Cryptanalysis of the Yi-Lam hash

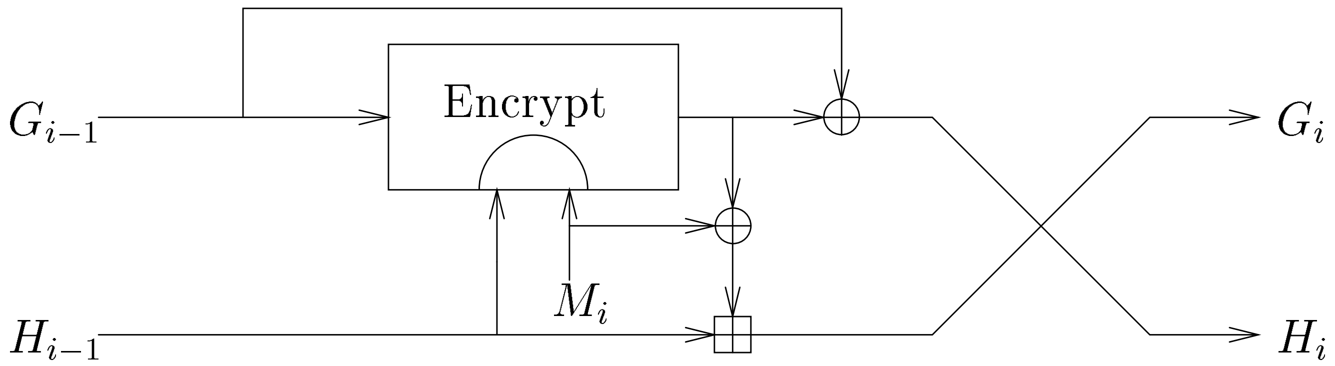
David Wagner

U.C. Berkeley

daw@cs.berkeley.edu

The Yi-Lam hash

- Define an iterated compression function h as follows:



- Define Hash$(M_1, \ldots, M_n) := G_n || H_n$.

Question. *Is this hash function secure?*

Outline of the talk

- Pseudo-collision attacks
  - Attacks on a simplified variant
  - Attacks on the full hash
- Full collision attacks
  - Analysis of a simplified variant
  - Attacks on the full hash

Towards a security analysis

Problem. Yi-Lam hash mixes addition ($\boxplus$) with xor ($\oplus$).

Solution. First, study simplified variants:

- Change all additions to xors.
- Consider pseudo-collision (i.e., free-start) attacks.

Then, generalize the results.

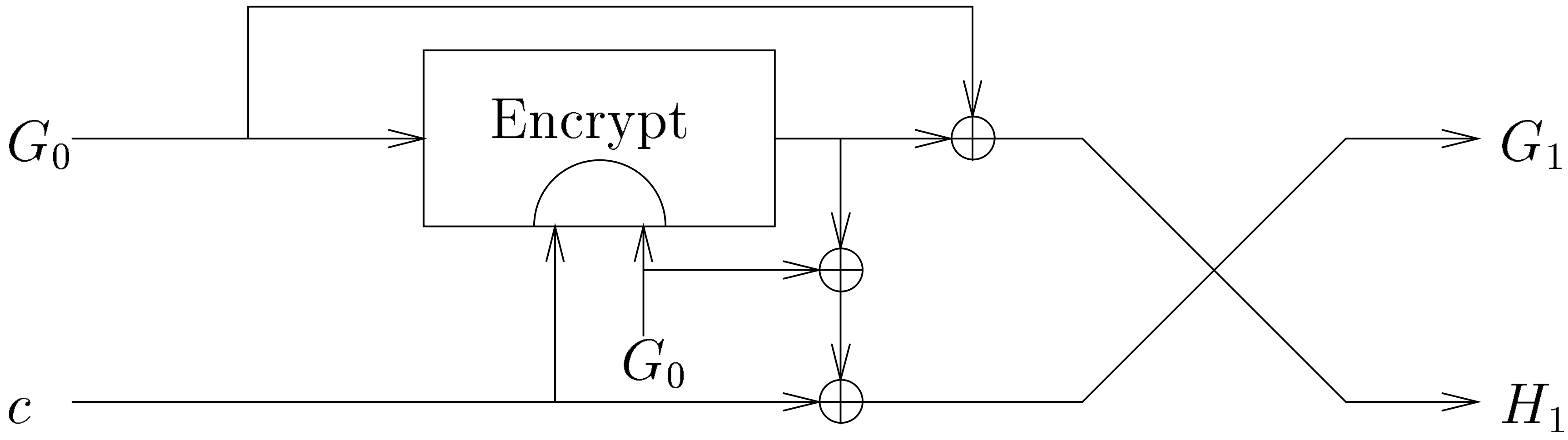
Pseudo-collision attacks

Attacker's goal. Find M, M' and $G_0||H_0, G'_0||H'_0$ so that $h(G_0||H_0, M) = h(G'_0||H'_0, M')$.

This is called a pseudo-collision attack.

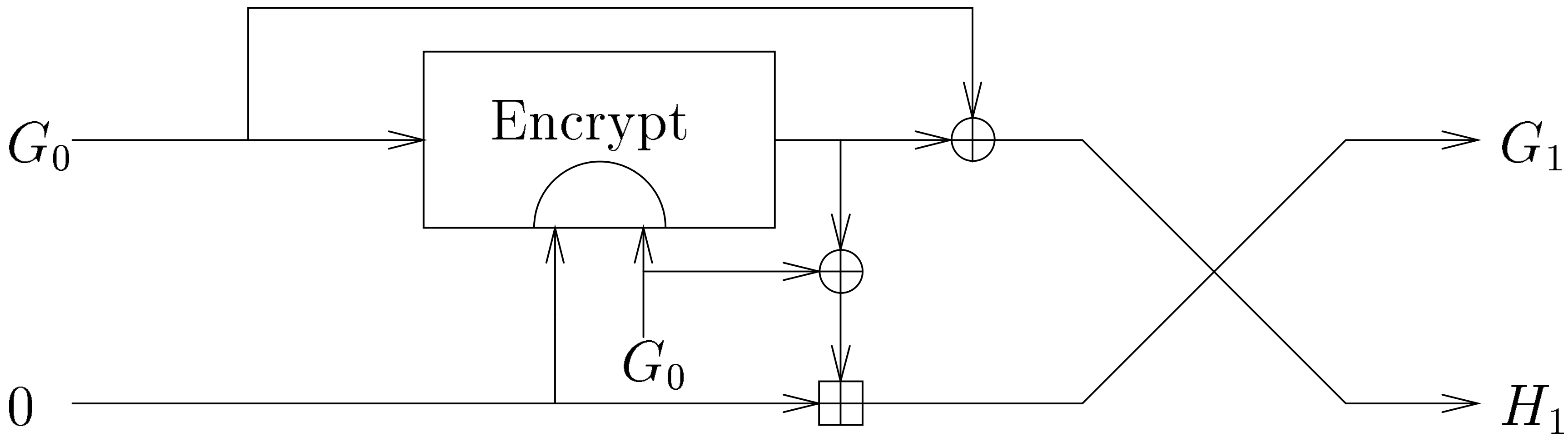
- Also known as a free-start collision attack.
- It is only of theoretical interest, but it makes analysis easier.

Pseudo-collisions in a simplified variant



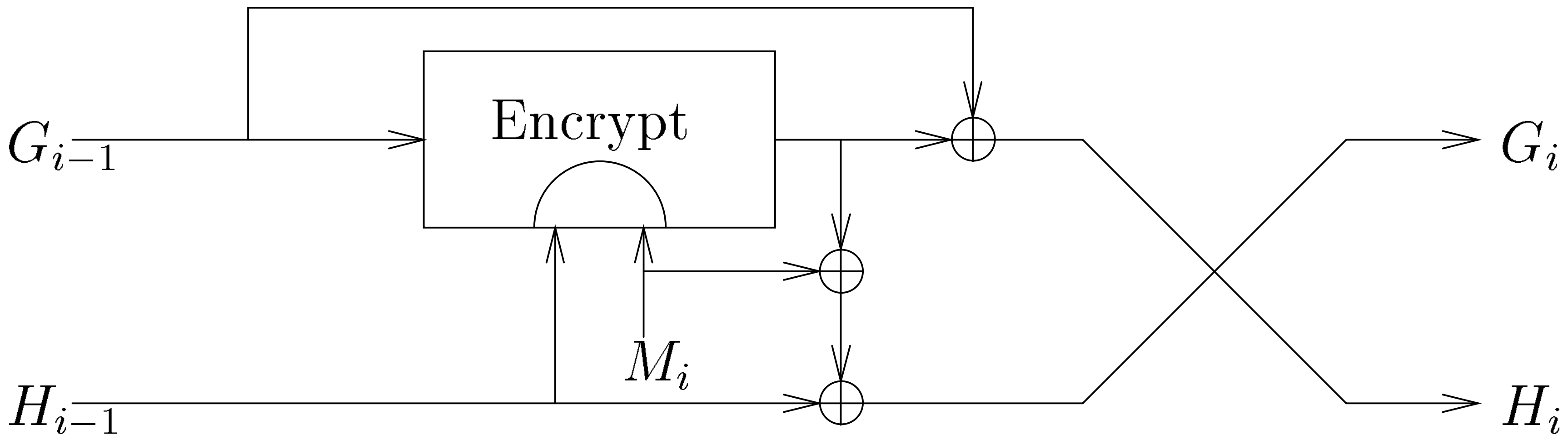
- Fix $H_0 = c$ in advance.
- Vary G_0 over $2^{m/2}$ values, and use $M_1 = G_0$.
- Note that $H_1 = G_1 \oplus c$, hence a collision in G_1 leads to an automatic collision in H_1, too. $\Rightarrow 2^{m/2}$ complexity.

Pseudo-collisions for the full hash



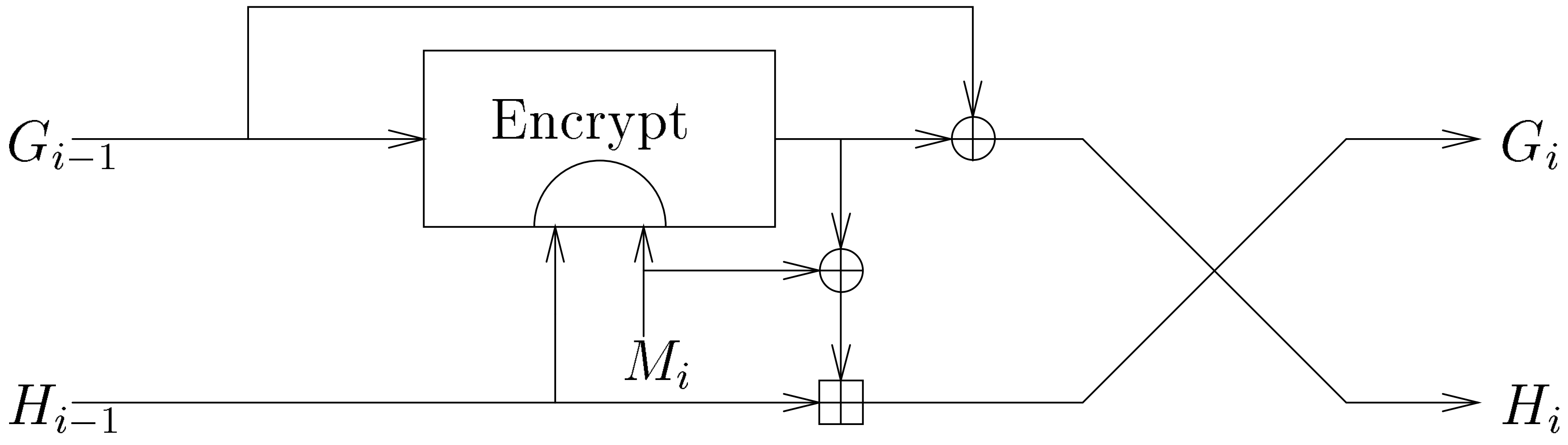
- Set $H_0 = 0$.
- Vary G_0 over $2^{m/2}$ values, and force $M_1 = G_0$.
- Note that $H_1 = G_1 \boxplus 0 = G_1$, and the rest is as before.

Full collisions for a simplified variant



- Vary G_{i-1}, H_{i-1} over $2^{m/2}$ values.
- Set $M_i := G_{i-1} \oplus H_{i-1}$.
- Note that $G_i = H_i$, and the rest is as before.

Full collisions for the full hash



- Vary G_{i-1}, H_{i-1} over $2^{.71m}$ values.
- Set $M_i := G_{i-1} \oplus (-H_{i-1})$.
- If $H_i = H_i'$, then

$$(H_i \oplus (-H_{i-1})) \boxplus H_{i-1} \equiv (H_i \oplus (-H_{i-1}')) \boxplus H_{i-1}'$$

with good probability; then $G_i = G_i'$ and the rest is as before.

Conclusions

- Collisions may be found faster than brute force
  - Complexity: $2^{.71m}$ work
  - Attack is practical, for typical parameters (e.g., $m = 64$)
- Simply mixing addition and xor is not sufficient
  - Attack exploited ability to control the carry bits
  - Designers should not rely too much on mixing add & xor

The Yi-Lam hash