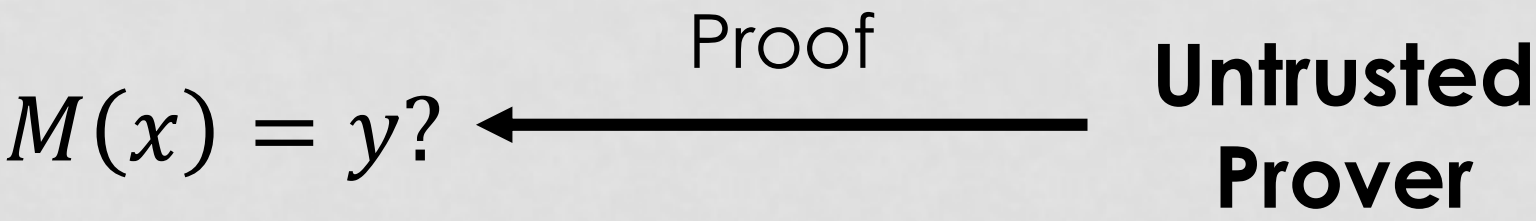
ON ZERO-TESTABLE HOMOMORPHIC ENCRYPTION AND PUBLICLY VERIFIABLE ARGUMENTS

Omer Paneth and Guy Rothblum

ePrint report 2014/981

Goal:

Efficiently verify the correctness of a long computation



Proof should save verifier time!

Publicly Verifiable Non-Interactive Arguments

CRS

$M(x) = y?$ ← Proof ← **Efficient Untrusted Prover**

Publicly Verifiable Non-Interactive Arguments

Non-Falsifiable
Knowledge Assumptions

(e.g. knowledge of exponent)

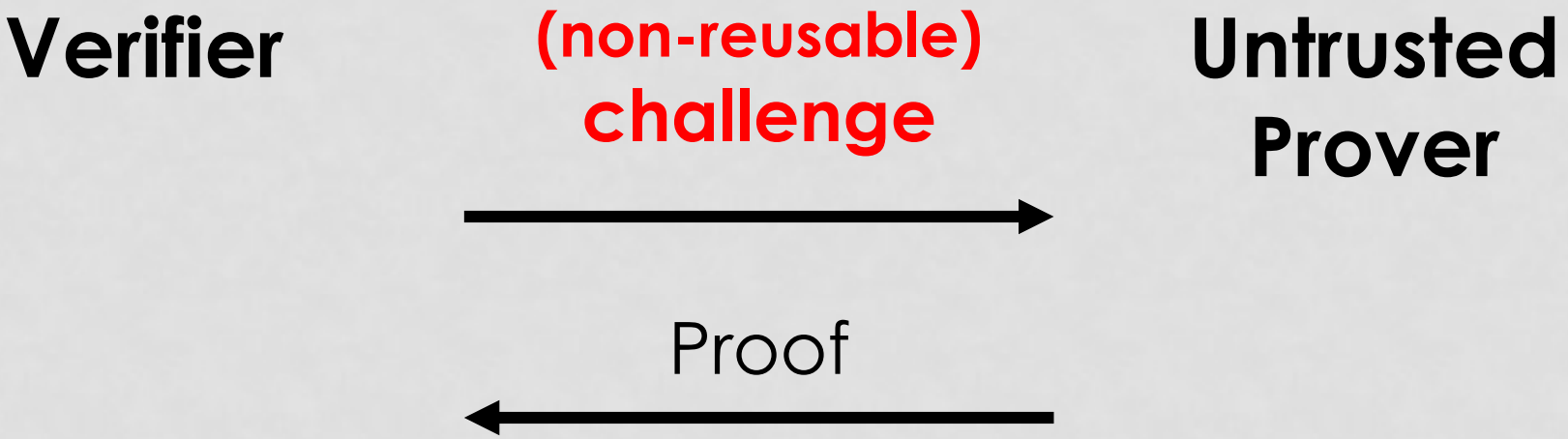
Indistinguishability
Obfuscation

Sub-exp.
reduction

Multilinear Maps \
Graded Encodings

No candidates

Privately Verifiable Two-Message Arguments



Kalai-Raz-Rothblum 14: construction assuming

Private Information Retrieval or

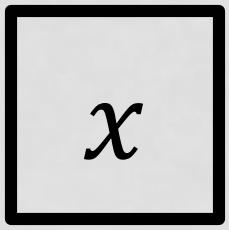
Somewhat Homomorphic Encryption

Publicly Verifiable Non-Interactive Arguments

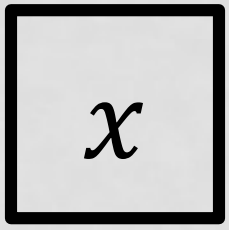
1. Efficiently falsifiable assumption
2. Adaptive soundness
3. Black box use of crypto

Zero-Testable Homomorphic Encryption

Somewhat
Homomorphic Encryption

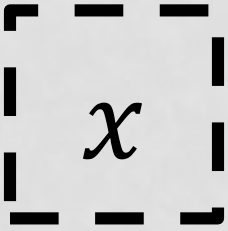


Zero-Testable
Homomorphic Encryption



Weak ZT

Graded Encodings



ZT

$\mathrm{ZT}\left(\boxed{C(x,y,z)}\right)$

Candidate: [van Dijk-Gentry-Halevi-Vaikuntanathan 10]

Somewhat Homomorphic Encryption over the Integers

$\boxed{x}$ $\boxed{y}$ $\boxed{z}$

Strong ZT

Trivial Zero:

$C(X, Y, Z) = 0 \Rightarrow$ ZT pass

Non-Zero:

$C(x, y, z) \neq 0 \Rightarrow$ ZT fail

Weak ZT

Trivial Zero:

$C(X, Y, Z) = 0 \Rightarrow$ ZT pass

Non-Zero:

$C(x, y, z) \neq 0 \Rightarrow$ ZT fail

Additional properties:

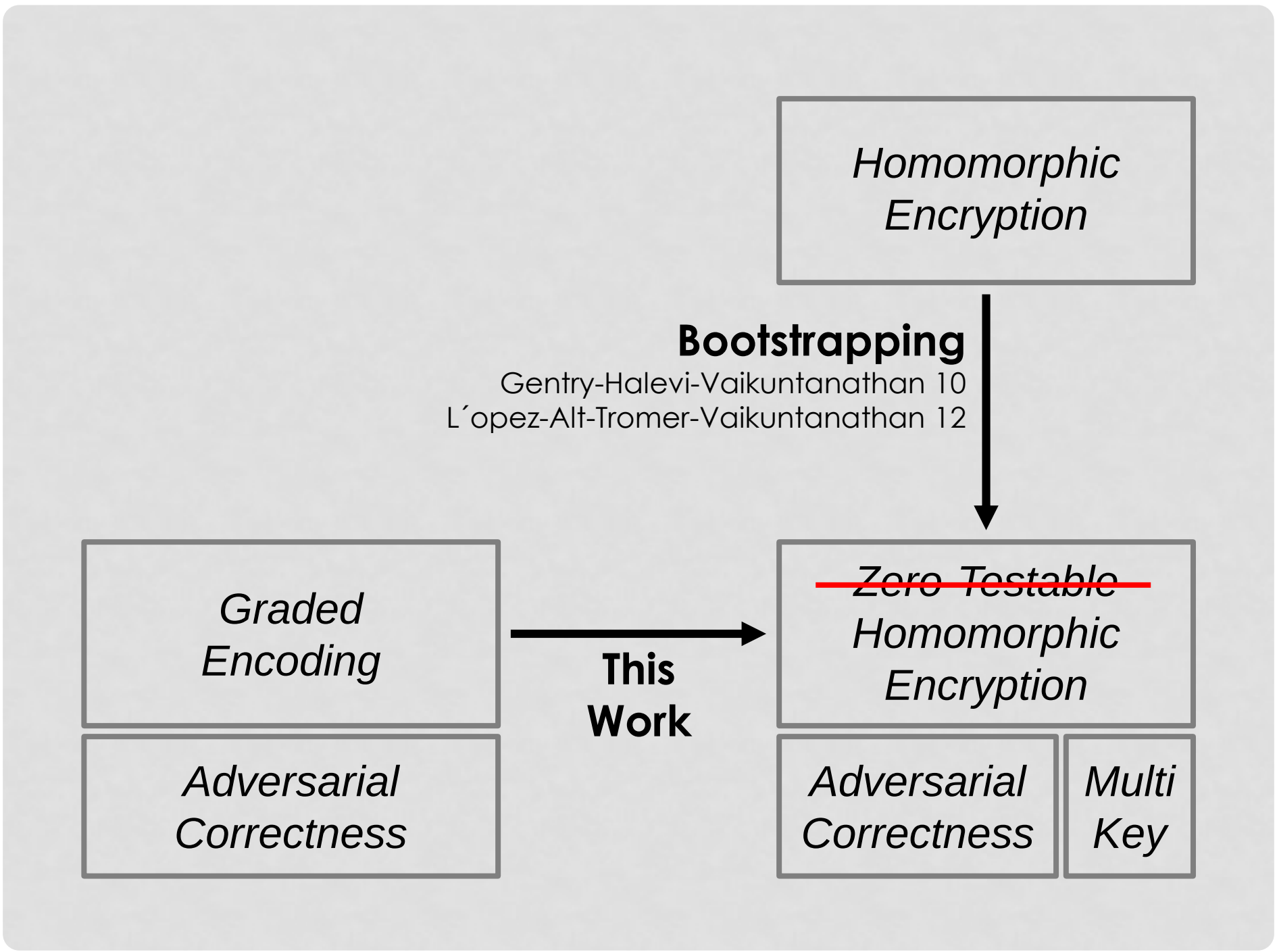
1. Multi-Key Homomorphism (for 3 keys)

$$\mathrm{Enc}_{sk_1}(x) \circ \mathrm{Enc}_{sk_2}(y) = \mathrm{Enc}_{(sk_1, sk_2)}(x \circ y)$$

2. Adversarial Correctness

Hard to find ciphertexts c_1^*, c_2^* s.t

$$\mathrm{Dec}(c_1^* \circ c_2^*) \neq \mathrm{Dec}(c_1^*) \circ \mathrm{Dec}(c_2^*)$$

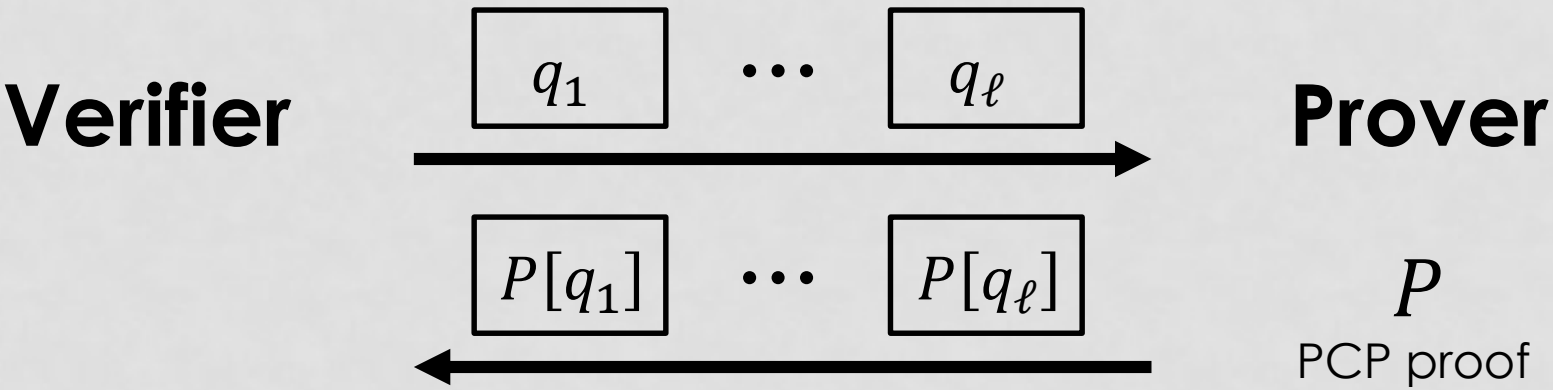

Homomorphic Encryption
Bootstrapping
Gentry-Halevi-Vaikuntanathan 10
L´opez-Alt-Tromer-Vaikuntanathan 12
Graded Encoding
Adversarial Correctness
This Work
Zero-Testable Homomorphic Encryption
Adversarial Correctness
Multi Key

Theorem:

Zero-testable 3-key homomorphic encryption
with adversarial correctness

black box

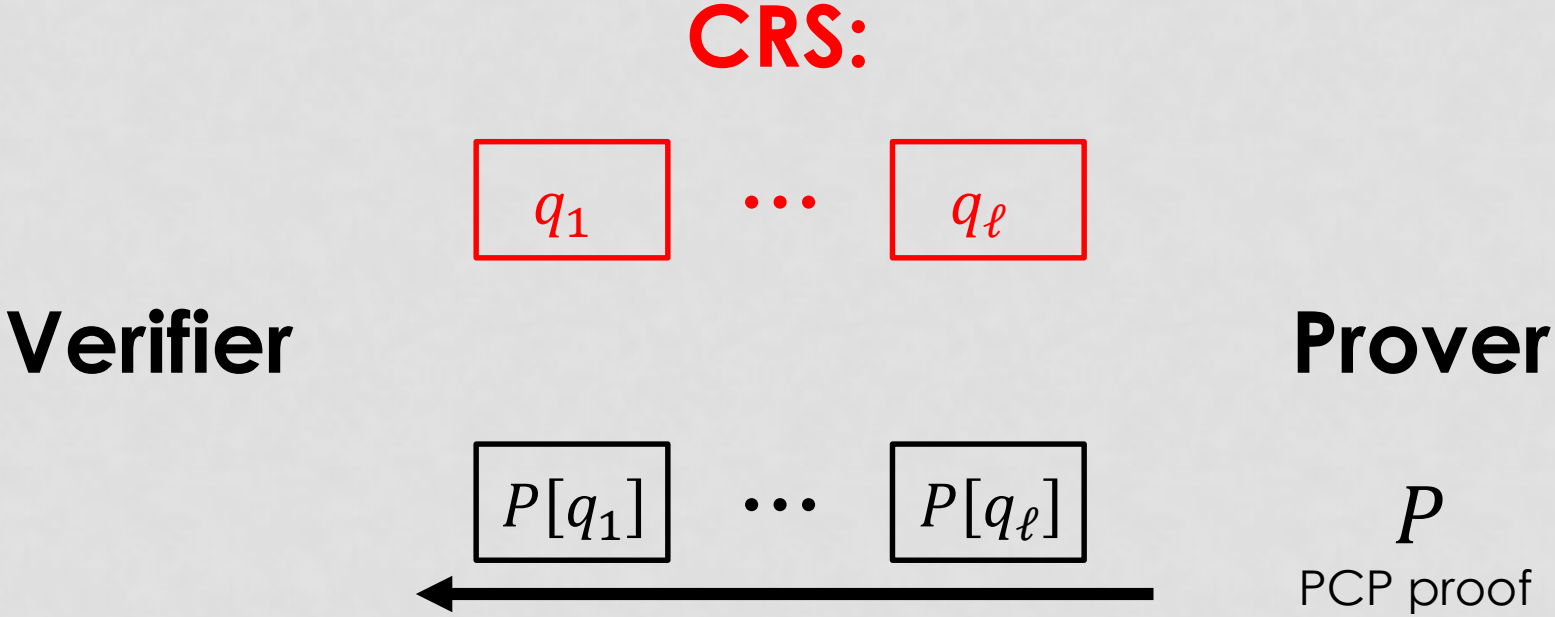
Publicly verifiable non-interactive arguments
with adaptive soundness



Privately verifiable two-message arguments from somewhat homomorphic encryption

Publicly verifiable non-interactive arguments **?**

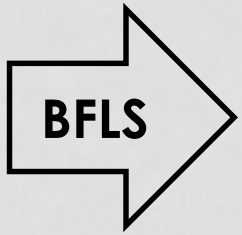
[Biehl-Meyer-Wetzel 98, Aiello-Bhatt-Ostrovsky-Rajagopalan 00, Kalai-Raz-Rothblum 14]



Prover's answers give public information about P

The PCP of Babai-Fortnow-Levin-Szegedy

$M(x) = y$



$P_1, \ldots, P_m$
Low-degree polynomials

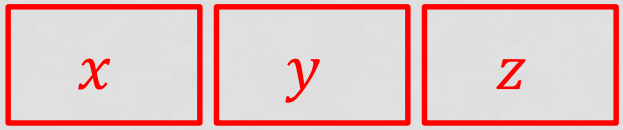
$\Updownarrow$

$P_1 + P_2 \equiv P_3$

$\vdots$

$P_m \equiv 0$

CRS:



Verifier **Prover**

$\{P_i(x,y,z)\}_{i\leq m}$ $P_1, \ldots, P_m$

$$\mathrm{ZT}\big(P_1(x,y,z) + P_2(x,y,z) - P_3(x,y,z)\big)$$

$$\vdots$$

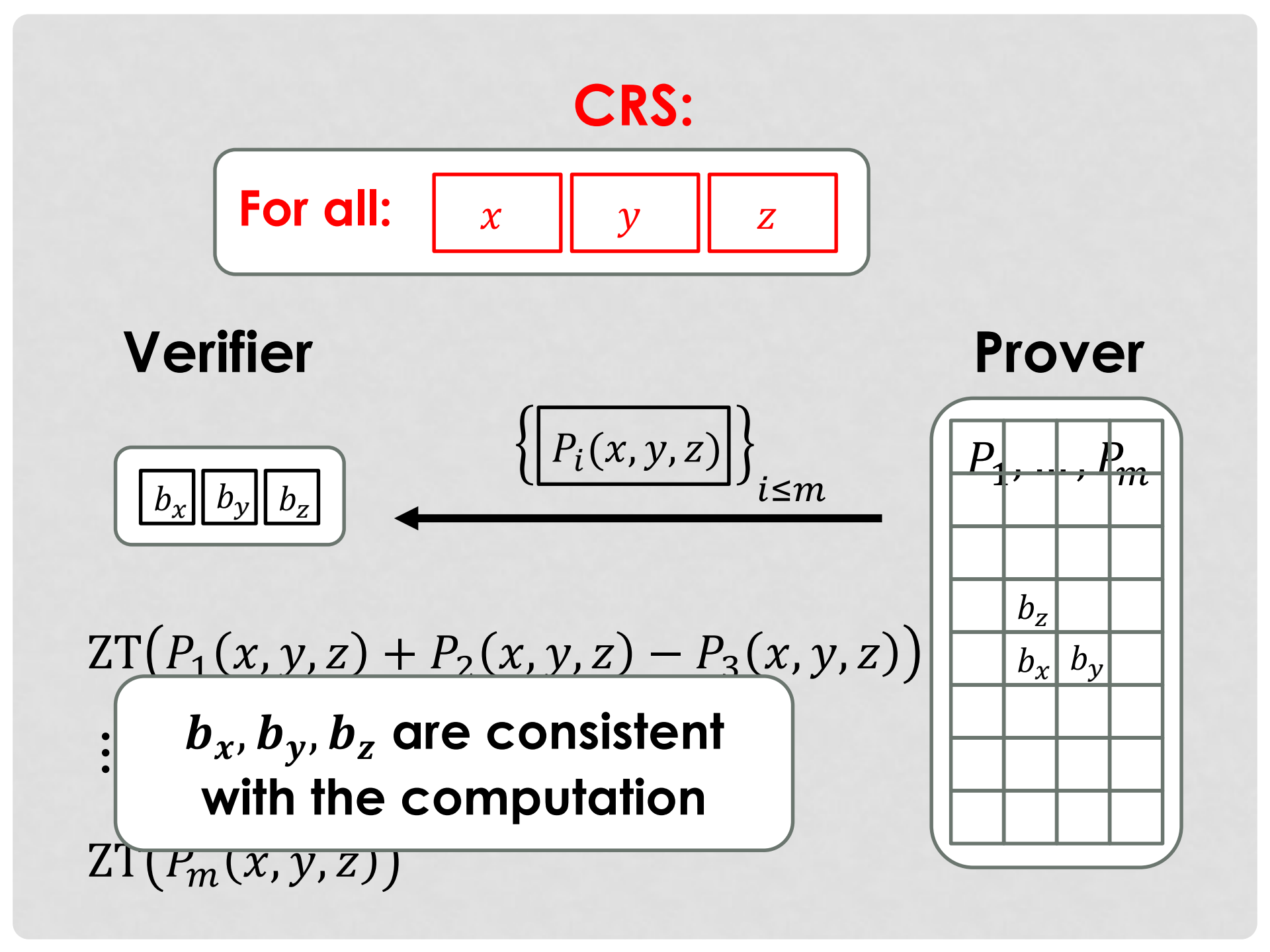
$$\mathrm{ZT}\big(P_m(x,y,z)\big)$$

Proof plan:

Local consistency at a random point

Local consistency everywhere

Global consistency


CRS:
For all:
x
y
z
Verifier
Prover
$\{P_i(x,y,z)\}_{i\le m}$
b_x b_y b_z
$P_1, \ldots, P_m$
b_z
b_x b_y
$\mathrm{ZT}(P_1(x,y,z) + P_2(x,y,z) - P_3(x,y,z))$
$\mathrm{ZT}(P_m(x,y,z))$
b_x, b_y, b_z are consistent with the computation

Conclusion

1. Sometimes weak ZT is sufficient.

2. Better publicly verifiable delegation trough private verifiability techniques.

3. Publicly verifiable delegation from standard assumptions?

Thanks!