Тезисы доклада на конференции «РусКрипто» 2008.

Веденьёв Л.Т., Леонтьев С.Е., Попов В.О.

Об опасности ошибок вычислений при использовании стандарта ГОСТ Р 34.10-2001

Рассмотрен вопрос о влиянии ошибок вычислений на стойкость криптоалгоритмов ЭЦП ГОСТ Р 34.10-2001 и Диффи-Хеллмана на базе эллиптических кривых.

В открытых публикациях регулярно поднимается вопрос об опасности влияния на различные криптографические приложения ошибок функционирования аппаратных средств (hardware) ПЭВМ. В публикации [1] А. Шамиром рассмотрен случай влияния трудно обнаруживаемого дефекта в микропроцессоре ПЭВМ: произведение хотя бы одной пары значений операндов (дефектная пара), выполненное микропроцессором, отличается от его истинного значения. Дефект такого рода может быть:

- дефектом разработки микропроцессора;
- технологическим дефектом изготовления микропроцессора различными производителями;
- дефектом, умышленно внедренным в микропроцессор.

На базе этого дефекта А. Шамир предложил модель атаки по вскрытию закрытого ключа алгоритма RSA с использованием китайской теоремы об остатках, отметив возможность применения аналогичной атаки также к другим известным алгоритмам асимметричной криптографии, в частности, при реализации их на эллиптических кривых.

В публикациях [3] и [4] рассмотрены атаки по вскрытию закрытых ключей в алгоритме RSA и в протоколах идентификации (Fiat-Shamir, Schnorr) при многократных битовых искажениях данных в процессе вычислений.

В общем случае речь идет об оценке опасности влияния ошибок вычислений в процессе выполнения криптографических алгоритмов и протоколов.

Представляет практический интерес оценка возможности и эффективности использования ошибок и дефектов в работе ПЭВМ для вскрытия закрытого ключа ЭЦП в алгоритме Эль-Гамаля. В отличие от алгоритма RSA, формирующего при повторных подписываниях одно и то же значение ЭЦП для данного сообщения, в алгоритме Эль-Гамаля за счет использования разового случайного ключа при повторных подписываниях того же сообщения получаются, вообще говоря, разные значения ЭЦП из множества, определяемого закрытым ключом и множеством всех случайных разовых ключей.

В стандарте ГОСТ Р 34.10-2001 алгоритм Эль-Гамаля функционирует на циклической группе точек эллиптической кривой простого порядка q. Криптографическая защищенность закрытого ключа (кратность точки кривой) как по открытому ключу (точка кривой), так и по ЭЦП обеспечивается сложностью логарифмирования в группе точек эллиптической кривой.

Вопрос об опасности влияния ошибок и дефектов в работе ПЭВМ на алгоритм ГОСТ Р 34.10-2001 и криптографические протоколы должен рассматриваться в следующих аспектах:

- характер криптографически опасных влияний на СКЗИ отклонений в работе ПЭВМ;
- противодействие криптографически опасным влияниям отклонений в работе ПЭВМ средствами СКЗИ и криптографических протоколов.

1. Характер криптографически опасных влияний ошибок вычислений при использовании стандарта ГОСТ Р 34.10-2001

Отклонения в работе ПЭВМ, связанные с ошибками вычислений при выполнении криптографических алгоритмов, являются криптографически опасными, если они создают условия для проведения атак, позволяющих понизить сложность определения закрытого ключа до уровня практического применения. Атаки представляют также теоретический интерес, если они позволяют получить более низкую оценку сложности определения закрытого ключа по сравнению с известными методами.

К отклонениям в работе ПЭВМ, требующим оценки их влияния на корректность использования алгоритма ГОСТ Р 34.10-2001, принципиально относятся:

- случайные сбои в отдельных разрядах регистров данных в процессе выработки открытого ключа. Характер влияния – при вычислении точки эллиптической кривой в качестве кратности используется закрытый ключ с одним (случай наиболее вероятный) инвертированным разрядом в его двоичном представлении. Факт искажения полученного при этом открытого ключа может быть установлен по неподтверждению ЭЦП; в системах открытого распределения ключей - по невозможности установления связи с другим абонентом. Предположение, что при выработке открытого ключа был искажен i-тый бит закрытого ключа, проверяется соответствием закрытому ключу суммы в группе точек эллиптической кривой искаженного открытого ключа с точкой кратности 2^i или -2^i; в первом случае i-тый бит закрытого ключа равен 1, во втором – 0; если в обоих случаях подпись не подтверждается, значит имела место какая-то другая ошибка;

- сбой состояния регистра данных в процессе выработки открытого ключа, приводящий к заполнению части его разрядов известным вектором. Характер влияния – при вычислении точки эллиптической кривой в качестве ее кратности используется закрытый ключ с заменой его части известным значением. Факт искажения полученного при этом открытого ключа устанавливается подписыванием произвольного хэша и неподтверждением полученной подписи при проверке ее с открытым ключом; в системах открытого распределения ключей - по невозможности установления связи с другим абонентом. В этом случае на первом этапе можно проводить опробование неискаженной части закрытого ключа, на втором - доопробование искаженной части;

- сбои и искажения в аддитивных и мультипликативных операциях при вычислении ЭЦП.

ЭЦП в алгоритме Эль-Гамаля содержит две компоненты:

- число, редуцируемое от элемента группы, определяемое как значение однонаправленной функции от случайного разового ключа;

- сумма по модулю q результата умножения этого числа на закрытый ключ ЭЦП с результатом умножения хэша сообщения на случайный разовый ключ.

Проведением атаки многократными запросами на получение подписи создается возможность целенаправленно инициировать интенсивность событий, в которых проявилось бы действие систематического дефекта микропроцессора, с целью повышения вероятности их наступления. В качестве индикатора наступления такого события используется факт не подтверждения ЭЦП по сертификату открытого ключа, соответствующему вскрываемому закрытому ключу. Будем представлять хэши и случайные разовые ключи как векторы над алфавитом операндов микропроцессора. Используя хэши, содержащие в разрядах указанного представления элементы дефектной пары, можно идентифицировать события, когда хотя бы один разряд случайного разового ключа окажется элементом дефектной пары микропроцессора. Это даёт возможность уменьшить ранг системы уравнений, связанной с функционированием закрытого ключа ЭЦП. При корневой оценке сложности логарифмирования в группе точек эллиптической кривой проведение такой атаки представляет интерес, если ранг набираемой при этом системы линейных уравнений будет не менее половины разрядов случайного разового ключа.

Аналогично строятся атаки на закрытый ключ ЭЦП, основанные на случайных сбоях в отдельных разрядах регистров данных ключей ЭЦП в процессе вычисления значения ЭЦП.

Расчеты показывают, что в случае стандарта ГОСТ Р 34.10-2001 с закрытым и разовым ключами 256 бит для получения системы линейных уравнений ранга не менее 128 потребуется подписать не менее 10^7 хэшей в случае использования рассматриваемого мультипликативного дефекта микропроцессора. Вероятность успешного проведения такой атаки мала.

Попытка проведения атаки по вскрытию закрытого ключа стандарта ГОСТ Р 34.10-2001 при битовых искажениях данных в регистрах в процессе вычислений потребует, чтобы остаться хотя бы на уровне корневой оценки, накопления 128 сбоев в определенных точках вычислений. При надежности современной вычислительной техники вероятность достижения таких условий для проведения этой атаки также мала.

Вместе с тем, нельзя не учитывать, что ЭЦП по алгоритму Эль-Гамаля является линейной формой закрытого ключа. Реализация ЭЦП по этому алгоритму на широком спектре современных аппаратно–программных платформ, оценить надежность и корректность функционирования которых в достаточном объеме не всегда представляется возможным, требует в

конкретных случаях использовать в СКЗИ и в криптографических протоколах дополнительные меры противодействия возможным опасным влияниям ошибок вычислений ПЭВМ.

2. Противодействие криптографически опасным влияниям ошибок вычислений средствами СКЗИ и криптографических протоколов

Возможность опасного влияния случайных сбоев и дефектов систематического характера в работе ПЭВМ на выполнение криптографических функций может в конкретных случаях привести к необходимости применения в СКЗИ и в криптографических протоколах дополнительных защитных мер. В случае стандарта ГОСТ Р 34.10-2001 в качестве таких мер могут использоваться:

- проверка принадлежности вырабатываемого открытого ключа группе точек эллиптической кривой;
- проверка соответствия выработанного открытого ключа соответствующему закрытому ключу;
- использование методов вычисления ЭЦП, гарантирующих не снижение стойкости ключа при выполнении операций формирования ЭЦП при сбоях и ошибках вычислений;
- доверенная верификация реализации процессором ПЭВМ критических арифметических операций при выполнении криптографических функций;
- двукратное выполнение криптографических преобразований и сравнение полученных результатов для защиты от битовых искажений в процессе вычислений;
- проверка ЭЦП сообщения после ее формирования, как это рекомендуется в открытых публикациях.

Литература.

1. A. Shamir. Research Announcement: Microprocessor Bugs Can Be Security Disasters. Computer Science Department The Weizmann Institute of Science, Israel, 2007. <http://cryptome.org/bug-attack.htm>

2. The New York Times J. Markoff. Adding Math to List of Security Threats. <http://www.nytimes.com/2007/11/17/technology/17code.html>

3. D.Boneh, R.DeMillo, R.Lipton. "On the Importance of checking cryptographic protocols for faults", in Proc/ of Eurocrypt '97.LNCS 1233, Springer-Verlag, pp. 37-51, 1997.

4. D.Boneh, R.DeMillo, R.Lipton. "On the Importance of Eliminating Errors in Cryptographic Computations". Расширенная версия [3].