ТЕМА 8 Типовые угрозы безопасности аппаратного обеспечения. Методы и средства защиты аппаратного обеспечения.

8.1. Классификация угроз.

Основная угроза для аппаратного обеспечения компьютерной системы связана с его доступностью. Аппаратное обеспечение больше всего подвержено атакам и менее всего поддается автоматическому управлению.

В число угроз входят:

случайный вывод оборудования из строя

преднамеренный вывод оборудования из строя

кража оборудования.

Для устранения угрозы подобного рода нужны административные меры по предотвращению физического доступа к системам.

Задачи по защите от угроз

Преднамеренные угрозы

угрозы, которые реализуются с постоянным участием человека;

после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без участия человека.

Задачи по защите от угроз каждого вида одинаковы:

запрещение несанкционированного доступа к ресурсам;

невозможность несанкционированного использования ресурсов при осуществлении доступа;

своевременное обнаружение факта несанкционированного доступа.

Устранение их причин и последствий.

8.2. Способы и средства защиты информации

Для предотвращения вышеперечисленных угроз существуют различные способы защиты информации.

Помимо естественных способов выявления и своевременного устранения причин, используют следующие специальные способы защиты информации от нарушений работоспособности компьютерных систем:

внесение структурной, временной информационной и функциональной избыточности компьютерных ресурсов;

защита от некорректного использования ресурсов компьютерной системы;

выявление и своевременное устранение ошибок на этапе разработки программно-аппаратных средств.

Избыточность компьютерных ресурсов

Структурная избыточность компьютерных ресурсов достигается за счет резервирования аппаратных компонентов и машинных носителей. Организация замены отказавших и своевременного пополнения резервных компонентов. Структурная избыточность составляет основу.

Внесение информационной избыточности выполняется путем периодического или постоянного фонового резервирования данных на основных и резервных носителях. Резервирование данных обеспечивает восстановление случайного или преднамеренного уничтожения или искажения информации. Для восстановления работоспособности компьютерной сети после появления устойчивого отказа кроме резервирования обычных данных, следовательно, заблаговременно резервировать и системную информацию.

Функциональная избыточность компьютерных ресурсов достигается дублированием функции или внесением дополнительных функций в программно-аппаратные ресурсы. Например, периодическое тестирование и восстановление самотестирование и самовосстановление компонентов систем.

Защита от некорректного использования ресурсов компьютерной системы

Программа может четко и своевременно выполнять свои функции, но не корректно функционировать с позиции использования ресурсов вычислительных систем

Защита, например:

изолирование участков оперативной памяти для операционной системы для прикладных программ

защита системных областей на внешних носителях.

Выявление и устранение ошибок при разработке программно-аппаратных средств

Выявление и устранение ошибок при разработке программно-аппаратных средств достигается путем качественного выполнения базовых стадий разработки на основе системного анализа концепции проектирования и реализации проекта.

Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства.

Наибольшее распространение получают следующие Аппаратные средства защиты информации:

специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;

устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты.

8.3. Биометрические системы контроля доступа

Условно, биометрические алгоритмы аутентификации можно условно разделить на два основных типа:

Статические – дактилоскопия, радужная оболочка глаз; измерение формы кисти, линии ладоней, размещения кровеносных сосудов, измерение формы лица в 2D и 3D алгоритмах;

Динамические – почерк и ритм набора текста; походка, голос и т.п.

Главные критерии выбора - два параметра:

FAR – определяет математическую вероятность совпадения ключевых биологических параметров двух различных людей;

FRR – определяет степень вероятности отказа в доступе лицу, имеющему на это право.

Также важными параметрами для комфортной эксплуатации являются:

Простота пользования и возможность осуществления идентификации, не останавливаясь перед устройством;

Скорость считывания параметра, обработки полученной информации и объем базы данных биологических эталонных показателей.

Отпечатки пальцев

Дактилоскопический анализ является наиболее распространенным, технически и программно совершенным способом биометрической аутентификации.

Главным условием развития является хорошо наработанная научно-теоретическая и практическая база знаний.

Методология и система классификации папиллярных линий.

При сканировании ключевыми точками являются:

окончания линии узора,

разветвления,

одиночные точки.

В особо надежных сканерах вводят систему защиты от латексных перчаток с отпечатками – проверку рельефа папиллярных линий и/или температуры пальца.

В соответствии с количеством, характером и размещением ключевых точек генерируется уникальный цифровой код, который сохраняется в памяти базы данных. Время оцифровки и сверки отпечатка обычно не превышает 1-1,5 сек., в зависимости от размеров базы данных.

Этот метод один из наиболее надежных.

У продвинутых алгоритмов аутентификации – Veri Finger SKD показатели надежности составляют FAR – 0,00%…0,10%, FRR – 0,30%… 0,90%, – достаточно для надежной и бесперебойной работы системы в организации с персоналом более 300 человек.

Отпечатки пальцев Достоинства и недостатки.

Неоспоримыми достоинствами такого метода считается:

Высокая достоверность;

Более низкая стоимость устройств и их широкий выбор;

Простая и быстрая процедура сканирования.

Из основных недостатков следует отметить:

Папиллярные линии на пальцах легко повреждаются, вызывая ошибки в работе системы и блокируя проход служащим, имеющим на это право;

Дактилоскопические сканеры должны иметь систему защиты от подделанного изображения: температурные сенсоры, детекторы давления и т.п.

Производители.

Зарубежные компании, которые занимаются производством биометрических систем, устройств для СКУД и ПО к ним необходимо отметить:

SecuGen – мобильные компактные USB сканеры для доступа в ПК;

Bayometric Inc – производство биометрических сканеров различных типов для комплексных систем безопасности;

DigitalPersona, Inc – выпуск комбинированных сканеров-замков с интегрированными дверными ручками.

Компании СНГ, выпускающие биометрические сканеры и ПО к ним:

BioLink

Сонда

СмартЛок

Сканирование глаза

Радужная оболочка глаза, окончательно сформировавшись в два года, фактически не меняется на протяжении всей жизни.

Исключение составляют травмы и острые патологии болезней глаз.

Это один из наиболее точных методов аутентификации пользователя.

Устройства производят сканирование и первичную обработку данных 300-500 мс, сравнение оцифрованной информации на ПК средней мощности производится со скоростью 50000-150000 сравнений в сек.

Метод не накладывает ограничения на максимальное число пользователей. Статистика FAR – 0,00%…0,10% и FRR – 0,08%… 0,19% собрана на основе алгоритма EyR SDK компании Casia.

Рекомендуется использование таких систем допуска в организациях с численностью персонала более 3000 чел.

В современных устройствах широко используются камеры с 1,3 Мр матрицей, что позволяет захватывать во время сканирования оба глаза, это существенно повышает порог ложных или несанкционированных срабатываний.

Преимущества и недостатки

Преимущества:

Высокая статистическая надежность;

Захват изображения может происходить на расстоянии до нескольких десятков сантиметров, при этом исключается физический контакт лица с внешней оболочкой механизма сканирования;

Методы, исключающие подделку – проверка аккомодации зрачка,

практически полностью исключают несанкционированный доступ.

Недостатки:

Цена существенно выше, чем дактилоскопических;

Готовые решения доступны только в выполнении больших компаний.

Основные игроки на рынке

Основными игроками на рынке являются:

LG, Panasonic, Electronics, OKI, которые работают по лицензиям компании Iridian Technologies.

Наиболее распространенным продуктом с которым можно столкнуться на российском рынке являются готовые решения: BM-ET500, Iris Access 2200, OKI IrisPass.

В последнее время появились новые компании, заслуживающие доверия AOptix, SRI International.

Сканирование сетчатки глаза

Еще менее распространенный, но более надежный метод – сканирование размещения сети капилляров на сетчатке глаза. Такой рисунок имеет стабильную структуру и неизменен на протяжении всей жизни. Однако очень высокая стоимость и сложность системы сканирования, а также необходимость длительное время не двигаться, делают такую биометрическую систему доступной только для государственных учреждений с повышенной системой защиты.

Распознавание по лицу

Различают два основных алгоритма сканирования:

2D – наиболее неэффективный метод, дающий множественные статистические ошибки. Заключается в измерении расстояния между основными органами лица. Не требует использования дорогостоящего оборудования, достаточно только камеры и соответствующего ПО. В последнее время получил значительное распространение в социальных сетях.

3D – более точен, для идентификации объекту даже нет необходимости останавливаться перед камерой.

Сравнение с информацией, занесенной в базу производится благодаря серийной съемке, которая производится на ходу. Для подготовки данных по клиенту объект поворачивает голову перед камерой и программа формирует 3D изображение, с которым сличает оригинал.

Основные производители

Основными производителями По и специализированного оборудования на рынке являются:

Geometrix, Inc.,

Genex Technologies,

Cognitec Systems GmbH,

Bioscrypt.

Из российских производителей можно отметить
Artec Group,
Vocord,
ITV.

Сканирование руки

Также делится на два кардинально различных метода:

Сканирование рисунка вен кисти под воздействием инфракрасного излучения;

Геометрия рук – метод произошел от криминалистики и в последнее время уходит в прошлое.

Заключается в замере расстояния между суставами пальцев.

Сегментация биометрического рынка по методам идентификации.

8.4. Методы защиты информации от утечки через ПЭМИН

Защита информации от утечки через ПЭМИН осуществляется с применением пассивных и активных методов и средств.

Пассивные методы защиты информации направлены на:

ослабление побочных электромагнитных излучений (информационных сигналов) ОТСС на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

ослабление наводок побочных электромагнитных излучений в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

исключение или ослабление просачивания информационных сигналов в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Методы защиты информации от утечки через ПЭМИН.

Активные методы защиты информации направлены на:

создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала;

создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала.

Побочные токи и поля.

При функционировании технических средств обработки, приема, хранения и передачи информации (ТСПИ) создаются побочные токи и поля, которые могут быть использованы злоумышленником для съема информации.

Между двумя токопроводящими элементами могут возникнуть следующие виды связи:

через электрическое поле;

через магнитное поле;

через электромагнитное поле;

через соединительные провода.

Побочные токи и поля.

Основной характеристикой поля является его напряженность.

Для электрического и магнитного полей в свободном пространстве она обратно пропорциональна квадрату расстояния от источника сигнала.

Напряженность электромагнитного поля обратно пропорциональна первой степени расстояния.

Напряжение на конце проводной или волновой линии с расстоянием падает медленно.

Следовательно, на малом расстоянии от источника сигнала имеют место все четыре вида связи.

По мере увеличения расстояния сначала исчезают электрическое и магнитное поля, затем - электромагнитное поле и на очень большом расстоянии влияет только связь по проводам и волноводам.

Экранирование технических средств

Одним из наиболее эффективных пассивных методов защиты от ПЭМИ является экранирование.

Экранирование - локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами.

Различают три вида экранирования:

электростатическое;

магнитостатическое;

электромагнитное.

Электростатическое экранирование

Электростатическое экранирование заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю (на корпус прибора) с помощью контура заземления, сопротивлением не больше 4 Ом.

Применение металлических экранов весьма эффективно и позволяет полностью устранить влияние электростатического поля.

При правильном использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника сигнала в ε раз, где ε - относительная диэлектрическая проницаемость материала экрана.

Требования к электрическим экранам:

– конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;

– в области низких частот (при глубине проникновения (δ) больше толщины (d), т.е. при δ > d) эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;

– в области высоких частот (при d < δ) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование

При экранировании магнитных полей различают низкочастотные магнитные поля и высокочастотные.

Магнитостатическое экранирование используется для наводок низкой частоты в диапазоне от 0 до 3…10 кГц.

Низкочастотные магнитные поля шунтируются экраном за счет направленности силовых линий вдоль стенок экрана.

Рассмотрим более подробно принцип магнитостатического *экранирования*.

Магнитостатическое экранирование

Вокруг элемента (пусть это будет виток) с постоянным током существует магнитное поле напряженностью H_0, которое необходимо экранировать.

Окружим виток замкнутым экраном, магнитная проницаемость μ которого больше единицы.

Экран намагнитится, в результате чего создастся вторичное поле, которое ослабит первичное поле вне экрана.

Силовые линии поля витка, встречая экран, обладающий меньшим магнитным сопротивлением, чем воздух, стремятся пройти по стенкам экрана и в меньшем количестве доходят до пространства вне экрана.

Такой экран одинаково пригоден для защиты от воздействия магнитного поля и для защиты внешнего пространства от влияния магнитного поля созданного источником внутри экрана

Основные требования, предъявляемые к магнитостатическим экранам

Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

– магнитная проницаемость μ материала экрана должна быть возможно более высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);

– увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;

– стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;

– заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Электромагнитное экранирование

Электромагнитное экранирование применяется на высоких частотах.

Действие такого экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданными вихревыми токами обратного напряжения.

Этот способ *экранирования* может ослаблять как магнитные, так и электрические поля, поэтому называется электромагнитным.

Упрощенная физическая сущность электромагнитного *экранирования* сводится к тому, что под действием источника электромагнитной энергии на стороне экрана, обращенной к источнику, возникают заряды, а в его стенках – токи, поля которых во внешнем пространстве противоположны полям источника и примерно равны ему по интенсивности.

Два поля компенсируют друг друга.

Электромагнитное экранирование

Эффект *экранирования* проявляется из-за многократного отражения электромагнитных волн от поверхности экрана и затухания энергии волн в его металлической толще.

Отражение электромагнитной энергии обусловлено несоответствием волновых характеристик диэлектрика, в котором расположен экран и материала экрана.

Чем больше это несоответствие, чем больше отличаются *волновые сопротивления* экрана и диэлектрика, тем интенсивнее частичный эффект *экранирования* определяемый отражением электромагнитных волн

Выбор материала для экрана ПЭМИ

Металлические материалы выбирают по следующим критериям и условиям:

– необходимость достижения определенной величины ослабления электромагнитного поля при наличии ограничения размеров экрана и его влияния на объект защиты;

– устойчивость и прочность металла как материала.

– (сталь, медь, алюминий, латунь – обладают достаточно высокой эффективностью *экранирования*.)

– Недостатки листовых металлических экранов:

– высокая стоимость,

– большой вес,
– крупные габариты,
– сложность монтажа.

Этих недостатков лишены металлические сетки.

Достоинства: легче, проще в изготовлении и размещении, дешевле..

Недостаток металлических сеток: высокий износ по сравнению с листовыми экранами.

Выбор материала для экрана ПЭМИ

Для *экранирования* также применяются:

фольговые материалы (электрически тонкие материалы толщиной 0,01…0,05 мм).

Фольговые материалы в основном производятся из диамагнитных материалов – алюминий, латунь, цинк.

токопроводящие краски

(дешевые, не требуют работ по монтажу, просты в применении).

Токопроводящие краски создаются на основе диэлектрического пленкообразующего материала с добавлением в него проводящих составляющих, пластификатора и отвердителя (коллоидное серебро, графит, сажа, оксиды металлов, порошковую медь, алюминий).

Токопроводящие краски лишены недостатков листовых экранов и механических решеток, так как достаточно устойчивы в условиях резких климатических изменений и просты в эксплуатации.

Экранирование помещений.

Следует отметить, что экранироваться могут не только отдельные ТСПИ, но и помещения в целом. В неэкранированных помещениях функции экрана частично выполняют железобетонные составляющие в стенах. В окнах и дверях их нет, поэтому они более уязвимы. При экранировании помещений используются: листовая сталь толщиной до 2 мм, стальная (медная, латунная) сетка с ячейкой до 2,5 мм.

В защищенных помещениях экранируются двери и окна. Окна экранируются сеткой, металлизированными шторами, металлизацией стекол и оклеиванием их токопроводящими пленками. Двери выполняются из стали или покрываются токопроводящими материалами (стальной лист, металлическая сетка).

Особое внимание обращается на наличие электрического контакта токопроводящих слоев двери и стен по всему периметру дверного проема.

При экранировании полей недопустимо наличие зазоров, щелей в экране.

Размер ячейки сетки должен быть не более 0,1 длины волны излучения.

8.5 Применение физически неклонируемых функций

Многие современные товары содержат в себе электронные компоненты:

одежда, обувь, часы, ювелирные изделия, автомобили.

Потери от незаконного копирования потребительской электроники и электронных компонентов в составе других товаров достигли порядка 0,5 трлн долл. США в 2016г.

Решение проблемы - различные методы защиты цифровой электроники от нелегального копирования, модификации и обратного проектирования:

аппаратное шифрование (AES, RSA и др.),
хеширование (например, SHA-256, MD-5),
внедрение цифровых водяных знаков,
отпечатков пальцев в проектное описание,
лексическая и функциональная обфускация,
формальная верификация и другие.

Недостаток большинства методов – значительные аппаратные затраты и высокое энергопотребление.

Требования к площади, занимаемой цифровым устройством на кристалле интегральной схемы, а также к энергопотреблению становятся более жесткими, поскольку из года в год размер устройств значительно уменьшается.

Применение физически неклонируемых функций

Один из самых экономичных методов защиты с точки зрения аппаратных затрат — применение физически неклонируемых функций (ФНФ) (Physical Unclonable Functions, PUF).

Даже в серийном производстве каждый объект получается уникальным за счет погрешностей и случайностей.

Особенности каждого отдельного объекта можно регистрировать и использовать как уникальный идентификатор, своеобразный «отпечаток пальца».

ПРИМЕР:

В расплавленное стекло, добавим пузырьки воздуха, остудим эту массу и разрежем на одинаковые бруски. Шанс получить два абсолютно одинаковых бруска ничтожно мал, т.к. пузырьки воздуха внутри будут распределены неравномерно.

Проверка – преломление лазерного луча

Применение физически неклонируемых функций

ФНФ (PUF) для защиты электроники основаны на использовании вариаций технологического процесса (Manufacturing Process Variations) изготовления интегральных схем:

- ✓ точных значений пороговых напряжений,
- ✓ задержек распространения сигналов,
- ✓ частоты работы компонентов и т.п.

Разработчики цифровых устройств стремятся уменьшить влияние вариаций на конечный продукт. В случае ФНФ, напротив, данное

неконтролируемое явление используется для извлечения случайности и уникальности цифрового устройства. ФНФ похожи на хеш-функции, уникальность выходного значения ФНФ основана на уникальности конкретной интегральной схемы, а не на математическом алгоритме.

Входной аргумент ФНФ принято называть запрос (Challenge, CH), а выходное значение — ответом (Response, R).

Таким образом, для некоторой интегральной схемы ICk множество запросов {CH0, …, CHN-1} будет уникально отображено в множество ответов {R0, …, RN-1} с помощью ФНФ:

Ri=PUF(Chi)

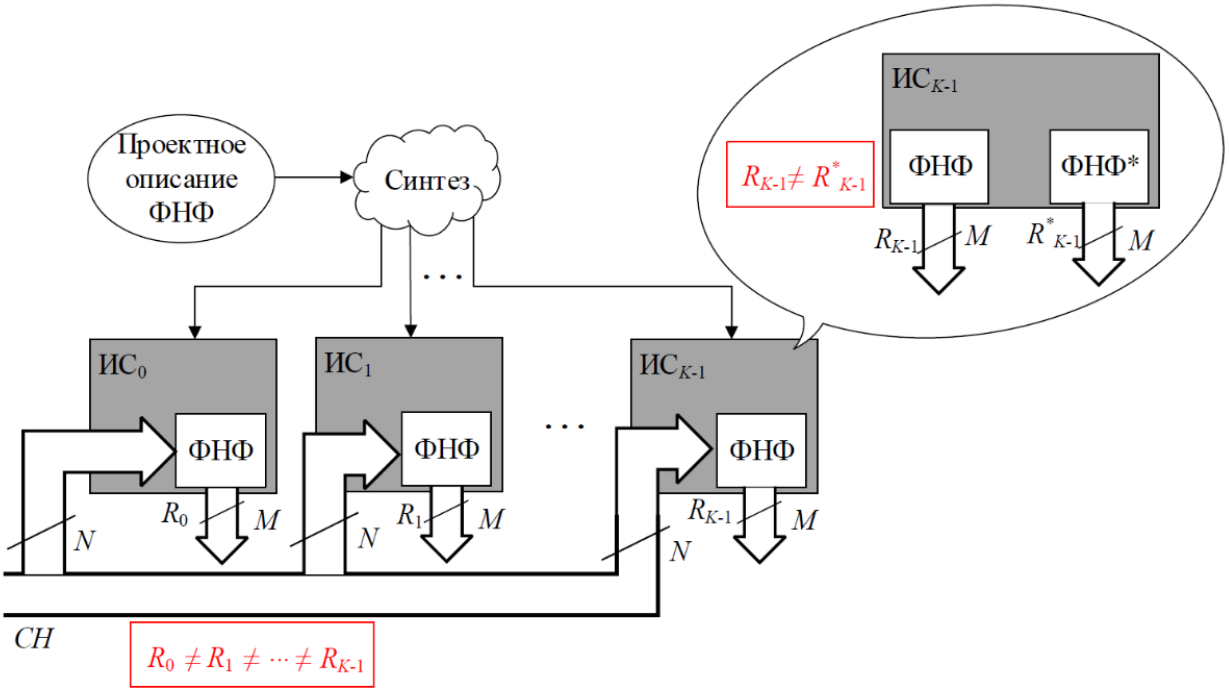

Рисунок 8.1. Применение физически неклонируемых функций

Множество пар запрос-ответ (Challenge-Response Pairs, CRP) {(CH0, R0), …, (CHN-1, RN-1)} уникально характеризует интегральную схему ICk и не может быть скопировано даже при условии использования абсолютно идентичного проектного описания.

Межкристальная и внутрикристальная уникальность интегральных схем (ИС)

Межкристальная уникальность: при реализации идентичного проектного описания ФНФ на различных ИС ответы Ri на одинаковый запрос CHi будут уникальны (значительно отличаться друг от друга) для каждой копии.

В случае использования идентичных реализаций ФНФ на одном кристалле для идентификации, например, различных компонентов интеллектуальной собственности (Intellectual Property, IP), наблюдается явление внутрикристальной уникальности.

Поскольку реализации ФНФ внутри кристалла различны как минимум по

взаимному расположению, внитрикристальная уникальность, как правило, более выражена, чем межкристальная.

Существующие реализации ФНФ и их применение.

В настоящее время существует множество реализаций ФНФ на основе:
Задержек распространения сигналов.

С помощью двоичного значения запроса задается конфигурация симметричных путей, по которым распространяются несколько копий одного сигнала.

Ответом ФНФ является результат сравнения задержек времени распространения сигналов.

Частоты работы компонентов.

Основа данной ФНФ — сравнение пар идентичных компонентов, частота которых является уникальной.

Запросами являются всевозможные пары индексов различных компонентов, а ответами — результат сравнения частоты их работы.

Состояние памяти.

В результате включения питания и/или сброса состояния статических запоминающих устройств (SRAM) значение, изначально хранимое в каждом из элементов памяти (0 или 1), является уникальным и случайным.

Запросом в данной ФНФ является включение/выключение питания, а ответом — наблюдаемое состояние каждого из элементов памяти, которое уникально характеризует интегральную схему, на которой ФНФ реализована.

Изображения на светочувствительной матрице.

Каждое изображение, создаваемое с помощью светочувствительной матрицы (Image Sensor) обладает постоянной составляющей шума, который характеризует уникальность реализованной матрицы.

Принцип работы данной ФНФ схож с ФНФ на основе сравнения частот с тем лишь отличием, что сравнение осуществляется по значениям порогового напряжения каждого из элементов матрицы.

Существующие реализации ФНФ и их применение

В настоящее время существует множество реализаций ФНФ на основе:
Токового зеркала. ФНФ данного класса основана на реализации массива токовых зеркал, значения напряжений в узлах которого уникально характеризуют интегральную схему. Запросом в данном случае являются номера столбцов и строк элементов, значения напряжений в которых необходимо сравнить. Ответом, соответственно, является результат сравнения разности напряжений в паре узлов с пороговым значением.

Силы давления пользователя на экран смартфона. В данной реализации ФНФ запросом является пользовательское действие, которое заключается в проведении пальцем по определенному рисунку (подобно графическому ключу в смартфонах). На основе значений силы давления пользователя на экран

смартфона вычисляется уникальное значение ответа, которое характеризует пользователя и смартфон и, таким образом, может быть использовано для аутентификации.

Структуры бумаги. Данная реализация ФНФ основана на уникальности структуры бумаги, обусловленной вариациями, вносимыми в нее в процессе производства. Соответственно, определенный бумажный носитель может быть использован в качестве источника уникальных криптографических ключей.

Пример ФНФ на основе памяти (SRAM).

Приведем пример реализации ФНФ на основе памяти с использованием ПЛИС Xilinx Spartan 3E, входящей в состав платы быстрого прототипирования Digilent Nexys-2.

Эмуляция элемента памяти была реализована в качестве бистабильного элемента, а включение/выключение питания было смоделировано с помощью перепрограммирования ПЛИС одним и тем же конфигурационном файлом.

На рисунке ниже показаны идентификаторы двух идентичных ПЛИС, полученные в результате их программирования одинаковым bit-файлом.

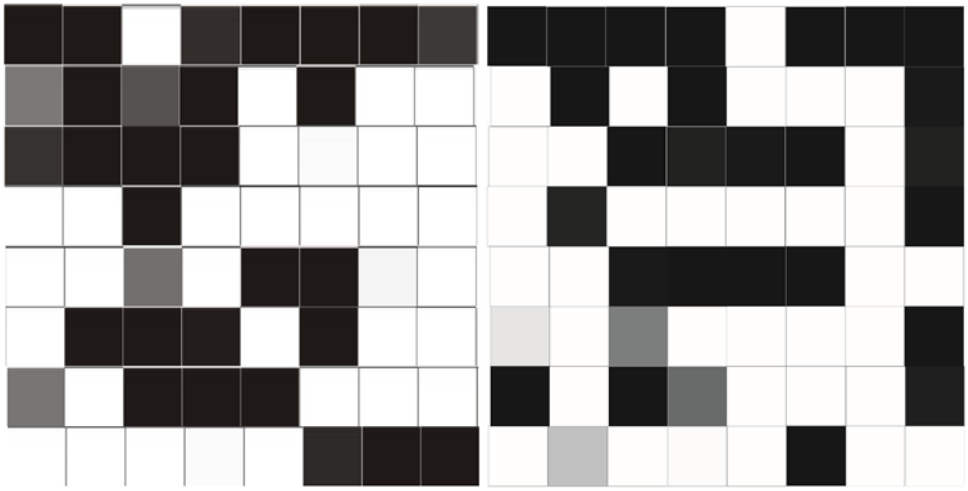

Рисунок 8.2. Идентификаторы двух идентичных ПЛИС

Черным цветом обозначены «элементы памяти», которые сохраняют значение 0 в результате 100 перепрограммирований, белым — сохраняющие значение 1. Оттенками серого обозначены те из них, которые меняют значение от запуска к запуску. Соответственно, чем больше в цвете «элемента» черного, тем больше значений 0 было выработано в результате перепрограммирования.

П64-разрядные идентификаторы двух идентичных ПЛИС

Как видно из рисунка, «карты памяти» отличаются значительно:

Хэммингово расстояние для 64-разрядных идентификаторов составляет порядка 20. Соответственно, вероятность того, что идентификатор будет одинаковым на различных ПЛИС достаточно мала (менее 0,01).

Приведенные выше «карты памяти» могут быть использованы двумя способами:

Для надежной идентификации потребуется использование кодов коррекции ошибок (Error Correction Codes, ECC) для стабилизации наблюдаемых «карт памяти». В данной работе был использован метод мажоритарного выбора.

Для реализации генератора случайных чисел, напротив, требуется «размножение» случайности тех «элементов памяти», значения которых нестабильны. С этой целью был использован сигнатурный анализ в качестве схемы сжатия данных с потерями. Также могут быть использованы стандартные алгоритмы хеширования (например, SHA-256), если ограничения по аппаратурным затратам не столь жесткие.

Применение физически неклонируемых функций

Первой коммерческой реализацией ФНФ в 2008 были радиочастотные идентификаторы, изготовленные компанией Verayo.

Также в настоящее время многие производители используют ФНФ в качестве встроенного неклонируемого идентификатора ПЛИС.

FPGA, Xilinx и Altera (Intel) и др.

Поскольку ФНФ используются в качестве криптографических примитивов (генераторов случайных чисел, уникальных идентификаторов, аппаратных хеш функций), многие производители не раскрывают факт использования ФНФ, чтобы хранить в тайне детали реализации их протоколов безопасности от злоумышленников.

Применение физически неклонируемых функций

Проблемы ФНФ:

Нестабильность некоторых из значений, что, в свою очередь, вынуждает разработчика прибегать к кодам коррекции ошибок и более надежным архитектурам ФНФ.

С другой стороны, наличие очень высокой стабильности подвергает ФНФ риску криптографической атаки с помощью методов машинного обучения.

Перспективы ФНФ:

Использование ФНФ в современных коммерческих приложениях в качестве криптографического примитива доказывает перспективность исследований в области поиска новых архитектур ФНФ, а также усовершенствования характеристик существующих реализаций.