Classic Paper Reading Group Session 2

On the role of definitions in and beyond cryptography [Rog05]

Simon Pohmann

October 30, 2022

Pseudorandom number generators

When should we consider a sequence of numbers to be "random"?

Pseudorandom number generators

When should we consider a sequence of numbers to be "random"?

Definition

A function $G : \{0,1\}^n \to \{0,1\}^N$ with $N > n \geq 1$ is called *pseudorandom generator*.

Pseudorandom number generators

When should we consider a sequence of numbers to be "random"?

Definition

A function $G : \{0,1\}^n \to \{0,1\}^N$ with $N > n \geq 1$ is called *pseudorandom generator*.

Remark

PRG are more like "randomness expanders"

“How random” is a PRG?

Definition

The advantage of an algorithm A when attacking a PRG G is

$$\mathbf{Adv}_G^{\mathrm{PRG}}(A) := \Pr[\mathbf{Game}_G^0(A) = 0] - \Pr[\mathbf{Game}_G^1(A) = 0]$$

in

$$\mathbf{Game}_G^0(A) \qquad\qquad \mathbf{Game}_G^1(A)$$

$$\begin{tikzcd} {} \arrow[d] & \\ A \arrow[r, dotted, bend left] \arrow[d] & G(U_n) \arrow[l, "\text{sample}"'] \\ \{0,1\} & \end{tikzcd} \qquad\qquad \begin{tikzcd} {} \arrow[d] & \\ A \arrow[r, dotted, bend left] \arrow[d] & U_N \arrow[l, "\text{sample}"'] \\ \{0,1\} & \end{tikzcd}$$

where U_n resp. U_N are uniformly random.

Provable security

Example

If $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, then this is also the case for

$$\begin{tikzcd}
\{0,1\}^n \arrow[r, "x_0"] & G \arrow[r, "x_1"] \arrow[drrr, bend right, "y_1"'] & \cdots \arrow[r, "x_m"] \arrow[drr, bend right, "y_m"'] & G \arrow[dr, bend left, "x_{m+1}"] & \\
 & & & & \{0,1\}^N
\end{tikzcd}$$

Proof: [KL21, Thm. 8.19]

Provable security

Example

If $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, then this is also the case for

$$\begin{tikzcd}
\{0,1\}^n \arrow[r, "x_0"] & G \arrow[r, "x_1"] \arrow[drrr, bend right, "y_1"'] & \cdots \arrow[r, "x_m"] \arrow[drr, bend right, "y_m"'] & G \arrow[dr, bend left, "x_{m+1}"] & \\
& & & & \{0,1\}^N
\end{tikzcd}$$

Proof: [KL21, Thm. 8.19]

- Definitions have a huge impact on the field

Provable security

Example

If $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, then this is also the case for

$$\begin{tikzcd}
\{0,1\}^n \arrow[r, "x_0"] & G \arrow[r, "x_1"] \arrow[drrr, bend right=10, "y_1"'] & \cdots \arrow[r, "x_m"] \arrow[drr, bend right=10, "y_m"'] & G \arrow[dr, bend left, "x_{m+1}"] & \\
& & & & \{0,1\}^N
\end{tikzcd}$$

Proof: [KL21, Thm. 8.19]

- Definitions have a huge impact on the field
- Definitions are about ideas

Provable security

Example

If $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, then this is also the case for

$$\begin{tikzcd}
\{0,1\}^n \arrow[r, "x_0"] & G \arrow[r, "x_1"] \arrow[drrr, bend right, "y_1"'] & \cdots \arrow[r, "x_m"] \arrow[drr, bend right, "y_m"'] & G \arrow[dr, bend left, "x_{m+1}"] & \\
 & & & & \{0,1\}^N
\end{tikzcd}$$

Proof: [KL21, Thm. 8.19]

- Definitions have a huge impact on the field
- Definitions are about ideas
- Good definitions are robust

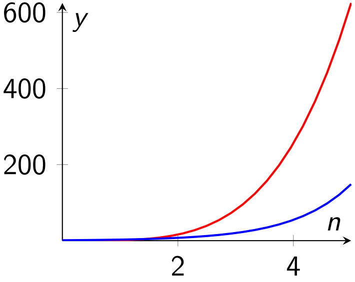
Asymptotic notions

Definition

A function $f : \mathbb{Z}_+ \to \mathbb{R}_+$ is *negligible*, if $f(n)$ is *eventually* smaller than any $1/\mathrm{poly}(n)$.

Definition

An algorithm A is *polynomial-time*, if there is a polynomial p such that the number of operations on an input of length n is at most $p(n)$.



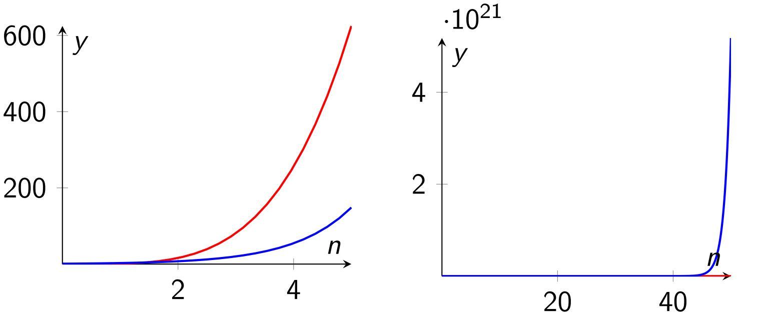
Asymptotic notions

Definition

A function $f : \mathbb{Z}_+ \to \mathbb{R}_+$ is *negligible*, if $f(n)$ is *eventually* smaller than any $1/\mathrm{poly(n)}$.

Definition

An algorithm A is *polynomial-time*, if there is a polynomial p such that the number of operations on an input of length n is at most $p(n)$.



Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory

Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory
no definition of "secure"	secure $:=$ advantage is negligible

Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory
no definition of "secure"	secure := advantage is negligible
constant in/output size	sizes depend on "security parameter"

Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory
no definition of "secure"	secure := advantage is negligible
constant in/output size	sizes depend on "security parameter"
attackers must be "feasible"	attackers must be polynomial-time

Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory
no definition of "secure"	secure := advantage is negligible
constant in/output size	sizes depend on "security parameter"
attackers must be "feasible"	attackers must be polynomial-time

- Definitions can change the way a theory develops

Asymptotic and concrete security

Concrete	Asymptotic
application oriented	originated in complexity theory
no definition of "secure"	secure := advantage is negligible
constant in/output size	sizes depend on "security parameter"
attackers must be "feasible"	attackers must be polynomial-time

- Definitions can change the way a theory develops
- Definitions come from a scientific culture

Blockciphers

Definition

A *blockcipher* is a function $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ such that $E(k, \cdot)$ is a permutation for all $k \in \mathcal{K}$.

$$\begin{tikzcd} & \mathcal{K} \arrow[d] & \\ \{0,1\}^n \arrow[r] & \boxed{A} \arrow[r] & \{0,1\}^n \end{tikzcd}$$

Blockciphers

Definition

A *blockcipher* is a function $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ such that $E(k, \cdot)$ is a permutation for all $k \in \mathcal{K}$.

$$\begin{tikzcd} & \mathcal{K} \arrow[d] & \\ \{0,1\}^n \arrow[r] & \boxed{A} \arrow[r] & \{0,1\}^n \end{tikzcd}$$

Remark

We did not specify the decryption function.

Advantage for blockciphers

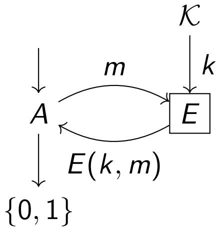
Definition

The advantage of an algorithm A during a *chosen-ciphertext attack* to blockcipher E is

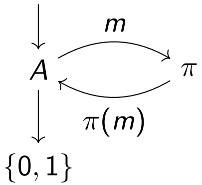
$$\mathbf{Adv}_E^{\mathsf{CPA}}(A) := \Pr[\mathbf{Game}_E^0(A,k) = 0] - \Pr[\mathbf{Game}_E^1(A,\pi) = 0]$$

for a uniformly random $k \in \mathcal{K}$ and $\pi \in \mathrm{Sym}(\{0,1\}^n)$ in the games

$\mathbf{Game}_E^0(A,k)$



$\mathbf{Game}_E^1(A,\pi)$



Advantage for blockciphers

$\mathbf{Game}^0_E(A, k)$

$$
\begin{tikzcd}
{} \arrow[d] & \mathcal{K} \arrow[d, "k"] \\
A \arrow[r, bend left, "m"] \arrow[d] & \boxed{E} \arrow[l, bend left, "{E(k, m)}"] \\
\{0, 1\} &
\end{tikzcd}
$$

$\mathbf{Game}^1_E(A, \pi)$

$$
\begin{tikzcd}
{} \arrow[d] & \\
A \arrow[r, bend left, "m"] \arrow[d] & \pi \arrow[l, bend left, "\pi(m)"] \\
\{0, 1\} &
\end{tikzcd}
$$

Advantage for blockciphers

$\mathbf{Game}_E^0(A, k)$

$$\begin{tikzcd} {} \arrow[d] & \mathcal{K} \arrow[d, "k"] \\ A \arrow[r, bend left, "m"] \arrow[d] & \boxed{E} \arrow[l, bend left, "E(k, m)"] \\ \{0, 1\} & \end{tikzcd}$$

$\mathbf{Game}_E^1(A, \pi)$

$$\begin{tikzcd} {} \arrow[d] & \\ A \arrow[r, bend left, "m"] \arrow[d] & \pi \arrow[l, bend left, "\pi(m)"] \\ \{0, 1\} & \end{tikzcd}$$

- For low-level primitives, simple & pessimistic definitions are better

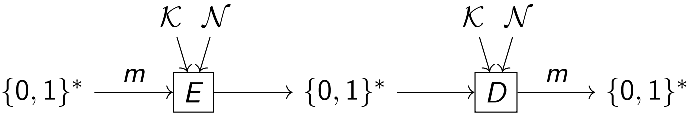
Authenticated Encryption

Definition

An AE scheme are two deterministic functions

$$\begin{aligned} E &: \mathcal{K} \times \mathcal{N} \times \{0,1\}^* \to \{0,1\}^* \quad \text{(encryption)} \\ D &: \mathcal{K} \times \mathcal{N} \times \{0,1\}^* \cup \{\perp\} \quad \text{(decryption)} \end{aligned}$$

such that $D(k, n, E(k, n, m)) = m$ for all k, n, m. Further, we require that $|E(k, n, m)| = |m| = \tau$.



Two contests

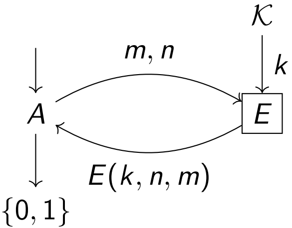
Definition (privacy advantage)

The advantage of an algorithm A for a privacy attack on an AE scheme (E, D) is

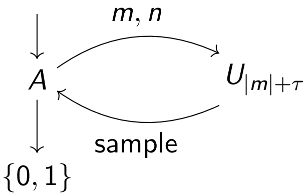
$$\mathbf{Adv}_E^{\text{AE-P}}(A) := \Pr[\mathbf{Game}_E^0(A, k) = 0] - \Pr[\mathbf{Game}_E^1(A) = 0]$$

for a uniformly random $k \in \mathcal{K}$ in the games

$\mathbf{Game}_E^0(A, k)$



$\mathbf{Game}_E^1(A, \pi)$



Two contests

Definition (authenticity advantage)

The advantage of A for an authenticity attack on an AE scheme (E, D) is

$$\mathbf{Adv}_E^{\text{AE-A}}(A) := \Pr[\mathbf{Game}_E(A, k) \neq \bot]$$

for a uniformly random $k \in \mathcal{K}$ in the game

$$\mathbf{Game}_E(A, k)$$

$$\begin{tikzcd}
 & \boxed{E} \arrow[d, bend left, "{E(k, n_i, m_i)}"] & & \mathcal{K} \arrow[ll, "k"] \arrow[d, "k"] & \\
{} \arrow[r] & A \arrow[u, bend left, "{m_i, n_i}"] \arrow[r, "{n, m \neq m_i}"'] & \mathcal{N} \times \{0,1\}^* \arrow[r] & \boxed{D} \arrow[r] & \{\bot\} \cup \{0,1\}^*
\end{tikzcd}$$

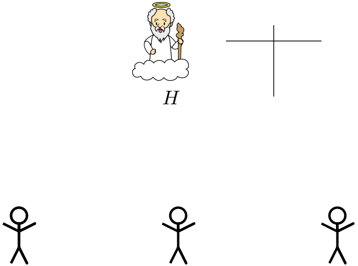
- Definitions emerge, change, and die more than people think

Session Key distribution

We'll skip this

Random oracle model

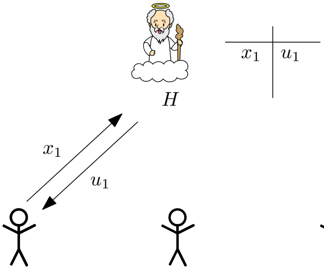
We assume the existence of a *idealized hash function* (or random oracle) $H : \{0,1\}^* \to \{0,1\}^n$.



- Defining and modelling are different, but similar

Random oracle model

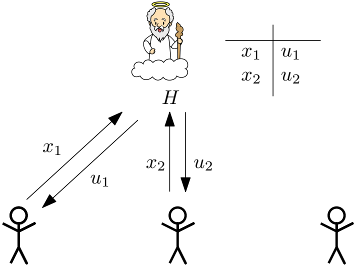
We assume the existence of a *idealized hash function* (or random oracle) $H : \{0,1\}^* \to \{0,1\}^n$.



- Defining and modelling are different, but similar

Random oracle model

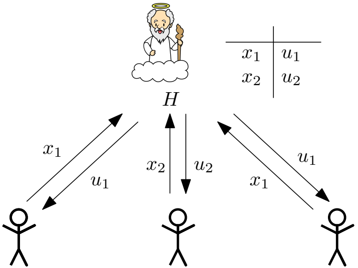
We assume the existence of a *idealized hash function* (or random oracle) $H : \{0,1\}^* \to \{0,1\}^n$.



- Defining and modelling are different, but similar

Random oracle model

We assume the existence of a *idealized hash function* (or random oracle) $H : \{0,1\}^* \to \{0,1\}^n$.



- Defining and modelling are different, but similar

References

Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography, 3rd edition*. CRC Press, 2021.

Phillip Rogaway. "On the Role Definitions in and Beyond Cryptography". In: *Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making*. Ed. by Michael J. Maher. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 13–32. ISBN: 978-3-540-30502-6.