

How to Build a Hash Function?

Yevgeniy Dodis (NYU) and Victor Shoup (NYU)



Hash Design Problem

Hash functions are used for:

- message digests
- key derivation functions
- message authentication codes
- random oracles
- signatures, encryption, ...

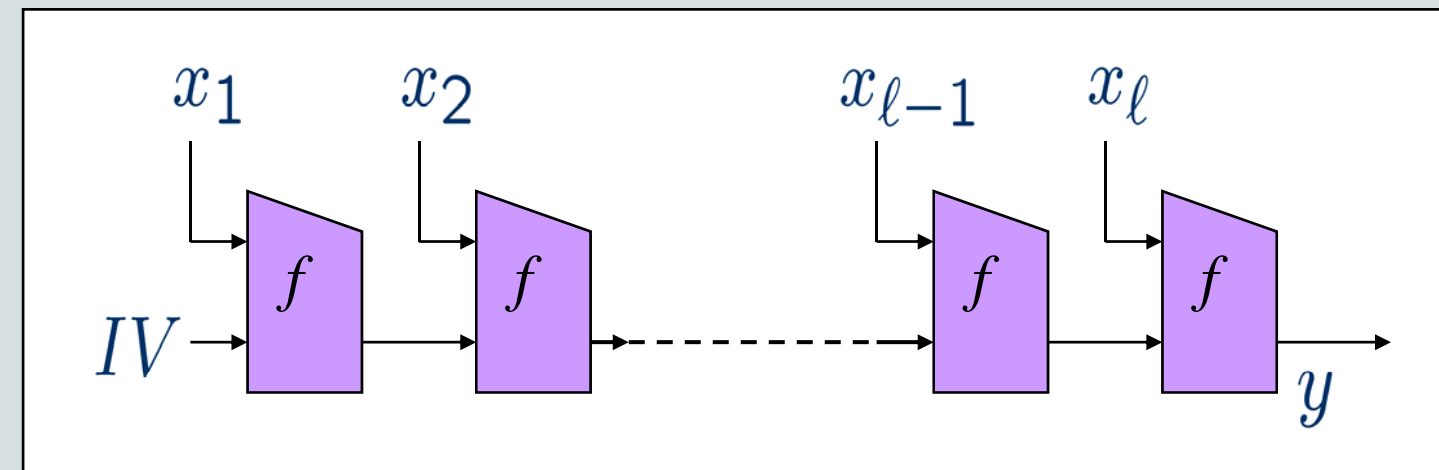
Recently, many attacks on existing hash functions found

- **New methodologies needed!!!**

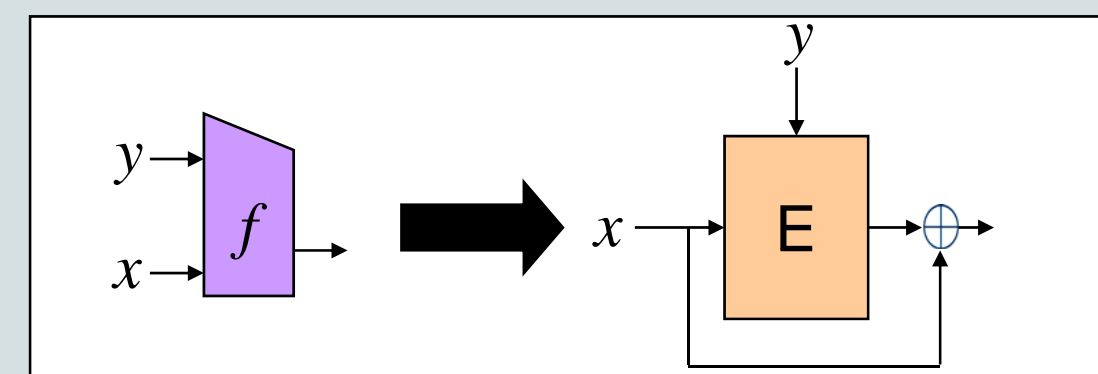
Our work encompasses new design criteria and novel implementations of hash functions which resist above deficiencies.

Common design methodology: build variable-input length (VIL) hash from a fixed-input length (FIL) primitive:

- FIL *compression function* f . Variants of cascade construction are used:



- *Block cipher* E . Build compression function via Davies-Meyer transform:



Known Approaches

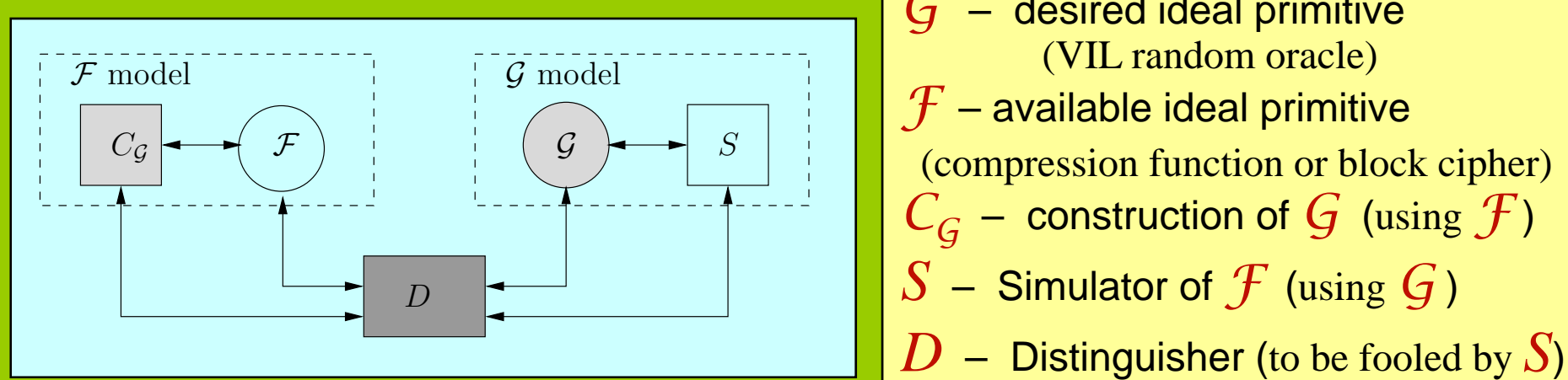
- Study one property at a time
- Theory: analyze new, ad hoc construction for each property
- Practice: use existing (often insecure) constructions and “hope for the best”

New Approaches

- Multi-property preservation with one design – both theory and practice
- New design criteria
 - ❖ Indifferentiability from random oracle
- New, provably secure constructions

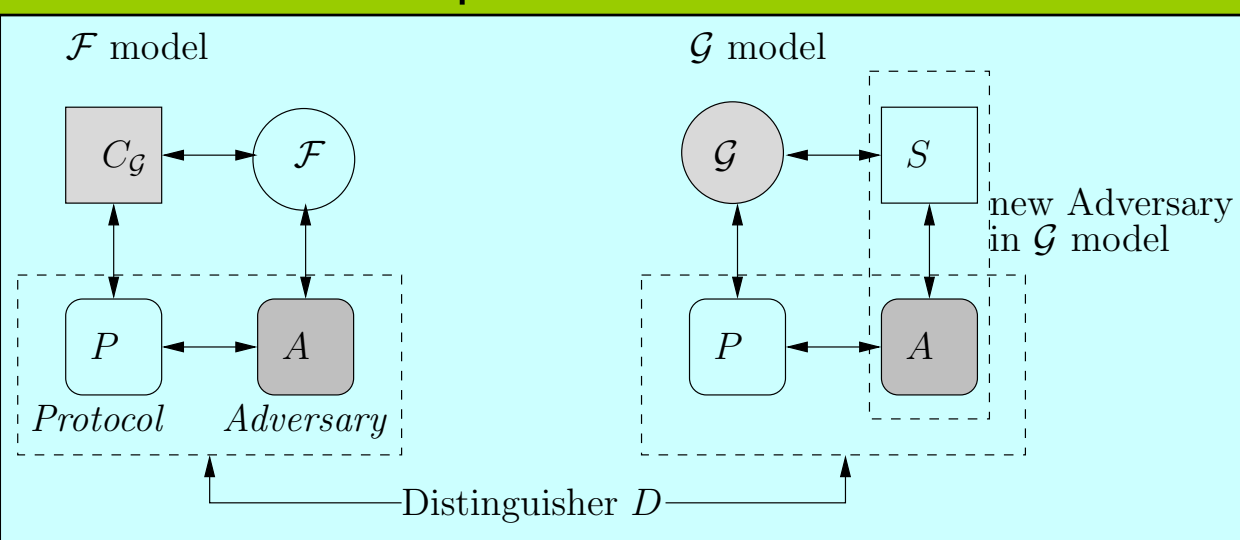
Indifferentiability from Random Oracle

Constructing ideal primitive \mathcal{G} using \mathcal{F}



\mathcal{G} – desired ideal primitive (VIL random oracle)
 \mathcal{F} – available ideal primitive (compression function or block cipher)
 C_G – construction of \mathcal{G} (using \mathcal{F})
 S – Simulator of \mathcal{F} (using \mathcal{G})
 D – Distinguisher (to be fooled by S)

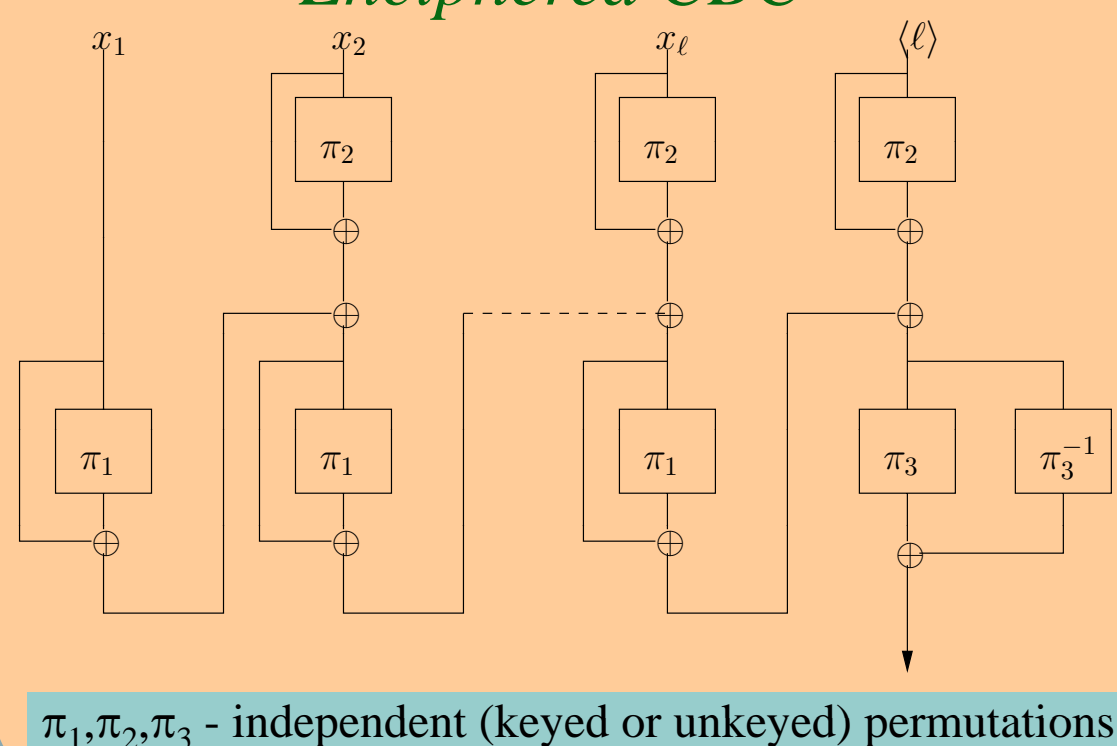
Composition Theorem



Any protocol P secure in \mathcal{G} model is also secure in \mathcal{F} model when C_G is used to implement \mathcal{G} (using \mathcal{F})

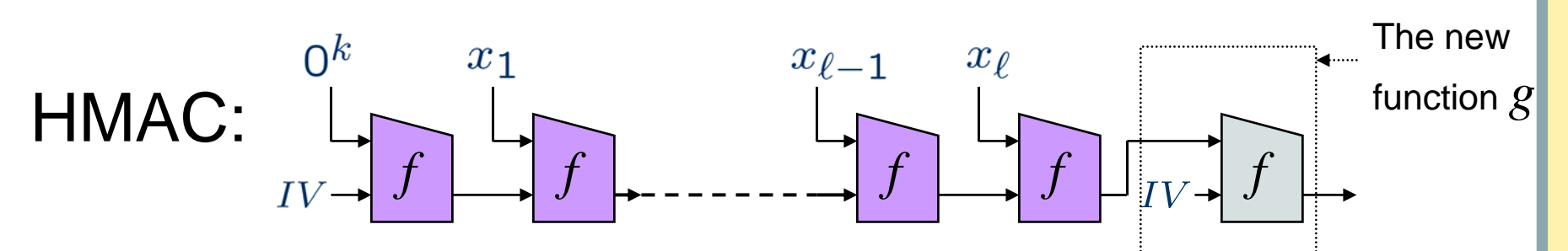
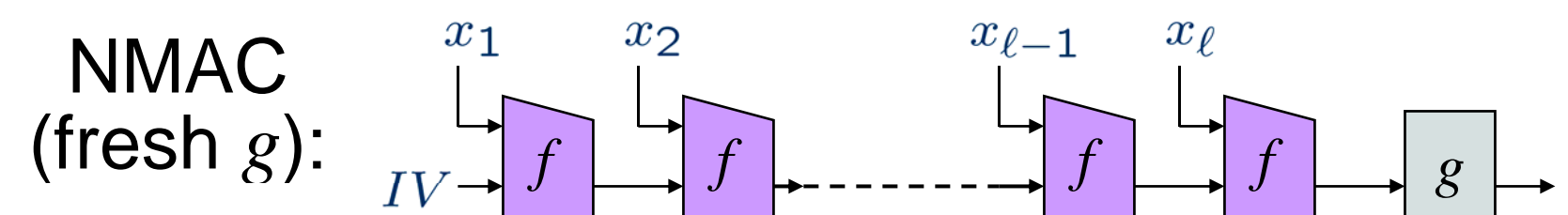
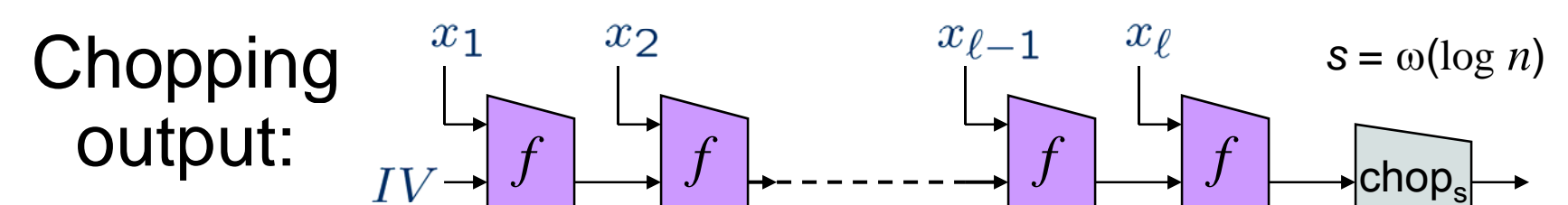
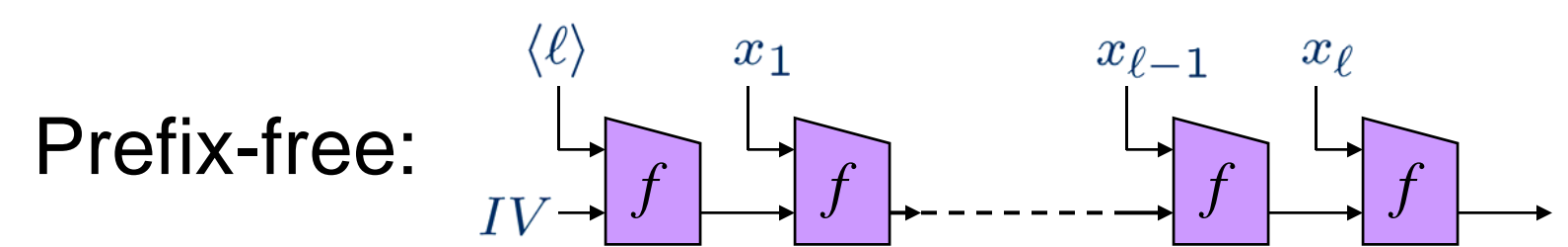
New Mode of Operation for Block Ciphers

Enciphered CBC



- Multi-property preserving mode
 - * (only) twice slower than CBC
 - * fixed keys, no re-keying !
- Preserves pseudorandomness and *unforgeability*:
 - * hedge against block cipher security
 - * first constant-rate domain extension of length-preserving MACs
- Yields random oracle (and, thus, collision-resistant hash function) in the ideal cipher model

Provably Indifferentiable Constructions



- All constructions can be implemented via “black-box calls” to SHA (or any cascade)
- All constructions work in the ideal cipher model with the Davies-Meyer construction:

$$f(x \parallel y) = E_x(y) \oplus y$$