(Second) preimage attacks on Codefish

Jean-Philippe Aumasson

Codefish hash function

In math journal *Periodica Mathematica Hungarica*, 2004

Outcome of a UE-funded project

Commercialized by KRIPTO Research ($1000 licence)

Compression function: circulant **determinant**

$$\det \begin{pmatrix} M_1 & M_2 & M_3 & 0 & 0 \\ 0 & M_1 & M_2 & M_3 & 0 \\ 0 & 0 & M_1 & M_2 & M_3 \\ M_3 & 0 & 0 & M_1 & M_2 \\ M_2 & M_3 & 0 & 0 & M_1 \end{pmatrix}$$

Reduction of preimage to solving norm form equations

Attacks

Preimages of zero: make matrix non-invertible

Second-preimages: circulant determinants have the nice property that

$$\det \mathrm{circ}(X_0, \ldots, X_{n-1})$$

equals

$$(-1)^{k(n-1)} \det \mathrm{circ}(X_k, X_{k+1}, \ldots, \ldots, X_{k-1})$$

(with mod *n* reductions)

In practice: **multi-second-preimages** for $<$4Kb messages

Conclusions

Doesnt contradict the “security proof”

Can be partially fixed by using padding, IV

One more imperfect provably secure hash