Michael Forbes
mforbes@illinois.edu

2018-03-12.4 → 2018-03-14.1
2018-03-14.2 ←
CS 579

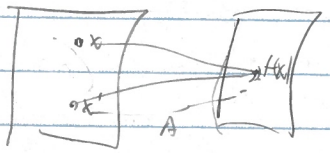
CS 579: Computational Complexity Lecture 17 57

today: OWF ⇒ ...

Zero knowledge

def: $f: \{0,1\}^* \to \{0,1\}^*$ is a one-way function (OWF) if
- easy to compute: $f \in FP$
- hard to invert: all probabilistic poly-time A

$$\Pr_{x \in \{0,1\}^n}\left[A(f(x)) \in f^{-1}(f(x)) \right] \le \text{negl}(n) = \frac{1}{n^{\omega(1)}}$$



eg: Scrambling an egg

Multiplying integer

lem: $P = NP \Rightarrow$ no OWF

Pf: $L = \{(w, y, 1^n) : \exists z \text{ s.t. } f(wz) = y \ |wz| = n\}$

$y = f(x) \Rightarrow (\lambda, y, |x|) \in L$

given $(w, y, |x|) \in L \Rightarrow (w0, y, |x|) \in L$ or $(w1, y, |x|) \in L$

$w < |x| \Rightarrow (w', y, |x|) \in L, |w'| = |w|+1$

$\Rightarrow (w'', y, |x|) \in L \quad |w''| = |x|$

$\Rightarrow f(w'') = y$

} $|x|$ steps

Q - what is randomness?

A: uniform distribution U_n on $\{0,1\}^n$

A: distribution "close" to U_n $\quad \Delta(D, U_n) \in$ small

$\Delta_{poly(n)}(D, U_n) \in$ small

E: cryptographic looking random to adversary sufficient

def: $G: \{0,1\}^* \to \{0,1\}^*$, $\ell: \mathbb{N} \to \mathbb{N}$ length function s.t. $\ell(n) > n$, $\forall n$

G is a cryptographic pseudorandom generator - stretch $\ell(n)$ if
- $x \in \{0,1\}^n \to |G(x)| = \ell(n)$
- G runs in deterministic polynomial time
- for every non-uniform polynomial algo A

$$\left| \Pr[A(G(U_n)) = 1] - \Pr[A(U_{\ell(n)}) = 1] \right| < \varepsilon(n)$$

Michael Farbes
msfarbes@illinois.edu
2016-03-14.2 ← 2016-03-14.1
→ 2016-03-14.3
CS579

Thm [HILL]: if OWF exist, $\exists$ cryptographic PRG w/ stretch $\ell(n) = n^c$

Ideas: define notion of "looks" "weakly random" computationally

eg: $p \in [0,1]$ $X_p = \begin{cases} 1 & w/p\ p \\ 0 & 1-p \end{cases}$

truly random $p = Y_2$

weakly random $0 << p << Y_2$

show any OWF looks weakly random

extractor ↗ to pure randomness ← more randomness

eg: $X_p \oplus X_p = \begin{cases} 1 & w/p\ 2p(1-p) \geq 2p >> p \\ 0 & 1- \text{ " } \end{cases}$

Cor: PRG $\Rightarrow$ encryption w/ short seeds

Pf: $Enc(x, k) = x \oplus \underbrace{G(k)}_{\approx U_{\ell(k)}}$

$\uparrow$ $k \in \{0,1\}^k$

$\in \{0,1\}^{\ell(k)}$

$Dec(y, k) = y \oplus G(k)$

$\Rightarrow Dec(Enc(x,k),k) = x$

security: suppose $x_1, x_2 \in \{0,1\}^{\ell(k)}$

want: $Enc(x_1, k) \approx Enc(x_2, k)$

$x_1 \oplus G(k)$ $x_2 \oplus G(k)$

But: any polynomial p

$$\Delta_{p(k)}(G(k), U_{\ell(k)}) \leq negl(k)$$

is $$|Pr[A(G(k)) = 1] - Pr[A(U_{\ell(k)}) = 1]| \leq negl(k)$$

want $$|Pr[\underbrace{A(x_1 \oplus G(k))}_{= A'_{x_1}(G(k))} = 1] - Pr[\underbrace{A(x_1 \oplus U_{\ell(k)})}_{A'_{x_1}(U_{\ell(k)})} = 1]| \leq negl(n)$$

use nonuniformity →

$\Rightarrow Enc(x_1, k) \approx$ uniform $\approx Enc(x_2, k)$ ∎

Q: do we need to know c s.t. $n \to n^c$ in advance?

Michael Fowles
mikebes@illinois.edu

2018-03-14.2 ⟶
2018-03-14.4 ⟵ 2018-03-14.3
CS574

Zero knowledge

mikebes —username=mikebes, password=pseudorandomness 1→ illinois.edu

Eve

Eve —username=mikebes, pass=" → illinois.edu

Q: Can authenticate w/o replay attacks?

real life: raw passwords not stored

hashed passwords are
↳ $h(\text{pseudorandom } 1)$

salted " $h(\text{NaCl pseudorandom } 1)$

leaking database does not allow impersonation

BUT replay still possible

idea:

mikebes —$K_2Cr_2O_7$→ illinois.edu
illinois.edu: $h(\text{NaCl pseudorandom } 1) = y$
$z = h(K_2Cr_2O_7\, y)$

random, pseudorandom

def: an interactive prod $P \leftrightarrow V$ is zero knowledge

if: completeness: $x \in L \Rightarrow P[(P \leftrightarrow V)(x) \text{ ca } \top] \geq 2/3$

soundness: $x \notin L \Rightarrow \leq 1/2$

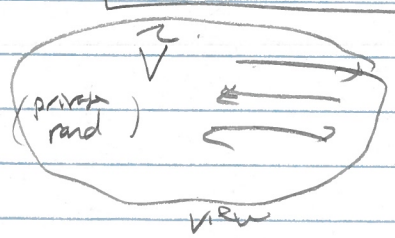
Zero knowledge: every probabilistic poly time malicious verifier $\tilde{V}$, there exists a probabilistic polynomial time simulator $S_{\tilde{V}}$ s.t.

$\forall x \in L$

$(P \leftrightarrow \tilde{V})(x) \overset{?}{=} S_{\tilde{V}}(x)$

view $\hat{V}$

- perfect
- statistical
- computational



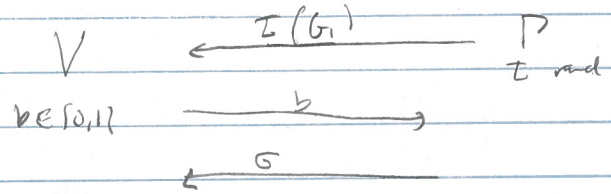
key obs: any info $\tilde{V}$ gets is in view ⇒ can get from $S_{\tilde{V}}(x)$ ↖ no prob

Michael Forbes
miforbes@illinois.edu
2016-03-14.4 ← 2016-03-14.3
CS57 → 2016-03-16.1

graph ISO: G_1, G_2 $\exists \pi$ s.t. $G_1 = \pi(G_2)$
$\in NP \subseteq IP$: provide π ← leaks information!

Prop: $GI \in PZK$ ← IP w/ perfect simulation

Pf:



check $\sigma(\tau(G_1)) = G_b$

complete & sound
zero knowledge: simulator guesses b ; O(1) expected steps
resets verifier if wrong

next time: concrete models of crypto