Hash Functions and Cayley Graphs: the end of the story?

Christophe Petit

Jean-Jacques Quisquater

UCL Crypto Group

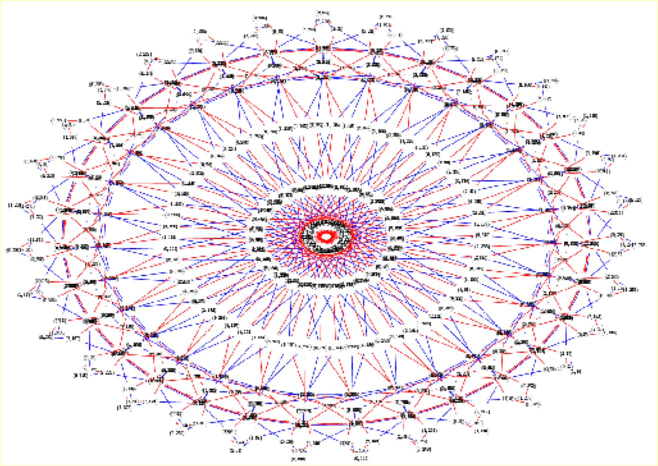
The dream


Collision resistance
(Second) Preimage resistance
Pseudorandom generator
Pseudorandom function
Key derivation
And many more ...

Recently

Hash functions (1990-...) designed by randomness?

Zemor-Tillich hash functions 1994-2009



Zémor-Tillich hash function (CRYPTO'94)

- Parameters $n \in \mathbb{Z}$ and $P(X)$ irreducible of degree n. Let

$$A_0 := \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix} \qquad A_1 := \begin{pmatrix} X & X+1 \\ 1 & 1 \end{pmatrix}.$$

  Then $h_{ZT}(m_1 m_2 \ldots m_k) := A_{m_1} A_{m_2} \ldots A_{m_k} \bmod P(X)$.
- Elegant design, graph and group-theoretical interpretations of main hash properties
- One of the oldest hash functions
- Full cryptanalysis of related schemes [TZ93,TZ08,PLQ08] but only partial attacks on ZT [CP94,G96,AK98,SGGB00,PQTZ09]

IACR eprint 2009-376

Grassl et al's collision attack [GIMS09]

- Change generators for

$$A_0' := A_0 = \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix} \qquad A_1' := A_0^{-1} A_1 A_0 = \begin{pmatrix} X+1 & 1 \\ 1 & 0 \end{pmatrix}.$$

- Observe that the hash of any palindrome has the form

$$M = \begin{pmatrix} a^2 & b \\ b & d^2 \end{pmatrix}$$

- Fix $a = P(X)$. Recover b, d and a preimage of this matrix, using an algorithm of Mesirov-Sweet (JoNT'87)
- Build the collision

$$A_0' M A_0' = A_1' M A_1'.$$

Second preimages for Zémor-Tillich

- Observe that if $a = 0 \bmod P(X)$ then

$$\begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a^2 & b \\ b & d^2 \end{pmatrix} = \begin{pmatrix} 1 & X+d^2 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} a^2 & b \\ b & d^2 \end{pmatrix}\begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ X+d^2 & 1 \end{pmatrix}$$

  and both matrices have order 2.
- We obtain collisions to the void message
  $\Rightarrow$ **second preimages** for any message

Preimages for Zémor-Tillich

- Given $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL(2, \mathbb{F}_{2^n})$,
- Write $\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix}^3 \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$
  with
  $$\begin{cases} \alpha = (DX+X+B)/(XB) \\ \beta = (B+X^3)/X^2 \\ \gamma = (X+B+X^2B+AX)/(XB) \end{cases}$$
- As $\begin{pmatrix} 1 & 0 \\ \sum \alpha_i & 1 \end{pmatrix} = \prod \begin{pmatrix} 1 & 0 \\ \alpha_i & 1 \end{pmatrix}$
  it is enough to precompute preimages for a set $\{\alpha_i\}$ forming a basis of $\mathbb{F}_{2^n}$

Precomputing part

- Until we have a basis of elements $\{\alpha_i\}$
  - Apply [MS87]'s algorithm to $a_i = P(X)Q_i(X)$ where $Q_i(X)$ random irreducible of degree R
  - If it succeeds, recover the corresponding preimage and value $\alpha_i = X + d_i^2$
  - If this new α_i is independent of the previous ones, add it to the list
- Remarks:
  - [MS87]'s algorithm guaranteed to succeed only when a is irreducible. However, we provide evidence that it succeeds with probability about $1/2$ when $a_i = P(X)Q_i(X)$.
  - If we cannot get a full basis, we increase the degree of $Q_i(X)$

Conclusion I

Conclusion II

- Zemor-Tillich is completely broken
- Preimage in few seconds with a small program
- Length of the preimage around 100.000 bits

End?

- No!
- Changing the generators
- More generators
- Working in other algebra
- A new field!