情報理論的暗号技術について:
理論と応用

四方 順司
Junji Shikata

横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences,
Yokohama National University, Japan

Cryptology

- The cryptology (or modern cryptography) is an interdisciplinary research field.

- It intersects the research fields of
  - mathematics (e.g., number theory, algebra, combinatorics,…),
  - computer science (e.g., complexity theory, algorithm theory,…),
  - informatics (e.g., information theory,…),
  - physics (e.g., quantum theory,…), etc.

- Two crucial papers in theory of modern cryptography:
  - by Shannon in 1949: Information-theoretic Cryptography
  - by Diffie and Hellman in 1976: Public-key Cryptography

Security in Cryptography

Computational Security (including public-key crypto.)

- Security is formalized based on Complexity Theory
- Adversary's computational power: limited (i.e., polynomial time Turing machines)
- Require computational assumptions such as number-theoretic ones

(e.g. Integer Factoring is hard, Discrete Log Problem is hard)

Information-theoretic Security (Unconditional Security)

- Security is formalized based on Information Theory, Probability Theory
- Adversary's computational power: unlimited (i.e., unbounded Turing machines)
- Require no computational assumption.

But, other assumptions are required (e.g., physical ones).

Why information-theoretic crypto?

- **(Merit) Essentially, information-theoretic security does not depend on computational models, computing powers of adversaries, progress of computer technology.**
  - Security is maintained even if quantum computers appear.
  - Not necessary to care about adversary's computing power.
  - Long term security (say, more than 10 years) is possible.
- **(Demerit) Essentially, each user in a system needs to have some secret information (e.g., uniformly random secret-key), <u>if there is no assumption</u>.**
  - It is impossible to realize public-key crypto. (e.g., encryption-key cannot be made public) by information-theoretic crypto.
- **(Demerit) In general, the size of secret information (secret-key) is large. Therefore, it is important to consider relationships between security and efficiency.**

Several Entropies (information-theoretic measure)

Let X be a random variable taking values in a finite set Ω .

$$H(X) = -\sum_{x \in \Omega} P_X(x) \log P_X(x), \quad \text{(Shannon entropy)}$$

$$R_\infty(X) = \min_x \{-\log P_X(x)\}, \quad \text{(min- entropy)}$$

$$R_0(X) = \log |\{x \in \Omega \mid P_X(x) > 0\}|. \quad \text{(Hartley entropy: log of cardinality)}$$

Then, the following relationship holds:

$$R_\infty(X) \le H(X) \le R_0(X)$$

Rényi entropy of order α

Let X be a random variable taking values in a finite set.

For a real number $\alpha \geq 0, \alpha \neq 1$, we define

$$R_\alpha(X) = \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha$$

Then, the following relationship holds:

$$\lim_{\alpha \to 0} R_\alpha(X) = R_0(X),$$

$$\lim_{\alpha \to 1} R_\alpha(X) = H(X),$$

$$\lim_{\alpha \to \infty} R_\alpha(X) = R_\infty(X).$$

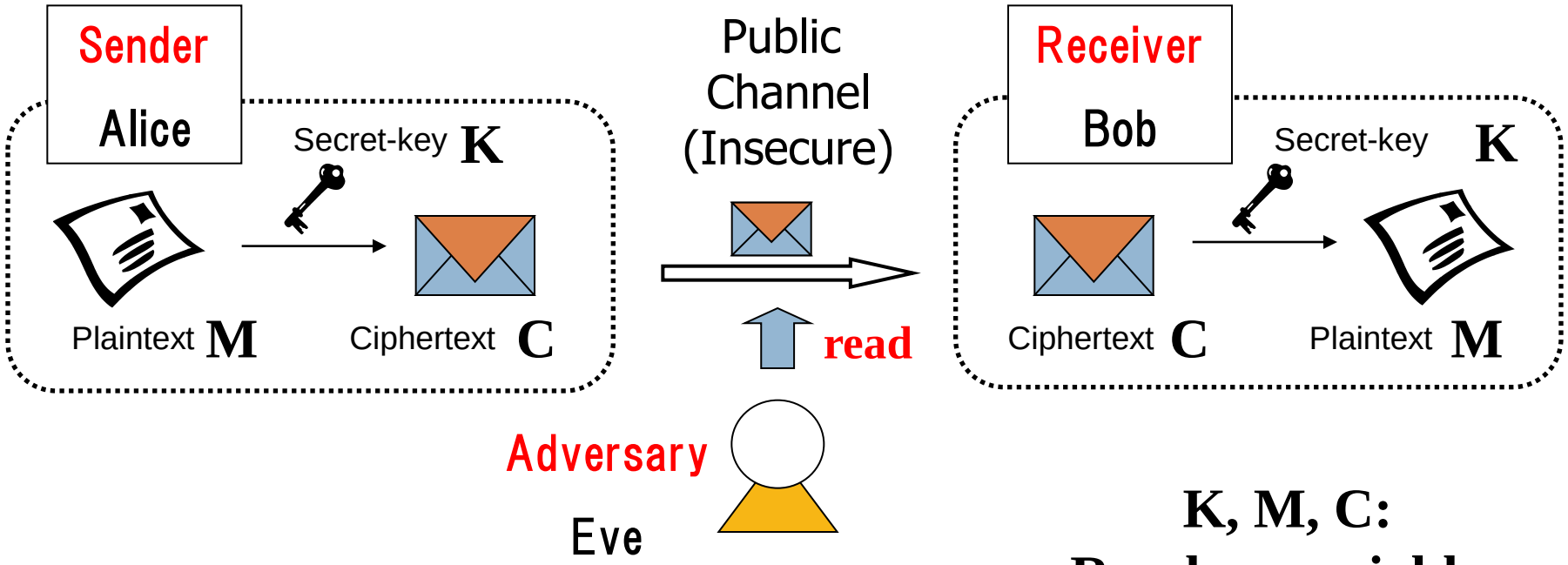
Basic Cryptographic Functionality

Basic cryptographic functionalities include:

- **Encryption**,
- **Authentication** / Signature,
- Key agreement,
- Secret Sharing,
- OT (Oblivious Transfer), BC (Bit Commitment)

Cryptosystems with Information Theoretic Security [Shannon49]

The cryptosystem (encryption) is the technique to provide **privacy** or **confidentiality**: keeping information secret from the adversary.



K, M, C: Random variables

Perfect Secrecy (PS) The adversary with unlimited computational power cannot obtain any information on the underlying plaintext after observing the target ciphertext: $H(M|C)=H(M)$

Traditional Security Definition by Shannon

Formalization of PS (by Shannon entropy)

For a random variable M,

$$H(M|C) = H(M) \Leftrightarrow I(M; C) = 0$$

- For random variables X and Y,

$$H(X \mid Y) = \sum_{y} P_Y(y) H(X \mid Y = y).$$

- $I(X;Y) = H(X) - H(X \mid Y)$

$$= H(Y) - H(Y \mid X)$$

Vernam Cipher

Vernam cipher is an example of the cryptosystem with perfect secrecy (PS).

Toy Example

m (=0 or 1): plaintext with 1 bit-length

c (=0 or 1): ciphertext with 1 bit-length

k (=0 or 1): key with 1 bitlength,

chosen uniformly at random from {0,1}

i.e. k=1 with probability 1/2,

k=0 with probability 1/2

Vernam Cipher (Cont.)

$$\text{Encryption} \qquad c = m \oplus k$$

$$\text{Decryption} \qquad m = c \oplus k$$

This cryptosystem is perfectly secure under the following conditions

- The key *k* is used only one time (So, this is also called the **one-time pad**).
- The adversary is allowed only to read ciphertexts in the public channel (but he/she cannot insert and/or replace a ciphertext with another one).

Lower Bounds on Key-size

[Shannon49] For any encryption satisfying PS,

$$|K| \geq |M| \text{ and } H(K) \geq H(M).$$

- It is impossible to realize PS if H(K) < H(M) (| K | < | M |) (Shannon's impossibility).
- Vernam cipher satisfies equality of the lower bounds.

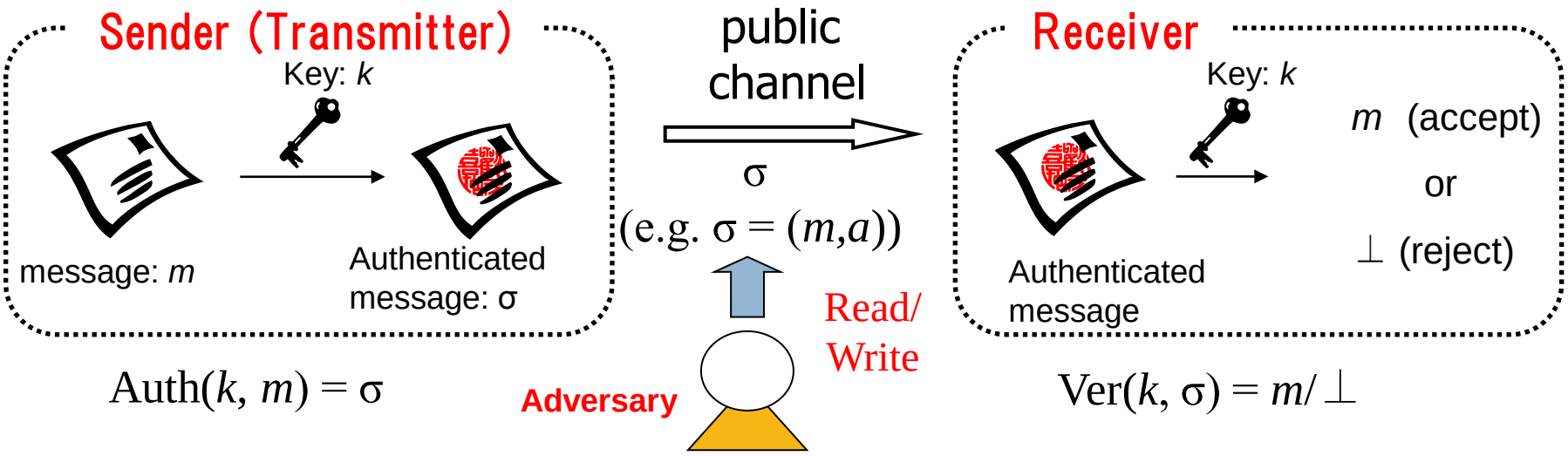
Therefore, in this sense,

- The above lower bounds are tight; and
- Vernam cipher is optimal in terms of key-size for symmetric-encryption having PS.

Authentication code (A-code)

[Gilbert, MacWilliams, Sloane 1974] [Simmons 1980's]

The authentication code is a cryptographic technique to provide **integrity**:
Receiver can check the validity of messages sent from Sender.



Attacks by the adversary

Impersonation: The adversary insert a fraudulent message into the channel

Substitution: The adversary replaces a legal authenticated message with another one.

Security The adversary with unlimited computational power succeeds in neither impersonation nor substitution effectively.

Security Formalization of A-codes

- Success probability of impersonation attack

$$P_I = \max_{\sigma} \Pr(\text{Receiver accepts } \sigma).$$

- Success probability of substitution attack

$$P_S = \max_{\sigma} \max_{\sigma' \neq \sigma} \Pr(\text{Receiver accepts } \sigma' | \sigma)$$

Definition. An A-code is said to be ε-*secure*, if it satisfies $\max(P_I, P_S) \leq \varepsilon$.

Construction for A-codes (by polynomials)

F_q : finite field with q elements

Key Generation.

$Gen \rightarrow k$:

$k := k_1 x + k_2 \in F_q[x]$.

Sender

$\sigma = (m, a)$

Receiver

Impersonation attack

Substitution attack

Authentication.

$\mathrm{Auth}(k, m) = (m, a)$:

$m \in F_q$,

$a := k_1 m + k_2$.

Verificaion.

$Ver(k, m, a) = m / \perp$:

If $a = k_1 m + k_2$, outputs m;

Otherwise, outputs $\perp$.

This construction results in a $\frac{1}{q}$-secure A-code.

Lower bound on key-size

Theorem.([Simmons84]) For any ε-secure A-code,

$$\log|K| \geq H(K) \geq -2\log\varepsilon.$$

- It is impossible to realize an ε-secure A-code if $|K| < \varepsilon^{-2}$ (i.e., with small size of keys).
- Because the previous construction meets equality of the bound,
- The above lower bound is tight; and
- The previous construction is optimal in terms of key-size.

Research Themes for Further Developing Information-Theoretic Crypto.

(i) Construction Methodology. Propose a new construction methodology for currently known cryptographic primitives by using (new) mathematical mechanisms (i.e., algebra, geometry, combinatorics etc.) or well-known primitives.

(ii) Protocol. Propose new cryptographic protocols based on the theoretical framework by Shannon/Simmons: propose a mathematical model, security formalization, (tight) bounds, and (optimal) constructions.

(iii) Theoretical Framework. Develop/discover a new theoretical framework beyond the ones by Shannon/Simmons: propose a new theoretical framework based on new security criteria which is also meaningful from a viewpoint of engineering.

Research Themes: (i) Construction Methodology

Propose a new construction methodology for currently known cryptographic primitives

- **Direct constructions** by using (new) mathematical mechanisms (e.g., algebra, geometry, combinatorics etc.)
- **Generic constructions** by well-known primitives (e.g., universal hash family, error-correcting code, extractor, etc.)

Cryptographic Primitives	Mathematical Structures used for Construction
Symmetric-key Encryption	**Polynomial over finite field**（代数）; **Latin square**, perpendicular array（組合せ論）.
A-code and its variants (extensions)	**Polynomial over finite field**（代数）; **Projective space in finite geometry**（幾何）; **Orthogonal array**, Steiner system, cover-free family（組合せ論）

Research Themes: (ii) Protocols

- Propose new cryptographic protocols based on the traditional theoretical frameworks (by Shannon/Simmons):
  - mathematical model, security formalization, (tight) bound, and (optimal) construction.

- Basic cryptographic functionality includes:
  - Encryption,
  - Authentication / Signature,
  - Key agreement,
  - Secret Sharing, etc.
- Consider additional interesting functionality.

Research Themes: (ii) Protocols

Example: Proposals from our research group

Cryptographic Protocols	Basic Functionality	Additional Functionality
Signature [HSZI00], [SHZI02]	Signature	–
Authenticated Encryption [SHZMI04]	Encryption+Authentication	–
Entity Authentication [HWS13]	Entity Authentication	–
Steganography [SM08]	Encryption	Hiding existence of ciphertexts
Group Authentication/Signature [HSHI06], [SHSM09]	Authentication/Signature	Anonymity of users
Blind Authentication/Signature [HSSM07], [HISM09], [TWS13]	Authentication/Signature	Anonymity of messages
Aggregate Authentication [KSW13]	Authentication	Secure compression
Time-release protocols [WSS12]	Enc./Auth./Key-agreement	Control by time signals
Key-insulated protocols [HHSI04], [SASM10], [SS11]	Enc./Auth./Key-agreement	Key leakage security

Research Themes: (iii) Theoretical Framework

Discover/develop a new framework beyond the ones by Shannon/Simmons:

- New security criteria or reasonable assumptions
  - by using some information-theoretic measure other than Shannon entropy; or
  - by using new reasonable (physical) assumptions (e.g., an ideal noisy channel /quantum channel is available)

which is also meaningful from a viewpoint of engineering.

Why do we consider physical assumptions?

The merit to consider physical assumptions lies in starting cryptograhic protocols with the following initial keys:

- **Short or weak shared secret-keys; or**
- **Correlated weak secret-keys (not necessarily symmetric ones); or**
- **No shared secrets.**

Known Physical Assumptions

(0) Trusted authority (or Trusted mechanism)

There is a trusted authority (or a trusted mechanism) which generates secrets and distributes them to entities in a secure way.

(1) Noisy channel [Wyner,75]

There is a (ideal) noisy channel between entities.

(2) Quantum channel [BBBW82], [BB84]

There is a (ideal) quantum channel between entities.

(3) Bounded storage [Maurer,92]

There is a source which generates a long random string, and the adversary's storage space is temporarily bounded so that the string is not stored.

Known Physical Assumptions

(4) Restricted authenticated channel (manual channel)

[Vaudenay,05], [Naor, Segev,Smith,08], [Maurer,13]

There is a unidirectional authenticated channel for a very short message between entities. (If the channel is used several times, we assume synchronization that every message arrives before the next one is sent.)

(5) Others（composite assumptions）

- **Bounded quantum-storage model**
  [Damgard,Fehr,Salvail,Schaffner,05]
- **Hybrid bounded storage model**
  [Dziembowski,Maurer,04]

Our recent results about (iii) Theoretical Framework

- **Encryption (by Shannon's model)**
  - **Security**: perfect secrecy by Shannon entropy, $H(M \mid C) = H(M)$.
  - **Tight lower bound**: $H(K) \geq H(M)$, $|K| \geq |M|$.
  - **Optimal construction**: Vernam cipher (one-time pad)
- **Encryption by [Iwamoto,Shikata,13]**
  - **Security**: ε-secrecy by conditional Renyi entropy

$$I_\alpha^{\mathrm{N}}(M;C) := R_\alpha(M) - R_\alpha^{\mathrm{N}}(M \mid C) \leq \varepsilon \qquad (\mathrm{N} \in \{\mathrm{A}, \mathrm{H}\})$$

  - **Tight lower bound**: $R_\alpha(K) \geq R_\alpha(M) - \varepsilon$ for any $\alpha \in [0, \infty]$.
  - **Optimal construction**: One-time pad with non-uniform random keys.

Conditional Rényi Entropies, Revisited

Known conditional Rényi entropies:

$$R_\alpha^C(X\,|\,Y) := \frac{1}{1-\alpha}\sum_y P_Y(y)\log\sum_x P_{X|Y}(x\,|\,y)^\alpha \qquad \textbf{[Cachin,97]}$$

$$R_\alpha^{JA}(X\,|\,Y) := \frac{1}{1-\alpha}\log\frac{\sum_{x,y} P_{XY}(x,y)^\alpha}{\sum_y P_Y(y)^\alpha} \qquad \textbf{[Jizba,Arimitsu,04]}$$

$$R_\alpha^{RW}(X\,|\,Y) := \frac{1}{1-\alpha}\max_y \log\sum_x P_{X|Y}(x\,|\,y)^\alpha \qquad \textbf{[Renner,Wolf,05]}$$

$$R_\alpha^{H}(X\,|\,Y) := \frac{1}{1-\alpha}\log\sum_y P_Y(y)\sum_x P_{X|Y}(x\,|\,y)^\alpha \qquad \textbf{[Hayashi,11]}$$

$$R_\alpha^{A}(X\,|\,Y) := \frac{\alpha}{1-\alpha}\log\sum_y P_Y(y)\left\{\sum_x P_{X|Y}(x\,|\,y)^\alpha\right\}^{1/\alpha} \qquad \textbf{[Arimoto,75]}$$

Application: Physical-Layer Security

- 安全な通信を実現するには？
  - 共通鍵暗号（AES等）、公開鍵暗号（RSA, 楕円曲線暗号等）の暗号技術を利用。
  - SSL/TLS, IEEE802.11i等の規格
  - 主に上位層で暗号技術を利用
- 物理層（Physical-Layer）について
  - 従来、電波や光等の通信媒体を介して行われる通信の信頼性確保がメイン
  - Physical-Layer Securityは、信頼性に加えて安全性も同時に実現することにより、通信全体の安全性をよりスマートに設計することを目的とする

Application: Physical-Layer Security

Level	Layer	Security Mechanism
5	Application	End-to-end crypto.
4	Transport	SSL (Secure Sockets Layer) TLS (Transport Layer Security)
3	Network	IPSec (Internet Protocol Security)
2	Link	End-to-end crypto.
1	Physical	Spreading against narrow-band jamming

TCP/IP architecture and its security mechanism

Application: Physical-Layer Security in Wireless Networks

- 無線環境におけるPhysical-Layer Securityの構成例 [Bloch et al. 2008]
  - 情報理論的に安全な鍵共有方式
  - 2者間の雑音無線通信路を仮定
  - 事前の秘密情報の共有無し：無線通信路（fading channel）の特性を利用
- 物理層（Physical-Layer）で利用するメリット
  - 【効率性】 物理層で共有した秘密鍵を、上位層で行う認証や暗号化に利用することで、処理全体をスマートにする。
  - 【安全性】上位層で利用する暗号プロトコルがどのような安全性（computational/information-theoretic security）に依拠していても、物理層で生成した情報理論的に安全な鍵を利用可能。

Application: Physical-Layer Security in Wireless Networks

- Physical-layer security (information-theoretic security)に関わるトピック
  - Cryptographic protocol design (in Cryptography)
  - Code design (in Coding Theory)
  - Cross-layer design (in Networking)
- Physical-layer securityの広がりへの期待
  - ITS (Intelligent Transport Systems), e.g., vehicular networking
  - M2M (Machine to Machine), e.g., sensor networking
  - IoT (Internet of Things), smart grids, etc.

Conclusion

(i). Develop construction methodology

- Direct construction
  - Polynomial, Projective space, Orthogonal arrays, …, **Others?**
- Generic construction
  - Universal hashing, error-correcting code, Extractor, …, **Others?**

(ii). Propose various cryptographic protocols

- Basic functionality + additional interesting functionality
- Model, Security formalization, Constructions
- **What is the additional interesting functionality?**

Conclusion

(iii). Develop/discover a new framework.

- **(Physical) Assumptions**
  - Trusted authority, Noisy channel, Bounded storage, Quantum channel, …, **Others?**
- **Security Criteria**
  - Shannon entropy, min-entropy, (smooth) Renyi entropy, statistical distance, …, **Others?**
- **What's the significance of new frameworks?**
  - It is possible with no initial shared keys, or weak secrets?
  - What is good applications?