Introduction to Modern Cryptography
Recitation 3

Orit Moskovich
Tel Aviv University
November 16, 2016

The group: $\mathbb{Z}_N^*$

- Let $N \geq 2$ be an integer
- The set $\mathbb{Z}_N^* = \{a \in \{1, \dots, N-1\} \mid \gcd(a, N) = 1\}$ with respect to multiplication modulo N is an abelian group
  - Identity: 1
  - Inverse of a exists
  - Closure?

- $\mathbb{Z}_p^* = \{1, \dots, p-1\}$

Cyclic Groups and Generators

Definition. Let G be a finite group of order $|G| = m$.
If there exist an element $g \in G$ of order m, then
G is called a **cyclic group** and g is a **generator** of $G = \{g^0, g^1, \dots, g^{m-1}\}$.

- If g is a generator of G, then for every element $h \in G$ there exist $x \in \{0, \dots, m-1\}$ such that $h = g^x$

The Discrete Logarithm

- If g is a generator of G, then for every element $h \in G$ there exist $x \in \{0, \dots, m-1\}$ such that $h = g^x$
- x is the discrete logarithm of h with respect to g

Definition. **The discrete logarithm problem**:
Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$.
Given: $h = g^x$ for $x \in \mathbb{Z}_m = \{0, \dots, m-1\}$
Output: x such that $g^x = h$

Definition. **The discrete logarithm assumption**:
There exists a cyclic group G for which the DL problem is hard

Diffie-Hellman Assumptions

Definition. **The computational Diffie-Hellman (CDH) problem**:
Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$.
Given: g^x, g^y for $x, y \in \mathbb{Z}_m = \{0, \dots, m-1\}$
Output: g^{xy}

(Informal) Definition. **The decisional Diffie-Hellman (DDH) problem**:
Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$.
Goal: To distinguish between 2 distributions:

- $D_0 = \{g^x, g^y, g^{xy} \mid (x, y) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m\}$
- $D_1 = \{g^x, g^y, g^z \mid (x, y, z) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_m\}$

Diffie-Hellman Assumptions

- The DL problem is believed to be hard in cyclic groups of prime order
- The DL problem is believed to be hard in $\mathbb{Z}_p^*$, for p prime
- The CDH problem is believed to be hard in $\mathbb{Z}_p^*$
- The DDH problem is not hard in $\mathbb{Z}_p^*$
- For $q = 2p + 1$, the DDH problem is believed to be hard in a subgroup of $\mathbb{Z}_q^*$ of order p (quadratic residues)

Indistinguishability

Definition. Let D_0, D_1 be two probability distributions over $\{0,1\}^n$. Then, D_0, D_1 are **ε-indistinguishable** for an adversary $A \iff$

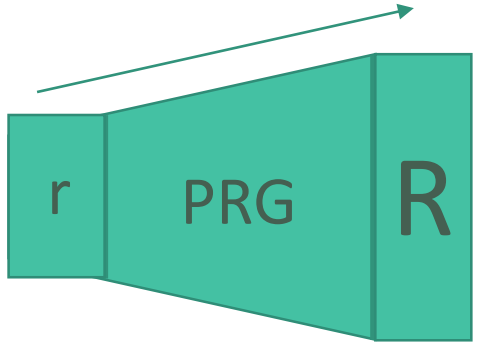
$$\left| \Pr_{d_0 \leftarrow D_0} [A(d_0) = 1] - \Pr_{d_1 \leftarrow D_1} [A(d_1) = 1] \right| \leq \varepsilon$$

1) If D_0, D_1 are ε-indistinguishable for any unbounded adversary A, we say that D_0, D_1 are **statistically indistinguishable**, denoted by $\boldsymbol{D_0 \approx_{s,\varepsilon} D_1}$
2) If D_0, D_1 are ε-indistinguishable for any polynomial adversary A, we say that D_0, D_1 are **computationally indistinguishable**, denoted by $\boldsymbol{D_0 \approx_{c,\varepsilon} D_1}$

Indistinguishability

- Symmetric: $\boldsymbol{D_0 \approx_\varepsilon D_1 \Leftrightarrow D_1 \approx_\varepsilon D_0}$
- Transitive: $\boldsymbol{D_0 \approx_\varepsilon D_1}$ and $\boldsymbol{D_1 \approx_\varepsilon D_2 \Longrightarrow D_0 \approx_{2\varepsilon} D_2}$

Pseudo-Randomness



- Motivation:
  - OTP
  - Want to extract from a short, random seed a longer pseudorandom key
  - A pseudorandom string looks like a uniformly distributed string

Definition. A function $G: \{0,1\}^n \to \{0,1\}^{n+s}$ $(s > 0)$ is a **ε-pseudorandom generator (ε-PRG)** $\Leftrightarrow$

$$G(U_n) \approx_{c,\varepsilon} U_{n+s}$$

- Meaning, we can't distinguish between the output of the PRG and true randomness

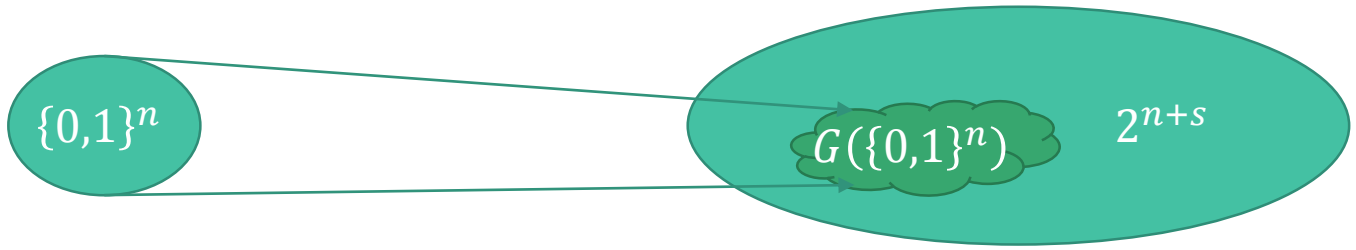
Pseudo-Randomness

Definition. A function $G: \{0,1\}^n \to \{0,1\}^{n+s}$ $(s > 0)$ is a ε-pseudorandom generator (ε-PRG) $\Leftrightarrow$

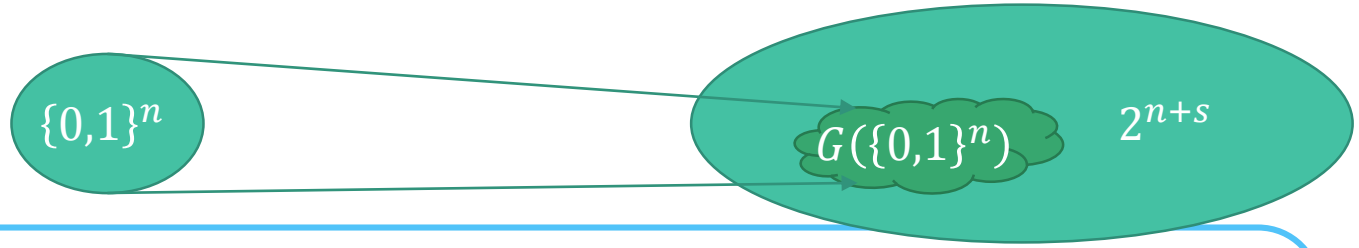
$$G(U_n) \approx_{c,\varepsilon} U_{n+s}$$

Claim. There exists an unbounded adversary A such that:

$$\left| \Pr_{u_0 \leftarrow U_n}[A(G(u_0)) = 1] - \Pr_{u_1 \leftarrow U_{n+s}}[A(u_1) = 1] \right| \geq 1 - \frac{1}{2^s} = 1 - \frac{2^n}{2^{n+s}}$$



Pseudo-Randomness



Claim. There exists an unbounded adversary A such that:

$$\left| \Pr_{u_0 \leftarrow U_n}[A(G(u_0)) = 1] - \Pr_{u_1 \leftarrow U_{n+s}}[A(u_1) = 1] \right| \geq 1 - \frac{1}{2^s}$$

$= 1$ $\qquad$ $= \frac{2^n}{2^{n+s}}$

1. The adversary A is given u
2. A computes the set $S = \{G(s) | s \in \{0,1\}^n\}$
3. A outputs $1 \Leftrightarrow u \in S$

Back to Diffie-Hellman

(Informal) Definition. **The decisional Diffie-Hellman (DDH) problem**:
Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$.
Goal: To distinguish between 2 distributions:

- $D_0 = \{g^x, g^y, g^{xy} \mid (x, y) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m\}$
- $D_1 = \{g^x, g^y, g^z \mid (x, y, z) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_m\}$

Definition. Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$. Define

- $D_0 = \{g^x, g^y, g^{xy} \mid (x, y) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m\}$
- $D_1 = \{g^x, g^y, g^z \mid (x, y, z) \leftarrow \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_m\}$

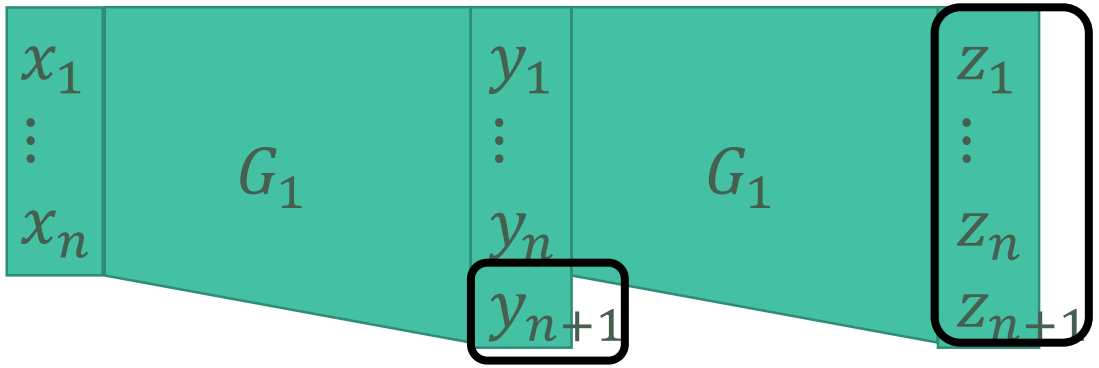
Then, we say that **The DDH problem is hard in G** $\Leftrightarrow D_0 \approx_{c,\varepsilon} D_1$

DDH → PRG

- Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$ in which DDH is hard
- Define the $PRG: \mathbb{Z}_m \times \mathbb{Z}_m \to G \times G \times G$
- $PRG(x, y) = g^x, g^y, g^{xy}$

PRG Expansion

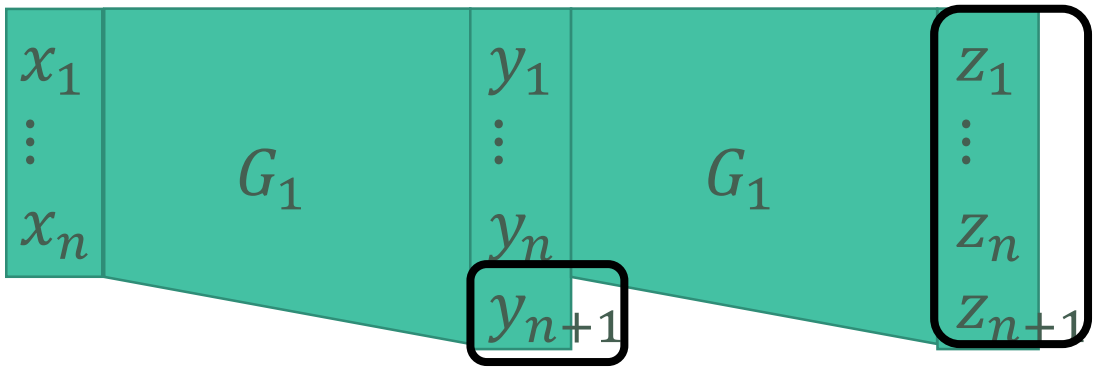
- Assume we have a PRG $G_1: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$
- We want to construct a PRG $G_2: \{0,1\}^n \rightarrow \{0,1\}^{n+2}$



- $G_2(x) = G_1\big(\underbrace{G_1(x)_{1,\ldots,n}}\big)||\underbrace{G_1(x)_{n+1}}$

$= y_1 \cdots y_n \qquad = y_{n+1}$

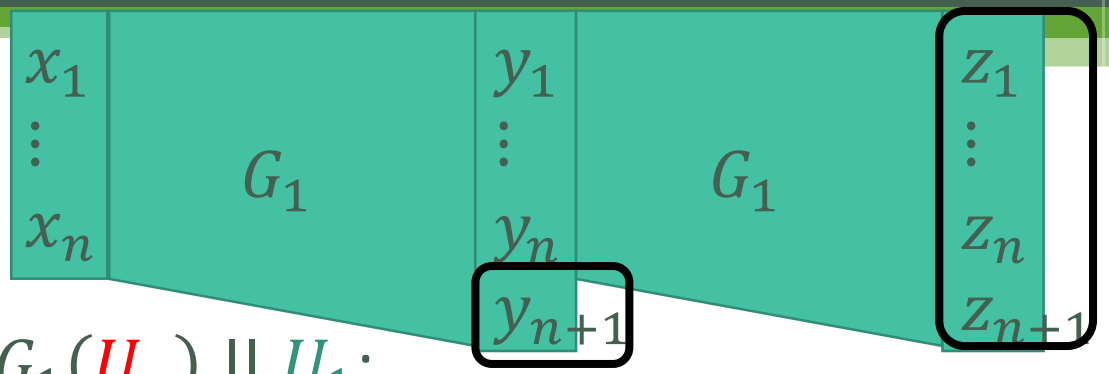
PRG Expansion



- $G_2(x) = G_1\left(G_1(x)_{1,\ldots,n}\right)||G_1(x)_{n+1}$
- How do we prove that this is a PRG?
  - We need to show $G_2(U_n) \approx_{c,2\varepsilon} U_{n+2}$
- We know
  - $G_1(U_n) \approx_{c,\varepsilon} U_{n+1}$

- We will prove two claims:
  1) $G_1\left(G_1(U_n)_{1,\ldots,n}\right) \,||\, G_1(U_n)_{n+1} \approx_{c,\varepsilon} G_1(U_n) \,||\, U_1$
  2) $G_1(U_n)||U_1 \approx_{c,\varepsilon} U_{n+2}$

PRG Expansion



1) $G_1\left(G_1(U_n)_{1,\dots,n}\right) \mid\mid G_1(U_n)_{n+1} \approx_{c,\varepsilon} G_1(U_n) \mid\mid U_1$:

- Assume that there exists an adversary A_2 such that

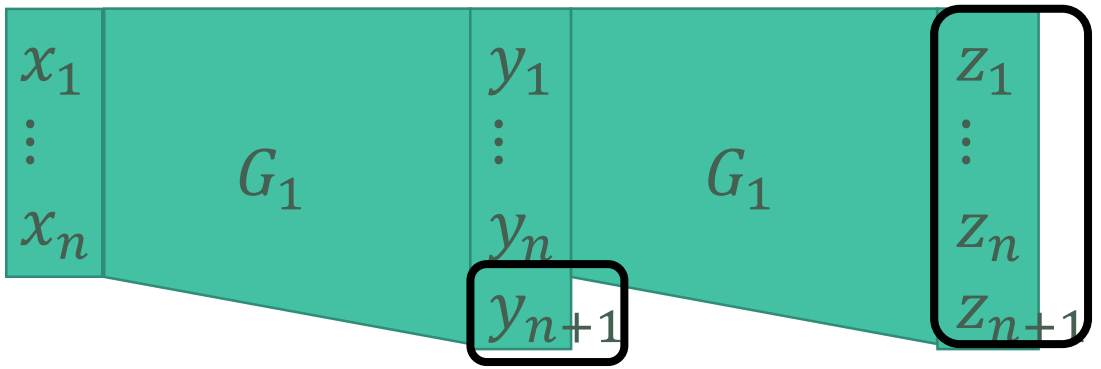
$$\left| \Pr_{d_0 \leftarrow \cdots}[A_2(d_0) = 1] - \Pr_{d_1 \leftarrow G_1(U_n) \mid\mid U_1}[A_2(d_1) = 1] \right| \geq \varepsilon$$

- Then, construct the following adversary A_1 that distinguish between $G_1(U_n)$ and U_{n+1}

1. The adversary A_1 is given u (either from $G_1(U_n)$ or U_{n+1})
2. Denote $x = u_{1,\dots,n}$ and $y = u_{n+1}$
3. A_1 runs $A_2(G_1(x)||y)$ and returns the same output

PRG Expansion

2) $G_1(U_n)||U_1 \approx_{c,\varepsilon} U_{n+2}$:



- Assume that there exists an adversary A_2 such that

$$\left| \Pr_{d_0 \leftarrow G_1(U_n)||U_1} [A_2(d_0) = 1] - \Pr_{d_1 \leftarrow U_{n+2}} [A_2(d_1) = 1] \right| \geq \varepsilon$$

- Then, construct the following adversary A_1 that distinguish between $G_1(U_n)$ and U_{n+1}

1. The adversary A_1 is given u (either from $G_1(U_n)$ or U_{n+1})
2. A_1 chooses at random $u' \leftarrow U_1$
3. A_1 runs $A_2(u||u')$ and returns the same output

One Way Function (OWF)

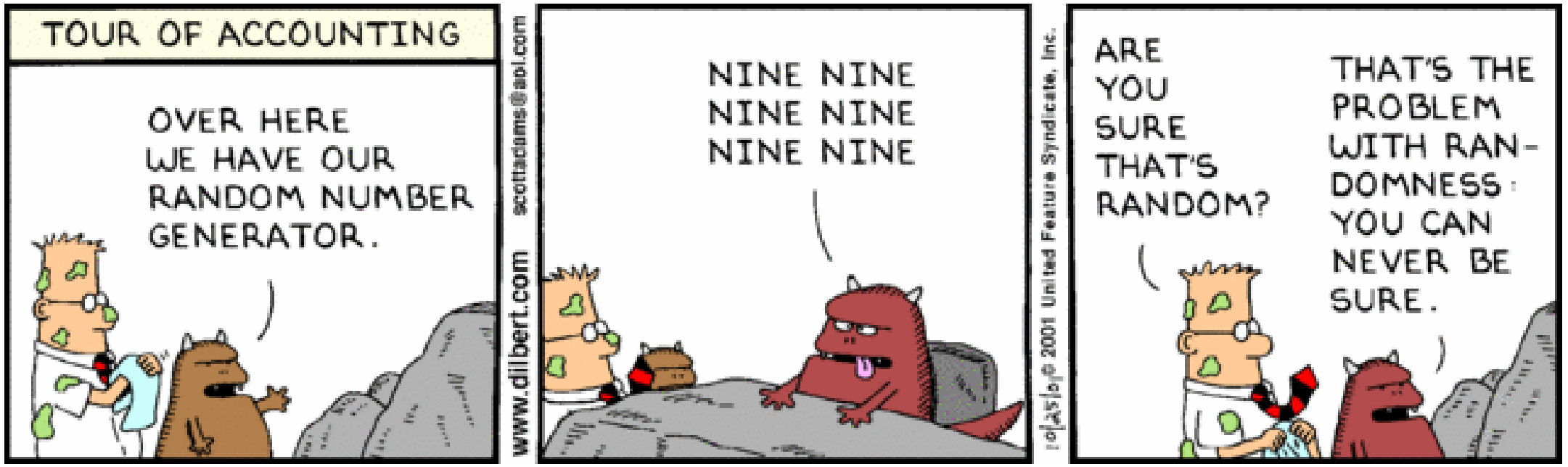
Definition. A function $f: \{0,1\}^n \to \{0,1\}^m$ is a **ε-one way function (ε-OWF)** if for any polynomial time adversary A:

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A\left(f(x)\right) = x\right] < \varepsilon$$

- What if f is not one-to-one?
- What is ε?

DL ➔ OWF

- Let p be a prime and a generator $g \in \mathbb{Z}_p^*$ (in which DL is hard)
- Define the OWF: $f(x) = g^x \ mod \ p$


DILBERT By Scott Adams
TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
© 2001 United Feature Syndicate, Inc.