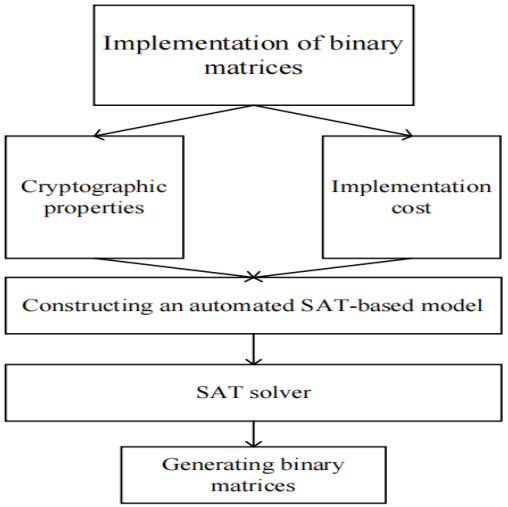
New SAT-based Model for Constructing Linear Layers with Good Cryptographic Properties and Implementation

Tianling WENG, Gaoli WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-025-40011-5

Problems & Ideas

- Problems of conventional Constructing Linear Layers approaches:
  - Existing methods often achieve optimality only for specific dimensions or branch numbers.
  - Techniques targeting high-dimensional layers usually incur increased implementation cost in low-dimensional cases.
- Ideas: This paper proposes a SAT-based method for constructing optimal linear layers by leveraging the link between XOR gate arrangement and linear layer design. The method achieves strong cryptographic properties, low implementation cost, and systematically generates involutory layers.



Main Contributions

- Contributions:
  - The paper introduces a novel SAT-based approach for constructing optimal linear layers, significantly extending the achievable dimension up to 14;
  - The constructed linear layers simultaneously achieve strong cryptographic properties and low implementation cost, supporting arbitrary branch numbers across dimensions 4 to 14;
  - The authors systematically construct involutory linear layers for dimensions 4 to 14, addressing a long-standing gap in the field.

Table 4 Experimental results for invertible linear layer.

[12]			[11]			This paper		
n	B_{dl}	XOR counts	n	B_{dl}	XOR counts	n	B_{dl}	XOR counts
4	4	6	4	4	6	4	4	6
6	4	9	6	4	9	6	4	9
8	4	-	8	4	12	8	4	12
8	5	16	8	5	-	8	5	16
10	6	25	10	6	-	10	6	24
12	8	-	12	8	-	12	8	38
14	4	-	14	4	-	14	4	21

Table 5 Experimental results for involutory linear layer.

n	B_{dl}	XOR counts	Reference
4	4	6	[12],This paper
6	4	9	This paper
8	4	12	This paper
8	5	16	This paper
10	6	24	This paper
12	8	38	This paper
14	4	21	This paper