

Fixing non-randomness in PGVs

Gauravaram, Praveen

Publication date:
2010

Document Version
Early version, also known as pre-print

[Link back to DTU Orbit](#)

Citation (APA):

Gauravaram, P. (2010). Fixing non-randomness in PGVs [Sound/Visual production (digital)]. 30th Annual International Cryptology Conference, Santa Barbara, CA, United States, 15/08/2010, <http://rump2010.cr.yp.to/>

DTU Library

Technical Information Center of Denmark

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Fixing non-randomness in the PGVs

Praveen Gauravaram, Nasour Bagheri* and Lars R.Knudsen

DTU, Denmark and IUST, Iran*

17th August 2010

Single block length compression functions

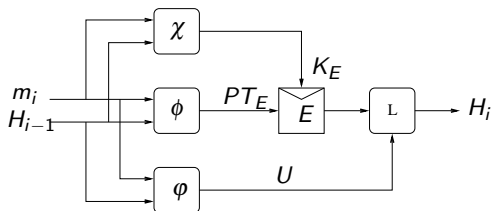


Figure: General form of a n -to- n bit PGV compression function

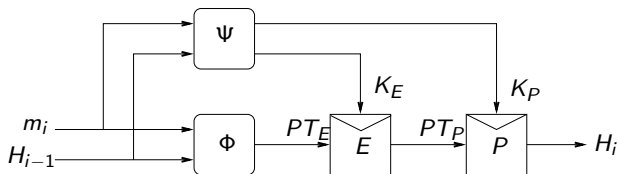
- 1 χ , ϕ and ϕ define linear combinations of m_i and H_{i-1} .
 - $K_E, PT_E, U \in \{m_i, H_{i-1}, m_i \oplus H_{i-1}, v\}$
- 2 Preneel, Govaerts and Vandewalle (PGV) showed 12 out of 64 possible designs are collision and (second) preimage resistant.
- 3 Black, Rogaway and Shrimpton confirmed this result in the ideal-cipher model.

Non-randomness in PGVs

For each f^i , it is possible to find a pair (H_{i-1}, m_i) which makes f^i non-ideal even if E is ideal.

Compression function (f^i)	Property
$i \in \{5, 8, 10, 11\}$	$f^i(H_{i-1}, m_i) = H_{i-1}$ (fixed points)
$i \in \{2, 3, 6, 7\}$	$f^i(H_{i-1}, m_i) = H_{i-1} \oplus m_i$
$i \in \{1, 4, 9, 12\}$	$f^i(H_{i-1}, m_i) = m_i$

General form of a $2n$ -to- n -bit Modified PGV compression function



- 1 Ψ and Φ define linear combinations of m_i and H_{i-1} :
- 2 $K_E, K_P, PT_E \in \{m_i, H_{i-1}, m_i \oplus H_{i-1}, v\}$
- 3 Sixty-four MPGVs can be derived from it.

Results

- ① Two ideal and independent block ciphers are sufficient to design indifferentiable compression functions. 24/64 MPGVs are indifferentiable.
 - ① The modified versions of 12 collision resistant PGVs are indifferentiable up to the birthday bound.
 - ② Some surprises.
- ② Interesting applications.

Thank you!!!!