An alternative to Gentry's fully homomorphic encryption scheme (We Do Exist!)

Carlos Aguilar Melchor, Philippe Gaborit et Javier Herranz

XLIM, Limoges University, FRANCE

August 17th, 2009

What are we talking about ?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Leveled Fully Homomorphic Encryption Scheme

For any d there is an instance allowing to evaluate polynomials of degree d

Fully Homomorphic Encryption Scheme

An instance can evaluate any polynomial

Gentry's amazing result

Existence of a fully homomorphic encryption scheme (1978) [Gentry 09]

Based on two new problems :

- The Ideal Coset Problem (close to decisional SVP)
- The SplitKey Distinguishing Problem (close to SSSP)

Theoretical achievement

"Making the full scheme practical remains an open problem" [Gentry 09]

A less theoretical leveled fully homomorphic scheme

Polynomials of degree d: SVP gap of $n^{2(d-1)}$
For $d = 3$ we must have $n^4 \sim O(1.01^n) \rightarrow n \simeq 6500$ [Gama and Nguyen 08]
A ciphertext : A few megabits

The proposed alternative

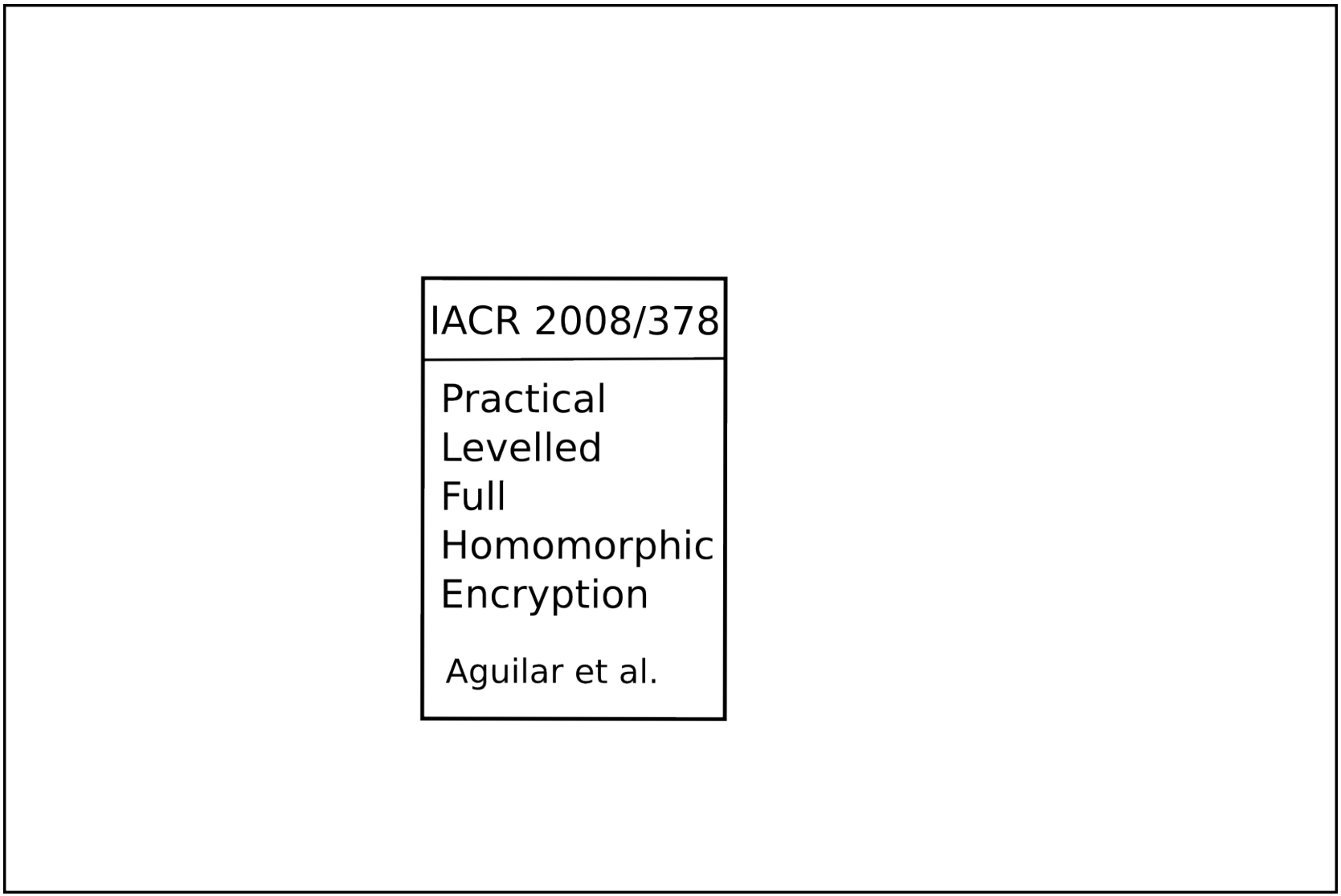
Additive Homomorphic Encryption with t-Operand Multiplications

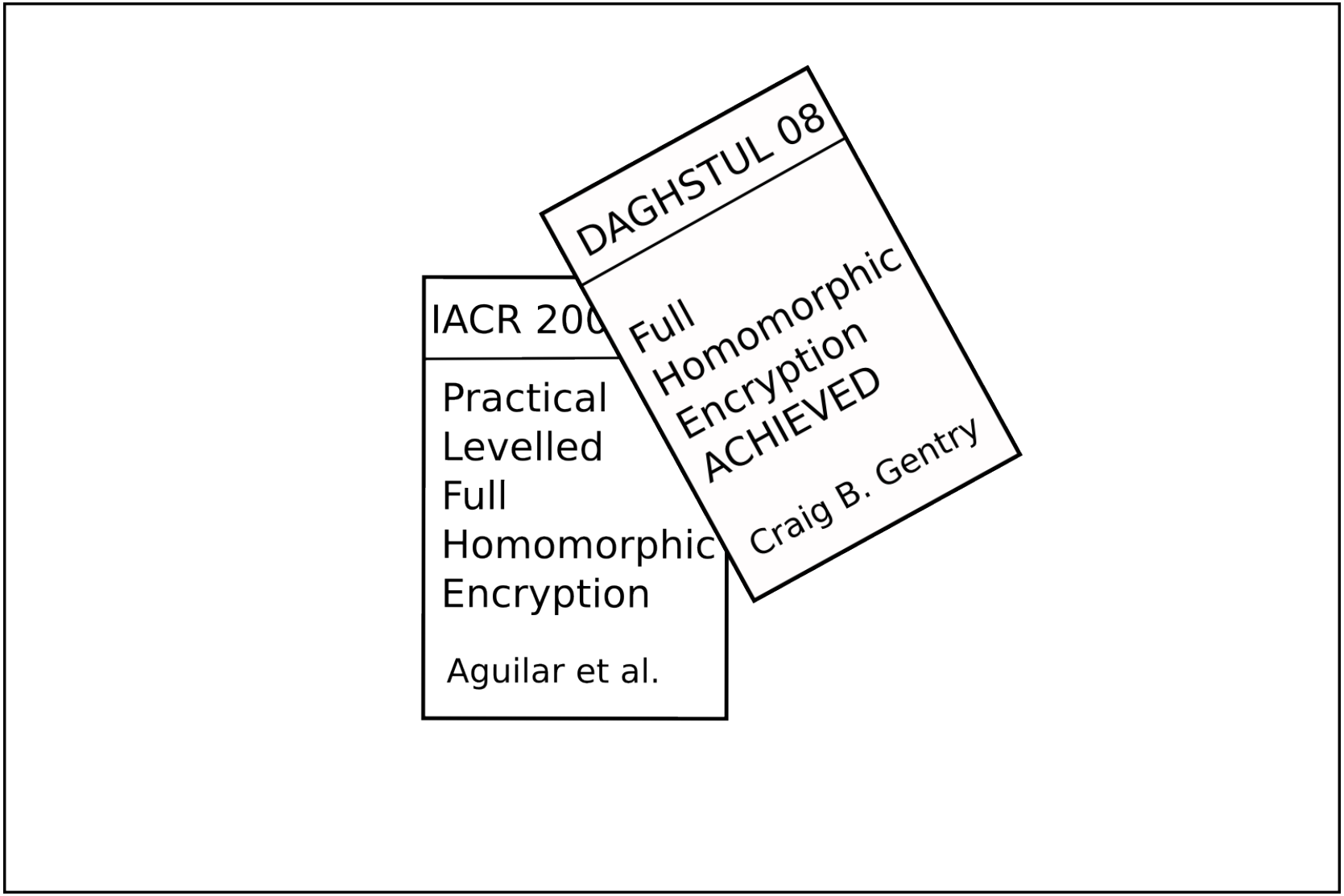
Aguilar Melchor C., Gaborit P., Herranz J.
`http://eprint.iacr.org/2008/378`

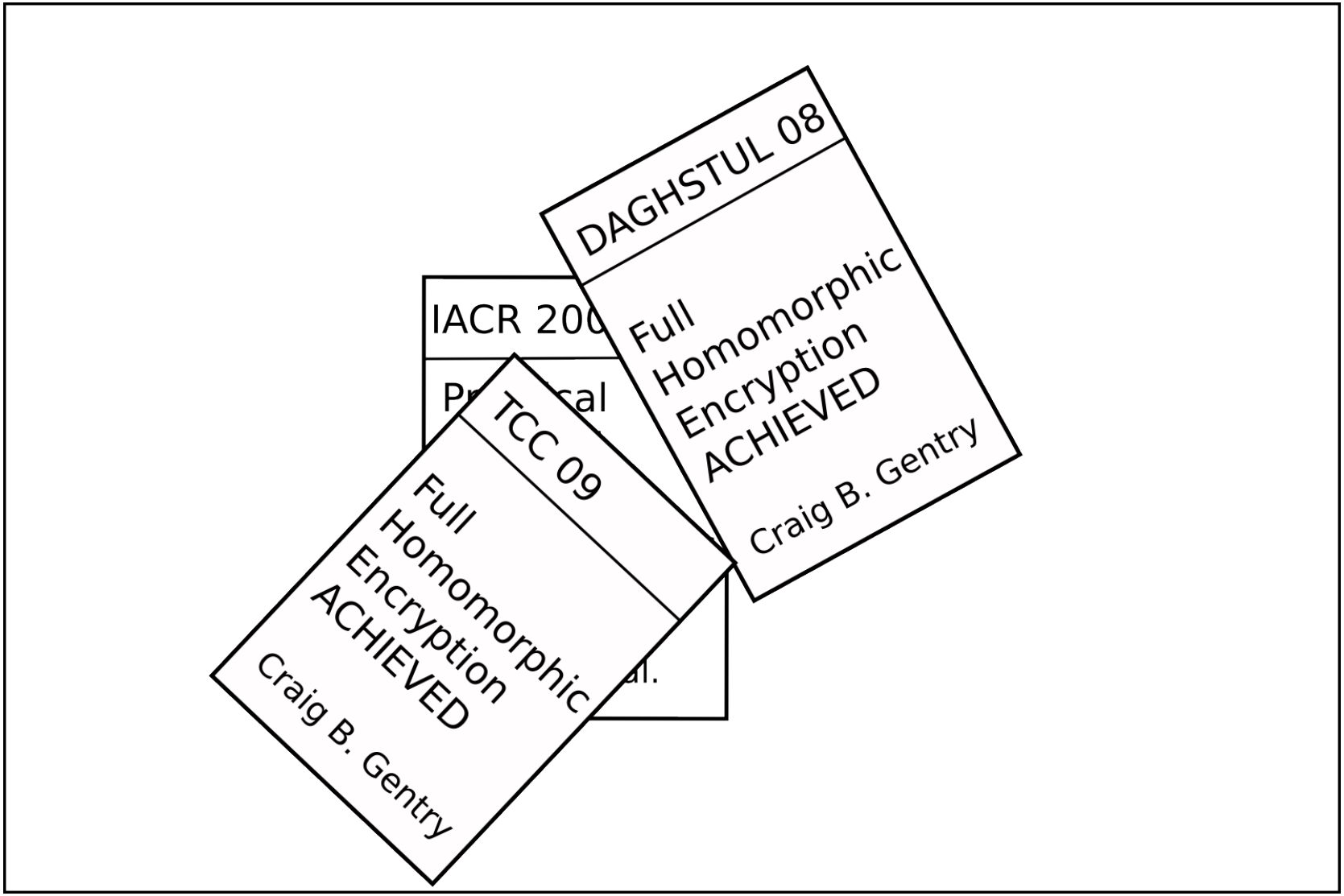
We propose

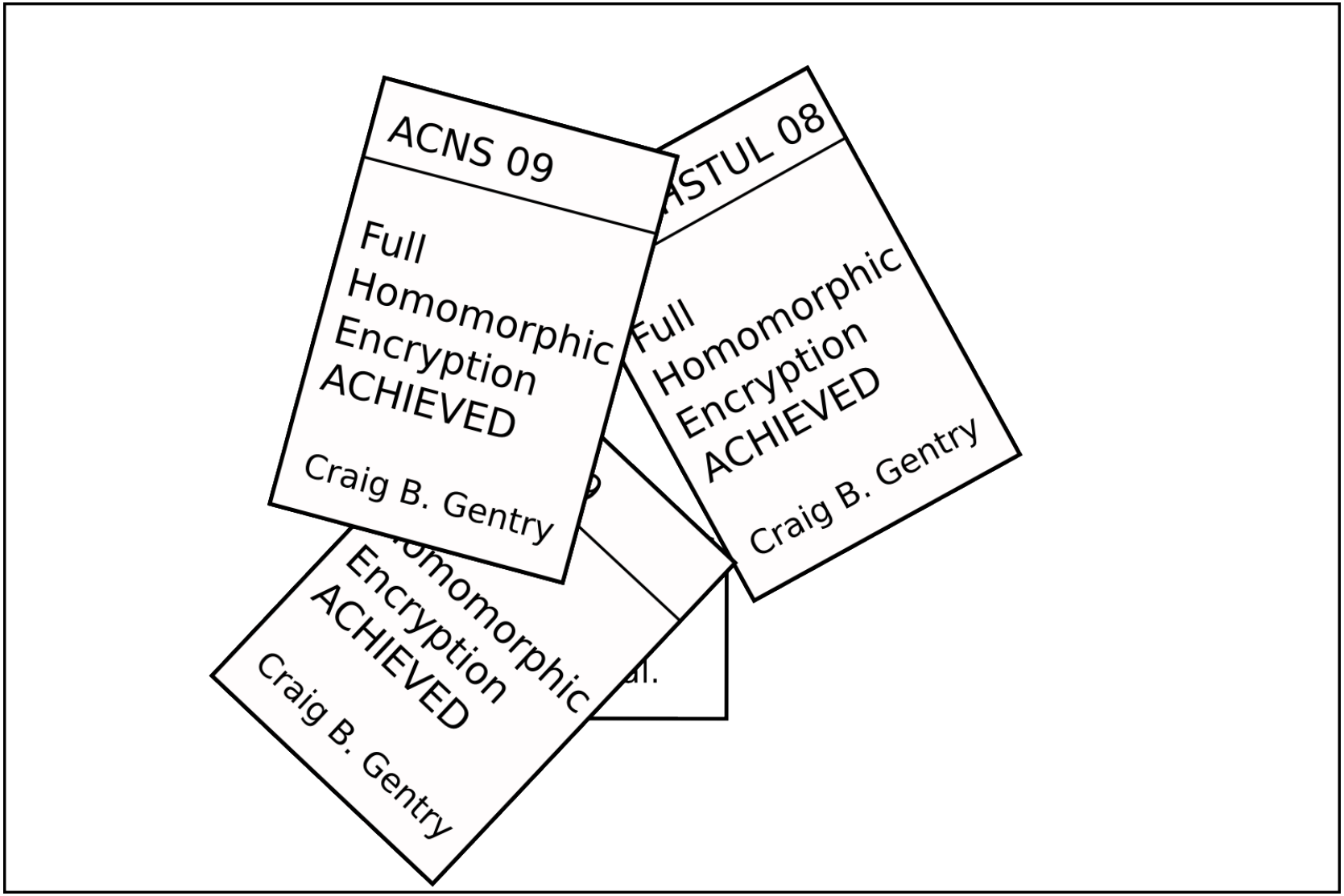
- A Generic construction to obtain leveled fully homomorphic schemes
- Two instances :
  - One based on a worst case/average case reduction to uSVP
  - One based on the DKVP

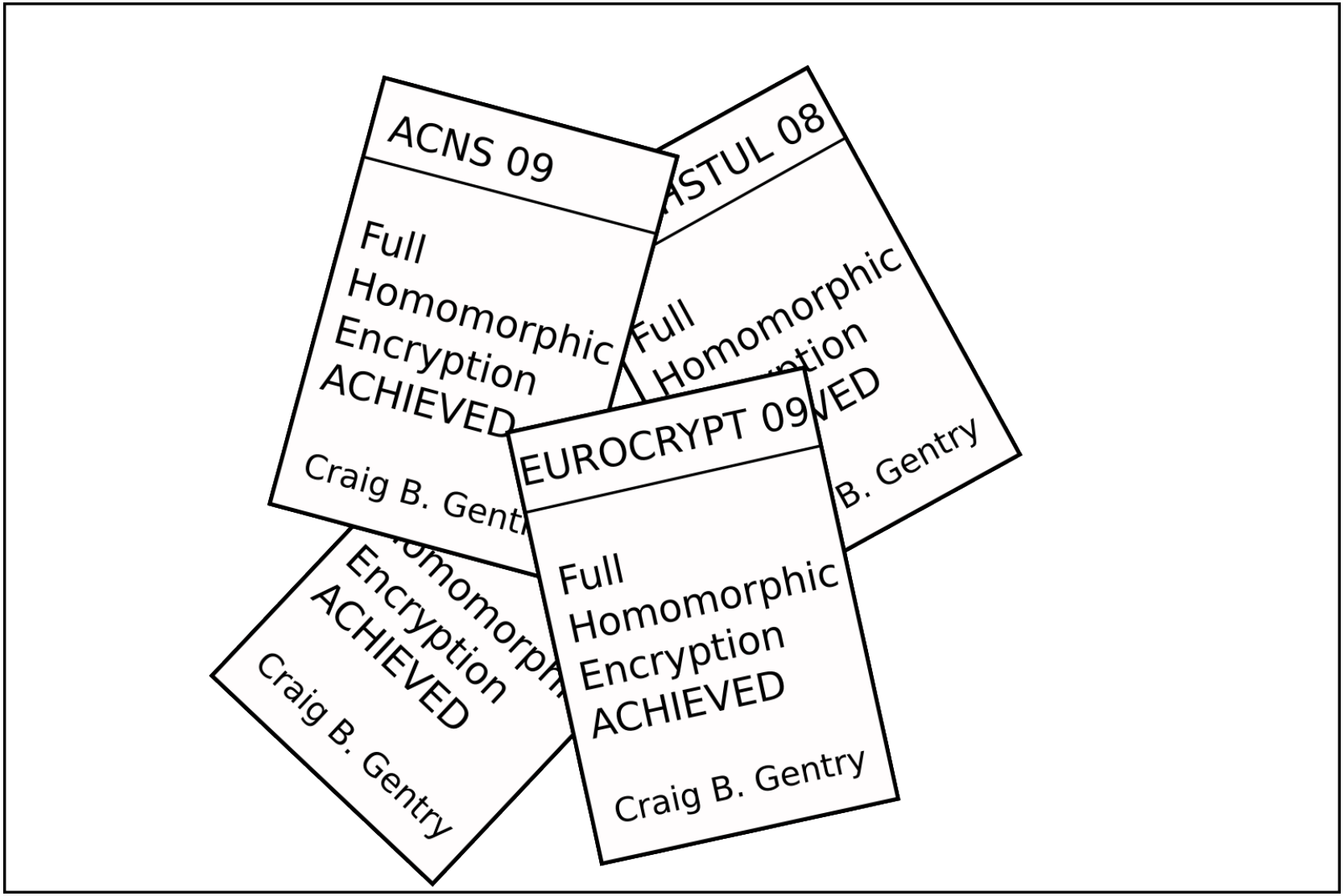
For $d = 3$: Ciphertexts of a few megabits

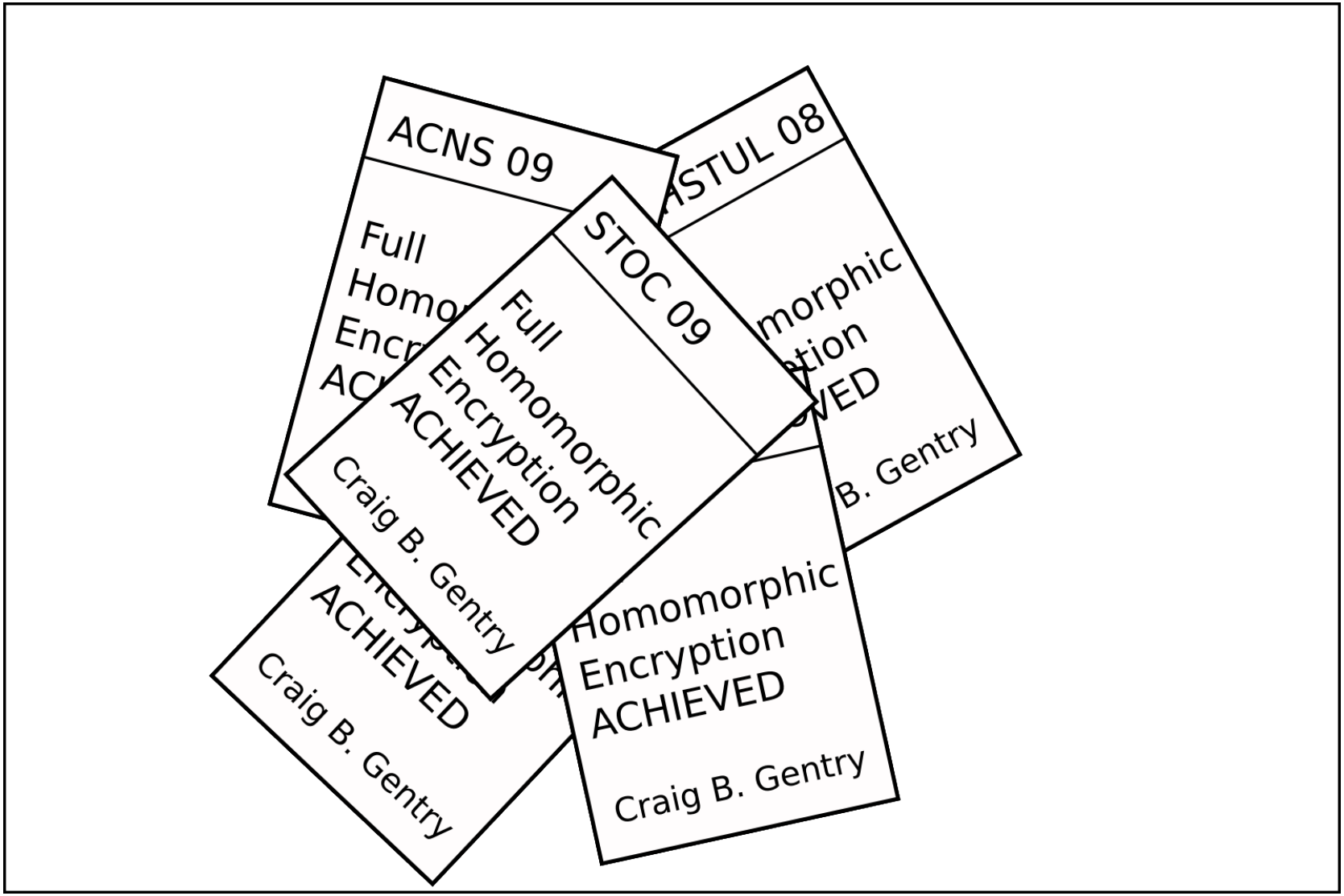

IACR 2008/378
Practical
Levelled
Full
Homomorphic
Encryption
Aguilar et al.

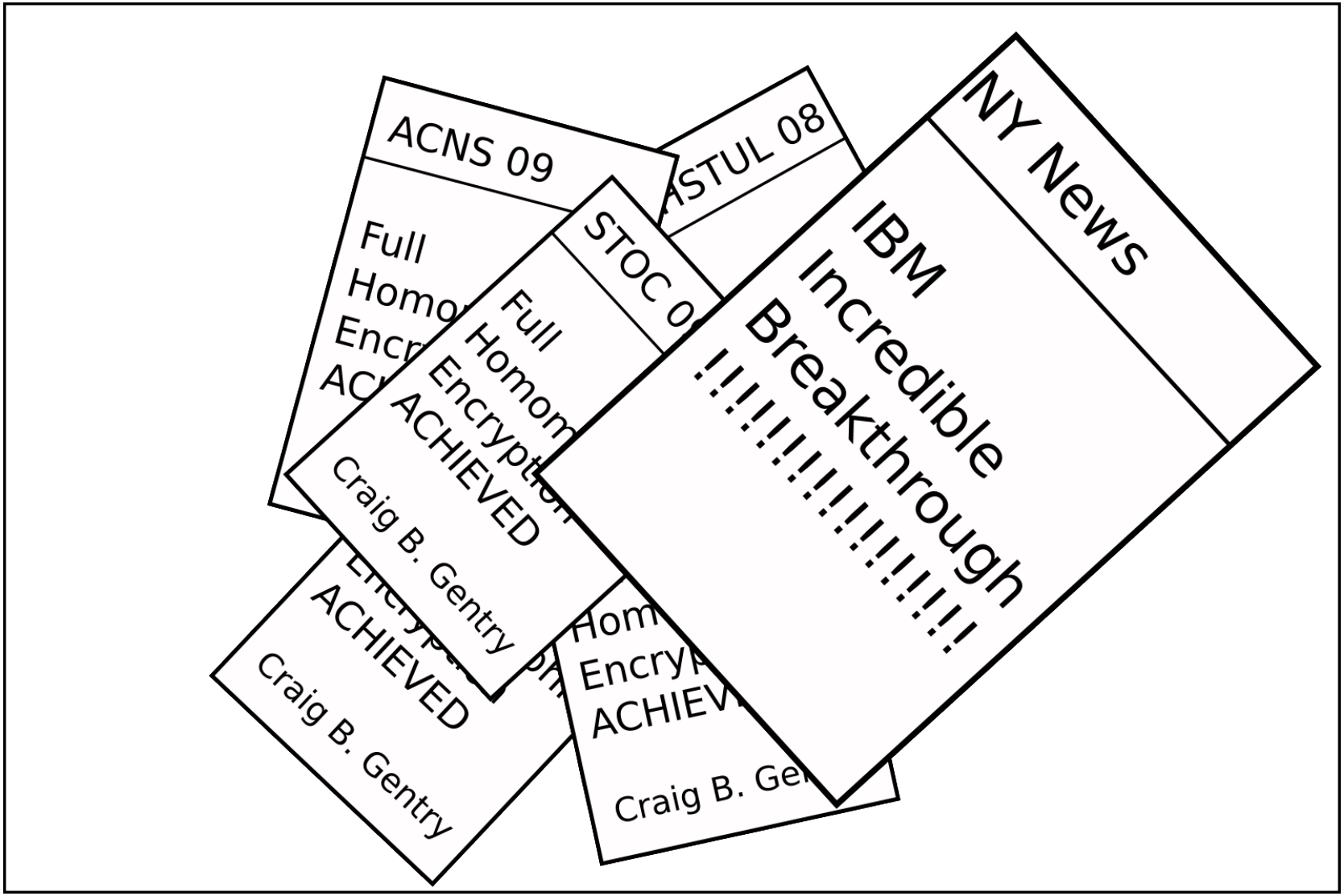

DAGHSTUL 08
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
IACR 200
Practical
Levelled
Full
Homomorphic
Encryption
Aguilar et al.

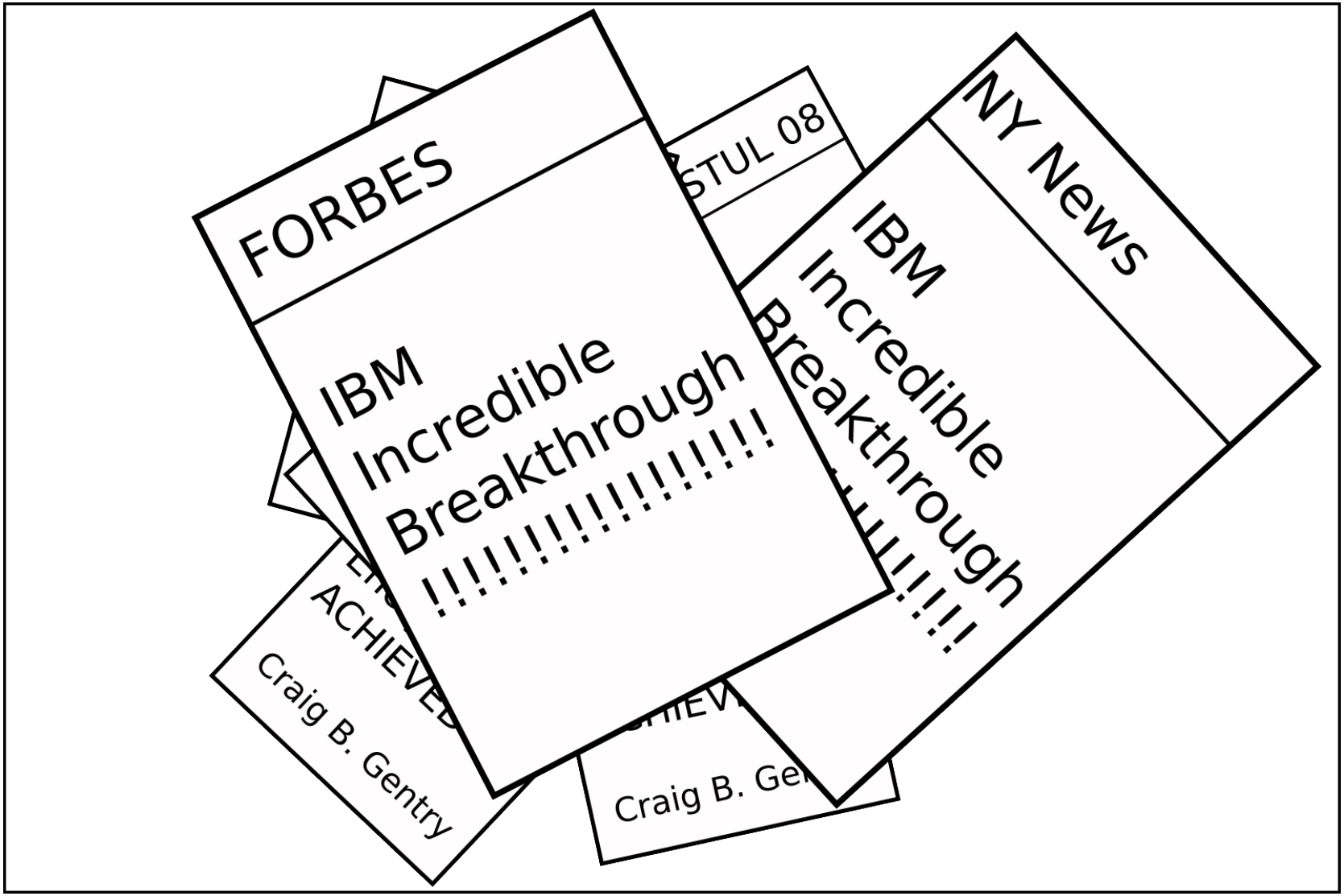

DAGHSTUL 08
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
IACR 200
TCC 09
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry

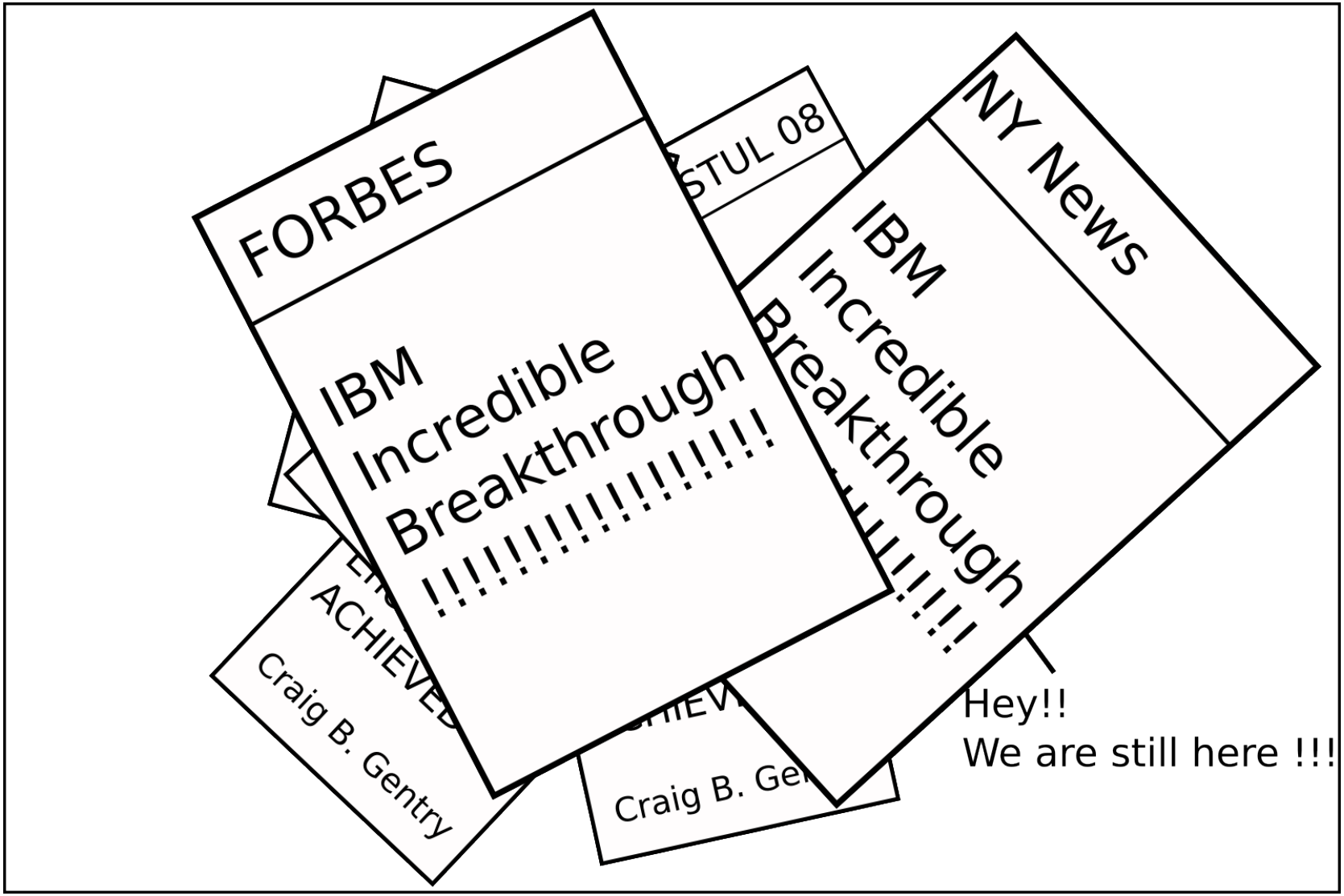

ACNS 09
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
ASTUL 08
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
Encryption
ACHIEVED
Craig B. Gentry


ACNS 09
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
EUROCRYPT 09
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry


ACNS 09
Full
Homo
Encr
AC
STOC 09
Full
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry
ASTUL 08
morphic
tion
VED
B. Gentry
Encryption
ACHIEVED
Craig B. Gentry
Homomorphic
Encryption
ACHIEVED
Craig B. Gentry


ACNS 09
Full
Craig B. Gentry
ACHIEVED
STOC 0
Full
Craig B. Gentry
ACHIEVED
ASTUL 08
Craig B. Ge
NY News
IBM
Incredible
Breakthrough
!!!!!!!!!!!!!!!


FORBES
IBM
Incredible
Breakthrough
!!!!!!!!!!!!!!!!!
STUL 08
NY News
IBM
Incredible
Breakthrough
!!!!!!!!
ACHIEVED
Craig B. Gentry
Craig B. Ge


FORBES
IBM
Incredible
Breakthrough
!!!!!!!!!!!!!!!!!
STUL 08
NY News
IBM
Incredible
Breakthrough
!!!!!!!!!!!!!!!!!
Hey!!
We are still here !!!
ACHIEVED
Craig B. Gentry
Craig B. Ge

Recent changes (for submission)

Complexity evaluation of LLL

uSVP-based instance is only theoretical

Introduction of ICP by Gentry

DKVP can be replaced by ICP

New practical construction

Polynomials can be evaluated in practice for $d \leq 10$