Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2

Jian Guo[1,2], San Ling[2], Christian Rechberger[3], Huaxiong Wang[2]

Institute for Infocomm Research, Singapore

Nanyang Technological University, Singapore

K.U.Leuven, and IBBT, Belgium

ASIACRYPT, 06 Dec 2010

2010 — Year of the Tiger

rat, ox, **tiger**, hare, dragon, snake, horse, ram, monkey, rooster, dog, pig

Hash Functions

arbitrary length string $\xrightarrow{H}$ fixed length digest

Hash Functions

$$\text{arbitrary length string} \xrightarrow{H} \text{fixed length digest}$$

Three basic security requirements:

- **Collision resistant**: it is computationally difficult ($2^{n/2}$) to find m, m' such that $H(m) = H(m')$.
- **Preimage resistant**: given digest h, it is computationally difficult (2^n) to find m, such that $H(m) = h$.
- **Second preimage resistant**: given message m, it is computationally difficult (2^{n-k}) to find m', such that $H(m) = H(m')$

Hash Functions

arbitrary length string $\xrightarrow{H}$ fixed length digest

Three basic security requirements:

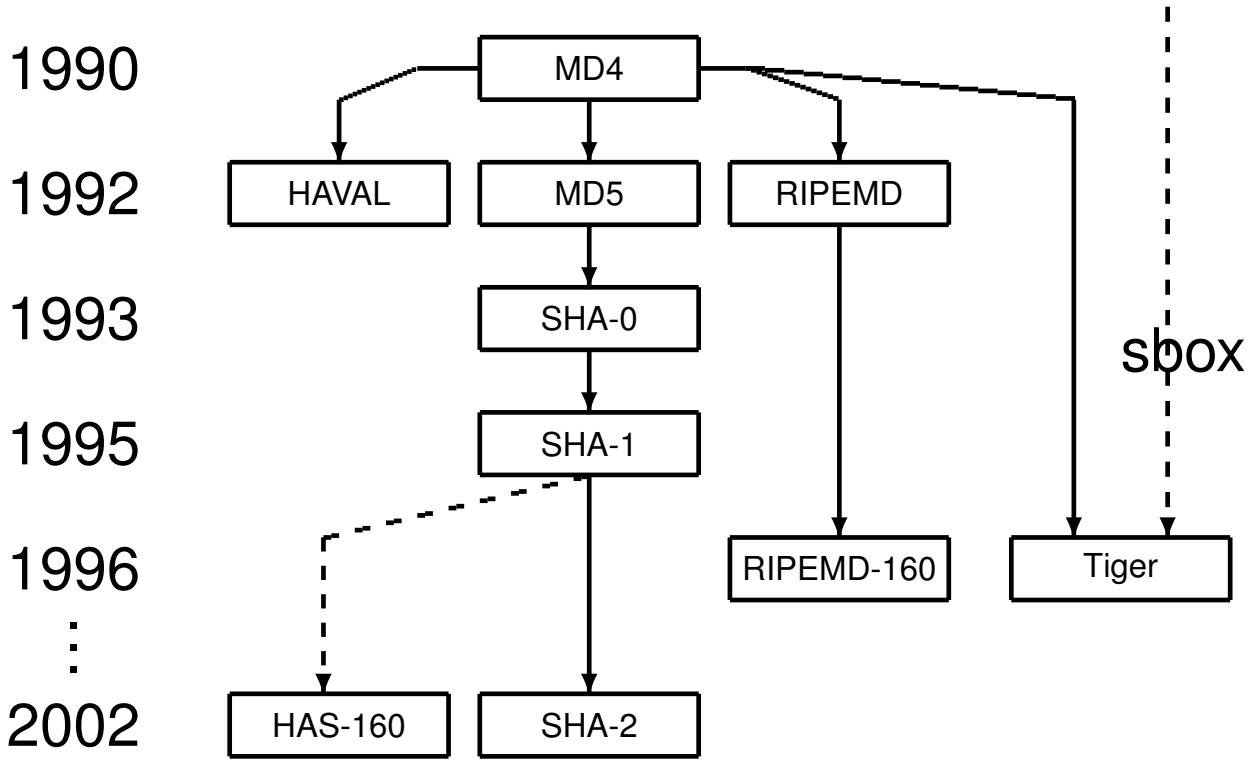
- **Collision resistant**: it is computationally difficult ($2^{n/2}$) to find m, m' such that $H(m) = H(m')$.
- **Preimage resistant**: given digest h, it is computationally difficult (2^n) to find m, such that $H(m) = h$.
- **Second preimage resistant**: given message m, it is computationally difficult (2^{n-k}) to find m', such that $H(m) = H(m')$

H should be easy to compute.

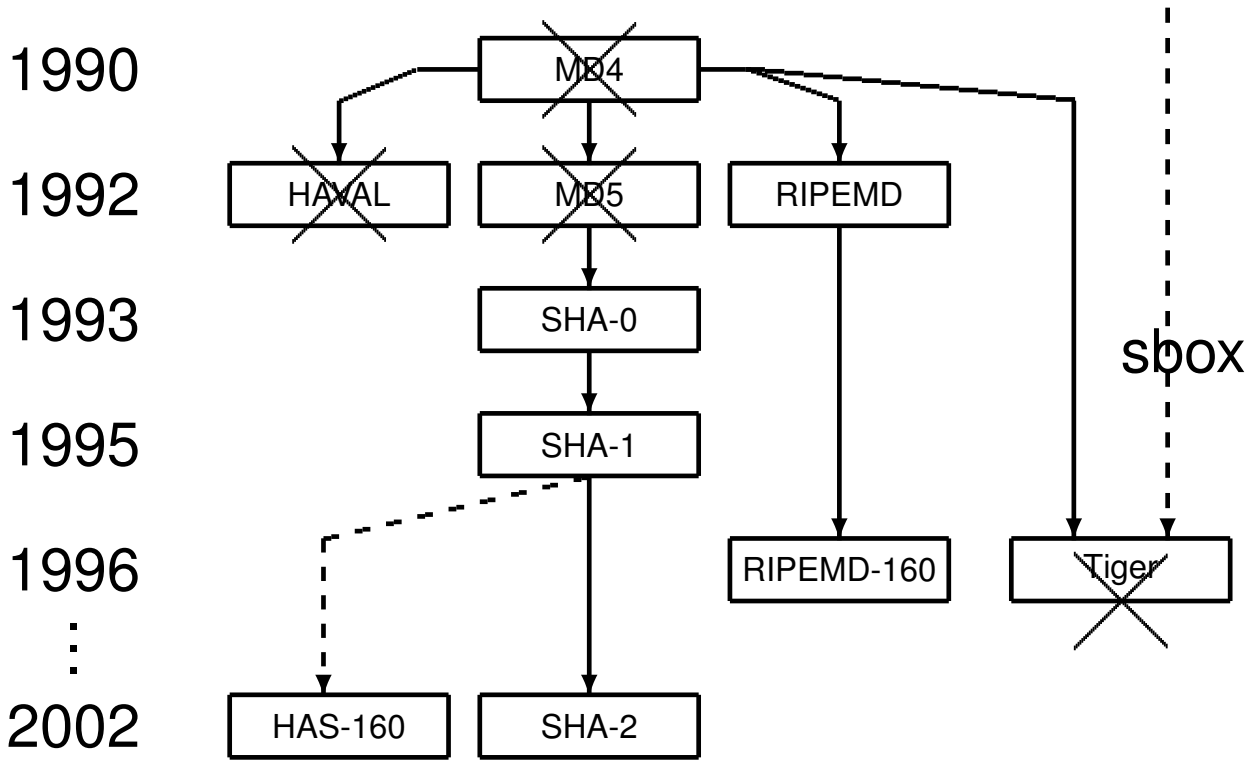
Tiger

- designed by Ross Anderson and Eli Biham
- published in FSE 1996
- used on the *Direct Connect* and *Gnutella* file sharing networks
- 192-bit digest
- ARX, sbox with 64-bit word
- $\sim$ 6.5 cycles per byte (eBASH) — fast!

Meet-in-the-Middle Preimage Attacks

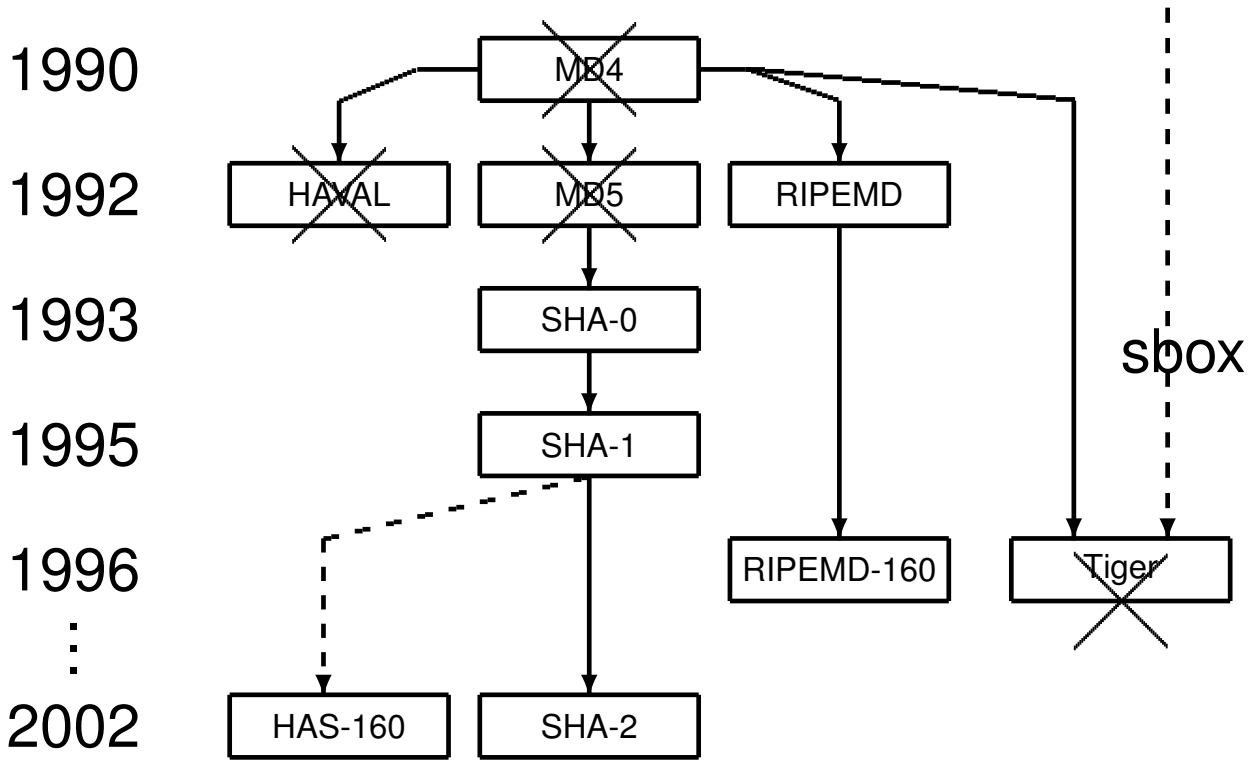


Meet-in-the-Middle Preimage Attacks



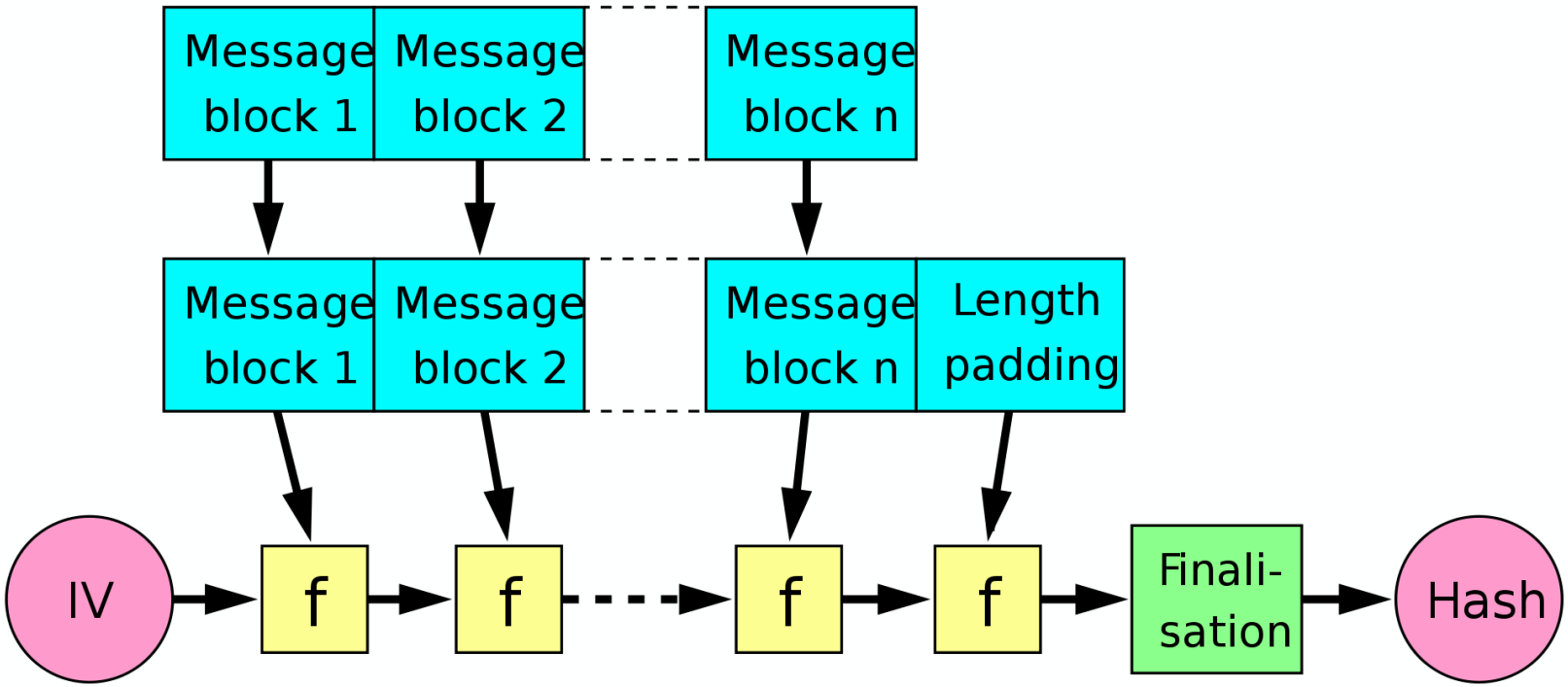
MITM preimage attack is invented by Aoki and Sasaki from 2008, and developed by many.

Meet-in-the-Middle Preimage Attacks



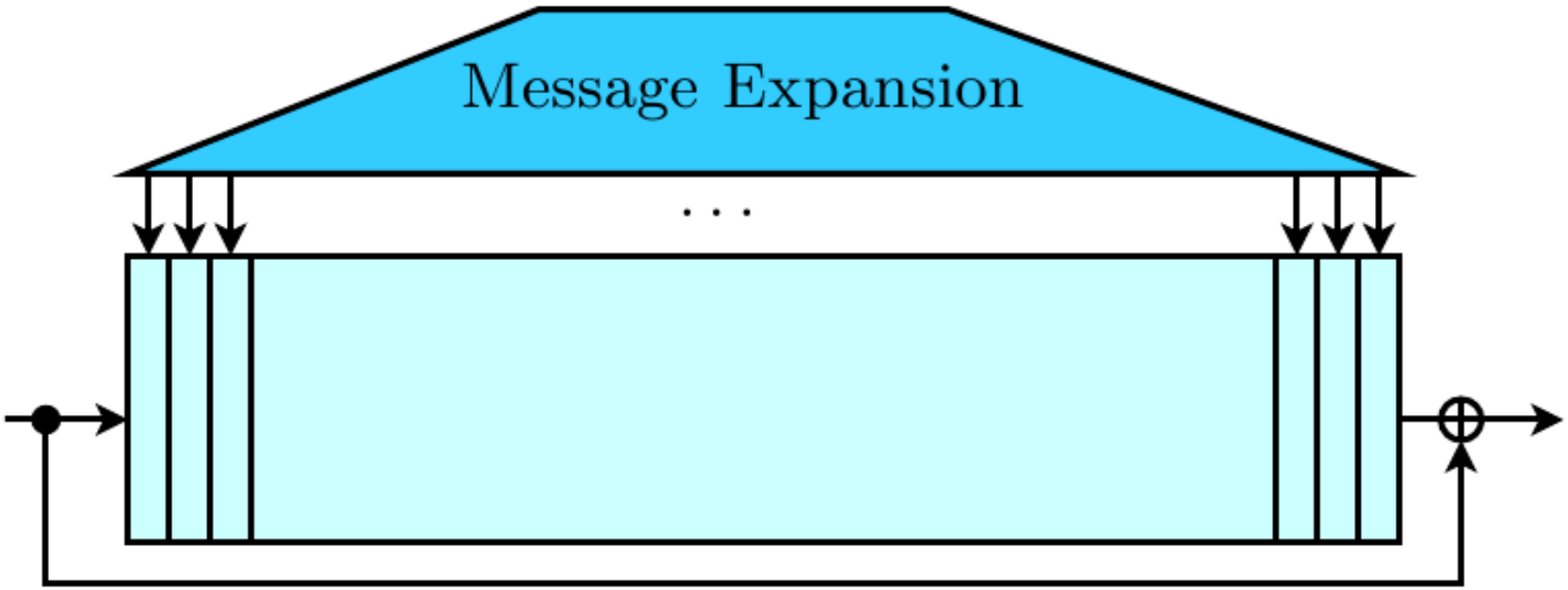
MITM preimage attack is invented by Aoki and Sasaki from 2008, and developed by many.
Applied to full HAVAL-3/4, MD4, MD5, Tiger, and reduced-HAS-160, RIPEMD, SHA-0, SHA-1, SHA-2.

Merkle Damgård Construction



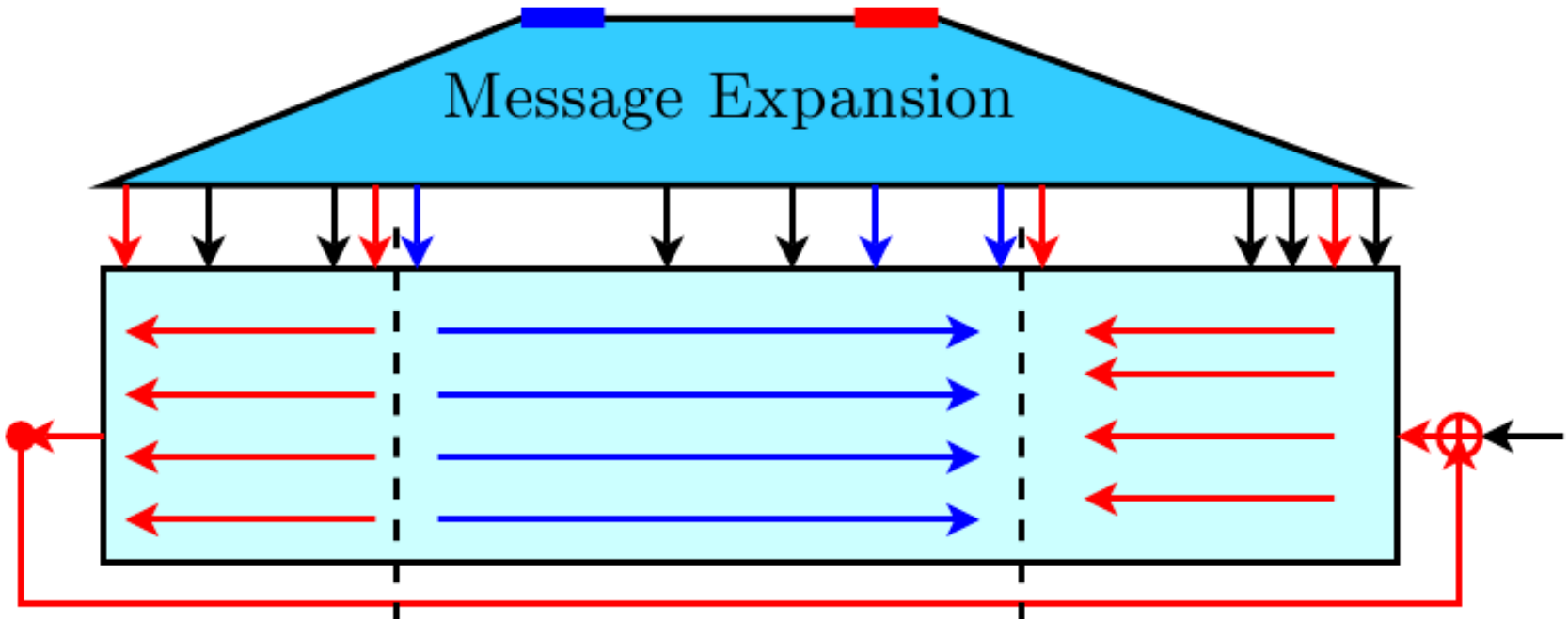
MITM Preimage Attacks: Pseudo-Preimages

Davies-Meyer: $E_m(h) \oplus h$



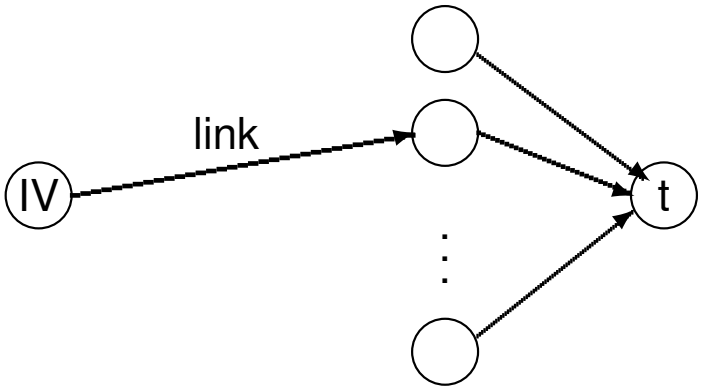
MITM Preimage Attacks: Pseudo-Preimages

Davies-Meyer: $E_m(h) \oplus h$



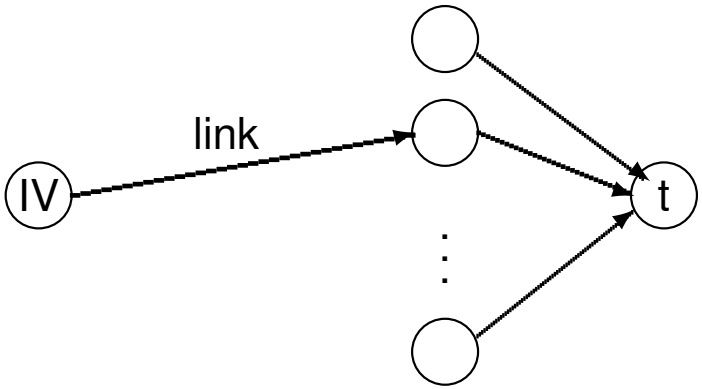
Converting Pseudo-Preimages to Preimages

First Method:

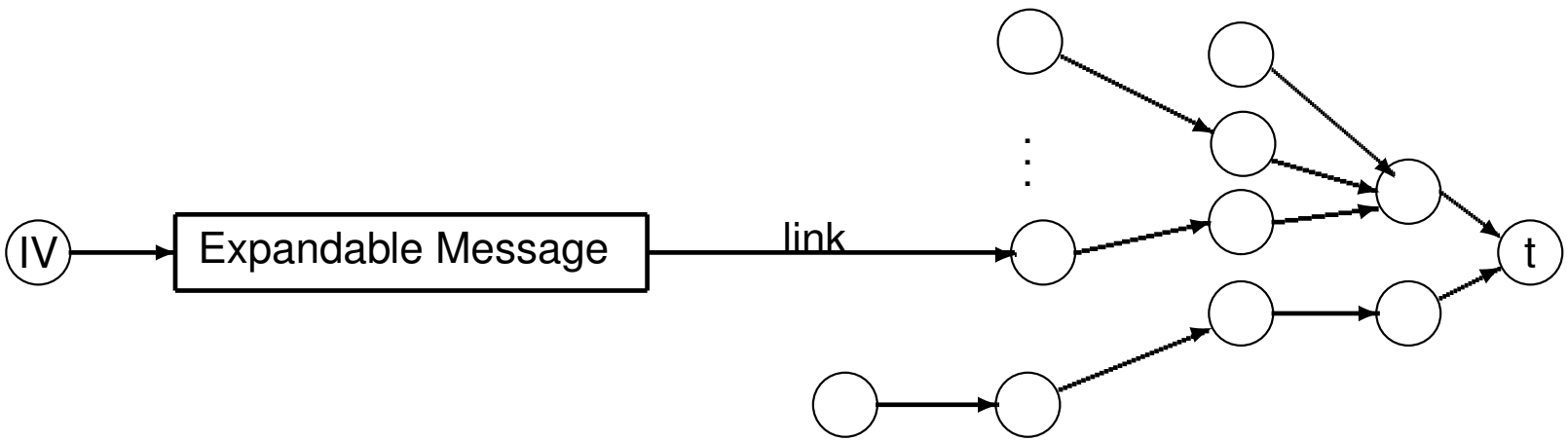


Converting Pseudo-Preimages to Preimages

First Method:

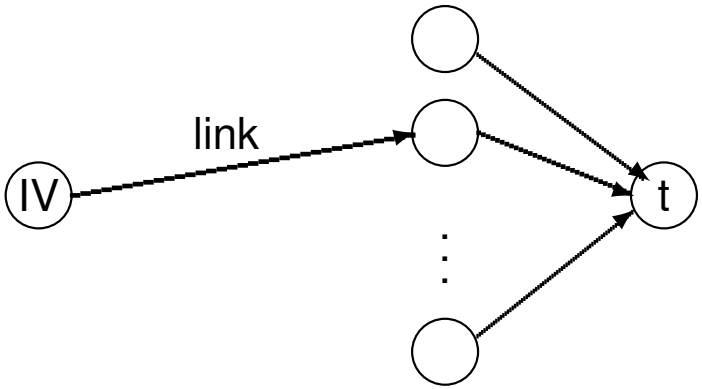


Second Method:

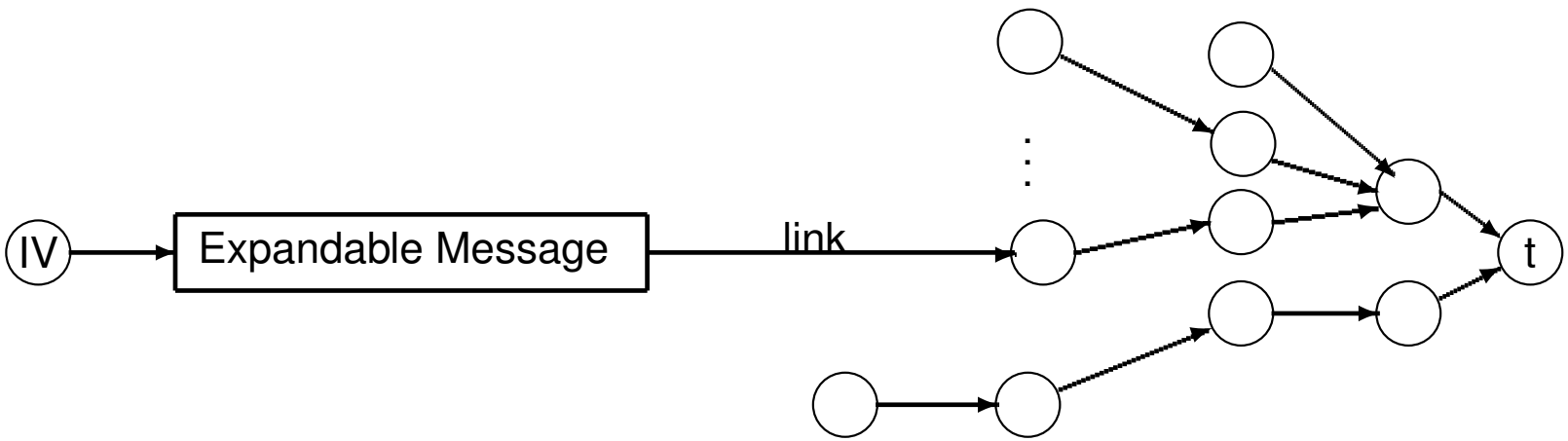


Converting Pseudo-Preimages to Preimages

First Method:



Second Method:



Third Method: large precomputation

Result Summary

- Enriched the toolbox for MITM preimage attacks.
- First preimage attack against full Tiger
- Improved best known preimage attacks against MD4 and SHA-2

Thank you!