Ciphers for MPC and FHE

Martin Albrecht (RHUL),
Christian Rechberger (DTU)
Thomas Schneider (TUD)
Michael Zohner (TUD)
Tyge Tiessen (DTU)

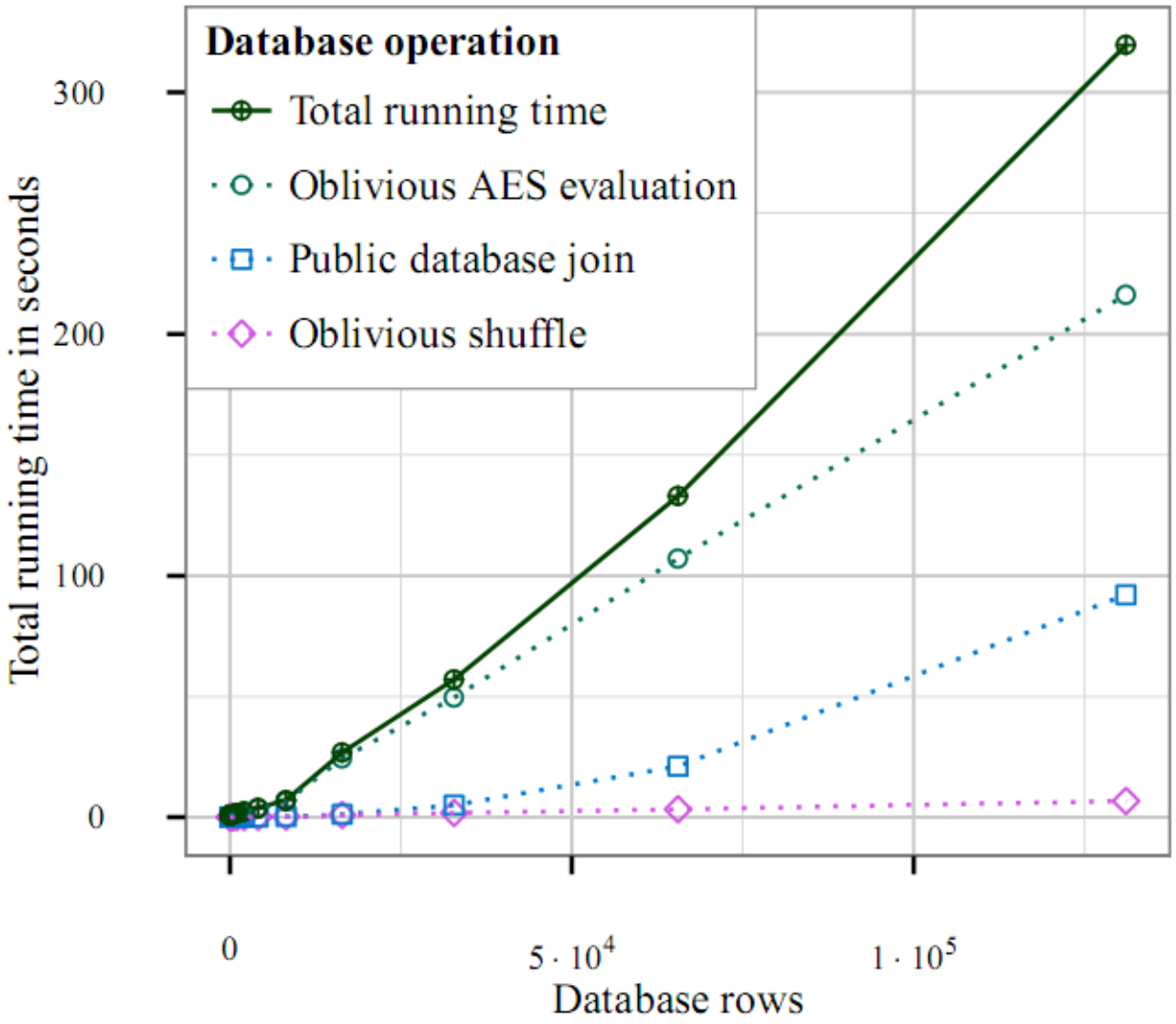
Example application: Secure database join, three parties

Way to combine several data sources in privacy preserving manner

Source: Cybernetica

Application:

- Merging databases from two different ministries in Estonia, while obeying various data-protection laws.



FHE application:
Avoid ciphertext expansion

FHE schemes typically come with a ciphertext expansion in the order of 1000s to 1000000s.

Proposed solution: encrypt with AES first!

Cloud homomorphically decrypts them (FHE AES needed).

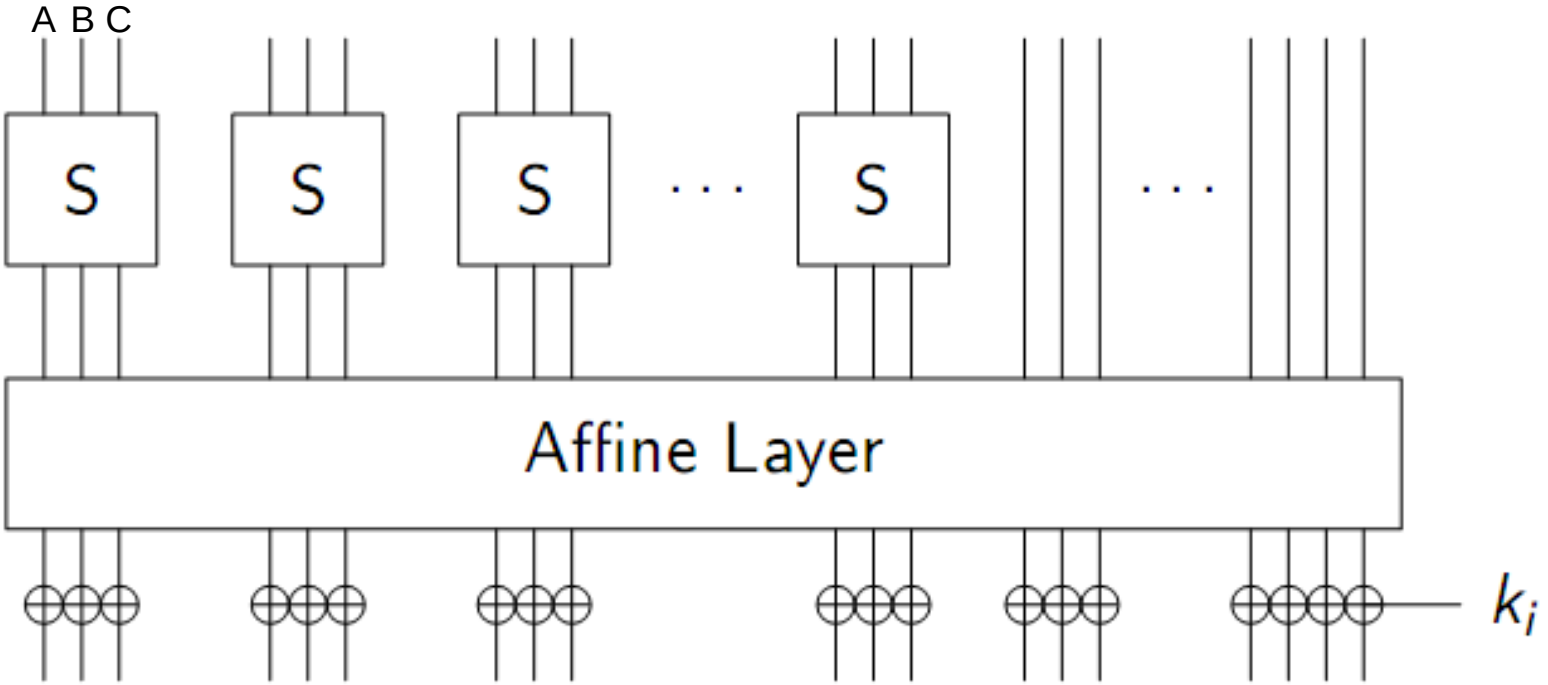
New designs for new computational models

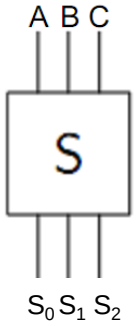
- Since 1970s: balance between linear and non-linear operations
- Idea: Explore ***extreme*** trade-offs

How would an efficient cipher look like if linear operations were for free?

- Metrics: AND-depth, #ANDs/bit, #ANDs

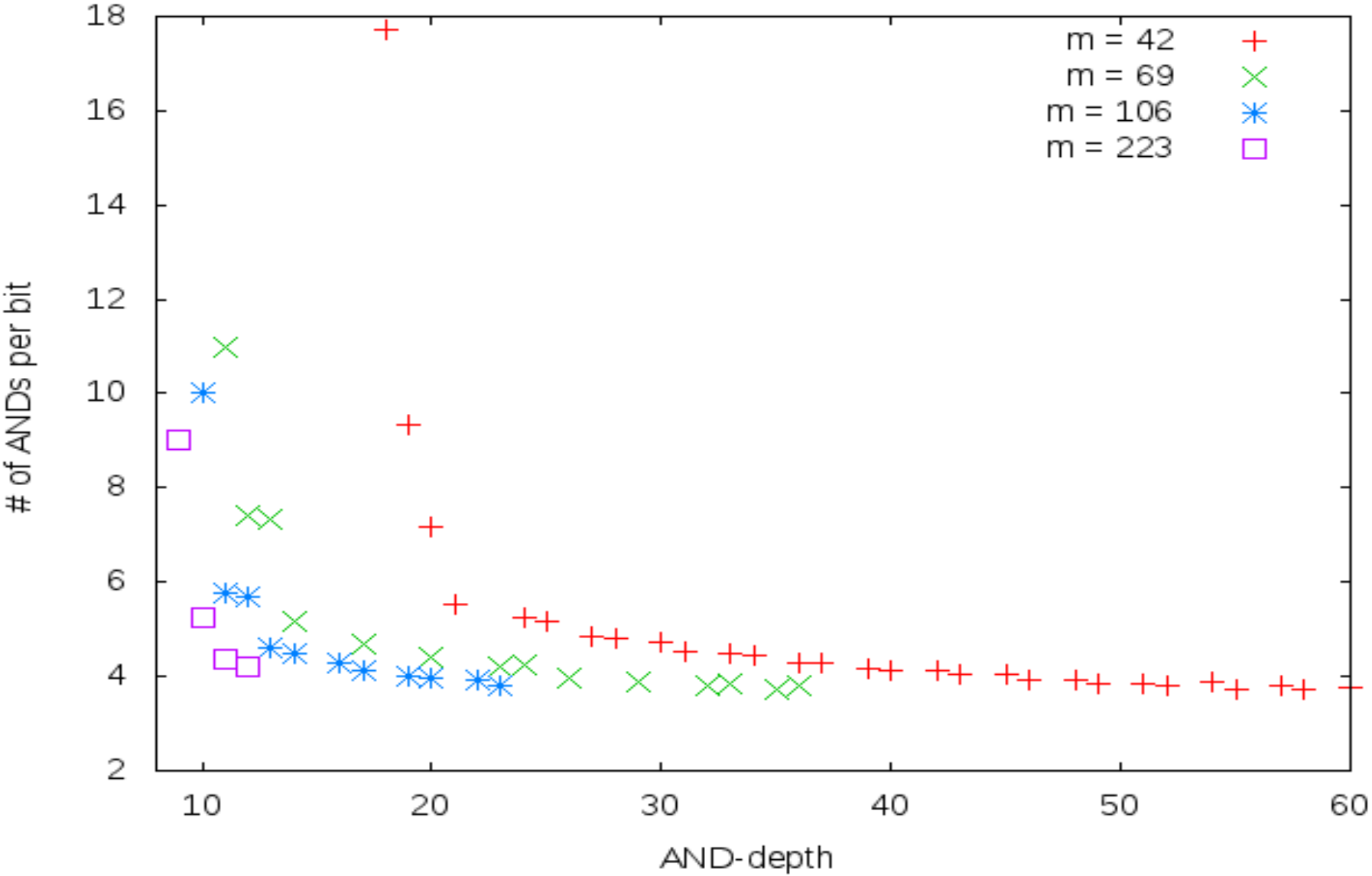
Round transformation





$$S_0(A, B, C) = A \oplus BC$$
$$S_1(A, B, C) = A \oplus B \oplus AC$$
$$S_2(A, B, C) = A \oplus B \oplus C \oplus AB$$

Visualizing the design space



Concrete instances

blocksize n	sboxes m	keysize k	data d	rounds r	ANDdepth	ANDs per bit
256	49	80	64	11	11	6.3
256	63	128	128	12	12	8.86

Properties and Advantages

- Low AND-depth and ANDs/encrypted bit
- Block size and security claims (data complexity and time complexity) de-coupled
- Differential and linear attacks will *provably* not work, except for extremely unlucky choices of linear layers

Implementation

- FHE:
  - 4 times faster than fastest AES Implementations
  - 20 times faster than fastest PRINCE Implementation
- MPC:
  - faster (detailed benchmarks in paper)

Conclusions

- New application for FSE research
- Balanced proposal, but also more extreme possibilities
  - AND-depth only 9 for 128-bit security
  - 3.5 ANDs per encrypted bit
- Of course, more cryptanalysis needed!

- Full version of EC2015 paper on eprint soon