Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Дорох Кирилл Юрьевич

«Защита аппаратно-программных средств криптографического преобразования данных от атак по сторонним каналам»

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 03 Аппаратное и программно-техническое обеспечение информационной безопасности

_____

Научный руководитель

Ползунов Владимир Васильевич

Кандидат технических наук, доцент

_____

Минск 2017

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Защита АПС КПД (аппаратно-программных средств криптографического преобразования данных) от атак по сторонним каналам является актуальной в области обеспечения информационной безопасности радиотехнических систем передачи информации.

Объектом исследования являются аппаратно-программные средства криптографического преобразования. Предметом является защита от атак по времени выполнения асимметричных криптоалгоритмов

Цель работы заключается в устранении каналов утечек информации АПС КПД в используемом ключевом пространстве по времени выполнения асимметричных криптоалгоритмов.

Задачи исследования:

1. Разработка алгоритмов выполнения основных операций ассиметричных криптопреобразований на базе СОК (системы остаточных классов).
2. Исследование влияния арифметики СОК на время выполнения ассиметричных криптоалгоритмов.

ВВЕДЕНИЕ

Атаки по сторонним (или побочным) каналам используют информацию, которая может быть получена с криптосистемы и не является открытым текстом или шифртекстом. Атаки по побочным каналам легко реализуемы во время мощных атак против криптографических реализаций, и в диапазоне их целей находятся примитивы, протоколы, модули и устройства криптографических модулей. Данный тип атак основан на корреляции между значениями физических параметров, измеряемых в разные моменты во время вычислений, и внутренним состоянием вычислительного устройства, имеющим отношение к секретному ключу. Этот подход менее обобщенный, но более мощный, чем классический криптоанализ.

Данный вид атак стал широко известен после публикации результатов исследования Полом Кохером в 1996 году, хотя подобные атаки были известны еще в 1980-е годы. В своих исследованиях он доказал наличие статистической зависимости между значением секретного ключа и временем, затрачиваемым криптоустройством на вычисление операции возведения в степень.

При анализе защищенности криптосистемы считается, что криптоалгоритм, используемый в системе, является стойким. Именно поэтому атаки на криптосистемы по побочным каналам направлены не на взлом самих криптоалгоритмов, а на перехват какой-либо "побочной" информации (например, электромагнитного излучения, потребляемой энергии, времени или даже звука). Анализ данной информации очень важен для криптоаналитика, так как он может избавить его от необходимости полного перебора.

В настоящее время данный вид атак очень распространён по двум причинам: доступность криптосистем (токены, банковские карты с чипом, SIM-карты и т.д.) и относительно низкая стоимость оборудования необходимого для проведения атаки. Эти атаки представляют серьезную угрозу для безопасности криптографических модулей. В результате нужно оценить криптографические реализации с точки зрения сопротивления таким атакам и рассмотреть введение контрмер.

КРАТКОЕ СОЖЕРЖАНИЕ РАБОТЫ

В последние годы исследователи все больше и больше осведомлены о возможности атак, которые используют определенные свойства реализации и операционной среды. Такие атаки по АПС КПД (аппаратно-программные средства криптографического преобразования данных) используют утечку информации во время выполнения протокола и не рассмотрены в традиционных моделях обеспечения безопасности. Например, криптоаналитик может быть в состоянии контролировать потребляемую мощность или электромагнитное излучение, испускаемое смарт-картой, в то время как выполняются операции с закрытым ключом, такие как генерация подписи и дешифрование. Он может также измерить время, которое требуется, чтобы выполнить криптографическую работу или проанализировать как криптографическое устройство ведет себя когда встречается с определенными ошибками. Информацию побочного канала можно легко собрать на практике и поэтому важно, чтобы угроза атак по АПС КПД была определена количественно при оценке полной безопасности системы.

Криптографическая модель, с учетом побочных каналов представлена на рисунке 1.1

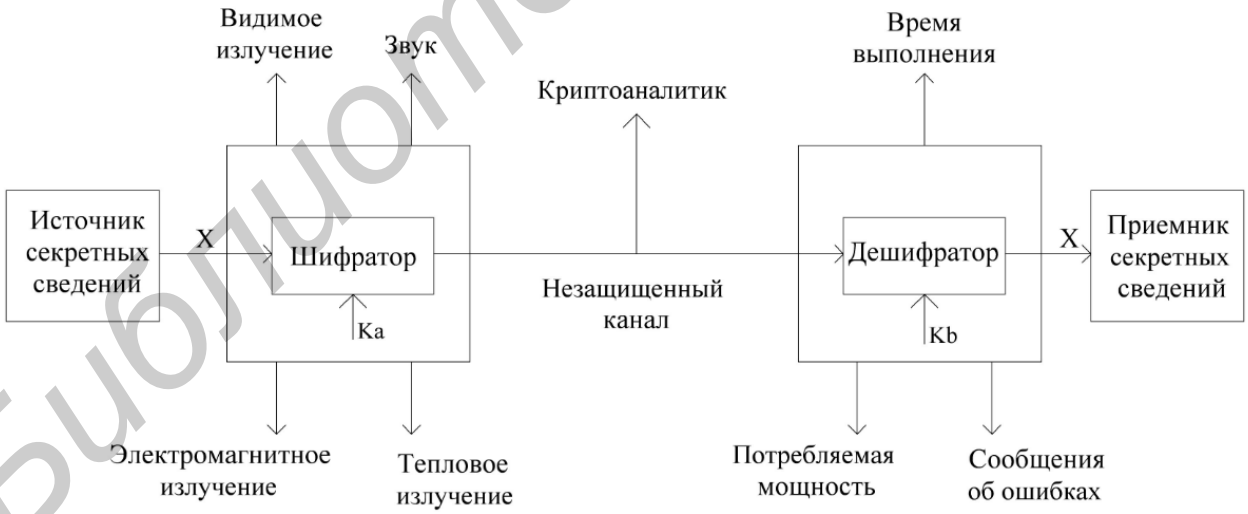

Рисунок 1.1 - Криптографическая модель, с учетом побочных каналов

Побочные каналы определяются как непреднамеренные выходные каналы из системы. Пол Кохер в 1996 году показывал, что непостоянное время работы шифров может привести к утечке информации о ключе. Когда реализации используют в своих интересах оптимизацию, проблема может стать более явной.

Нужно подчеркнуть, что определенная атака по побочным каналам может не быть реальной угрозой в некоторых средах. Например, атаки, которые измеряют потребляемую мощность криптографического устройства, можно считать очень вероятными, если устройство — смарт-карта, которая использует питание внешнего, недоверенного источника. С другой стороны, если устройство — рабочая станция, расположенная в безопасном офисе, то атаки по потребляемой мощности — незначительная угроза.

ИЗВЕСТНЫЕ ТИПЫ АТАК

1. Атаки по времени выполнения (Timing Attack)

2. Атаки по ошибкам вычисления (Fault Attack)

3. Атаки по мощности (Power Analysis Attack)

4. Атаки по видимому свету (Visible Light Attack)

5. Атаки по электромагнитному излучению (Electromagnetic Analysis Attack)

6. Акустические атаки (Acoustic Attack)

СУЩЕСТВУЮЩИЕ МЕТОДЫ ЗАЩИТЫ ОТ АТАК ПО ВРЕМЕНИ ВЫПОЛНЕНИЯ

1 Введение дополнительных задержек.

2 Выравнивание времени выполнения операций умножения и возведения в квадрат.

3 Различная маскировка времени выполнения операций.

Криптоанализ по побочным каналам является специфическим для конкретной реализации и в диссертации рассматривается защита от атак по времени выполнения современных асимметричных криптоалгоритмов ЭЦП (электронная цифровая подпись) над простым полем (в мультипликативных группах).

ЭЦП — реквизит электронного документа, служащий для определения источника данных и защиты документа от подделки. Для получения ЭЦП выполняется криптографическое преобразования электронного документа, которое потом присоединяется к документу или логически объединяется с

ним. Это дает возможность подтвердить его целостность и идентифицировать подписавшего.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Иначе говоря, открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ.

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, как и в асимметричных системах шифрования, используются разные математические схемы, основанные на применении однонаправленных функции. Эти схемы разделяются на две группы. В основе такого разделения лежат две известные сложные вычислительные задачи: задача факторизации (разложения на множители) больших целых чисел и задача дискретного логарифмирования.

Современные криптографические средства осуществляют алгоритмы электронной подписи используя *алгоритмы RSA, Эль-Гамаля, схему Шнорра*.

В основе криптостойкости этих алгоритмов лежит задача дискретного логарифмирования, т.е. для шифрования используется операция возведения в степень по модулю p.

$$c = a^b \ mod \ p, \qquad (1.1)$$

А по времени выполнения данной операции можно судить о весе экспоненты b. Эта информация снижает криптостойкость системы так как сокращает область неопределенности. Таким образом можно значительно сократить перебор.

Современные асимметричные криптоалгоритмы ЭЦП над простым полем (в мультипликативных группах часто используют позиционные системы счисления. Реализация криптоалгоритмов в ПСС (позиционная система счисления) снижает криптостойкость используемых криптоалгоритмов. Для устранения этого недостатка такие операции могут быть выполнены в непозиционных системах типа СОК (система остаточных

классов). Но в СОК нужна проработка операций умножения, сложения, деления с остатком и мультипликативного обращения. Достоинства системы в том, что она легко распараллеливается, благодаря наличию простых делителей она равномерно распределяет время выполнения операций: сложения, умножения, деления, возведения в степень.

В работе были рассмотрены алгоритмы сложения, вычитания, умножения, возведения в степень и деления в системе остаточных классов. Рассчитана вычислительная сложность. Теоретические вычисления алгоритмов ЭЦП над простым полем примерно одинаковы в обоих системах счисления.

Разработан алгоритм возведения в степень по модулю в СОК, не зависящий от веса экспоненты.

Алгоритм возведения в степень по модулю в СОК представлен на рисунке 1.2.

Рисунок 1.2 - Алгоритм возведения в степень по модулю в СОК

Были рассмотрены алгоритмы возведения в степень по модулю $c = a^b \ mod\ p$, изменяя только степень b. На рисунках 1.3 и 1.4 представлены зависимости времени выполнения алгоритма от веса b в системе остаточных классов и позиционной системе счисления.

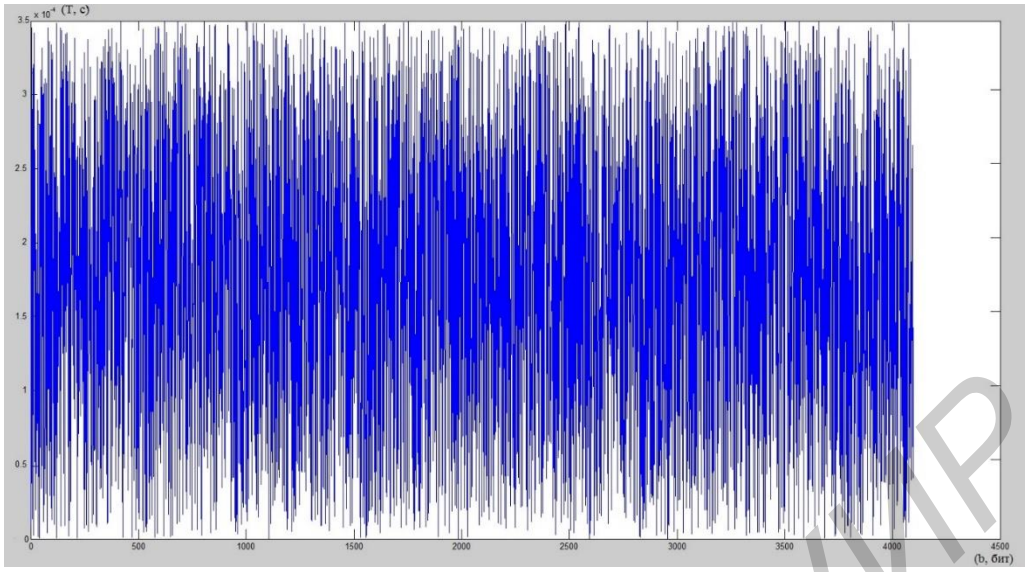

Рисунок 1.3 Зависимость времени выполнения от веса экспоненты в СОК

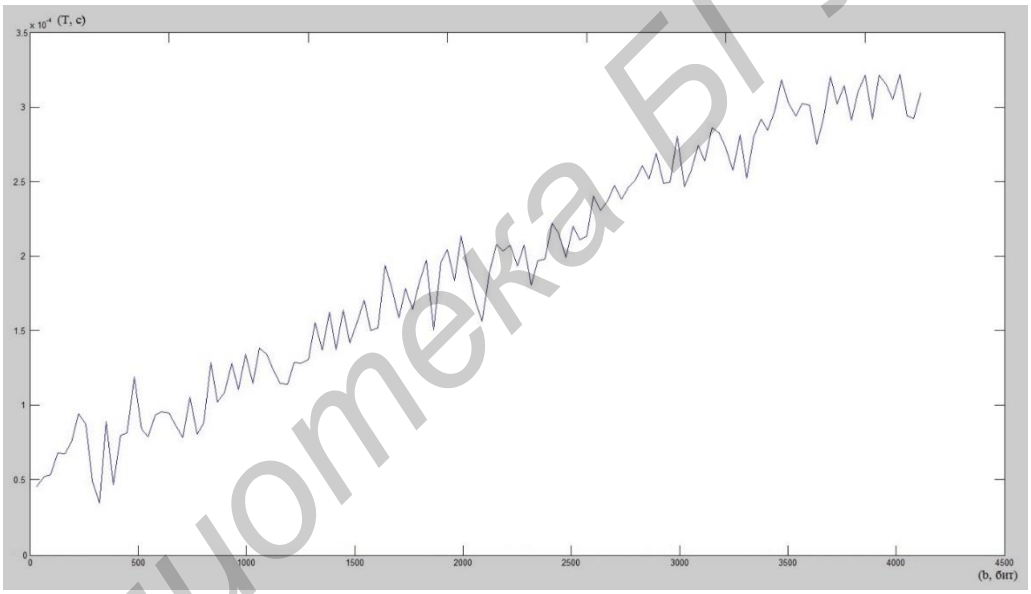

Рисунок 1.4 Зависимость времени выполнения от веса экспоненты в ПСС

Как видно по графикам в системе остаточных классов нет зависимости времени выполнения возведения в степень по модулю, а в ПСС время выполнения линейно возрастает от увеличения веса экспоненты.

Получившийся метод возведения в степень по модулю в системе остаточных классов можно использовать в алгоритмах выработки ЭЦП для улучшения их стойки от атак по времени выполнения. Время выполнения алгоритмов увеличится, но не зависит от веса b. Используя параллельные вычисления можно достичь лучшего результата.

ЗАКЛЮЧЕНИЕ

Таким образом, были рассмотрены атаки по побочным каналам, в частности атаки по времени выполнения. В диссертации рассматривается защита от атак по времени выполнения современных асимметричных криптоалгоритмов ЭЦП над простым полем (в мультипликативных группах). В основе криптостойкости этих алгоритмов лежит задача дискретного логарифмирования, т.е. для шифрования используется операция возведения в степень b по модулю p.

$$c = a^b \ mod \ p,$$

А по времени выполнения данной операции можно судить о весе экспоненты b. Эта информация снижает криптостойкость системы так как сокращает область неопределенности. Таким образом можно значительно сократить перебор.

Для устранения этого недостатка такие операции могут быть выполнены в непозиционных системах счисления типа СОК (система остаточных классов). Были проработаны операций умножения, сложения, деления с остатком и возведения в степень в СОК, разработан алгоритм выработки ЭЦП в СОК. Проведена теоретическая оценка и сравнение алгоритмов данных в позиционной системе счисления и в непозиционной типа СОК в среде MATLAB. По итогу сравнения можно сказать, что использование непозиционной системы счисления в асимметричных криптоалгоритмах позволит справится с атаками по времени выполнения. Получившийся методы арифметических операций в системе остаточных классов можно использовать в алгоритмах выработки ЭЦП для улучшения их стойкости к атакам по времени выполнения. Время выполнения алгоритмов незначительно увеличится, но время выполнения не зависит от веса степени b . Используя параллельные вычисления можно достичь лучшего результата. СОК имеет структуру легко адаптирующуюся к параллельным вычислениям. Поэтому важным является разработка параллельных алгоритмов криптографического преобразования данных в СОК.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Качественные характеристики алгоритмов параллельных вычислений – 11-я Международная молодёжная научно-техническая конференция «Современные проблемы радиотехники и телекоммуникаций РТ-2016», 16 — 20 ноября 2015 г., Севастополь, Российская Федерация;
2. Защита криптоалгоритмов от атак по времени выполнения – 12-я Международная молодёжная научно-техническая конференция «Современные проблемы радиотехники и телекоммуникаций РТ-2016», 14 — 18 ноября 2016 г., Севастополь, Российская Федерация;