Cryptographic Protocols

Spring 2017

Part 3

Distinguishing Advantage

Setting: Random variables X and Y, distributions P_X and P_Y

Distinguisher

- Algorithm A to distinguish X from Y
- Goal: on input $x \leftarrow X$, output „X“; on input $y \leftarrow Y$, output „Y“

Advantage: $\Delta_A(X,Y) := \left|\Pr_X[A(x) = \text{„X“}] - \Pr_Y[A(y) = \text{„X“}]\right|$

Asymptotics

- Families of random variables $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$
- $\Delta_A(X_n,Y_n) := \left|\Pr_{X_n}[A(x) = \text{„X“}] - \Pr_{Y_n}[A(y) = \text{„X“}]\right|$

Indistinguishability Levels

- Perfect: $P_X = P_Y$, i.e. $\forall A : \Delta_A(X_n,Y_n) = 0$
- Statistical: $\forall A : \Delta_A(X_n,Y_n) =$ negligible in n
- Computational: $\forall$ polytime $A : \Delta_A(X_n,Y_n) =$ negligible in n

Proofs of Knowledge

Let $Q(\cdot,\cdot)$ be a binary predicate and let a string z be given. Consider the problem of proving knowledge of a secret x such that $Q(z,x) =$ true.

Definition: A protocol (P,V) is a **proof of knowledge for $Q(\cdot,\cdot)$** if there exists an efficient program (knowledge extractor) K, which can interact with any program P' for which V accepts with noticeable (also called non-negligible) probability, and outputs a valid secret x.

Note: K can rewind P' (restart with same randomness).

2-Extractability

Definition: A three-move protocol (round) with challenge space C is **2-extractable** if from any two triples (t,c,r) and (t,c',r') with $c \neq c'$ accepted by V one can efficiently compute an x with $Q(z,x) =$ true.

Theorem: An interactive protocol consisting of s 2-extractable rounds with challenge space C is a proof of knowledge $Q(\cdot,\cdot)$ if $1/|C|^s$ is negligible.

Proof: Knowledge extractor K:

1. Choose randomness for P' and execute the protocol between P' and V.
2. Execute the protocol again (same randomness for P').

3a. If V accepts in both executions, identify first round with different challenges c and c' (but same t). Use 2-extractability to compute an x, and output it (and stop).

3b. Otherwise, go back to Step 1.

Witness Hiding POKs

Definition: A POK (P,V) is **witness-hiding (WH)** if there exists no efficient algorithm which, after interacting arbitrarily with P (possibly in many protocol instantiations), can make V accept with non-negligible probability.

For predicate $Q(\cdot,\cdot)$ and value z, let $\mathcal{W}_z = \{x : Q(z,x) = \text{true}\}$ be the set of witnesses for z. Consider a setting where $|\mathcal{W}_z| \geq 1$.

Definition: A POK (P,V) is **witness-independent (WI)** if for any verifier V' the transcript is independent of which witness the prover is using in the proof.

Theorem: If one can generate a pair (x,z) with x uniform in $\mathcal{W}_z$ and it is computationally infeasible to find a triple (z,x,x') with $x \neq x'$ and $x,x' \in \mathcal{W}_z$, then every witness-independent POK for $Q(\cdot,\cdot)$ is witness-hiding.