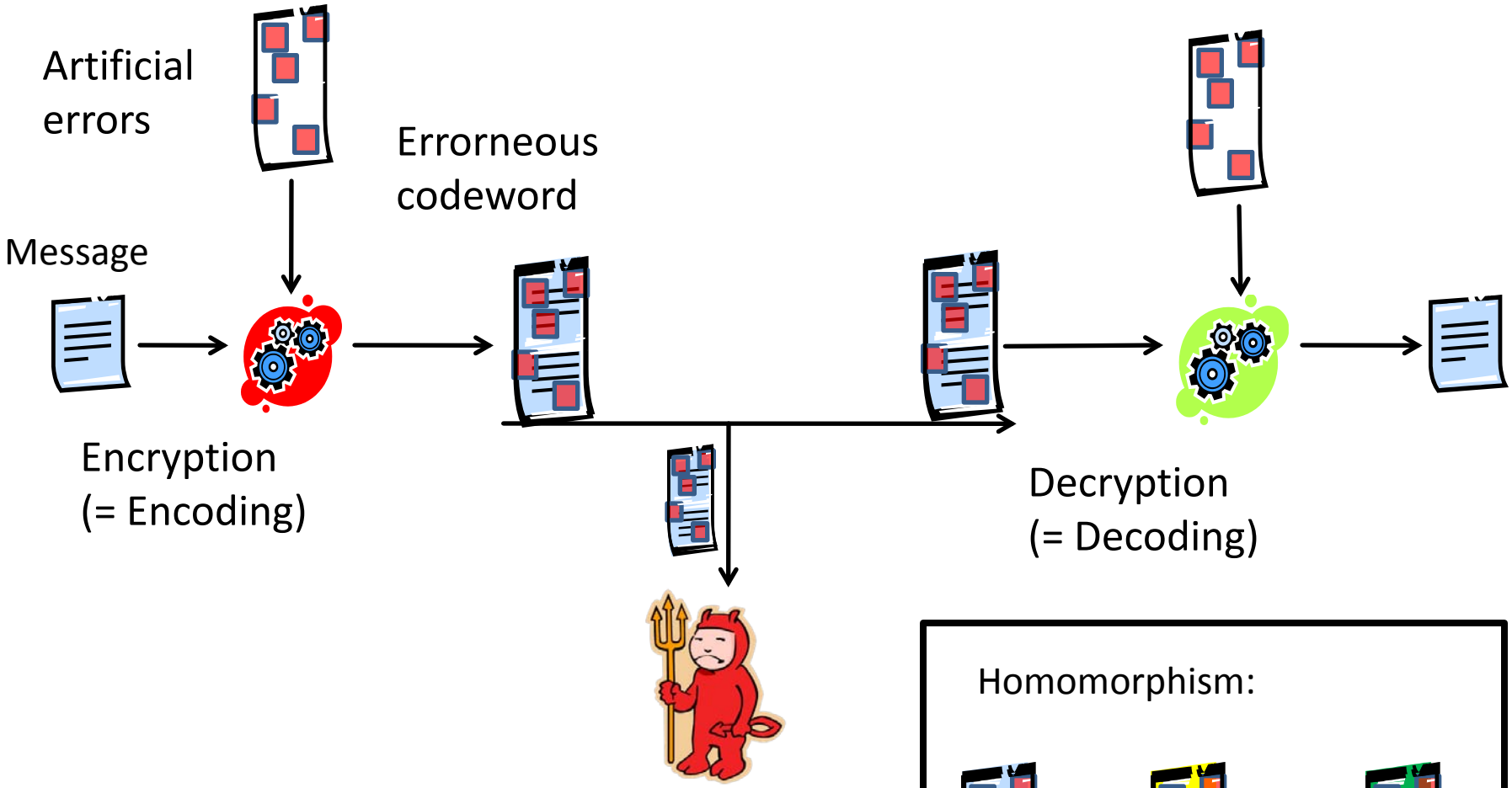
Constructing Full Homomorphic Encryption Schemes from Coding Theory

Frederik Armknecht[1,2], Daniel Augot[3], Ludovic Perret[4], Ahmad-Reza Sadeghi[1]

[1]HGI, Ruhr-Universität Bochum, Germany
[2] Technische Universität Darmstadt, Germany
[3] LIX - INRIA Saclay-le de France
[4] UPMC, University Paris 06/INRIA, France

Asiacrypt 2009 Rump Session
Tokyo, Japan, December 7, 2009

Basic Idea



Addition: use Linear Codes
Multiplication: use Evaulation Codes

Comparison

Scheme	Gentry	Ours
Public/Secret key	Asymmetric	Symmetric
Homomorphism	∞ add., ∞ mult.	∞ add., (m-1) mult.
Ciphertext Length	$O(s^2)$	$O(m^3 \cdot s)$
Effort Encryption	$O(s^4)$	$O(m^6 \cdot s^2)$
Effort Decryption	$O(s^6)$	$O(m^3 \cdot s)$
Effort Addition	$O(s^2)$??	$O(m^3 \cdot s)$
Effort Multiplication	$O(s^4)$??	$O(m^3 \cdot s)$
Underlying Problem(s)	Ideal Coset and Key Dstg.	Decisional Synchron. Codes

„s“ = Security parameter
„??“ = Effort not officially stated but based on own understanding.

Some concrete values

Security Parameter	s=80	s=128	S=256
m=2	9.81 KByte	18.48 KByte	53.87 KByte
m=3	31.34 KByte	60.95 KByte	178.84 Kbyte
m=5	146.91 KByte	278.78 KByte	821.92 Kbyte
m=10	1.17 MByte	2.47 MByte	6.68 MByte
m=100	1.42 GByte	2.95 GByte	7.72 Gbyte

(m-1) Multiplications