MODES OF OPERATION

2-D Encryption Mode

Ahmed A. Belal

Moez A. Abdel-Gawad

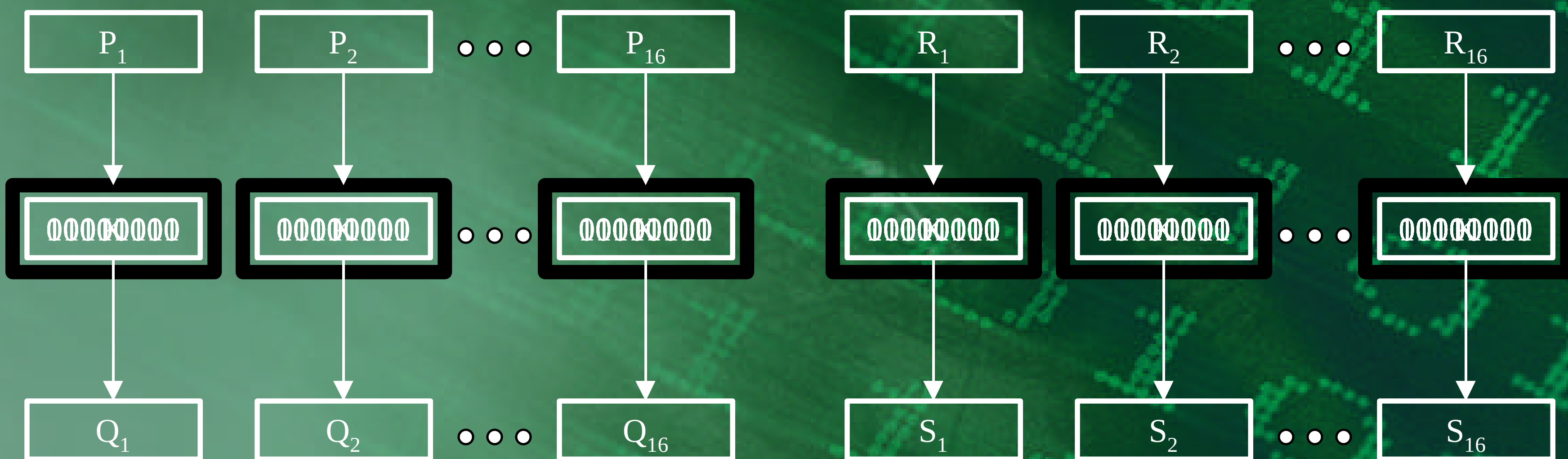
2DEM

$P = < P_1\, P_2\, P_3 \ldots P_{16} >$

Each $P_i = < P_i^{\,1}\, P_i^{\,2}\, P_i^{\,3} \ldots P_i^{\,16} >$

Each $Q_i = < Q_i^{\,1}\, Q_i^{\,2}\, Q_i^{\,3} \ldots Q_i^{\,16} >$

Set Each $R_i = < Q_1^{\,i}\, Q_2^{\,i}\, Q_3^{\,i} \ldots Q_{16}^{\,i} >$



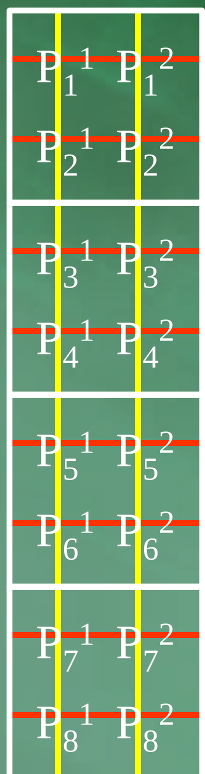
Each $S_i = < S_i^{\,1}\, S_i^{\,2}\, S_i^{\,3} \ldots S_i^{\,16} >$

Then $C = < C_1\, C_2\, C_3 \ldots C_{16} >$

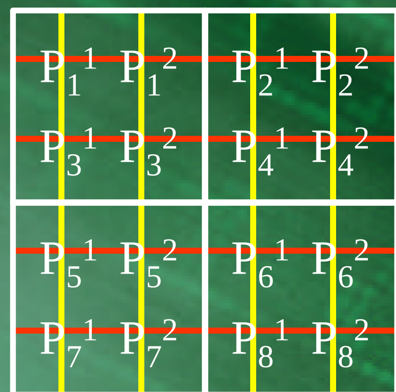
Where Each $C_i = < S_1^{\,i}\, S_2^{\,i}\, S_3^{\,i} \ldots S_{16}^{\,i} >$

2DEM

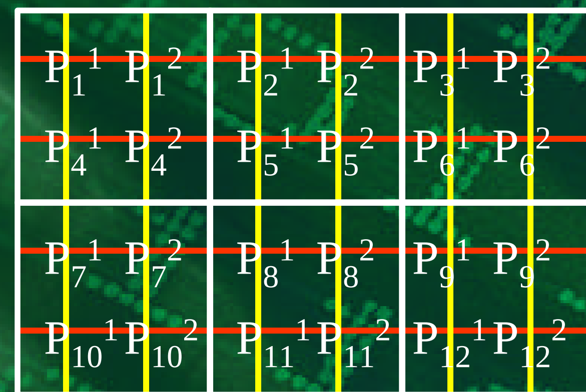
BPR = Blocks Per Row



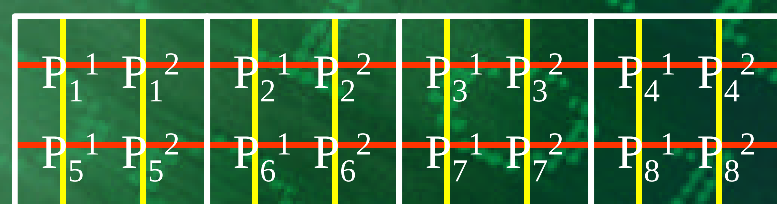
BPR = 1



BPR = 2



BPR = 3



BPR = 4

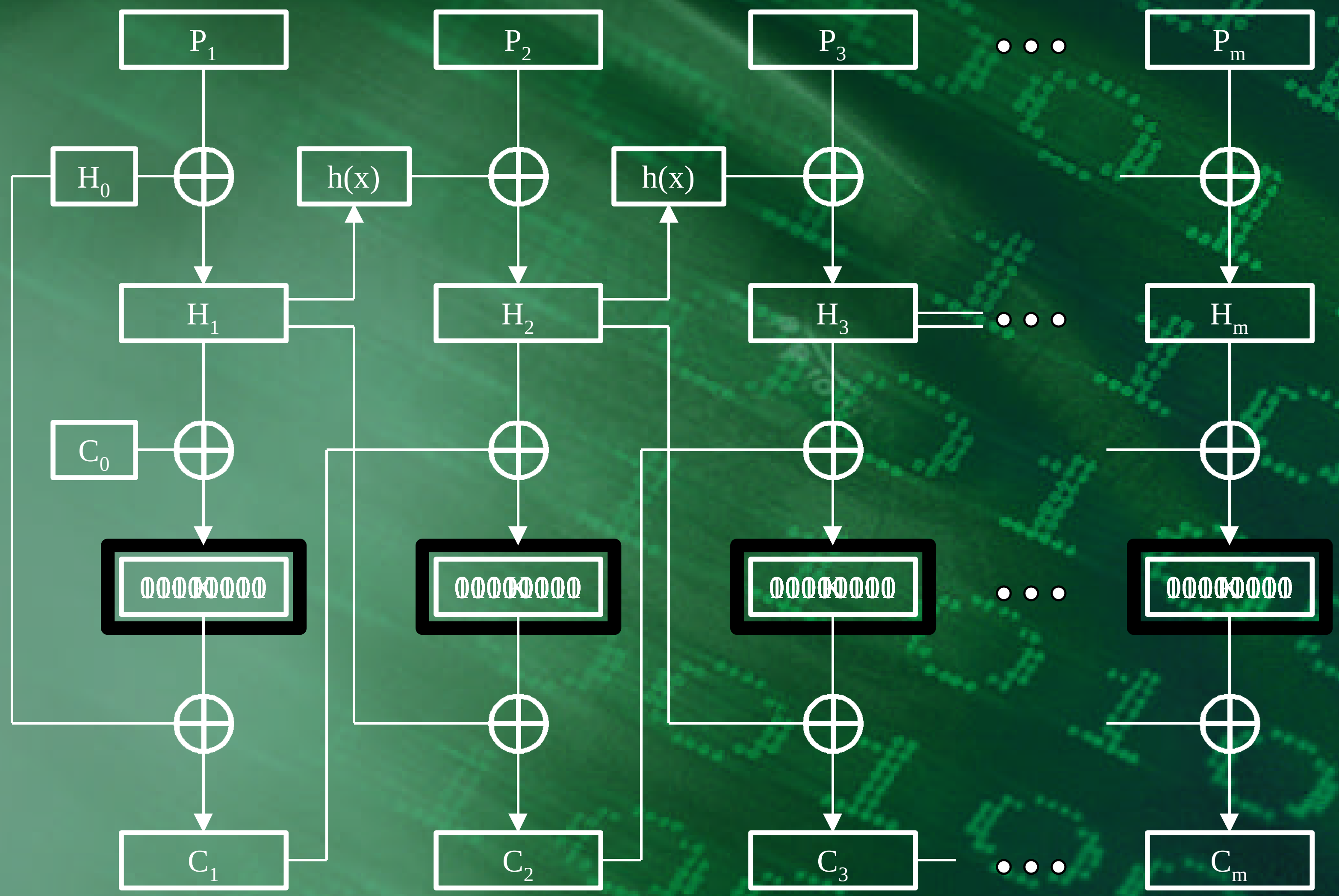
2DEM

- **Works great with images**
- **BPR value and Key needed**
- **Resistance to certain attacks due to interleaving**

Accumulated Block Chaining Mode

Lars R. Knudsen

ABC



Where $h(x) = x$ or $h(x) = x^{<<1}$

ABC

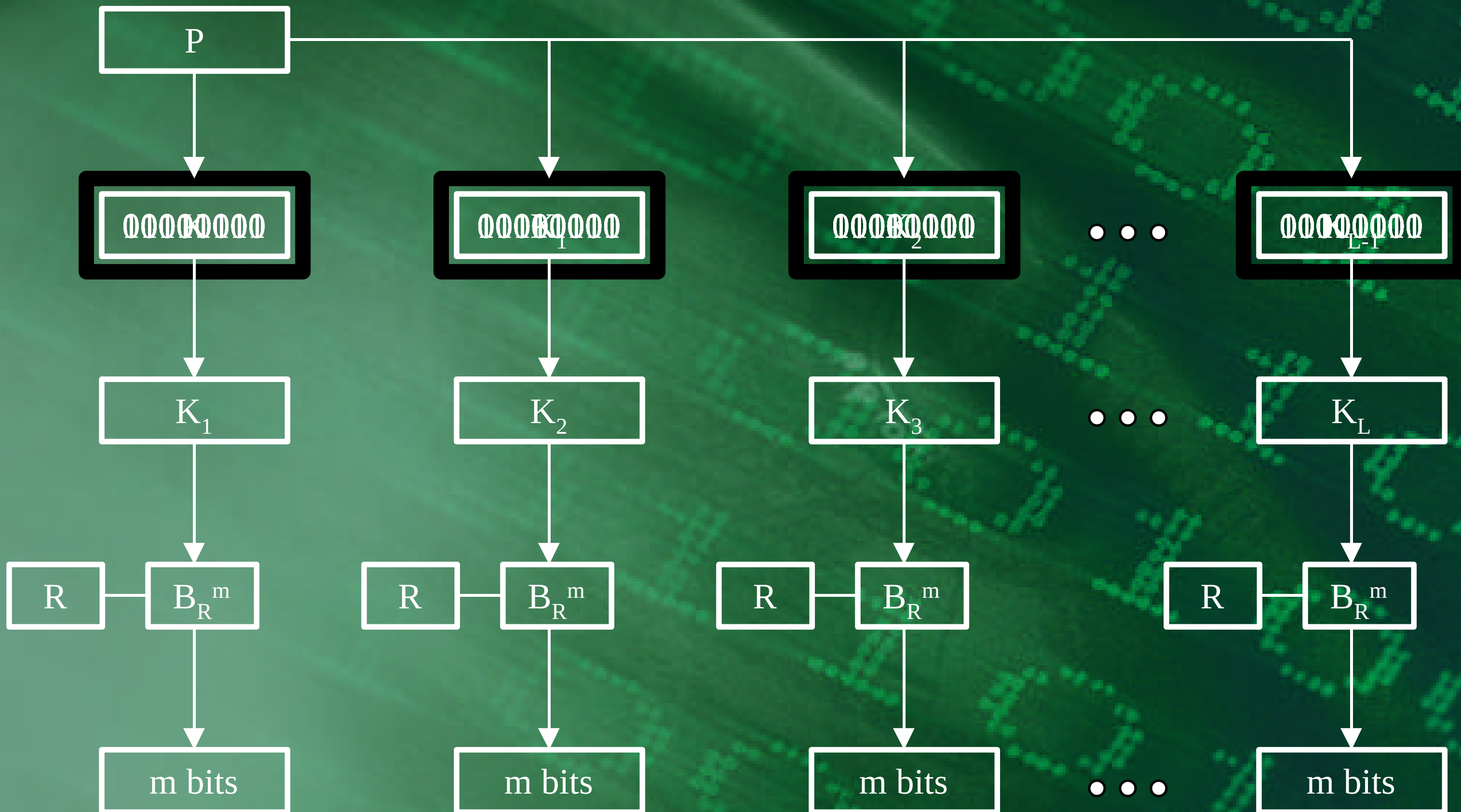
- **Has infinite error propagation**
- **Authentication is not intended as part of mode**
- **Infinite error propagation provides more diffusion**
- **2 initial vectors and Key needed**
- **The mode acts more like a giant block cipher**
- **Resists birthday attacks**

Key Feedback Mode

Johan Håstad

Mats Näslund

KFB



Where R is mxn matrix

and B is multiplication of R and K_i mod 2

KFB

- **Random Bit Generator**
- **Initial matrix, constant, and Key needed**
- **Does not assume that the block cipher is a pseudo-random permutation**
- **Does assume that one or more iterations of the block cipher (with varying keys and a fixed plaintext) are hard to invert**
- **Under this assumption, the KFB outputs are pseudo-random**

Propagating Cipher Feedback Mode

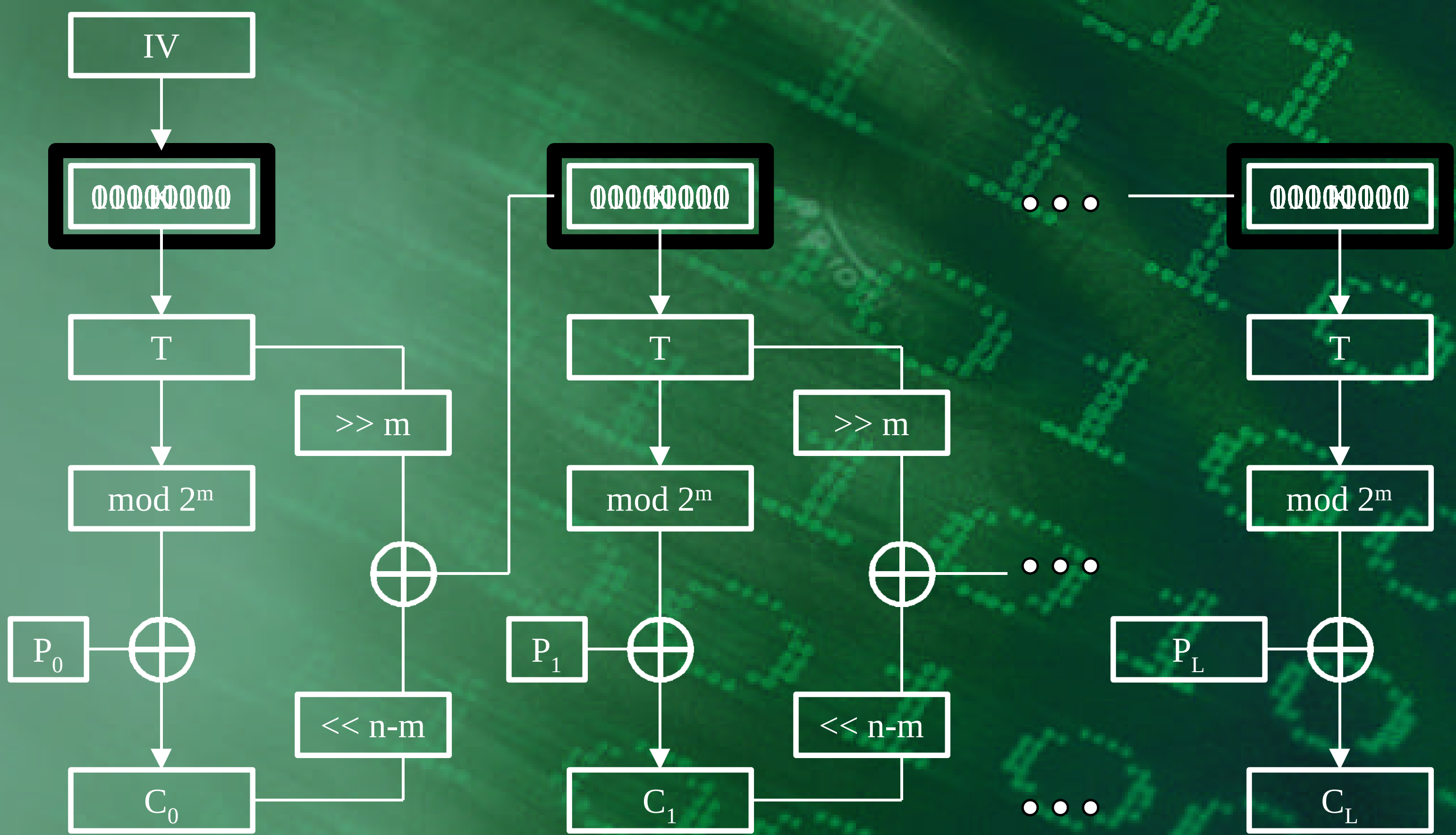
Henrick Hellström

PCFB

L = # of plaintext blocks $P = (P_1, P_2, \ldots P_L)$ Each P_i is m bits long

n = number of bits in the key

m = number of bits in each plaintext block



PCFB

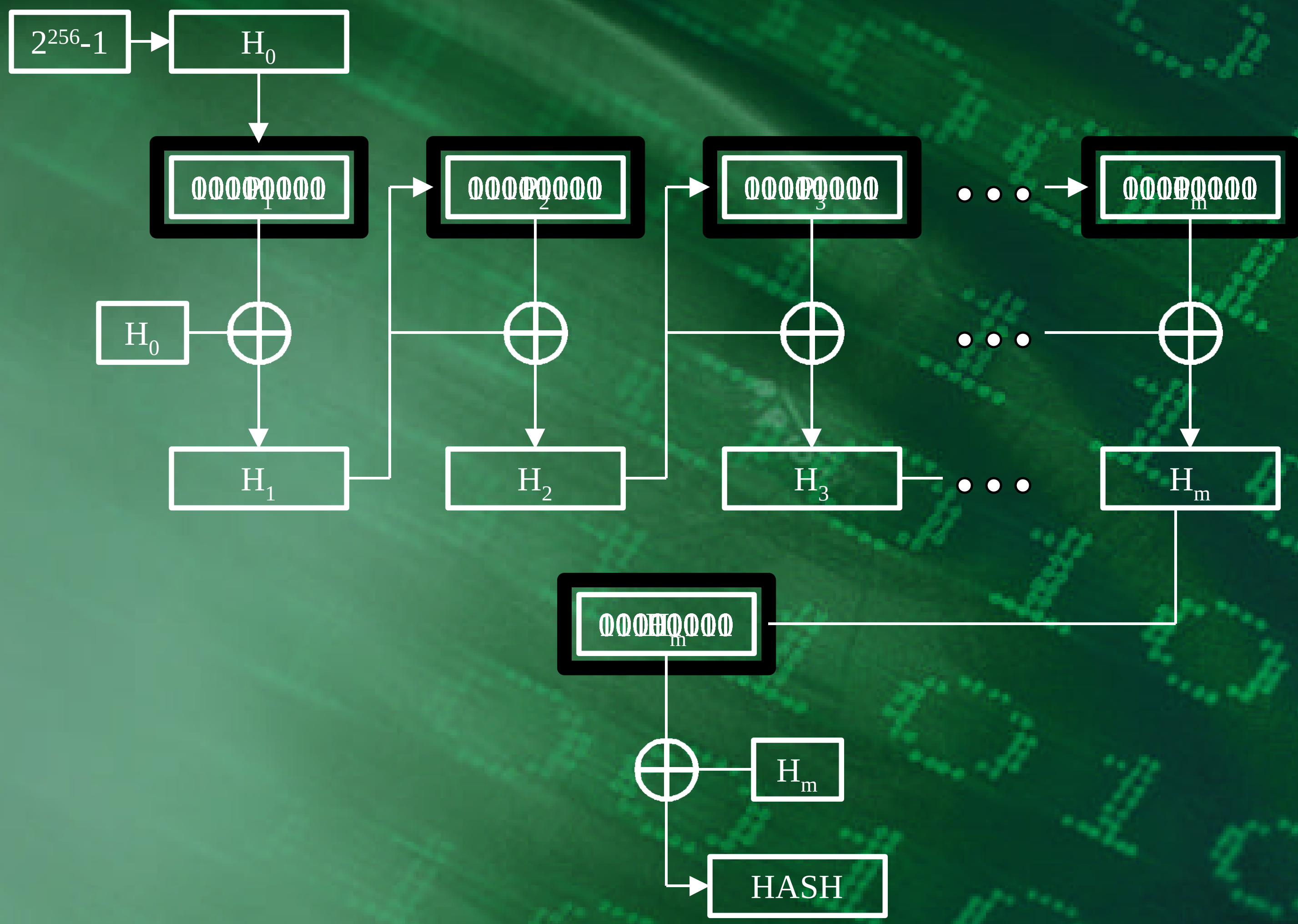
- **Has two way error propagation**
- **Claims that no additional authentication is needed**
- **Authentication mode was proposed**
- **Initial vector and Key needed**

AES-hash

Bram Cohen

Ben Laurie

AES-hash



P is padded with 0’s to the next odd multiple of 128 bits and then appended with the 128-bit Big Endian encoding of the number of bits in the original file. Each P_i is 256 bits.

AES-hash

- **Uses AES-256**
- **Variation of the Davies-Meyer hash construction**
- **Using last step prevents an adversary from creating a new hash for a related message**
- **Only the Key is needed**

QUESTIONS