Provable Seconde Preimage Resistance Revisited

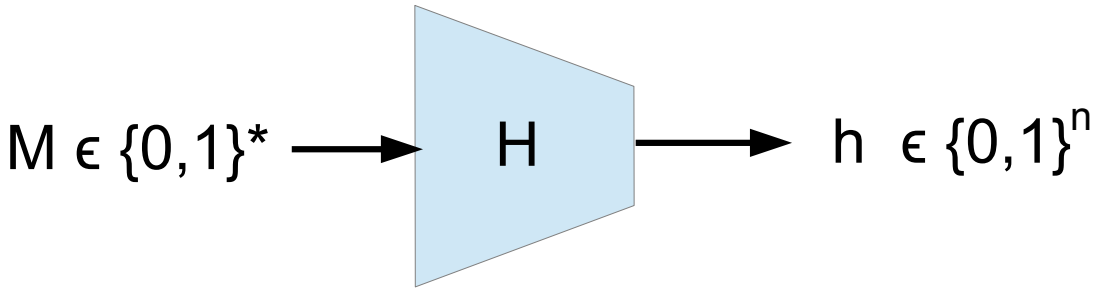
Charles Bouillaguet[1] Bastien Vayssiere[2]

[1]LIFL
University of Lille, France

[2]PRISM
University of Versailles, France

SAC 2013

Cryptographic Hash Functions



It should behave "like a random oracle".
In particular, with respect to the following cryptanalysis :

- **Collision attacks** :
  Find $M \neq M'$ such that $H(M') = H(M)$. Ideal security : $2^{n/2}$
- **Second Preimage attacks** :
  Given M, find M' such that $H(M') = H(M)$. Ideal security : 2^n
- **Preimage attacks** :
  Given $h \in \{0,1\}^n$, find M such that $H(M) = h$. Ideal security : 2^n

Second Preimage Notions of Security

Usually defined with the execution time (t) and the probability of success (ε) of an adversary. Global complexity : t/ε.

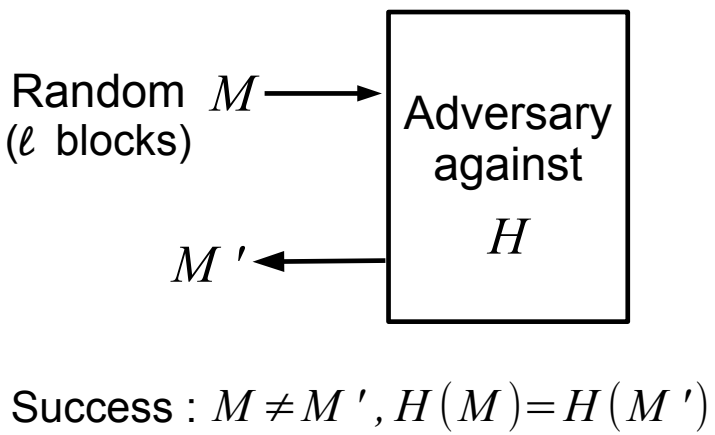
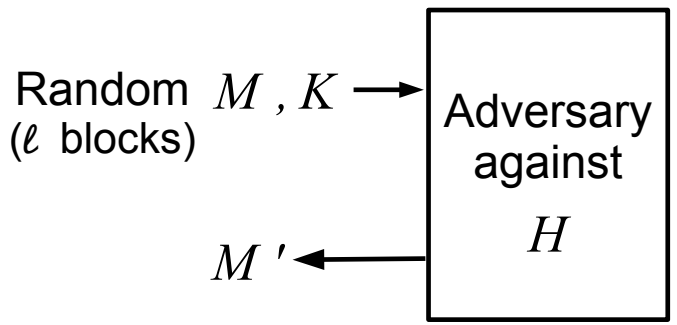


Figure: Spr[ℓ] notion, for unkeyed hash functions

Second Preimage Notions of Security

Usually defined with the execution time (t) and the probability of success (ε) of an adversary. Global complexity : t/ε.

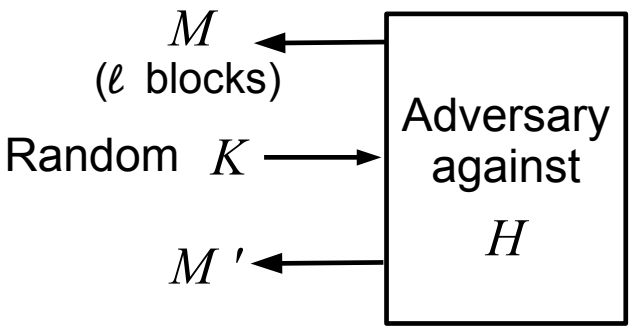


Success : $M \neq M'$, $H(M, K) = H(M', K)$

Figure: Sec[ℓ] notion, for keyed hash functions

Second Preimage Notions of Security

Usually defined with the execution time (t) and the probability of success (ε) of an adversary. Global complexity : t/ε.

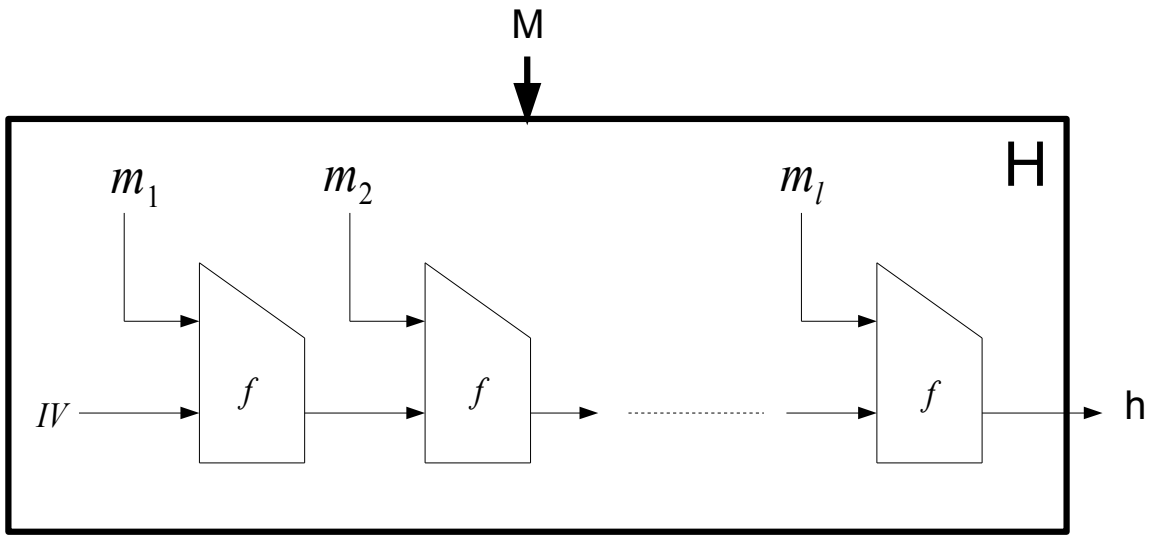


Success : $M \neq M', H(M, K) = H(M', K)$

Figure: eSec[ℓ] notion, for keyed hash functions

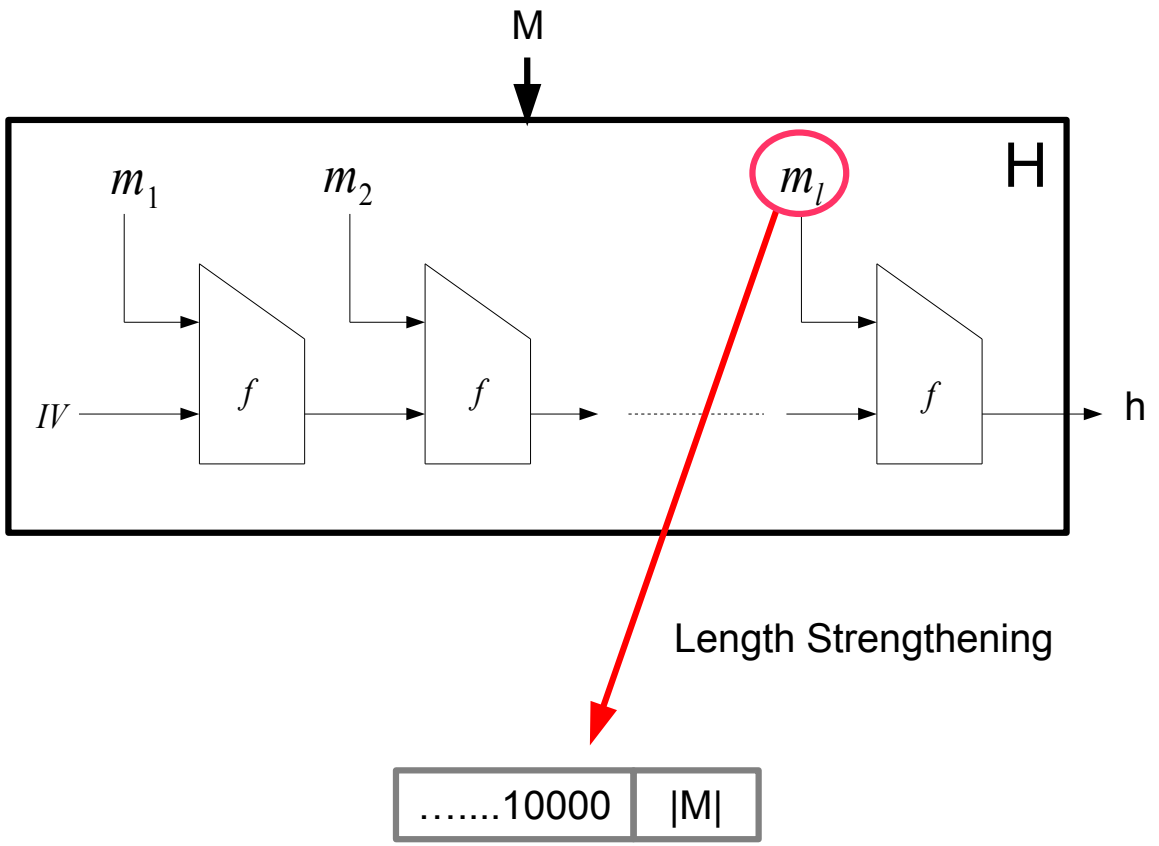
Iterated Hash Functions

Most hash functions are iterated hash functions.
Classical mode : Merkle-Damgård [Merkle Damgård, 1989]. Used in MD5, SHA0, SHA1, SHA2.



Iterated Hash Functions

Most hash functions are iterated hash functions.
Classical mode : Merkle-Damgård [Merkle Damgård, 1989]. Used in MD5, SHA0, SHA1, SHA2.



Provable Security of Modes

Generic attacks on hash functions

The attack works on H^f for any f.
$\Longrightarrow$ the mode of operation itself is unsecure !

How to measure the security against generic attacks ?

1. Replace f by a Random Oracle
2. Find an upper bound on the advantage of the adversaries against H^f.

One also need to know about the security of H^f when f is a real life compression function ($\neq$ Random Oracle).

Reductions in the Standard Model

Idea : exhibit a reduction which transform any adversary against H^f into an adversary against f.
For a given security notion, the reduction proves that the property of f is preserved by the mode of operations.

Example : Merkle-Damgård was published with a reduction which convert any collision on H^f into a collision on f, in linear time.

Generic attacks on Merkle-Damgård

Generic attacks on Merkle-Damgård:

- Multi-collisions [Joux, 2004]
- Second Preimages Attacks [Kelsey and Schneier, 2005]
- Herding Attacks [Kelsey and Kohno, 2006].

Generic Second Preimage Attack of Kelsey and Schneier

Second preimage of messages of ℓ blocks in

$$\frac{2^n}{\ell} + log(\ell)2^{n/2}$$

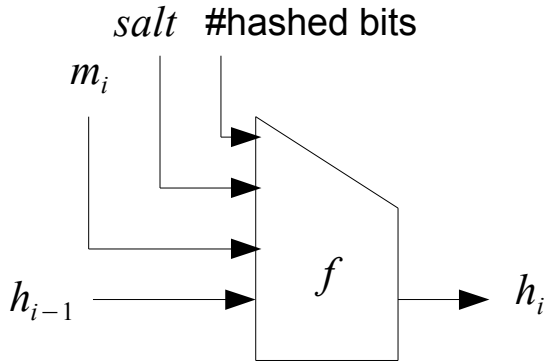
... even for f replaced by a random oracle. (Ideal security : 2^n)

Research for new modes

- "wide-pipe" modes : extend the internal state [Lucks, 2005]
- design narrow-pipe modes with proofs of resistance to collisions, preimages ... and second preimages !

We focus on the second issue.

HAIFA mode of operations [Biham Dunkelman, 2006]



Provable Security in the Random Oracle Model [BDFJ 2009]

For f a Random Oracle, the success probability of any adversary breaking the Spr[ℓ] notion of H^f in q queries is lower than $\frac{q}{2^{n-1}}$.

Reduction in the Standard Model

Three narrow-pipe mode with a proof of security in the Standard Model :

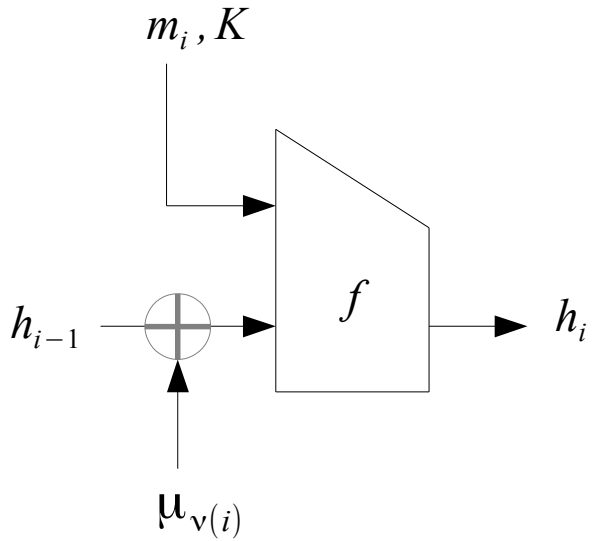
1. Shoup's UOWHF, [Shoup, 2000]
2. Backward Chaining Mode, [Andreeva and Preneel, 2008]
3. Split Padding, [Yasuda, 2008]

The designers provided a reduction of a notion of second preimage security of f which :

- terminates in $t + \mathcal{O}(\ell)$ time
- with success probability ε/ℓ.

defined for an adversary (t, ε)-breaking a notion of H^f.

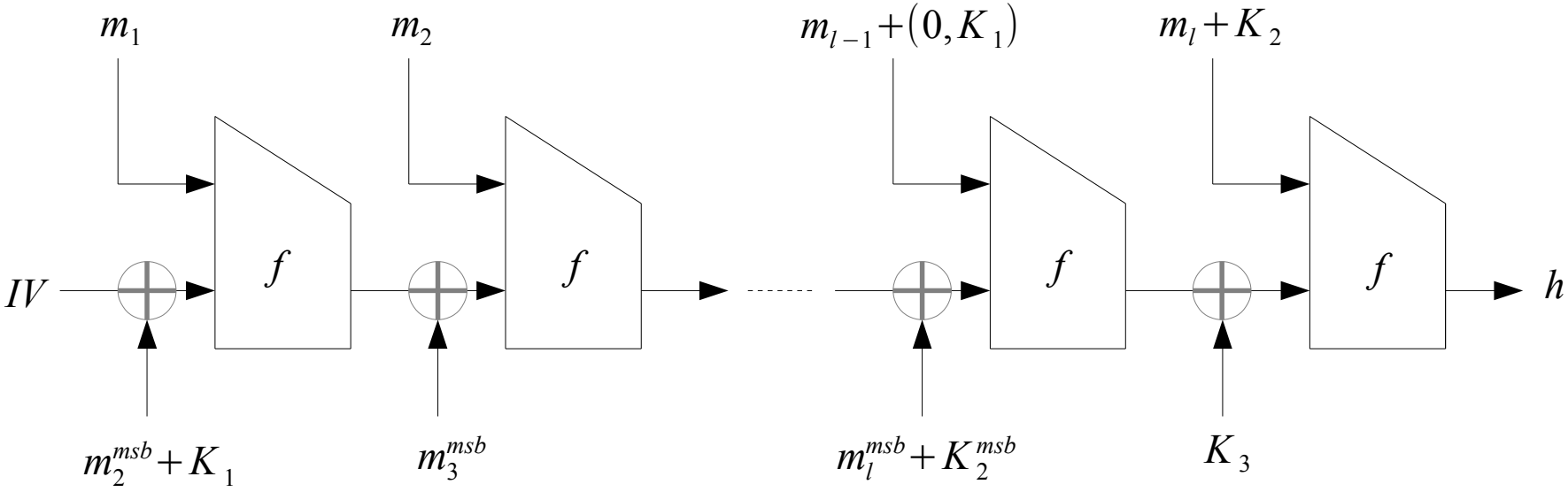
Shoup's UOWHF, [Shoup, 2000]



Provable Security in the Standard Model

If an adversary is able to break the eSec[ℓ] notion of H^f with probability ε in time t, then one can construct an adversary that breaks the eSec notion of f in time $t + \mathcal{O}(\ell)$, with probability ε/ℓ.

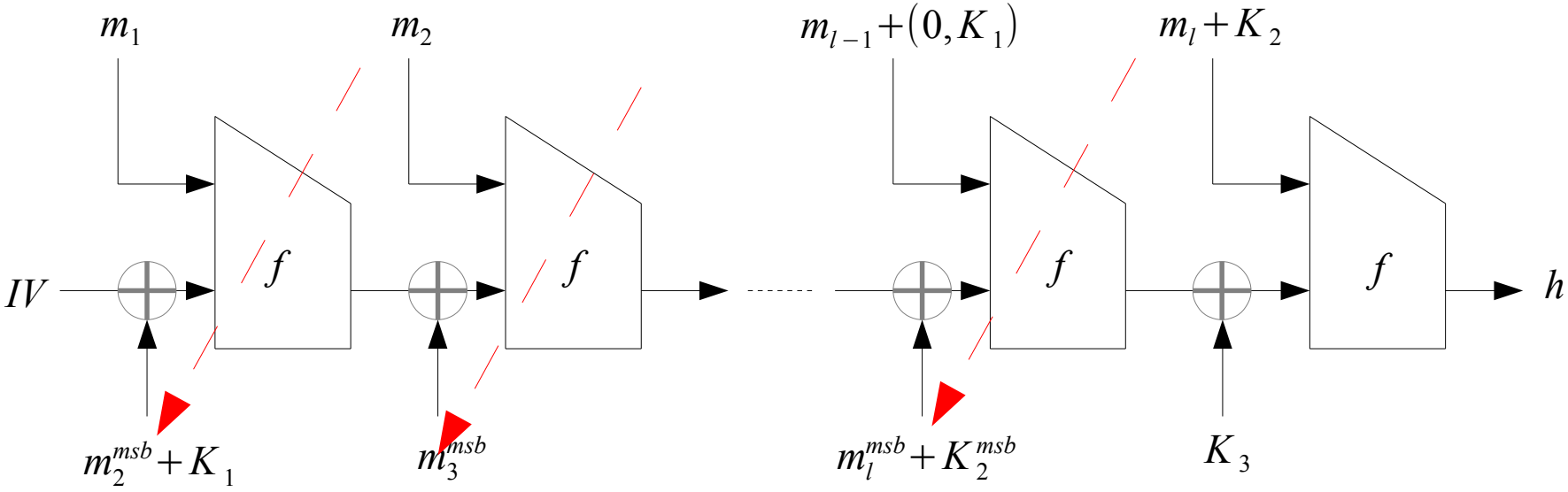
Backward Chaining Mode, [Andreeva and Preneel, 2008]



Provable Security in the Standard Model

If an adversary is able to break the Sec[ℓ] notion of H^f with probability ε in time t, then one can construct an adversary that breaks the Spr notion of f in time $t + \mathcal{O}(\ell)$, with probability ε/ℓ.

Backward Chaining Mode, [Andreeva and Preneel, 2008]



Provable Security in the Standard Model

If an adversary is able to break the Sec[ℓ] notion of H^f with probability ε in time t, then one can construct an adversary that breaks the Spr notion of f in time $t + \mathcal{O}(\ell)$, with probability ε/ℓ.

Objectives

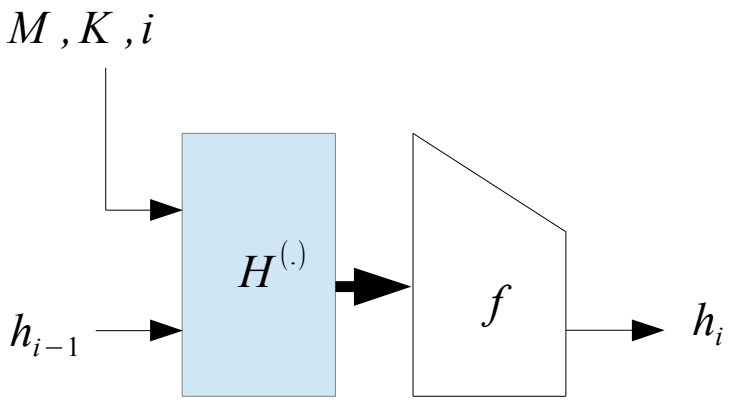


Figure: Abstract narrow-pipe mode of operations

For the narrow-pipe modes in this abstract model, we provide simple sufficient properties to obtain :

- optimal second preimage security in the Random Oracle Model,
- optimal second preimage security in the Standard Model, **for a narrow-pipe mode**,

...and keep the proof of Merkle-Damgård that it preserves the collision resistance !

Sufficient Conditions to Preserve the Collision Resistance

Three sufficient conditions :

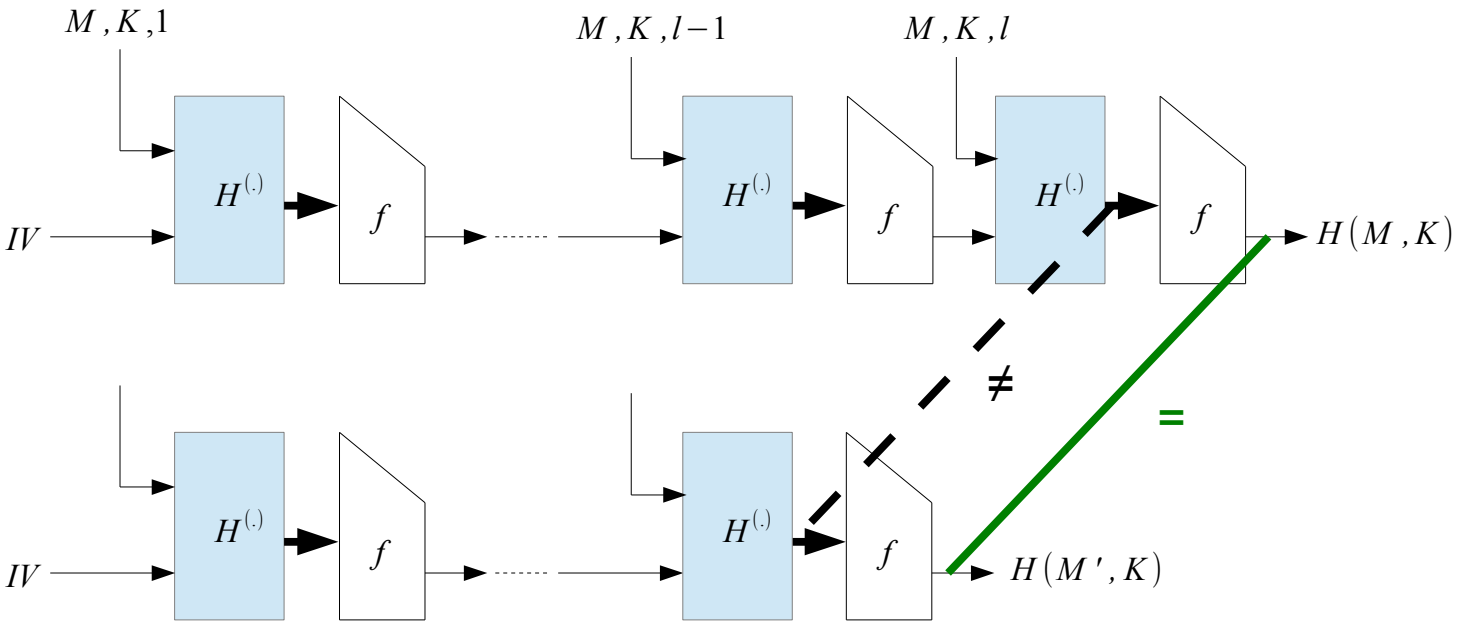
- Length strengthening : the last input of f contains $|M|$
- Message injectivity : $M \neq M' \implies \exists i, x_i \neq x'_i$
- Chaining value injectivity : $h_{i-1} \neq h'_{i-1} \implies x_i \neq x'_i$

At our knowledge, those properties are verified by all existing narrow-pipe modes.

Any collision between messages of less than ℓ blocks on H^f can be transformed into a collision on f in $\mathcal{O}(\ell)$ computations.

Reuse the Proof of Merkle-Damgård

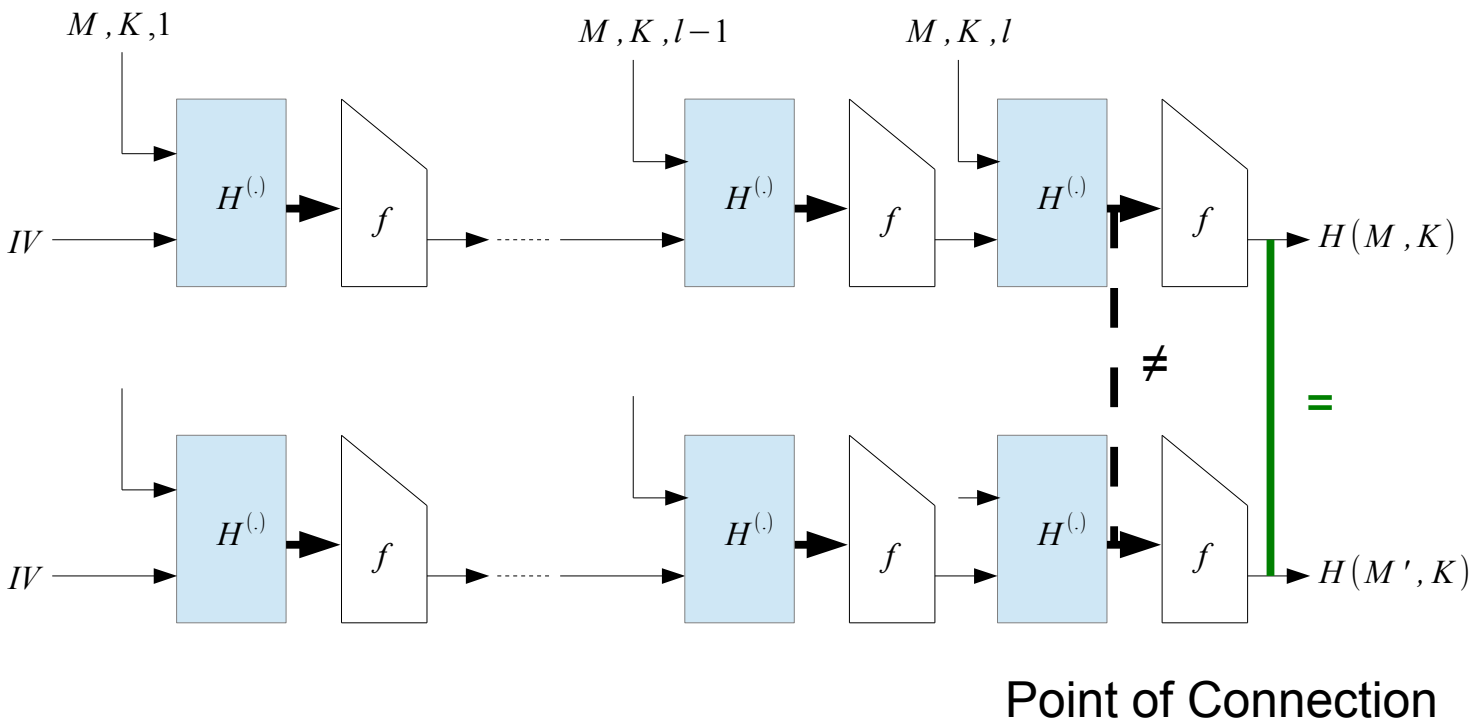
If $|M| \neq |M'|$, and the last input block involves the message length, then we have a collision at the end.



Reuse the Proof of Merkle-Damgård

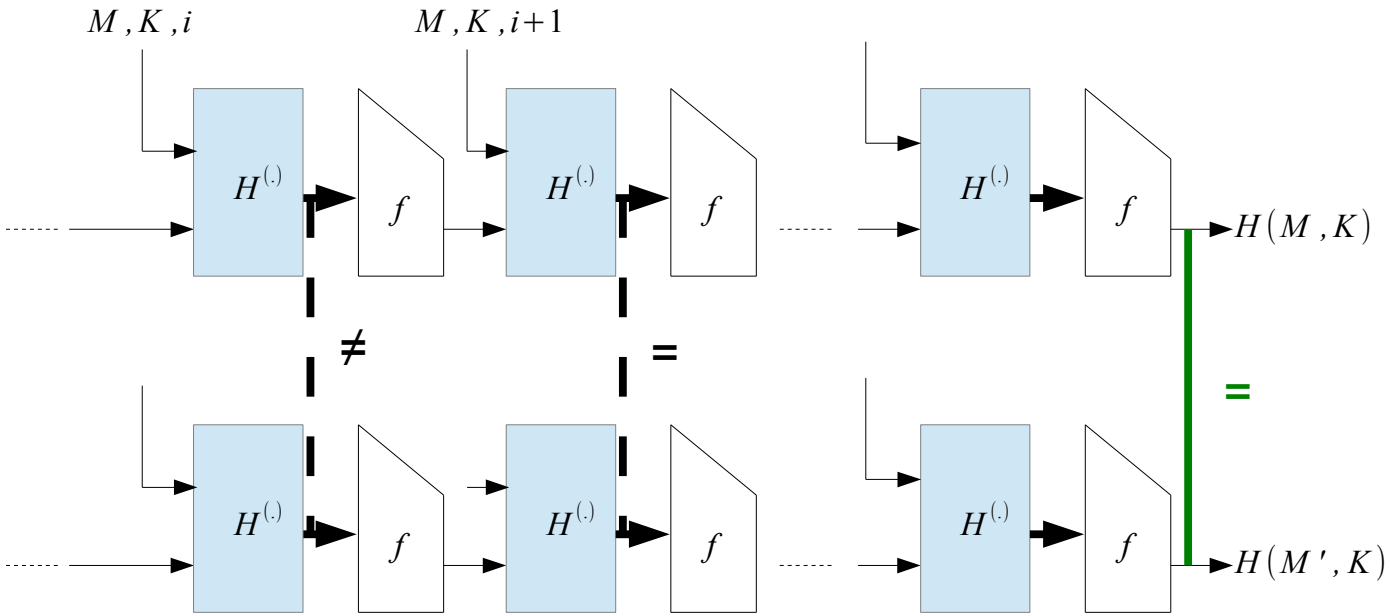
Case $|M| = |M'|$. Since M' is a second preimage of (M, K), $M' \neq M$ and it has a distinct sequence of blocks.
The point of connection will be the last index i such that $x'_i \neq x_i$.
If $i = \ell$, the collision on H^f directly implies the collision

$$f(x'_\ell) = f(x_\ell) = H(M, K)$$



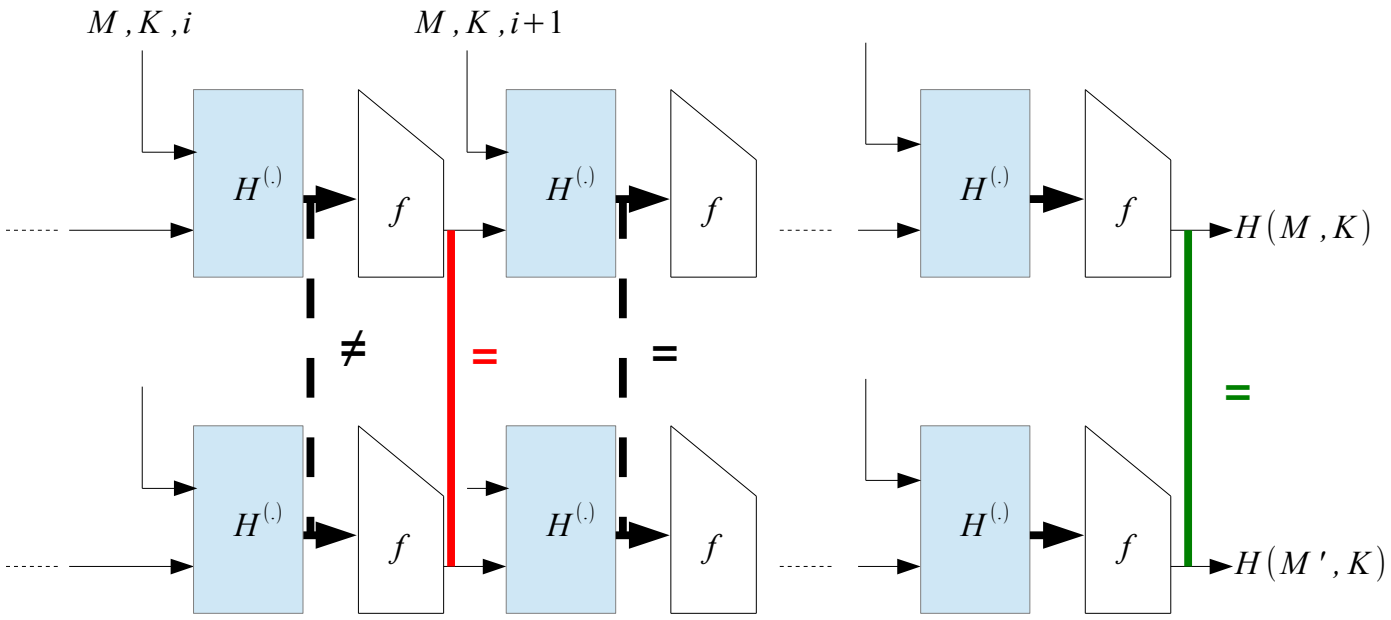
Reuse the Proof of Merkle-Damgård

If the point of connection is not the last iteration, since identical inputs of f are always due to identical previous chaining values, we obtain a collision too.



Reuse the Proof of Merkle-Damgård

If the point of connection is not the last iteration, since identical inputs of f are always due to identical previous chaining values, we obtain a collision too.



Resistance to Generic Attacks

Suppose f is a Random Oracle.
We want to give an upper bound on the probability that q queries enable an adversary to find a second preimage M' of a random challenge (M, K).

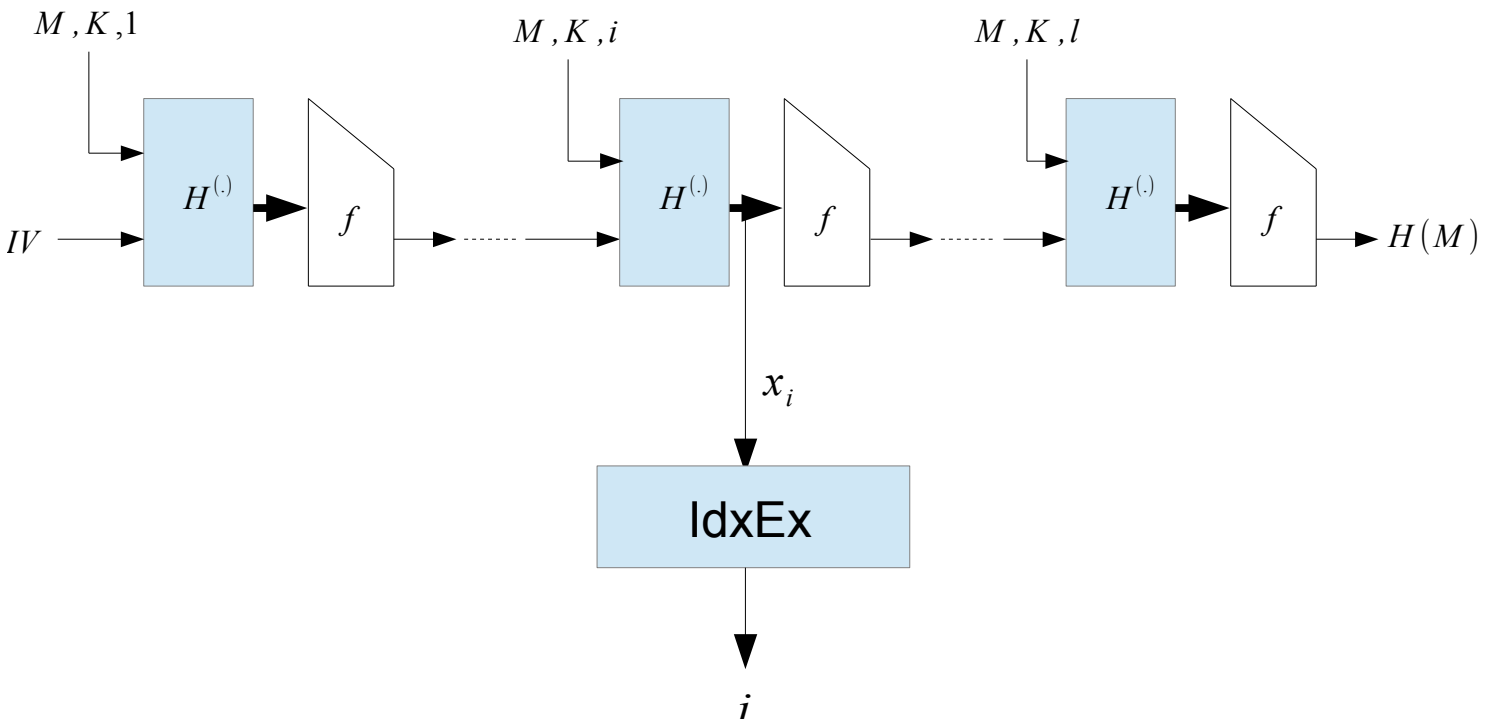
- if $|M| \neq |M'|$, the length strenghtening provide that $x_{\ell'}$ is a preimage of $h = H^f(M, K)$.
  With q queries it cannot happen with probability higher than $q2^{-n}$.

- if $|M| = |M'|$, the point of connection can happen at ℓ distinct positions...

Domain separation

Domain separation of the mode : existence of a generic algorithm ($IdxEx$) such that for any M, K and any i-th input x of f

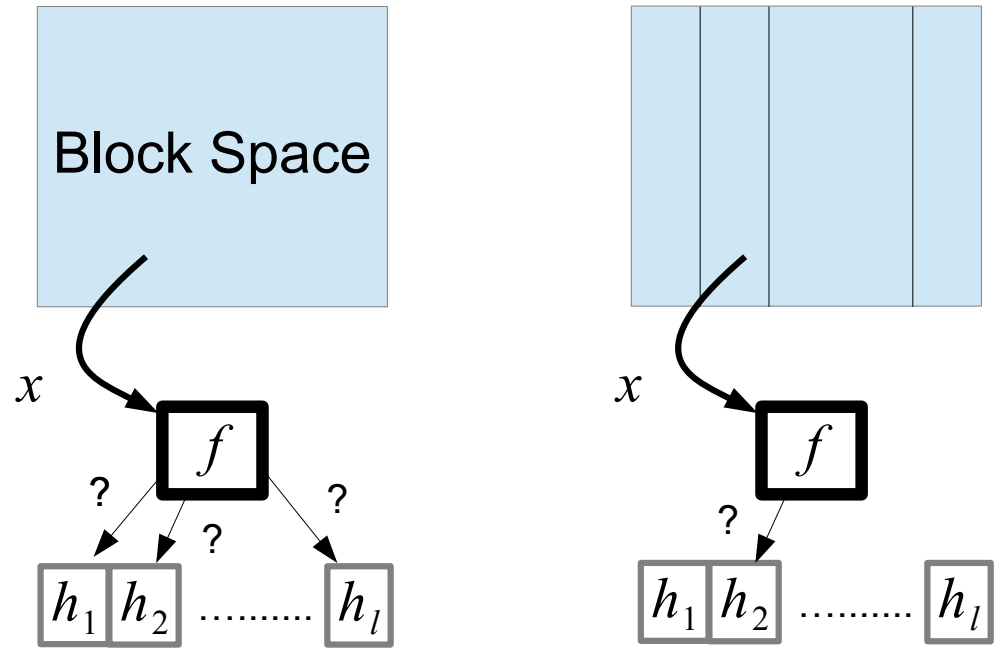
$$IdxEx(x) = i$$



For HAIFA : $IdxEx(x_j) = \dfrac{\#hashed\ bits}{\text{block bit length}}$

Domain separation

If $|M| = |M'|$ and M' is a second preimage of (M, K), there is a point of connection. There was a query x' to f which verified $f(x') = f(x_i) = h_i$.



Can succeed as a preimage of any one of a set of ℓ blocks

With domain separation : only 1 case

Each query has a probability 2^{-n} to bring this point of connection. In q queries, the probability to have at least one such query is

$$1 - (1 - 2^{-n})^q \leq q2^{-n}$$

Optimal Resistance to Generic Attacks

Theorem

Let $H^{(\cdot)}$ be a narrow-pipe mode with **domain separation**, *length-strengthening, message and chaining value injectivities. This mode has optimal resistance to generic second preimage attacks.*

Proof.

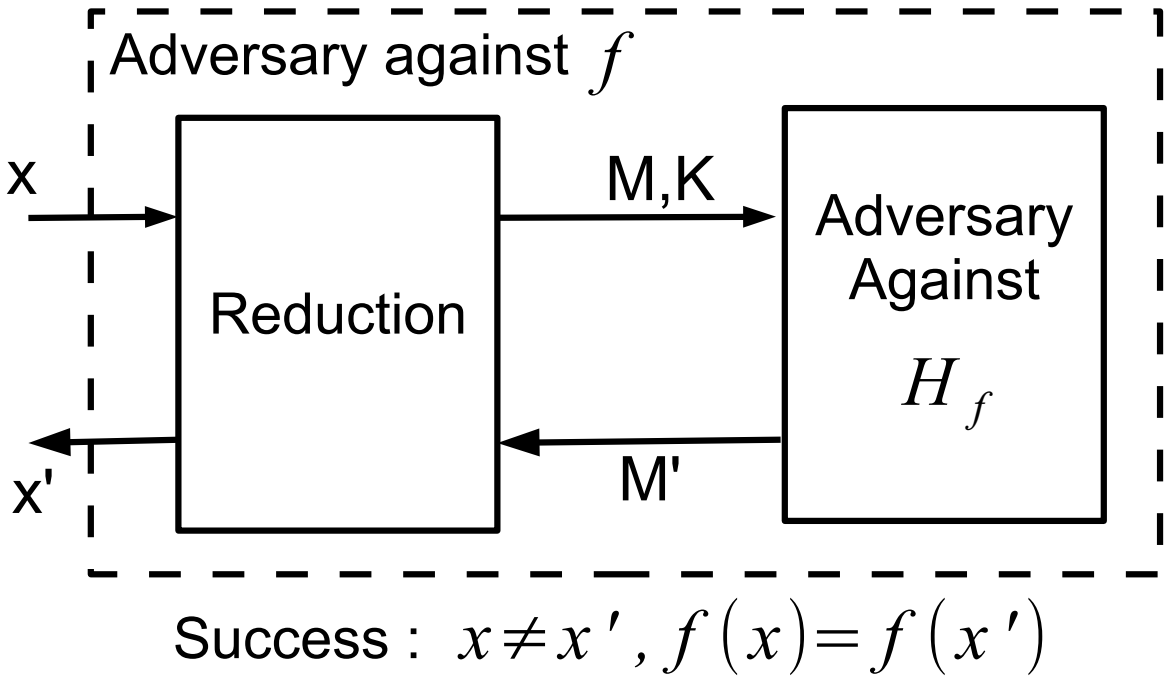
Let ε be the success probability of the adversary against H^f, f is replaced by a Random Oracle. Let M' be a second preimage of (M, K) for H^f.

1. If $|M| \neq |M'|$:
   Length-strenghtening $\implies$ $\mathcal{A}$ found a preimage of h.
   Probability $\leq q2^{-n}$**.**
2. If $|M| = |M'|$: point of connection $i = idxEx(x'_i)$
   Each query x' to the oracle f can only succeed if $f(x') = h_{idxEx(x')}$.
   Probability $\leq q2^{-n}$**.**

$$\varepsilon \leq q(2^{-n} + 2^{-n}) = \frac{q}{2^{n-1}}$$

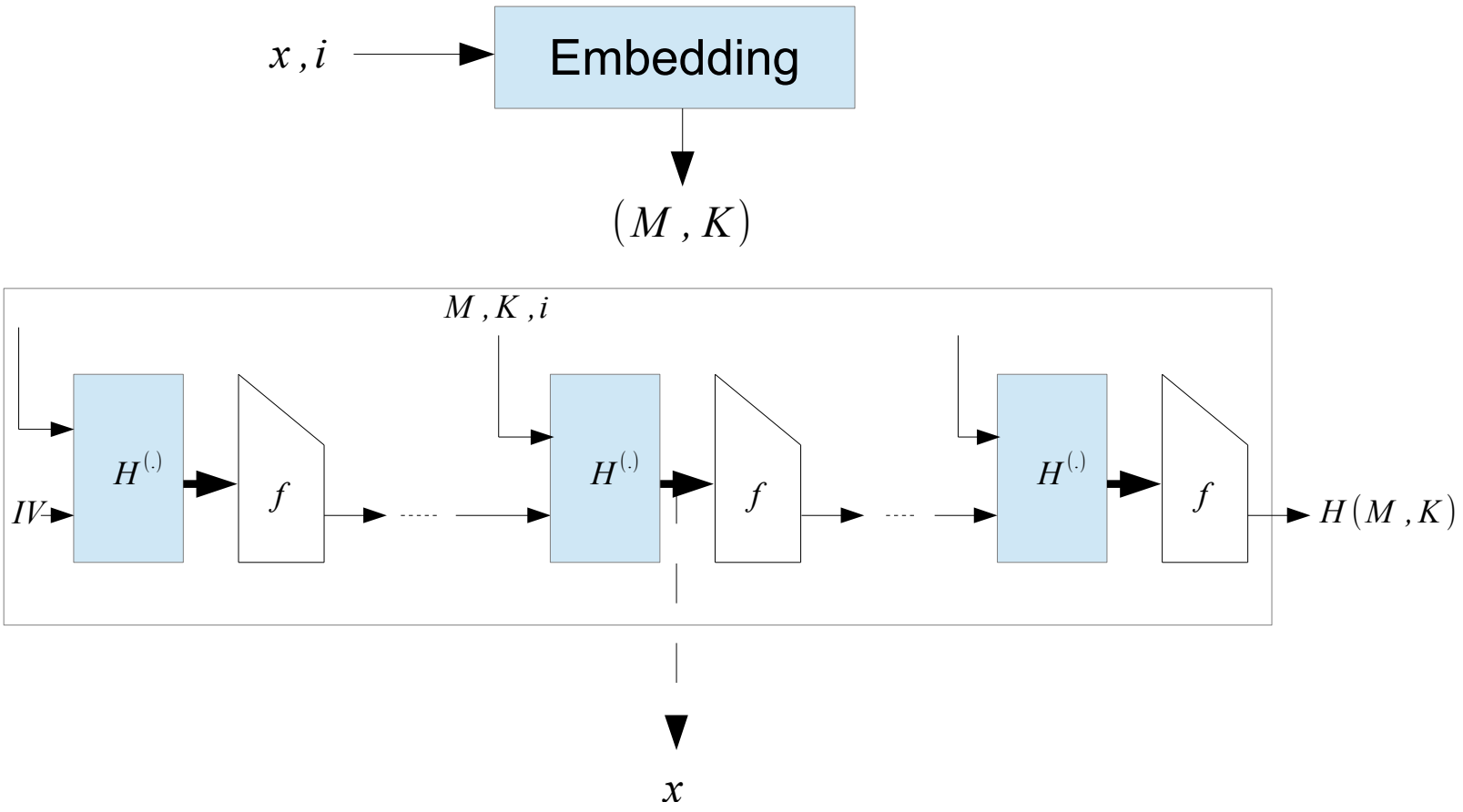
Reduction in the Standard Model

Goal : find a sufficient property which permits to design a reduction which convert any adversary of Sec[ℓ] notion of H^f into an adversary for the notion Spr of f.



The level of security is the lower bound provided on t/ε when f is secure for the notion Spr.

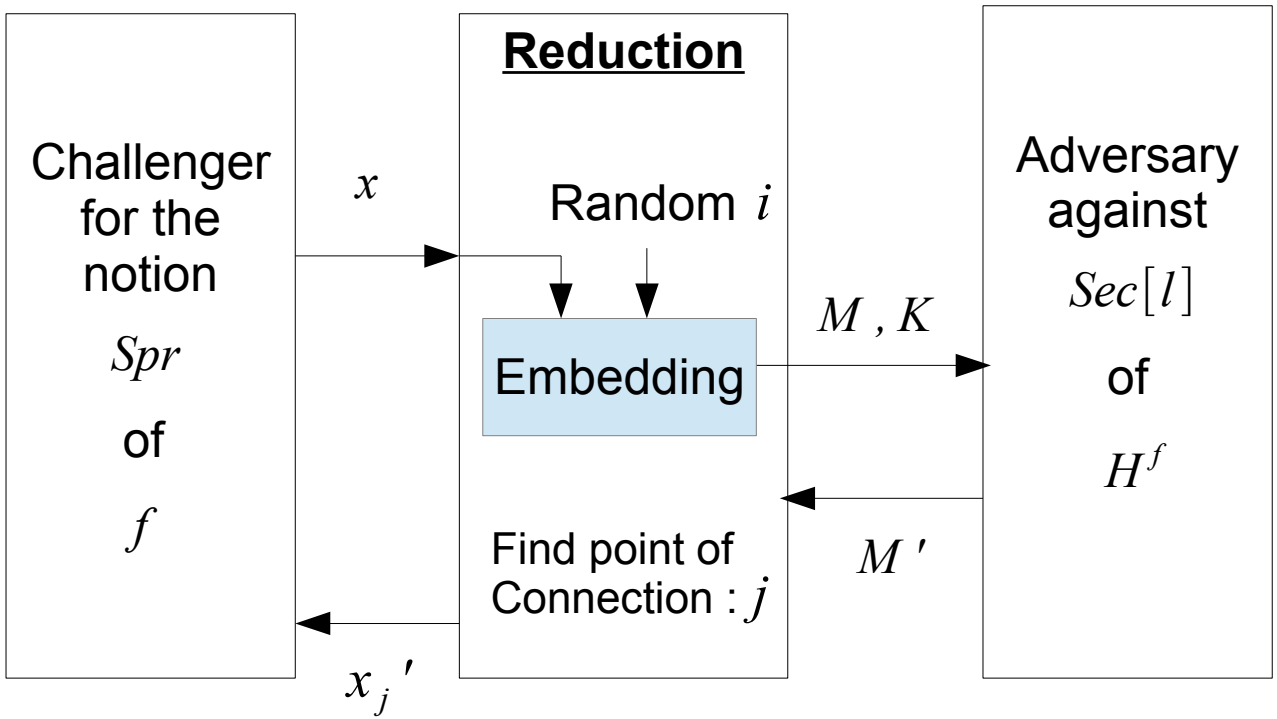
Embedding of the Challenge into the Query



Embedding : an efficient algorithm which computes a uniformly distributed challenge (M, K) from an input (x, i), in time $\mathcal{O}(\ell)$.

Probable Security in the Standard Model

A reduction breaking the Spr notion of f in $t + \mathcal{O}(\ell)$.



The reduction succeeds when

- the adversary succeeds (probability ε) **and**
- point of connection $=$ point of embedding (probability $\frac{1}{\ell}$)

The probability of success of the Reduction is ε/ℓ.

Unavoidable Security Loss

If f is secure for Spr notion :

$$\frac{t + c\ell}{\varepsilon/\ell} \geq 2^n$$

This reduction only gives the lower bound

$$\frac{t}{\varepsilon} \geq \frac{2^n}{\ell} - \frac{c\ell}{\varepsilon}$$

For long messages, the reduction does not guarantee any security ...

Question

Can we get a better reduction ? Is there a narrow-pipe mode with a better reduction ?

Unfortunately, this security loss is unavoidable for a narrow-pipe mode, with this type of reduction.

Thanks for your attention !

Questions ?