CR15: Advanced topics in cryptography
Functional Encryption

Teacher: Alain Passelègue   Scribe: Fabrice Lécuyer

December 17th 2019

1 Definitions

1.1 Universal Circuits

Just like there exists a universal Turing machine that can emulate any other machine, Valiant proved in 1976 that there exist universal circuits. The universal Turing machine $\mathcal{U}$ is defined so that $\forall \mathcal{M}$ Turing machine and $\forall x$ input for $\mathcal{M}$, there is a binary description $d(\mathcal{M})$ such that $\mathcal{U}(d(\mathcal{M}), x) = \mathcal{M}(x)$. Now we want to similarly define a universal circuit.

Definition 1. *Let $\mathcal{C}(s, n)$ be the class of Boolean circuits with binary description of size s and input of size n. We note $c_f : \{0,1\}^n \to \{0,1\}$ the circuit described by the bit-string $f_1 \dots f_s \in \{0,1\}^s$.*

Definition 2. *A **Universal Circuit** is an infinite family $u = (u_{s,n})_{s \in \{0,1\}^*, n \in \{0,1\}^*}$ of circuits such that $\forall s \in \mathbb{N}, \forall n \in \mathbb{N}, \forall f \in \{0,1\}^s, \forall x \in \{0,1\}^n$, we have $u_{s,n}(f_1, \dots, f_s, x_1, \dots, x_n) = c_f(x)$.*

Remark: Valiant provided an algorithm to generate $u_{s,n}$ efficiently for any given s and n.

1.2 Public key functional encryption

Definition 3. *A **Public-key functional encryption scheme** for a class of functions $\mathcal{F}$ consists in 4 PPT algorithms (Setup, Keygen, Enc, Dec) such that:*

- $Setup(1^\lambda) = msk, mpk$
- $Keygen(msk, f \in \mathcal{F}) = sk_f$
- $Enc(mpk, m) = ct$
- $Dec(sk_f, ct) = m'$

Its correctness is given by $\forall (msk, mpk) = Setup(1^\lambda), \forall f \in \mathcal{F}, \forall m, Dec(Keygen(msk, f), Enc(mpk, m)) = f(m)$.

All the topics we have studied so far are instances of functional encryption: symmetric encryption, public key encryption, identity or attribute-based encryption...

- Symmetric and public-key encryption: $f = Identity$.
- IBE: $m = (id, m')$ and $f_{id}(id', m') = \begin{cases} m' & \text{if } id = id' \\ \perp & \text{otherwise.} \end{cases}$
- ABE: $m = (A, m')$ and $f_P(A, m') = \begin{cases} m' & \text{if } P(A) = 1 \\ \perp & \text{otherwise.} \end{cases}$

There are many definitions for **security**:

- adversary sends messages m_0, m_1 to challenger.

- challenger sends mpk and $Enc(mpk, m_b)$ after choosing $b \in \{0, 1\}$.
- adversary sends $f \in \mathcal{F}$ such that $f(m_0) = f(m_1)$.
- challenger sends sk_f.
- adversary outputs b' and wins if $b' = b$.

This is selective 1-key security, but the adversary could ask for several secret keys for different functions $f_1, \ldots, f_q$ with $f_i(m_0) = f_i(m_1)$: this is multiple-keys security.

2 Garbled circuits

2.1 Definition

Definition 4. *A* ***Garbling scheme*** *is a pair of PPT algorithms:*

- $Garble\Big(1^\lambda, c : \{0,1\}^n \leftarrow \{0,1\} \text{ circuit}\Big) = \tilde{c}, \Big\{\ell_{i,b}\Big\}_{i \in [1,n], b \in \{0,1\}}$ *labels.*
- $Eval(\tilde{c}, \{\ell_{i,x_i}\}) = b \in \{0,1\}, x \in \{0,1\}^n$.

The scheme is correct when $\forall c, \forall x, Eval(\tilde{c}, \{\ell_{i,x_i}\}) = c(x)$.

Security is obtained when minimum information is given about c and x while outputting $c(x)$. For a pair $(\tilde{c}, \{\ell_{i,x_i}\})$ given by $Garble$, we want a PPT simulator $Sim(1^\lambda, c, c(x)) \simeq_c (\tilde{c}, \{\ell_{i,x_i}\})$. For simplicity, we usually assume that c is public so Sim has it as an input. If this simulation is possible, it means that $(\tilde{c}, \ell)$ does not give more information.

2.2 Construction

Without loss of generality, we assume that circuits are made of gates with two inputs and one output ($fanin2 - fanout1$).

Definition 5. *A* ***circuit*** *is a set of wires $W = \{w_i\}$ and gates $G = \{g_i\}$ positioned on a graph defined by tuples (w_i, w_j, g_k, w_ℓ) when gate g_k has inputs w_i, w_j and output w_ℓ.*

Let (Gen, Enc, Dec) denote a secret-key encryption scheme. For every wire $w_i \in W$, we generate two secret keys k_i^0, k_i^1 with $Gen(1^\lambda)$. Then for a gate (w_i, w_j, g_k, w_ℓ) we compute and shuffle four encryptions:

$$\Big\{\tilde{g}_k = Enc\big(k_i^a, Enc(k_j^b, 0^\lambda \cdot k_\ell^{g_k(a,b)}\big)\Big\}_{a,b \in \{0,1\}}$$

The output is $\tilde{c} = \Big(\{\tilde{g}_k\}, k_{out}^0 \rightarrow 0, k_{out}^1 \rightarrow 1\Big)$, labels $\Big\{k_{in}^b\Big\}$. Out of four outputs, only one can be deciphered given the two input labels.

Proof. A formal security proof would require a hybrid proof with one step for each gate and each ciphertext. We want $Sim(1^\lambda, c, c(x)) \simeq_c (\tilde{c}, \{\ell_{i,x_i}\}$. Define Sim as follows:

- compute a garbling of c with minor tweak: $\forall w_i \in W$, mick $k_i^b = Gen(1^\lambda$ and $\forall (w_i, w_j, g_k, w_\ell)$, output arbitrary $\tilde{g}_k = Enc\big(k_i^a, Enc(k_j^b, 0^\lambda \cdot k_i^0)\big), k_{out}^0 = c(x), k_{out}^1 = 1 - c(x)$.
- for $\frac{3}{4}$ of ciphertexts, there is at least one missing key in each gate to decrypt, so the SE security guarantees that $Enc_{k_1} \circ Enc_{k_2}(0^\lambda \cdot m) \simeq Enc_{k_1} \circ Enc_{k_2}(0^\lambda \cdot 0^\lambda)$ as long as k_1 or k_2 is unknown.

$\square$

3 Functional Encryption

With universal and garbled circuits, we construct functional encryption for the class of circuits $\mathcal{C}(s, n)$. Let $PKE^* = (Gen^*, Enc^*, Dec^*)$ a PKE-scheme. FE is defined by:

- $Setup(1^\lambda)$ generates (pk_i^b, sk_i^b) with Gen^* for all $i \in [1, s], b \in \{0, 1\}$ and outputs $mpk = \{pk_i^b\}, msk = \{sk_i^b\}$.
- $Keygen(msk, c_f) = \{sk_i^{f_i}\} = sk_f$.
- $Enc(mpk, m)$ takes a universal circuit $\mathcal{U} : \{0, 1\}^s \times \{0, 1\}^n \to \{0, 1\}$ and computes $(\tilde{\mathcal{U}}, \{\ell_{i,b}\} = Garble(1^\lambda, \mathcal{U})$ as well as $ct_i^b = Enc(pk_i^b, l_{i,b})$. It outputs the set $(\tilde{\mathcal{U}}, \{ct_i^b\}, \{\ell_{i+s,m_i}\})$.
- $Dec(sk_f, ct)$ recovers $\{\ell_{i,f_i}\}$ and $Eval(\tilde{\mathcal{U}}, \{\ell_{i,f_i}\}, \{\ell_{i+s,m_i}\})$.

Proof. Correctness follows from the correctness of PKE and garbling. □

Proof. 1-key security requires $Enc(mpk, m_0) \simeq_c Enc(mpk, m_1)$ if $f(m_0) = f(m_1)$ given sk. The only difference between the two encryptions is in the set $\{\ell_{i+s,m_i}\}$. Security of garbling proves that $(\tilde{c}, \{\ell_{i,x_i}\}) \simeq_c Sim(1^\lambda, c, c(x))$. □