Королевский институт управления, экономики и социологии

«Криптографическая защита информации »

Специальность № 090103

“Организация и технология защиты информации”

Поточные системы шифрования

- Синхронизация поточных шифрсистем
- Принципы построения поточных шифрсистем
- Шифрсистема A5

Сравнение блочных и поточных шифрсистем

Недостатки блочных шифров

- эффект размножения ошибок, снижающий эксплуатационные качества шифра.
- возможность применения *метода анализа "со словарем"* в режиме простой замены связан.

Такими недостатками не обладают поточные шифры, осуществляющие позначное шифрование в алфавитах небольшой мощности. Кроме того, существующая практика показывает, что пока лишь поточные шифры обеспечивают максимальные скорости шифрования. Это важно при магистральном шифровании больших потоков информации.

Эти, а также многие другие соображения делают поточные шифры в некоторых ситуациях более предпочтительными, чем блочные.

Проблема синхронизации в поточных шифрсистемах

Потеря (или искажение) отдельных знаков шифрованного текста при использовании поточных шифров простой замены приводит к локальным потерям: все знаки шифртекста, принятые без искажений, будут расшифрованы правильно (т.к. алгоритм шифрования не зависит ни от расположения знаков в тексте, ни от их конкретного вида).

Многоалфавитные поточные шифры также не размножают ошибок при искажении отдельных знаков шифрованного текста, но оказываются неустойчивыми к пропускам знаков шифрованного текста, т.к. это приводит к неправильному расшифрованию всего текста, следующего за пропущенным знаком.

Учитывая наличие помех практически во всех каналах передачи данных, в системах криптографической защиты, использующих поточное шифрование, приходится заботиться о согласованном порядке применения преобразований при зашифровании и расшифровании, другими словами, решать проблему *синхронизации* процедур зашифрования и расшифрования.

Способы решения проблемы синхронизации в поточных шифрсистемах

- *синхронные* системы;
- системы *с самосинхронизацией.*

Свойства синхронных поточных шифрсистем

- Выбор применяемых шифрующих преобразований однозначно определяется распределителем и зависит только от номера такта шифрования.
- Каждый знак шифртекста зависит только от соответствующего знака открытого текста и номера такта шифрования и не зависит от того, какие знаки были зашифрованы до или после него.
- Поэтому применяемое при расшифровании преобразование не зависит от последовательности принятых знаков шифртекста. В этом случае размножение ошибки полностью отсутствует: каждый знак, искаженный при передаче, приведет к появлению только одного ошибочно расшифрованного знака.

Недостатки и способы их устранения в синхронных поточных шифрсистемах

Потеря знака шифртекста приводит к нарушению синхронизации и невозможности расшифрования оставшейся части сообщения.

Для таких систем необходимо предусмотреть специальные процедуры восстановления синхронности работы.

Синхронизация достигается:

Вставкой в передаваемое сообщение специальных *маркеров.* В результате этого знак шифртекста, пропущенный в процессе передачи, приводит к неверному расшифрованию лишь до тех пор, пока не будет принят один из маркеров.

Реинициализацией состояний, как шифратора отправителя, так и шифратора получателя при некотором

Свойства поточных шифрсистем с самосинхронизацией. Примеры режимов работы

Возможность производить правильное расшифрование и в том случае, когда синхронизация передающего и приемного шифраторов нарушается вследствие потери знака шифртекста.

Наиболее распространенный режим использования шифрсистем с самосинхронизацией — это режим **обратной связи по шифртексту**, при котором текущее состояние системы зависит от некоторого числа *N* предыдущих знаков шифртекста.

В этом режиме потерянный в канале знак влияет на *N* последовательных состояний. После приема *N* правильных последовательных знаков из канала связи состояние приемного шифратора становится идентичным состоянию

Принципы построения поточных шифрсистем. Классификация

Наиболее распространены:

Эндоморфные поточные многоалфавитные шифры замены с множествами шифрвеличин и шифробозначений, совпадающих с алфавитом открытых сообщений.

Математическая модель поточных шифрсистем

A — алфавит открытых сообщений, совпадающий с множествами шифрвеличин и шифробозначений

$\{\varphi_a: A \to A\}$ — совокупность из r биекций множества A

$x=a_1,a_2,\ldots a_l$ — произвольный открытый текст

$k \in K$ —выбранный ключ зашифрования.

Пусть $\psi(k,l) = a_1^{(k)} \square\ a_j^{(k)} \qquad a_l^{(k)} \in N_r,\ j = \overline{1,l}$

является распределителем, отвечающим данным значениям $k \in K$, $l \in N$,

Где $\psi : K \times N \to N_r^*$ — некоторое отображение в множество $N_r=[1,2,\ldots,r]$.

Тогда правило зашифрования $E_k(x)$ определяется формулой $E_k(x)= y$, где $y=b_1,b_2\ldots b_l$ и $b_j = \varphi_{a_j^{(k)}}(a_j),\ j = \overline{1,l}$

Таким образом, задача построения рассматриваемого шифра сводится к выбору множества шифрующих преобразований $\{\varphi_a\}$ и отображения ψ, задающего распределитель.

Архитектура поточных шифрсистем

Выделяют два основных блока, отвечающих за выработку распределителя и собственно зашифрование очередного знака открытого текста.

Управляющий блок- вырабатывает последовательность номеров шифрующих преобразований, то есть фактически управляет порядком процедуры шифрования.

Вырабатываемую им последовательность номеров преобразований называют *управляющей последовательностью (или управляющей гаммой).*

Шифрующий блок - реализует собственно алгоритм зашифрования текущего знака в соответствии со знаком управляющей последовательности .

Архитектура поточных шифрсистем

Обычно управляющая гамма представляет собой псевдослучайную последовательность, удовлетворяющую некоторой рекуррентной зависимости. В общем случае, рекуррентная последовательность (на заданном множестве *A*) определяется формулой

$$x(i+m) = f(x(i), \square\ , x(i+m-1)), i \geq 0$$

в которой $f : A^m \rightarrow A$ — некоторая функция от *m* переменных.

Архитектура поточных шифрсистем

Для получения рекуррентных последовательностей используются различные *датчики псевдослучайных чисел.*

В настоящее время большинство датчиков псевдослучайных чисел, в том числе реализованных в программных продуктах ведущих фирм, построены на основе регистров сдвига с линейными функциями обратной связи, или коротко — *линейных регистров сдвига* (ЛРС).

Требования, предъявляемые к блокам поточной шифрсистемы,

Требования к управляющему блоку:

— период управляющей гаммы должен превышать максимально возможную длину открытых сообщений, подлежащих шифрованию;

— статистические свойства управляющей гаммы должны приближаться к свойствам случайной равновероятной последовательности;

— в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками;

— криптографический алгоритм получения знаков управляющей гаммы должен обеспечивать высокую сложность определения секретного ключа.

Требования, предъявляемые к блокам поточной шифрсистемы,

Требование к шифрующему блоку:

— применение алгоритма шифрования должно носить универсальный характер и не зависеть от вида шифруемой информации.

Дополнительное требование:

— способ построения шифрующего блока должен обеспечивать криптографическую стойкость шифра при перекрытиях управляющей гаммы, в частности при повторном использовании ключей.

Задачи обеспечения безопасности в современных СПРС

- аутентификация пользователей;
- конфиденциальность информации;
- скрытность перемещения и неотслеживаемость соединений абонента.

Все задачи реализуются с помощью соответствующих криптографических алгоритмов:

A3 - алгоритм аутентификации («прошит» в SIM-карте);

A8 - алгоритм формирования ключа шифрования («прошит» в SIM-карте);

A5 - алгоритм шифрования/дешифрования сообщений. (прописан в телефоне).

История создания и развития

Французские ВС создали поточный шифр для использования в военных целях.

В конце 80х для стандарта GSM потребовалось создание новой, современной системы безопасности.

В её основу легли три секретных алгоритма: A3, A8 и A5 (французская разработка).

Экспорт стандарта из Европы не предполагался, но вскоре в этом появилась необходимость.

A5 -переименовали в A5/1 для распространения в Европе и США

A5/2 - экспортный вариант для остальных стран (в том числе и России) – модификация с пониженной криптостойкостью.

A5/0 - шифрование отсутствует

A5/3 – основан на алгоритме Касуми и утверждённый для использования в сетях 3G

История создания и развития. Появление в широком доступе

В основе A5 принцип Security by Obscurity (Безопасность упрятыванием)

Т.е. алгоритмы труднее взломать, если они не доступны публично.

Данные предоставлялись операторам GSM только по необходимости.

Тем не менее, детали алгоритма A5 были известны: британская телефонная компания

British Telecom передала всю документацию Брэдфордскому университету без соглашения о неразглашении информации.

К 1994 году :

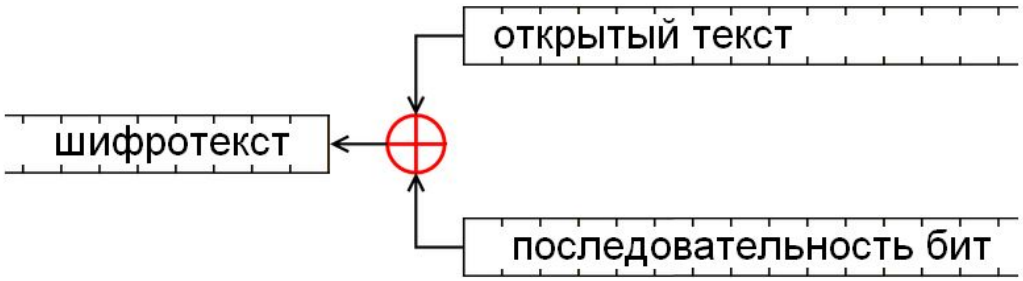
- материалы о стандарте появились на конференции в Китае.

- Ross Anderson и Michael Roe из Кембриджа опубликовали криптосхему и дали оценку её криптостойкости

Полный алгоритм был представлен Йоваком Голичем на Eurocrypt'97

Принципы A5

В основе A5 – потоковое шифрование



Принципы A5

- Увеличения быстродействия - только простейшие операции: (XOR) и сдвиг регистра
- Сложения потока открытого текста с гаммой
- Зависимость безопасности системы от свойств гаммы
- Генерация гаммы на основе сессионного ключа

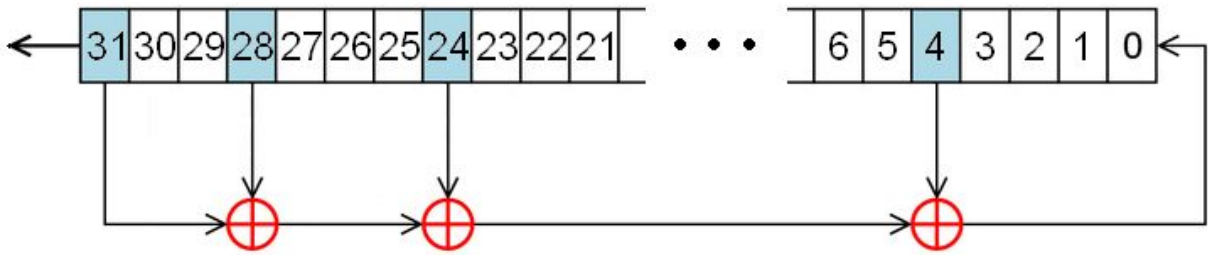
Принципы А5. РСЛОС

Состав РСЛОС:

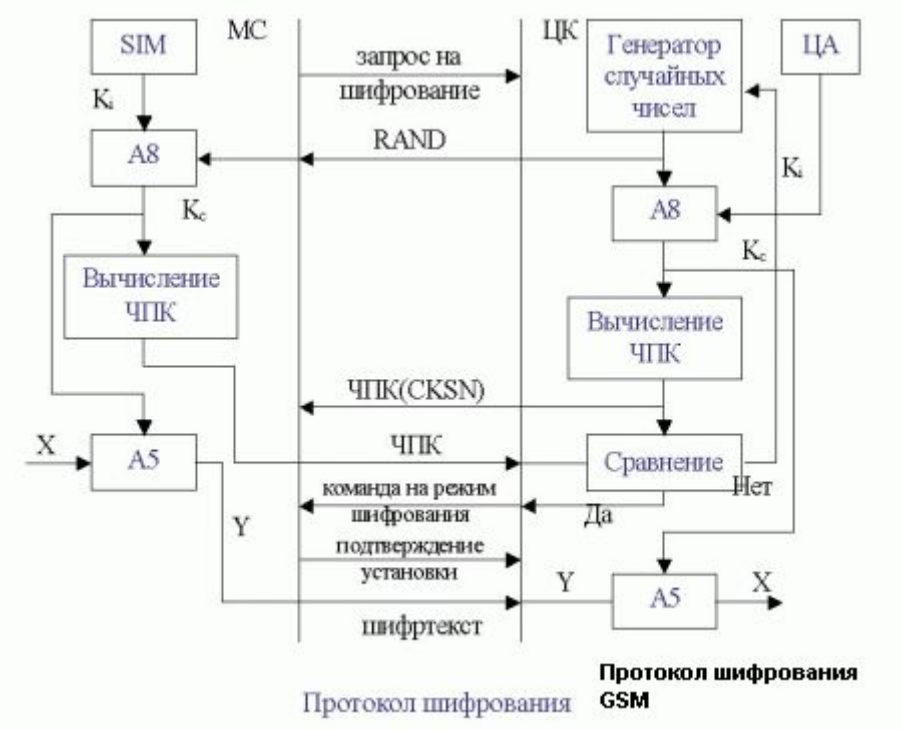
- Регистр
- Обратная связь

Принцип действия:

- крайний левый бит (старший бит) извлекается
- последовательность сдвигается влево
- в опустевшую правую ячейку (младший бит) записыва
связи.



Использование A5 в GSM. Этапы работы



Использование A5 в GSM. Этапы работы

При регистрации мобильной станции (МС) сеть выделяет ей секретное число ki, которое хранится в SIM.

МС посылает запрос на шифрование.

Центр коммутации (ЦК) генерирует случайное число RAND, которое передается на МС и используется на обеих сторонах для вычисления единого сеансового ключа Kc по A8.

Т.к. возможно искажение RAND, и ключ на МС будет отличаться от вычисленного ЦК, то для проверки идентичности ключей вычисляется ЧПК

После подтверждения правильности установки ключей производится поточное шифрование данных по A5

Использование A5 в GSM. Работа РСЛОС

В GSM – одна посылка каждые 4.6 мс

Каждый кадр состоит из 114-ти бит информации от Абонента к Базовой станции и 114-ти бит от Базовой станции к Абоненту

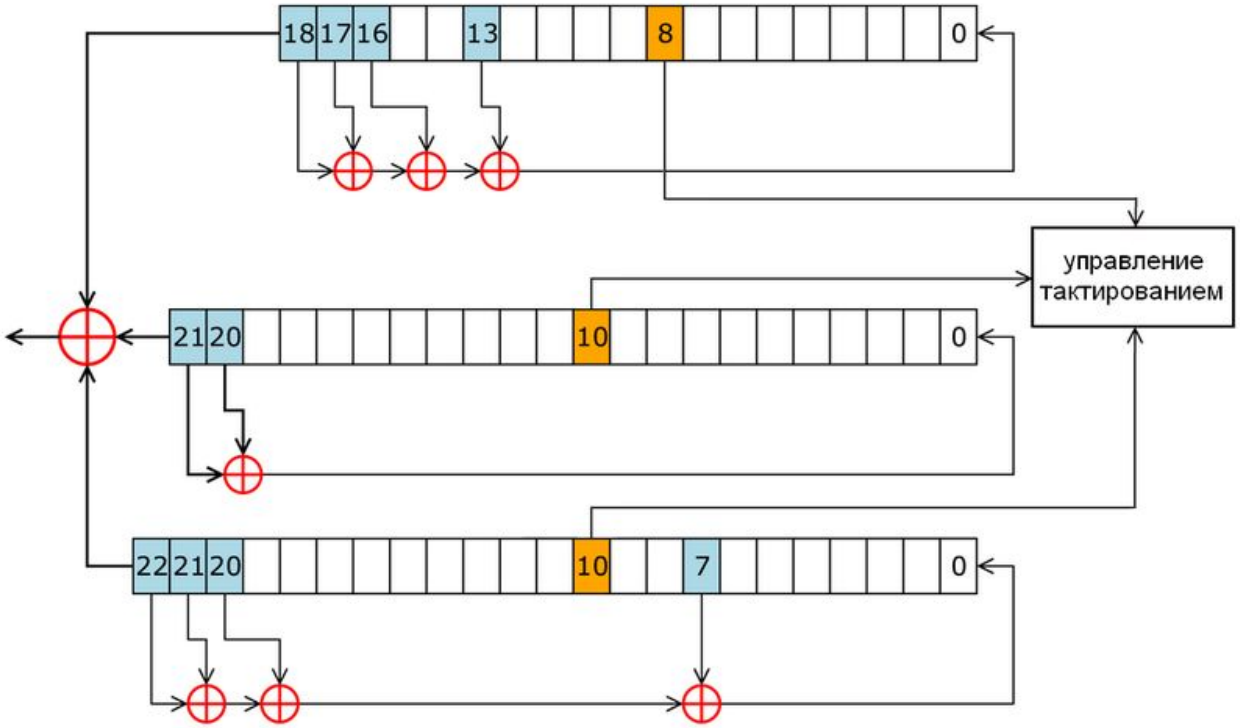
Каждый новый разговор может быть зашифрован новым сессионным ключом K

Для шифрования каждого кадра используется сессионный ключ K (64 бита) и номер кадра Fn (22 бита)

(для начальной инициализации генератора псевдослучайной последовательности)

Биты с выхода генератора используют для операции XOR с передаваемым сообщением

Использование A5 в GSM. Работа РСЛОС



Характеристики РСЛОС:

- Длина регистров
- Биты обратной связи
- Операция по расчету нулевого бита
- Управление сдвигом

Использование A5 в GSM. Работа РСЛОС

Три регистра R1, R2 и R3 с длинами 19, 22 и 23 бита

Самый младший бит регистра называется нулевым битом. Обратная осуществляется битами связи:

-в R1 – 13, 16, 17, 18

-в R2 – 20, 21

-в R3 – 7, 20, 21, 22

При сдвиге регистра значения битов обратной связи подвергается операции XOR и результат записывается в нулевой бит сдвинутого регистра

Управление сдвигом регистров происходит с помощью мажоритарного правила: каждый регистр имеет один бит «синхронизации» (бит 8 для R1, бит 10 для R2 и бит 10 для R3). Каждый такт вычисляется функция от трёх битов синхронизации $F(x,y,z)=x*y+x*z+y*z$ и на данном такте сдвигаются только те регистры, в которых биты синхронизации совпадают с F.

Использование A5 в GSM. Работа РСЛОС

Мажоритарная функция

Булевы функции трех аргументов

Таблица

x_1	x_2	x_3	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Функции трех аргументов задаются на восьми наборах. Количество функций трех аргументов равно $2^8 = 256$.

Одной из функций трех аргументов является мажоритарная функция. Таблица истинности этой функции имеет следующий вид (табл. 3).

Функция равна 1, если во входном наборе два или три аргумента принимают значение 1, и равна 0 в остальных случаях. Эта функция обладает корректирующей способностью, поэтому на заре развития вычислительной техники были работы, в которых рекомендовалось все комбинационные схемы строить на мажоритарных элементах.

спользование A5 в GSM. Процесс .энерации (~ алгоритм, структура)

- Все регистры равны нулю. Сессионный ключ K (64 бита) и номер кадра Fn (22 бита)
- 64 такта (без управления сдвигом). На каждом такте каждый бит K (от младшего к старшему) XOR с младшим битом каждого регистра
- 22 такта (без управления сдвигом), причем младшие биты регистров XOR с битами Fn (от младшего к старшему). Окончание этого шага называется начальным состоянием кадра.
- 100 тактов с управлением сдвигом, но без генерирования выходной псевдослучайной последовательности
- 228 тактов с управлением сдвигом и генерируются 228 бит выходной последовательности. На каждом такте генерируется один выходной бит как XOR старших битов трёх регистров
- Инициализация производится заново, используется новый номер кадра

Использование A5 в GSM. Процесс генерации (альтернативное описание)

- три регистра(R1, R2, R3) имеют длины 19, 22 и 23 бита,
- многочлены обратных связей:
  - $X^{19} + X^{18} + X^{17} + X^{14} + 1$ для R1,
  - $X^{22} + X^{21} + 1$ для R2 и
  - $X^{23} + X^{22} + X^{21} + X^{8} + 1$ для R3,
- управление тактированием осуществляется специальным механизмом:
  - в каждом регистре есть биты синхронизации: 8 (R1), 10 (R2), 10 (R3),
  - вычисляется функция F = x&y|x&z|y&z, где & — булево AND, | - булево OR, а x, y и z — биты синхронизации R1, R2 и R3 соответственно,
  - сдвигаются только те регистры, у которых бит синхронизации равен F,
  - фактически, сдвигаются регистры, синхробит которых принадлежит большинству,
- выходной бит системы — результат операции XOR над выходными битами регистров.

A5/2. Модификация для понижения стойкости

В A5/2 добавлен ещё один короткий регистр длиной 17 бит, который управляет движением бит в остальных трёх регистрах

Официальная позиция:

MoU (Memorandum of Understand Group Special Mobile standard): «… целью разработки A5/2 было понижение криптостойкости шифрования».

В официальных результатах тестирования говорится, что неизвестно о каких-либо недостатках алгоритма

A5. Свойства, ослабляющие защиту

- 10 бит ключа принудительно занулены,
- отсутствие перекрестных связей между регистрами (кроме управления сдвигами),
- излишняя избыточность шифруемой служебной информации, известной криптоаналитику,
- свыше 40 % ключей приводит к минимальной длине периода генерируемой последовательности, а именно $\frac{3}{4}\left(2^{23}-1\right)$
- в начале сеанса осуществляется обмен нулевыми сообщениями (по одному кадру),
- в A5/2 движение осуществляется отдельным регистром длиной 1,0 бит.

A5. Известные пассивные атаки

- Скомпрометирована длина ключа. Длина ключа составляет 64 бит, 10 из которых принудительно занулены, что ослабляет систему на три порядка.
- Скомпрометирован сильный алгоритм шифрования A5/1. Из-за конструктивных дефектов сложность полного перебора составляет не 2^64, а всего 2^40 (то есть ослабление системы на 6 порядков). Кроме того, ослабляет систему независимость трёх регистров: для каждого регистра значение бит других регистров влияет только на управление смещением, но не на содержание самого регистра.
- Скомпрометирован слабый алгоритм шифрования A5/2. Этот алгоритм изначально создавался слабым, но в результате он оказался настолько слабым, что для его вскрытия достаточно знать 2 кадра по 114 бит.
- Обнаружены серьёзные недостатки в структуре дополнительных алгоритмов стандарта. В частности код коррекции ошибок прибавляется к сообщению до шифрования, что приводит к лишней избыточности и позволяет сильно упростить процесс вскрытия шифра.

A5. Известные активные атаки

Обнаружена и описана группой израильских криптографов (Элад Баркан, Эли Бихам и Натан Келлер).

При аутентификации телефона в сети сессионный ключ Kc не зависит от протокола шифрования.

Перехватывается телефонный звонок, который был зашифрован A5/1 или даже более сильным A5/3, и надо узнать содержание этого разговора.

Рядом с телефоном включается ложная базовая станция и посылается вызов на телефон.

Для установления связи высылается число RAND, которое использовалось в том звонке, который надо расшифровать.

При этом сессионный ключ Kc будет такой же, как и в предыдущем случае.

Если же теперь потребовать от телефона шифрования в слабом режиме A5/2, который легко вскрывается, то можно легко узнать сессионный ключ и расшифровать интересующий нас разговор.

A5. Выводы

- Стандарт, стойкость которого основана на том, что злоумышленник не знает внутренней структуры системы, не может быть надежным

  Security by Obscurity = Security by Ostrich

- Слабость системы определяется самой слабой её частью – разработав умышленно ослабленный шифр A5/2, разработчики GSM в результате поставили под удар всю систему
- Новые стандарты должны

A5. Выводы

Have the A5 algorithms been broken?

- ***Alex Biryukov, Adi Shamir and David Wagner showed that they can find the A5/1 key in less than a second on a single PC with 128 MB RAM and two 73 GB hard disks, by analyzing the output of the A5/1 algorithm in the first two minutes of the conversation.***
- ***Ian Goldberg and David Wagner of the University of California at Berkeley published an analysis of the weaker A5/2 algorithm showing a work factor of 2^16, or approximately 10 milliseconds.***
- ***Elad Barkhan, Eli Biham and Nathan Keller of Technion, the Israel Institute of Technology, have shown a ciphertext-only attack against A5/2 that requires only a few dozen milliseconds of encrypted off-the-air traffic. They also described new attacks against A5/1 and A5/3.***