Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

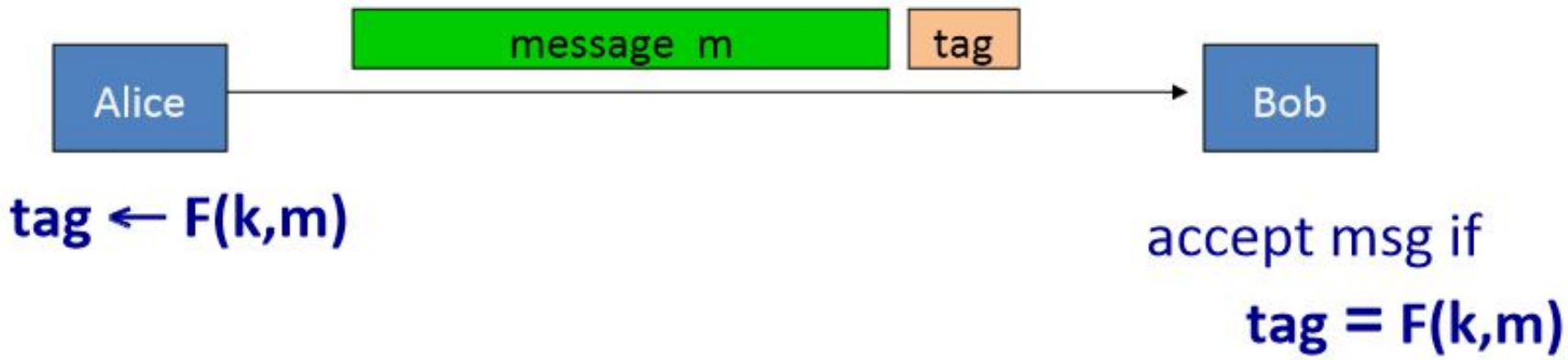
Москва, 2014

Раздел 7 - Код целостности сообщения

Код целостности сообщения

MAC, message authentication code

Цель: обеспечить целостность открытой инф-и.



MAC передается вместе с сообщением. CRC не годится.

Опр.

MAC $I = (S, V)$ - это пара алгоритмов $S, V \in \mathrm{PT}$:
алгоритм $S : K \times M \to T$ (to sign)
алгоритм $V : K \times M \times T \to \{0, 1\}$ (to verify)

Криптостойкий MAC

Модель атаки: с выбранным открытым текстом.
$\forall m_1, ..., m_q$ злоум-к получает $t_i = S(k, m_i)$
Цель: создать новую пару
$(m, t) \not\in \{(m_1, t_1), ..., (m_q, t_q)\} : V(k, m, t) = 1.$

Т.е. верный тэг t для нового сообщения m
или новый верный тэг $t_i' \neq t_i$ для сообщения m_i.

Опр.

MAC над K, M, T наз. *криптостойким*, если для любого злоум-ка $A \in \mathrm{PPT}$ вероятность успешной атаки пренебр. мала. Т.е.
$Adv_{MAC}[A, I] = P(\text{успешная атака}) < \varepsilon(min(log(|K|), log(|T|)))$,
$\varepsilon(n)$ - пренебр. малая функция.

На практике требуем $\forall A: \ time(A) < N$
$Adv_{MAC}[A, I] = P(\text{успешная атака}) < \varepsilon = const$

Задача

пусть (S,V) - MAC и всем известно сообщение m_0: для половины значений ключей $k \in K$ злоум-к может найти $m_1 \neq m_0 : S(k, m_0) = S(k, m_1)$. Будет ли этот MAC криптостойким?

Задача

пусть (S,V) - MAC и $T = \{0,1\}^5$. Будет ли он криптостойким? (Чему равна вероятность угадать MAC?)

Пример

использование MAC при размещении баннеров на сайтах.

Реализация MAC с помощью ПСФ:

Утверждение

Пусть $F : K \times X \to Y$ - ПСФ и $1/|Y|$ - пренебр. малая, $1/|Y| < \varepsilon$. Тогда I_F - стойкий MAC.
В частности, для любой атаки $A \in \mathrm{PPT}$ на MAC, $\exists$ атака $B \in \mathrm{PPT}$ на ПСФ F такая, что
$Adv_{MAC}[A, I_F] \leq Adv_{PRF}[B, F] + 1/|Y|$

Док-во

злоум-к берет некоторое сообщение. Может или просто угадать тэг для него, или использовать атаку на ПСФ.

Поэтому вер-ть успешной атаки на MAC = P(успеш. атака на ПСФ)$+P$(угадали тэг)$-P$(оба эти события).
Ч.т.д.

Лемма

Пусть $F : K \times X \to Y$ - ПСФ. Тогда $F_t(k, m) = F(k, m)[1, ..., t]$ - ПСФ для $1 \leq t \leq n$.
Т.е., если обрежем стойкую ПСФ, снова получим стойкую ПСФ.

Задача

доказать лемму (от противного).

Задача

Следствие из леммы: MAC, построенный по обрезанной стойкой ПСФ, будет стойким, если ...

Пример

для 128-битного сообщения можно MAC $= AES(m)$.

Раздел 7 - Код целостности сообщения

MAC

CBC-MAC, NMAC, CMAC

PMAC

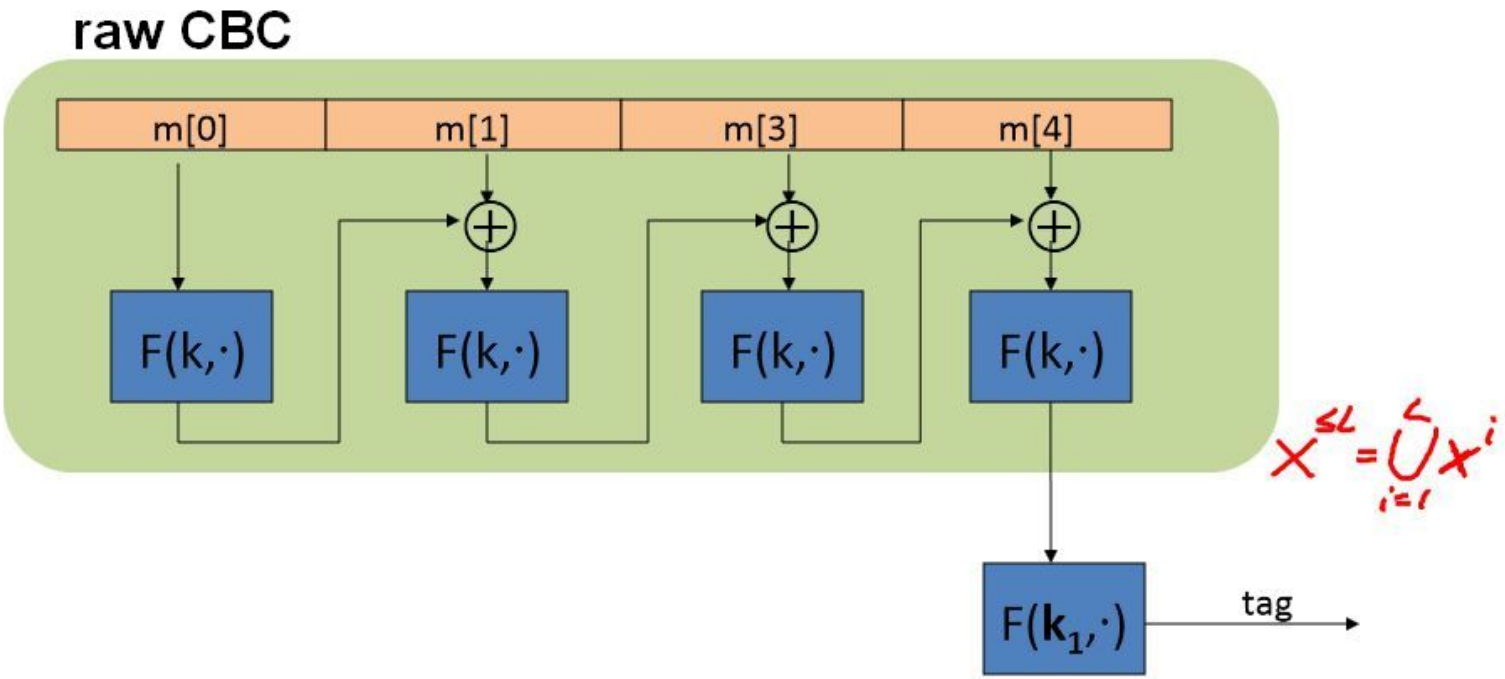
Построение MAC для длинного сообщения по ПСФ для короткого сообщения

$X = \{0,1\}^{128}$, n - длина блока.

1) Зашифрованный CBC-MAC (ECBC-MAC)

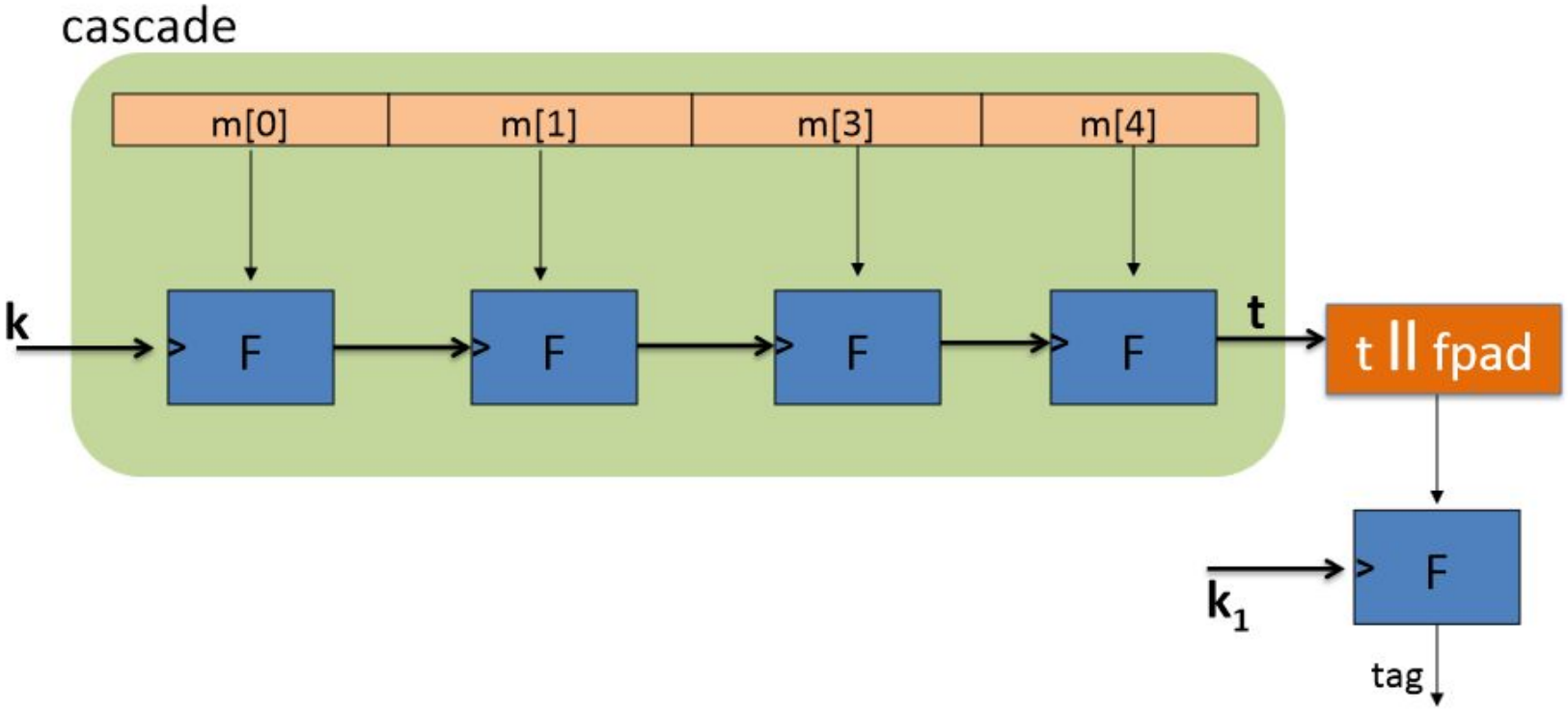
Зашифрованный код целостности сообщения в режиме сцепления блоков.

$F : K \times X \to Y$ - криптостойкая ПСФ. $F_{ECBC} : K^2 \times X^{\leq L} \to X$



2) вложенный MAC (NMAC)

$F : K \times X \to Y$ - криптостойкая ПСФ. $F_{NMAC} : K^2 \times X^{\leq L} \to K$



NMAC медленнее CBC-MAC: каждый раз новое расписание ключей у шифра, реализующего F.

Задача (Обосновать уязвимости без последнего шага - шифрования)

1. NMAC: Известно $cascade(k, m)$ и w. Получить $cascade(k, m||w)$ при неизв. k
2. Пусть для raw CBC-MAC известна пара (m, t), длина m - один блок. Предложить сообщение длиной 2 блока вида $m||u$ (т.е значение второго блока u), для которого можно найти верный тэг, и вычислить верный тэг для этого сообщения.

Пример

На основе ECBC-MAC построен стандарт NIST - CMAC.

Утверждение

$\forall L > 0$, $\forall$ оракула $A \in \mathrm{PPT}$ на ECBC-MAC (NMAC), совершающего q запросов пар (m, t), $\exists F \in \mathrm{PPT}$ - алгоритм атаки на ПСФ:

$$Adv_{PRF}[A, F_{ECBC-MAC}] \leq Adv_{PRP}[B, F] + 2q^2/|X|$$

$$Adv_{PRF}[A, F_{NMAC}] \leq qL \cdot Adv_{PRF}[B, F] + 2q^2/(2|K|)$$

ECBC-MAC стойкий при $q \ll \sqrt{|X|}$,

NMAC стойкий при $q \ll \sqrt{|K|}$.
Если F - блочный шифр, NMAC на каждом шаге требует вычисления нового расписания ключей.

Без док-ва.

Частота замены ключа

Пусть хотим $Adv_{PRF}[A, F_{ECBC}] < 2^{-32}$
$\Rightarrow \ q^2/|X| < 2^{-32}$

AES: $q < 2^{48}$, 3DES: $q < 2^{16}$

Задача (Свойство "продолжения" у ECBC-MAC и NMAC)

$\forall x, y, w$ верно
$MAC(k, x) = MAC(k, y) \Rightarrow MAC(k, x||w) = MAC(k, y||w)$
Это полезное свойство или вредное?

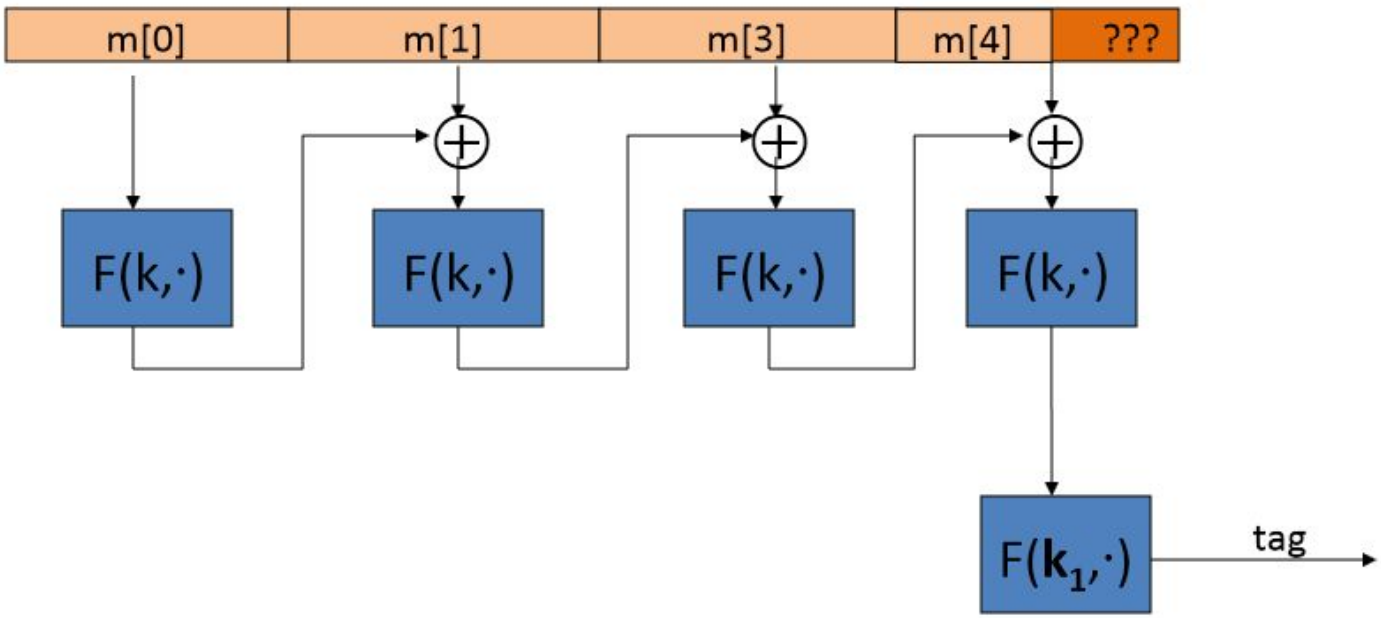
Атака на MAC за счет коллизии при парадоксе дня рождения

Пусть $F : K \times X \to Y$ - ПСФ, имеющая свойство продолжения. Тогда на соответствующий ей MAC возможна следующая атака:

1. получить $\sqrt{|Y|}$ пар сообщений (m_i, t_i) для случайных сообщений.
2. по парадоксу дня рождения, с вер-ю более $1/2$ в полученных тэгах $\exists$ коллизия $t_u = t_v$ при $m_u \neq m_v$
3. возьмем любое продолжение w и получим тэг $t = F(m_u||w)$
4. имеем новую коллизию $(m_v||w, t)$, $(m_u||w, t)$.

Продление сообщения до длины блока

Используем ECBC-MAC на осн. блочного шифра - нужно продление сообщения.

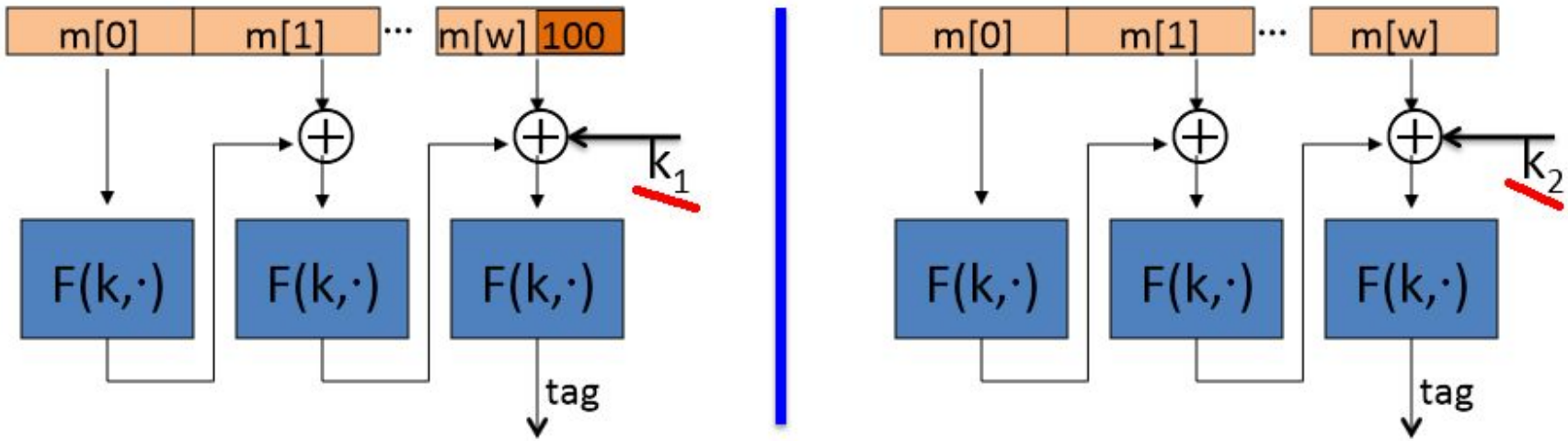


Продлим нулями: $MAC(k, m) = MAC(k, m||0..0)$
Тогда: Продлить посл-тью 10..0, а если длина сообщ. кратна длине блока, допишем целый блок 10..0.

TODO: в 2015, возможно, убрать CMAC? Их и так слишком много.

CMAC (стандарт NIST)

Ключ $k \Rightarrow$ два ключа k_1, k_2 и слегка изменим схему CBC-MAC:



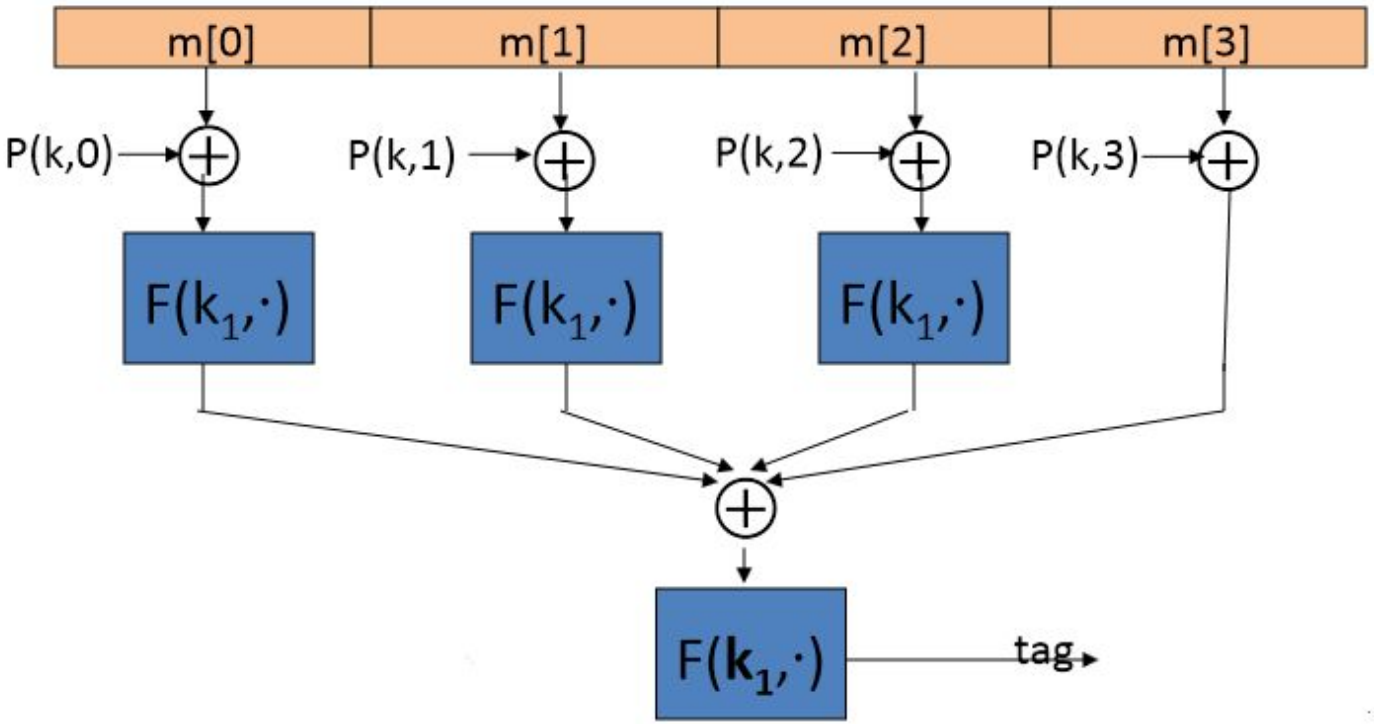
- не нужно шифрование результата, т.к. $\oplus k_i$
- не нужен лишний блок, если длина сообщ. кратна длине блока.

Раздел 7 - Код целостности сообщения

TODO: в 2015 точно убрать PMAC. Их и так слишком много.

3) PMAC, параллельный MAC

ключ $= (k, k_1)$, дополнение до длины блока как в CBC-MAC.



Задача

Пусть (m_0, t_0) - верная пара. Пусть m_1 - сообщ. m_0, измененное в j-м блоке: $m_0[j] \neq m_1[j]$, $m_0[i] = m_1[i]$, $i \neq j$. Найти быстрый способ вычисления t_1 по t_0 и m_1.

Утверждение

$\forall L > 0$, $\forall A \in \mathrm{PPT}$ - алгоритма атаки на PMAC, совершающего q запросов пар (m, t), $\exists B \in \mathrm{PPT}$ - алгоритм атаки на ПСФ F:

$$Adv_{PRF}[A, F_{PMAC}] \leq qL \cdot Adv_{PRF}[B, F] + 2q^2L^2/(|X|)$$

Без док-ва.

PMAC стойкий при $qL < \sqrt{|X|}$.

Литература к лекции

1. Black, Rogaway, *A Block-Cipher Mode of Operation for Parallelizable Message Authentication*, 2002.
`http://web.cs.ucdavis.edu/~rogaway/ocb/pmac.pdf`