

Key-Distinguishing Attack on XOR Operations Under Uncertain Ciphertext

Zeben Yang¹, Yi Tian², Jun Yan³, and Zhenqiang Wu^{4, 5}

¹School of Mathematics and Statistics, Shaanxi Normal University, Xi'an, 710119, China

²School of Economics and Management, Shangluo University, Shangluo, 726000, China

³School of Mathematics and Computer Applications, Shangluo University, Shangluo, 726000, China

⁴Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, 710071, China

⁵School of Artificial Intelligence and Computer Science, Shaanxi Normal University, Xi'an, 710119, China

With the rapid development of emerging network infrastructures, including the Internet of Things (IoT), non-terrestrial networks, and edge computing, lightweight cryptography has been widely adopted in resource-constrained network devices. As the exclusive-or (XOR) operation is commonly used for linear mixing and masking, the distinguishability of its outputs over noisy channels warrants dedicated investigation. Standard models of classical cryptanalysis generally adopt an idealized noise-free assumption, under which an adversary can obtain complete and accurate ciphertexts. In practical transmission, however, channel noise and environmental interference may cause random bit flips in ciphertexts, producing uncertain ciphertext observations and severely degrading or even invalidating conventional distinguishing attacks. To address this issue, this paper constructs a noise-perturbation model based on a transition probability matrix, investigates key-bit distinguishing from repeated XOR observations over a binary asymmetric channel, and proposes a Manhattan-distance-based mean-prototype key-bit distinguishing framework. When the channel noise parameters are known, deterministic prototypes are constructed from the theoretical means of the two conditional distributions, and each key bit is classified according to the Manhattan distances between the observation vector and the two prototypes. A closed-form Gaussian approximation to the single-key-bit distinguishing success rate is derived, followed by an analysis of the special case of symmetric perturbations. When the channel noise parameters are unknown, a data-driven approach to prototype construction using method-of-moments estimation is further developed. An approximate expression for the probability of correctly distinguishing a single key bit is then derived to account for the effect of training sample size. Monte Carlo experiments compare the theoretical approximations with empirical results under different channel parameters and sample sizes, demonstrating that $p+q=1$ constitutes the non-identifiability boundary of the observation channel. The proposed method provides a low-complexity and interpretable statistical tool for XOR key-bit distinguishing in noisy network environments, as well as methodological and theoretical support for key-recovery attacks in practical network scenarios.

Index Terms—Applied cryptography, binary asymmetric channel, uncertain ciphertext, key-bit distinguishing attack, Manhattan distance.

I. INTRODUCTION

THE rapid development of the Internet of Things (IoT), edge computing, and non-terrestrial networks is driving the integration of large numbers of sensors, embedded terminals, and low-power communication devices into open networks. Compared with conventional servers and personal computers, these nodes are subject to stricter constraints on processing capability, storage capacity, power supply, and communication bandwidth [1, 2]. Ensuring both communication security and reliability under limited resources and unstable link conditions has therefore become an important issue in the design of emerging network systems [3].

The computation and storage overhead of conventional general-purpose cryptographic implementations can be difficult to accommodate on resource-constrained devices, which has motivated the development of lightweight cryptographic algorithms and implementation techniques [4, 5]. SIMON and SPECK exemplify lightweight block ciphers designed for constrained hardware [6]. Ascon, meanwhile, combines confidentiality, integrity, and implementation efficiency through lightweight authenticated encryption and hashing [7] and has

been incorporated into the NIST lightweight cryptography standards for constrained devices [8]. The exclusive-or (XOR) operation is simple to implement, incurs low hardware overhead, and is readily parallelizable; it is therefore widely used for key mixing, state updates, and data masking in lightweight cryptographic designs.

Standard models of classical cryptanalytic techniques, such as differential and linear cryptanalysis, generally assume that an adversary has access to accurate plaintext-ciphertext data, so that the relationships among plaintexts, ciphertexts, and keys remain deterministic [9–12]. In practical transmission environments, however, complex propagation conditions and interference may leave residual bit errors or introduce random bit flips into ciphertexts, resulting in uncertain and perturbed ciphertext observations [13–17]. Such uncertainty can directly disrupt the statistical features on which conventional cryptanalysis relies, causing distinguishers to fail and substantially reducing attack success rates.

Cryptanalysis in noisy environments has received increasing attention in recent years. Unlike idealized noise-free channels, practical wireless channels may introduce bit flips that pose significant challenges to conventional analytical methods. Jamieson and Balakrishnan investigated partial packet recovery in wireless networks and showed that corrupted packets

may still retain useful correct information [15]. Measurements of IEEE 802.11 links by Han et al. showed that bit-error distributions may vary across bit positions and channel conditions [16]. Schmidt et al. further observed characteristic error distributions and bit-mutation patterns in low-power wireless networks [17]. Nevertheless, research specifically addressing cryptanalysis with noisy ciphertexts remains limited. Khiabani et al. investigated linear cryptanalysis in noisy communication environments [18]. Xi et al. subsequently examined block-cipher analysis under noise interference through a case study of XOR operations, providing a direct basis for XOR distinguishing when the noise parameters are known [19]. Overall, existing studies have mainly considered key recovery when the noise parameters are known or controllable, whereas key recovery with completely unknown noise parameters has received comparatively little attention.

To address this gap, this paper develops a systematic theoretical framework that progresses from an idealized setting to a practical one. First, a unified noise-perturbed attack model is established. A transition probability matrix is used to describe bit-flip noise, the adversary's capabilities and objectives under a chosen-plaintext attack are specified, and key recovery is formulated as a statistical binary-classification problem between two bit distributions. Second, for the known-parameter setting, a Manhattan-distance-based mean-prototype attack is proposed. Deterministic prototype vectors are constructed from theoretical means, and key bits are distinguished by comparing Manhattan distances. Based on the central limit theorem, a Gaussian approximation to the single-key-bit distinguishing success rate is derived, and the performance under symmetric perturbations is analyzed. The method is then extended to the practical setting in which the noise parameters are unknown. In this data-driven attack, prototype vectors are estimated from training samples, and an approximate success-rate expression incorporating the training sample size is obtained. Finally, multiple Monte Carlo experiments are conducted to assess the agreement between the theoretical approximations and empirical results.

The remainder of this paper is organized as follows. Section II reviews the preliminaries. Section III establishes the XOR encryption attack model under noise perturbations. Section IV presents the Manhattan-distance-based mean-prototype attack for known noise parameters, including the success-rate approximation and boundary analysis. Section V extends the attack to the unknown-parameter setting, introduces the data-driven prototype attack, and analyzes the effects of estimation errors. Section VI presents Monte Carlo simulations that evaluate the agreement between the theoretical approximations and empirical results, and examines the effects of the key parameters. Section VII concludes the paper and discusses directions for future research.

II. PRELIMINARIES

This section introduces the preliminary notation and statistical tools used throughout the paper. We first define the basic symbols and system parameters. We then present the transition probability matrix that characterizes the binary asymmetric

channel. Finally, we recall the binomial distribution and the central limit theorem, which provide the basis for the Gaussian approximations used in the subsequent analysis.

A. Notation

The main symbols and operators used in this paper are defined in Table I.

TABLE I: Mathematical Notations

Symbol	Description
n	Key length in bits
N	Number of observations
p	Probability that a ciphertext bit "0" remains "0"
q	Probability that a ciphertext bit "1" remains "1"
m	Number of training vectors per class
$\Phi(\cdot)$	Cumulative distribution function of the standard normal distribution
δ	$p + q - 1$, the distinguishability margin
$\mathbf{o} = (o_1, o_2, \dots, o_N)$	Observation vector

B. Transition Probability Matrix

The transition probability matrix is a core mathematical tool for describing stochastic state transition processes. For the scenario of binary bit noise perturbation, the state space is $\{0, 1\}$. Let p denote the probability that bit 0 remains unchanged as 0, and $1 - p$ denote the probability that it flips to 1; let q denote the probability that bit 1 remains unchanged as 1, and $1 - q$ denote the probability that it flips to 0. The corresponding second-order transition probability matrix is given by:

$$Q = \begin{pmatrix} P(0|0) & P(1|0) \\ P(0|1) & P(1|1) \end{pmatrix} = \begin{pmatrix} p & 1-p \\ 1-q & q \end{pmatrix}. \quad (1)$$

Where the matrix element Q_{ij} denotes the probability that the output becomes j after perturbation, given that the original bit is i . This model is known as the Binary Asymmetric Channel (BAC) in information theory[20, 21].

C. Binomial Distribution and the Central Limit Theorem

If m independent and identically distributed Bernoulli trials are conducted, each with success probability p , then the total number of successes X follows a binomial distribution with parameters (m, p) , denoted as $X \sim B(m, p)$. Its expectation and variance are respectively:

$$\mathbb{E}[X] = mp, \quad \text{Var}(X) = mp(1 - p). \quad (2)$$

The frequency estimator $\hat{p} = X/m$ of the binomial distribution has expectation p and variance $p(1-p)/m$, and is an unbiased estimator of the true probability p .

The Central Limit Theorem is a core theorem in probability theory for approximating the distribution of sums. Let $X_1, X_2, \dots, X_n$ be independent and identically distributed random variables with finite expectation μ and variance σ^2 .

Then, as n becomes sufficiently large, the standardized sum converges in distribution to the standard normal distribution:

$$\frac{\sum_{i=1}^n X_i - n\mu}{\sqrt{n}\sigma} \xrightarrow{d} \mathcal{N}(0, 1). \quad (3)$$

This theorem serves as the core theoretical basis for deriving the closed-form Gaussian approximation of the success rate in this paper. By approximating the sum of multi-bit differences as a normal distribution, the distinguishing success rate can be calculated via the cumulative distribution function.

III. SYSTEM MODEL AND PROBLEM FORMULATION

This section presents the system and threat model, covering the XOR encryption scheme under noise perturbation, the adversary model and attack objective, and the core separability metric.

A. XOR Encryption and Noise Perturbation Model

This paper studies the most basic binary XOR encryption mechanism. For an n -bit key $\mathbf{k} \in \{0, 1\}^n$ and an n -bit plaintext $\mathbf{m} \in \{0, 1\}^n$, the original ciphertext obtained by encryption is $\mathbf{c} = \mathbf{m} \oplus \mathbf{k}$, where $\oplus$ denotes the bitwise XOR operation.

The original ciphertext is subject to independent and identically distributed bit-flip noise during transmission, and the attacker finally observes the uncertain ciphertext $\mathbf{c}'$, the model follows Fig. 1. The perturbation process of each bit follows the transition probability matrix Q , and the bits are mutually independent.

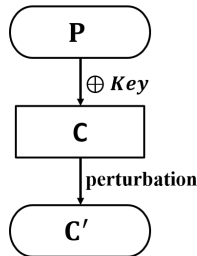


Fig. 1: Model of XOR-Perturb

B. Adversary Model and Attack Objective

This paper adopts the Chosen Plaintext Attack (CPA) model: the attacker can freely choose any plaintext and obtain the corresponding perturbed ciphertext. To simplify the analysis and highlight the core attack idea, the attacker chooses either the all-zero plaintext or the all-one plaintext for the attack. When the all-zero plaintext is chosen, the original ciphertext satisfies $\mathbf{c} = \mathbf{0} \oplus \mathbf{k} = \mathbf{k}$. When the all-one plaintext is chosen, the original ciphertext satisfies $\mathbf{c} = \mathbf{1} \oplus \mathbf{k} = \bar{\mathbf{k}}$ (i.e., the bitwise complement of the key). In both cases, the original ciphertext has a deterministic one-to-one correspondence with the key. This is a standard setting in XOR cipher analysis, which maximally highlights the impact of noise on key recovery.

The adversary knows that the encryption algorithm performs bitwise XOR operations and can obtain multiple noise-corrupted ciphertext observations generated under the same

fixed key. According to the adversary's knowledge of the channel statistics, two scenarios are considered. In the known-parameter scenario, the adversary has obtained the transition probabilities p and q through channel probing, device measurement, or prior calibration, and can therefore construct the distinguishing prototypes directly from the theoretical conditional distributions. In the unknown-parameter scenario, the adversary has no precise prior knowledge of p and q but can obtain labeled training or calibration samples from the same stationary channel, where the labels of the original input bits are known. The empirical frequencies of these samples are then used to estimate the two observation prototypes, representing a setting in which prior channel information is limited.

The attack objective is to recover the complete n -bit key, which can be performed bitwise: the value of each key bit is determined using the statistical characteristics of multiple ciphertext samples, and the complete key is obtained by concatenating the results. Therefore, the core problem reduces to single-bit binary classification, and the evaluation metric is the single-bit distinguishing success rate.

C. Core Separability Metric

The statistical characteristics of the perturbed ciphertext corresponding to the two types of key bits are fundamentally different: When the key bit $k_i = 0$, the original ciphertext is 0, and the probability of the perturbed ciphertext being 0 is p , while the probability of being 1 is $1 - p$. When the key bit $k_i = 1$, the original ciphertext is 1, and the probability of the perturbed ciphertext being 0 is $1 - q$, while the probability of being 1 is q .

We define the distinguishability measure as $\delta = p - (1 - q) = p + q - 1$. The magnitude of $|\delta|$ directly determines the degree of separability between the two distributions: a larger $|\delta|$ indicates a more significant statistical difference, making the attack easier. When $\delta = 0$ (i.e., $p + q = 1$), the two distributions completely overlap, and the attack degenerates into random guessing. This conclusion will be rigorously verified through theoretical derivations in subsequent sections.

IV. MEAN PROTOTYPE ATTACK BASED ON MANHATTAN DISTANCE WITH KNOWN NOISE PARAMETERS

This section considers the ideal scenario where the noise parameters p and q are known, and proposes a mean prototype distinguishing attack method based on Manhattan distance. Rigorous probabilistic derivations are then performed to obtain a closed-form Gaussian approximation for the single-bit distinguishing success rate.

A. Attack Basic Principle

The core idea of the mean prototype attack is using the known noise parameters, pre-construct standard statistical prototypes (i.e., theoretical mean vectors) corresponding to the two types of key bits. For the observed vector to be classified, compute its Manhattan distance to both prototypes and assign it to the closer category.

For an N -bit observed vector (i.e., N independent perturbation observations of the same key bit):

- Class 0 prototype (corresponding to key bit 0): The theoretical probability of each bit being 1 is $1 - p$, so each element of the prototype vector is $1 - p$, denoted as $\mu_0 = (1 - p, 1 - p, \dots, 1 - p) \in [0, 1]^N$;
- Class 1 prototype (corresponding to key bit 1): The theoretical probability of each bit being 1 is q , so each element of the prototype vector is q , denoted as $\mu_1 = (q, q, \dots, q) \in [0, 1]^N$.

The Manhattan distance (L1 distance) is defined as the sum of the absolute differences of the corresponding elements of two vectors. For the observed vector $\mathbf{o} = (o_1, o_2, \dots, o_N)$, its distance to the Class 0 prototype is

$$d_0 = \sum_{i=1}^N |o_i - (1 - p)|, \quad (4)$$

and its distance to the Class 1 prototype is

$$d_1 = \sum_{i=1}^N |o_i - q|. \quad (5)$$

The decision rule of the attack is:

$$\hat{k} = \begin{cases} 0, & d_0 < d_1, \\ 1, & d_0 > d_1, \\ \text{random guess}, & d_0 = d_1. \end{cases} \quad (6)$$

That is, the observed vector is classified as the corresponding key bit of the closer prototype. When the distances are equal, the probability of this event tends to 0 for large N , so its impact on the overall success rate can be neglected.

To simplify subsequent analysis, define the single-bit difference variable

$$\Delta_i = |o_i - q| - |o_i - (1 - p)|, \quad (7)$$

then the total difference variable is

$$D = \sum_{i=1}^N \Delta_i = d_1 - d_0. \quad (8)$$

The decision rule can be equivalently transformed into:

- When $D > 0$, $d_1 > d_0$, classify as 0;
- When $D < 0$, $d_1 < d_0$, classify as 1.

This equivalent transformation reduces the double distance comparison problem to a single-variable sign determination problem, greatly simplifying the subsequent probability derivation.

B. Attack Algorithm Flow

Based on the above principle, the single-bit key distinguishing algorithm with known parameters can be divided into the following steps, as formalized in Algorithm 1.

Algorithm 1 Manhattan Mean Prototype Distinguishing Attack with Known Noise Parameters

Require: Noise parameters p, q , Number of observations N , Observation bit vector $\mathbf{o} = (o_1, \dots, o_N) \in \{0, 1\}^N$ obtained via N independent noisy perturbations

Ensure: Estimated key bit $\hat{k}$

- 1: Construct class-0 theoretical prototype:

$$\mu_0 = (1 - p, \dots, 1 - p) \in [0, 1]^N$$

- 2: Construct class-1 theoretical prototype:

$$\mu_1 = (q, \dots, q) \in [0, 1]^N$$

- 3: Compute Manhattan distance d_0 from observation vector to class-0 prototype:

$$d_0 = \sum_{i=1}^N |o_i - (1 - p)|$$

- 4: Compute Manhattan distance d_1 from observation vector to class-1 prototype:

$$d_1 = \sum_{i=1}^N |o_i - q|$$

- 5: **if** $d_0 < d_1$ **then return** $\hat{k} \leftarrow 0$
- 6: **else if** $d_0 > d_1$ **then return** $\hat{k} \leftarrow 1$
- 7: **else**
- 8: Randomly return either 0 or 1
- 9: **end if**

C. Closed-Form Derivation of the Single-Bit Distinguishing Success Rate

This section derives the analytical expression for the single-bit distinguishing success rate through rigorous probabilistic analysis. The derivation consists of three steps: first, analyzing the conditional distribution of the single-bit difference variable; second, calculating its conditional expectation and variance; and finally, applying the Central Limit Theorem to approximate the total difference variable as a normal distribution, thereby obtaining the closed-form Gaussian approximation for the success rate.

1) Conditional Distribution of the Single-Bit Difference Variable

Lemma 1 Given the value of the true key bit, the single-bit difference variable Δ_i follows a two-point distribution:

- When the true key bit satisfies $k = 0$, the random variable Δ_i is defined as

$$\Delta_i = \begin{cases} \delta, & \text{with probability } p, \\ -\delta, & \text{with probability } 1 - p, \end{cases} \quad (9)$$

where $\delta = p + q - 1$ denotes the distinguishability measure defined previously.

- When the true key bit satisfies $k = 1$, the random variable Δ_i satisfies

$$\Delta_i = \begin{cases} \delta, & \text{with probability } 1 - q, \\ -\delta, & \text{with probability } q. \end{cases} \quad (10)$$

The above conclusion can be verified as follows. We only discuss the case of $k = 0$, and the case of $k = 1$ can be deduced in the same way. If $k = 0$, the observed bit o_i equals 0 with probability p and equals 1 with probability $1 - p$.

When $o_i = 0$, substituting it into the definition of the difference variable, we have

$$\begin{aligned}\Delta_i &= |0 - q| - |0 - (1 - p)| \\ &= p + q - 1 = \delta.\end{aligned}\quad (11)$$

When $o_i = 1$, we further obtain

$$\begin{aligned}\Delta_i &= |1 - q| - |1 - (1 - p)| \\ &= -(p + q - 1) = -\delta.\end{aligned}\quad (12)$$

Combining the probability distribution of o_i , we can confirm the distribution rule of Δ_i .

It can be seen that Δ_i only takes two values $\pm\delta$ for both $k = 0$ and $k = 1$, and the only difference lies in the corresponding occurrence probabilities. This symmetric property facilitates the subsequent calculation of expectation and variance.

2) Conditional Expectation and Variance

Lemma 2 For the single-bit difference variable Δ_i , its conditional expectation under different key bits is calculated as follows.

- When $k = 0$,

$$\begin{aligned}\mathbb{E}[\Delta_i | k = 0] &= p \cdot \delta + (1 - p) \cdot (-\delta) \\ &= (2p - 1)\delta.\end{aligned}\quad (13)$$

- When $k = 1$,

$$\begin{aligned}\mathbb{E}[\Delta_i | k = 1] &= (1 - q) \cdot \delta + q \cdot (-\delta) \\ &= (1 - 2q)\delta.\end{aligned}\quad (14)$$

Lemma 3 The second-order moment of the single-bit difference variable is independent of the key bit value, which always satisfies

$$\mathbb{E}[\Delta_i^2] = \delta^2. \quad (15)$$

The conditional variance is given by:

- For $k = 0$:

$$\begin{aligned}\text{Var}(\Delta_i | k = 0) &= \delta^2 - [(2p - 1)\delta]^2 \\ &= 4p(1 - p)\delta^2.\end{aligned}\quad (16)$$

- For $k = 1$:

$$\begin{aligned}\text{Var}(\Delta_i | k = 1) &= \delta^2 - [(1 - 2q)\delta]^2 \\ &= 4q(1 - q)\delta^2.\end{aligned}\quad (17)$$

Since Δ_i is always equal to δ or $-\delta$, we have

$$\Delta_i^2 = \delta^2. \quad (18)$$

Thus the second moment satisfies

$$\mathbb{E}[\Delta_i^2] = \delta^2, \quad (19)$$

which is independent of the value of the key bit. According to the variance formula

$$\text{Var}(X) = \mathbb{E}[X^2] - (\mathbb{E}[X])^2, \quad (20)$$

the conditional variance can be derived.

3) Closed-Form Gaussian Approximation of the Success Rate

Define the total difference variable

$$D = \sum_{i=1}^N \Delta_i, \quad (21)$$

which is the sum of N independent and identically distributed random variables. According to the Central Limit Theorem, D approximately obeys the normal distribution when N is sufficiently large.

If $k = 0$, we have

$$D | k = 0 \stackrel{\text{approx.}}{\sim} \mathcal{N}(N\eta_0, N\sigma_0^2), \quad (22)$$

where

$$\eta_0 = (2p - 1)\delta, \quad (23)$$

$$\sigma_0^2 = 4p(1 - p)\delta^2. \quad (24)$$

If $k = 1$, we have

$$D | k = 1 \stackrel{\text{approx.}}{\sim} \mathcal{N}(N\eta_1, N\sigma_1^2), \quad (25)$$

where

$$\eta_1 = (1 - 2q)\delta, \quad (26)$$

$$\sigma_1^2 = 4q(1 - q)\delta^2. \quad (27)$$

When the true key bit is 0, the attack succeeds if and only if $D > 0$. Standardizing the random variable D yields

$$P(D > 0 | k = 0) = P\left(\frac{D - N\eta_0}{\sqrt{N\sigma_0^2}} > \frac{-N\eta_0}{\sqrt{N\sigma_0^2}}\right). \quad (28)$$

Let $Z = \frac{D - N\eta_0}{\sqrt{N\sigma_0^2}}$, then Z approximately follows the standard normal distribution $\mathcal{N}(0, 1)$. Substitute the expressions of η_0 and σ_0 :

$$\frac{N\eta_0}{\sqrt{N\sigma_0^2}} = \frac{\sqrt{N} \cdot (2p - 1)\delta}{2\sqrt{p(1 - p)}\delta^2} = \frac{\text{sgn}(\delta) \cdot (2p - 1) \cdot \sqrt{N}}{2\sqrt{p(1 - p)}}. \quad (29)$$

The sign of δ is determined by $p + q$. If $p + q > 1$, then $\delta > 0$; if $p + q < 1$, then $\delta < 0$. Using the symmetry property of the standard normal distribution $\Phi(-x) = 1 - \Phi(x)$, all results can be uniformly expressed by the standard normal cumulative distribution function.

Similarly, for the case $k = 1$, the attack succeeds when $D < 0$. After standardization, the success probability can also be written in the form of the standard normal cumulative distribution function.

Theorem 1 (Single-bit Distinguishing Success Rate with Known Parameters) Given known noise parameters p, q , when the number of observations N is sufficiently large, the success rate of single-bit key distinguishing is given by:

$$\begin{aligned}P_{\text{success}} &= \frac{1}{2}\Phi\left(\frac{\text{sgn}(\delta) \cdot (2p - 1) \cdot \sqrt{N}}{2\sqrt{p(1 - p)}}\right) + \\ &\quad \frac{1}{2}\Phi\left(\frac{\text{sgn}(\delta) \cdot (2q - 1) \cdot \sqrt{N}}{2\sqrt{q(1 - q)}}\right).\end{aligned}\quad (30)$$

Here $\Phi(\cdot)$ denotes the cumulative distribution function of the standard normal distribution.

The i.i.d. assumption is used to obtain the simple variance expressions and the Gaussian success-rate approximations derived in this paper. If the noise is stationary but weakly correlated, the Manhattan-distance decision rule may still be applied, but the variance of the distance-difference statistic should be replaced by its long-run variance. In particular, denoting the lag-(h) autocovariance by γ_h , the variance takes the form

$$\text{Var}(D | k) = N\gamma_0 + 2 \sum_{h=1}^{N-1} (N-h)\gamma_h.$$

Positive correlation effectively reduces the number of independent observations and may make the i.i.d.-based approximation optimistic. Under burst errors or time-varying channels, the conditional distributions and the corresponding prototypes may also change over time. These cases are beyond the present model and will be investigated in future work.

The above formula is the closed-form analytical expression of the attack success rate. It reveals the relationship between the success rate, noise parameters and the number of observations. When the Manhattan-distance decision direction is aligned with both conditional distributions, the success rate increases monotonically with $\sqrt{N}$, which means that more observed samples will bring higher attack success rate.

D. Special Cases and Boundary Analysis

1) Symmetric Perturbation Case ($p = q$)

When the parameter satisfy $p = q$, the noise perturbation is symmetric. At this time, the success rates corresponding to two kinds of key bits are equal, and the success rate formula can be simplified as

$$P_{\text{success}} = \Phi \left(\frac{|2p-1| \cdot \sqrt{N}}{2\sqrt{p(1-p)}} \right). \quad (31)$$

This symmetric model corresponds to the classic Binary Symmetric Channel(BSC), which is widely adopted in practical communication and cryptanalysis scenarios. The simplified formula can be directly used to evaluate the key recovery performance under symmetric noise.

2) Non-Identifiability Boundary ($p + q = 1$)

When $p + q = 1$, the separation parameter satisfies $\delta = 0$. Under the two hypotheses that the key bit is 0 or 1, the probability of observing an output bit 0 is p in both cases, while the probability of observing an output bit 1 is $1-p = q$. Consequently, the conditional distributions induced by the two key-bit hypotheses coincide, and the observations no longer contain statistical information that can support class discrimination. Under equal prior probabilities for the two key-bit values, even the optimal decision rule can do no better than random guessing, yielding

$$P_{\text{success}} = 0.5.$$

This result shows that $p + q = 1$ is not merely a failure point caused by the selected distance metric, but an intrinsic

non-identifiability boundary of the observation model itself. Because the two conditional distributions are identical, no statistical distinguisher based solely on the available noise-corrupted observations can recover useful class information. This boundary therefore characterizes the relationship between the observation-channel conditions and the information available for key-bit distinguishing, while also providing a theoretical basis for understanding the interplay among noise perturbation, information loss, and key identifiability.

3) Large Observation Limit

As the number of observations N increases, the influence of random fluctuations on the distance-based decision decreases. Repeated observations therefore progressively reinforce the statistical trends arising from differences between the two conditional distributions, causing the attack performance to move from a finite-sample regime dominated by random fluctuations toward an asymptotic regime governed jointly by the channel parameters and the decision boundary.

Consequently, within parameter ranges where the decision direction induced by the Manhattan-distance rule is aligned with the conditional distributions, increasing N reduces the effect of sampling variability and improves the single-key-bit distinguishing success rate.

V. DATA-DRIVEN EXTENDED ATTACK WITH UNKNOWN NOISE PARAMETERS

This section extends the attack from the ideal scenario to the more realistic case with unknown noise parameters. A data-driven prototype attack based on moment estimation is proposed, a general success rate formula is derived, and the impact of estimation error on attack performance is analyzed.

A. Challenges in the Realistic Scenario

In practice, the attacker often cannot know the noise transition probabilities p and q in advance. On the one hand, the noise strength of satellite or wireless channels varies dynamically and is difficult to measure accurately. On the other hand, prior information is limited, so the complete statistical characteristics of the noise cannot be obtained. In this case, the theoretical prototype method in Section IV cannot be directly applied, since it relies on known p and q to construct prototypes.

To address these challenges, this paper proposes a data-driven attack strategy: using part of the training samples to estimate the frequency of bits in each class and constructing data-driven prototypes; the remaining samples are used as test samples for distance calculation and classification. This method does not require prior knowledge of p and q , and the attack can be completed only through observed samples, which is more suitable for the constraints of realistic scenarios.

In the unknown-parameter setting, the attacker is assumed to obtain labeled calibration samples from the same stationary channel. Such samples may be provided by pilot or reference transmissions, controlled channel probing, device testing, or a separate calibration configuration in which the transmitted class labels are known. If only unlabeled target ciphertexts are available, the two class prototypes cannot be directly estimated

by the proposed method. Moreover, when the calibration and target channels differ, increasing the training sample size reduces estimation variance but does not eliminate the resulting distributional bias.

B. Parameter Identification and Prototype Construction via Moment Estimation

Since each bit is independent and identically distributed, the sample mean is an unbiased estimator of the population expectation. This paper uses the method of moments to estimate the noise parameters.

Assume the attacker has obtained m perturbed ciphertext vectors of dimension N with known class 0 (i.e., corresponding key bit is 0), and m perturbed ciphertext vectors of dimension N with known class 1 (i.e., corresponding key bit is 1). Let $f_{0,i}$ denote the frequency of bit i being 1 in the class 0 training samples, and $f_{1,i}$ denote the frequency of bit i being 1 in the class 1 training samples.

According to the properties of the binomial distribution, the sample frequency is an unbiased estimator of the theoretical probability:

$$\mathbb{E}[f_{0,i}] = 1 - p, \quad \text{Var}(f_{0,i}) = \frac{p(1-p)}{m}, \quad (32)$$

$$\mathbb{E}[f_{1,i}] = q, \quad \text{Var}(f_{1,i}) = \frac{q(1-q)}{m}. \quad (33)$$

The data-driven prototype vectors are directly constructed from the frequencies of the training samples:

- Class 0 data prototype:

$$\hat{\mu}_0 = (f_{0,1}, f_{0,2}, \dots, f_{0,N}) \in [0, 1]^N, \quad (34)$$

- Class 1 data prototype:

$$\hat{\mu}_1 = (f_{1,1}, f_{1,2}, \dots, f_{1,N}) \in [0, 1]^N. \quad (35)$$

Although each observation o_i is binary, the estimated prototype coordinate $f_{c,i}$ is a real-valued empirical frequency in $[0, 1]$. Therefore, the Manhattan distance $|o_i - f_{c,i}|$ is computed between a binary observation and a continuous mean prototype in $\mathbb{R}^N$, which is mathematically well-defined.

As the training sample size m tends to infinity, by the law of large numbers, the sample frequency converges in probability to the true probability. Thus, the data-driven prototypes will approach the theoretical prototypes in Section IV, and the performance of the unknown-parameter attack will converge to the ideal performance with known parameters.

C. Data-Driven Distinguishing Attack Algorithm

The proposed method does not require prior numerical knowledge of p and q , but it assumes access to labeled calibration samples collected from the same or approximately stationary channel, thus offering strong adaptability to practical scenarios. For full key recovery, the above process is performed bitwise for each key position.

Algorithm 2 Data-Driven Manhattan Prototype Distinguishing Attack with Unknown Noise Parameters

Require: Number of training vectors m , Number of observations N , m training vectors with known class 0, m training vectors with known class 1 (all N -dimensional), Observation vector to be classified

Ensure: Estimated key bit $\hat{k}$

- 1: Class-0 prototype estimation: For the m training vectors labeled class 0, calculate the frequency $f_{0,i}$ that each bit position takes the value 1, and construct the data prototype of class 0:

$$\hat{\mu}_0 = (f_{0,1}, \dots, f_{0,N}) \in [0, 1]^N$$

- 2: Class-1 prototype estimation: For the m training vectors labeled class 1, calculate the frequency $f_{1,i}$ that each bit position takes the value 1, and construct the data prototype of class 1:

$$\hat{\mu}_1 = (f_{1,1}, \dots, f_{1,N}) \in [0, 1]^N$$

- 3: Distance calculation: Given test observation vector o , compute Manhattan distances to the two prototypes respectively:

$$\hat{d}_0 = \sum_{i=1}^N |o_i - f_{0,i}|, \quad \hat{d}_1 = \sum_{i=1}^N |o_i - f_{1,i}|$$

- 4: Classification decision: Compare $\hat{d}_0$ and $\hat{d}_1$, return the class with smaller distance as the estimated key bit
- 5: **if** $\hat{d}_0 < \hat{d}_1$ **then return** $\hat{k} \leftarrow 0$
- 6: **else if** $\hat{d}_0 > \hat{d}_1$ **then return** $\hat{k} \leftarrow 1$
- 7: **else**
- 8: Randomly return either 0 or 1
- 9: **end if**

D. General Success Rate Analysis Considering Estimation Errors

Due to sampling errors in the data-driven prototypes, the attack success rate in the unknown-parameter setting is lower than in the ideal known-parameter case. This section derives a general success rate formula that explicitly includes the training sample size m , which quantifies the impact of estimation error on attack performance.

1) Extended Distribution of the Single-Bit Difference Variable

In the data-driven scenario, the single-bit difference variable is defined as

$$\Delta'_i = |o_i - f_{1,i}| - |o_i - f_{0,i}|, \quad (36)$$

where $f_{0,i}$ and $f_{1,i}$ are frequency estimates obtained from m training samples, and are independent of the test observation o_i .

Following a derivation similar to that in Section IV, the difference variable takes only two values, $\pm(f_{0,i} - f_{1,i})$, when conditioned on the prototype values. Since m is typically large, by the Central Limit Theorem, both $f_{0,i}$ and $f_{1,i}$ are

approximately normally distributed. Therefore, their difference $Z_i = f_{0,i} - f_{1,i}$ is also approximately normally distributed:

$$Z_i \stackrel{\text{approx.}}{\sim} \mathcal{N}\left(-\delta, \frac{p(1-p) + q(1-q)}{m}\right), \quad (37)$$

where $\delta = p + q - 1$ is the true distinguishability measure. The expectation of $f_{0,i}$ is $1 - p$ and the expectation of $f_{1,i}$ is q , so the expectation of Z_i is

$$(1 - p) - q = 1 - p - q = -\delta. \quad (38)$$

2) Closed-form Gaussian approximation of the General Success Rate

Using the derivation framework from Section IV and incorporating the variance of the prototype estimates, the parameters of the approximate normal distribution for the total difference variable can be obtained. For the case where the true key is 0, the expectation of the total difference variable remains $N(2p - 1)\delta$, but the variance increases due to the randomness of the prototype estimates, introducing additional error terms from m .

Theorem 2 (General Single-bit Distinguishing Success Rate with Unknown Parameters) The single-bit success rate of the data-driven attack, when both the training sample size m and the number of observations N are sufficiently large, is:

$$P_{\text{success}}(m) = \frac{1}{2} \Phi\left(\frac{(2p - 1)\delta \cdot \sqrt{N}}{\sqrt{\delta^2 + \frac{p(1-p) + q(1-q)}{m} - [(2p - 1)\delta]^2}}\right) + \frac{1}{2} \Phi\left(\frac{(2q - 1)\delta \cdot \sqrt{N}}{\sqrt{\delta^2 + \frac{p(1-p) + q(1-q)}{m} - [(2q - 1)\delta]^2}}\right). \quad (39)$$

For simplicity, the formula above assumes $p + q > 1$; when $p + q < 1$ can be deduced in the same way, and the form of the success rate expression remains unchanged.

This result is the most general conclusion in this paper, which includes the ideal known-parameter case: when $m \rightarrow \infty$, the estimation error term

$$\frac{p(1-p) + q(1-q)}{m} \rightarrow 0, \quad (40)$$

and the formula for $P_{\text{success}}(m)$ reduces to the known-parameter formula in Section IV, verifying the self-consistency of the theory.

VI. SIMULATION EXPERIMENTS AND RESULT ANALYSIS

To verify the correctness of the theoretical derivations and analyze the influence of key parameters on attack performance, several sets of Monte Carlo simulation experiments are designed in this section. All experiments are implemented in Python, using the ‘numpy’ library for random number generation and numerical computation, and the ‘matplotlib’ library for result visualization. To reduce the influence of random fluctuations, each set of parameters is independently repeated 1000 times, and the average success rate is taken as the final experimental result.

A. Theoretical Validation in the Known-Parameter Scenario

This section evaluates the performance of the theoretical mean-prototype attack when the channel noise parameters are known.

We first examine the agreement between the theoretical approximation and the simulated attack results in the known-parameter scenario. Figs. 2, 3, and 4 show the empirical success rate and the theoretical approximation as functions of the number of observations N for the asymmetric high-flip-probability setting with $p = 0.3$ and $q = 0.4$, the asymmetric low-flip-probability setting with $p = 0.7$ and $q = 0.8$, and the zero-flip-probability setting with $p = 1.0$ and $q = 1.0$, respectively.

Mean Prototype Attack with Known Noise Parameters ($p=0.3, q=0.4$)

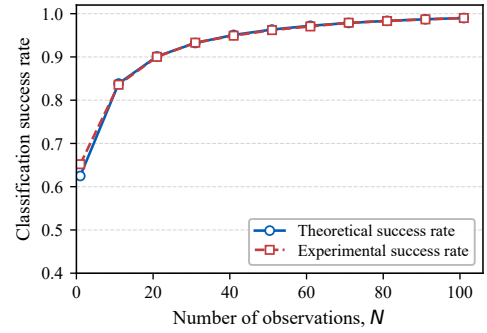


Fig. 2: Attack with known $p = 0.3, q = 0.4$

Mean Prototype Attack with Known Noise Parameters ($p=0.7, q=0.8$)

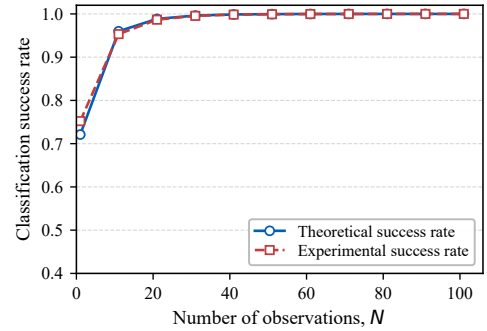


Fig. 3: Attack with known $p = 0.7, q = 0.8$

Mean Prototype Attack with Known Noise Parameters ($p=1.0, q=1.0$)

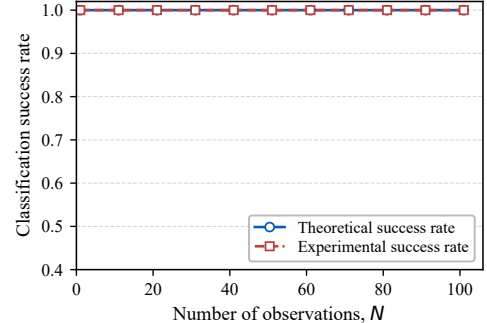


Fig. 4: Attack with known $p = 1.0, q = 1.0$

The figures show that the empirical success rates are generally in close agreement with the theoretical approximations over the tested parameter ranges, indicating that the success-rate approximation in Theorem 1 adequately characterizes the attack performance under the corresponding conditions. Slight discrepancies remain for small N , which may arise from both the finite-sample approximation error of the central limit theorem and random fluctuations in the Monte Carlo simulations. As N increases, the empirical results and theoretical approximations exhibit better overall agreement.

B. Performance Analysis in the Unknown-Parameter Scenario

This section evaluates the data-driven attack when the channel noise parameters are unknown and investigates the effect of the per-class training sample size m on the attack success rate.

We first examine the agreement between the theoretical approximation and the simulated attack results in the unknown-parameter scenario. Figs. 5, 6, and 7 show the empirical success rate and the theoretical approximation as functions of N when the per-class training sample size is fixed at $m = 1000$, corresponding to a total of $2m = 2000$ training vectors. The three parameter settings are the symmetric high-flip-probability case with $p = 0.3$ and $q = 0.3$, the asymmetric low-flip-probability case with $p = 0.8$ and $q = 0.9$, and the full-flip-probability case with $p = 0.0$ and $q = 0.0$, respectively.

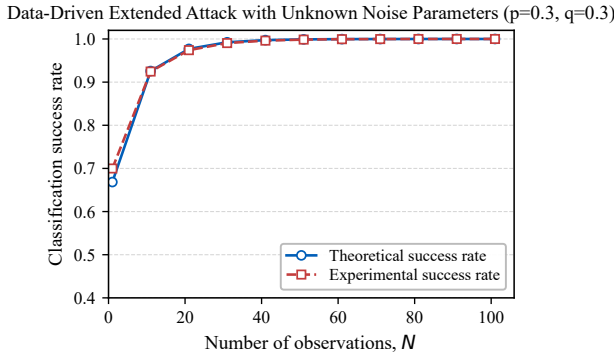


Fig. 5: Attack with unknown $p = 0.3$, $q = 0.3$

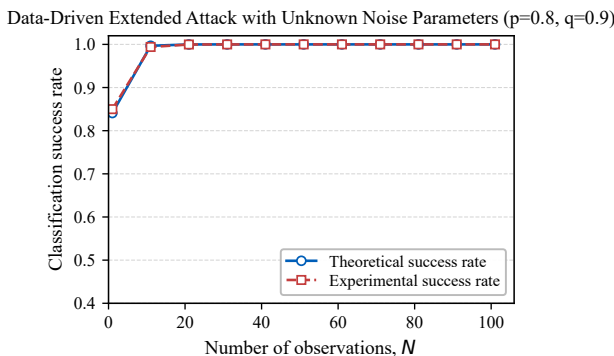


Fig. 6: Attack with unknown $p = 0.8$, $q = 0.9$

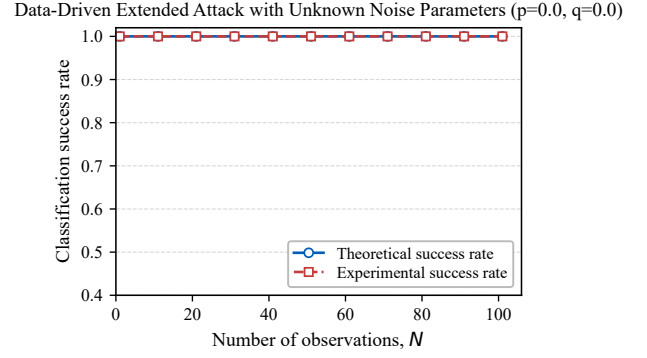


Fig. 7: Attack with unknown $p = 0.0$, $q = 0.0$

The figures demonstrate good overall agreement between the empirical success rates and the theoretical approximations over the tested parameter ranges, indicating that the success-rate approximation in Theorem 2 adequately describes the attack performance under the corresponding conditions. With $m = 1000$ training samples per class, the empirical curves remain close to the approximations given by Theorem 2, suggesting that the approximation effectively captures the prototype-estimation fluctuations introduced by finite training data.

We next investigate the effect of the per-class training sample size m on the attack success rate while holding the number of observations N and the channel parameters p and q fixed. Figs. 8, 9, and 10 show the empirical success rate and the theoretical approximation as functions of m for a fixed number of observations $N = 25$. The three parameter settings are the symmetric high-flip-probability case with $p = 0.3$ and $q = 0.3$, the asymmetric high-flip-probability case with $p = 0.2$ and $q = 0.3$, and the asymmetric low-flip-probability case with $p = 0.7$ and $q = 0.8$, respectively.

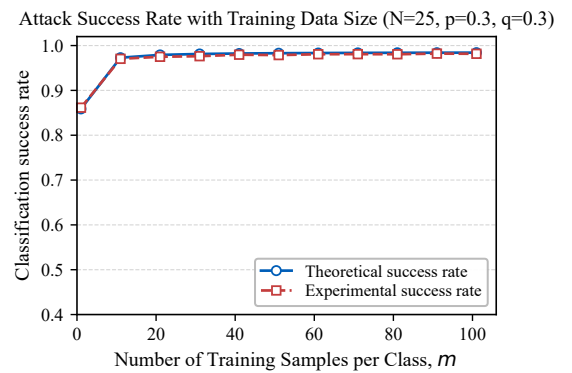
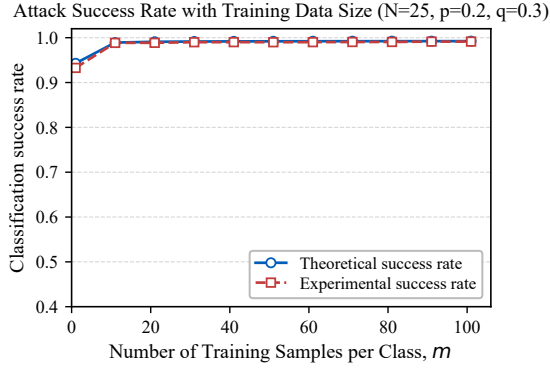
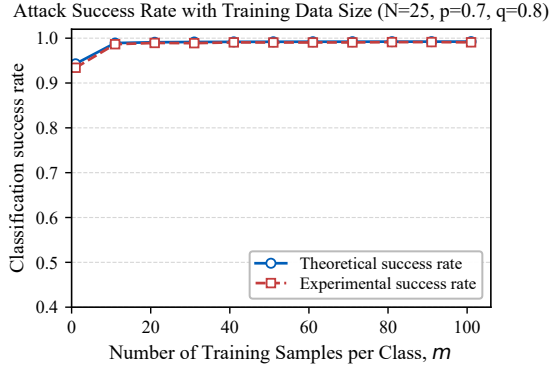


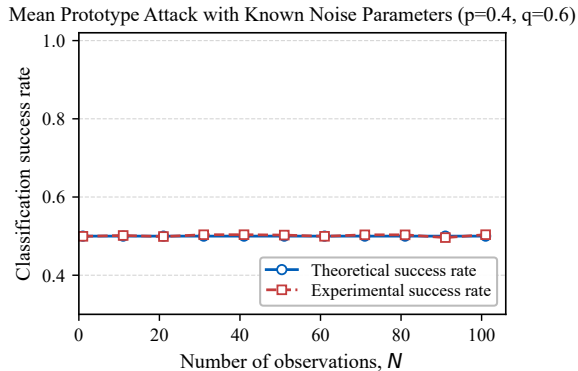
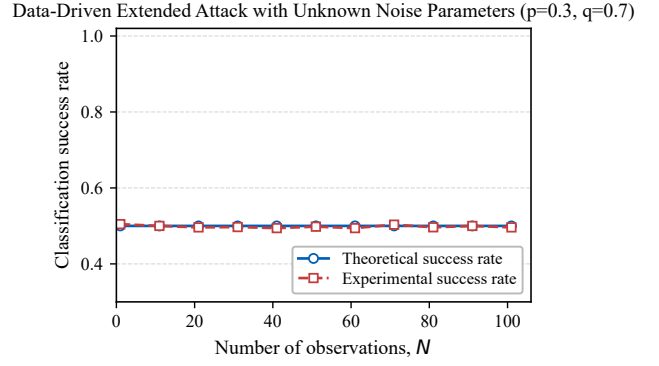
Fig. 8: Attack with unknown $p = 0.3$, $q = 0.3$, $N = 25$

Within the tested parameter settings, the prototype-estimation fluctuations decrease as the per-class training sample size m increases, and the attack performance gradually approaches the theoretical known-parameter benchmark. This trend is consistent with the estimation-error term in Theorem 2, which decreases with increasing m , and demonstrates that additional training samples can effectively mitigate the performance loss caused by finite-sample estimation.

Fig. 9: Attack with unknown $p = 0.2$, $q = 0.3$, $N = 25$ Fig. 10: Attack with unknown $p = 0.7$, $q = 0.8$, $N = 25$

C. Non-Identifiability Boundary Verification

To validate the non-identifiability boundary corresponding to $p + q = 1$, a comparative experiment was conducted with known-parameter $p = 0.4$, $q = 0.6$ and with unknown-parameter $p = 0.3$, $q = 0.7$. As shown in Figs. 11 and 12, the attack success rate remains close to 0.5 throughout the tested range of N , exhibits no significant difference from random guessing, and shows no systematic improvement as N increases. These empirical results agree with the theoretical analysis: when $p + q = 1$, the conditional observation distributions induced by key bits 0 and 1 are identical, and the attack loses its distinguishing capability.

Fig. 11: Attack with known $p = 0.4$, $q = 0.6$ Fig. 12: Attack with unknown $p = 0.3$, $q = 0.7$

This phenomenon further demonstrates that the effectiveness of a statistical attack depends not only on the number of observations and the decision rule, but is also fundamentally constrained by the information preserved by the observation channel. When channel perturbations map distinct key hypotheses to the same output distribution, the key information becomes unidentifiable at the observation level. No classifier based solely on these observations can obtain a stable advantage over random guessing. This result establishes a clear boundary for cryptanalysis under noisy conditions and highlights the fundamental role of channel statistics in evaluating attack feasibility.

D. Full Key Recovery Performance

Assuming that the bitwise recovery events are independent and share a common single-bit success rate, the probability of correctly recovering the complete n -bit key is the n th power of the single-bit success rate. For a 16-bit key, a single-bit success rate of 90% yields a full-key recovery probability of approximately 18.5%. When the single-bit success rate increases to 95%, the full-key recovery probability rises to approximately 44%; at a single-bit success rate of 99%, it reaches approximately 85%.

These results show that full-key recovery compounds the decision errors arising at individual bit positions. Even when the single-bit success rate appears high, a small number of bit errors can substantially reduce the probability of recovering the entire key correctly in a single attempt. Therefore, within parameter ranges where the Manhattan-distance decision direction is aligned with the conditional distributions, increasing the number of observations N can reduce sampling fluctuations and improve the single-bit distinguishing success rate, thereby enhancing full-key recovery performance. This analysis more precisely characterizes how performance propagates from local key-bit distinguishing to complete-key recovery and underscores the importance of bit-level decision reliability for successful full-key recovery.

VII. CONCLUSION AND FUTURE WORK

This paper investigated key-bit distinguishing from repeated XOR observations over noisy channels. To characterize random bit flips in ciphertext observations, a transition probability

matrix was employed to model a noise process whose transition probabilities may differ in the two directions, and key-bit recovery was formulated as a binary-classification problem between two conditional distributions. When the channel noise parameters were known, deterministic prototypes were constructed from the theoretical means of the two observation distributions, and each key bit was classified by comparing the Manhattan distances between the observation vector and the two prototypes. By applying the central limit theorem to the distance-difference statistic, a Gaussian approximation to the single-key-bit distinguishing success rate was obtained. When the channel noise parameters were unknown, data-driven prototypes were constructed from the empirical frequencies of training samples, and the prototype-estimation error was incorporated into the success-rate analysis.

The theoretical analysis and Monte Carlo experiments showed close agreement between the empirical results and the theoretical approximations over the tested parameter ranges. Finite training samples introduced additional statistical fluctuations, causing the attack performance to deviate from the known-parameter benchmark. As the training sample size increased, the prototype estimates became more stable and, under suitable conditions, the attack performance approached that of the known-parameter setting. In particular, when $p + q = 1$, the observation distributions induced by key bits 0 and 1 are identical; hence, no statistical distinguisher relying solely on the available observations can obtain useful class information. Therefore, $p + q = 1$ constitutes the non-identifiability boundary of the observation channel.

The proposed method has a simple computational structure and strong interpretability, and it can be used to analyze how the noise parameters, the number of observations, and the training sample size affect XOR key-bit distinguishing performance. However, the study is limited to repeated XOR observations under independent noise and relies on training or calibration data that reflect the target channel. Moreover, the central-limit-theorem-based results may exhibit approximation errors in the small-sample regime. Future work will extend the method to lightweight ciphers containing S-boxes, permutation layers, and multiple rounds; investigate burst noise, correlated noise, and time-varying channels; and derive more accurate finite-sample success-rate expressions and error bounds, thereby advancing the development of a cryptanalytic framework for complex noisy environments.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (62372076, 62572371, 62672293, 62572221) and the Shaanxi Provincial Natural Science Foundation project (2024JC-YBMS-543).

REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, *Internet of Things: A survey on enabling technologies, protocols, and applications*, IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
- [2] C. Bormann, M. Ersue, and A. Keränen, *Terminology for Constrained-Node Networks*, RFC 7228, 2014.
- [3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, *Security, privacy and trust in Internet of Things: The road ahead*, Computer Networks, vol. 76, pp. 146–164, 2015.
- [4] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, *Report on Lightweight Cryptography*, NISTIR 8114, 2017.
- [5] M. Rana, Q. Mamun, and R. Islam, *Lightweight cryptography in IoT networks: A survey*, Future Generation Computer Systems, vol. 129, pp. 77–89, 2022.
- [6] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, *The SIMON and SPECK lightweight block ciphers*, in Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6, 2015.
- [7] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläpfer, *Ascon v1.2: Lightweight authenticated encryption and hashing*, Journal of Cryptology, vol. 34, no. 3, Article 33, 2021.
- [8] M. S. Turan, K. A. McKay, D. Chang, J. Kang, and J. Kelsey, *Ascon-Based Lightweight Cryptography Standards for Constrained Devices*, NIST SP 800-232, 2025.
- [9] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, vol. 4, no. 1, pp. 3–72, 1991.
- [10] M. Matsui, *Linear cryptanalysis method for DES cipher*, in Advances in Cryptology—EUROCRYPT '93, pp. 386–397, 1994.
- [11] L. R. Knudsen, *Truncated and higher order differentials*, in Fast Software Encryption, pp. 196–211, 1995.
- [12] N. Mouha, Q. Wang, D. Gu, and B. Preneel, *Differential and linear cryptanalysis using mixed-integer linear programming*, in Information Security and Cryptology, pp. 57–76, 2012.
- [13] D. J. Costello and G. D. Forney, *Channel coding: The road to channel capacity*, Proceedings of the IEEE, vol. 95, no. 6, pp. 1150–1177, 2007.
- [14] M. Giordani and M. Zorzi, *Non-terrestrial networks in the 6G era: Challenges and opportunities*, IEEE Network, vol. 35, no. 2, pp. 244–251, 2021.
- [15] K. Jamieson and H. Balakrishnan, *PPR: Partial packet recovery for wireless networks*, ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 409–420, 2007.
- [16] B. Han, L. Ji, S. Lee, B. Bhattacharjee, and R. R. Miller, *All bits are not equal: A study of IEEE 802.11 communication bit errors*, in IEEE INFOCOM 2009, pp. 1602–1610, 2009.
- [17] F. Schmidt, M. Ceriotti, and K. Wehrle, *Bit error distribution and mutation patterns of corrupted packets in low-power wireless networks*, in Proceedings of WINTech '13, pp. 49–56, 2013.
- [18] Y. S. Khiabani, S. Wei, J. Yuan, and J. Wang, *Linear cryptanalysis against block ciphered system under noisy ciphertexts*, in IEEE GLOBECOM 2012, pp. 856–861, 2012.
- [19] Y. Xi, R. Feng, Y. Zhou, H. Liu, and L. Lu, *Analysis*

methods for block ciphers under noise interference: A case study of XOR operations, in 2025 International Conference on Satellite Internet, pp. 67–72, 2025.

- [20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley, 2006.
- [21] G. Cotardo and A. Ravagnani, *Parameters of Codes for the Binary Asymmetric Channel*, IEEE Transactions on Information Theory, vol. 68, no. 5, pp. 2941–2950, 2022.

Zeben Yang received the B.S. degree in Mathematics and Applied Mathematics from Shijiazhuang Tiedao University, Shijiazhuang, China, in 2021. He is currently pursuing the M.S. degree in Mathematics at the School of Mathematics and Statistics, Shaanxi Normal University, Xi'an, China. His research interests include cryptanalysis and information security.

Yi Tian received his B.S. degree from Kunming University of Science and Technology, in 2005, the M.S. degree from Northwest University, Xi'an, China, in 2011, and the Ph.D. degree from Wakayama University, Wakayama, Japan, in 2021. Since 2025, he has been a Professor at Shangluo University. His research interests include data analysis, wireless networks and Internet Things.

Jun Yan received the M.S. degree from the College of Earth Exploration Science and Technology, Jilin University, and the Ph.D. degree from the College of Computer Science, Shaanxi Normal University. He is currently a lecturer with Shangluo University, China. His research interests include network security and privacy preserving.

Zhenqiang Wu received the B.S. degree in 1991 from Shaanxi Normal University, China, and received the M.S. and Ph.D degrees in 2002, and 2007 respectively, all from Xidian University, China. He is currently a full professor of Shaanxi Normal University, China. Dr. Wu's research interests include computer communications networks, mainly wireless networks, network security, anonymous communication, and privacy protection etc. He is a member of ACM and senior of CCF.