $R_1 = (x_R, y_R) = k_1Q$ и подпись s согласно выражению (??). Поскольку показатель s не зависит от наложения и снятия маски, уравнение проверки подписи не меняется.

На последующих процедурах уравнение формирования подписи преобразовывается по индукции:

$$\begin{aligned} s &\equiv k_i u_{i-1} (k_i^{-1} (u_{i-1}^{-1} l) x_R + u_{i-1}^{-1} e) \pmod{r}, \\ u_i &\equiv u_{i-1} k_i \pmod{r}. \end{aligned}$$

Для формирования i -й подписи необходимо хранить текущее значение u_{i-1} и $u_{i-1}^{-1}l$ вместо ключа l .

Поскольку параметры s , x_R не зависят от маски, процедура проверки подписи соответствует стандарту ГОСТ Р 34.10–2001.

Механизм защиты ключа определяется двумя составляющими. Во-первых, становится затруднительным независимое вскрытие слов ключа l , так как каждое слово ключа зависит от всех слов чисел u_i и $u_i^{-1}l$. Во-вторых, вместо одиночного числа l используется пара чисел u_i и $u_i^{-1}l$ того же размера, содержащая полную информацию о ключе.

Вычисление ключа требует определения всех битов чисел u_i и $u_i^{-1}l$. Поскольку ошибка в одном бите любого из этих битов с вероятностью $\approx 0,5$ меняет любой бит ключа, для вскрытия ключа требуется правильный прием обоих слов, что практически невозможно, так как энергия шума значительно превышает энергию одиночного сигнала. Использование методов выделения сигнала из шума практически не повышает достоверность приближения для ключа по сравнению с одиночным сигналом. Это обусловлено тем, что накапливать отклики нужно для ключа l , а не для чисел u_i и $u_i^{-1}l$.

Однако даже малые в хемминговом смысле ошибки при определении этих чисел приводят к случайным изменениям ключа. Действительно, если вместо чисел u_i и $u_i^{-1}l$ получены $v_1 = u_i + \Delta_1$ и $v_2 = u_i^{-1}l + \Delta_2$, соответственно, то их произведение даст приближение для ключа l :

$$l \equiv l(1 + u_i^{-1}\Delta_2) + v_1\Delta_2 \pmod{r}.$$

Предположим, что нарушитель может оценить хеммингов вес вероятной ошибки. Наилучшим алгоритмом для вычисления l является перебор по всем векторам ошибки Δ_1, Δ_2 малых весов, начиная с нулевого. Пусть каждый бит сигнала определяется с вероятностью $0,5 + \delta$. Для $r \approx 2^{255}$ сложность перебора будет превышать оценку сложности алгоритма Полларда [?], если вес вероятной ошибки Δ_1 и Δ_2 не превышает некоторого значения z . Из условия $2^{128} \leq (\sum_{i=0}^z \binom{256}{i})^2$ находим граничный вес вектора ошибки $z = 11$.

Если задаться вероятностью P того, что сложность данной атаки будет меньше, чем сложность алгоритма Полларда, то можно определить допустимую погрешность приема одиночного бита сигналов $u_i, u_i^{-1}l$:

$$P = \sum_{i=0}^{11} \binom{256}{i} (0,5 + \delta)^{256-i} (0,5 - \delta)^i.$$

Численное решение этого уравнения для $P = 10^{-3}$ показывает, что $\delta \approx 0,403$. Следовательно, если вероятность правильного приема одного бита информации меньше, чем $0,5 + \delta = 0,903$, то нарушитель не может улучшить оценку сложности для алгоритма Полларда. На практике это условие обычно выполняется, поэтому данный метод защиты ключа подписи практически исключает атаки типа side channel attack.

4 Защита ключа симметричного шифра

Шифр представляет собой композицию обратимых отображений. Автоморфизмы кольца \mathbf{G}_n позволяют согласованно изменять вход, выход и само отображение. Защита ключа с помощью перестановочных автоморфизмов реализуется следующим образом.

1. На вход, выход и отображение накладывается автоморфизм φ_i .
2. Выполняется текущее отображение.
3. На вход, выход и очередное отображение накладывается очередной автоморфизм φ_{i+1} .
4. С полученных данных снимается предыдущий автоморфизм φ_i .
5. Выполняется очередное отображение и т.д.

Стандарт шифрования ГОСТ 28147–89 [?] как фейстелев шифр обладает вычислимым изоморфизмом (инверсия старшего бита в словах ключа, открытого текста, шифртекста). Этот изоморфизм защищает только один бит и поэтому неэффективен. Эффективные изоморфизмы шифра неудобны в реализации.

Шифр Rijndael [?] представляется более удобным для построения изоморфизмов, поскольку все операции описываются в терминах поля \mathbf{F}_{256} и полиномов над этим полем. Такая структура шифра позволяет использовать случайные автоморфизмы для 8-битовых полиномов Жегалкина, допускающие простое описание. Например, для операции обращения в поле \mathbf{F}_{256} (в блоке подстановки) мультипликативная маска входа $x \rightarrow ax$ приводит к линейному изменению выхода, а аддитивная маска входа — к полиномиальному изменению выхода.

Список литературы

- [1] Kelsey J., Schneier B., Wagner D. and Hall S. Side channel cryptanalysis of product ciphers // Proceedings of ESORICS'98. Springer-Verlag, 1998. P. 97–110.
- [2] Side channel attack // http://en.wikipedia.org/wiki/Side_channel_attack.
- [3] Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Advances in Cryptology — CRYPTO '90. Lecture Notes in Computer Science. Springer-Verlag. 1991. Vol. 537. P. 2–21.
- [4] Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT '93. Lecture Notes in Computer Science. Springer-Verlag. 1994. Vol. 765. P. 386–397.
- [5] Pollard J. Monte Carlo methods for index computation mod p // Mathematics of Computation. 1978. Vol. 32. P. 918–924.
- [6] Clavier C. Side Channel Analysis for Reverse Engineering (SCARE) — An Improved Attack Against a Secret A3/A8 GSM Algorithm <http://eprint.iacr.org/2004/049>.
- [7] ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Госстандарт России, 2001.
- [8] ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР, 1989.
- [9] Announcing the advanced encryption standard (AES). Federal Information Processing Standards Publication, 2001.