SecureFirst
123 Security St.
Aveley, Western Australia, 6069

28/05/2025

Bob Bobby
789 Vulnerability Ave.
Perth, Western Australia, 6000

Dear Mr. Bobby:

I hope this letter finds you well. I am writing today to ensure ABSecure are made aware of a vulnerability named Return of the Copper Smith Attack (ROCA). This letter will discuss its discovery, its presence at a global scale and a more detailed understanding on the potential negative impacts to Estonia and its citizens if it were exploited. In addition, an understanding of what digital security features were taken advantage of and the resources an attacker would require are explored. Finally, it is determined whether ABSecure's cryptosystem is vulnerable to ROCA, or whether other vulnerabilities similar to those of ROCA can be exploited.

## What is ROCA

On august 30th 2017, Estonia's Information Security Authority were made aware of the vulnerability ROCA, a mathematical attack taking advantage of poor RSA encryption implementation within Infineon chips (Information Security Authority, n.d.; National Institute of Standards and Technology, 2025; Valtna-Dvořák et al., 2021). Estonia implemented these chips within electronic ID used by 66% of its population for identity and permit authentication (Valtna-Dvořák et al., 2021). In addition, these chips were used globally within bank and access cards (Information Security Authority, n.d.). It is estimated that 1 billion chips contained the vulnerability, with 750,000 of these residing within Estonian electronic IDs (Information Security Authority, n.d.; Valtna-Dvořák et al., 2021).

## What is RSA

These chips used RSA for securing the exchanging of encryption keys between entities required for decrypting secured messages known as ciphertext, with the additional ability of allowing the message and its sending entity to be verified (Infineon, n.d.). RSA uses the concept of key pairs (public and private), where public keys are widely accessible and allow entities to secure encryption keys (used for converting the ciphertext into plaintext) which only the private key entity can then reverse. Furthermore, it allows messages and the private key entity itself to be verified. The private key is known only by a single entity, providing the ability to decrypt the secured encryption key during the key exchange, which then allows the ciphertext to be decrypted. In addition, it allows a private key entity to ‘fingerprint’ their message to prove themselves and their message is authentic. The private key is built around the public key e value, allowing only the keypair to encrypt, decrypt and authenticate within its pair. The keys are generated from two large prime numbers, with the private key containing a single value (denoted d) and public key with two (denoted n and e). The use of large primes ensure that n is unable to be factorised, which if successful would reveal the primes used and thus, allow the private key to be generated by a third-party (Ruzai et al., 2024).

## The Discovery of ROCA

A researcher at the Centre for Research and Security within Masaryk University discovered that the formula Infineon used for producing prime numbers was exploitable (Nemec et al., 2017). It would allow the infeasible brute-forcing of factorising n to become achievable, resulting in the victim’s private key (National Cyber Security Centre, 2025; Nemec et al., 2017). From this, the attacker has the ability to reverse secured key exchanges and receive encryption keys and therefore, decrypt ciphertexts meant only for the private key entity (Information Security Authority, n.d.). In addition, the attacker can impersonate the private key entity to send malicious data to another which has been confirmed through message verification that the entity is legitimate (Information Security Authority, n.d.).

## How Did ROCA Exploit the Infineon Prime Formula

The formula uses a large value (denoted as M) which remains constant across both primes generated and is further used to also create two more values (denoted as a and k) (Nemec et al., 2017). ROCA takes advantage of this concept as the large M produces a small a and k value, which in turn allows only a limited number of primes to be created; this causes the generation of primes to lose randomness and become more predictable (Nemec et al., 2017). With this, factorising becomes possible since the attacker needs to only try factorising n with a more limited set of possible primes (Nemec et al., 2017).

## Was ROCA Exploited

Due to the mathematical complexity of ROCA and secrecy by the finders and organisations alerted, the attack had not been implemented before fixes were implemented (Information Security Authority, n.d.; Kohler, 2020). Furthermore, the vulnerability is no longer a concern within affected Infineon chips which received the required software updates (Valtna-Dvořák et al., 2021). It must be noted however with a minimum of 1 billion chips being vulnerable within various device types, there is the possibility of devices not being updated and thus, remaining exploitable (Nemec et al., 2017; Valtna-Dvořák et al., 2021).

## Resources Required to Exploit ROCA

To exploit ROCA, the attacker would have required the public key values (e and n), in addition to the constant M value (Nemec et al., 2017). Utilising a commercial desktop from 2017, a 512-bit private key was discoverable in 1.93 CPU hours, with 1024-bit private keys in 97.1 CPU days (where a CPU hour or day is the time taken for a single processor to execute while using 100% of its power) (Nemec et al., 2017). Although this may seem infeasible for finding 1024-bit keys and greater, hardware with greater performance capabilities for instance, third-party servers had the ability to compute 512-bit private keys in 0.63 CPU hours (costing $0.063) and 1024-bit private keys in 31.71 CPU days (costing $76) (Nemec et al., 2017).

## Is ABSecure Vulnerable

ABSecure's cryptosystem is not vulnerable to ROCA due to not implementing the Infineon formula for its prime generation (Nemec et al., 2017). In addition, assuming ABSecure uses up-to-date chips (whether Infineon or not), the ROCA vulnerability is no longer exploitable (Valtna-Dvořák et al., 2021). As a result, the improved factorisation brute-force technique is unable to be implemented and thus, maintains private key secrecy. Despite this, due to ABSecure's poor choices in the primes chosen, the unoptimized brute force can quickly result in the private key.

## Other Vulnerabilities in ABSecure's Cryptosystem

The primes chosen by ABSecure include two 40-bit values (1,000,000,000,163 and 1,000,000,006,793) producing an n value of 80-bits; this can be factorised in an unoptimized brute-force attempt within less than 3 hours. As a result, an attacker can read and manipulate all messages received by ABSecure in less than 3 hours. Due to the simplicity and speed of factorising n, it is not a case of if ABSecure will be attacked, rather when. Although ABSecure's cryptosystem also involves other cryptographic implementations for instance, the stream cipher (which produces encryption keys and secures messages into ciphertext), the security it provides is bypassed as the attacker now gains the encryption key and reverses the ciphertext. Furthermore, the encryption keys produced by ABSecure's stream cipher are all the same therefore, by obtaining the single encryption key within any key exchange, all messages to ABSecure are vulnerable.

## Solutions to the Vulnerability Concerns

There are two solutions which ABSecure must implement simultaneously to improve their cryptosystem. The first involves increasing the value of the primes to at most 512-bits to produce an n value of at most 1024-bits. Doing so results in factorisation becoming computationally infeasible for the next 10 to 15 years. The next solution involves introducing randomness into each encryption key produced by the stream cipher for securing messages. It is to be noted that this does not improve the RSA key pairs however, it means if ABSecure notices their private key has been breached and produce a new key pair, the attacker will only be able to decrypt the messages related to the key exchanges they intercepted. This would be implemented using numbers used only once (nonces), a unique value implemented in the encryption key creation process. Even if duplicate messages are encrypted, the unique value ensures it produces a different encryption key and ciphertext which additionally improves security.

## Consequences for ABSecure

If ABSecure were to maintain the use of their vulnerable cryptosystem, attackers will have no trouble in gaining the private key, resulting in all data received by ABSecure being susceptible to manipulation or viewing by unauthorised entities. This could be used in a variety of situations for instance, attackers manipulating messages to increase the money received from a transaction or change the bank account which receives it. In addition, the attacker will also have the ability to impersonate ABSecure, manipulating other banks into accepting malicious data as it is believed to be from a reliable entity. Regardless of security, this could also harm the reputation which ABSecure upholds as clients become aware that their money and personal data are at risk.

## Summary

Despite ROCA being a vulnerability which existed within 1 billion affected chips, it was never exploited (Information Security Authority, n.d.; Valtna-Dvořák et al., 2021). Regardless, it shows ABSecure the dangers of poor cryptographic algorithm implementations allowing RSA private keys to be found from public keys, having negative impacts on a global and country scale (Information Security Authority, n.d.; Ruzai et al., 2024; Valtna-Dvořák et al., 2021). Furthermore, by understanding ROCA and how it is exploited, the discussion of other vulnerabilities within ABSecure's cryptosystem similar to it have been successfully highlighted.

I look forward to hearing from you in taking the next steps to secure the digital security of ABSecure.

Jordan Farrow
Jfarrow0@our.ecu.edu.au

## References

Infineon. (n.d.). *Background information on software update of RSA key generation function*. Retrieved May 24, 2025, from https://www.infineon.com/cms/en/product/promopages/rsa-update/rsa-background

Information Security Authority. (n.d.). *ROCA vulnerability and eID: Lessons Learned*. https://www.ria.ee/sites/default/files/documents/2022-11/Roca-vulnerability-and-eID-lessons-learned-2018.pdf

Kohler, K. (2020). *Estonia's national cybersecurity and cyberdefense posture*. Center for Security Studies. https://doi.org/10.3929/ethz-b-000438276

National Cyber Security Centre. (2025, October 19). *ROCA: Infineon TPM and Secure Element RSA Vulnerability Guidance*. Retrieved May 10, 2025, from https://www.ncsc.gov.uk/guidance/roca-infineon-tpm-and-secure-element-rsa-vulnerability-guidance

National Institute of Standards and Technology. (2025, April 19). *CVE-2017-15361*. Retrieved May 10, 2025, from https://nvd.nist.gov/vuln/detail/CVE-2017-15361

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3133956.3133969

Ruzai, W. N. A., Ariffin, M. R. K., Asbullah, M. A., & Ghafar, A. H. A. (2024). New simultaneous diophantine attacks on generalized RSA key equations. *Journal of King*

*Saud University - Computer and Information Sciences*, *36*(5), 102074. https://doi.org/10.1016/j.jksuci.2024.102074

Valtna-Dvořák, A., Lips, S., Tsap, V., Ottis, R., Priisalu, J., & Draheim, D. (2021). Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. Electronic Government and the Information Systems Perspective. *Electronic Government and the Information Systems Perspective*, 73–85. https://doi.org/10.1007/978-3-030-86611-2_6