OLE extension *from* **OT** extension

Manoj Prabhakaran

joint work with
Guru Vamsi Policharla
Rajeev Raghunath
Parjanya Vyas

IIT Bombay

New Results for OLE over GF(2^n)

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

New Results for OLE over GF(2^n)

- Random OLE over GF(2^n): Alice gets (a, t) & Bob gets (b, u) s.t. $a+b = tu$
- O(n) string OTs → perfect security → OLE over GF(2^n)

New Results for OLE over GF(2^n)

- Random OLE over GF(2^n): Alice gets (a, t) & Bob gets (b, u) s.t. $a+b = tu$
- O(n) string OTs $\xrightarrow{\text{perfect security}}$ OLE over GF(2^n)
  - Optimal: $\Omega(n)$ string OTs necessary (no matter how long the strings are)

New Results for OLE over GF(2^n)

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

- Random OLE over GF(2^n): Alice gets (a, t) & Bob gets (b, u) s.t. $a+b = tu$
- O(n) string OTs $\xrightarrow{\text{perfect security}}$ OLE over GF(2^n)
  - Optimal: $\Omega(n)$ string OTs necessary (no matter how long the strings are)
- Gives OLE Extension
  - A few OLEs $\longrightarrow$ a few string OTs $\longrightarrow$ many string OTs $\longrightarrow$ many OLEs

New Results for OLE over GF(2^n)

- Random OLE over GF(2^n): Alice gets (a, t) & Bob gets (b, u) s.t. $a+b = tu$
- O(n) string OTs $\xrightarrow{\text{perfect security}}$ OLE over GF(2^n)
  - Optimal: $\Omega(n)$ string OTs necessary (no matter how long the strings are)
- Gives OLE Extension
  - A few OLEs $\longrightarrow$ a few string OTs $\longrightarrow$ many string OTs $\longrightarrow$ many OLEs

    OT extension

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

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

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

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

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

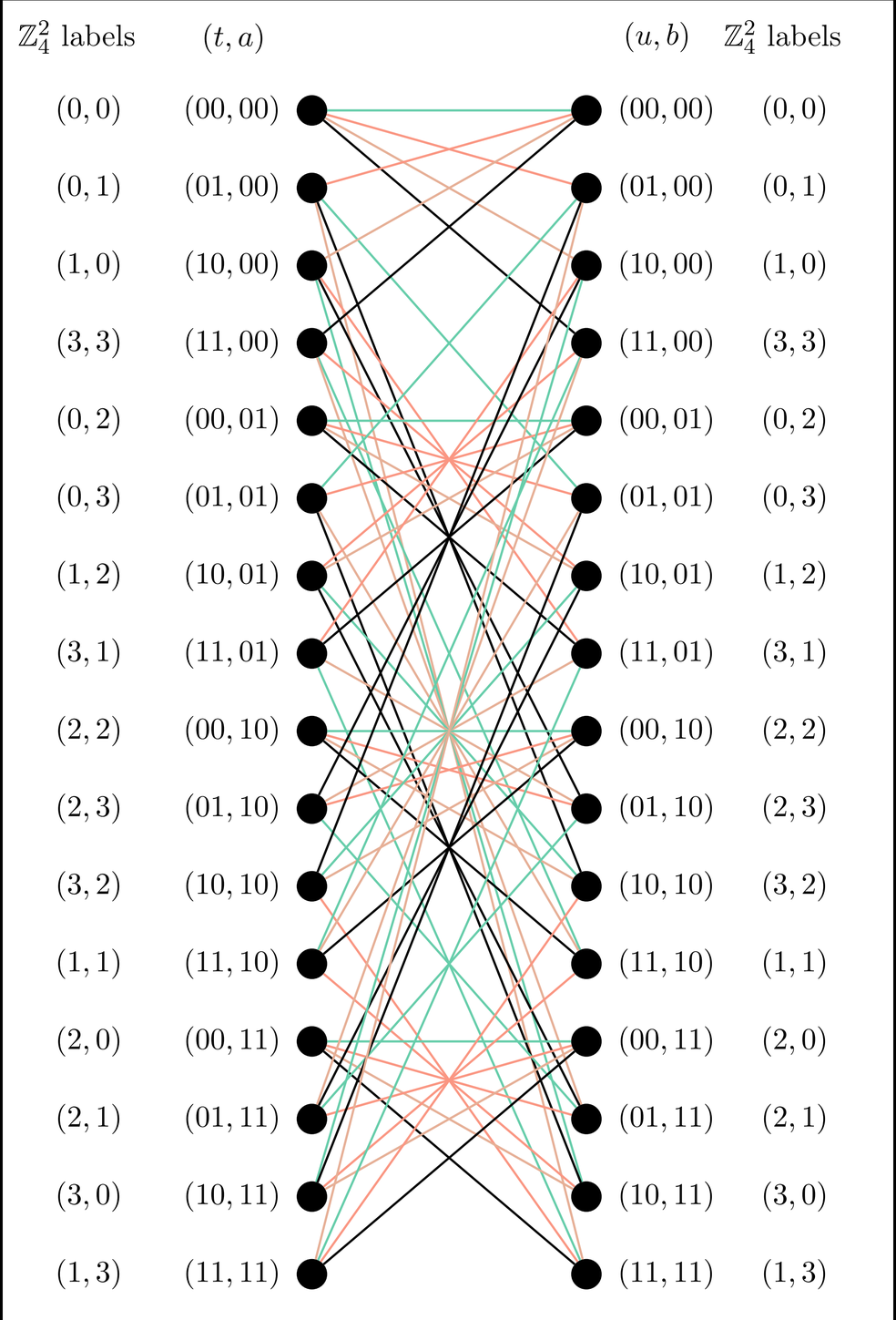
$$f, g : \mathrm{GF}(2^n) \longrightarrow \mathbb{Z}_4^n$$

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

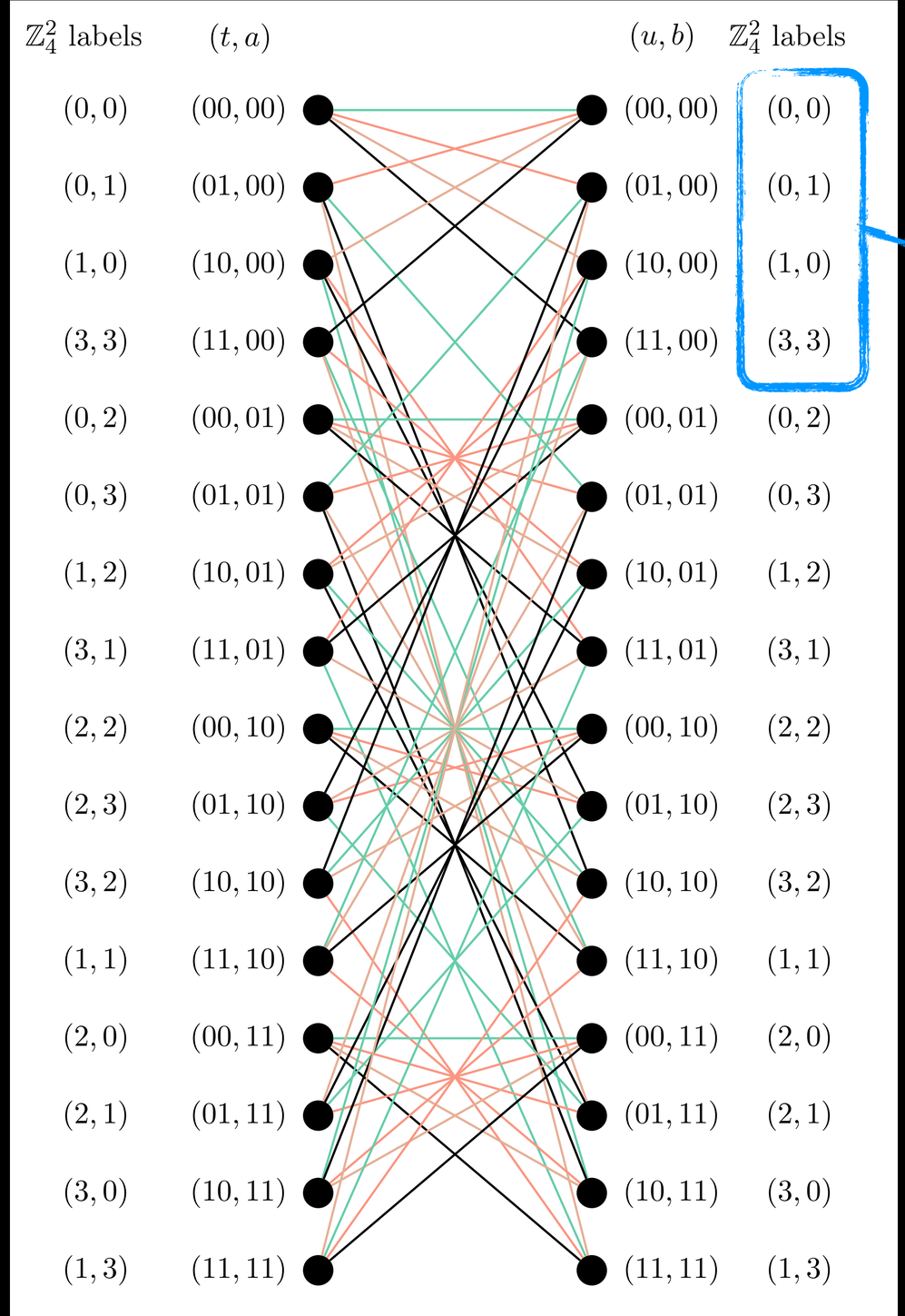
$$g(x) + g(y) - g(x+y) = f(xy)$$

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

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



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



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

S

New Results for OLE over GF(2^n)

- $O(n)$ string OTs $\xrightarrow{\text{perfect security}}$ OLE over GF(2^n)
  - Optimal: $\Omega(n)$ string OTs necessary (no matter how long the strings are)
- Gives OLE Extension
  - A few OLEs $\longrightarrow$ a few string OTs $\longrightarrow$ many string OTs $\longrightarrow$ 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)