Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files

Presented by

Danilo Gligoroski

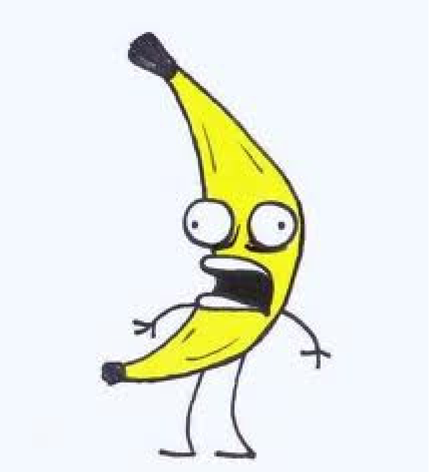
Department of Telematics,
Faculty of Information Technology, Mathematics and Electrical Engineering
Norwegian University of Science and TechnologyTechnology - NTNU, NORWAY

NTNU
Innovation and Creativity

Last year at CRYPTO 2010, Rump Session

Banana Attack

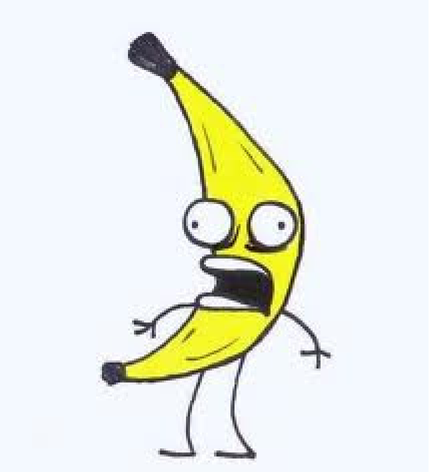
On Blue Midnight Wish by Gaëtan Leurent



Last year at CRYPTO 2010, Rump Session

Banana Attack

On Blue Midnight Wish by Gaëtan Leurent



This year on Rump Session

Bananb Attack

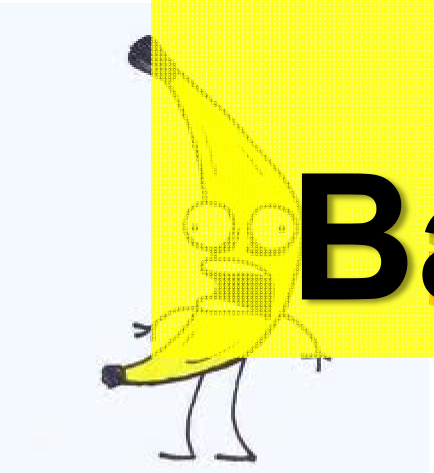
On Skein (and others)

Bananb Attack is a philosophical sibling to Banana Attack

CRYPTO 2010, Rump Session

Banana Attack

Bananb Attack



Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: ”Banana Attacks are crap”

Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: ”Banana Attacks are crap”

Message 2: ”Banana Attacks are craq”

Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: ”h(s&@h3w%!Banana Attacks are crap”

Message 2: ”h(s&@h3w%!Banana Attacks are craq”

Prepend a garbage

(computed by an undisclosed algorithm)

Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Transform to hexadecimal

Message 1: ”h(s&@h3w%!Banana Attacks are crap”

6828732640683377252142616E616E612041747461 636B7320617265206372617０

Message 2: ”h(s&@h3w%!Banana Attacks are craq”

6828732640683377252142616E616E612041747461 636B73206172652063726171

Demonstration of Bananb Target Collisions for Skein with NIST KAT file

Produce a NIST KAT file ShortMsgKAT.txt

```
# ShortMsgKAT.txt
# Algorithm Name: Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files
# Principal Submitter: Danilo Gligoroski for the Rump Session CRYPTO 2011

Len = 260
Msg = 682873264068337725214261 6E616E6120417474616 36B73206172652063726170
MD = ??

Len = 260
Msg = 682873264068337725214261 6E616E6120417474616 36B73206172652063726171
MD = ??
```

Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Compile and run genKAT256.exe provided in Skein submission package over ShortMsgKAT.txt and see the produced file ShortMsgKAT_256.txt

NTNU
Innovation and Creativity

Demonstration of Bananb Target Collisions for Skein with NIST KAT files

```
# ShortMsgKAT_256.txt
# Algorithm Name: Practical demonstration of Bananb Target Collisions for
# Principal Submitter: Danilo Gligoroski for the Rump Session CRYPTO 201

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726170
MD = EBFEF527B76D55D886A5B91E64765274BFCAB9E78253F3411B4A0840CA5055D2

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726171
MD = EBFEF527B76D55D886A5B91E64765274BFCAB9E78253F3411B4A0840CA5055D2
```

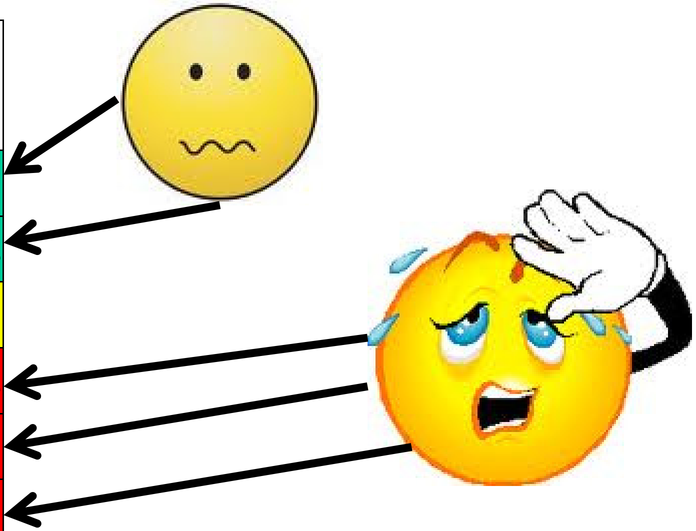
Why Skein, why not the other SHA-3 finalists?

Why Skein, why not the other SHA-3 finalists?

- Well, personally I could do BLAKE too, but I am not interested for the others

amd64; Sandy Bridge (206a7); 2011 Intel Core i7-2600K; 4 x 3400MHz; threads; sandy0, supercop-20110708

	64-bit mode, 512 bit hash	Speed cycles/byte
1.	skein512	7.83
2.	blake512	7.94
3.	sha512	11.67
4.	keccakc512	12.84
5.	jh512	13.70
6.	groestl512	15.59



Thank you for your attention!

NTNU
Innovation and Creativity