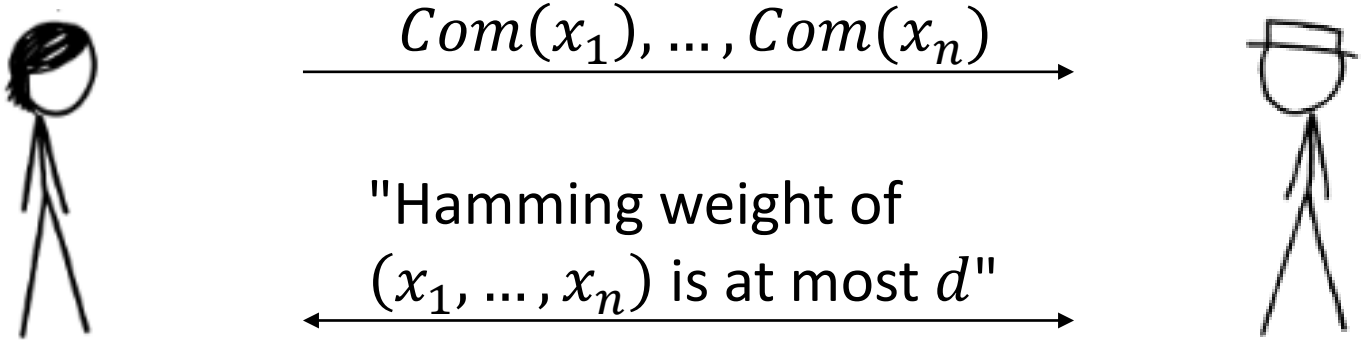
Compact Zero-Knowledge Proofs of Small Hamming Weight

Sabine Oechsner
Aarhus University

Joint work with
Ivan Damgård, Peter Scholl, Mark Simkin (Aarhus University),
Ji Luo (Tsinghua University)

THE SETTING

Proof of small Hamming weight



efficient zero-knowledge proof

Our contribution

Zero-knowledge protocol with

- unconditional soundness
- communication overhead independent of n

Applications: actively secure protocols

Outline

1. Zero-knowledge protocol for small Hamming weight

2. Applications:
   - k-out-of-n OT with active security
   - Separable accountable ring signatures

ZERO-KNOWLEDGE PROTOCOL OF SMALL HAMMING WEIGHT

Building blocks

Homomorphic commitments

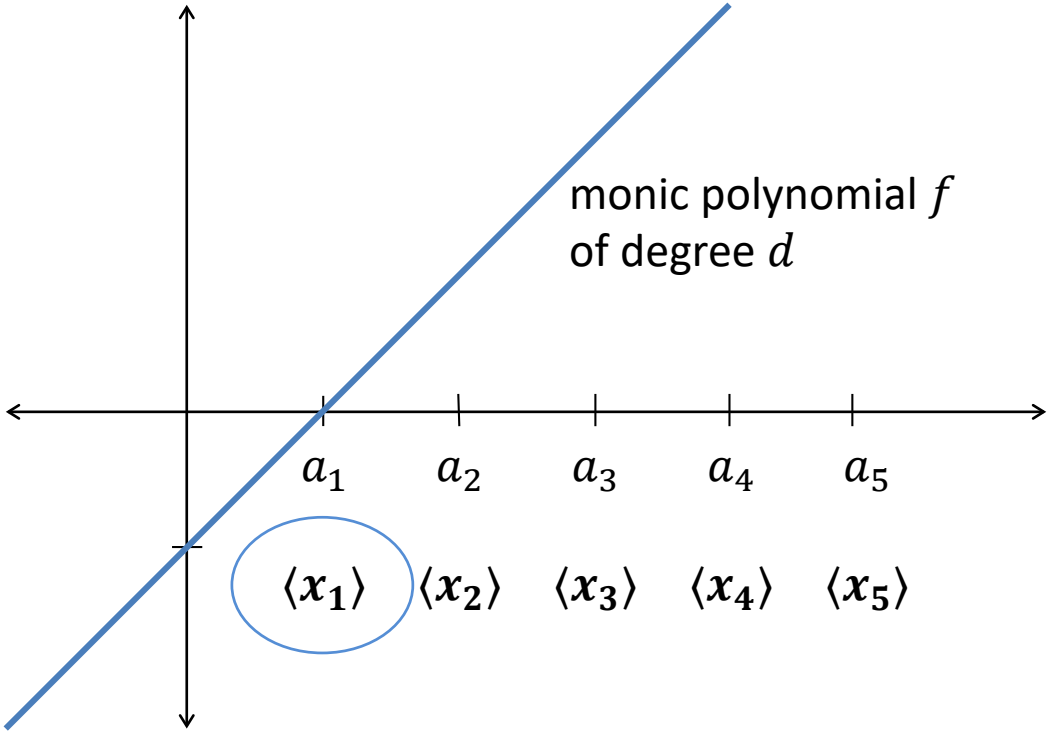
- Notation: $\langle x \rangle$
- Additively homomorphic:

$$u \cdot \langle x \rangle + v \cdot \langle y \rangle = \langle ux + vy \rangle$$

Zero-knowledge protocols

- $\boldsymbol{\pi_{zero}}$: proof of commitment $\langle 0 \rangle$ to 0
- $\boldsymbol{\pi_{mult}}$: proof of multiplication of $\langle r \rangle$ and $\langle s \rangle$ in commitment $\langle r \cdot s \rangle$

The idea



for all $i \in \{1, \ldots, n\}$,
$f(a_i) \cdot x_i = 0$

Protocol:

- compute f
- commit to f
- prove that
  $\sum_{i=1}^{n} f(a_i) x_i = 0$

Our protocol idea

Inputs $\langle x_1 \rangle, \ldots, \langle x_n \rangle$
public $a_1, \ldots, a_n$ and d

Prover

$(x_1, \ldots, x_n)$,
$weight(x_1, \ldots, x_n) \leq d$

compute polynomial f

commit to f →

← β

$\beta \xleftarrow{\$} \mathbb{F}$

randomize inputs $\langle y_i \rangle = \beta^{i-1} \langle x_i \rangle$

Verifier

randomize inputs $\langle y_i \rangle = \beta^{i-1} \langle x_i \rangle$

compute $\langle \sum_{i=1}^{n} f(a_i) y_i \rangle$

- when multiplying $\langle \alpha_j \rangle$, $\langle z_j \rangle$:

$\langle \alpha_j z_j \rangle$ →

← π_{mult}

compute $\langle \sum_{i=1}^{n} f(a_i) y_i \rangle$

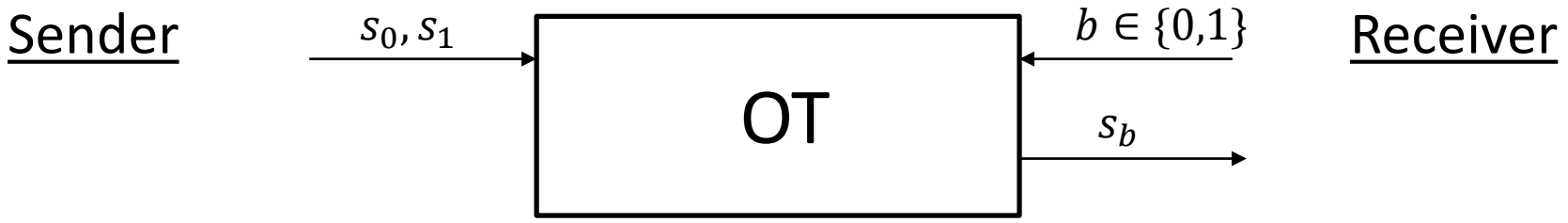
π_{zero} ←

check for $\langle 0 \rangle$

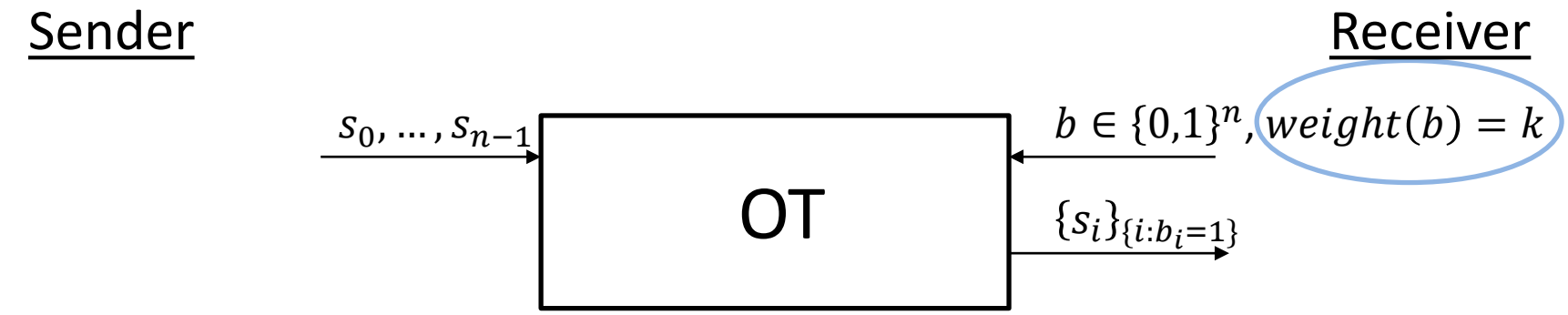
APPLICATION: K-OUT-OF-N OT WITH ACTIVE SECURITY

Oblivious transfer

1-out-of-2:



k-out-of-n:



k-out-of-n OT from 1-out-of-2 OT

- Passive security:

- Security against malicious receiver: Ensure that receiver can't learn more than k strings

k-out-of-n OT with active security

Previous solutions:

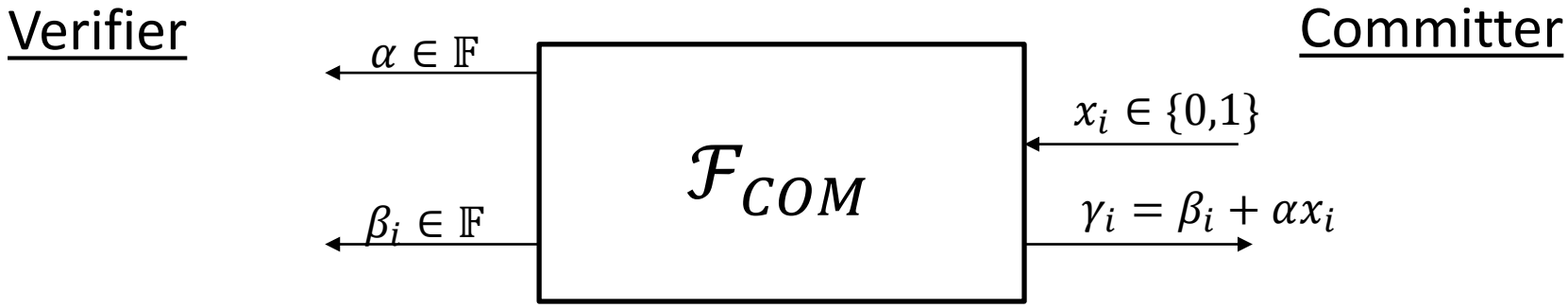
- either "approximately k"-out-of-n OT
- or require generic 2PC

Our result:

- black-box construction from 1-out-of-2 OT and correlation-robust hash function
- amortized communication overhead of $O(\kappa n)$

k-out-of-n OT with active security

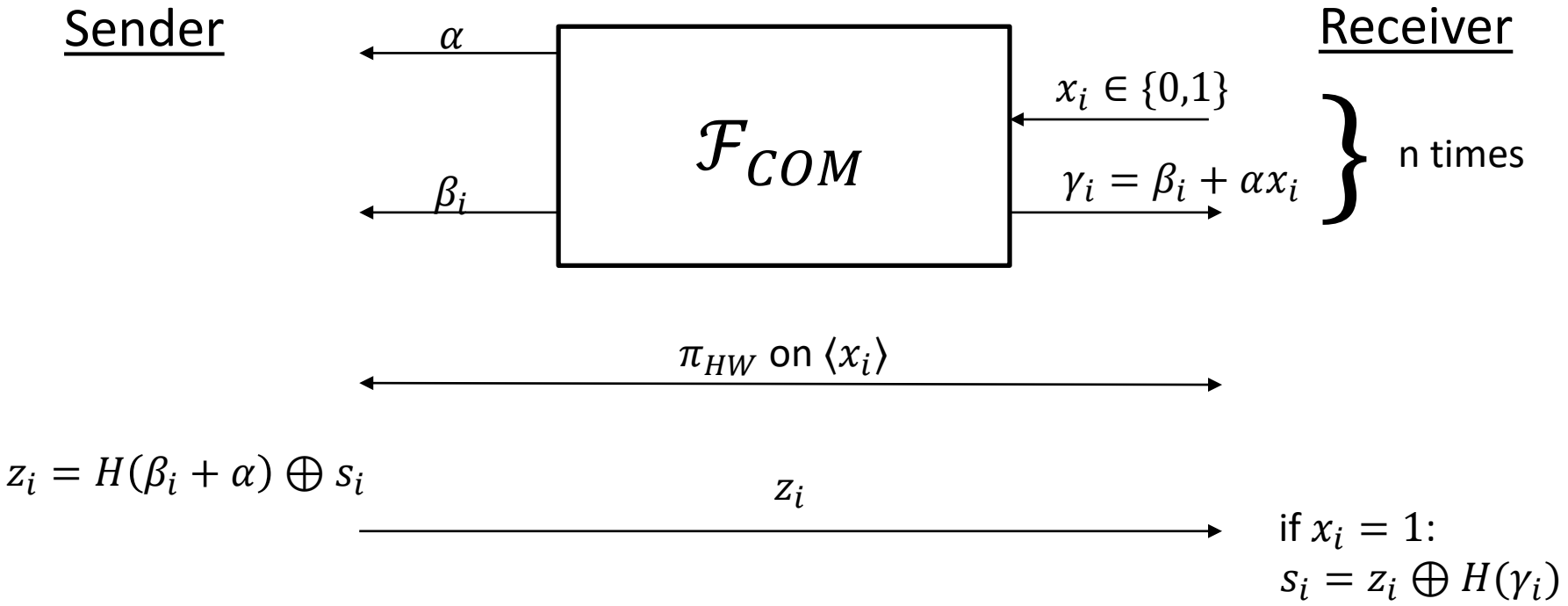
Step 1: From 1-out-of-2 OT to homomorphic commitment scheme



(extending known constructions)

k-out-of-n OT with active security

Step 2: From $\mathcal{F}_{COM}$ to correlated 1-out-of-2 OT to k-out-of-n OT with hash function

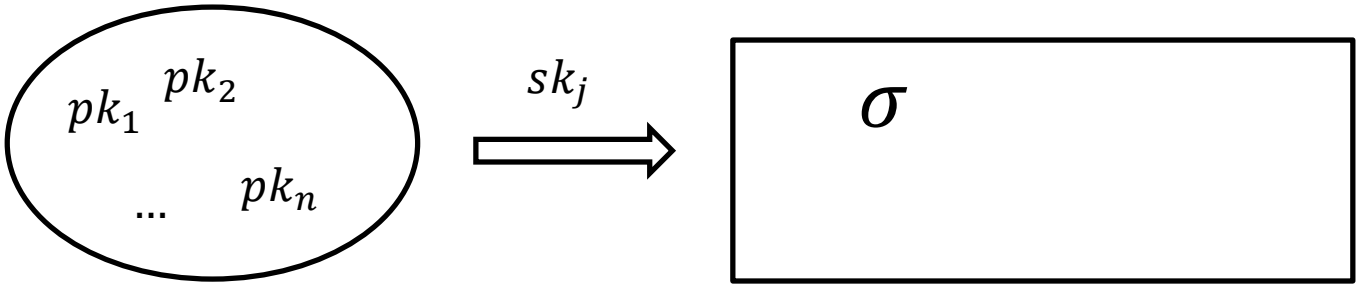


APPLICATION: SEPARABLE ACCOUNTABLE RING SIGNATURE

Ring signatures

Dynamic ring of potential signers $P_1, \ldots, P_n$

Any P_j can sign anonymously of behalf of ring



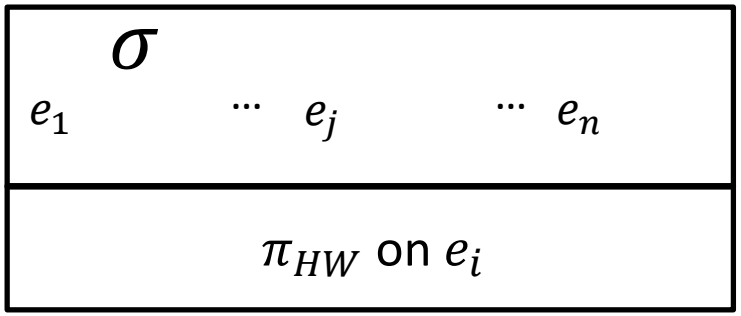
Separability: different signing algorithms or keys

Accountability: signer can dynamically pick a designated opener that can revoke anonymity

Our construction

Separable ring signatures:

- Or-composition of Σ-protocols for knowledge of one of secret keys [CDS94] + Fiat-Shamir
- Signer controls randomness



Accountability:

- Encode identity into "randomness"
- Prove correct encoding using π_{HW}
- Designated opener gets trapdoor

MORE APPLICATIONS

More applications

Active security for …

- More efficient preprocessing for TinyTables
- Mixing with public verifiability
- PIR with malicious client

CONCLUSION

Conclusion

Efficient proof of small Hamming weight

- Zero-knowledge with unconditional soundness
- Communication overhead independent of n
- Idea: prove that secret polynomial evaluates to 0

Applications:

- k-out-of-n OT with active security
- Separable accountable ring signatures
- …

Thank you.