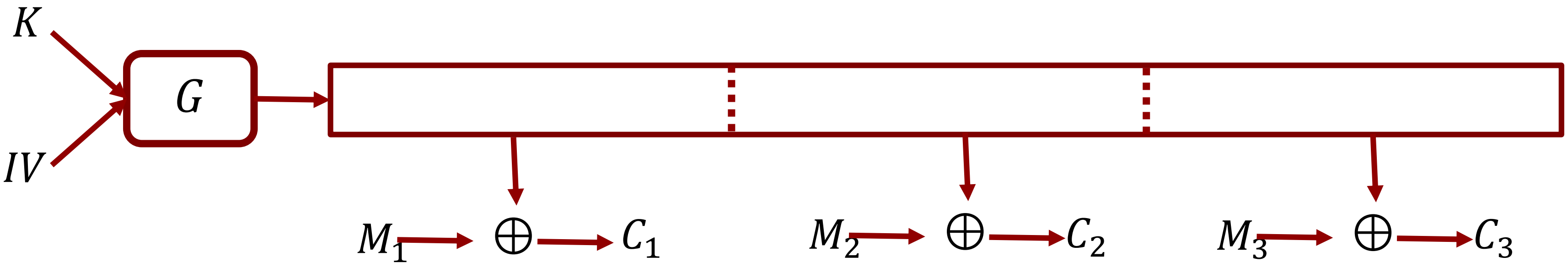
CSL759: Cryptography and Computer Security

Ragesh Jaiswal

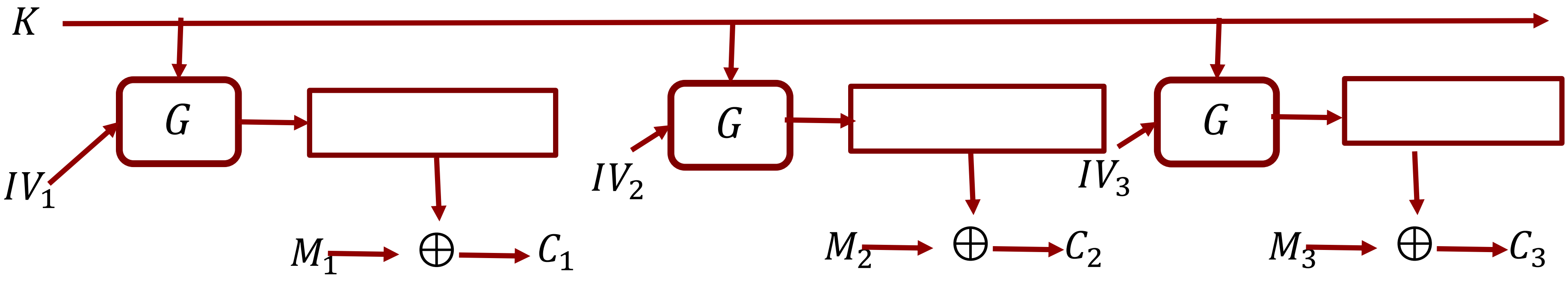
CSE, IIT Delhi

Stream Ciphers: Summary

- Multiple encryptions using Stream Ciphers.



Synchronized mode



Asynchronized mode

Asymptotic security: Pseudorandom generator

- Solution: Time of the adversary and error probability should not be concrete numbers but functions of a parameter of interest. This parameter is called the *security parameter*.
- Asymptotic Security: A scheme is called secure if every PPT (Probabilistic Polynomial Time) adversary succeeds in *breaking* the scheme with only negligible probability.
- Security parameter: discussion
  - Security parameter is very closely related to the key size that is used. Usually it is the same as the key size. Asymptotic security implies that the larger the key size the more secure the scheme will be.
  - Example: Consider a PRG $G: \{0,1\}^k \rightarrow \{0,1\}^{l(k)}$. The deterministic algorithm G stretches arbitrary size seeds to longer strings.

Stream Ciphers: Summary

- Stream ciphers are synonymous with pseudorandom generators (PRG).
- PRGs are algorithms that map $\{0,1\}^k$ to $\{0,1\}^{l(k)}$ with the following properties:
  - $\forall k, l(k) > k.$
  - The mapping algorithm G is deterministic and efficient.
  - Indistinguishability: For every PPT algorithm A (k here is the security parameter) and every polynomial $p(.)$, there is some integer N such that

    $$\forall k > N \,, |\, Pr\big[A\big(G(K)\big) = 1\big] - \Pr[A(R) = 1]| \leq \frac{1}{p(k)} \,.$$

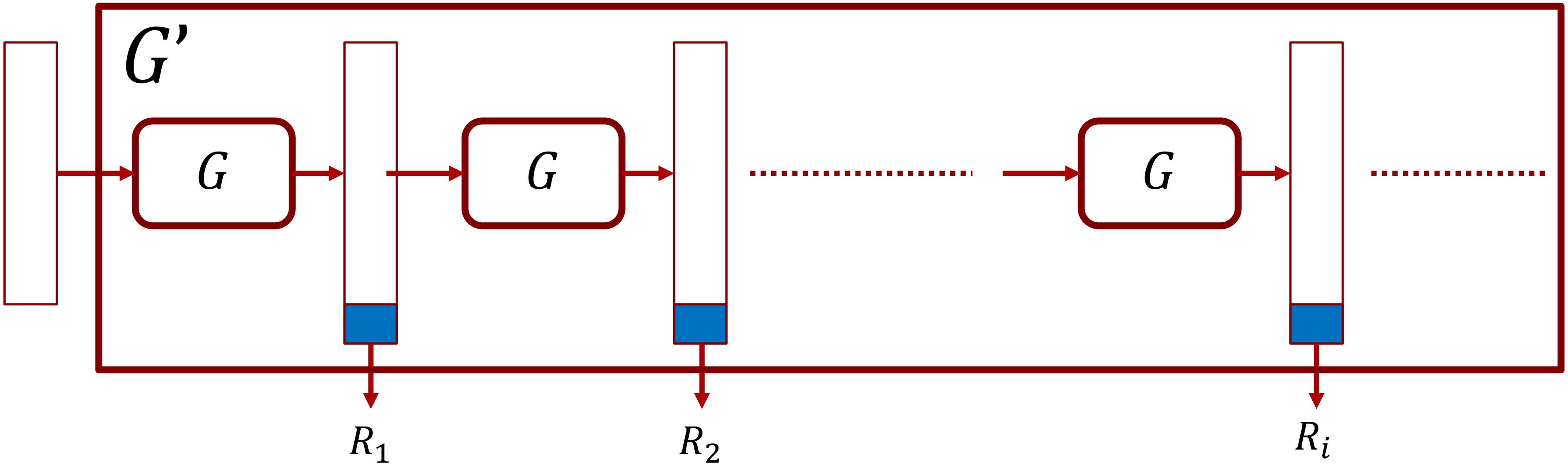
    In other words the success probability of all PPT algorithms should be negligible.

Stream Ciphers: Summary

- Stream ciphers are synonymous with pseudorandom generators (PRG).
- PRGs are algorithms that map $\{0,1\}^k$ to $\{0,1\}^{l(k)}$ with the following properties:
  - $\forall k, l(k) > k$.
  - The mapping algorithm G is deterministic and efficient.
  - Indistinguishability: The success probability of all PPT algorithms should be negligible.
- Question: Suppose we have a secure PRG where $l(k) = k + 1$, i.e., the PRG stretches the bits by 1. Can we construct a secure PRG with longer stretch?

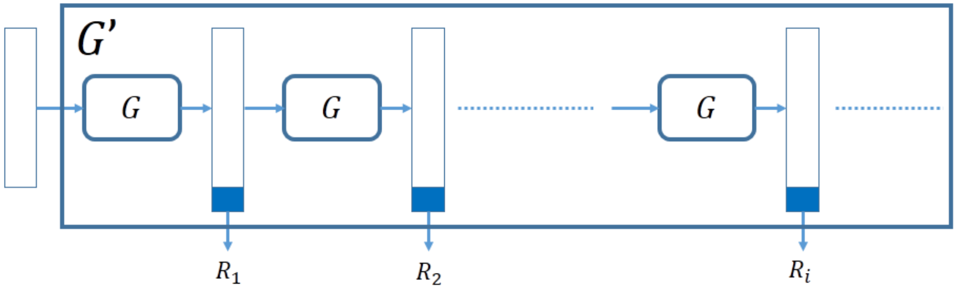
Stream Ciphers: PRG expansion

- Question: Suppose we have a secure PRG where $l(k) = k + 1$, i.e., the PRG stretches the bits by 1. Can we construct a secure PRG with longer stretch?



- Question: Why does the above construction give a secure PRG?

Stream Ciphers: PRG expansion

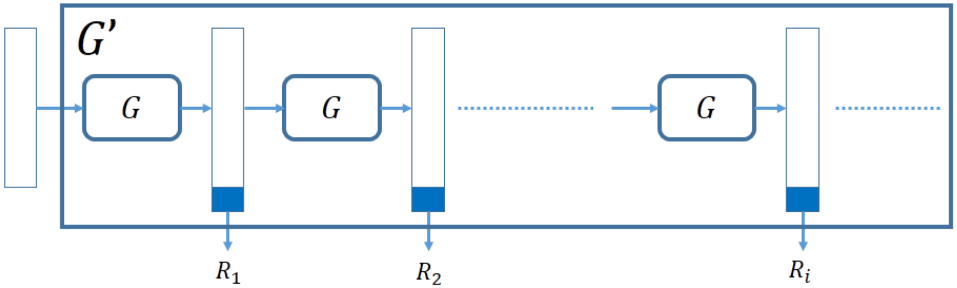


- Question: Why does the above construction give a secure PRG?
- Theorem: If $G: \{0,1\}^n \to \{0,1\}^{n+1}$ is a secure PRG, then $G': \{0,1\}^n \to \{0,1\}^{l(n)}$ is a secure PRG.
- Proof: Suppose G' is insecure. This means that there is an adversary A that runs in time $poly(n)$ and the following holds:

$$\left|\Pr_{K\leftarrow\{0,1\}^n}[A(G'(K)) = 1] - \Pr_{R\leftarrow\{0,1\}^{l(n)}}[A(R) = 1]\right| > \frac{1}{q(n)}.$$

Where $q(.)$ is some polynoimial.

Stream Ciphers: PRG expansion



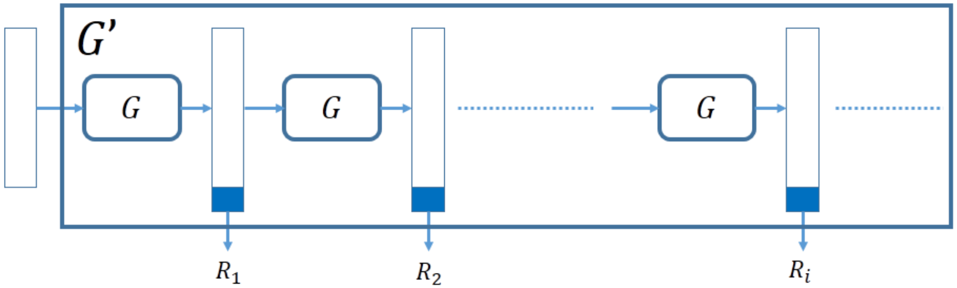
- Theorem: If $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ is a secure PRG, then $G': \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is a secure PRG.
- Proof: Suppose G' is insecure. This means that there is an adversary A that runs in time $p(n)$ and the following holds:

  $$\left| \Pr_{K \leftarrow \{0,1\}^n}[A(G'(K)) = 1] - \Pr_{R \leftarrow \{0,1\}^{l(n)}}[A(R) = 1] \right| > \frac{1}{q(n)}.$$

  Where $q(.)$ is some polynomial.
- We will show that *there exists* adversary B that runs in time $r(n)$ such that:

  $$| \Pr_{K \leftarrow \{0,1\}^n}[B(G(K)) = 1] - \Pr_{R \leftarrow \{0,1\}^{n+1}}[B(R) = 1] | > \frac{1}{q(n) \cdot l(n)}.$$

Stream Ciphers: PRG expansion



- Theorem: If $G:\{0,1\}^n \rightarrow \{0,1\}^{n+1}$ is a secure PRG, then $G':\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is a secure PRG.
- Proof: Suppose G' is insecure. This means that there is an adversary A that runs in time $p(n)$ and the following holds:
  $\left|\Pr_{K\leftarrow\{0,1\}^n}[A(G(K))=1] - \Pr_{R\leftarrow\{0,1\}^{l(n)}}[A(R)=1]\right| > \frac{1}{q(n)}$.
  Where $q(.)$ is some polynomial.
- $B(x_1 \dots x_{n+1})$:
  - Let $R_{i+1} = x_{n+1}, R_{i+2} = G(x_1 \dots x_n)[n+1], R_{i+3} = G(G(x_1 \dots x_n)[1 \dots n])[n+1], \dots$
  - Let $R_1 = r_1, \dots, R_i = r_i$, where $r_1, \dots, r_i$ are independent random bits.
  - Execute A with the input $(R_1, \dots, R_n)$. Output 1 iff A outputs 1.

Stream Ciphers: Summary

- So, do secure PRGs exist?
  - Not known.
  - <u>Conditional existence</u>: Secure PRGs exist if *one way functions (OWFs)* exist. Many people believe that they do.
    - Example of OWF: $f(x,y) = x \cdot y$ for large primes x and y.

Types of Attacks

Types of Attacks

- Until now we have seen security analysis in a restrictive setting.

  1. *Secure communication*
  2. *One-time encryption*: Secret key used to send only one secret message.
  3. *Ciphertext-only adversary*: Adversary only listens to the public channel.

  We would like to relax these restrictions.

- We only analysed the *ciphertext-only adversary* case, when all an adversary does is listen to the channel. Here are some other attack scenarios:

  1. Ciphertext-only attack
  2. Known Plaintext Attack
  3. Chosen Plaintext Attack (**CPA**)
  4. Chosen Ciphertext Attack (**CCA**)

Types of Attacks

- We only analysed the *passive adversary* case, when all an adversary does is listen to the channel. Here are some other attack scenarios:

1. Ciphertext-only Attack: The adversary only gets to see the ciphertexts.
2. Known Plaintext Attack: The adversary gets to know messages of a few ciphertexts.
3. Chosen Plaintext Attack (**CPA**): The adversary is capable to obtaining ciphertexts for messages of its choice.
4. Chosen Ciphertext Attack (**CCA**): The adversary can obtain decryptions of ciphertexts of its choice.

Types of Attacks: KPA

- Known Plaintext Attack (KPA): Examples
  - The plaintext may be deduced from the context.
    - Alice sends Bob a message “Meet me at the coffee shop at 5pm”. Eve observes Alice and Bob at the coffee shop at 5pm and deduce the plaintext.
  - The plaintext may be made public after the secrecy of the message becomes irrelevant.
    - Alice sends Bob a message “Meet me at the coffee shop at 5pm”. Once the meeting is over, Alice makes the plaintext public as it is no more required to keep it a secret.
    - On the other hand, Alice keeps using the same key for future communication with Bob.

Types of Attacks: CPA

- Chosen Plaintext Attack (CPA): Examples
  - In World War-II, the English would mine specific areas. This would evoke response from the Germans to sweep that area.
  - A router may be programmed to encrypt any packet that it sends.
  - An email program may forward an email after encryption.

Types of Attacks: CCA

- Chosen Ciphertext Attack (CCA): Examples
  - Eve send an arbitrarily chosen ciphertext and observe the behaviour of Bob to figure out the plaintext.
  - In cases where encryption is used as an authentication mechanism. A person may be authenticated using the knowledge that the person can successfully decrypt an encrypted message.

End