

3-Collisions with less memory

Antoine Joux (joint work with Stefan Lucks)

AfricaCrypt Rump Session
June 23th, 2009

Generic multicollisions

- ▶ A k -collision for F is a k -uple such that:

$$F(a_1) = F(a_2) = \dots = F(a_k)$$

- ▶ Hard to find (in general), need at least:

$$k! N^{(k-1)/k}$$

evaluations of F .

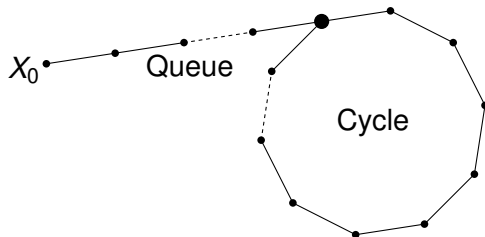
Folklore algorithm for k -collisions

- ▶ Evaluate F at $k! N^{(k-1)/k}$ random points
- ▶ Sort (or hash if you prefer)
- ▶ Search for k consecutive equalities

High memory cost

Case of (2-)collisions

- ▶ Memoryless method
- ▶ Cycle finding on $X_{n+1} = F(X_n)$
 - ▶ Brent
 - ▶ Floyd
 - ▶ Nivasch



For 3-collisions

- ▶ Folklore algorithm \Rightarrow Time: $N^{2/3}$, Memory: $N^{2/3}$

Can we do better ?

A teaser solution

- ▶ Use cycle finding on $F \circ \pi$
- ▶ Build $N^{1/4}$ distinct collisions.
- ▶ Evaluate F in $N^{3/4}$ random values.

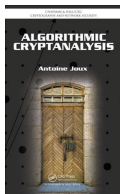
Collision between two sets \Rightarrow 3-Collision.

- ▶ Time: $N^{3/4}$, Memory: $N^{1/4}$

A more complete solution

- ▶ Time: $N^{2/3}$, Memory: $N^{1/3}$
- ▶ Key is to construct $N^{1/3}$ collisions in $N^{2/3}$

Ask Stefan or me for the preprint



Conclusion