About a new generation of block ciphers and hash functions - DN and HDN

Vlastimil Klíma

v.klima@volny.cz

Independent consultant

http://cryptography.hyperlink.cz

Prague, Czech Republic

SPI 2007, Security and Protection of Information, May 2 – 4, 2007, Brno, Czech Republic,
www.unob.cz/spi

Introduction

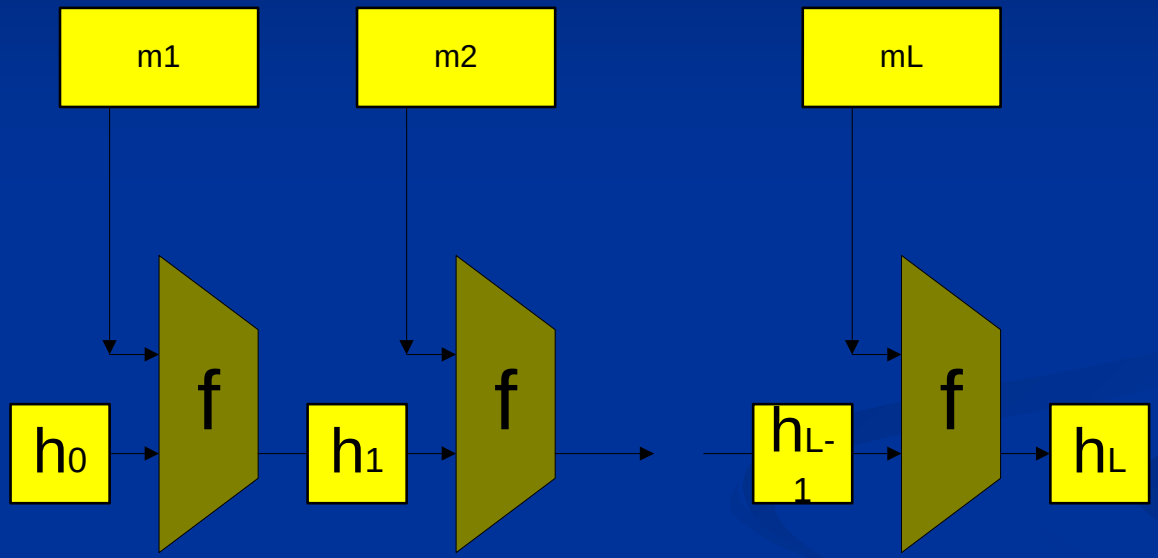
- This work arose from the study of hash functions for Czech NSA, presents some parts of the projects ST20052006018 and ST20052005017 for Czech NSA.
- contemporary hash functions
  - several generic attacks
  - practical collision attacks on hash functions families MD and SHA.
- Both generic attacks and practical attacks showed us that we underestimated the underlying problems
- Antoine Joux, who discovered in 2004 the hash functions generic problem (multi-collisions), said at the Second Cryptographic Hash Workshop, USA, August 24 - 25, 2006:

"We do not understand what we are doing and we do not really know what we want".

Special block ciphers

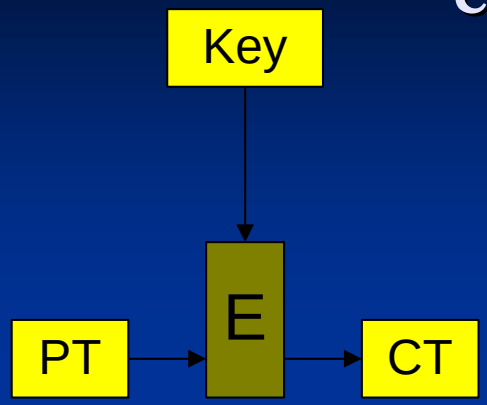
- build a hash function from the classical block cipher is a vain effort like squaring the circle
- special block cipher
- It is something strange – a symmetric block cipher, whose encryption key is under full control of the attacker. The attacker can know the key, select it and change it. This is a new cryptographic primitive.
- In 1975, a similar idea in another context triggered a revolution in cryptography and gave rise to a new branch: Public Key Cryptography. In this case an attacker could know the encryption key, which had until then seemed foolish. But now PKC is a reality.
- Special block ciphers have much stricter requirements: an attacker can select and discretionarily tamper with the key, which seems even more foolish.
- In February this year we proposed the first special block cipher family DN. Double Net DN(n, k)-r has n-bit block, k-bit key and r rounds. And, based on DN, we defined hash functions family HDN(n, k)-r with n-bit hash code.

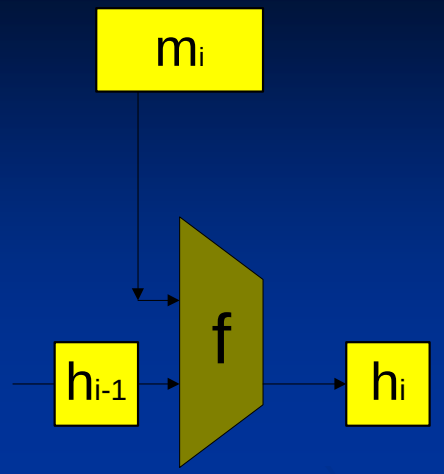
classical Merkle-Damgard construction of a hash function



- Instead of compression function f classical block ciphers are used. But there are differences.

Main differences between classical block ciphers and compression functions

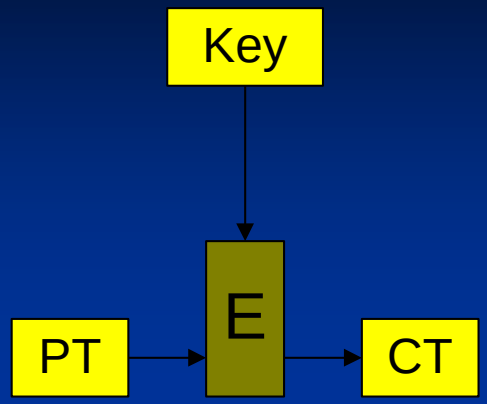


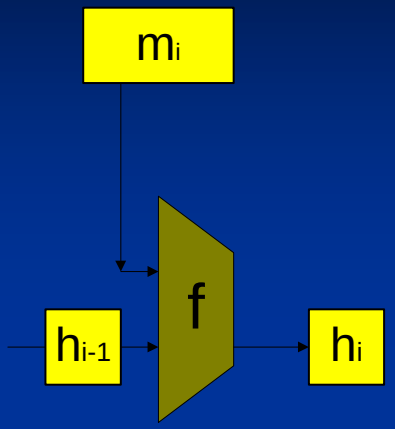


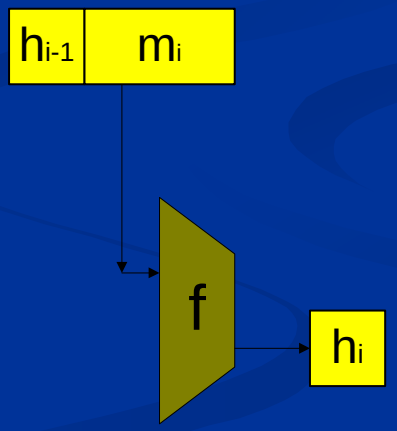
Classical Block Cipher	Compression Function
contains an element unknown to an attacker	an attacker knows all inputs and is able to spool them
is meant to hide the **plaintext** in the ciphertext, based on a **secret** element (unknown to an attacker)	is meant to hide **all inputs** in the output, based on a **public** function
is a permutation for fixed-key	is a random transformation
it is invertible	one-wayness is needed
it is easy to create collisions	collision resistance is needed

- **The main difference is that the compression function has only one input (mi, hi-1) and does not differentiate between its bits.**

We should draw…

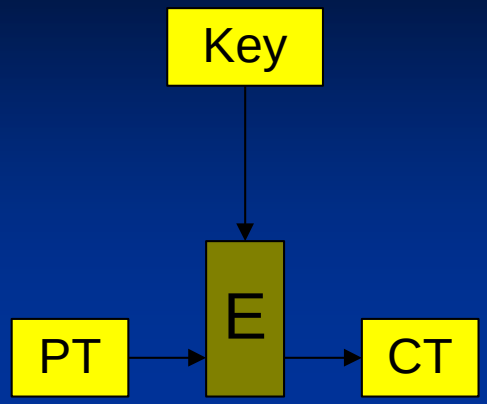


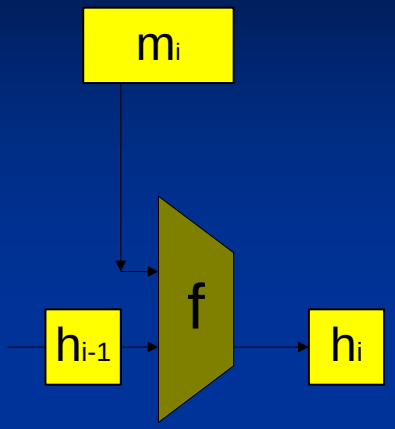


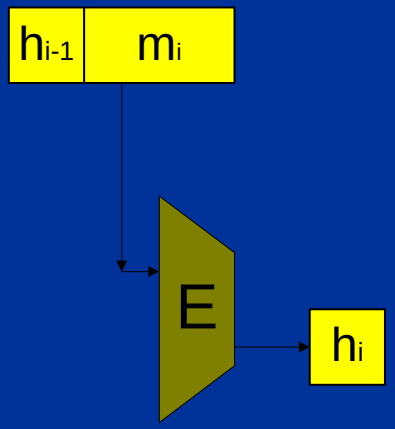


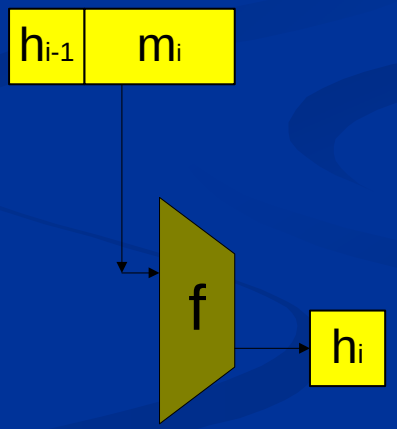
- The main difference is that the compression function has only one input (mi, hi-1) and does not differentiate between its bits.

We should draw…



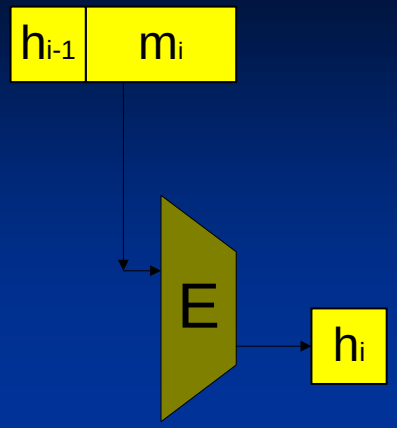


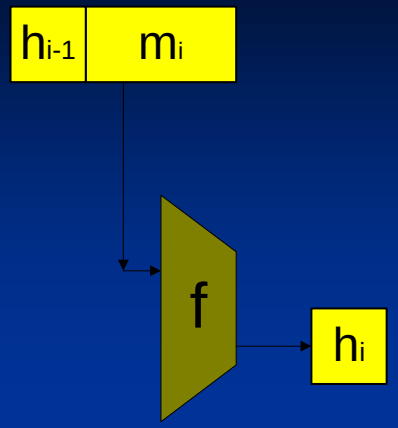




- The main idea is to move both inputs of the classical block cipher into one input – to the key. And to set the plaintext to constant.

Now

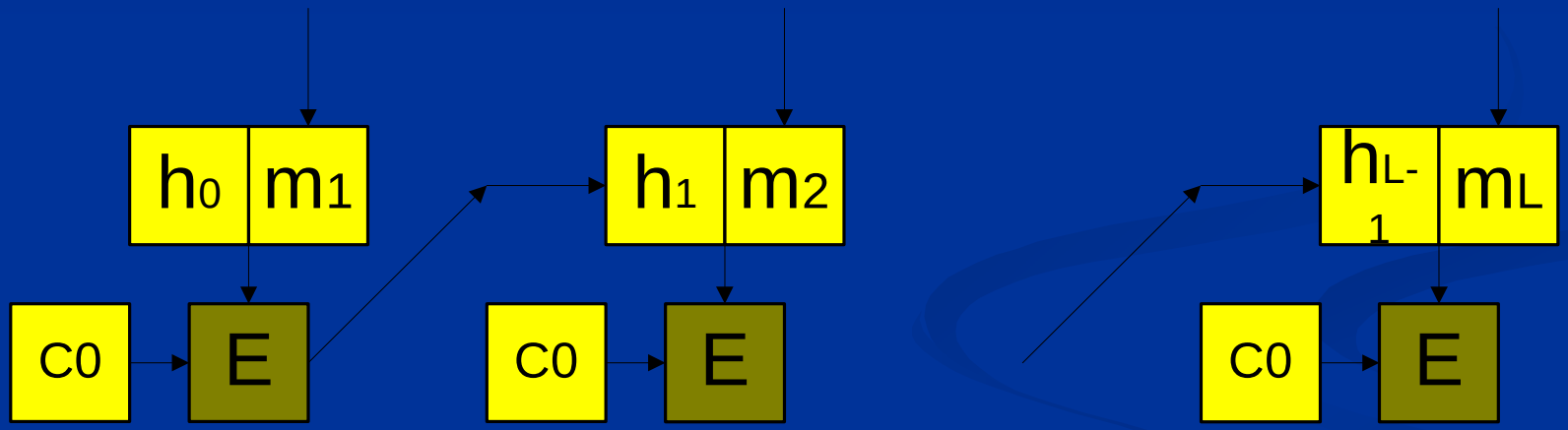




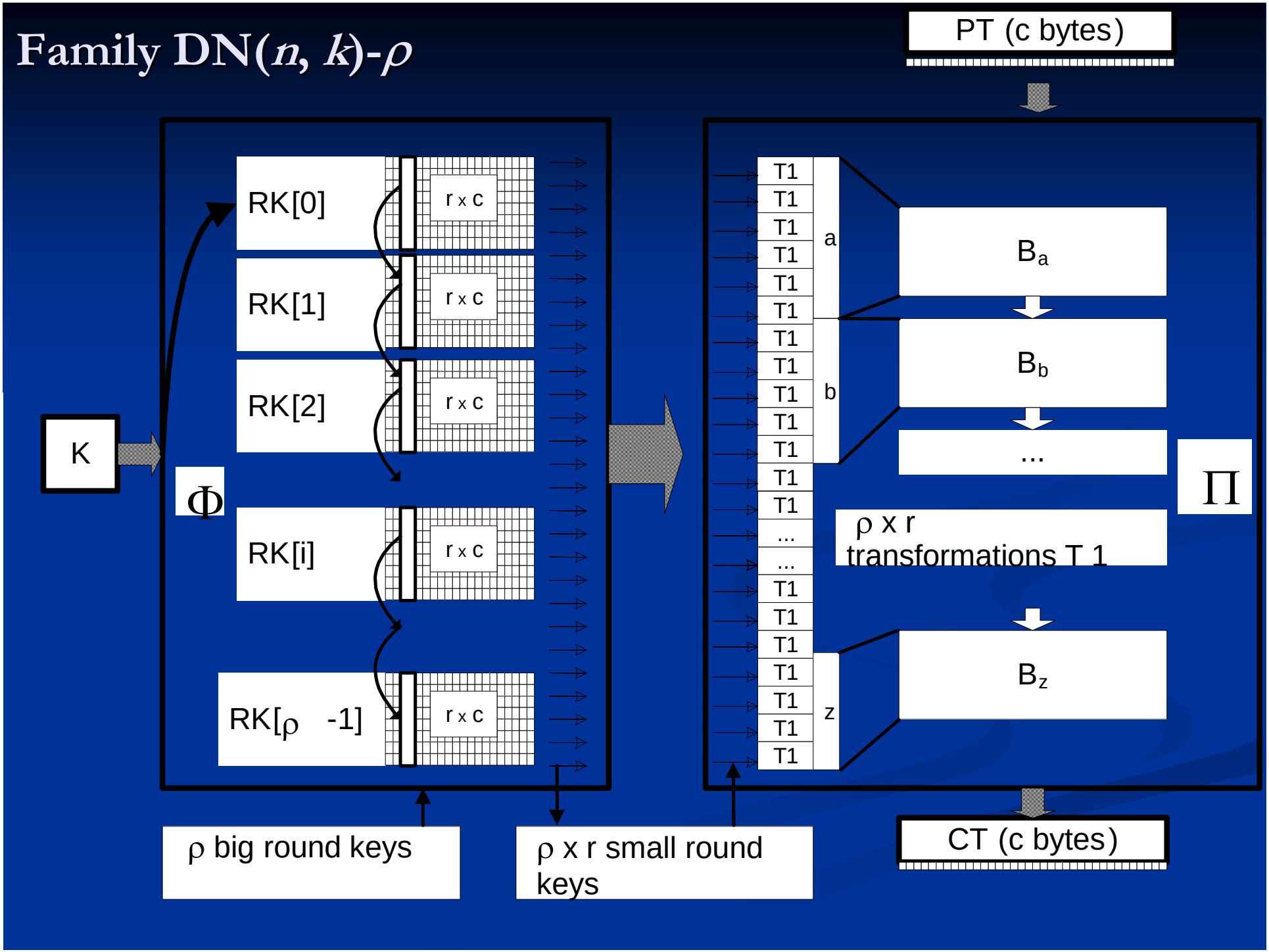
Special Block Cipher	Compression Function
	an attacker knows all inputs and is able to spool them
No difference	is meant to hide **all inputs** in the output, based on a **public** function
	is a random transformation
	one-wayness is needed
	collision resistance is needed

- **the special block cipher has to process the key very strong, as the classical block cipher processes the plaintext.**

Resulting hash function

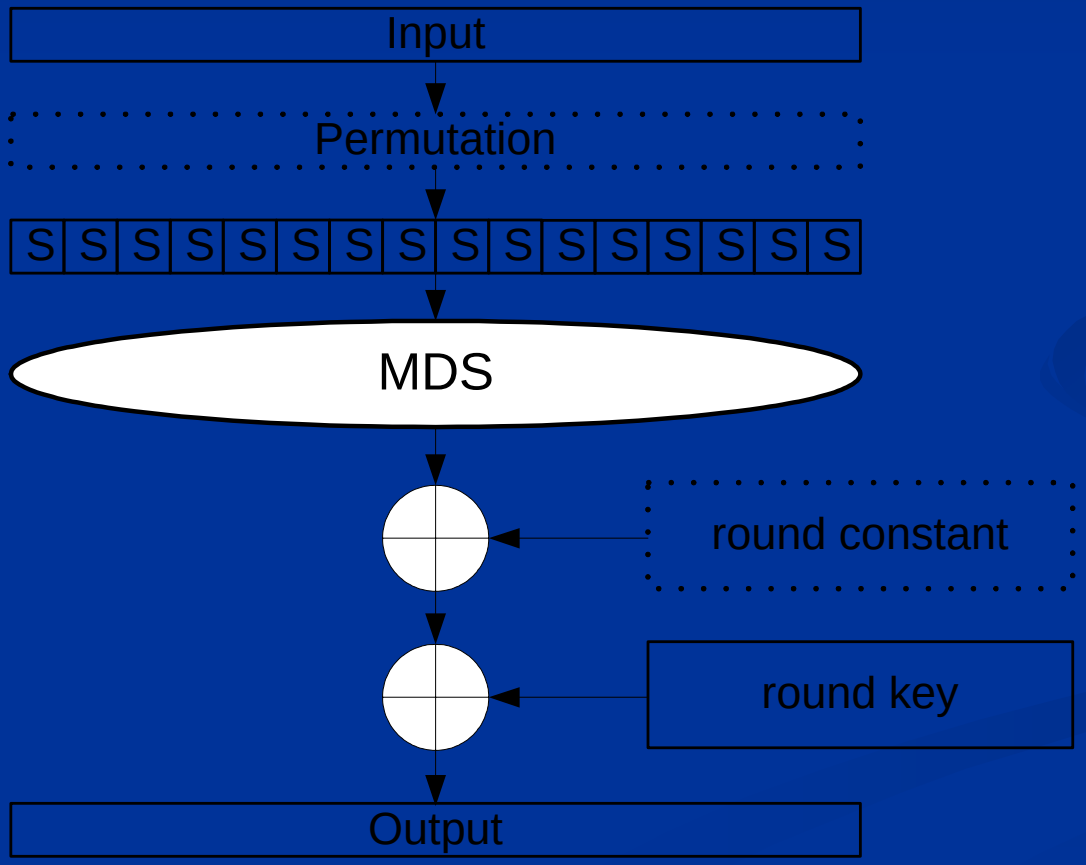


Family DN(n, k)-ρ



The function Π

- is a product of ρ x r elementary transformations T1.
- Each transformation T1 consists of a substitution, a permutation, a linear transformation and round key addition. All these variables can be different for different transformations T1.



Permutation (byte level, optional, can be a part of linear level)

Substitution boxes (byte level)

Linear transformation (bit level)

Add round constant (optional)

Add round key

The function Φ

- The function Φ uses also SP networks for preparing round keys.

Characteristics

- Security proofs:
- Resistance Φ and Π to DC and LC expressible in terms of resistence of used S-boxes.
- Parameters:
- Dimensions, all variables (MDS, S-boxes, permutations, constants,...).

Special block cipher as a strengthened encryption primitive

- the technological progress will provide the attackers with new possibilities weakening both classical assumptions:
  - the attacker doesn´t know the key
  - impossibility to manipulate with it, as well.
- Side channel attacks are good example of these possibilities.
- Special block cipher will be resistant against partial key knowledge attacks and manipulation key attacks and various kinds of side channel attacks. This is its main advantage as a cryptographic primitive, used for encryption.

Conclusion

- We have designed new cryptographic primitive - Special Block Cipher. It is a symmetric block cipher, whose encryption key can be revealed to an attacker. Moreover, an attacker can select and discretionarily tamper with the key.
- Using special block cipher we proposed a new family of hash functions.
- We present special block cipher family DN and the family of hash functions HDN. These are not just theoretical concepts, but practically employable functions. HDN(512, 8192)-10 is roughly 3 times slower than SHA-512 (and Whirlpool).
- Basic idea behind the special block cipher DN is simple – contrary to classical block cipher approach, the same attention is paid to key and plaintext processing.
- Once the special block cipher concept is examined and accepted in hash functions, it can be used in advance in its original purpose – data encryption. The employment of these stronger functions might not seem as a must in the present block ciphers, but it probably will be in the future. In the hash functions, it is a necessity today already.

Details of DN and HDN

- V. Klima, A New Concept of Hash Functions **SNMAC** Using a Special Block Cipher and NMAC/HMAC Constructions, IACR ePrint archive Report 2006/376, October, 2006, http://eprint.iacr.org/2006/376.pdf
- V. Klima, Special block cipher family **DN** and new generation SNMAC-type hash function family **HDN**, homepage http://cryptography.hyperlink.cz/SNMAC/SNMAC_EN.html, IACR ePrint archive: Report 2007/050, February, 2007, http://eprint.iacr.org/2007/050.pdf.
- **Source codes** are available on the homepages
- http://cryptography.hyperlink.cz/SNMAC/SNMAC_EN.html, http://cryptography.hyperlink.cz/SNMAC/SNMAC_CZ.html.