

Der AES Kandidat MARS

- Einführung

- Design

- Algorithmus

- Performanz

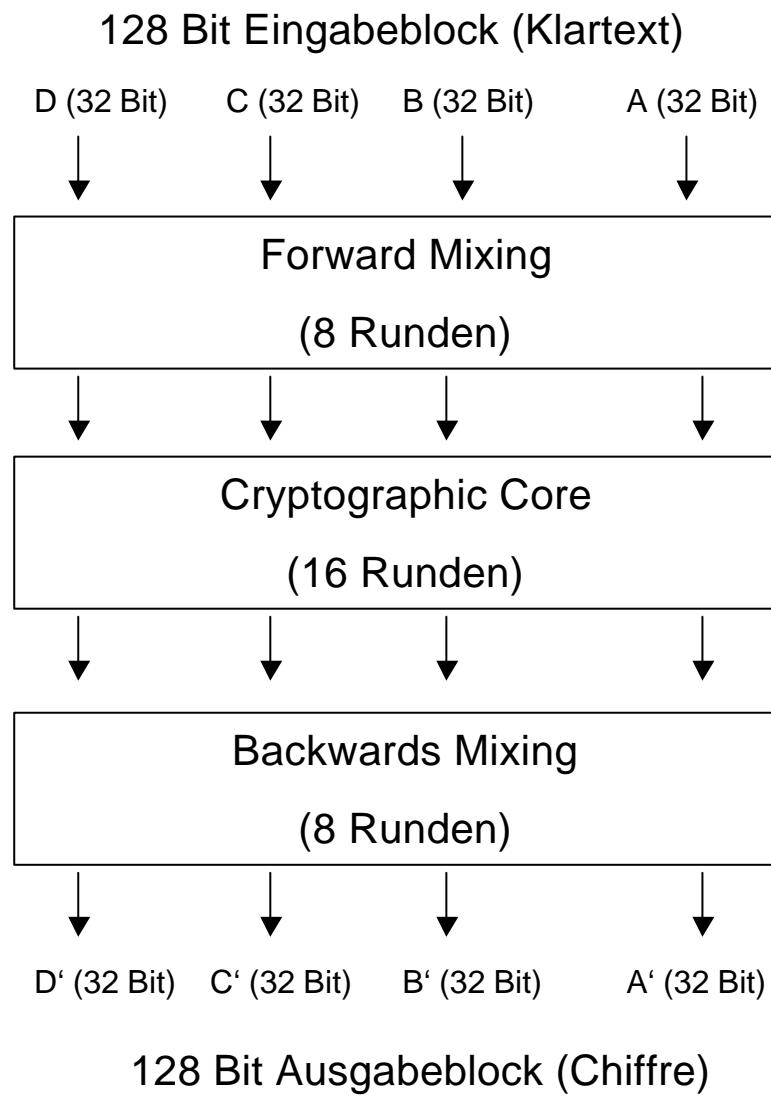
- Sicherheit

- Literatur

- symmetrisches Blockchiffre
- AES Kandidat der zweiten Runde
- Blockgröße 128 Bit
- Schlüssellänge variabel von 128 Bit – 448 Bit
- Feistelnetzwerk (Typ 3)
- S - Box
- Smart Card fähig
- konservatives Design

Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur



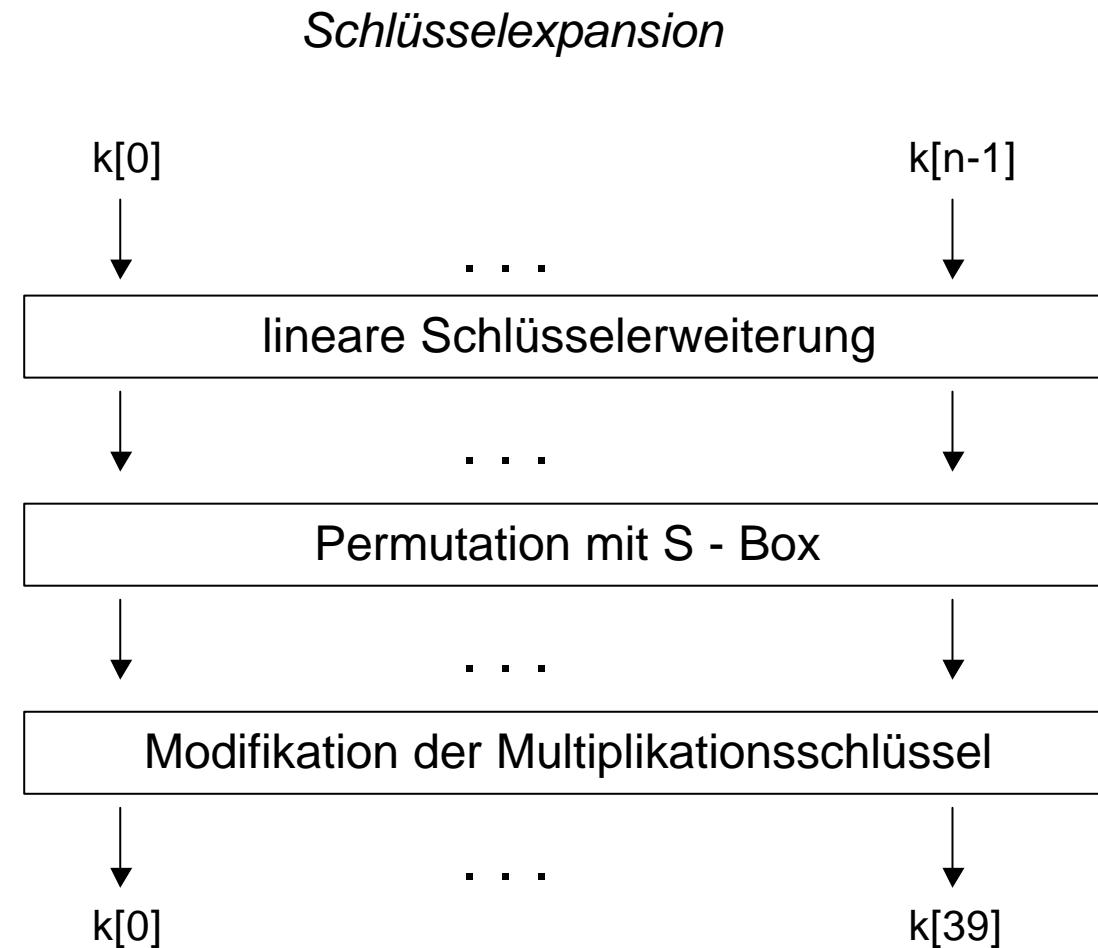
Der AES Kandidat MARS

-
- Einführung
 - Design
 - Algorithmus
 - Performanz
 - Sicherheit
 - Literatur

- Schlüssellänge variiert in Längen von 4 bis 14 Wörtern
- MARS expandiert dann auf einen Array aus 40 Wörtern
- verwendete Operationen: xor, +, -, x und rot
- S - Box mit 512 Wörtern für Rundenfunktion und
Schlüsselexpansion

Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

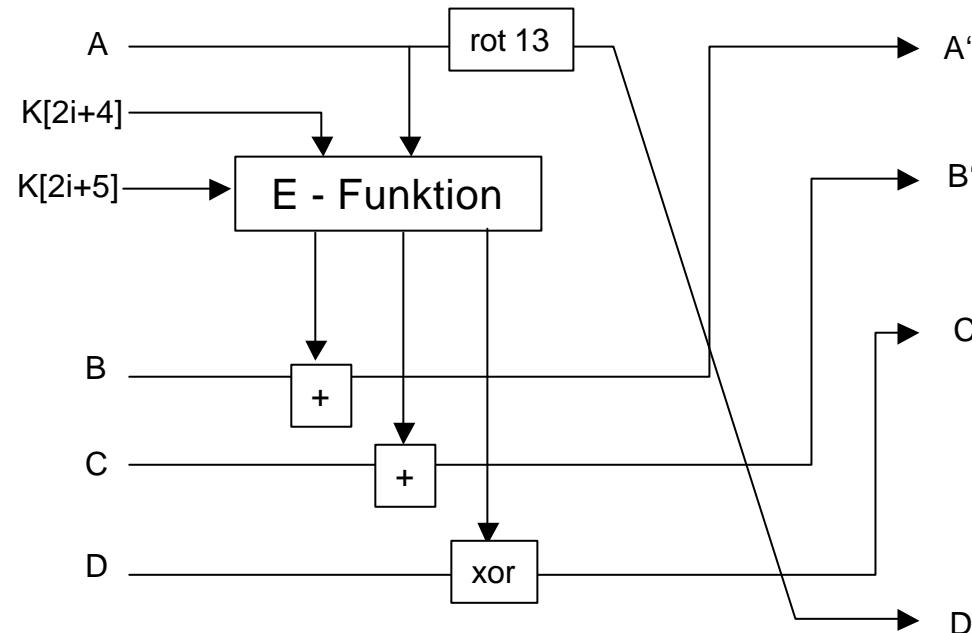


Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

Cryptographic Core: Forward Mode

Rundenfunktion $i = 0, \dots, 7$

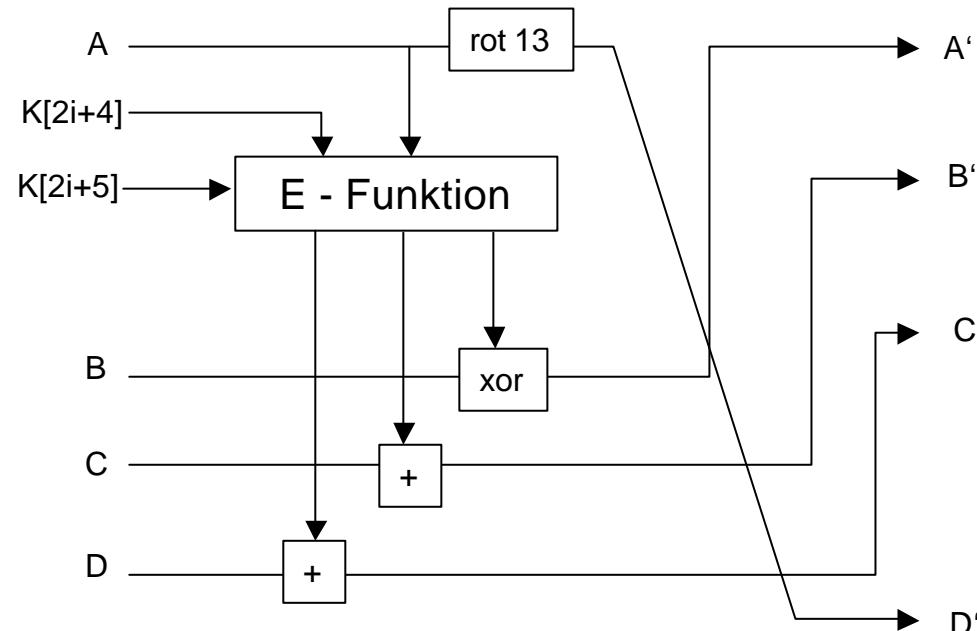


Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

Cryptographic Core: Backward Mode

Rundenfunktion $i = 8, \dots, 15$

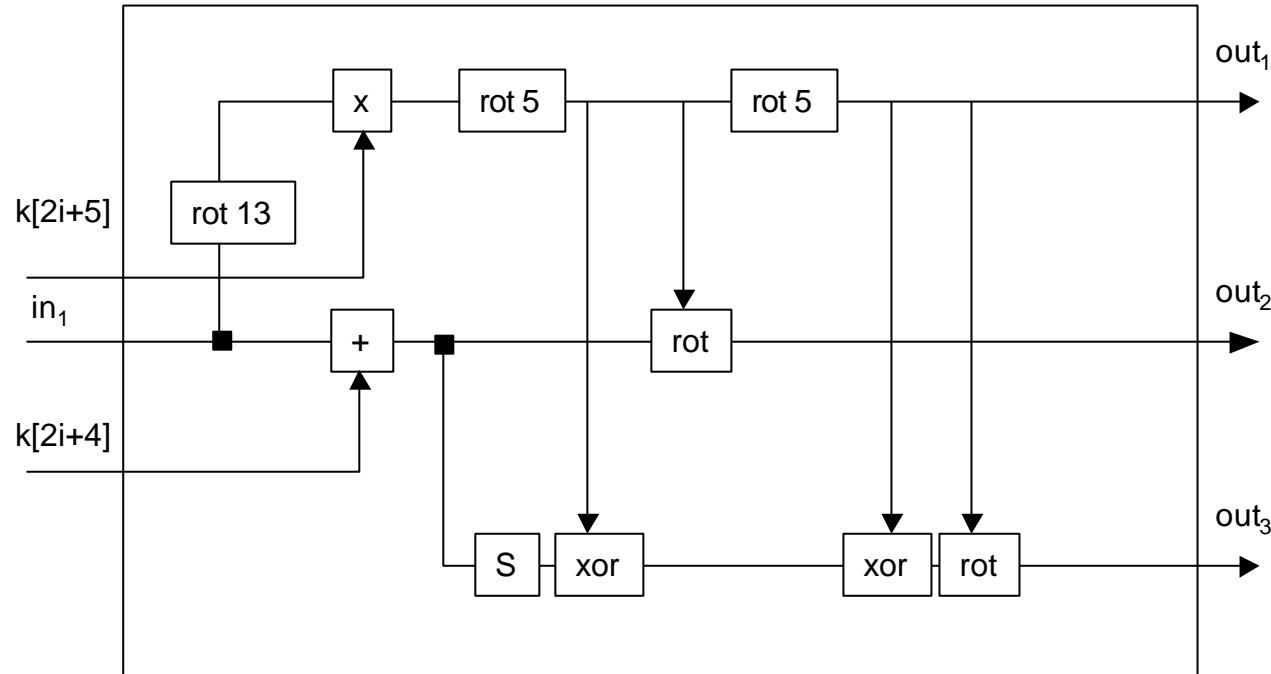


Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

Cryptographic Core: E - Funktion

$i = 0, \dots, 15$



Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

		<i>Software</i>	
		PowerPC 200 MHz	Pentium Pro 200 MHz
	DES (MBit/s)	-	7.3
	Triple DES (MBit/s)	-	16.7
	gesamt (MBit/s)	85	65
	Cryptographic Core (MBit/s)	160	104
	Schlüsselerweiterung (keys/s)	121,000	52,000

Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

Hardware

	Komplexität	Pipelining (Kopien)	Gesamt (MBit/s)
--	-------------	---------------------	-----------------

	70,000	2	640
--	--------	---	-----

	70,000	4 + 4	4,000
--	--------	-------	-------

	393,000	4 + 8	8,000
--	---------	-------	-------

Der AES Kandidat MARS

- Einführung
- Design
- Algorithmus
- Performanz
- Sicherheit
- Literatur

Vergleich

		Key Setup (Takte)	Verschlüsselung (Takte)	Smart Card RAM (bytes)
	MARS	4,400	390	195
	Serpent	2,500	1,030	50
	Rijndael	850	440	52
	RC6	1,700	260	210
	Twofish	8,600	400	60

Der AES Kandidat MARS

Einführung
Design
Algorithmus
Performanz
■ Sicherheit
Literatur

- Brute Force benötigt maximal 2^n Schritte (n – Schlüssellänge)
- lineare oder differentielle Kryptoanalyse für 128 Bit Blöcke aussichtslos
- AES Analysen erbrachten keine verwertbaren Lücken und bescheinigten einen hohen Sicherheitsabstand

Der AES Kandidat MARS

Einführung	
Design	
Algorithmus	
Performanz	
Sicherheit	
■ Literatur	<ul style="list-style-type: none">[1] The MARS Encryption Algorithm URL: http://www.research.ibm.com/security/mars.pdf[2] Reinhard Wobst; Abenteuer Kryptologie; Addison Wesley, 1998[3] Schneier, Kelsey, Whiting, Wagner und Hall; Performance Comparison of the AES Submissions; URL: http://csrc.nist.gov/encryption/aes/round2/performace.pdf[4] MARS and the AES Selection Criteria; URL: http://www.research.ibm.com/security/final-comments.pdf[5] Nechvatal, Barker, Bassham, Burr, Dworkin, Foti, Roback; Report on the Development of the Advanced Encryption Standard; URL: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf[6] Third AES Candidate Conference – Proceedings URL: http://csrc.nist.gov/encryption/aes/round2/AES3proceedings.pdf