Encrypt your channels!

On the (in)security of GMW with authenticated communication

Peter Scholl

TPMPC 2019 Rump Session, Bar-Ilan University

AARHUS
UNIVERSITY

MPC 101: the GMW protocol

- [Goldreich-Micali-Wigderson 87]
  - Additively secret share inputs
  - XOR gates: local
  - AND gates: OT
  - Outputs: reconstruct shares

MPC 101: the GMW protocol

- [Goldreich-Micali-Wigderson 87]
  - Additively secret share inputs
  - XOR gates: local
  - AND gates: OT
  - Outputs: reconstruct shares

- Question: what kind of communication channels are necessary?

MPC 101: the GMW protocol

- [Goldreich-Micali-Wigderson 87]
  - Additively secret share inputs
  - XOR gates: local
  - AND gates: OT
  - Outputs: reconstruct shares

- Question: what kind of communication channels are necessary?

Encrypted vs Unencrypted (but authenticated)

Let’s ask the experts

[GMW 87]

Let’s ask the experts

[GMW 87]

means of $n \cdot (n-1)$ special tapes. Machine i publically sends messages (strings) to machine j by means of a special tape $i \rightarrow j$ on which only i can write and that all other machines can read. There is

Let’s ask the experts

[GMW 87]

At the start, each party takes each of his private bits and encodes it by a 5-permutation σ as in [Ba]. Then he divides σ. That is, he selects at random n-1 5-permutations $\sigma_1,\ldots,\sigma_{n-1}$ and gives the pair

Let’s ask the experts

[GMW 87]

What the *#!? is this GMW protocol, anyway?

At the start, each party takes each of his private bits and encodes it by a 5-permutation σ as in [Ba]. Then he divides σ. That is, he selects at random n-1 5-permutations $\sigma_1,\ldots,\sigma_{n-1}$ and gives the pair

Let’s try again

Foundations of Cryptography
[Gol 04]

Let’s try again

We comment that the said protocols happen to maintain their security *even if the adversary can wire-tap all communication lines*. This follows from the fact that *privacy with respect to wire-tapping adversaries* happens to hold for all privacy reductions presented in the current section, as well as for the protocols presented in Section 7.3.

Foundations of Cryptography

[Gol 04]

Let's try again

We comment that the said protocols happen to maintain their security *even if the adversary can wire-tap all communication lines.* This follows from the fact that *privacy with respect to wire-tapping adversaries* happens to hold for all privacy reductions presented in the current section, as well as for the protocols presented in Section 7.3.

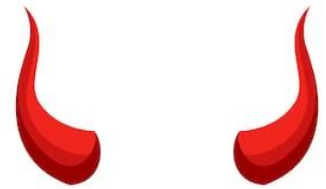
Foundations of Cryptography
[Gol 04]

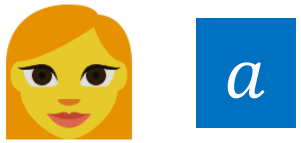
functionality $\mathcal{G}$ in the $\mathcal{G}$-hybrid model, then π UC realizes $\mathcal{G}$ from scratch.

We consider a network where the adversary sees all the messages sent, and delivers or blocks these messages at will. (The fact that message delivery is not guaranteed frees us from the need to

Universally Composable Two-Party and Multi-Party Secure Computation
[CLOS '02]

Securely computing $z = a + b + c$



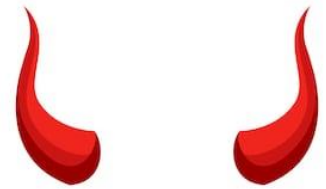


a

b

c

Securely computing $z = a + b + c$



a

a_1

b_1

c_1

b

a_2

b_2

c_2

c

a_3

b_3

c_3

Securely computing $z = a + b + c$

a

a_1

b_1

c_1

b

a_2

b_2

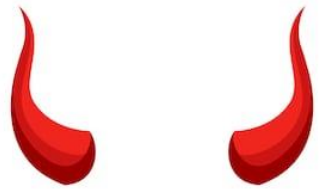
c_2

c

a_3

b_3

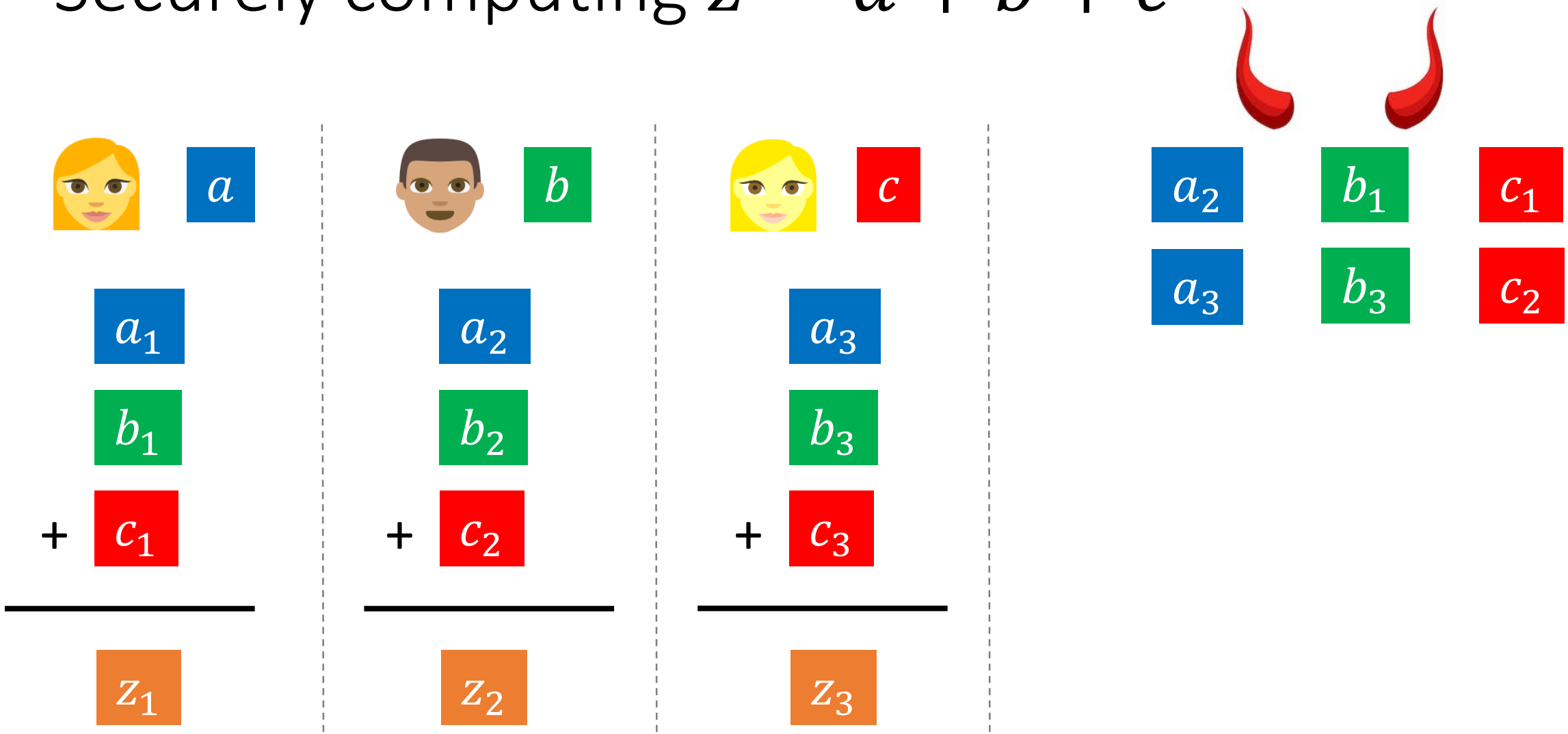
c_3



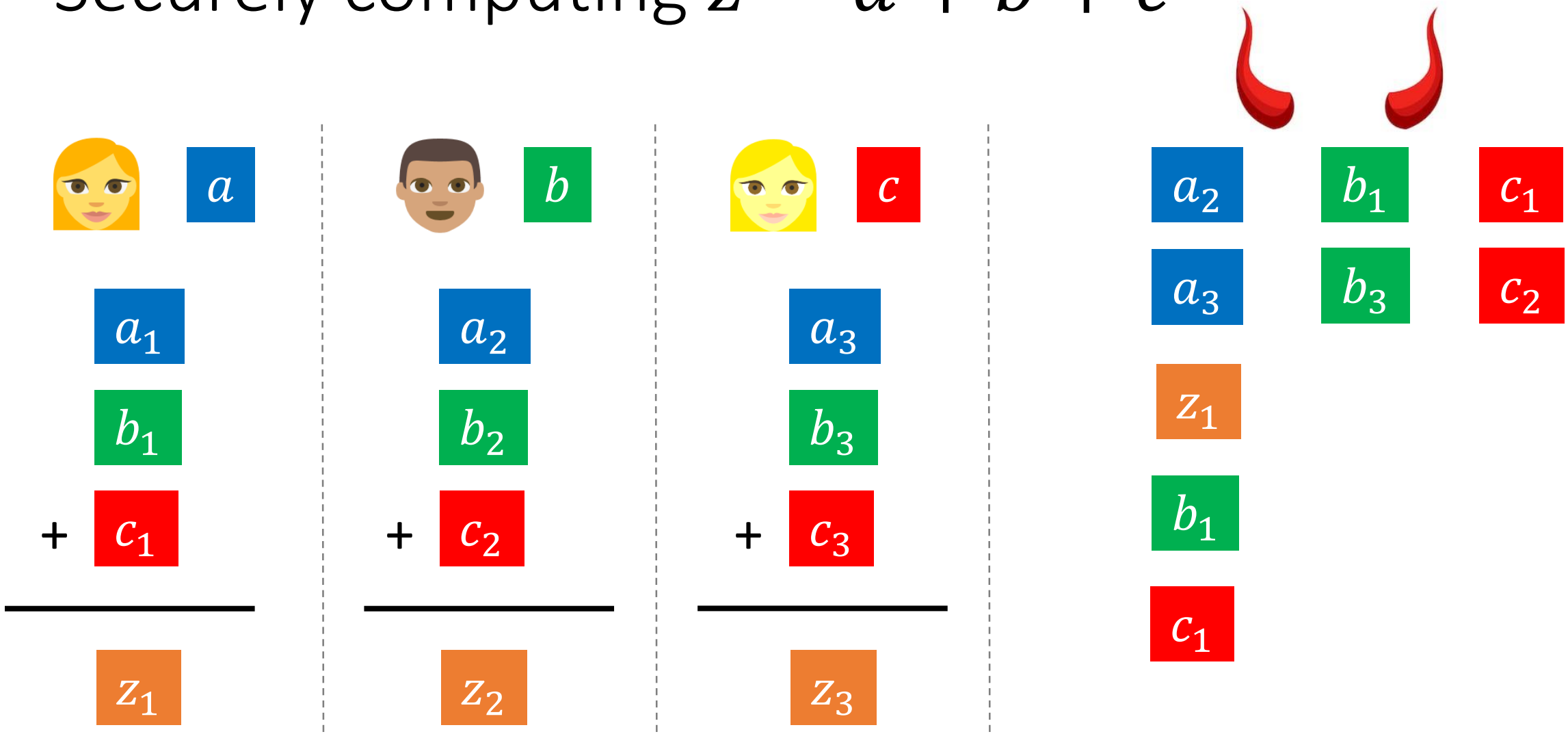
a_2 b_1 c_1

a_3 b_3 c_2

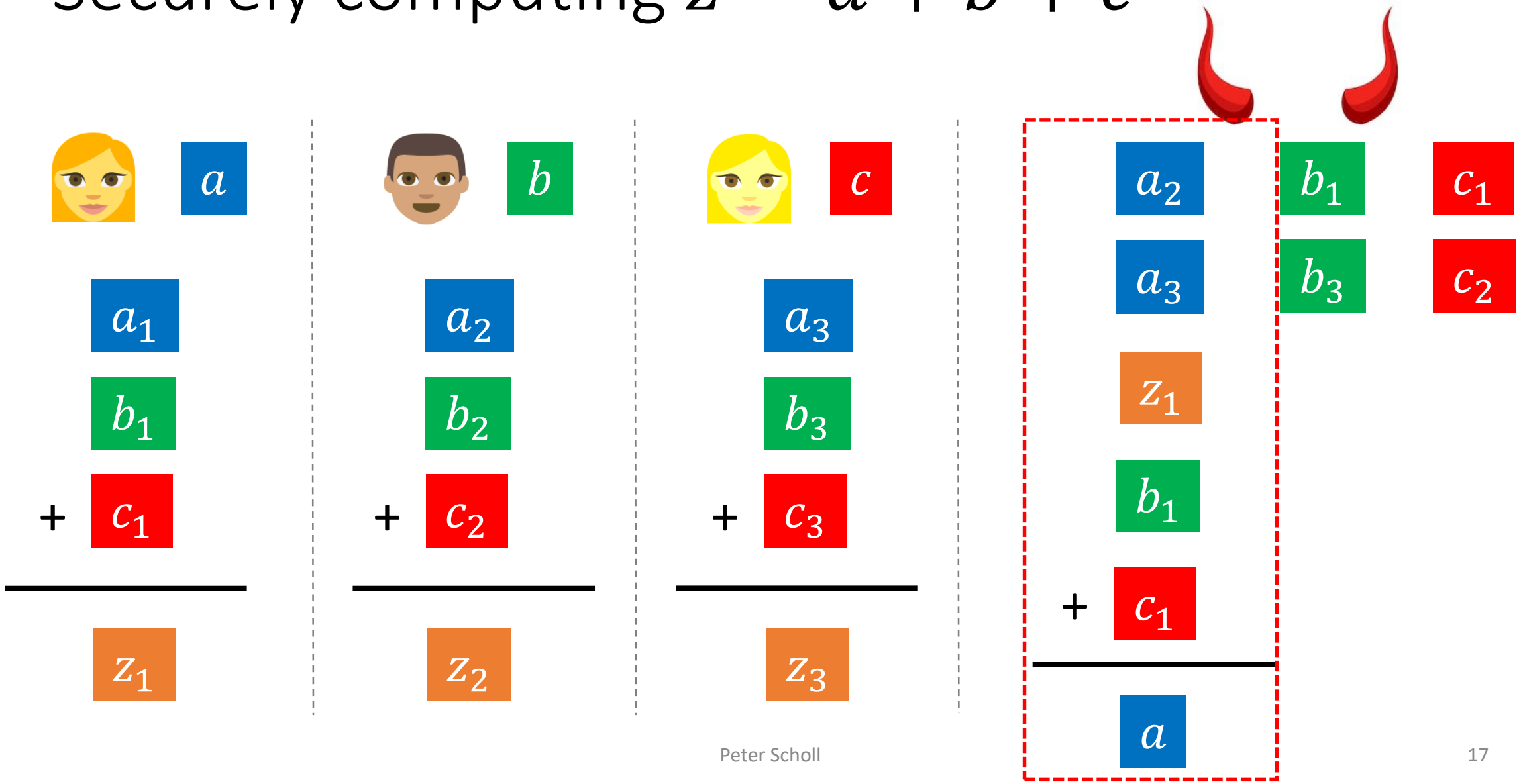
Securely computing $z = a + b + c$



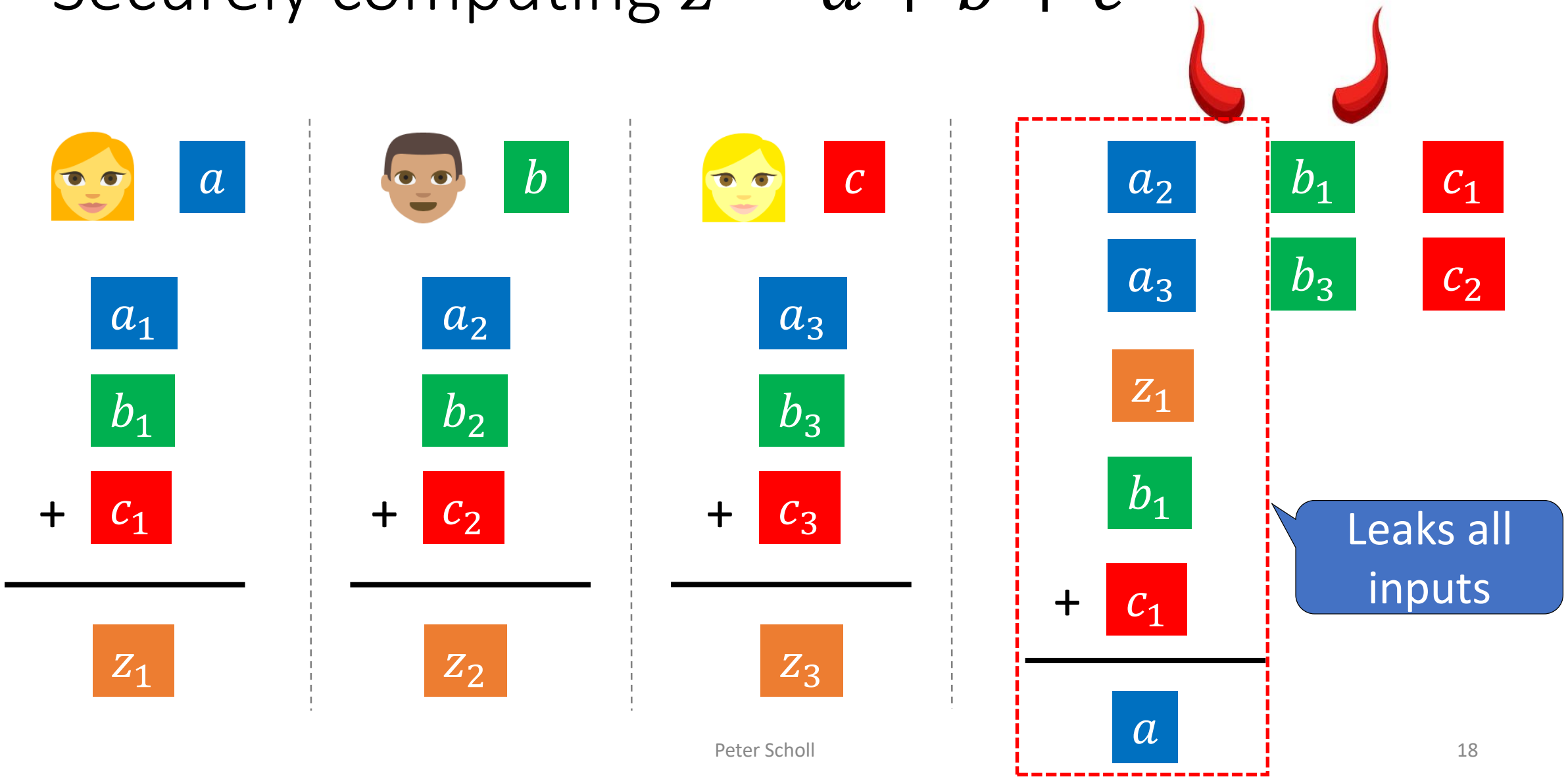
Securely computing $z = a + b + c$



Securely computing $z = a + b + c$



Securely computing $z = a + b + c$



Conclusion: use secure and authenticated channels in GMW

- In practice:
  - Hopefully real-world implementations do this already…
- In theory: [GMW 87], [CLOS 02] can still work with unencrypted channels
  - Secure for circuits where every output wire passes through an AND gate
  - Generic fix: AND every output wire with itself [Goldreich 17]
- A theoretical question:
  - For what functionalities does security with $t = n - 1 \Rightarrow$ security with $t < n$?

Thank you!

Acknowledgements:

- Thanks to Oded Goldreich, Yehuda Lindell and Claudio Orlandi for valuable discussions.

References:

[GMW 87] Goldreich, Micali, Wigderson. *How to Play Any Mental Game*

http://www.wisdom.weizmann.ac.il/~oded/X/gmw2a.pdf

[CLOS 02] Canetti, Lindell, Ostrovsky, Sahai. *Universally Composable Two-Party and Multi-Party Secure Computation*

https://eprint.iacr.org/2002/140.pdf

[Gol 04] Goldreich. *Foundations of Cryptography - Volume 2: Basic Applications*

[Gol 17] Goldreich. *List of Corrections for Foundations of Cryptography - Volume 2*

http://www.wisdom.weizmann.ac.il/~oded/foc-vol2.html