OLE *extension* from **OT** *extension*

Manoj Prabhakaran

joint work with Guru Vamsi Policharla, Rajeev Raghunath, Parjanya Vyas

IIT Bombay

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

- A perfectly secure protocol to sample an OLE pair over $\mathrm{GF}(2^n)$ from $O(n)$ invocations of string OTs
  - Optimal: $\Omega(n)$ invocations 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

OLE and $\mathbb{Z}_4$

- Random OLE over GF(2^n)
  - Alice gets (a, t) & Bob gets (b, u) s.t. $a+b = tu$ (both operations in the field)
- A map from GF(2^n) × GF(2^n) to $\mathbb{Z}_4^n$:
  - A homomorphism f : GF(2^n)$\longrightarrow \mathbb{Z}_4^n$: $f(x) = 2[\sqrt{x}\,]$
  - Another function g : GF(2^n) $\longrightarrow \mathbb{Z}_4^n$ s.t. $g(x) + g(y) - g(x+y) = f(xy)$
  - $\varphi(a,t) = f(a) + g(t)$
  - $a+b = tu$ iff $\varphi(a,t) + \varphi(b,u) \in S$, where $S = \{\, g(x) \mid x \in \mathrm{GF}(2^n) \,\} \subseteq \mathbb{Z}_4^n$

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

- A perfectly secure protocol to sample an OLE pair over $\mathrm{GF}(2^n)$ from $O(n)$ invocations of string OTs
  - Optimal: $\Omega(n)$ invocations 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

Group Correlations: This and more

(Coming soon on eprint)