Laconic Function Evaluation for Turing Machines

Nico Döttling[*], **Phillip Gajland**[†,‡], **Giulio Malavolta**[‡]

[*] CISPA Helmoltz Center for Information Security

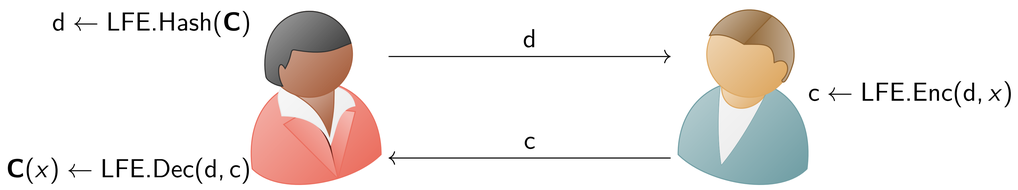
[†] Ruhr University Bochum

[‡] Max Planck Institute for Security and Privacy

CASA
Cyber Security in the Age of Large-Scale Adversaries

Laconic Function Evaluation [1]

Laconic function evaluation (LFE) **is a powerful cryptographic primitive recently introduced. Alice can compress a large circuit C into a small digest** d**. Bob can encrypt some input** x **under** d **in a way that enables Alice to recover** $\mathbf{C}(x)$ **without learning anything about** x**. The scheme is said to be laconic if the size of** d**, the run-time of the encryption algorithm** $\mathsf{LFE.Enc}$ **and the size of the ciphertext** c **are all much smaller than the size of C.**



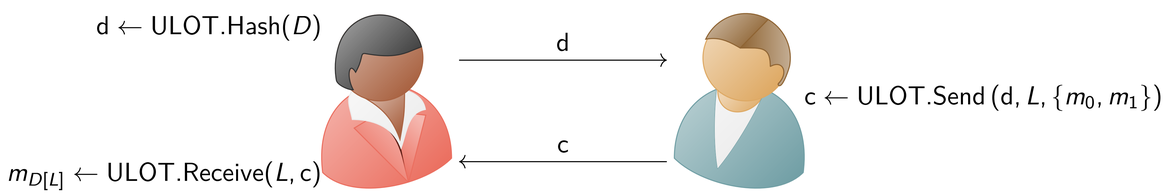
Indistinguishability Obfuscation [2, 3]

Two circuits are said to be functionally equivalent if they return the same result when evaluated on the same input. Given two functionally equivalent circuits, their obfuscations are computationally indistinguishable.

$$\boxed{\mathbf{C}_0(x)} \quad = \quad \boxed{\mathbf{C}_1(x)} \quad \Longrightarrow \quad \boxed{i\mathcal{O}(\mathbf{C}_0)(x)} \quad \approx \quad \boxed{i\mathcal{O}(\mathbf{C}_1)(x)}$$

Updatable Laconic Oblivious Transfer [4]

Updatable Laconic Oblivious Transfer (ULOT) **allows Alice to commit to a large database** D **via a short message** d**. Subsequently, a single short ciphertext** c **from Bob allows Alice to learn** $m_{D[L]}$**, where the messages** m_0**,** m_1 **and the location** $L \in [|D|]$ **are dynamically chosen by Bob.**

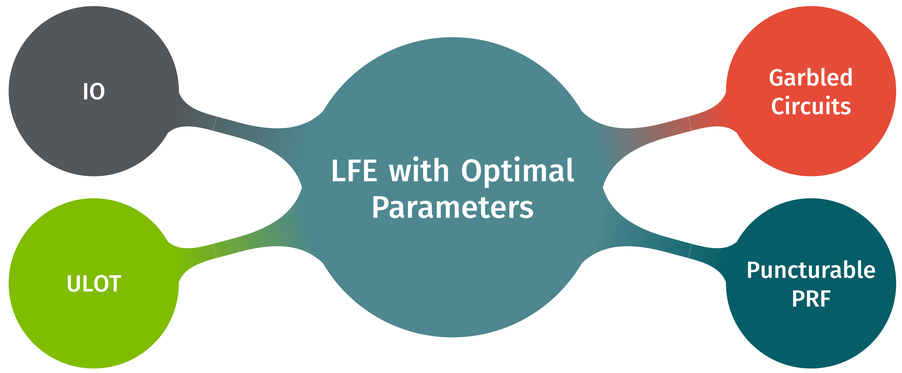


LFE with Optimal Parameters

We construct an LFE scheme with asymptotically optimal parameters. I.e. the size of Bob's message is $|x| + \mathsf{poly}(\lambda)$**, where** x **is Bob's input. Note that, unlike [1], for our construction the size of the Bob's message does not depend on the depth of the circuit used for evaluation.**

Applications

- **Reverse Delegation [5]**
- **NIZK with Optimal Prover Complexity**
- **Bob-optimised 2PC**



$\mathsf{LFE.Enc}(\mathsf{d}, x)$

1 : **Obfuscate Step Circuit** SC **as**

$i\mathcal{O}(\mathsf{SC}) \leftarrow$ **Step Circuit**

1 : **Perform 1 step of the computation**

2 : **Write outputs to DB using** $\mathsf{ULOT.Send}$

2 : **Encrypt input** x

3 : **Return** $i\mathcal{O}(\mathsf{SC})$ **and encrypted** x

$\mathsf{LFE.Dec}(\mathsf{d}, \mathsf{c})$

1 : **Compute obfuscated Step Circuit at** i

2 : $\mathsf{ULOT.Receive}$ **returns the inputs for** $i\mathcal{O}(\mathsf{SC}_{i+1})$

3 : **Return final output from Step Circuit**

References

[1] Willy Quach, Hoeteck Wee, Daniel Wichs. *Laconic Function Evaluation and Applications*. FOCS, 2018.

[2] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, Ke Yang. *On the (Im)possibility of Obfuscating Programs*. CRYPTO, 2001.

[3] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters. *Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits*. FOCS, 2013.

[4] Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, Antigoni Polychroniadou. *Laconic Oblivious Transfer and Its Applications*. CRYPTO, 2017.

[5] Nico Döttling and Sanjam Garg and Vipul Goyal and Giulio Malavolta. *Laconic Conditional Disclosure of Secrets and Applications*. FOCS, 2019.

RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HGI Horst Görtz Institut