Self-Defence Against Fresh Fruit

Gaëtan Leurent

École Normale Supérieure
Paris, France

How to defend yourself against a man armed with a banana

How to defend yourself against a man armed with a banana

1. First of all you force him to drop the banana;
2. then, second, you eat the banana, thus disarming him.
3. You have now rendered him 'elpless.

How to defend yourself against a man armed with a banana

1. First of all you force him to drop the banana;
2. then, second, you eat the banana, thus disarming him.
3. You have now rendered him 'elpless.

How to defend yourself against a man armed with a banana

1. First of all you force him to drop the banana;
2. then, second, you eat the banana, thus disarming him.
3. You have now rendered him 'elpless.

And Now for Something Completely Different

How to attack a hash function with a banana

New notion introduced by Aumasson.

Definition ([Aumasson 2010])

A banana is a non-randomness property in a compression function.

See also, distinguisher, pseudo-distinguisher, open-door distinguisher, known-key distinguisher, free-start distinguisher, non-ideality, ...

- Easier to pronounce.

How to attack a hash function with a banana

New notion introduced by Aumasson.

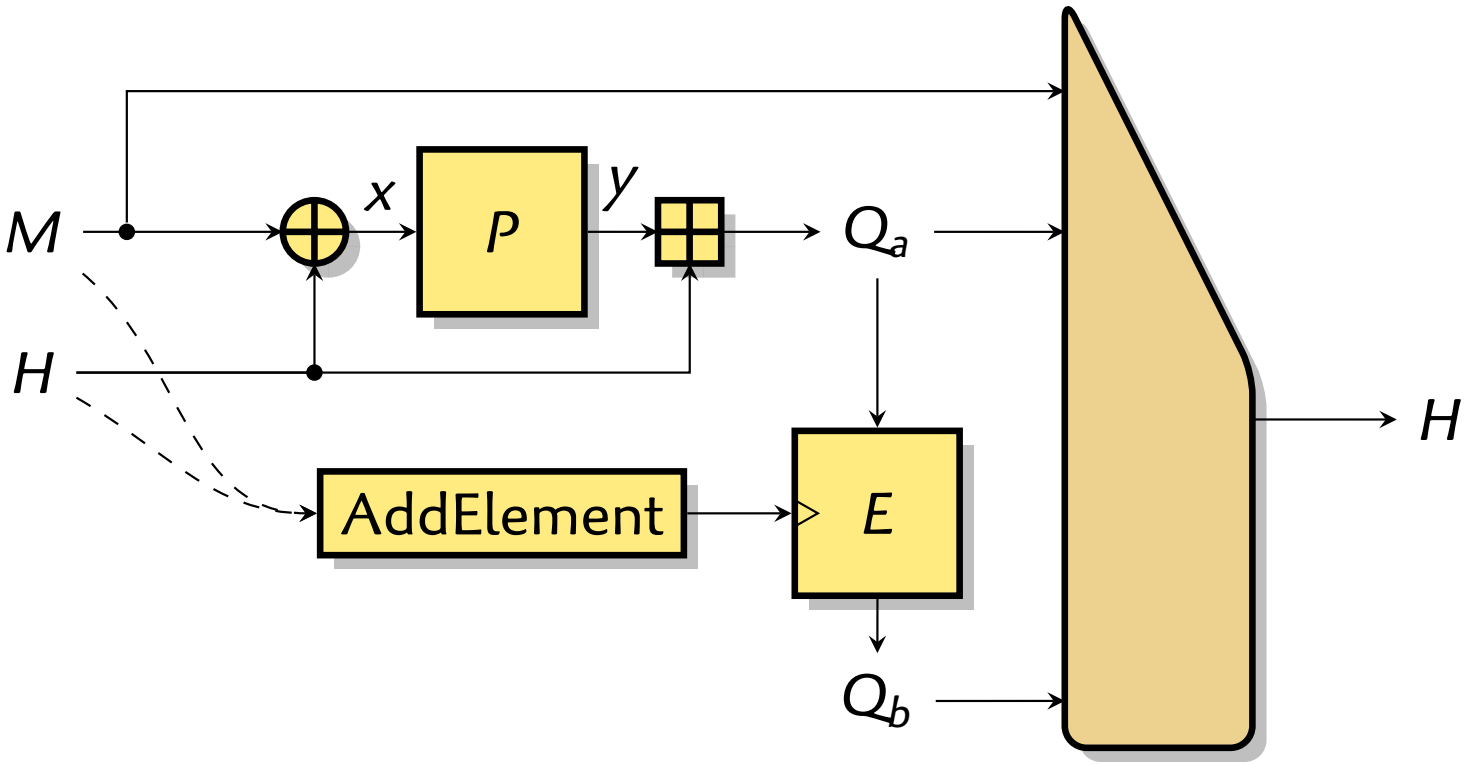
Definition ([Aumasson 2010])

A banana is a non-randomness property in a compression function.

See also, distinguisher, pseudo-distinguisher, open-door distinguisher, known-key distinguisher, free-start distinguisher, non-ideality, ...

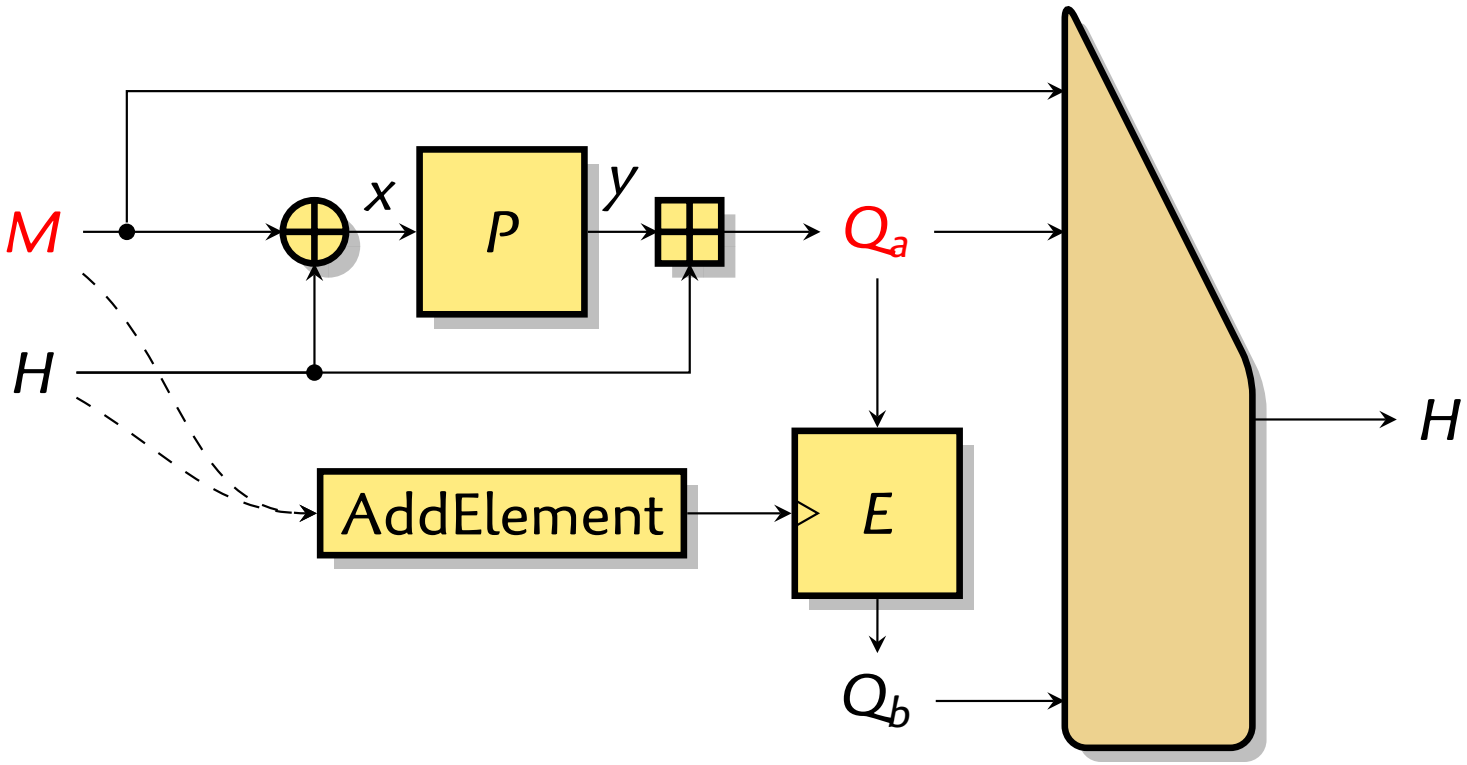
- Easier to pronounce.

Banana Midnight Wish



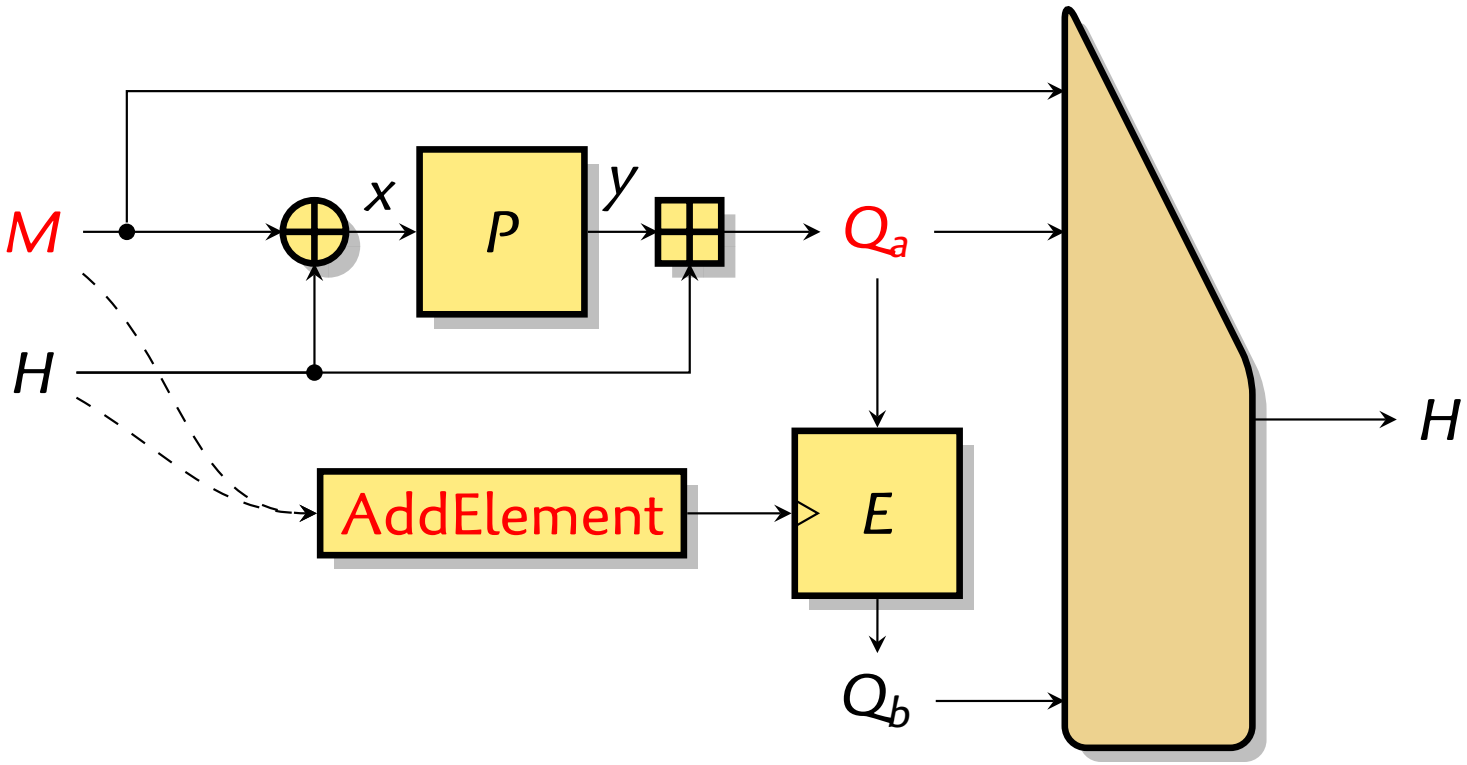
1. First of all you find collisions in Q_a with a fixed message;
2. then, second, you modify them to collide in AddElements.
3. You have now rendered the hash function 'elpless.

Banana Midnight Wish



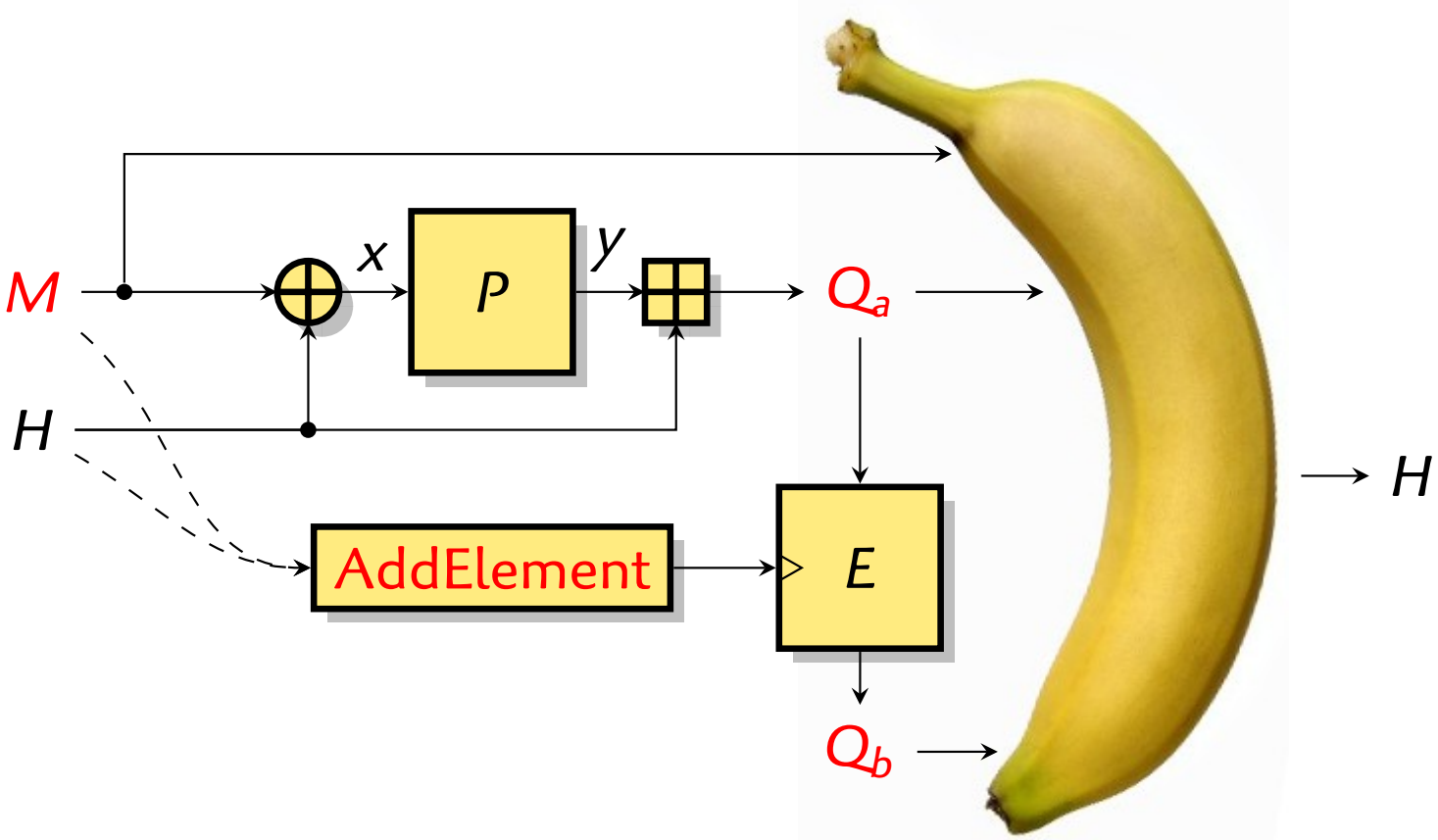
1. First of all you find collisions in Q_a with a fixed message;
2. then, second, you modify them to collide in AddElements.
3. You have now rendered the hash function 'elpless.

Banana Midnight Wish



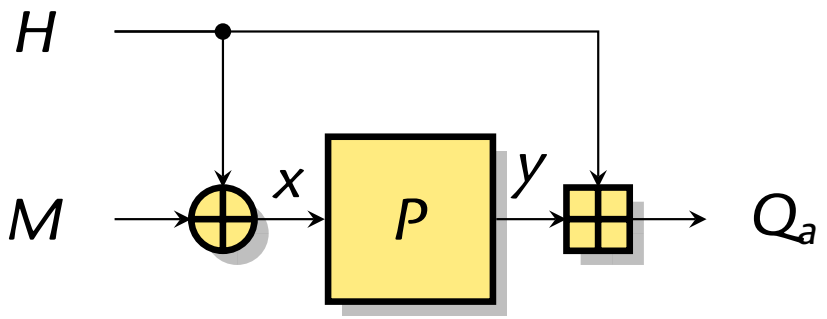
1. First of all you find collisions in Q_a with a fixed message;
2. then, second, you modify them to collide in AddElements.
3. You have now rendered the hash function 'elpless.

Banana Midnight Wish



1. First of all you find collisions in Q_a with a fixed message;
2. then, second, you modify them to collide in AddElements.
3. You have now rendered the hash function 'elpless.

Main idea



- We want no difference in Q_a, no difference in M

- Pick a random pair of x, compute y
- The XOR-difference in x is the XOR-difference in H
- The mod-difference in y is the mod-difference in H
- Solve H from LSB to MSB

Results so far

- We can achieve collision in Q_0 to Q_{26} for a small cost
- For a cost of 2^{32} we can also collide in XH
- This gives a collision in 96 output bits,
  and strong relations between more bits

Conclusion

Chaining Value	
6ae0a10c 4f14abca 57e66e71 6075a601	6ae0a10c 4f14abcb a819918f 9f8a59fe
bba141a1 46fb0506 e001fffd e89b2ebf	445ebe5f 8934faf9 9ffe0002 e89b2ebf
cb1e82d3 ae2d53d6 cb55b67f e6b080a1	cb1e82d3 ae2d53d6 34aa4980 194f7f5e
8b8c0a70 98d0080b adaacc99 88f0cf2d	7473f58f 98d0080b adaacc99 88f0cf2d
Message	
4f5381d3 f96e7f0a 72879df2 e8150fa2	4f5381d3 f96e7f0a 72879df2 e8150fa2
476caf9f fbacf685 d1c47cb8 73a7bf61	476caf9f fbacf685 d1c47cb8 73a7bf61
445261cf a4c0f69f a2316fdd 12dbc43a	445261cf a4c0f69f a2316fdd 12dbc43a
e5197bf4 af952392 c2966021 46cab397	e5197bf4 af992392 3d699fde 39354c6b
Output	
fe57177e d1e1157d ccf82758 6aecc4d0	fe57177e d1e1157d ccf82758 80b0c87d
cf3d27ab 590788dc eafe31d9 0e95fe74	0f1b49b9 e0b92229 cf1c1fb4 1fd1f3ab
5b069cc1 b1039e9e a5049da0 c38e8490	174ab741 7768d4bc 947374c1 74ddf4f9
cb6f569c 96fff629 ee5d89a4 71e405a4	8b4d7466 d075a056 0f8d8b0c d987e0cb

- Stay tuned for the chocolate strawberry attack!