Защита музыкальной информации на SACD.

Эссе подготовил студент 012гр. Чудновец Андрей

Super Audio CD (SACD) – новый формат, который был разработан фирмами Sony и Philips. Основные его отличия от CD - это улучшенное качество звука и лучшая защищённость от копирования и ошибок .

Качество звука улучшено за счёт нового способа кодирования аналогового сигнала (DSD). По мнению меломанов, именно PCM-кодирование, которое используется в CD и DVD-Audio, делает звучание искусственным, непохожим на магнитную ленту и винил. С помощью такого формата можно бы было скопировать имеющиеся магнитные ленты в студиях на цифровой носитель, не разрушающийся со временем, абсолютно без потери качества.

Стандарт был “выпущен в свет” в сентябре 1999 года.

Вот некоторые из данных сравнения его с CD и DVD-Audio:

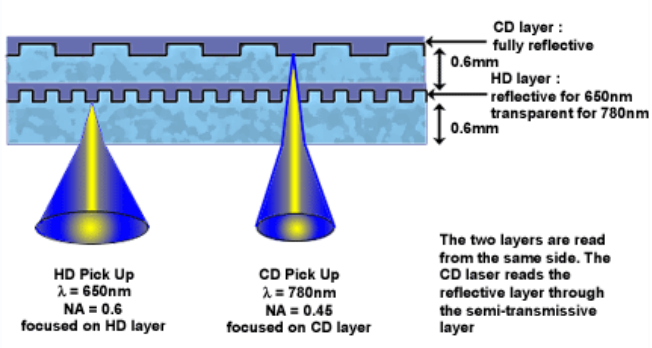
Сравнение звуковых форматов

	DVD-Audio	**SACD**	**CD**
Объем одного слоя диска, GB	4,7	4,7	0,7
Динамический диапазон, db	>120	144	96
Частота дискретизации, кГц	44,1 - 192	2 822,4	44,1
Разрядность, бит	16/20/24	1	16
Основной аудиосигнал	PCM	DSD	PCM
Воспроизводимый диапазон, Гц	5 - 96 000	2 - 100 000	5 - 20 000
Цифровой выход	Да	нет	да
Защита данных	Да	многоступенчатая	нет

SACD – схожи с обычными DVD тем, что у них тот же размер сектора, тот же метод коррекции ошибок и модуляция и та же файловая система (UDF плюс ISO 9660).

Гибридные диски.

SACD содержит 2 слоя, позволяющие сделать SACD двойной плотности или так называемые гибридные диски. Один слой – SACD звук, другой – обычный CD. Такие диски могут играться на обычных приводах, но будет качество обычного CD, так как читается только слой CD.



DSD (Direct Stream Digital)

Основное отличие SACD от других форматов – новый способ кодирования аналоговой информации – DSD. Главная идея DSD – убрать промежуточные этапы, использующиеся в PCM – кодировании, потенциально ухудшающие качество звука (интерполяция и прореживание).

Основными преимуществами нового способа кодирования являются:

- Прямая запись на диск информации, полученной из аналогового сигнала и представленной в виде 1-битных сэмплов.
- Частота дискретизации 2.8224 MHz приводит к гораздо лучшей частотной характеристике и большему динамическому диапазону, чем были возможны на CD.

Рассмотрим **защиту информации на SACD** с двух точек зрения:

1.Защита от нарушения целостности – т.е. как происходит кодирование, позволяющее корректировать ошибки. Ошибки могут возникнуть, например, при каком то физическом воздействии на диск, например царапины.

2.Защита от несанкционированного копирования.

1.Защита от нарушения целостности.

Пусть у нас уже есть звуковая информация в цифровом виде. Рассмотрим логическую структуру её записи на диск.

Область данных на диске разбивается на секторы. Сектор (данных) – наименьшая адресуемая часть дорожки, к которой можно обращаться независимо. Группу секторов также называют ECC-блок. Длина сектора – 2064 байт. Из них 2048 – музыкальные данные, 12 байт – ID – идентификационные данные, и 4 байта – EDC- Error Detection Code – дополнительный код для обнаружения ошибки.

После записи такого сектора к каждой группе из 16 секторов добавляется дополнительные байты кода Рида Соломона, нужные для восстановления ошибок (Reed-Solomon error correcting codes). В итоге формируются ECC-блоки с добавочными байтами чётности PI (inner-code parity) и PO (outer-code parity). Секторы, которые реально записываются на диск, получаются перемешиванием PO-строк в ECC-блоке и разбиением снова на 16 секторов.

В конце ещё используется EFM+ channel modulation, но это не имеет отношения к защите.

Как показано в табличке, первая часть сектора содержит ID, а также 2 дополнительных байта для восстановления ошибки в ID.

Identification Data (ID)	4 bytes
ID Error Detection (IED)	2 bytes
Зарезервировано	6 bytes
Главные данные	2048 bytes
Error Detection Code (EDC)	4 bytes

В CD-формате использовались ещё данные синхронизации, и был дополнительный ECC-слой. Тут этого не надо, благодаря синхронизации, которая присутствует в EFM-модуляции.

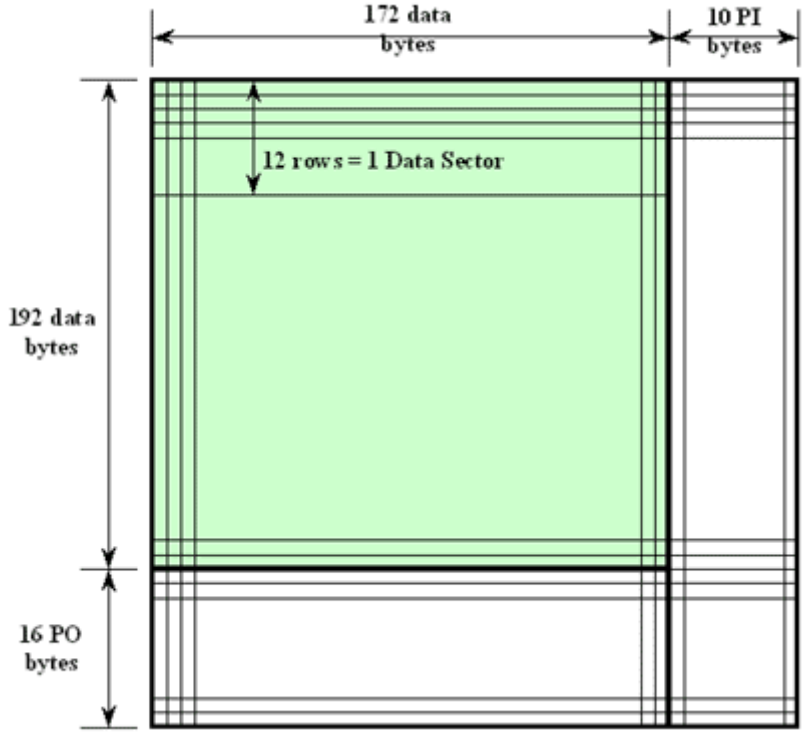
EDC поддерживается, так как он даёт простой и мощный способ обнаружения ошибки на уровне сектора.

SACD использует коды Рида-Соломона для восстановления ошибок. Такое кодирование можно применить к большому объёму данных с большими возможностями

восстановления. Это уменьшает избыточность ECC-кода примерно до 13 %, что примерно в 2 раза меньше, чем на CD.

После вычисления EDC над секторами, ECC применяется к 16 секторам данных, или одному ECC-блоку. (33024 байта).

Представим данные ECC-блока в виде матрицы 192 строки на 172 столбца. Добавляются 16 байт PO-чётности к каждому столбцу. Потом 10 байт PI-чётности добавляются к каждой из получившихся 208 строк. Получается Reed-Solomon Product Code – RSPC.



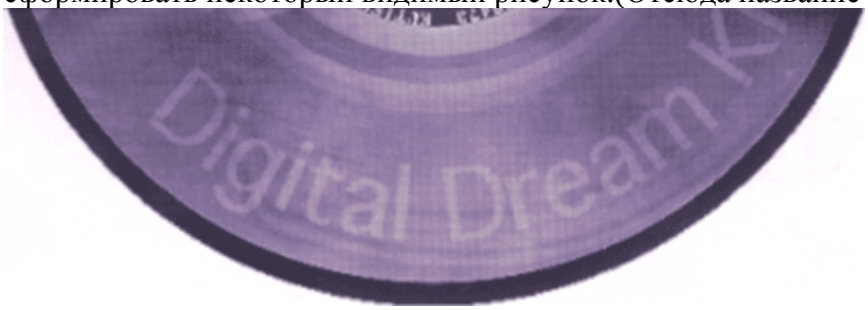
Такой код может восстановить как минимум 5 ошибок байта в каждой строке и как минимум 8 ошибок байта в каждом столбце.
Применяя несколько чередующихся вычислений над строками и столбцами, можно восстановить гораздо большие объёмы ошибок!
Далее, PO-строки перемешиваются с обычными строками. А именно идут 12 обычных, одна PO, и т.д. Потом всё разбивается на 16 секторов. Каждый уже будет содержать 2366 байт.

Данный метод кодирования эффективнее и менее избыточен, чем тот, что используется в CD-формате.

2.Защита от копирования.

Для начала кратко рассмотрим систему водяных знаков, которая применяется на SACD – Digital Watermarking.
Водяные знаки – это некоторые данные, встроенные в полезные звуковые данные. Был разработан способ, как включить в знаки информацию о защите прав, так, чтобы их трудно было убрать, и чтобы это не повлияло ни на сами исходные данные, ни на коды ECC. Т.е. фактически придуман полностью прозрачный Digital Watermarking.
Его суть – в модуляции ширины углублений, составляющих дорожки на поверхности SACD. Чтобы сделать копию такого диска, надо иметь специальное оборудование, умеющее это делать. Такое оборудование предусмотрительно лицензировано.

Кроме того, модуляция ширины углублений может быть сделана так, что можно сформировать некоторый видимый рисунок.(Отсюда название – водяные знаки):



Это тоже можно использовать, например для лейбла фирмы, выпустившей диск.

Защита содержимого SACD обеспечивает :
-Защиту против пиратов, копирующих коммерческие диски, и подделок.
-Защиту против нелегального копирования потребителем, т.е. побитовых копий например на DVD-R
-Возможность записи SACD в студиях и авторских системах.

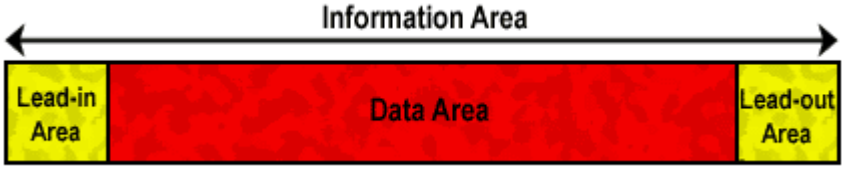
Для начала, надо знать, что полезные данные на диске – заскремблированы специальным синхронным потоковым шифром. Выбор ключей для него основан на сдвиговых регистрах, контролируемых часами. Этот алгоритм оптимизирован так, чтобы он быстро выполнялся в аппаратуре. Рассмотренный код для восстановления ECC добавляется уже к заскремблированным данным.

A.Защита содержимого диска

Защита данных на SACD – пятисторонняя. Каждая сторона ставит различные препятствия против нелегального копирования.
Эти средства защиты до некоторой степени независимы, т.е. если одну из них сломать, то остальные будут продолжать работать.

Первое. Существующие дисковые приводы для ПК не смогут прочесть SACD.

Логическая структура диска такова:



Видно, что есть некоторая область Lead-in area. Она, как и обычные данные, использует ECC. Но в качестве данных в некоторых байтах используются нули, а в некоторых – заскремблированная скрытая информация, параметры, которые необходимы для инициализации чтения.
Эта область недоступна на программном уровне, а читается и расшифровывается незаметно внутри привода SACD. Ключ для расшифрования (дескремблирования) зашит в аппаратуре. Приводы, которые не лицензированы для чтения SACD, не смогут прочесть SACD и отвергнут его. Эта технология называется “SACD mark”. Лицензированные приводы могут читать SACD, но должны выполнять правила защиты, которые определены в лицензионном соглашении.

SACD mark – это значительное препятствие для хакеров, имеющих целью сломать скремблирующую систему в SACD, т.к. они не могут получить образ диска – его не читают даже новейшие DVD+-RW приводы.

Второе. Если даже и скопировать данные с SACD, их нельзя будет использовать.
Наиболее серьёзной дырой в защите от копирования является случай, когда потребители делают побитовое копирование в образ или на болванку. Такой диск можно бы было проигрывать на обычном оборудовании, если копия содержит ключи, нужные для дескремблирования.
На SACD система защиты основана на ключах, которые расположены в lead-in. Хотя эта область и недоступна обычным программам, теоретически возможно модифицировать записывающее устройство так, что можно будет прочесть и записать данные в эту область. Тогда можно будет безгранично делать любые копии.
Против этого недостатка были приняты меры так, чтобы побитовая копия была нечитаема на SACD-плеере. Для этого и используется Digital Watermarking, а именно невидимые водяные знаки. Система называется “Pit Signal Processing Physical Disc Mark”, или “PSP-PDM”,). Информация, содержащаяся в PSP-PDM, содержит часть ключа для дескремблирования аудио-информации на диске. Другая часть содержится в аппаратуре.
Потребительские рекордеры НЕ МОГУТ писать PSP-PDM. Мастеринг таких знаков делается только на специальном лицензированном оборудовании. Отсутствие этого знака делает невозможным проигрывание диска, полученного полным побитовым копированием, так как теперь отсутствует часть ключа, нужного для дескремблирования.
Кроме того, PSP-PDM содержит некоторую информацию о защите прав. Если её нет, или она видоизменена, то сделано так: Диск начнёт проигрываться, но через несколько секунд просто открывается привод SACD и всё. Такая система уже доказала свою эффективность.
И ещё, PSP-PDM просто должно присутствовать в каком-то виде, иначе даже заскремблированные данные просто не будут читаться!

Третье. Взлом скремблирования заголовка является очень дорогим.
Пусть заскремблированные данные могут быть прочтены. Поиск ключа полным перебором занял бы слишком много времени даже на супер-современных компьютерах.
Для дескремблирования нужен 80-битный ключ. Кроме как перебором, эти биты трудно получить, т.к. они никогда не появляются ни на какой шине и ни на каком проводе связи в приводе, даже в заскремблированном виде. Некоторые биты скрыты в “железе” в приводе, другие содержатся в PSP-PDM на самом диске.
Поиск ключа требуется повторять для каждой отдельной области данных на SACD, т.к.он каждый раз разный.
На диске нет какого-нибудь поля типа media-key-block или album-id , которое можно бы было прочесть, а потом взломать с помощью специального программного обеспечения.

Четвёртое. Детали скремблирующей системы являются закрытыми.
Дескремблирующий алгоритм заложен в железе. Лицензия не позволяет встроить его в программу. Таким образом, нет смысла передавать ключи для скремблирования из привода в программу. Это устраняет общую утечку в защите. Более того, этот алгоритм доступен лицензированным производителям только в виде защищённого блока в железе – некоторой платы.

Пятое. Сложная защита против подделок.
Средства форматирования SACD и PSP-PDM- кодеры не будут доступны на открытом рынке. Следовательно, будет невозможно нелицензированным производителям пересоздать SACD, просто оцифровав аналоговые данные на выходе. Форматеры и кодеры будут даваться в аренду только лицензированным производителям, а продаваться

– никогда. Т.о. не будет рынка, где можно будет купить хотя бы уже использованное устройство.

B.Защита содержимого CD-DA.

CD слой на гибридном диске защищён обычным способом, как защищаются все CD. Но для дополнительной защиты можно сделать сильный водяной знак сигнала, использующий схему SDMI, препятствующую нелегальному использованию.

C.Хорошее решение для шин для защиты цифровых сигналов высокого разрешения. – дополнительная защита DTCP.

SACD – привод имеет только аналоговый выход. Стандартный цифровой интерфейс возможен, но не будет позволен до тех пор, пока не будет достигнуто соглашение о надёжной защите передаваемых по этому интерфейсу данных.

Сейчас - в версии SACD 1.2 передача цифровых данных между приводом и ЦАП происходит с помощью некоторого интерфейса IEEE 1394, который защищён патентом, разрешающим использовать его, только если передаваемые данные нигде не записываются.

D.Управление копированием в системах творческой деятельности и студиях.

Это управление можно осуществлять по разному, но важно то, SACD формат можно записать с помощью профессионального студийного программного обеспечения. Такие инструменты могут быть сделаны только в кооперации между лицензерами SACD и музыкальной индустрией. Такая лицензия должна гарантировать, что эти инструменты ни в коем случае не будут использоваться для пиратства.

E.Развитие системы защиты SACD.

Система защиты SACD содержит заготовки на будущее. Примеры улучшений, которые ещё можно ввести – Водяные знаки сигналов (signal watermarks) и дополнительные знаки на диске (physical disc marks).

SACD – яркий пример того, что можно соединить эффективную систему защиты от копирования с высокотехнологичным аудио-форматом, который никак не изменяется этой системой, и таким образом, может передавать оригинальную музыку в тончайших деталях.

The end.

Использованные источники:

1.Super Audio CD Web Site.
http://www.superaudio-cd.com/
2.SACD web sites of Sony.
http://www.sonymusic.com/sacd/
http://interprod5.imgusa.com/son-637/technology.asp
3.Digital Audio Industrial Supply (DAISy) web site.
http://www.daisy-laser.com/technology/techsacd/techsacd.htm
4.SACD web site of Philips.
http://www.sacd.philips.com/d_technology.php
5. Deluxe Global Media Services web site
http://www.disctronics.co.uk/technology/dvdaudio/dvdaud_sacd.htm
6. “Super Audio CD Moves Ahead” *by Richard Elen, August 24, 2000*
http://www.ambisonic.net/sacd0800.html
7.Сайт “Super Audio CD в России”
http://www.sacd.ru/format.htm