

# OLE extension *from* OT extension

Manoj Prabhakaran

*joint work with*

**Guru Vamsi Policharla**

**Rajeev Raghunath**

**Parjanya Vyas**

**IIT Bombay**

# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$

# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$




# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$



- **Optimal:**  $\Omega(n)$  string OTs necessary (no matter how long the strings are)


# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$
- 

```
graph LR; A["O(n) string OTs"] -- "perfect security" --> B["OLE over GF(2^n)"]
```

  - **Optimal:**  $\Omega(n)$  string OTs necessary (no matter how long the strings are)
- Gives OLE Extension

# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$
- 

The diagram consists of two blue rounded rectangular boxes. The left box contains the text "O(n) string OTs". An orange arrow points from this box to the right box, which contains the text "OLE over GF(2^n)". The text "perfect security" is written in black above the orange arrow.
- **Optimal:**  $\Omega(n)$  string OTs necessary (no matter how long the strings are)
- Gives OLE Extension
  - A few OLEs  $\rightarrow$  a few string OTs  $\rightarrow$  many string OTs  $\rightarrow$  many OLEs

# New Results for OLE over $\text{GF}(2^n)$

- Random OLE over  $\text{GF}(2^n)$ : Alice gets  $(a, t)$  & Bob gets  $(b, u)$  s.t.  $a+b = tu$



- **Optimal:**  $\Omega(n)$  string OTs necessary (no matter how long the strings are)
- Gives OLE Extension

- A few OLEs  $\rightarrow$  a few string OTs  $\rightarrow$  many string OTs  $\rightarrow$  many OLEs
- $\text{OT extension}$

# OLE over $\text{GF}(2^n)$ and $\mathbb{Z}_4$

- A bijection from  $\text{GF}(2^n) \times \text{GF}(2^n)$  to  $\mathbb{Z}_4^n$ :



# OLE over $\text{GF}(2^n)$ and $\mathbb{Z}_4$

- A bijection from  $\text{GF}(2^n) \times \text{GF}(2^n)$  to  $\mathbb{Z}_4^n$ :

$$\varphi(a, t) = f(a) + g(t)$$

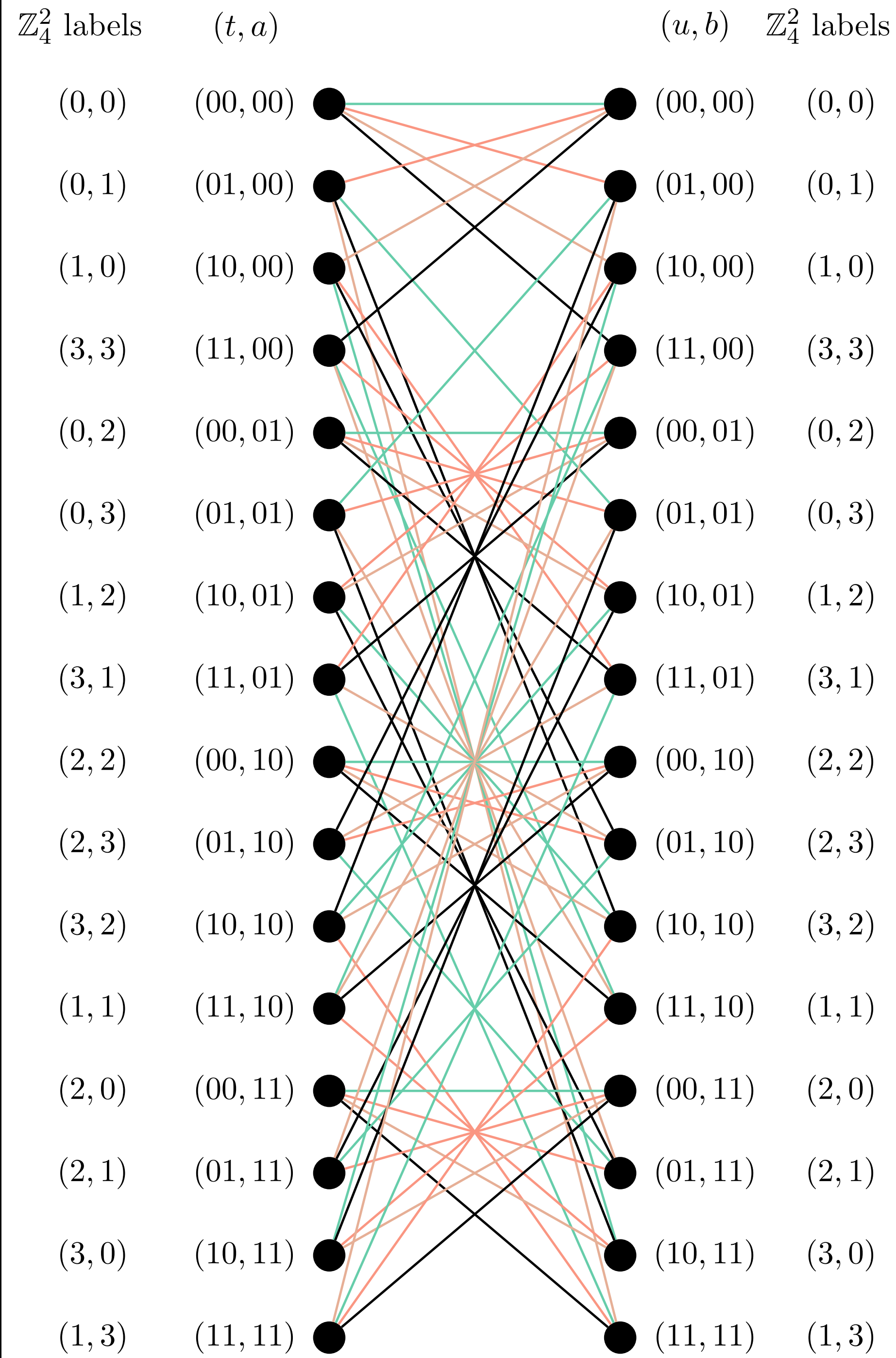
$$f, g : \text{GF}(2^n) \rightarrow \mathbb{Z}_4^n$$

$$f(x) = 2[\sqrt{x}]$$

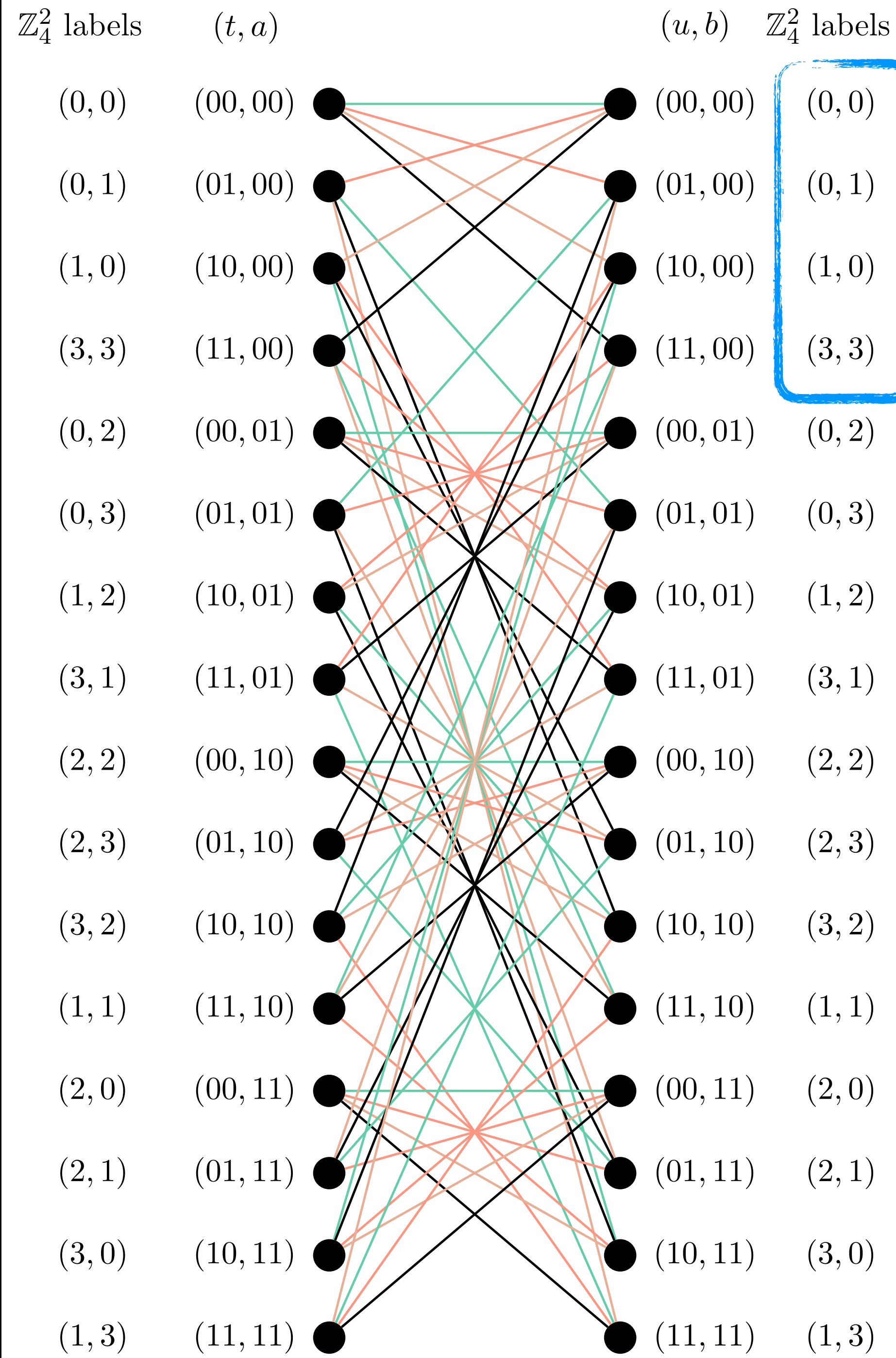
$$g(x) + g(y) - g(x+y) = f(xy)$$

$$a+b = tu \iff \varphi(a, t) + \varphi(b, u) \in S$$

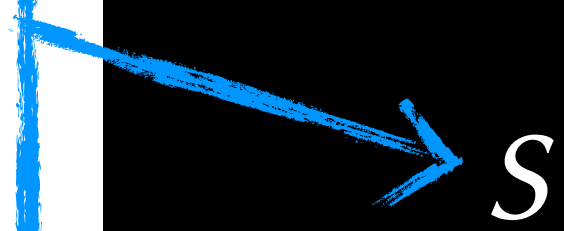
$$\text{where } S = \{ g(x) \mid x \in \text{GF}(2^n) \} \subseteq \mathbb{Z}_4^n$$




$$\alpha \sim \beta \iff \alpha + \beta \in S$$



$$\alpha \sim \beta \iff \alpha + \beta \in S$$



# New Results for OLE over $\text{GF}(2^n)$

- 

A diagram showing a blue rounded rectangle containing the text  $O(n)$  string OTs. An orange arrow points from this rectangle to another blue rounded rectangle containing the text OLE over  $\text{GF}(2^n)$ . The text "perfect security" is written in black on the orange arrow.
- **Optimal:**  $\Omega(n)$  string OTs necessary (no matter how long the strings are)
- Gives OLE Extension
  - A few OLEs  $\rightarrow$  a few string OTs  $\rightarrow$  many string OTs  $\rightarrow$  many OLEs

OT extension

**Group Correlations: This and more**  
**(Coming soon on eprint)**

# Bi-affine Correlations

- E.g., Bilinear correlations (like OT, OLE, vector OLE, Beaver's triples, ...)
- E.g., Alice gets  $(a_1, a_2)$ , Bob gets  $(b_1, b_2)$  s.t.  $a_1 + b_1 + a_2 + b_2 = 0$
- Generic 2-round protocols for random self-reduction, self-testing etc.

**Group Correlations: This and more**  
**(Coming soon on eprint)**