CSE 575: Advanced Cryptography
Fall 2024
Lecture 2

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Information-theoretic security
- Computational hardness

Agenda for this lecture

- Announcements
- Information-theoretic security
- Computational hardness

Announcements

- NO discussion Friday – I am moving
- HW1 is online, due Monday 9/9

News

What We Know About the Telegram Founder's Arrest

Pavel Durov has been detained in France, as part of wide-ranging investigation into criminal activities on the messaging platform he runs.

Agenda for this lecture

- Announcements
- Information-theoretic security
- Computational hardness

Symmetric-Key Encryption

Eve

algorithm $E : \boldsymbol{C} \to \boldsymbol{*}$

Alice $\longrightarrow$ Bob

Enc : $\boldsymbol{K} \times \boldsymbol{M} \to \boldsymbol{C}$

Dec : $\boldsymbol{K} \times \boldsymbol{C} \to \boldsymbol{M}$

Instead, allow both Enc and Dec to take a ***key*** k.
K is generated by a randomized algorithm Gen

Desired functionality: for any m in ***M*** and k in ***K***, Dec(k, Enc(k, m)) = m

Shannon Secrecy

Definition 2.1 (Shannon secrecy)**.** A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *Shannon secret with respect to a probability distribution* D over $\mathcal{M}$ if for all $\bar{m} \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow D,\ k \leftarrow \mathsf{Gen}}[m = \bar{m} \mid \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution D over $\mathcal{M}$.

Rewriting Shannon Secrecy

Definition 2.1 (Shannon secrecy). A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *Shannon secret with respect to a probability distribution D over $\mathcal{M}$* if for all $\bar{m} \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow D,\, k \leftarrow \mathsf{Gen}}[m = \bar{m} \mid \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution D over $\mathcal{M}$.

$$\Pr_{\substack{k \leftarrow \mathrm{Gen} \\ m \leftarrow D}}[m = \bar{m} \mid \mathrm{Enc}_k(m) = \bar{c}]$$

$$= \frac{\Pr_{k,m}[m = \bar{m} \wedge \mathrm{Enc}_k(\bar{m}) = \bar{c}]}{\Pr_{k,m}[\mathrm{Enc}_k(m) = \bar{c}]}$$

$$= \frac{\Pr_m[m = \bar{m}] \Pr_k[\mathrm{Enc}_k(\bar{m}) = \bar{c}]}{\Pr_{k,m}[\mathrm{Enc}_k(m) = \bar{c}]}$$

$$\Pr_k[\mathrm{Enc}_k(\bar{m}) = \bar{c}] = \Pr_{k,m}[\mathrm{Enc}_k(m) = \bar{c}]$$

Perfect Secrecy

Definition 2.2 (Perfect secrecy)**.** A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secret* if for all $m_0, m_1 \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_0) = \bar{c}] = \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_1) = \bar{c}].$$

The One-Time Pad

- Gen:
  $\underbrace{K \leftarrow \$ \{0,1\}^n}_{2}$
  Return K
- $Enc(K, m)$:
  Return $K \oplus m$
- $Dec(k, c)$
  Return $K \oplus c$

$$c_1 \oplus c_2$$

$$(\cancel{K} \oplus m_0) \oplus (\cancel{K} \oplus m_1) = m_0 \oplus m_1$$

The One-Time Pad

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

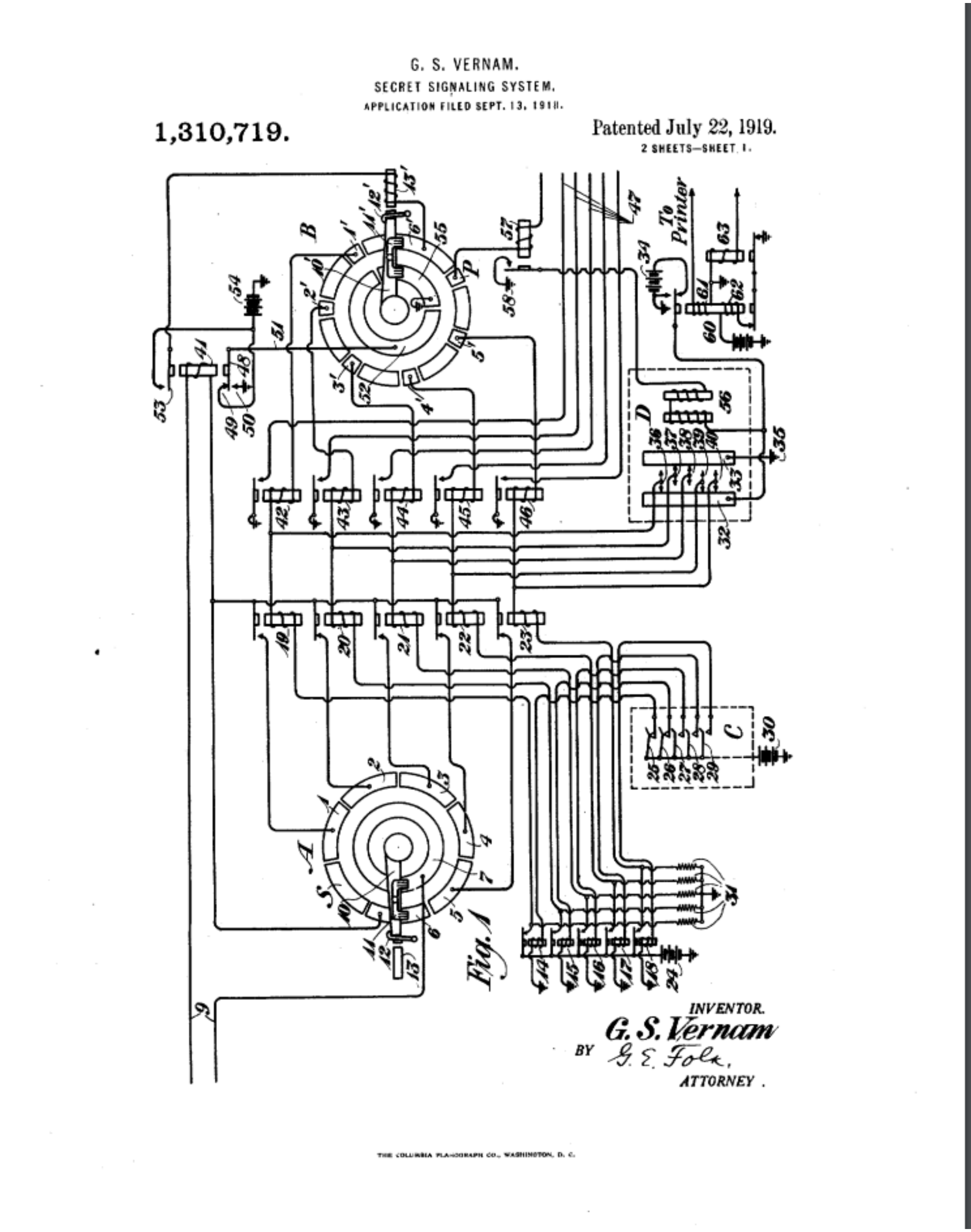
1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

tact with the ring 7 and the segmental contacts repectively. When the apparatus is at rest this arm is detained by the latch 12 which may be withdrawn by means of magnet 13 under the control of the operator. The receiving side of the distributer has five



Perfect Secrecy of the One-Time Pad

Theorem 2.4. *The one-time pad is a perfectly secret symmetric-key encryption scheme.*

Proof:

$\forall m_0, m_1, \forall \bar{c},$

$$\Pr_K[\mathrm{Enc}_K(m_0)=\bar{c}] = \Pr_K[\mathrm{Enc}_K(m_1)=\bar{c}]$$

$$\Pr_{K\leftarrow\{0,1\}^n}[\mathrm{Enc}_K(m_0)=\bar{c}] = \Pr_{K\leftarrow\{0,1\}^n}[K\oplus m_0=\bar{c}]$$

$$= \Pr_K[K=m_0\oplus\bar{c}] = 2^{-n}$$

$$= \Pr_K[K=m_1\oplus\bar{c}] \qquad \boxtimes$$

Limitations of the One-Time Pad

- $|K| = |M|$
- True randomness
- No authentication
- length leakage

Limitations of Perfect Secrecy

Theorem 2.2 (Shannon's theorem). *If a shared-key encryption scheme (with key space $\mathcal{K}$ and message space $\mathcal{M}$) is ~~Shannon~~ Perfect secret, then $|\mathcal{K}| \geq |\mathcal{M}|$.*

Proof:

By contradiction: Assume P.S. scheme with $\{|K| < |\mathcal{M}|\}$.

we know $|C| \geq |\mathcal{M}|$. Take $\bar{c}$

$$D = \{ Dec_k(\bar{c}) : k \in \mathcal{K} \}$$

$$|D| < |\mathcal{M}| \qquad m_0 \in D$$

$$m_1 \in \mathcal{M} \setminus D$$

$$\Pr_k[Enc_k(m_1) = \bar{c}] = 0 \quad \rightarrow \Leftarrow$$

$$\Pr_k[Enc_k(m_0) = \bar{c}] > 0$$

Agenda for this lecture

- Announcements
- Information-theoretic security
- Computational hardness

Model of Computation: Algorithms

- "Turing Machine"
- Running Time
  - Basic operations, mem. access $O(1)$
- Randomness $A(x; r)$
- non-uniformity
  - Advice about problem.

    Depends on problem length

Model of Computation: Asymptotics

One-Way Functions