Private constrained pseudorandom functions with succinct keys

Pedro Capitão

Instituto Superior Técnico
Universidade de Lisboa

22 February 2021

Introduction

Pseudorandom functions (PRFs) are deterministic functions that are indistinguishable from random functions. They have many applications in cryptography.

In a **constrained PRF**, the owner can delegate constrained keys which only allow computing the value of the function at points that satisfy a given constraint.

Private constrained PRFs require that constrained keys do not reveal the corresponding constraints. Applications of private constrained PRFs include watermarking PRFs and private constrained MACs.

Pseudorandom functions: syntax

A pseudorandom function scheme consists of two algorithms:

- KeyGen(1^λ) : Probabilistic algorithm that generates a key K.
- Eval(K, x) : Deterministic algorithm that outputs a value y.

A PRF is said to be secure if it is pseudorandom (its outputs are indistinguishable from those of a random function). This notion is defined in terms of a game between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$ (probabilistic polynomial time algorithm).

For each $\lambda \in \mathbb{N}$, let $\text{Eval}(K, \cdot) : X_\lambda \to Y_\lambda$ for all $K \leftarrow \text{KeyGen}(1^\lambda)$.

Pseudorandom functions: security

1. $\mathscr{C}$ randomly chooses $b \leftarrow \{0,1\}$.
   - If $b = 0$: $\mathscr{C}$ generates $K \leftarrow \mathsf{KeyGen}(1^\lambda)$.
   - If $b = 1$: $\mathscr{C}$ chooses uniformly a function $f : X_\lambda \to Y_\lambda$.
2. $\mathscr{A}$ can make queries as many times as desired, each time choosing a point $x \in X_\lambda$ and sending it to $\mathscr{C}$.
   - If $b = 0$: $\mathscr{C}$ replies with $y = \mathsf{Eval}(K, x)$.
   - If $b = 1$: $\mathscr{C}$ replies with $y = f(x)$.
3. Finally, $\mathscr{A}$ outputs a guess $b' \in \{0,1\}$.

$\mathscr{A}$ wins the game if $b = b'$.
We say that the PRF is secure if, for any adversary $\mathscr{A}$ and any positive polynomial $p(\cdot)$,

$$\Pr[b = b'] - \frac{1}{2} < \frac{1}{p(\lambda)}$$

for sufficiently large λ.

Lattice-based cryptography

- **Classical cryptography:** Security is commonly based on number-theoretic problems such as factorization and discrete logarithm, that can be solved by quantum computers (e.g. Shor's algorithm).
- **Post-quantum cryptography:** Based on problems that are hard for both classical and quantum algorithms. Lattice cryptography uses conjectured hard problems on lattices in $\mathbb{R}^n$ as a basis for cryptographic protocols.

Given $n, m, q \in \mathbb{N}$ and an error distribution χ over $\mathbb{Z}$, the decisional learning with errors (LWE) problem is to distinguish the distributions

$$(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T) \text{ and } (\mathbf{A}, \mathbf{u}^T),$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{u} \leftarrow \mathbb{Z}_q^m$ and $\mathbf{e} \leftarrow \chi^m$.

A pseudorandom function from LWE

PRF scheme by Boneh, Lewi, Montgomery, Raghunathan (2013):

- Public parameters: $\mathbf{A}_0, \mathbf{A}_1 \leftarrow \{0,1\}^{m \times m}$.
- Secret key: $\mathbf{s} \leftarrow \mathbb{Z}_q^m$.
- Function value: On input $x \in \{0,1\}^z$, output

$$\mathrm{Eval}(\mathbf{s}, x) = \left\lfloor \mathbf{s}^T \cdot \prod_{i=1}^{z} \mathbf{A}_{x_i} \right\rceil_p,$$

where the rounding function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ is defined for $p < q$ by $\lfloor y \rceil_p = \lfloor y \cdot p/q \rceil$.

ABE and Constrained PRFs

Attribute-based encryption:

- Setup$(1^\lambda) \to$ (mpk, msk)
- Enc(mpk,$x, \mu) \to c$
- Constrain(msk,f) $\to \mathsf{sk}_f$
- Dec(sk_f, c) $\to \mu$

A constrained key sk_f allows one to decrypt c associated to x iff x satisfies f.

Constrained PRF:

- KeyGen$(1^\lambda) \to$ msk
- Eval(msk,x) $\to y$
- Constrain(msk,f) $\to \mathsf{sk}_f$
- ConstrainEval(sk_f, x) $\to y$

A constrained key sk_f allows one to evaluate the PRF at x iff x satisfies f.

Constraints are usually circuits $f : \{0,1\}^z \to \{0,1\}$, in binary representation: $f = (f_1, \ldots, f_\ell) \in \{0,1\}^\ell$.
We say that an ABE or CPRF has *succinct keys* if the size of sk_f is independent of the circuit size ℓ.

A technique to shorten constrained keys

Constrained PRF of Brakerski and Vaikuntanathan (2015):

Original scheme:
The constrained key sk_f for a constraint $f \in \{0,1\}^\ell$ consists of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_\ell$ where ℓ is the size of f.

Succinct keys variant:

- KeyGen(1^λ): Encrypt with ABE the vectors $\mathbf{b}_i$ for all possible constraints and publish them in the public parameters.
- Constrain(msk,f): Output as sk_f an ABE constrained key for a constraint Φ_f which only allows decryption of the components corresponding to f.
- ConstrainEval(sk_f, x): Using sk_f decrypt the relevant components $\mathbf{b}_1, \ldots, \mathbf{b}_\ell$. Compute y as in the original scheme.

Succinct keys for private constrained PRFs

The main objective of my thesis is to present a construction of a private constrained PRF scheme with succinct keys, based on the private constrained PRF of Brakerski et al. (2017).

We can apply the technique we just saw to make the keys of this scheme succinct.

Problem: The ABE key for Φ_f reveals Φ_f, which reveals f. Hence the constraints are no longer private.

Succinct keys for private constrained PRFs

Candidate approach: Instead of using ABE, use function-hiding predicate encryption (FHPE), which can be achieved from LWE (in the symmetric key setting).

Key size: The FHPE scheme does not have succinct keys. However, we can divide a constrained key for f into two parts:

- A constrained key for an underlying predicate encryption scheme, which is independent of the size of f. We send it as the constrained key.
- A symmetric key encryption of f. We add it to the public parameters.

References

- C. Peikert. *A decade of lattice cryptography* (2016).
- D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan. *Key homomorphic PRFs and their applications* (2013).
- Z. Brakerski and V. Vaikuntanathan. *Constrained key-homomorphic PRFs from standard lattice assumptions* (2015).
- Z. Brakerski, R. Tsabary, V. Vaikuntanathan, and H. Wee. *Private constrained PRFs (and more) from LWE* (2017).