UDC 004.056.5
IRSTI 81.93.29

https://doi.org/10.55452/1998-6688-2026-23-3-160-175

[1]Kapalova N.A.,
Cand. Sc. (Tech.), associate professor, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[1,2]*Khaumen A.,
PhD student, ORCID ID: 0000-0002-1670-2520,
*e-mail: haumen.armanbek@gmail.com
[1]Algazy K.T.
PhD, associate professor, ORCID ID: 0000-0003-3670-2170,
e-mail: kunbolat@mail.ru

[1]Institute of Information and Computational Technologies, CS MES, Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan

RESISTANCE OF LIGHTWEIGHT ALGORITHMS TO SIDE-CHANNEL ATTACKS

Abstract

The rapid development of the Internet of Things (IoT) and embedded systems necessitates cryptographic solutions tailored for resource-constrained devices. Lightweight cryptography provides a balance between security, performance, and low power consumption, which makes it suitable for sensors, RFID tags, medical devices, and other IoT components. However, in practice, such algorithms are vulnerable to side-channel attacks that exploit leakage of power consumption, electromagnetic emissions, or timing characteristics to recover secret keys. The most threatening among them are differential and correlation power analysis techniques, which can compromise an implementation with a relatively small number of measurements. This article presents an overview of side-channel attacks targeting lightweight algorithms such as PRESENT, SIMON, SPECK, and PRINCE. Key protection techniques are examined, including masking, hiding, operation shuffling, threshold implementations, and hardware countermeasures. A comparative analysis of their effectiveness and overhead is provided, highlighting the strengths and weaknesses of each approach. Particular attention is given to the practical applicability of protective mechanisms under the resource constraints of IoT devices. The results demonstrate that no single countermeasure is universal; the most effective solutions are combined approaches that integrate masking with hiding techniques. The study emphasizes the need for further research aimed at developing robustness evaluation methodologies and improving protective mechanisms for lightweight cryptography.

Keywords: lightweight cryptography, side channels, SCA attacks, DPA, CPA, IoT security.

Received December 5, 2025; revised February 27, April 29, 2026; accepted June 7, 2026.

Introduction

In recent years, there has been a rapid growth in the number of Internet of Things (IoT) devices, embedded systems, and intelligent sensors used in industry, transportation, healthcare, and other sectors. The expansion of such infrastructure makes the task of ensuring information security highly relevant. At the same time, most IoT devices operate under strict constraints in terms of computational power, memory capacity, and energy consumption, which complicates the use of traditional cryptographic algorithms in their classical form. Under these conditions, lightweight cryptography acquires particular importance, as it is aims to provide an acceptable level of security with minimal hardware and software overhead.

Among the most prominent lightweight algorithms are PRESENT, SIMON, SPECK, PRINCE, and their modifications, which have gained widespread use due to their simplicity of implementation

and efficiency in resource-constrained environments. However, high performance and compactness do not guarantee the robustness of such solutions at the level of practical implementation. A significant threat to similar algorithms is posed by side-channel attacks, which are based on the analysis of physical manifestations of device operation, including power consumption, electromagnetic radiation, timing delays, and fault injection. Even theoretically secure cryptographic schemes may be compromised in practice if observable leakages arise during their operation.

In this regard, improving the resistance of lightweight cryptographic algorithms to side-channel attacks is one of the important tasks of modern applied cryptography. This problem is especially significant for IoT infrastructure, where security, performance, and low resource consumption must be ensured simultaneously. The present work is devoted to analyzing the vulnerability of lightweight algorithms to this class of attacks, examining existing protection approaches and assessing their practical applicability under resource-constrained conditions.

Research objective and tasks

The objective of this study is to systematize and analyze existing side-channel attacks on lightweight cryptographic algorithms, as well as to examine and assess the protection methods applied against them.

To achieve this objective, the following tasks were defined to:

- Review the main types of side-channel attacks applicable to lightweight cryptography
- Analyze successful examples of attacks on the PRESENT, SIMON, SPECK, PRINCE algorithms and others
- Examine modern protection methods (masking, hiding, hardware- and algorithm-level approaches) and compare their effectiveness
- Systematize existing limitations and identify directions for future research

This article aims to provide a comprehensive examination of the problem of lightweight cryptography resilience to side-channel attacks and to formulate recommendations for the further development of robust solutions. It may also serve as a foundation for subsequent research focused on designing a lightweight ARX/RX-type cryptographic algorithm with enhanced resistance to side-channel attacks.

In contrast to studies focused either on individual algorithms or on specific countermeasures, the present research aims to compare representative lightweight ciphers and protection methods within a unified analytical context. The authors do not claim to develop a universal standardized evaluation methodology; instead, they consider a simplified research model that enables the identification of general relationships between the algorithm structure, the nature of leakage, and the effectiveness of basic countermeasures.

Materials and methods

Within the framework of this study, the main focus is placed on analyzing the resistance of lightweight cryptographic algorithms to side-channel attacks. Unlike classical cryptanalysis, such attacks are based not on identifying mathematical weaknesses of a cipher, but on examining the physical manifestations of its implementation that arise during the execution of cryptographic operations. These manifestations include, in particular, characteristics of power consumption, electromagnetic radiation, timing behavior, and responses to external influences.

The paper considers the most significant types of attacks of this class applicable to lightweight cryptography: SPA, DPA, CPA, electromagnetic analysis, and combined methods involving fault injection. Their selection is due to the fact that these approaches are most frequently used in assessing the practical resistance of cryptographic implementations in resource-constrained devices.

Threat model and assumptions

Within the framework of this study, the adversary is assumed to have the ability to passively observe the execution of a cryptographic algorithm on a resource-constrained device. It is assumed that the attacker knows the algorithm specification and can repeatedly obtain power traces or

equivalent leakages associated with the processing of key-dependent intermediate values, but does not have access to the secret key or the internal state of the device.

The main analysis scenario corresponds to first-order attacks, in which statistical dependencies between the observed leakage and hypotheses about intermediate data are exploited. CPA and DPA are considered the basic attack methods, while masking is evaluated as a countermeasure against attacks of this class. Active invasive manipulations, physical chip decapsulation, probing of internal interconnections, and higher-order attacks are beyond the scope of this work.

For the purpose of comparing literature data and simulation results, it is assumed that leakage is generated at the implementation level and depends both on the algorithm structure and on platform-specific features. Thus, the subject of this study is not the proof of the absolute security of a particular cipher, but rather a comparative analysis of typical factors affecting the practical vulnerability of lightweight cryptographic implementations.

Criteria for evaluating resistance and applicability

To ensure a more rigorous comparison of algorithms and countermeasures, a unified set of evaluation criteria is used in this study. In the analysis of attacks, the following factors are taken into account: the probability of successful key recovery, the minimum number of traces required to achieve a given success rate, the sensitivity of the result to the noise level, and the type of observable leakage. In the analysis of protection mechanisms, additional consideration is given to hardware and operational costs, including area overhead, power consumption, timing delays, and overall applicability in IoT devices.

This set of criteria does not claim the status of a universal evaluation standard; however, it makes it possible to compare different algorithms and countermeasures within a common system of indicators. This is especially important for lightweight cryptography, where the practical value of a solution is determined not only by its level of security, but also by the acceptable resource costs.

The proposed system of criteria is not a normalized universal methodology; however, it ensures the comparability of literature data and simulation results within a unified research context.

Types of side-channel attacks

Differential power analysis. DPA (Differential Power Analysis) is a statistical method that allows extracting key information from multiple measured power-consumption traces without physical interference with the device. A trace represents the power-versus-time dependency during the execution of a cryptographic operation.

By comparing groups of traces averaged according to the values of intermediate variables, the researcher identifies differences associated with hypothesized key bits. The quality of the attack depends on the noise level, synchronization accuracy, the choice of the selection function, and the leakage model (e.g., Hamming weight or Hamming distance).

In practice, alignment, filtering, averaging, PCA/ICA-based processing, and profiled methods (template attacks) are used to reduce the number of required traces. DPA has been successfully applied against hardware implementations of AES, DES, and lightweight block and stream ciphers [1].

Correlation power analysis. CPA (Correlation Power Analysis) is a widely used variant of DPA based on computing the correlation between measured power-consumption traces and a theoretical leakage model. The model describes how the consumed power depends on intermediate values computed under key hypotheses, most often using the Hamming-weight or Hamming-distance model.

For each hypothesis, the correlation between the predicted and measured power values is evaluated; the hypothesis with the highest correlation is considered the most likely. CPA is more efficient than classical DPA because it relies on a quantitative leakage model and requires fewer traces when the model aligns well with the actual power consumption [2].

Electromagnetic analysis. EM (Electromagnetic Analysis) attacks rely on examining the unintentional electromagnetic emissions produced by a chip during operation. Conceptually, the method is similar to DPA/CPA: EM recordings are used to extract temporal waveforms, which are then aligned and grouped, followed by applying statistical, correlation-based, or profiling techniques to recover intermediate values and the secret key.

The key advantages of EM analysis are its non-contact acquisition and high spatial resolution: small probes can be aimed at specific modules (for example, an S-box), resulting in less noisy signals. Practical EM analysis techniques include spatial scanning, time-frequency processing (STFT, wavelet analysis), and spectral visualization to isolate informative signal components [3].

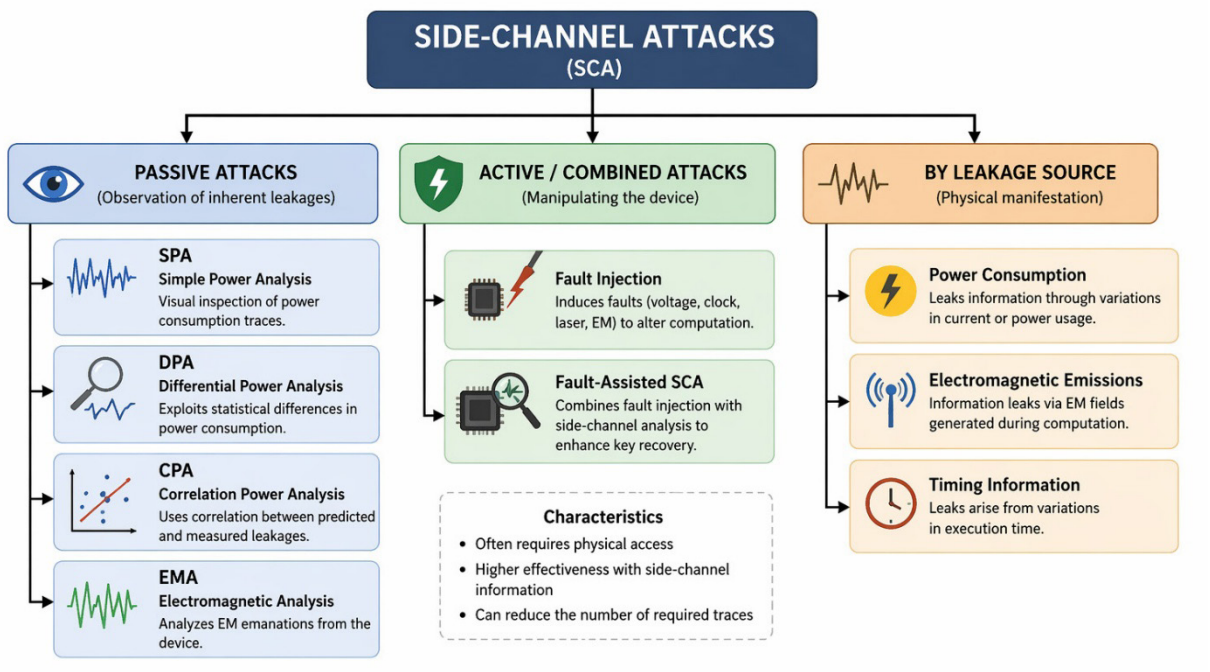

Figure 1 – Taxonomy of side-channel attacks

Figure 1 presents the generalized classification of side-channel attacks used within the framework of this study. It makes it possible to relate the type of observed leakage, the nature of the influence on the device, and the analysis method employed.

Lightweight cryptographic algorithms

After discussing side-channel attack methods, we provide a brief overview of the lightweight cryptographic algorithms examined in this article. We consider several representative schemes, their structure and characteristics, and then analyze how DPA/CPA/EM attacks affect them.

PRESENT is a compact 64-bit block cipher with an 80/128-bit key, built on an SPN structure; it features low hardware complexity and is used in embedded devices [4, 5].

SIMON is a family of block ciphers with a Feistel-like structure and simple bitwise operations (AND, XOR, rotations), optimized for hardware implementation [6, 7].

SPECK is a software-oriented ARX cipher (Add-Rotate-XOR), providing high performance on resource-constrained microcontrollers [6].

PRINCE is a low-latency block cipher with a mirrored structure, using a 64-bit block and a 128-bit key, optimized for fast hardware implementations [8].

ARX schemes (Add-Rotate-XOR structures) employ three basic operations: modular addition modulo 2^W, rotation, and XOR. Their simplicity makes them efficient on microcontrollers and flexible in terms of parameters, which makes them popular in lightweight and stream ciphers.

ARX algorithms provide a good balance between speed and simplicity but may leak information during addition, requiring careful implementation and making masking-based protection more challenging [9]. All lightweight ciphers are designed for constrained resources – small area, low power, and limited memory – but remain vulnerable to side-channel leaks; achieving security requires a trade-off between speed and protection, along with testing on real implementations [10].

It should be emphasized that cryptographic strength at the algorithmic level does not automatically guarantee resistance at the implementation level. Even efficiently designed lightweight primitives may exhibit exploitable leakage in practical environments, underscoring the necessity of systematic side-channel evaluation.

Review of scientific literature and existing approaches

This section presents the results of analyzing side-channel attacks on lightweight block ciphers that are widely used in IoT environments and embedded devices. The focus is on four algorithms: PRESENT, SIMON, SPECK, and PRINCE. For each algorithm, summarized information from experimental studies is provided, including the type of attack employed (SPA, DPA/CPA, EM analysis, fault injection), the number of collected traces, the achieved results (e.g., full or partial key recovery), and the experimental conditions (type of hardware platform, sampling rate, probes used, etc.).

Results

Results of analysis for the PRESENT algorithm

The study by Gunathilake, Lo, Buchanan, and Al-Dubai [11] focuses on the vulnerability of the lightweight cipher PRESENT-80/64 to electromagnetic attacks. The authors employed CEMA as the primary method, with SEMA and SEMFA used for additional analysis. Experiments were conducted on an Arduino Uno using NF probes and an oscilloscope with up to 2.5 GSa/s; the attack targeted the S-box.

The results showed that the radiation level increases during encryption; optimally positioning the probe perpendicular to the chip reduces noise, and the loop diameter affects sensitivity. SEMFA revealed new frequency peaks (11.25–112.66 MHz), confirming the presence of leakage.

CEMA proved to be the most effective method: with only 256 traces, 8 out of 10 key bytes (80%) could be recovered, while with 2048 traces, the probability of successful recovery reached 100%. This significantly outperforms the results of Nozaki et al., who required 12,000–17,000 traces. Recovering eight bytes substantially reduces the brute-force effort needed for the remaining two bytes.

The authors note that for the full 31-round PRESENT with protective mechanisms, the attack efficiency decreases, but EM leakage cannot be completely eliminated. The study demonstrates the practical vulnerability of PRESENT to electromagnetic attacks and underscores the necessity of applying countermeasures – masking, power balancing, and noise protections – in IoT devices.

Results of analysis for the SPECK algorithm

The study by Hasindu Gamaarachchi, Harsha Ganegoda, and Roshan Ragel [12] presents a practical analysis of the vulnerability of the SPECK algorithm to power-consumption attacks. Despite its simple ARX structure without S-boxes, the cipher was shown to be susceptible to CPA analysis.

Experiments on 8-bit and 16-bit microcontrollers demonstrated that for an 8-bit implementation, approximately 500 traces are sufficient for full key recovery (about 30 minutes), while 16-bit implementations require up to 1000 traces (about one hour). In optimized low-power systems, up to 20–30 thousand traces were needed, yet key extraction was still achievable.

The authors emphasized the importance of proper data preprocessing, since noise and untrimmed recordings lead to false correlations. The study showed that SPECK requires the deployment of dedicated countermeasures against side-channel attacks, since key recovery remains feasible even under constrained resources.

Results of analysis for the SIMON algorithm

The study by Yoshikawa and Nozaki [13] investigated the resilience of the lightweight block cipher SIMON, developed by the US NSA, against power-consumption attacks. The cipher is attractive for IoT due to its minimal hardware requirements, but such implementations are particularly vulnerable to side-channel leaks.

The authors applied HW- and HD-type DPA to a SIMON implementation on FPGA and demonstrated that the standard design exhibits correlation dependencies that enable key recovery. To mitigate this, they proposed masking registers with random values, which disrupts predictable power-consumption patterns.

Experiments confirmed the effectiveness of masking: correlation peaks disappeared and the success rate of attacks decreased. The study was the first to demonstrate the practical vulnerability of SIMON to DPA and showed that even lightweight and theoretically secure ciphers require hardware countermeasures in real-world scenarios.

Results of analysis for the PRINCE algorithm

The study by Jizheng Xue, Xiaowen Jiang, Peng Li, Wei Xi, Changbao Xu, and Kai Huang [14] investigated the vulnerability of the PRINCE block cipher in an unrolled architecture, which provides high throughput but increases leakage sensitivity. The authors proposed an optimized chosen-input attack, which allowed them to recover the key as early as the fourth round, whereas previous analyses were limited to the first two or three rounds.

Experiments showed that the CPA method is more effective than DPA and can recover the full key using approximately 150 differential inputs. Attempting to protect the implementation with Threshold Implementation (TI) significantly increased hardware costs: area by up to 441 %, delay by up to 147 %, and power consumption by up to 255 %.

The study demonstrated a serious vulnerability of PRINCE in an unrolled architecture and highlighted that existing countermeasures are too resource-intensive for lightweight systems, indicating the need for more efficient solutions.

Table 1 – Results of side-channel attack assessment on lightweight block ciphers

Algorithm	Attack type	Hardware/software platform	Number of traces	Achieved result
PRESENT-80	CEMA (correlation EM analysis)	Arduino Uno, 2.5 GSa/s oscilloscope	256 – 2048	8 out of 10 key bytes recovered (80%)
SPECK-64/128	CPA (correlation power analysis)	8-bit and 16-bit MCUs (Atmel AVR, TI MSP430)	500 – 1000 (up to 30,000 on low-power boards)	Full key recovery with ≤1000 traces
SIMON-64/128	DPA (HW/HD models)	FPGA (Xilinx Spartan-6)	≈1000	Full key recovery; masking significantly reduces the effect
PRINCE-128	CPA (chosen-input attack)	ASIC unrolled architecture	≈150 differential input sets	Key recovery up to the 4th round; TI increases costs (area +441%)
AES-128 (for comparison)	DPA / CPA	FPGA and ARM MCUs	5000 – 20,000	Full key recovery without countermeasures

The results reported in the literature are further interpreted using a unified evaluation framework that includes the type of leakage, the attack technique employed, the required number of traces, the achieved level of key recovery, and the applicability of protective measures in a resource-constrained environment.

Countermeasures Against Side-Channel Attacks

As shown in the studies by Gunathilake et al. [11], Gamaarachchi et al. [12], Yoshikawa and Nozaki [13], and Xue et al. [16], lightweight block ciphers used in IoT are vulnerable to leakage through electromagnetic emissions, timing, and power consumption.

To enhance resistance, the following protection methods are applied:

- Data masking – adding random masks to intermediate values [18, 19]
- Power balancing – equalizing consumption across all logical states [20, 21]
- Introducing randomness during execution – random delays and operation permutations [22, 23]
- Architectural solutions (Threshold Implementation, noise blocks, spatial isolation) [24, 25]
- Adding noise components – artificial current fluctuations or EM interference [26]
- Using ARX structures without S-boxes – uniform power consumption and simple implementation [27, 28]

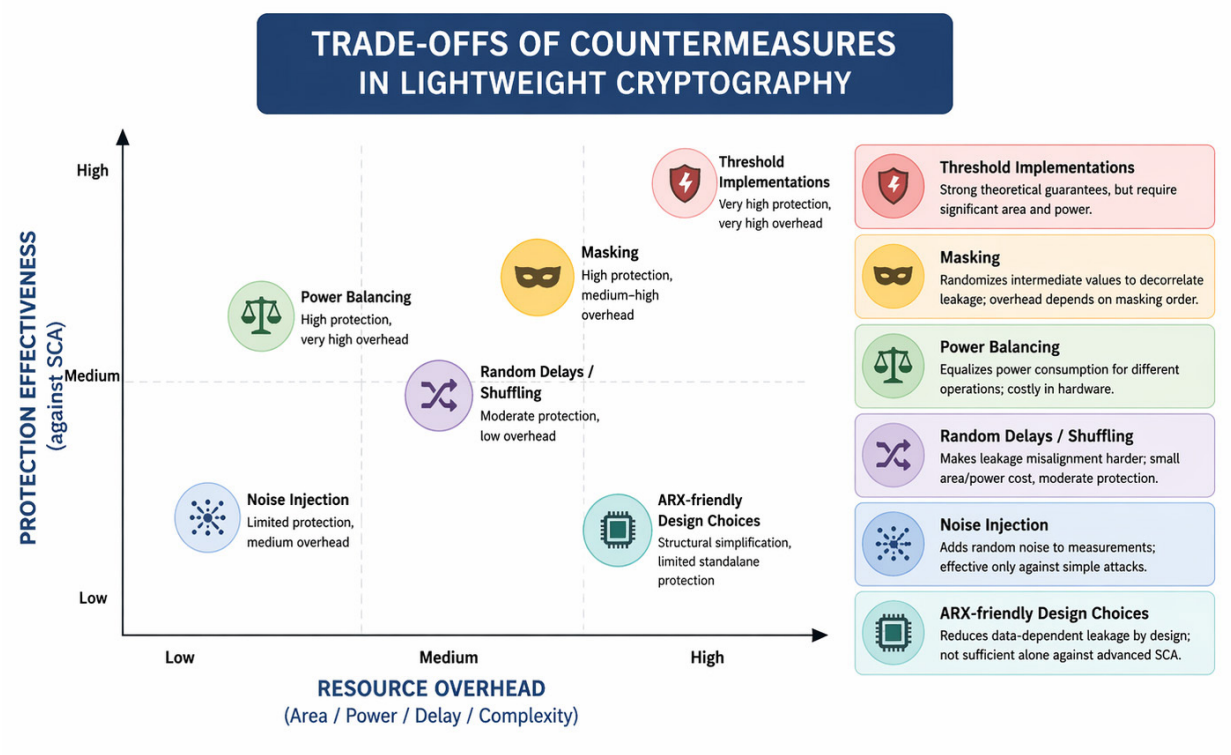

Figure 2 – Trade-offs of countermeasures in lightweight cryptography

Figure 2 schematically illustrates the trade-off between the effectiveness of the main countermeasures and their resource costs, which is particularly important for IoT devices with limited power capacity and implementation area.

Choice of cipher structure: the role of S-boxes and ARX operations

The use of S-boxes in lightweight ciphers increases the risk of side-channel leakage, since nonlinear transformations are often accompanied by non-uniform power consumption and electromagnetic radiation profiles. These characteristics make S-boxes a convenient target for DPA, CPA, and EM attacks [26, 29].

ARX structures, by contrast, do not rely on substitution tables and are based on addition, rotation, and XOR operations, which are usually implemented in a more uniform manner. This reduces the prominence of certain side-channel dependencies and makes such schemes more suitable for resource-constrained platforms [27, 28]. At the same time, ARX algorithms do not provide automatic protection against leakage and still require additional countermeasures, especially when implemented on low-power microcontrollers.

In this work, a software-based simulation of power consumption leakage was performed to experimentally evaluate the vulnerability of lightweight cryptographic algorithms to side-channel attacks. This approach makes it possible to reproduce the statistical properties of real power

measurements without the use of physical hardware, while fully controlling the noise parameters and the leakage model.

The standard Hamming weight model, widely used in the power analysis of digital devices, was employed as the leakage model. It assumes that the instantaneous power consumption of a circuit is proportional to the number of active logic lines, i.e., the number of bits set to one in the processed value. Within this model, the observed leakage is described by the following expression:

$$L = HW\left(S(p \oplus k)\right) + \varepsilon \quad (1)$$

where p is the input value (plaintext), k is the secret key, S is a nonlinear transformation (S-box), HW is the Hamming weight function, and ε is random additive Gaussian noise modeling measurement inaccuracies:

$$\varepsilon \sim \mathrm{N}(0, \sigma^2) \quad (2)$$

In the experiment, the 4-bit S-box of the PRESENT algorithm was used, and the analysis was conducted on a single nonlinear operation containing a key-dependent intermediate value. Such a simplification is standard practice in side-channel analysis research and allows one to focus on the statistical properties of the leakage.

To evaluate resistance to first-order attacks, a masking mechanism was additionally considered. In this case, the intermediate value was combined with a random mask m, unknown to the attacker, prior observation:

$$L = HW\left(S(p \oplus k) + m\right) + \varepsilon \quad (3)$$

It is assumed that the mask is uniformly distributed and generated independently for each operation.

The experiment was conducted for different noise levels and different numbers of observed traces. The following parameters were varied:

Number of traces $N \in \{50, 100, 200, 400, 800\}$

Noise standard deviation $\sigma \in \{0.5, 1.0, 1.5\}$

Presence or absence of masking

Number of independent experimental repetitions (200 runs for each configuration)

Three statistical methods were used for key recovery: correlation power analysis (CPA), classical differential power analysis (DPA), and an optimized DPA variant selecting the most informative bit (best-bit DPA).

In the CPA method, for each key hypothesis, the Pearson correlation coefficient between the measured leakage and the predicted Hamming weight was computed:

$$\rho_k = \frac{cov(L, HW_k)}{\sigma_L \sigma_{HW_{kx}}} \quad (4)$$

The key estimate was taken as the hypothesis yielding the maximum value of $|\rho_k|$.

In the DPA method, traces were divided into two groups depending on the value of a selected bit of the intermediate result, after which the difference of means was computed:

$$D_k = |\mu_1 - \mu_0| \quad (5)$$

In the optimized DPA variant, the computation was performed for all bits, and for each key hypothesis, the maximum statistic was selected.

The correctness of key recovery was verified using the statistical peak principle. For all key hypotheses, the corresponding statistic was computed, and it was analyzed whether a pronounced maximum occurred at the correct key hypothesis.

Discussion

The literature review and simulation results show that the resistance of lightweight algorithms to side-channel attacks is determined not only by their cryptographic design, but also by implementation-specific features. The most vulnerable solutions are those in which key-dependent intermediate values exhibit pronounced statistical dependencies in power consumption or electromagnetic radiation.

The obtained results are consistent with the findings reported in published studies on the PRESENT, SIMON, SPECK, and PRINCE algorithms: even with a limited number of traces, key-related information can be recovered in the absence of countermeasures [11–17]. The simulation performed in this work also demonstrated that CPA outperforms DPA in terms of efficiency, while masking significantly reduces the probability of successful key recovery.

The integration of literature data and simulation results within the proposed evaluation criteria made it possible to compare not only individual algorithms, but also the practical applicability of basic countermeasures under resource constraints, although this approach does not claim to represent a universal standardized methodology.

Thus, in the design of lightweight cryptographic solutions, the most promising direction is not the selection of a single “ideal” type of cipher, but rather the combination of structures suitable for resource-constrained implementation with mechanisms for mitigating side-channel leakage. Such an approach makes it possible to achieve a more realistic balance between security, performance, and hardware costs.

Figure 3 shows the distribution of absolute correlation coefficient values for all key hypotheses. A pronounced statistical maximum is observed, corresponding to the correct key value. This confirms that the predicted power consumption model for the correct hypothesis aligns best with the observed data. The presence of such a peak serves as a direct indicator of successful key recovery using correlation power analysis (CPA).

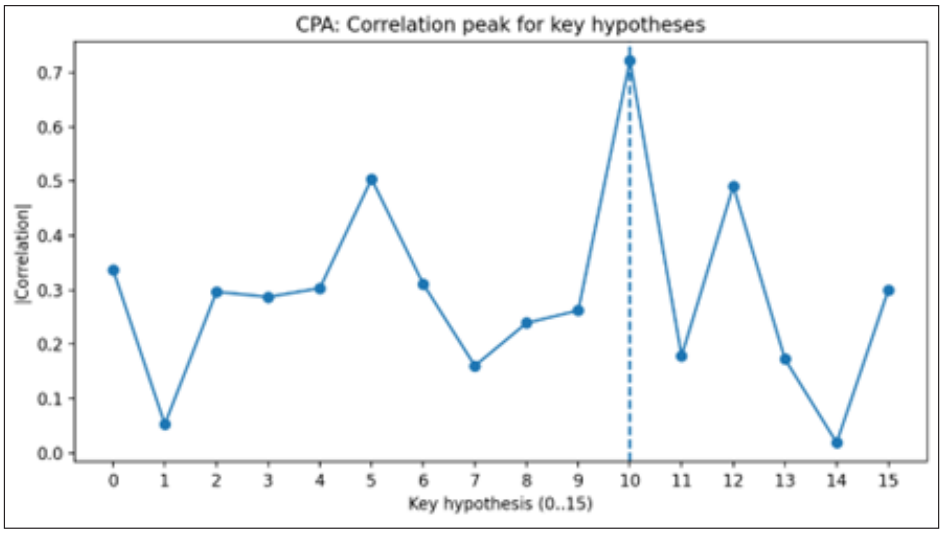

Figure 3 – Distribution of the correlation coefficient for all key hypotheses.
The maximum corresponds to the correct key

The convergence of the attack is illustrated in Figure 4. As the number of traces increases, the correlation for the correct hypothesis stabilizes at a significantly higher level, while the other hypotheses remain clustered considerably lower. This reflects a fundamental property of statistical attacks: as the amount of data increases, noise averages out, and the useful dependency between power consumption and the key-dependent intermediate value strengthens. Consequently, the correct hypothesis gradually begins to dominate.

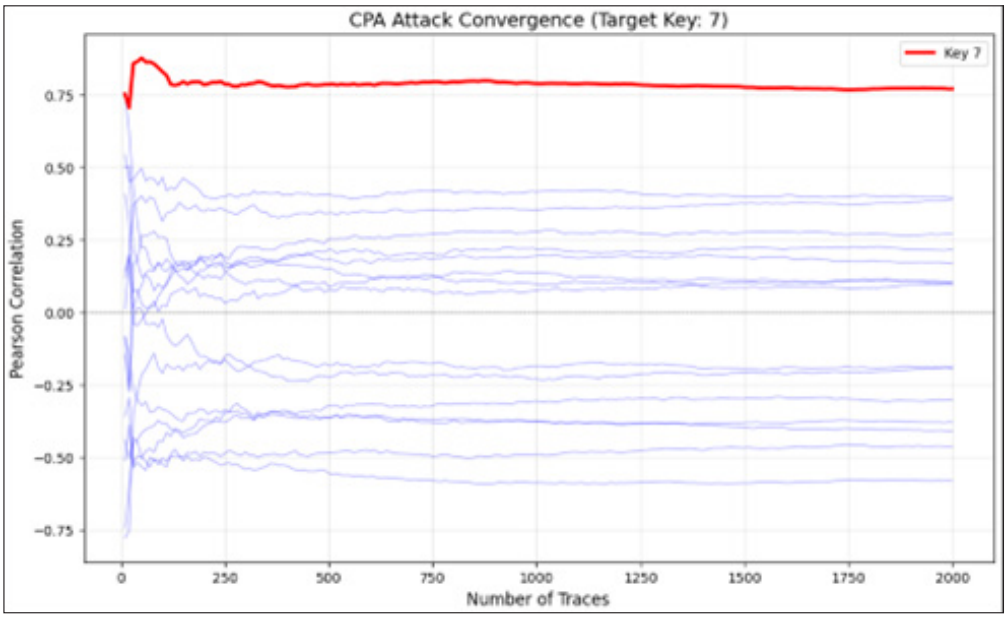

Figure 4 – CPA convergence without masking:
correlation as a function of the number of traces

The quantitative dynamics of the key recovery probability are presented in Figure 5. It can be seen that CPA rapidly achieves a high success probability even with a relatively small number of traces and practically saturates as the amount of data grows further. In contrast, DPA-based methods demonstrate significantly lower efficiency and a much slower increase in success rate. Even the optimized DPA variant (best-bit) remains noticeably less effective than CPA. This can be explained by the fact that CPA uses a continuous leakage model (Hamming weight), whereas DPA relies on binary trace partitioning and therefore loses part of the statistical information.

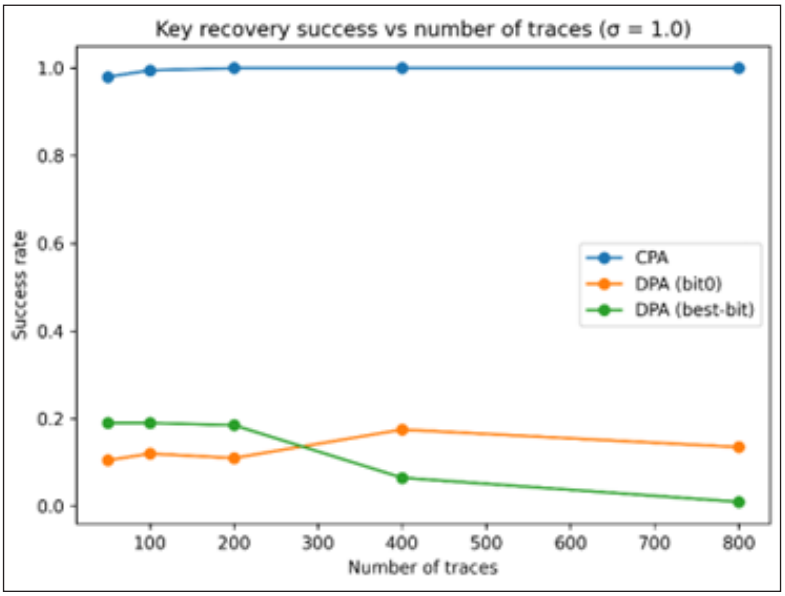

Figure 5 – Probability of successful key recovery as a function
of the number of traces (σ = 1.0)

The numerical success rates are presented in Table 2. They confirm the trends observed in the figure: under identical conditions, CPA demonstrates the highest key recovery probability. Table 3 additionally shows the minimum number of traces required to achieve a recovery probability of at least 90%. For CPA, the required data volume is substantially smaller than for DPA, indicating the higher statistical efficiency of the correlation-based approach.

Table 2 – Key recovery success rates for multiple σ and N

Noise level σ	Number of traces N	CPA success rate	DPA(bit 0) success rate	DPA(best-bit) success rate
0.5	100.0	1.0	0.1	0.1
0.5	200.0	1.0	0.095	0.035
0.5	400.0	1.0	0.15	0.025
0.5	800.0	1.0	0.13	0.0
1.0	100.0	0.995	0.12	0.19
1.0	200.0	1.0	0.11	0.185
1.0	400.0	1.0	0.175	0.065
1.0	800.0	1.0	0.135	0.01
1.5	100.0	1.0	0.14	0.165
1.5	200.0	1.0	0.13	0.17
1.5	400.0	1.0	0.14	0.12
1.5	800.0	1.0	0.125	0.08

Table 3 – Trace complexity for different noise levels (≥ 90% success rate)

Noise level σ	CPA (≥ 90%)	DPA(bit 0) (≥ 90%)	DPA(best-bit) (≥ 90%)
0.5	50	> 800	> 800
1.0	50	> 800	> 800
1.5	100	> 800	> 800

Special attention was given to the analysis of the effect of masking. The results presented in Table 4 show that when masking is applied, the probability of successful key recovery decreases to a level close to random guessing. For a 4-bit subkey, the probability of a random guess is 1/16, which is consistent with the obtained results.

Table 4 – Comparison of masked and unmasked cases (σ = 1.0)

Masking	Number of traces N	CPA success rate	DPA(bit 0) success rate	DPA(best-bit) success rate
No	200	1.0	0.11	0.185
Yes	200	0.06	0.11	0.05
No	400	1.0	0.175	0.065
Yes	400	0.065	0.07	0.04
No	800	1.0	0.135	0.01
Yes	800	0.05	0.05	0.065

The behavior of the correlation under masking is illustrated in Figure 6. Unlike the unprotected case, the correlation corresponding to the correct hypothesis does not exhibit stable growth and remains close to zero even when the number of traces increases to 2000. This indicates the absence of a first-order statistical dependency between power consumption and the key-dependent intermediate value. Thus, masking effectively disrupts the observable correlation structure and suppresses the possibility of key recovery using first-order methods.

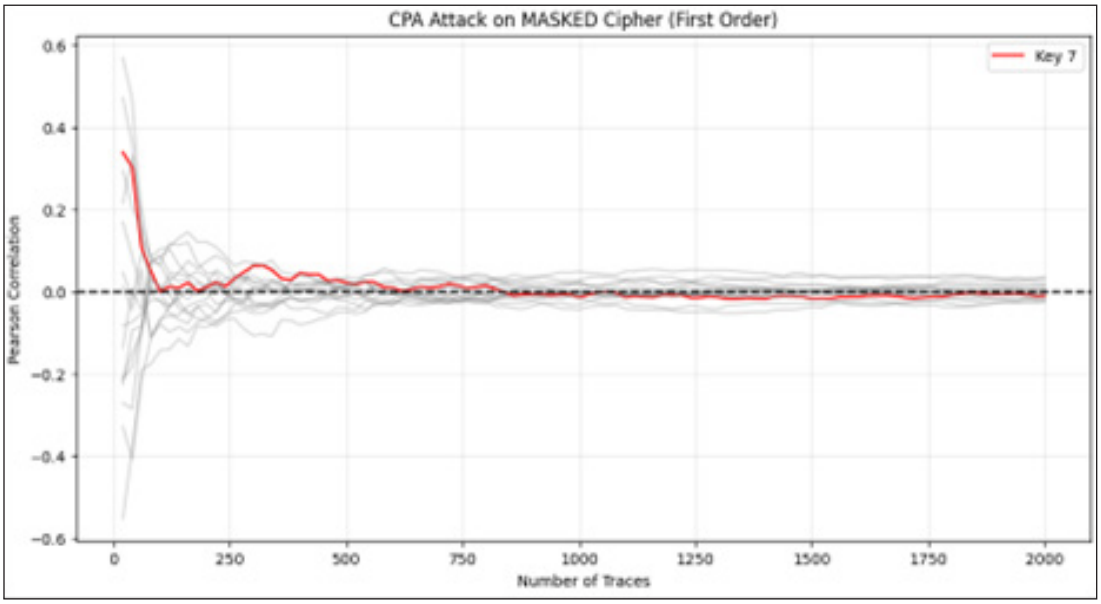

Figure 6 – Correlation behavior under first-order masking

A comprehensive analysis of all presented results leads to the following conclusions. First, the unprotected implementation exhibits stable statistical leakage sufficient for key recovery. Second, correlation power analysis is significantly more efficient than differential power analysis. Third, the application of first-order masking substantially reduces attack effectiveness and disrupts the observable statistical dependency.

Thus, the conducted experimental validation confirms the theoretical principles underlying side-channel attacks and demonstrates the practical importance of masking as a countermeasure for lightweight cryptographic implementations.

It should be noted that the proposed approach is limited in scope and does not replace a standardized certification methodology. The experimental setup used in this study represents a simplified first-order leakage model and is aimed primarily at identifying general patterns rather than providing an exhaustive comparison of all algorithm classes and countermeasures. At the same time, it is precisely this simplification that makes it possible to introduce unified analysis criteria and to track the influence of cipher structure, noise level, and masking on the success of basic attacks.

Conclusion

The conducted analysis examined the characteristics and outcomes of side-channel attacks on the lightweight block ciphers PRESENT, SPECK, SIMON, and PRINCE. It has been shown that even with a small number of traces, DPA, CPA, and EM-based methods can recover secret keys if the cipher implementation lacks hardware- or software-level protection. This confirms the necessity of a comprehensive approach to the design of lightweight cryptographic solutions – one that considers not only mathematical security but also the behavior of the implementation under real operating conditions.

The analysis of existing studies and countermeasures revealed that the use of S-boxes in block-cipher structures increases the risk of leakage due to complex nonlinear operations and uneven power consumption. At the same time, ARX-based algorithms demonstrate better resistance to side-channel attacks because of their uniform structure and the absence of substitution tables. However, even such constructions require additional protection mechanisms.

A comparison of various countermeasures – masking, power balancing, random delays, and architectural approaches – showed that each of them has both advantages and limitations. The most

effective strategy is to combine several protection techniques to achieve an optimal balance between security, performance, and hardware efficiency.

The conducted experimental validation demonstrated that the unprotected lightweight implementation exhibits stable statistical leakage sufficient for key recovery using correlation power analysis (CPA). It was found that CPA outperforms DPA in terms of efficiency and requires fewer traces to achieve a high probability of success.

At the same time, the application of first-order masking significantly reduces the probability of key recovery and disrupts the observable correlation dependency. This confirms the effectiveness of masking as a practical countermeasure against side-channel attacks.

The conducted analysis makes it possible to draw a broader conclusion that the practical resistance of lightweight cryptographic algorithms to side-channel attacks is determined not only by the choice of the cryptographic construction itself, but also by a combination of interrelated factors. These include the type of key-dependent intermediate values, the nature of the resulting leakage, the statistical efficiency of the analysis method, and the acceptable resource costs of implementing protection. In this sense, resistance to side-channel attacks should be regarded as a comprehensive implementation-specific characteristic rather than as an isolated property of the algorithm.

Thus, the obtained results quantitatively confirm the vulnerability of unprotected implementations and demonstrate the importance of protective mechanisms for enhancing the resilience of lightweight cryptographic algorithms.

The scientific novelty of the present work lies not in developing a universal formal model for the side-channel attack evaluation, but in the systematization and comparison of data on the practical vulnerability of lightweight algorithms and the applied countermeasures within a unified analytical context. The proposed approach makes it possible to relate the structural features of ciphers, the nature of the observed leakages, and the resource constraints of IoT devices, thereby providing a foundation for the further transition to more rigorous and unified evaluation methodologies.

The results of the analysis indicate that a promising direction in lightweight cryptography is the development of a new ARX-based algorithm with integrated countermeasures against side-channel leakage. This approach will enable more reliable and robust solutions for resource-constrained devices, including sensor networks, intelligent controllers, and Internet-of-Things systems.

Future work will focus on transitioning from theoretical justification to the practical implementation of a prototype of the proposed algorithm, followed by its experimental evaluation and comparison with existing solutions in terms of security, speed, and hardware efficiency.

Acknowledgment

This research was carried out under the project BR24993052 "Development and study of cryptographic algorithms for information protection in resource-constrained systems and assessment of their security" at the Institute of Information and Computational Technologies of the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan.

REFERENCES

1 Randolph, M., and Diehl, W. Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. Cryptography, 4 (2), 15 (2020). https://doi.org/10.3390/cryptography4020015

2 Socha, P., Miškovský, V., and Novotný, M. A Comprehensive Survey on the Non-Invasive Passive Side-Channel Analysis. Sensors, 22 (21), 8096 (2022). https://doi.org/10.3390/s22218096

3 Sayakkara, A., Le-Khac, N.-A., and Scanlon, M. A Survey of Electromagnetic Side-Channel Attacks and Discussion on Their Case-Progressing Potential for Digital Forensics. Digital Investigation, 29, 43–54 (2019). https://doi.org/10.1016/j.diin.2019.03.002

4 Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., and Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems – CHES 2007 (Berlin: Springer, 2007), Vol. 4727, pp. 450–466. https://doi.org/10.1007/978-3-540-74735-2_31

5 Damodharan, J., Susai Michael, E.R., and Shaikh-Husin, N. High Throughput PRESENT Cipher Hardware Architecture for the Medical IoT Applications. Cryptography, 7 (1), 6 (2023). https://doi.org/10.3390/cryptography7010006

6 Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., and Wingers, L. The SIMON and SPECK Lightweight Block Ciphers. Proceedings of the 52nd Annual Design Automation Conference (DAC 2015) (2015), Article No. 175. https://doi.org/10.1145/2744769.2747946

7 Lu, J., Liu, G., Sun, B., Li, C., and Liu, L. Improved (Related-Key) Differential-Based Neural Distinguishers for SIMON and SIMECK Block Ciphers. The Computer Journal, 67 (2023). https://doi.org/10.1093/comjnl/bxac195

8 Rasoolzadeh, S., and Raddum, H. Cryptanalysis of PRINCE with Minimal Data. Applied Cryptography and Network Security (ACNS 2016) (Cham: Springer, 2016), pp. 109–126. https://doi.org/10.1007/978-3-319-31517-1_6

9 Mohd Esa, N.F., Latip, S., and Baharon, M.A. Survey of ARX-Based Symmetric-Key Primitives. International Journal of Communication Networks and Information Security, 11 (3) (2022). https://doi.org/10.17762/ijcnis.v11i3.4258

10 Gundaram, P.K. Cryptanalysis of Selected ARX-Based Block Ciphers. Vietnam Journal of Computer Science, 11 (4), 553–568 (2024). https://doi.org/10.1142/S2196888824500143

11 Gunathilake, N., Lo, O., Buchanan, W., and Al-Dubai, A. Electromagnetic Side-Channel Analysis of PRESENT Lightweight Cipher. arXiv preprint (2025). https://doi.org/10.48550/arXiv.2503.12248

12 Gamaarachchi, H., Ganegoda, H., and Ragel, R. Breaking SPECK Cryptosystem Using Correlation Power Analysis Attack. Journal of the National Science Foundation of Sri Lanka, 45 (4), 393–402 (2017). https://doi.org/10.4038/jnsfsr.v45i4.8233

13 Yoshikawa, M., and Nozaki, Y. Power Analysis Attack and Its Countermeasure for a Lightweight Block Cipher Simon. Information Security and Cryptology (ICISC 2016) (Cham: Springer, 2016), pp. 151–160. https://doi.org/10.1007/978-3-319-32467-8_15

14 Zhang, Y., Wu, N., Zhou, F., Zhang, J., and Yahya, M.R. A Countermeasure against DPA on SIMON with an Area-Efficient Structure. Electronics, 8 (2), 240 (2019). https://doi.org/10.3390/electronics8020240

15 Shanmugam, D., Selvam, R., and Annadurai, S. Differential Power Analysis Attack on SIMON and LED Block Ciphers. Information and Communications Security (Cham: Springer, 2014), pp. 110–125. https://doi.org/10.1007/978-3-319-12060-7_8

16 Xue, J., Jiang, X., Li, P., Xi, W., Xu, C., and Huang, K. Side-Channel Attack of Lightweight Cryptography Based on MixColumn: Case Study of PRINCE. Electronics, 12 (3), 544 (2023). https://doi.org/10.3390/electronics12030544

17 Yli-Mäyry, V., Ueno, R., Miura, N., Nagata, M., Bhasin, S., Mathieu, Y., Graba, T., Danger, J.-L., and Homma, N. Diffusional Side-Channel Leakage From Unrolled Lightweight Block Ciphers: A Case Study of Power Analysis on PRINCE. IEEE Transactions on Information Forensics and Security, 16, 1351–1364 (2021). https://doi.org/10.1109/TIFS.2020.3033441

18 Mangard, S., Oswald, E., and Popp, T. Power Analysis Attacks: Revealing the Secrets of Smart Cards (Berlin: Springer, 2007), 240 p. https://doi.org/10.1007/978-0-387-38162-6

19 Rivain, M., and Prouff, E. Provably Secure Higher-Order Masking of AES. Cryptographic Hardware and Embedded Systems – CHES 2010 (Berlin: Springer, 2010), pp. 413–427. https://doi.org/10.1007/978-3-642-15031-9_28

20 Tiri, K., and Verbauwhede, I. Design Method for Constant Power Consumption of Differential Logic Circuits. arXiv preprint (2007). https://doi.org/10.48550/arXiv.0710.4756

21 Kim, H. Power-Balancing Software Implementation to Mitigate Side-Channel Power Analysis Attacks. Applied Sciences, 10 (7), 2454 (2020). https://doi.org/10.3390/app10072454

22 Coron, J.-S., and Kizhvatov, I. Analysis and Improvement of the Random Delay Countermeasure of CHES 2009. Cryptographic Hardware and Embedded Systems – CHES 2010 (Berlin: Springer, 2010), pp. 95–109. https://doi.org/10.1007/978-3-642-15031-9_7

23 Ambrose, J., Ragel, R., Jayasinghe, D., Li, T., and Parameswaran, S. Side Channel Attacks in Embedded Systems: A Tale of Hostilities and Deterrence. Proceedings of the 16th International Symposium on Quality Electronic Design (2015), pp. 452–459. https://doi.org/10.1109/ISQED.2015.7085468

24 Nikova, S., Rechberger, C., and Rijmen, V. Threshold Implementations Against Side-Channel Attacks and Glitches. Information and Communications Security (ICICS 2006) (Berlin: Springer, 2006), pp. 529–545. https://doi.org/10.1007/11935308_38

25 Gross, H., Mangard, S., and Korak, T. Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2017, 163–189 (2017). https://doi.org/10.1145/2996366.2996426

26 Sangodoyin, S., Dufour, M., D'Errico, R., Sauleau, R., Wiart, J., and Fleury, M. Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices. IEEE Transactions on Antennas and Propagation, 69 (6), 3470–3484 (2021). https://doi.org/10.1109/TAP.2020.3037659

27 Seok, B., and Lee, C. Fast Implementations of ARX-Based Lightweight Block Ciphers (SPARX, CHAM) on 32-Bit Processor. International Journal of Distributed Sensor Networks, 15 (9) (2019). https://doi.org/10.1177/1550147719874180

28 Yan, Y., Oswald, E., and Vivek, S. An Analytic Attack against ARX Addition Exploiting Standard Side-Channel Leakage. Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021) (2021), pp. 89–97. https://doi.org/10.5220/0010223600890097

29 Jungk, B., Petri, R., and Stöttinger, M. Efficient Side-Channel Protections of ARX Ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018 (3), 627–653 (2018). https://doi.org/10.13154/tches.v2018.i3.627-653

[1]Капалова Н.А.,
т.ғ.к., қауымдастырылған профессор, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[1,2] *Хаумен А.,
докторант, ORCID ID: 0000-0002-1670-2520,
*e-mail: haumen.armanbek@gmail.com
[1]Алғазы К.Т.
PhD, қауымдастырылған профессор, ORCID ID: 0000-0003-3670-2170,
e-mail: kunbolat@mail.ru

[1]Ақпараттық және есептеу технологиялар институты, Алматы қ., Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан

ЖЕҢІЛ САЛМАҚТЫ АЛГОРИТМДЕРДІҢ ЖАНАМА АРНАЛАР АРҚЫЛЫ ЖАСАЛАТЫН ШАБУЫЛДАРҒА ТӨЗІМДІЛІГІ

Аңдатпа

Заттар интернетінің (IoT) және кіріктірілген жүйелердің қарқынды дамуы шектеулі ресурстармен жұмыс істейтін құрылғыларға бейімделген криптографиялық шешімдерді қолдану қажеттілігін арттырды. Жеңіл салмақты криптография қауіпсіздік, өнімділік және энергия тұтыну арасындағы тепе-теңдікті қамтамасыз етеді, сондықтан ол сенсорларда, RFID-таңбаларда, медициналық құрылғыларда және басқа да IoT компоненттерінде кеңінен қолданылады. Алайда іс жүзінде мұндай алгоритмдер жанама арналар арқылы жүзеге асырылатын шабуылдарға осал болуы мүмкін. Мұндай шабуылдар энергия тұтыну, электромагниттік сәулелену немесе уақыттық сипаттамалар сияқты жанама ақпараттың сыртқа шығуын пайдалана отырып, құпия кілттерді қалпына келтіруге мүмкіндік береді. Ең қауіпті түрлері – қуаттың дифференциалды және корреляциялық талдауына (DPA, CPA) негізделген әдістер, олар аз ғана өлшеулердің көмегімен шифрді іске асыруды бұза алады. Мақалада PRESENT, SIMON, SPECK және PRINCE сияқты жеңіл салмақты алгоритмдерге бағытталған жанама арналық шабуылдарға шолу жасалған. Сонымен қатар қорғаныс әдістері – маскалау, жасырындыру, есептеу ретін өзгерту, threshold-реализациялар және аппараттық қарсы шаралар қарастырылған. Олардың тиімділігі мен ресурстық шығындары салыстырмалы түрде талданып, әр тәсілдің артықшылықтары мен әлсіз тұстары айқындалды. Зерттеуде шектеулі ресурстары

бар IoT құрылғылары жағдайында қорғаныс шешімдерін практикалық қолдануға ерекше назар аударылған. Нәтижелер көрсеткендей, әмбебап қорғаныс әдісі жоқ, ал ең жоғары тиімділікке маскалау мен жасырындыру тәсілдерін біріктіретін кешенді амалдар арқылы қол жеткізуге болады. Бұл жұмыс жеңіл салмақты криптография үшін тұрақтылықты бағалау және қорғаныс тетіктерін жетілдіру бағытындағы зерттеулердің өзектілігін айқындайды.

Түйін сөздер: жеңіл салмақты криптография, жанама арналар, SCA-шабуылдар, DPA, CPA, IoT қауіпсіздігі.

[1]Капалова Н.А.,
к.т.н, ассоциированный профессор, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[1,2] *Хаумен А.,
докторант, ORCID ID: 0000-0002-1670-2520,
*e-mail: haumen.armanbek@gmail.com
[1]Алгазы К.Т.
PhD, ассоциированный профессор, ORCID ID: 0000-0003-3670-2170,
e-mail: kunbolat@mail.ru

[1]Институт информационных и вычислительных технологий КН МНВО, г. Алматы, Казахстан
[2]Казахский национальный университет им. аль-Фараби, г. Алматы, Казахстан

УСТОЙЧИВОСТЬ ЛЕГКОВЕСНЫХ АЛГОРИТМОВ К АТАКАМ ПО ПОБОЧНЫМ КАНАЛАМ

Аннотация

Стремительное развитие Интернета вещей (IoT) и встраиваемых систем приводит к необходимости применения криптографических решений, адаптированных для устройств с ограниченными ресурсами. Легковесная криптография обеспечивает баланс между безопасностью, производительностью и низким энергопотреблением, что делает ее востребованной в сенсорах, RFID-метках, медицинских устройствах и других IoT-компонентах. Однако на практике данные алгоритмы подвержены атакам по побочным каналам, использующим утечки энергии, электромагнитного излучения или временных характеристик для восстановления секретных ключей. Наибольшую угрозу представляют методы дифференциального и корреляционного анализа мощности, которые позволяют компрометировать реализацию за относительно небольшое количество измерений. В статье представлен обзор атак по побочным каналам на легковесные алгоритмы, таких как PRESENT, SIMON, SPECK и PRINCE. Рассмотрены основные методы защиты, включая маскирование, сокрытие, перестановку вычислений, threshold-реализации и аппаратные меры противодействия. Проведен сравнительный анализ их эффективности и накладных расходов, выявлены сильные и слабые стороны каждого подхода. Особое внимание уделено проблеме практической применимости защитных решений в условиях ограниченных ресурсов IoT-устройств. Результаты исследования показывают, что ни один метод защиты не является универсальным и наибольшую эффективность демонстрируют комбинированные подходы, сочетающие маскирование и методы сокрытия. Работа подчеркивает необходимость дальнейших исследований, направленных на формирование подходов к оценке стойкости и совершенствованию защитных механизмов для легковесной криптографии.

Ключевые слова: легкая криптография, побочные каналы, атаки SCA, DPA, CPA, IoT-безопасность.