Security and Safety, Vol. 2, 2023004 (2023)
https://doi.org/10.1051/sands/2023004
sands.edpsciences.org

Views OPEN ACCESS

Information Network

From perfect secrecy to perfect safety & security: Cryptography-based analysis of endogenous security

Liang Jin[1], Xiaoyan Hu[1,*], and Jiangxing Wu[1,2]

[1] *PLA Strategic Support Force Information Engineering University, Zhengzhou 450002, China*
[2] *Purple Mountain Laboratories: Networking, Communications and Security, Nanjing 211111, China*

Received: 16 December 2022 / Revised: 6 March 2023 / Accepted: 10 April 2023 / Published online: 06 July 2023

Abstract In this paper, we propose a conjecture that endogenous security without any prior knowledge is similar to perfect secrecy without any prior knowledge. To prove the conjecture, we first establish a cryptography model of instinct function security to transform the security problem in the network domain into an encryption problem in the cryptographic domain. Then, we inherit and apply the established ideas and means of Perfect Secrecy, and propose the concept, definition and corollaries of the perfect instinct function security (PIFS) corresponding to Perfect Secrecy. Furthermore, we take the DHR system as a concrete implementation of PIFS and propose the DHR Perfect Security Theorem corresponding to Shannon's Perfect Secrecy Theorem. Finally, we prove that the DHR satisfying the "One-Time Reconstruction" constraint is the sufficient and necessary condition to achieve perfect security. This means that the existence of PIFS is also proven. The analysis shows that any reconfigurable system can be encrypted by its construct and that the PIFS converts the one-way transparent superiority of the attacker into a double-blind problem for both the attacker and the defender, which leads to that the attacker is impossible to obtain useful construction information from the attacks and unable to find a better way than blind trial-and-error or brute-force attacks. Since the attackers are required to have the new powerful ability to crack the structure cryptogram, the threshold of cyber security is raised to at least the same level as cryptogram deciphering, thereafter the ubiquitous cyber threats are destined to be significantly reduced.

Keywords perfect instinct function security, perfect secrecy, DHR, endogenous security, One-Time Reconstruction, generalized safety and security, perfect security

Citation Jin L, Hu XY and Wu JX. From perfect secrecy to perfect safety & security: Cryptography-based analysis of endogenous security. Security and Safety 2023; **2**: 2023004. https://doi.org/10.1051/sands/2023004

1 Introduction

1.1 Endogenous safety and security problems in cyberspace

Due to the open industrial ecology at present, the number of endogenous security problems permeating the entire cyberspace is proportional to the scale of hardware and software products. On the one hand, it leads to functional safety threats such as physical failure of hardware and software that are difficult to circumvent. On the other hand, it also leads to artificially injected security vulnerabilities and deliberate backdoors that cannot be eliminated [1]. As shown in Figure 1, if there are some traditional types of uncertain turbulence within the cyber-physical systems (*e.g.*, random errors, failures, malfunctions and

[*] Corresponding author (email: ndscpls@163.com)

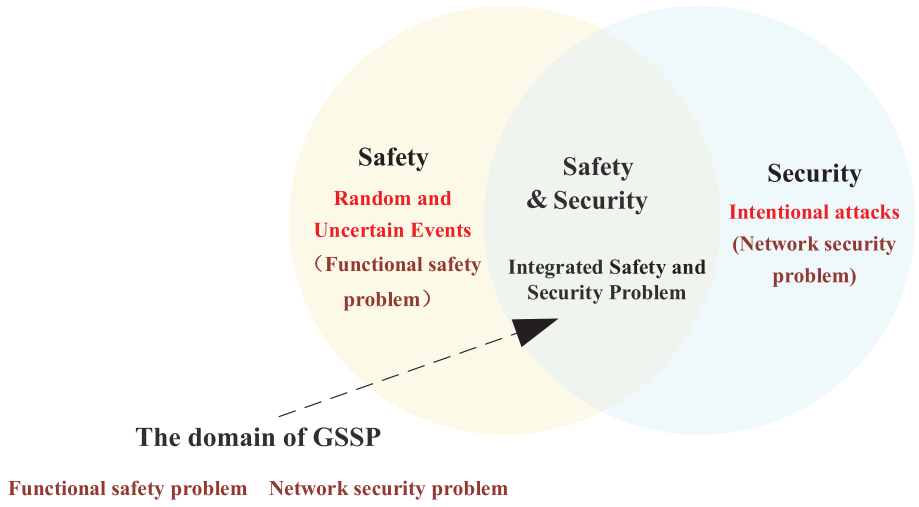
Safety
Random and Uncertain Events
（Functional safety problem）
Safety & Security
Integrated Safety and Security Problem
Security
Intentional attacks
(Network security problem)
The domain of GSSP
Functional safety problem
Network security problem

Figure 1. Generalized Safety and Security Problems domain for information physical systems

other reliability issues) as well as unknown cyberattack turbulence that is artificially aimed at the target system vulnerabilities, backdoors and other "dark functions", all of them are called Generalized Safety and Security Problems (GSSP) [2]. Most of these problems are formed by the interaction between the exogenous cause of the attack and the endogenous special or common security problems of the target object itself. In this paper, the main object considered is to investigate how to solve the problem of cyber-attacks based on unknown endogenous security problems of the target object without prior knowledge, and thus to solve the intertwined problem of functional safety and cyber security in an integrated way.

Obviously, the variety of the target object representations will create a significant cognitive barrier for the attacker [2]. This suggests that if a cyber-physical system's internal structure and operating environment exhibit variety and randomness externally, it is possible to reverse the one-way transparent superiority of attackers. Without any *a priori* knowledge, this can put the attacker in the predicament of not being able to launch an effective attack due to his inability of being cognizant of the "system architecture". If a system can make the "historical attack results" independent of the "next attack results" through the endogenously constructed properties of the system (*i.e.*, endogenous security properties), then it will have the following capabilities: no matter how much information an attacker obtains about the "historical attack results", it is of no help for him to be cognizant of the system constructs or control the "next attack result".

This is the desired effect of endogenous security, which can be expressed as follows.

$$\Pr\left(\text{next attack result}|\text{historical attack results}\right) = \Pr\left(\text{next attack result}\right), \tag{1}$$

where Pr ( ) is the probability. The above equation implies that: (1) The "next attack result" and "historical attack results" are statistically independent; (2) The mutual information between the "next attack result" and the "historical attack results" is zero; (3) The attacker cannot derive the "next attack result" by analyzing the "historical attack results", which means that the posterior probability when the "historical attack results" is known is equal to the prior probability when the "historical attack results" is unknown.

1.2 The enlightenment of perfect secrecy

It is not difficult to discover that the desired "incognizable system structure" of the endogenous security mechanism is quite similar to the perfect secrecy defined in cryptography [4]. Both have the same connotation of "A and B is independent of each other" and "Not any *a priori* knowledge is required", indicating that some endogenous security mechanisms' properties are probably similar to those of classical cryptography and can achieve similar security effects under certain conditions. To explore this issue, we first study the definition of perfect secrecy.

Definition 1. (Perfect Secrecy [4])
An encryption scheme over a message space $\mathcal{M}$ is a perfect secrecy scheme if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ $(\Pr(\mathcal{C} = c) > 0)$:

$$\Pr(M = m|\mathcal{C} = c) = \Pr(M = m), \tag{2}$$

The definition is consistent with Equation (1) in form and concept. The obvious implication is that "constructing a system in which the result of the next attack is independent of the results of the historical attacks" and "constructing a cryptographic scheme in which the plaintext is independent of the ciphertext" are likely to be coincident in principle.

The definition of perfect secrecy suggests that when the decipherer cannot obtain any information about the plaintext from the ciphertext, there is no better way to decipher the plaintext than by guessing it blindly. Note that this does not mean that the probability is 100% at which the decipherer guesses wrong, but that the decipherer cannot find a better way than a brute-force attack. This is the underlying logic of perfect secrecy, *i.e.*, by perfectly isolating the plaintext information out of the ciphertext, the defender makes it meaningless for the decipherer to analyze the ciphertext so that the decipherer has no better method than brute-force attack [11].

1.3 A conjecture

The above analysis shows that both perfect secrecy and endogenous security have the same assumptions, such as "without any prior knowledge" and "no need to consider the capabilities and the means of the attacker". In addition, they have the same desired goals, such as both Equations (1) and (2) imply the security effect of "no information about the system structure (plaintext) can be obtained from the attacked target (ciphertext)", which makes the attacker fall into a cognitive dilemma ("mimic dilemma effect"). Inspired by the above, we propose a conjecture that there are some identical or similar properties between endogenous security and perfect secrecy.

If the conjecture is true, it can provide a new perspective on the interpretation of endogenous security mechanisms using the basic principles of cryptography. More importantly, it implies that a perfect endogenous security system can be developed in network security, benefiting from the concept of perfect secrecy in information security. The "perfect security system" can maximize the cognitive dilemma (*i.e.*, maximize the randomness) and minimize the information of the defect pattern exposed during the attack, so as to ensure the realization of the instinct function to the greatest extent possible without any *a priori* or a posterior knowledge of the defect pattern, the attacker ability, the attack mode and the attack effect. Even if the attacker has all the information about the set of defect patterns in the "perfect security system", he can only attack by blind trial and error because he does not know the current construction state of the system.

This goal can be summarized by the following axiom:

Under the premise that the set of defect patterns is one-way transparent to the attacker and the defender does not have any information about the defects if the information about the defect pattern can be perfectly shielded from being obtained by the attacker while the instinct function is achieved, then there is no better way for the attacker to achieve the system non-instinct function than indiscriminate trial and error.

To prove the above conjectures and axioms, we intend to transform the GSSP into a perfect secrecy problem in the cryptographic domain with the help of the perfect secrecy principle of cryptography and propose a perfect instinct function security. The core idea lies in taking the system reconstruction as an encryption method. Randomly reconstructing the system state enables the defender to perfectly hide the internal defect pattern of the system without prior information about the defects and the attackers. In other words, system reconstruction makes no stable mapping relationship between input and output. This converts the one-way transparent superiority of the attacker into a double-blind problem for both the attacker and the defender. Furthermore, it leads to the attacker being unable to obtain useful information from the attack inputs and outputs (*i.e.*, keeping the entropy of the defect pattern from decreasing), and unable to find better attacks than blind trial-and-error and brute-force attacks. On this basis, it is shown that the DHR architecture satisfying the "One-Time Reconstruction" feature can achieve perfect instinct function security, and sufficient and necessary conditions are given. The overall logic of the paper is shown in Figure 2.

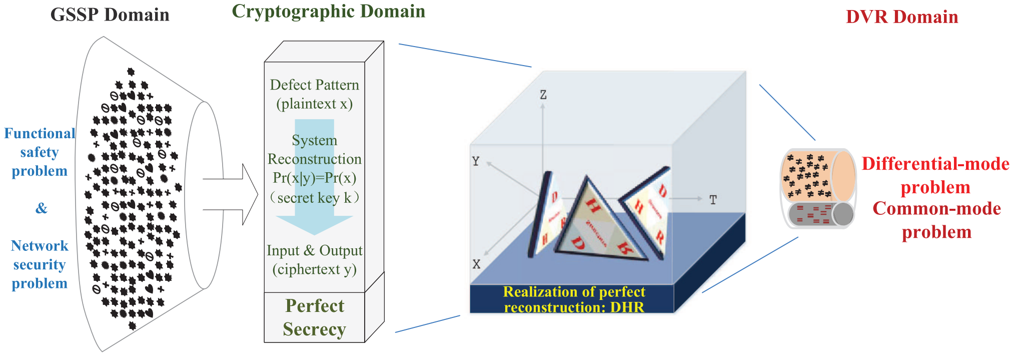
GSSP Domain
Functional safety problem
&
Network security problem
Cryptographic Domain
Defect Pattern (plaintext x)
System Reconstruction Pr(x|y)=Pr(x) (secret key k)
Input & Output (ciphertext y)
Perfect Secrecy
DVR Domain
Z
Y
X
T
Realization of perfect reconstruction: DHR
Differential-mode problem
Common-mode problem

Figure 2. The general logic of the research content

2 Perfect Instinct function Security (PIFS)

Based on the above axioms and conjectures, this section gives the mathematical model, definition, and physical interpretation of perfect functional safety and security.

2.1 The cryptography model of instinct function security

The following concepts are introduced first.

(1) Defect pattern S_t^q: The structural pattern of defects (hereinafter referred to as defect pattern) is the distribution form manifesting the survival status spectrogram of single or multiple defects on each system component at the *t-th* system output.

(2) Defect pattern space $\mathcal{S}_t^q$: The space where the defect pattern S_t^q takes its value. For example, suppose the defect patterns S_t^q may be a, b or c, then $\mathcal{S}_t^q = \{a, b, c\}$ and $|\mathcal{S}_t^q| = 3$. Note that the defect pattern space of the system is recoverable, *i.e.*, $\mathcal{S}_t^q$ at the *t-th* output can be recovered to $\mathcal{S}_{t-i}^q$ at the $t - i$ $(i = 1, 2, \ldots, t)$ output by reconstruction (including restarting, resetting, purge, backing up and replacement, *etc.*), *i.e.*, $\mathcal{S}_{t-i}^q = \mathcal{S}_t^q$ can be realized by reconstructing the defect pattern.

(3) Instinct function and non-instinct function: When the system outputs the designed or desired function for a given input, the output is called the Instinct Function (IF) with the corresponding defect pattern $S_t^q = s_{\text{IF}}^q$; otherwise, it is a Non-Instinct Function (NIF) with the corresponding defect pattern $S_t^q = s_{\text{NIF}}^q$.

(4) For a given input, the current defect pattern of the system determines uniquely whether or not to output non-instinct functionality. If the system state changes to make the defect pattern uncertain to the attacker, the critical information about the currently existing defect is hidden from the attacker.

In the above premise, the defect pattern S_t^q determines the output of the system when the input is given. Since it is hard to define the unknown defect pattern, the unknown attacker, or the unknown attack method, the probable worst case has to be considered: the information about the system components and the executor pool is public and the defects of each executor are one-way transparent to the attacker (public to the attacker, unknown to the defender). In other words, once the attacker knows the S_t^q, the attack is sure to succeed. Therefore, even if each defect exists independently, the way multiple defects are combined (*i.e.*, which state pattern the defects exist in) must be encrypted.

Correspondingly, the following corollaries are given.

(5) The plaintext that the defender intends to protect is the defect pattern S_t^q.

(6) The ciphertext known to the attacker is the input x_{t-i} and the output y_{t-i} at any $t - i\,(i = 1, 2, \ldots, t)$ moment in the past time before the present attack.

2.2 Definition

Definition 2. (Perfect Instinct Function Security, PIFS)
If for any given $\varepsilon(0 < \varepsilon < 1)$ and any input $x \in \mathcal{X}$, the defect pattern of the system at any moment t satisfies

$$\Pr\left[S_t^q = s_{\text{IF}}^q\right] = 1 - \Pr\left[S_t^q = s_{\text{NIF}}^q\right] = 1 - \varepsilon_x \geq 1 - \varepsilon, \tag{3}$$

where $\varepsilon_x (0 < \varepsilon_x \leq \varepsilon < 1)$ is the non-instinct function probability at the input x, and for any defect pattern $S_t^q \in \mathcal{S}_t^q$ at moment t, the input x_{t-i} and output y_{t-i} at any $t-i\,(i = 1, 2, \ldots, t)$ moment, if the defect pattern satisfies

$$\Pr\left[S_t^q = s_t^q | x_{t-i}, y_{t-i}\right] = \Pr\left[S_t^q = s_t^q\right], \tag{4}$$

then the system is defined as a Perfect Instinct Function Security system with parameter ε.

Assuming that a super attacker can obtain the exact defect pattern $S_{t-i}^q \in \mathcal{S}_{t-i}^q$ from the input x_{t-i} and output y_{t-i} at any moment in the past, the above equation can be transformed into

$$\Pr\left[S_t^q = s_t^q | S_{t-i}^q = s_{t-i}^q\right] = \Pr\left[S_t^q = s_t^q\right], \tag{5}$$

where $S_{t-i}^q \in \mathcal{S}_{t-i}^q$ is the defect pattern at any $t-i$ moment.

The above definition states that even if a super-strong attacker can control x_{t-i} and observe y_{t-i}, or even infer the system defect pattern S_{t-i}^q, it is of no practical significance for him to anticipate S_t^q.

It is easy to find that the key to achieving the above definition is to make S_t^q and S_{t-i}^q independent, *i.e.*, the independent reconstruction of the defect pattern. Equation (5) is the result from the perspective of the attacker, but the defect pattern may never be known to the defender. Therefore, from the perspective of the defender, it is necessary to find a "blind encryption" method without any prior knowledge of defects, *i.e.*, changing the system construction state to pull the defect pattern changed, so that the defect patterns at different moments are independent. This is because S_t^q is generally determined by the system construction, and system reconstruction is self-reliant and steerable for the defender and can be operated randomly without affecting the reliability of the instinct function.

(7) The system state S_t and the system state space $\mathcal{S}_t$: S_t is the running environment and construction of the system at the *t-th* output, which determines the defect pattern S_t^q. $\mathcal{S}_t$ is the space from which S_t takes its values.

(8) The state control key K and the system state space $\mathcal{K}$: K determines the system state at t. $\mathcal{K}$ is the space from which K takes its values.

On this basis, if the system state and the defect state are linked to change together, *i.e.*, the following assumptions are satisfied,

Assumption 1. Executor changes are equivalent to defect pattern changes (scheduling mechanism controls heterogeneity),

Assumption 2. System structure state changes are equivalent to executor changes, then the system state change is equivalent to the defect pattern change, *i.e.*, there is a "one-to-one mapping" relationship between the defect pattern and the system state. Therefore, the independence of system structure states can be derived from the independence of S_t^q and S_{t-i}^q in Equation (5). The significance to the defender is that the system reconstruction is equivalent to the reconstruction of the defect pattern, *i.e.*, the encryption of the defect pattern. Accordingly, the goal of the attacker is turned from deciphering the defect pattern equivalently to the identification of the system structure. Thus, the focus is turned from the defect pattern of Equation (5) for the attacker into the controllable system state for the defender.

$$\Pr\left[S_t = s_t | S_{t-i} = s_{t-i}\right] = \Pr\left[S_t = s_t\right], \tag{6}$$

That is, the system state S_t is independent of S_{t-i}, also known as the independent reconstruction of the system state.

Consequently, the condition of Equation (4) in Definition 2 can be equivalently replaced by the defender-oriented condition of Equation (6).

2.3 Analysis and Corollary

Definition 2 gives a perfectly secure system that "invalidates the experience of attacks". The key is to make the mapping from "historical attack results" to "future attack results" perfectly secure (*i.e.*, completely random). The analysis and several corollaries of Definition 2 are as follows.

(1) Equation (3) is the instinct condition of the system, which means that the existence and reliability of the instinct function is a prerequisite. If we disregard the instinct function and consider only the

perfect security defined by Equation (4)–(6), then any randomly reconfigured system that can "blind" the attacker satisfies the above requirements. However, the consequence is a cognitive dilemma for everyone and the instinct function cannot be achieved. The system instinct function considered in this paper should be "transparent", *i.e.*, the mapping from "historical instinct function" to "future instinct function" is essentially fixed (*i.e.*, probabilistically constant). In this meaning, the perfect system is different from the perfect secrecy, where the mapping between any plaintext and any ciphertext is completely random. This is because the scenario conditions and original requirements for system security and information security cannot be identical after all.

To make the system satisfy the Equation (3) at any time, we should prevent attackers from adding defeats by system reconstruction (including reboot, restarting, resetting, purging, backing up and replacement, *etc.*). This will leave the defect pattern space unchanged after each reconstruction to keep ε unchanged.

(2) Equations (4)–(6) are the security conditions of the system. They are consistent with the definition of perfect secrecy and mean that the defect pattern is perfectly encrypted by the state control key. Since the system structure determines the defect pattern, it can also be called the perfectly encrypted system structure. This results in the system structure being independent of each other after each system reconstruction, and this system can also be considered as a "white system with ε-probability 0/1 distribution". The "white" stems from the classical "white noise signal with Gauss distribution", where the noise at different moments is independent of each other. Since bandwidth limitation is equivalent to the existence of inertia, white noise with infinite bandwidth means that the noise signal does not have any inertia. Similarly, a white system (*i.e.*, a completely non-inertial system) will make all attack experiences worthless due to the non-inertial nature of the attacked object and therefore be perfectly secure. This means that any attack theoretical framework based on inertial systems collapses. Accordingly, any attack method is nothing but a blind trial-and-error, or an indiscriminate attack with ε as the probability of success.

(3) The meaning of the parameter ε in Definition 2 is the probability that the system generates a non-instinct function. As long as ε is given in advance, it can be made arbitrarily small (certainly, the corresponding implementation costs increase) by redundancy, heterogeneity and other mechanisms. In other words, the system can achieve the instinct function by independent reconstruction with probability 1-ε under the condition that the vulnerability, attacker, and attack method are unknown. Moreover, the attacker cannot increase ε by obtaining useful information from the results of attacks being made mutually independent by the defender. Similarly, past unintentional turbulences such as physical failures, software and hardware errors, or faults of the component do not affect the current system. Under this definition, the reliability of the system can be represented by 1-ε, where ε can be arbitrarily small implying that the probability of reliability can be arbitrarily close to 1. In other words, the GSSP of CPS can be solved integrally with "ε-perfection".

(4) Corollary 1: If there is a system satisfying Definition 2, then the "existence of perfect systems with ε as a quantitative design specification" is proved. Moreover, there are the following conclusions.

a. ε is corresponds to the quantifiable design metric and the measurable test metric for the Generalized Safety and Security System.
b. According to the definition of endogenous security [2], a system or model is said to be of endogenous security properties if there are interwoven functional safety and cyber security properties which are originated from the endogenous constructs or structure, and can be quantifiably designed and verifiably evaluated. Accordingly, if the PIFS system is proved to be achievable (*e.g.*, proving that the DHR system is a PIFS system), the existence of endogenous security is equivalently proved.

(5) Corollary 2: PIFS has the effect of keeping entropy from decreasing, for both system state and defect pattern. From Equation (5) it can be directly derived that

$$H(S_t^q|S_{t-i}^q) = H(S_t^q), \tag{7}$$

That is, under the condition that S_{t-i}^q is known, the conditional entropy of the defect pattern $H(S_t^q|S_{t-i}^q)$ is equal to its original entropy $H(S_t^q)$ [4], *i.e.*, the entropy of the defect pattern does not decrease. Similarly, according to Equation (6) we can obtain

$$H(S_t|S_{t-i}) = H(S_t), \tag{8}$$

That is, the entropy of the system state does not decrease.

2.4 Correspondence to the perfect secrecy

In summary, a PIFS system can be regarded as a system with "guaranteed instinct function as well as perfect random reconstruction", or a system within which "the construction information is kept perfectly confidential".

(1) "System defect pattern" corresponds to "plaintext" and "ciphertext". For an unencrypted system, it is obvious that an attacker can speculate the current defect pattern (plaintext) based on the previously obtained defect pattern (ciphertext). For the PIFS, the attacker only knows the probability distribution of the current defect pattern and the defect pattern space (*i.e.*, the probability distribution of the plaintext and the plaintext space), but does not know what the current specific defect pattern is (*i.e.*, does not know what the plaintext is).

(2) "System reconstruction" corresponds to "encryption". System reconstruction can be regarded as a kind of encryption of system structure, *i.e.*, a kind of "dynamic structure encryption" of hardware, software, and even the GSSPs in the system. "One-Time Reconstruction" corresponds to "One-Time Pad": the system changes the state control key every time at each reconstruction, which corresponds to the encryptor changing the key every time at each encryption.

(3)"System reconstruction control manner" corresponds to "key". The system state at any moment is determined by the state control key. This key refers to the mapping from S_{t-i}^{q} to S_{t}^{q}.

(4) The encryption of system defects is achieved by independent reconstruction of the system. Thus, any construct-empowered system can be structurally encrypted, and the encryption effect can be guaranteed by any given index ε.

(5) The "brute-force attack" corresponds to the "brute-force decipher". The method of "deducing system from its output/input" corresponds to "deducing plaintext from ciphertext" in cryptography. For a perfect system, "its input/output" is independent of the "current system state", so there is no better way to attack than "searching all inputs exhaustedly", which is the same method of "brute-force deciphering" as the perfect secrecy scheme in cryptography.

(6) PIFS turns the one-way transparent superiority of the attacker into a double-blind problem for both the attacker and the defender. Without any prior knowledge, the defender can achieve "blind shielding" against arbitrary attacks by "construct encryption" of the GSSPs within the construct. The attacker must be able to decipher the system construct if he wants to exploit the defects for a robust attack, given the known set of defect patterns and their carriers inside the system.

(7) For the instinct function, the PIFS is logically transparent, dilemma-free, and equivalently unencrypted. For the non-instinct functions, the PIFS is perfectly scrambled with a cognitive (mimic) dilemma.

(8) The "plaintext" protected by PIFS is the system defect pattern, which does not need to be transmitted to the outside world, so decryption and key distribution are unnecessary. Thus, the security of key distribution can be ignored.

(9) The "One-Time Reconstruction" of the perfect instinct function system not only reconfigures the defect pattern of the system but also maintains the defect pattern space before and after the reconstruction, *i.e.*, the defect pattern space at any two moments is equal (*e.g.*, $\mathcal{S}_{t-i}^{q} = \mathcal{S}_{t}^{q}$), which can be achieved by reconfiguring the defect pattern. The former is to encipher the defect pattern *via* "One-Time Pad", and the latter is to recover the defect pattern space (*i.e.*, to prevent attackers from inserting defects) by system reconstruction (including restarting, resetting, purging, backing up and replacement, *etc.*).

(10) The PIFS is "One-Time Reconstruction" for any two inputs or any two outputs. So it can cope with the injection vulnerability attacks with inputs only and no outputs or the backdoor defects with outputs only and no inputs. From the perspective of the PIFS definition, both can be seen as special cases of Equation (4) in Definition 2.

2.5 Key elements to achieve PIFS

Based on the above definition, we will discuss how to achieve PIFS next. As seen from the previous analysis, three core technical elements are required, namely Dynamicity/randomness, Variety/heterogeneity, and Redundancy [2], as shown in Figure 3, where the randomness can be considered a special case of dynamicity. Similarly, heterogeneity can be considered a special case of variety. Furthermore, we enumerate several possibilities to achieve PIFS.

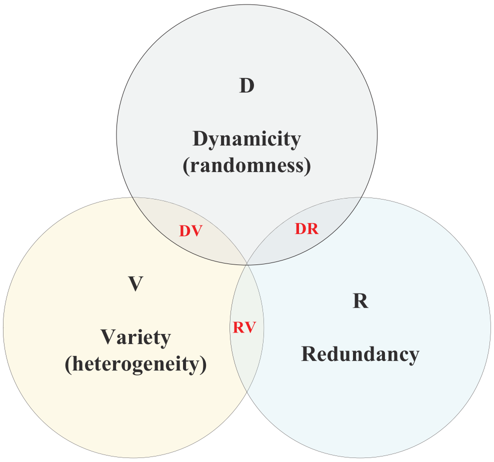

Figure 3. DVR ternary deconstruction model

(1) DV Intersection: The typical technology is the Moving Target Defense (MTD) [5]), which is characterized by randomly selecting target objects to provide service functions. Even if it is indeed a "One-Time Reconstruction" (satisfying Equations (4)–(6) of Definition 2), the lack of redundancy and the redundancy-based adjudication mechanism results in the instinct function following a 0/1 probability distribution that ε cannot be arbitrarily given (*i.e.*, the Equation (3) is not satisfied).

(2) DR intersection: Typical technique is dynamic isomorphic redundancy [5]. However, since it is isomorphic, even "One-Time Reconstruction" cannot change the defect pattern, which results in the condition Equations (4)–(6) are not satisfied.

(3) VR intersection: Typical techniques are Dissimilar Redundancy Structure (DRS) [6], which refers to multiple redundant bodies working in parallel with a selective multi-judgment mechanism. However, due to the reconstruction does not satisfy the randomness requirement of perfect security, the entropy of the system decreases with the increase of the number of attack trials, *i.e.*, it is a "dissipative system" and therefore does not satisfy the conditional Equations (4)–(6).

In summary, although D, V, and R are the key elements of perfect eigen security, any two combinations of them cannot satisfy all the requirements of Definition 2, so the next section will explore how to use the intersection of the three core elements to achieve perfect security.

3 The condition and proof that the DHR system is a PIFS system

3.1 Nature of the general DHR system

The DHR system can be used as an implementation scheme of the PIFS system. As shown in Figure 4, the DHR system architecture [7] transforms the generalized functional safety and security problem into a differential-mode or common-mode problem in the DVR domain. Its main features are: (1) By introducing feedback-control-based dynamicity, heterogeneity, and redundancy to the cyber-physical system, the DHR uses heterogeneous executors with the same instinct function to obtain the endogenous safety capability of system reconfiguration. Thus, DHR transforms GSSP into a differential-mode or common-mode problem that can be expressed by probabilistic tools in the DVR domain; (2) DHR adjudicates the outputs of heterogeneous executors with the same instinct function based on the policy adjudication mechanism of the "relatively correct" axiom [3]. As a result, the DHR can automatically sense and shield "known" and "unknown" threats. In other words, it can guarantee the provision of instinct function services even if the system is "toxic and germy" internally; (3) No prior knowledge of GSSPs or uncertain perturbations is required to counter any form of trial-and-error or blind attacks so that the attack experience is not inheritable.

The DHR architecture can achieve the designed instinct function with high probability against traditional types of random or uncertain perturbations (such as random errors, failures, malfunctions, and other reliability problems) and unknown cyber-attacks such as artificially designed vulnerabilities and

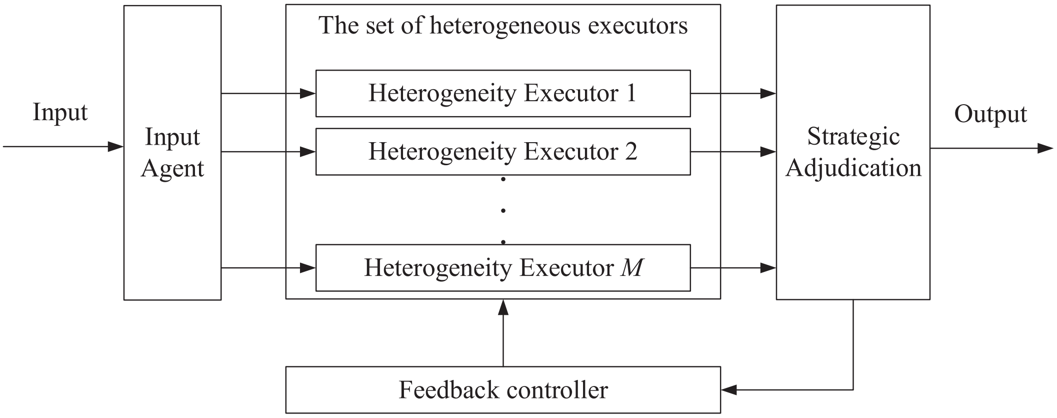

Figure 4. DHR architecture abstraction model

backdoors at the target system hardware and software. This is because the executors in the system are heterogeneous with the same instinct function, by the "relatively correct" strategic adjudication mechanism, the instinct function can be output with high probability even if there are defects in individual executors [2].

As a result, the properties of DHR can be briefly summarized as follows (which can be considered as proven) [3]:

i. Feature (1) (Seiendheit of instinct function): Since each executor has the same instinct function when the non-instinct functions of some executors are triggered, the system can be guaranteed to produce the instinct function output with a given probability (1-ε) due to the existence of the "relatively correct" strategic adjudication and feedback cleaning mechanism.

ii. Feature (2) (Determinability of differential-mode perturbation): When the non-instinct functions of some executors are triggered with differential mode, it is a deterministic event that they can be detected due to the redundancy/heterogeneity of the set of executors.

iii. Feature (3) (Escapabilty of common-mode perturbation): When the non-instinct functions of some executors are triggered simultaneously and pass the "relatively correct" strategic adjudication mechanism, a common-mode escape occurs and a non-desired output appears.

iv. Feature (4) (Reconfigurability of the state): The existence of mechanisms such as feedback control for differential-mode/common-mode perturbations, timing executor cleaning, *etc.*, makes the system operating state or construction dynamically reconfigurable.

In principle, the DHR architecture strategic adjudication mechanism does not exclude most executors with the same output, which results in the case of common-cause defects or common-mode escape a small probability. Only by making the common-mode escape a "very small probability event" as much as possible, and by making it impossible for an attacker to obtain useful information from "this event", can the maximum prevention of sensible or insensible common-mode escape become stable [2]. Therefore, whether and how the DHR architecture can achieve the PIFS is the focus of the following concerns.

3.2 DHR perfect instinct function security theorem

From the properties in the previous section, it is clear that the DHR architecture can satisfy the required instinct function condition of Equation (3) in Definition 2. Hence in the following part, we consider how to satisfy the security condition of Definition 2.

In accordance with Shannon's perfect secrecy theorem [4], as follows, we propose the DHR perfect instinct function security theorem.

Theorem 1. (Shannon's Perfect Secrecy Theorem): Let (Gen, Enc, Dec) be an encryption scheme over a message space $\mathcal{M}$ for which $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$. This scheme is perfectly secret if and only if:

(1) Every key k from $\mathcal{K}$ is chosen with equal probability $1/|\mathcal{K}|$ by the secret key generator algorithm Gen, *i.e.*, $\Pr(\mathcal{K} = k) = 1/|\mathcal{K}|$

(2) For every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$, there is one and only one secret key $k \in \mathcal{K}$ such that the plaintext m maps to the ciphertext c.

To correspond to Shannon's perfect secrecy theorem, the DHR system is analyzed as follows.

(a) For a DHR system, the encryption algorithm consists of the executor pool, the number of online executors, the adjudication strategy, the feedback mechanism [2], and so on. As in the case of cryptographic encryption schemes, the encryption algorithm is public, but the choice of executors each time is private and determined by the state control key.

(b) For heterogeneous executors with the same instinct function in the DHR architecture [8], the heterogeneous nature determines that defect patterns have variety and differentiation over different executors. Therefore, the system architecture of DHR is strongly associated with system defects, *i.e.*, there is a one-to-one mapping between defect patterns and system states.

(c) From Features (1) to (4), it is clear that the heterogeneity, redundancy, and adjudication mechanisms of the DHR architecture allow the ε in Definition 2 to be arbitrarily small. Among them, the adjudication mechanism can optimize and reduce ε by automatically sensing and shielding the "known" and "unknown" defects under the axiom of "relatively correct".

(d) Theorem 1 requires that the plaintext space remains unchanged at each encryption. For a DHR system, the system state space $\mathcal{S}_t$ before and after reconstruction can be kept constant by restarting, resetting, and cleaning at each reconstruction (*e.g.*, when differential-mode turbulence occurs). On the basis of (b), when the input and adjudication mechanisms are fixed, the invariant $\mathcal{S}_t$ implies that ε remains unchanged, thus satisfying the Equation (3) of Definition 2.

The logic of Shannon's perfect secrecy theorem is that it is valid only for $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$ encryption schemes, *i.e.*, the encryption schemes where the ciphertext space, plaintext space and secret key space are equal and that the encryption schemes have to satisfy those two sufficient and necessary conditions. Corresponding to the DHR system, it satisfies $|\mathcal{S}_t| = |\mathcal{S}_{t-i}|$ itself because the system state space is independent of time [2]. To satisfy $|\mathcal{S}_t| = |\mathcal{S}_{t-i}| = |\mathcal{K}|$, it is sufficient to normalize the secret key space of the control system states $|\mathcal{K}|$ so that for any t and i, each system state s_{t-i} at time $t-i$ and each system state s_t at time t, there is one and only one state control key k that transforms s_{t-i} to s_t, and also there is one and only one state control key k that transforms s_t to s_{t-i}.

So far, cf. the logic of Theorem 1 and its conditions, only one additional constraint over the general DHR is needed to achieve perfect instinct function security.

v. Feature (5) (Independentivity constraint): For any two inputs, the system state is reconstructed independently at each input and the probability that the system is in any state is $1/|\mathcal{K}|$. Equivalently, for any two outputs, the system state is reconstructed independently at each output and the probability that the system is in any state is $1/|\mathcal{K}|$.

Combining the above analysis, we follow the logic of Shannon's perfect secrecy law to give the DHR perfect instinct function security theorem as follows.

Theorem 2. (DHR perfect instinct function security theorem): The sufficient and necessary conditions for a DHR system satisfying Features (1)–(4) to be a perfect instinct function security system are as follows.

(Condition 1) The system changes its state each time, and picks any state control key from $\mathcal{K}$ each time with a uniform distribution (equivalently possible), *i.e.*, $\Pr(\mathcal{K} = k) = 1/|\mathcal{K}|$;

(Condition 2) For any $t$and i, there is one and only one state control key k such that transforms s_{t-i} to s_t; similarly, there is one and only one state control key k such that s_t transforms to s_{t-i};

See the Appendix for proof.

3.3 Analysis and Corollary

From the Theorem 2 in the previous subsection, it is clear that by adding the above constraints (*i.e.*, Condition 1 and Condition 2) to the general DHR system, the constrained Enhanced DHR (eDHR) system can be guaranteed to be a PIFS system with endogenous security strength ε. The ε is related to the number of executors deployed, the redundancy/heterogeneity among executors, and the adjudication/cleaning strategy, independent of the nature and the expression of defects which indicates that the DHR construct has network resilience.

The significance of the "One-Time Reconstruction" of the DHR system is not only to randomly reselect executors but also to ensure that the system state space remains unchanged by reconstruction (under the premise that there is a one-to-one mapping between the defect pattern and the system state, which means that the system reconstruction can maintain the defect pattern space at any two moments.) The former enables the DHR system to encrypt the system state directly through reconstruction, the latter enables the DHR system to recover the defect pattern space of the system (*e.g.*, to prevent attackers from injecting defects) through reconstruction (including restarting, resetting, cleaning, backing up and replacing executors).

From Feature (5), it is clear that the DHR system is a "One-Time Reconstruction" system for any two inputs or any two outputs, so it can withstand the attacks *via* injection vulnerability without outputs, or the backdoor defects that can trigger non-instinct functions and generate outputs without inputs.

4 Information-theoretic mechanism of DHR "relative correct" strategic adjudication mechanism

It is not difficult to find that the "relatively correct" strategic adjudication of DHR makes the "ciphertext" information obtained by the attacker incomplete, which is equivalent to filtering the output of each executor once more. In other words, it performs a multi-to-one (*i.e.*, high-dimension to low-dimension) "entropy reduction mapping" [9].

Equivalently, it is to impose an additional multiple-input single-output (MISO) channel and the channel response is a diverse selection of the majority with symbolic erasure. The amount of information in its output is reduced compared to that in the input. An additional equivocation is inevitably induced in the sense of information theory [10], which implies that the information of the channel input cannot be completely recovered from the channel output even if the channel response is known.

The "relative correctness" strategic adjudication is asymmetric for the defender and the attacker. It is positive to the defender and negative to the attacker, which leads to a loss of the entropy of the attacker's observation. This step is equivalent to the defender's initiative to accomplish one-way encryption of the system construction information in order to produce equivocation for the attacker during the system identification. Even if the output is known, to inverse the construction is still impossible. So this is one more fold of the means to reduce or even eliminate the "one-way transparency" to the attacker.

Therein, the loss of entropy or equivocation is related to the number of multiple inputs (heterogeneity & redundancy [2]), *i.e.*, the number of heterogeneous executors involved in the voting (*i.e.*, M). The larger the M in "M:1 mapping" is, and the larger spatial degrees of freedom in the original high-dimensional space is, then the larger the loss of spatial degrees of freedom after reduction to 1-dimensional space is, and the larger the equivocation is. When M tends to infinity (*e.g.*, the heterogeneity and redundancy tend to infinity, and the intersection of defects tends to zero), the equivocation is infinite. When the equivocation is large enough, theoretically the attacker is impossible to identify the system, *i.e.*, the defect structure pattern is perfectly shielded.

Therefore, the DHR sets the first fold of encryption by the reconstruction of the online executor, and then increases the attacker's equivocation once more by strategic adjudication, which is the second fold of encryption to the construction information before the system output, and further enhances the security.

5 Conclusion and analysis

5.1 Conjecture

This paper provides preliminary proof of the existence of the proposed conjecture that endogenous security without any prior knowledge is similar to perfect secrecy without any prior knowledge.

The logic and process of the proof are as follows. First, a cryptography model of instinct function security is established, which transforms the security problem in the network domain into the encryption problem in the cryptography domain, so that we can inherit and apply the established ideas and methods of perfect secrecy to give the concept, definition, and corollaries of Perfect Instinct Function Security.

Furthermore, we take the DHR system as a concrete implementation of PIFS. In accordance with Shannon's perfect secrecy theorem, we propose the DHR perfect security theorem and prove that the DHR system satisfying the "One-Time Reconstruction" constraint (*i.e.*, eDHR) is the sufficient and necessary condition for PIFS, which means that the existence of perfect instinct function security (hereafter referred to as "perfect security" in this section) systems is proved as well.

The extensive value of this proposition is not only to provide a brand-new perspective and method to interpret and evaluate the endogenous security mechanism *via* cryptography principles but also more importantly, to provide some enlightenment for the further improvement and development of endogenous security.

5.2 Interpretation

The proposition that both are similar holds, which means that complex network endogenous security problems can be equalized and interpreted with relatively simple and popular cryptography knowledge.

(1) From the cryptography point of view, essentially endogenous security may be the creation of encrypting the system structure in a physical manner, which discriminatively achieves encryption of non-instinct functions instead of the instinct function. An attacker who intends to exploit the internal defects of the system to carry out an attack must first decipher the structure cryptogram. The security of the system or network is converted to the secrecy of the cryptogram.

(2) Any system empowered by the construct can be encrypted by the construct itself. We argue that the encryption strength is strongly correlated with the intersection of the DVR elements and that the simultaneous presence of the DVR is the essential factor to achieve the perfect system.

(3) Since the attackers are required to have the new powerful ability to crack structure cryptogram, the threshold of cyber security is raised to at least the same level as cryptogram deciphering, thereafter the ubiquitous cyber threats are destined to be significantly reduced.

(4) Just as the One-Time Pad is a well-known cryptographic scheme for perfect secrecy, the One-Time Reconstruction DHR is a classical implementation of perfect security, especially with both instinct function achievability and perfect shielding of defect pattern, which proves the existence of the perfect system with ε as a quantitative specification, accordingly proves the existence of endogenous security from the cryptography point of view.

(5) The "Relatively Correct" adjudication means that the redundancy, heterogeneity and multimode adjudication of the DHR system takes effect simultaneously, enabling the DHR system to reduce the probability of non-instinct functions by automatically sensing and shielding "known" and "unknown" defects, and thus can be regarded as a guarantee for the existence of ε. From the engineering point of view, the greater the redundancy/heterogeneity and the abundance of multimode adjudication mechanisms the DHR has, the greater the freedom of the value space the ε has. Thus, the adjudication mechanism is an optimization means to achieve perfect security.

(6) The DHR adjudication mechanism corresponds to the Equation (3) of Definition 2. The heterogeneity, dynamicity, redundancy and cleaning mechanism of the DHR system correspond to the reconstruction in Definition 2, *i.e.*, Equations (4)–(6). So far, the DHR system corresponds perfectly to the definition of PIFS, and the connotation of the adjudication mechanism is included as well.

(7) The perfect security is suitable for generalized safety and security including functional safety and cyber security. Proving the existence of a perfect system with ε as a quantitative specification is equivalent to proving that the generalized safety and security can be of a quantifiable design and measurable verification.

(8) It has been strictly proved herein that perfect security has the nature of "keeping system defect pattern entropy from decreasing", which theoretically proves the existence of the "mimic dilemma effect" of endogenous security structure.

5.3 Enlightenment

(1) Under the open-loop conditions, *i.e.*, the assumption that there is neither any prior knowledge nor any posterior knowledge (*e.g.*, awareness and feedback), the perfect security and the perfect secrecy are theoretically equivalent in terms of encryption. The two are comparable only under the open loop premise.

Since the cryptographic encryptor cannot perceive the cryptanalyst method and its result, perfect secrecy has to assume the more severe scenario.

(2) Even under the open-loop condition, the perfect security is "encryption-only" security, *i.e.*, there is no legitimate decryption party, which avoids private key distribution, *i.e.*, one of the biggest problems in perfect secrecy applications. Therefore, the two are asymmetric in this respect. Perfect security has relative innate advantages and security gains and should be more practicable and achievable.

(3) Under closed-loop conditions, *i.e.*, without any prior knowledge but with a posterior knowledge of the attack and the ability to adjust the security strategy through feedback control, perfect security and perfect secrecy are theoretically not equivalent. For example, the "determinability of differential-mode perturbation" of the DHR makes it possible to detect the triggered non-instinct functions when they appear in differential mode, which means that the defender can apply the DHR to obtain a posterior knowledge of the system defects. This advantage may break some limitations of cryptography and allows the defender to use the feedback provided by the DHR to evolve over the primitive "blind encryption", thereby disrupting the attack chain with higher effectiveness, lower engineering complexity and more specificity.

For example, "one-time reconstruction" stems from the assumption that the open loop is available only, as does "one-time pad". It may be sufficient but not necessary in closed-loop conditions (it may be too strong and should be relaxed). At least what "one-time" is or what the optimal "one-time" interval is should be studied. For instance, the defender can use the feedback information provided by the DHR to adaptively and purposefully optimize the reconstruction timing, to make the reconstruction interval just smaller than the establishment time of the attack chain, instead of striving to reduce the reconstruction interval to an extreme extent ("each-time reconstruction"), so that the generation of the attack chain can be disrupted at a smaller cost.

(4) Consequently, under closed-loop conditions, the problem of attacking and defending over the perfect DHR system can be transformed into a game of "building an attack chain" and "breaking the attack chain". It is similar to the game of computing power between the decipherer and the computational-complexity-based encipher in traditional cryptography. Both of them cannot escape from the contradiction between the perfect vision and the feasible reality. Accordingly, it is worthwhile to trade the quantifiable and manageable loss of security for the feasibility of implementation and even a significant increase in efficiency. Since the DHR judgment feedback control mechanism provides additional degrees of freedom for the system, it is possible to further optimize the security under closed-loop conditions in the direction of "maximizing efficiency while satisfying security constraints". This will be part of the subsequent research.

(5) The perfect security under open-loop conditions makes the win-or-lose rules of the network attack-and-defence game no longer judged by which side owns more *a priori* knowledge about the other one. Both sides return to the "Stone Age" scenario without any prior knowledge. Furthermore, the network attack and defence under closed-loop conditions would return to the routine which is "easy to defend and difficult to attack". The defending side can not only encrypt itself but also sense the adversary and clean the defects *via* "differential-mode adjudication", thereby changing the overall situation from passive to active.

(6) The process that proves the existence of perfect DHR also answers the question of "how much randomness of DHR reconstruction is perfect enough without any prior knowledge", *i.e.*, how to design a "perfectly random DHR", which can be applied as a guideline for designing the randomness and dynamicity of DHR, so that the potential problems in DHR design can be re-examined from the perspective of perfect secrecy, and subsequent research can be conducted on the related issues.

(7) Thereafter it is possible to create a class of concepts, guidelines, and implementation methods for construct-enabled resilient systems and even resilient networks, which depends on future research.

(8) As the security goal is raised to the level of "perfection", the conditions imposed on the defender are generally more demanding (*e.g.*, one-time reconstruction) and correspondingly the costs become higher (perhaps not so higher for the DHR). If the pursuit is perfect security, this paper demonstrates that these costs are necessary but worthwhile. If the pursuit is a compromise between theoretical perfection and engineering implementation, the "sub-perfection", the asymptotic perfection, the average perfection, the short-time perfection, *etc.* can be defined based on this paper.

(9) Shannon proposed the concept of information entropy in [9] and pointed out that communication systems should be optimally designed in the direction of "keeping source entropy from decreasing", in which the channel coding theorem is the origin of the concept of DHR security construction coding. In the

following year, in his other book “Communication Theory of Secured Systems” [4], he pointed out how to use information theory to guide the design of secrecy systems in the direction of “keeping plaintext entropy from decreasing”, in which the perfect secrecy theorem is the origin of the perfect security in this paper. Obviously, both facts reveal the same “first principle” as holding the entropy non-decreasing. Shannon not only discovered the objective law when he pioneered the fields of both reliable communication and secure communication but also seemed to preset the drama magically for the coding-theorem-based construction and the perfect-secrecy-based PIFS. All the related issues in this field are worthy research directions for the future.

5.4 Postscript

During World War II, Shannon was responsible for researching the encryption of transoceanic telephone calls between Churchill and Roosevelt, where the primary issue was how to scientifically define and quantify 201CSecrecy” (since classical cryptography at that time was essentially mystical). Before defining the information secrecy, what the “information” is and how it is delivered must be clarified first. This led to the two profound papers after the war that was in fact strongly interconnected with internal logic [4, 9]. From the perspective of Shannon, fundamentally a cryptosystem has no different from a noisy communication system. For the encryptor, he endeavours to make the information flow as much like random noise (the “whiter”, the better) as possible while maintaining the original amount of information unchanged (*i.e.*, the instinct function). The decipherer strives to recover as much information as possible from “the noise” – mostly generated by a human.

Regardless of the present and future development of information systems and networks including security, as long as they do not break through Shannon’s information theory framework, they are destined to have an inevitable correlation due to the complete homogeneity of their theoretical roots. Specifically, the so-called “conjecture” that the three $\mathcal{S}$, *i.e.*, Secrecy, Security and Safety, are inherently related to each other, and even its proof is logically unnecessary. In this sense, there is no “discovery” or “invention” in the paper, but only a statement of objective facts.

6 Appendix: Proof of the perfect instinct function security theorem

Referring to the proof of Shannon’s Perfect Secrecy Theorem, we give the following proof of Theorem 2. For simplicity and intuition, let $S_t = M$, $\mathcal{S}_t = \mathcal{M}$, $S_{t-\tau} = C$ and $\mathcal{S}_{t-\tau} = \mathcal{C}$, where $\tau = 1, 2, \ldots, t-1$.

First, we prove the sufficiency.

According to Theorem 2-(Condition 1) and Theorem 2-(Condition 2) we have

$$\Pr\left[C = c | M = m\right] \overset{(a)}{=} \Pr\left[\mathcal{K} = k\right] \overset{(b)}{=} 1/\left|\mathcal{K}\right|, \tag{9}$$

where (a) holds because of Theorem 2-(Condition 2) and (b) holds because of Theorem 2-(Condition 1). Then, for any two system states $m_1 \in \mathcal{M}$ and $m_2 \in \mathcal{M}$ at t, and any system state $c \in \mathcal{C}$ at $t - \tau$, we have

$$\Pr\left[\mathcal{C} = c | M = m_1\right] = \Pr\left[\mathcal{C} = c | M = m_2\right] = 1/\left|\mathcal{K}\right|, \tag{10}$$

According to Lemma 2.3 in [11] (*i.e.*, an equivalent definition of perfect secrecy: perfect indistinguishability), the following equation can be derived from (10)

$$\Pr\left[M = m | C = c\right] = \Pr\left[M = m\right], \tag{11}$$

Thus, Theorem 2-(Condition 1) and Theorem 2-(Condition 2) are sufficiency.

Second, we prove that Theorem 2-(Condition 2) is necessary.

For any $c \in \mathcal{C}$ at $t - \tau$, it may stem from any system state in space $\mathcal{M}$ at t. Without losing generality, we assume that $c \in \mathcal{C}$ stems from $m_i \in \mathcal{M}$, then there may be n state control secret keys that can cause m_i at t to be transformed into the c at $t - \tau$, and these state control keys are $k_1, k_2, ..., k_n \in \mathcal{K}_i$ and satisfy $\mathcal{K}_i \in \mathcal{K}$. For another system state $m_j \in \mathcal{M}$, we also assume that the space of state control secret keys that enable $m_j \in \mathcal{M}$ to be transformed into c is $\mathcal{K}_j \in \mathcal{K}$. Based on the above assumptions, we have the following corollaries.

(a) For any i, j, $\mathcal{K}_i$ does not intersect with $\mathcal{K}_j$, *i.e.*, $\mathcal{K}_i \cap \mathcal{K}_j = \emptyset$
Suppose that $\mathcal{K}_i$ intersects with $\mathcal{K}_j$, then there must exist $k \in \mathcal{K}_i$ and $k \in \mathcal{K}_j$. This means that k satisfies "m_i is converted to c according to k" and "m_j is converted to c according to k" simultaneously, which contradicts the deterministic requirement of structure encryption(*i.e.*, the system cannot reconstruct two different states based on the same key), so $\mathcal{K}_i \cap \mathcal{K}_j = \emptyset$.

(b) For any i, there is only one state control secret key in $\mathcal{K}_i$, *i.e.* $|\mathcal{K}_i| = 1$

Since (a) holds, we can deduce that any two $\mathcal{K}_i$ are mutually disjoint, and for every system state $m_i \in \mathcal{M}$ at t, there must exist $\mathcal{K}_i \in \mathcal{K}$ such that all the state control secret keys in $\mathcal{K}_i$ satisfies "m_i is converted to c according to k". Thus, we can deduce that $\sum \mathcal{K}_i = \mathcal{K}$.

Similarly, we assume that for every $m_i \in \mathcal{M}$, there exists $m_i \in \mathcal{M}_i$ and $\mathcal{M}_i \in \mathcal{M}$, so any two $\mathcal{M}_i$ are also disjoint from each other (because any two system states in $\mathcal{M}$ are different). Then, we have $|\mathcal{M}_i| = 1$ and $\sum \mathcal{M}_i = \mathcal{M}$. And because $|\mathcal{K}| = |\mathcal{M}|$, we have $|\mathcal{K}_i| = 1$.

Thus, Theorem 2-(Condition 2) is necessary from the above (a) and (b).

Then, we prove that Theorem 2-(Condition 1) is necessary.

According to the Theorem 2-(Condition 2), for any system state $c \in \mathcal{C}$ at $t-\tau$, the system state $m_i \in \mathcal{M}$ at t is transformed into c when and only when the unique state control secret key k_i is chosen. Thus, we have $\Pr\lceil \mathcal{C} = c | \mathcal{M} = m_i \rceil = \Pr\lceil \mathcal{K} = k_i \rceil$. Similarly, the system state $m_j \in \mathcal{M}$ at t is transformed into c when and only when the unique state control secret key k_j is chosen, hence we have $\Pr\lceil \mathcal{C} = c | \mathcal{M} = m_j \rceil = \Pr\lceil \mathcal{K} = k_j \rceil$.

According to Lemma 2.3 in [11], a perfect secrecy scheme must satisfy $\Pr\lceil \mathcal{C} = c | \mathcal{M} = m_j \rceil = \Pr\lceil \mathcal{C} = c | \mathcal{M} = m_i \rceil$, *i.e.*, the probability that the system state $c \in \mathcal{C}$ stems from any two system states $m_i \in \mathcal{M}$ and $m_j \in \mathcal{M}$ is the same. Thus, for each i and j, the equation $\Pr\lceil \mathcal{K} = k_j \rceil = \Pr\lceil \mathcal{K} = k_i \rceil$ always holds, which means that each secret key is chosen with the same probability, *i.e.*, $\Pr\lceil \mathcal{K} = k \rceil = 1/|\mathcal{K}|$.

Thus, Theorem 2-(Condition 1) is necessary.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Liang Jin is mainly responsible for the formulation of overarching ideas and goals. Xiaoyan Hu is mainly responsible for writing the manuscript and theoretical derivation. Jiangxing Wu is mainly responsible for the overarching conception and revision suggestions of the manuscript.

Acknowledgements

We are grateful for the careful review and guidance of Qingfeng Cheng, Caixia Liu, Quan Ren, Lei He, Ruyun Zhang, Yangming Lou, Xinsheng Ji, and Yi Peng. Their professional backgrounds and revisions are undoubtedly helpful.

Funding

This work was supported by the National Natural Science Foundation of China (No.U22A2001), and by the National Key Research and Development Program under Grants 2022YFB2902205.

References

[1] Wu JX. Development paradigms of cyberspace endogenous safety and security (in Chinese). Sci Sin Inf 2022; **52**: 189–204.
[2] Jin L, Hu XY, Lou YM, et al. Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions. China Commun 2021; **18**: 99-114.
[3] Wu JX. Cyberspace endogenous safety and security. Engineering 2022; **15**: 179–185.
[4] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949; **28**, 656-715.
[5] Jajodia S, Ghosh AK, Swarup V, et al. Moving target Defense: Creating Asymmetric Uncertainty for Cyber Threats, Advances in Information Security. New York: Springer, 2011.
[6] Wu JX. Principles of Cyberspace Mimic Defense: General Robust Control and Endogenous Safety & Security. Beijing: Science Press, 2018.
[7] Wu JX. Cyberspace Endogenous Safety and Security: Mimic Defense and General Robust Control. Beijing: Science Press, 2020.
[8] Wu JX. Research on cyber mimic defense. J Cyber Secur 2016; **1**: 1–10.

[9] Shannon CE, Weaver W. The mathematical theory of communication. Urbana: University of Illinois Press, 1949.
[10] Shannon CE. A mathematical theory of communication. Bell Syst Tech J 1948; **27**: 379-423.
[11] Katz J and Lindell Y. Introduction to Modern Cryptography. Boca Raton: CRC Press, 2020.

Liang Jin received a Ph.D. degree from Xi'an Jiaotong University. He is currently a Professor and Ph.D. Supervisor of the PLA Strategic Support Force Information Engineering University, Zhengzhou, China. His research interests include wireless communication, physical layer security, and smart antenna.

Xiaoyan Hu received an M.S. degree and Ph.D. degree in information and communication engineering from PLA Strategic Support Force Information Engineering University. He is currently an assistant researcher at PLA Strategic Support Force Information Engineering University. His research interests include physical layer security and information security.

Jiangxing Wu received a B.S. degree from the Institute of Engineering and Technology of the PLA in 1982. He is currently a professor and the Director of China National Digital Switching System Engineering and Technological R&D Center (NDSC). He is an academician at the China Academy of Engineering. He is an active scientist in communication and information systems as well as in computer and network technologies. He created the mimic computing and mimic security theory, and developed the first mimic computer in the world. His general research interests include communication and information systems, computer architecture, and cyber security.