A New Mode of Operation for Block Ciphers and Length-Preserving MACs

Yevgeniy Dodis
New York University

Krzysztof Pietrzak
CWI Amsterdam

Prashant Puniya
New York University

April 15, 2008

Modes of Operation

Construction of a Variable Input Length (VIL) primitive from a Fixed Input Length (FIL) primitive.

- VIL primitives: MAC, PRF, Random Oracle (RO), ...
- FIL primitive(s): by far, most dominant is a block-cipher.
  - well understood, standardized (AES).
  - directly used in the CBC mode.
  - indirectly used in the Merkle-Damgård (MD) mode: the compression function of SHA/MD5 is instantiated via Davies-Myers $h(x, y) = E_x(y) \oplus y$.

Subject of this talk: building VIL-primitives from block ciphers (more generally, *length-preserving functions*).

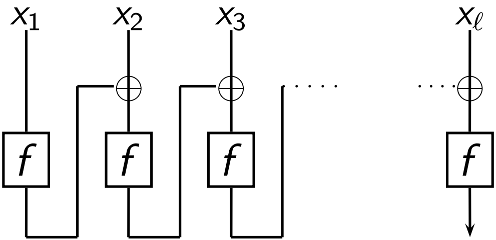
A mode of operation for block-ciphers?

Construction $C[f]$, based on a block-cipher f, should be:

- Efficient: no re-keying, constant rate.
- MAC preserving: $C[f]$ is a VIL-MAC if f is a FIL-MAC.
- PRF preserving: $C[f]$ is a VIL-PRF if f is a FIL-PRF.
- RO preserving: $C[f]$ is indifferentiable from a VIL-RO if f is a FIL-RO.
    - in particular, $C[f]$ is collision-resistant (if f is a FIL-RO).

What about existing constructions?

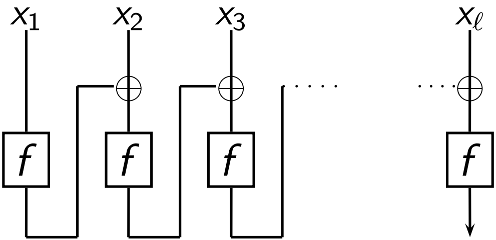
CBC Mode



Good News:

Bad News:

CBC Mode

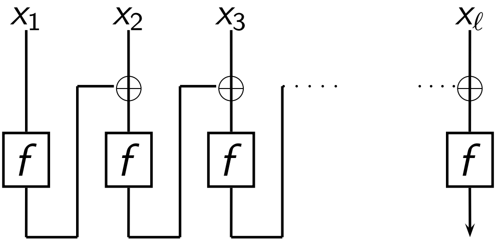


Good News:

- PRF preserving [BKR94]: if f is a PRF then $CBC[f]$ with prefix-free encoding is a VIL-PRF.

Bad News:

CBC Mode



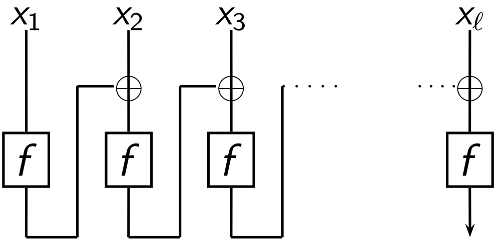
Good News:

- PRF preserving [BKR94]: if f is a PRF then $CBC[f]$ with prefix-free encoding is a VIL-PRF.

Bad News:

- $CBC[f]$ is not always a MAC, even if f is a MAC [AB'99].

CBC Mode



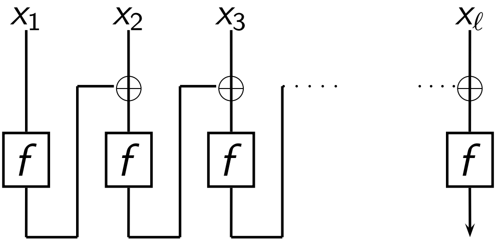
Good News:

- PRF preserving [BKR94]: if f is a PRF then $CBC[f]$ with prefix-free encoding is a VIL-PRF.

Bad News:

- $CBC[f]$ is not always a MAC, even if f is a MAC [AB'99].
- $CBC[f]$ is never collision resistant, for any f.

CBC Mode



Good News:

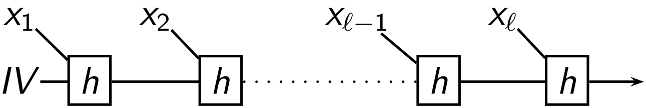
- PRF preserving [BKR94]: if f is a PRF then $CBC[f]$ with prefix-free encoding is a VIL-PRF.

Bad News:

- $CBC[f]$ is not always a MAC, even if f is a MAC [AB'99].
- $CBC[f]$ is never collision resistant, for any f.
- In particular, $CBC[f]$ is not a VIL-RO if f is a FIL-RO.

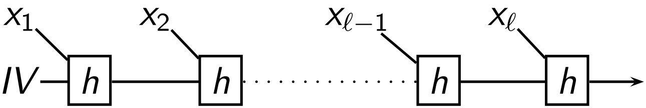
Merkle-Damgård Mode

"Plain Merkle-Damgård" $MD[f] : \{0,1\}^* \rightarrow \{0,1\}^n$.
Uses a compression function $h : \{0,1\}^{n+t} \rightarrow \{0,1\}^n$.



Merkle-Damgård Mode

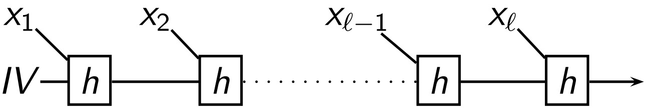
"Plain Merkle-Damgård" $MD[f] : \{0,1\}^* \to \{0,1\}^n$.
Uses a compression function $h : \{0,1\}^{n+t} \to \{0,1\}^n$.



Good News: Although "plain MD" is too simple, minor variants of it preserve PRF, MAC [AB99] and RO [CDMP05].

Merkle-Damgård Mode

"Plain Merkle-Damgård" $MD[f] : \{0,1\}^* \rightarrow \{0,1\}^n$.
Uses a compression function $h : \{0,1\}^{n+t} \rightarrow \{0,1\}^n$.



Good News: Although "plain MD" is too simple, minor variants of it preserve PRF, MAC [AB99] and RO [CDMP05].

Bad News: Need a compression function h.

Can we build a compression function from a block-cipher?

Compression function from a block-cipher?

- Davies-Meyers $h(x, y) = E_x(y) \oplus y$ works for RO [CDMP'05], but uses re-keying.
  Doesn't make sense for keyed primitives (PRF, MAC).

Compression function from a block-cipher?

- Davies-Meyers $h(x, y) = E_x(y) \oplus y$ works for RO [CDMP'05], but uses re-keying.
  Doesn't make sense for keyed primitives (PRF, MAC).
- Chopping (i.e. ignoring some bits of the output) works, but terrible security, especially for MACs.

Compression function from a block-cipher?

- Davies-Meyers $h(x, y) = E_x(y) \oplus y$ works for RO [CDMP'05], but uses re-keying.
  Doesn't make sense for keyed primitives (PRF, MAC).
- Chopping (i.e. ignoring some bits of the output) works, but terrible security, especially for MACs.
- Best previous construction for MACs is Luby-Rackoff with superlogarithmic number of rounds [DP'07].
  - Open before this work: constant rate VIL-MAC from a length preserving MAC.

Enciphered CBC

$f_i = f(k_i, .)$ with k_1, k_2, k_3 independent keys.

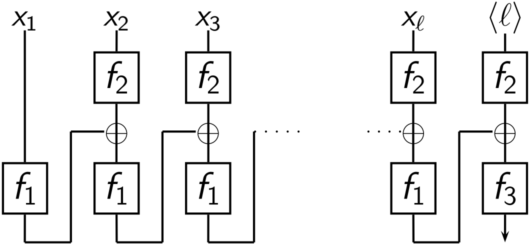


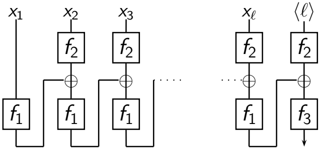
Figure: $H[f_1, f_2, f_3]$, the basic three-key enciphered CBC construction

$H[f_1, f_2, f_3]$ a VIL-PRF/MAC/RO if f is a length-preserving PRF/MAC/RO.
Rate is 2.

Outline

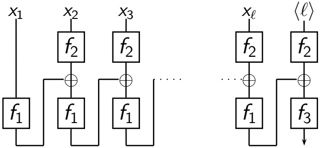
- Proof sketch of MAC property.
- Proof sketch of RO property.
- The RO property and invertability.
- In the paper: Variant having just one key.

A High Level View



Can view this construction as $f_3(MD[h])$ where $h(x \| x') = f_1(x) \oplus f_2(x')$.

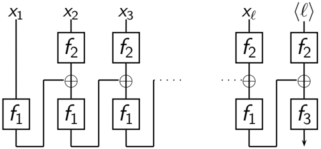
A High Level View



Can view this construction as $f_3(MD[h])$ where $h(x \| x') = f_1(x) \oplus f_2(x')$.

Proof structure for MAC/RO

A High Level View

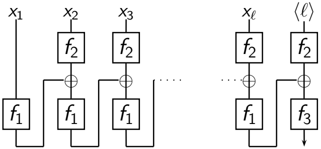


Can view this construction as $f_3(MD[h])$ where $h(x \| x') = f_1(x) \oplus f_2(x')$.

Proof structure for MAC/RO

- Define appropriate notion of "collision resistance" CR (different for MAC and RO).

A High Level View

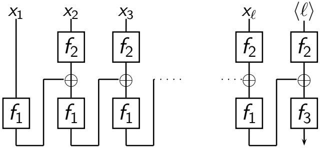


Can view this construction as $f_3(MD[h])$ where $h(x\|x') = f_1(x) \oplus f_2(x')$.

Proof structure for MAC/RO

- Define appropriate notion of "collision resistance" CR (different for MAC and RO).
- Prove that $h(x\|x') = f_1(x) \oplus f_2(x')$ is FIL-CR.

A High Level View

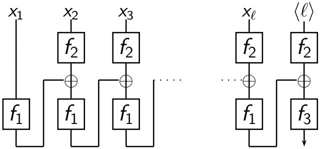


Can view this construction as $f_3(MD[h])$ where $h(x \| x') = f_1(x) \oplus f_2(x')$.

Proof structure for MAC/RO

- Define appropriate notion of "collision resistance" CR (different for MAC and RO).
- Prove that $h(x \| x') = f_1(x) \oplus f_2(x')$ is FIL-CR.
- Show that MD is preserving for CR: MD[FIL-CR]$\rightarrow$VIL-CR.

A High Level View



Can view this construction as $f_3(MD[h])$ where $h(x\|x') = f_1(x) \oplus f_2(x')$.

Proof structure for MAC/RO

- Define appropriate notion of "collision resistance" CR (different for MAC and RO).
- Prove that $h(x\|x') = f_1(x) \oplus f_2(x')$ is FIL-CR.
- Show that MD is preserving for CR: MD[FIL-CR]$\rightarrow$VIL-CR.
- Show that FIL-MAC(VIL-CR)$\rightarrow$VIL-MAC and similarly FIL-RO(VIL-CR)$\rightarrow$VIL-RO.

Message Authentication Codes

$\{0,1\}^x \stackrel{\text{def}}{=} \{0,1\}^x$

Definition (FIL-MAC)

A family of functions $f : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^n$ is a (t, q, ϵ) secure Fixed-Input-Length Message-Authentication-Code (FIL-MAC) if for every adversary A of size t making at most q queries

$$\Pr[K \leftarrow \{0,1\}^k; A^{f(K,.)} \rightarrow (M, \phi); f(K, M) = \phi] \leq \epsilon$$

Message Authentication Codes

$\{0,1\}^x \stackrel{\text{def}}{=} \{0,1\}^x$

Definition (FIL-MAC)

A family of functions $f : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^n$ is a (t, q, ϵ) secure Fixed-Input-Length Message-Authentication-Code (FIL-MAC) if for every adversary A of size t making at most q queries

$$\Pr[K \leftarrow \{0,1\}^k; A^{f(K,.)} \rightarrow (M, \phi); f(K, M) = \phi] \leq \epsilon$$

Definition (VIL-MAC)

A family of functions $f : \{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^n$ is a (t, q, ϵ) secure Variable-Input-Length Message-Authentication-Code (FIL-MAC) if for every adversary A of size t making queries of total length at most q blocks

Theorem (Enciphered CBC is MAC preserving)

If $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ *is a* (t, q, ε)*-secure FIL-MAC, then enciphered CBC instantiated with* f *is a* $(t', q, \varepsilon \cdot q^4)$*-secure variable input-length MAC, where* $t' = t - O(qn)$.

Weak Collision Resistance [AB'99]

Definition

A family of functions $f : \{0,1\}^k \times \{0,1\}^m \longrightarrow \{0,1\}^n$ is (t, q, ϵ) weakly collision-resistant (WCR) if for any adversary A of size t making at most q queries

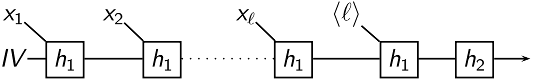
$$\Pr[K \leftarrow \{0,1\}^k; A^{f(K,.)} \rightarrow (M \neq M'); f(K,M) = f(K,M')] \leq \epsilon$$

Weak Collision Resistance [AB'99]

Definition

A family of functions $f : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$ is (t, q, ϵ) weakly collision-resistant (WCR) if for any adversary A of size t making at most q queries

$$\Pr[K \leftarrow \{0,1\}^k; A^{f(K,.)} \to (M \neq M'); f(K,M) = f(K,M')] \leq \epsilon$$



Lemma (AB'99)

- *FIL-MAC$\rightarrow$FIL-WCR*
- *MD[FIL-WCR]$\rightarrow$VIL-WCR*
- *FIL-MAC(VIL-WCR)$\rightarrow$VIL-MAC*

Weak collision resistance of $f_1 \oplus f_2$

Lemma

Let $f : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ *be a family of functions. Define* $h : \{0,1\}^{2k} \times \{0,1\}^{2n} \rightarrow \{0,1\}^n$

$$h(k_1, k_2, x \| x') = f(k_1, x) \oplus f(k_2, x')$$

If f *is a* (t, q, ϵ)*-secure MAC, then* h *is* $(t', q, \epsilon \cdot q^4)$*-weakly collision-resistant.*

Proof.

Weak collision resistance of $f_1 \oplus f_2$

Lemma

Let $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Define $h : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^n$

$$h(k_1, k_2, x \| x') = f(k_1, x) \oplus f(k_2, x')$$

If f is a (t, q, ϵ)-secure MAC, then h is $(t', q, \epsilon \cdot q^4)$-weakly collision-resistant.

Proof.

- Assume $\Pr[A^{f_1, f_2}$ finds a collision with q queries$] > \delta$.

Weak collision resistance of $f_1 \oplus f_2$

Lemma

Let $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Define $h : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^n$

$$h(k_1, k_2, x\|x') = f(k_1, x) \oplus f(k_2, x')$$

If f is a (t, q, ϵ)-secure MAC, then h is $(t', q, \epsilon \cdot q^4)$-weakly collision-resistant.

Proof.

- Assume $\Pr[A^{f_1,f_2}$ finds a collision with q queries$] > \delta$.
- To forge f_K: Guess $1 \leq j_1 < j_2 < j_3 < j_4 \leq 2q$ run A^{f_1,f_2} with $f_2 = f_K$ (or $f_1 = f_K$).

Weak collision resistance of $f_1 \oplus f_2$

Lemma

Let $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Define $h : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^n$

$$h(k_1, k_2, x\|x') = f(k_1, x) \oplus f(k_2, x')$$

If f is a (t, q, ϵ)-secure MAC, then h is $(t', q, \epsilon \cdot q^4)$-weakly collision-resistant.

Proof.

- Assume Pr[A^{f_1,f_2} finds a collision with q queries] $> \delta$.
- To forge f_K: Guess $1 \leq j_1 < j_2 < j_3 < j_4 \leq 2q$ run A^{f_1,f_2} with $f_2 = f_K$ (or $f_1 = f_K$).
- Stop when A makes j_4'th query x_{j_4} and output forgery guess $(x_{j_4}, f_1(x_{j_1}) \oplus f_2(x_{j_2}) \oplus f_1(x_{j_3}))$ for $f_2 = f_K$.

Weak collision resistance of $f_1 \oplus f_2$

Lemma

Let $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions. Define $h : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^n$

$$h(k_1, k_2, x \| x') = f(k_1, x) \oplus f(k_2, x')$$

If f is a (t, q, ϵ)-secure MAC, then h is $(t', q, \epsilon \cdot q^4)$-weakly collision-resistant.

Proof.

- Assume $\Pr[A^{f_1, f_2}$ finds a collision with q queries$] > \delta$.
- To forge f_K: Guess $1 \leq j_1 < j_2 < j_3 < j_4 \leq 2q$ run A^{f_1, f_2} with $f_2 = f_K$ (or $f_1 = f_K$).
- Stop when A makes j_4'th query x_{j_4} and output forgery guess $(x_{j_4}, f_1(x_{j_1}) \oplus f_2(x_{j_2}) \oplus f_1(x_{j_3}))$ for $f_2 = f_K$.
- Forgery correct if $f_1(x_{j_1}) \oplus f_2(x_{j_2}) = f_1(x_{j_3}) \oplus f_2(x_{j_4})$.

Indifferentiability [MRH'04],[CDMP'05]

Theorem

$H[f_1, f_2, f_3]$ is $\frac{q^4}{2^n}$ indifferentiable from a VIL-RO (here q is the number of queries the distinguisher is allowed to make).

Right notion of collision resistance:

- We say $h(x_1 \| x_2) = f_1(x_1) \oplus f_2(x_2)$ is ϵ-extractable (EX), if there's an efficient E s.t. for all A_1, A_2
  - $A_1^{f_1,f_2} \rightarrow (y, \phi)$
  - $E(y, \text{oracle calls of } A_1^{f_1,f_2}) \rightarrow z$
  - $A_2^{f_1,f_2}(\phi) \rightarrow z'$
  - $\Pr[z \neq z' \wedge h(z') = y] \leq \epsilon$.

Lemma

- *MD[FIL-EX]→VIL-EX*
- *FIL-RO(VIL-EX)→VIL-RO*

$f_1 \oplus f_2$ is extractable

Lemma

If f_1, f_2 are FIL-RO then $h(x_1 \| x_2) = f_1(x_1) \oplus f_2(x_2)$ is $q^4/2^n$ FIL-EX.

$f_1 \oplus f_2$ is extractable

Lemma

If f_1, f_2 are FIL-RO then $h(x_1 \| x_2) = f_1(x_1) \oplus f_2(x_2)$ is $q^4/2^n$ FIL-EX.

$E(y, \text{oracle calls of } A_1^{f_1,f_2})$ finds oracle calls x_1, x_2 s.t. $f_1(x_1) \oplus f_2(x_2) = y$. If x_1, x_2 unique output them, otherwise "give up".

Indifferentiability from Permutations

- $H[f_1, f_2, f_3]$ is indifferentiable from a random oracle if $f_i : \{0,1\}^n \longrightarrow \{0,1\}^n$ are random functions.

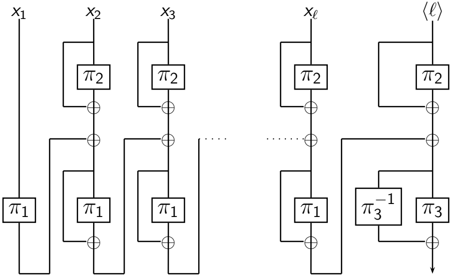
Indifferentiability from Permutations

- $H[f_1, f_2, f_3]$ is indifferentiable from a random oracle if $f_i : \{0,1\}^n \to \{0,1\}^n$ are random functions.
- In practice, one would instantiate f_i with a block-cipher with a fixed key, but then not only f_i but also its inverse f_i^{-1} can be evaluated by the attacker.

Indifferentiability from Permutations

- $H[f_1, f_2, f_3]$ is indifferentiable from a random oracle if $f_i : \{0,1\}^n \rightarrow \{0,1\}^n$ are random functions.
- In practice, one would instantiate f_i with a block-cipher with a fixed key, but then not only f_i but also its inverse f_i^{-1} can be evaluated by the attacker.
- Unfortunately $H[\pi_1, \pi_2, \pi_3]$ is *not* indifferentiable if the π_i's are random permutations where the attacker gets access to π_i and its inverse π_i^{-1}.

Indifferentiability from Permutations



This construction is indifferentiable from a random oracle if instantiated with random permutations π_1, π_2, π_3 over $\{0,1\}^n$ where the adversary can query π_i and π_i^{-1}.

Note that this is $H[f_1, f_2, f_3]$ with $f_1(x_1) = \pi_1(x_1) \oplus x_1$, $f_2(x_2) = \pi_2(x_2) \oplus x_2$, $f_3(x_3) = \pi_3(x_3) \oplus \pi_3^{-1}(x_3)$

Indifferentiability from Permutations cont.

$f_1(x_1) = \pi_1(x_1) \oplus x_1$, $f_2(x_2) = \pi_2(x_2) \oplus x_2$,
$f_3(x_3) = \pi_3(x_3) \oplus \pi_3^{-1}(x_3)$

Lemma

$f_3(x_3) = \pi_3(x_3) \oplus \pi_3^{-1}(x_3)$ *is indifferentiable from a FIL-RO.*

Indifferentiability from Permutations cont.

$f_1(x_1) = \pi_1(x_1) \oplus x_1$, $f_2(x_2) = \pi_2(x_2) \oplus x_2$,
$f_3(x_3) = \pi_3(x_3) \oplus \pi_3^{-1}(x_3)$

Lemma

$f_3(x_3) = \pi_3(x_3) \oplus \pi_3^{-1}(x_3)$ is indifferentiable from a FIL-RO.

Lemma

$f_1(x_1) \oplus f_2(x_2) = \pi_1(x_1) \oplus x_1 \oplus \pi_2(x_2) \oplus x_2$ is extractable.

Conclusions and Open Problems

Conclusions

- Mode of operations for length preserving primitives preserving MAC, PRF, RO.

Conclusions and Open Problems

Conclusions

- Mode of operations for length preserving primitives preserving MAC, PRF, RO.
- First domain expansion for length-preserving MACs with constant rate.

Conclusions and Open Problems

Conclusions

- Mode of operations for length preserving primitives preserving MAC, PRF, RO.
- First domain expansion for length-preserving MACs with constant rate.
- Hedge against security of underlying primitive: if its a PRF we get a PRF, if its only a MAC we're guaranteed to get a MAC.

Conclusions and Open Problems

Conclusions

- Mode of operations for length preserving primitives preserving *MAC*, *PRF*, *RO*.
- First domain expansion for length-preserving MACs with constant rate.
- Hedge against security of underlying primitive: if its a *PRF* we get a *PRF*, if its only a *MAC* we're guaranteed to get a MAC.

Open Problems

- Security loss of reduction for MAC and indifferentiability is q^4 (compared to q^2 achieved by An-Bellare for shrinking MACs), can this be improved?

Conclusions and Open Problems

Conclusions

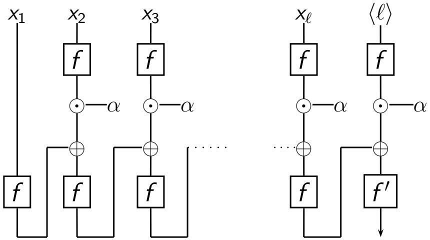
- Mode of operations for length preserving primitives preserving *MAC*, *PRF*, *RO*.
- First domain expansion for length-preserving MACs with constant rate.
- Hedge against security of underlying primitive: if its a *PRF* we get a *PRF*, if its only a *MAC* we're guaranteed to get a MAC.

Open Problems

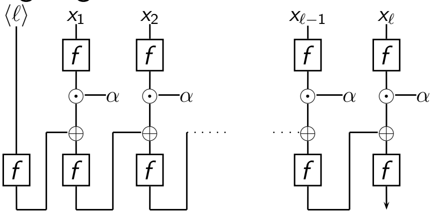
- Security loss of reduction for MAC and indifferentiability is q^4 (compared to q^2 achieved by An-Bellare for shrinking MACs), can this be improved?
- We achieve rate 2, is this optimal? Is there an efficiency/security trade-off as Rogaway & Steinberger (next talk!) prove for constructions of CRHF from random permutations.

any questions?

One-key Construction

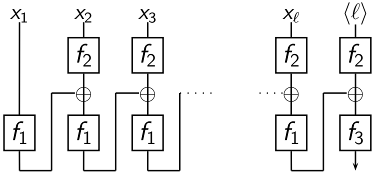


We can replace f' also with f, and the mode still stays secure for MACs when we prepend (and not append) the length $\langle \ell \rangle$. This can be a problem as the message length must be known before processing begins.



Two-key Construction

The basic three-key construction



Can replace $f_2(.)$ with $\alpha \odot f_2(.)$ where α is a constant (not 0 or 1) in $\mathbb{GF}(2^n)$. With $\alpha = 2$ multiplication is very efficient (one shift and at most one XOR).