Politechnika Śląska

# ROZPRAWA DOKTORSKA

System kryptograficzny implementowany w pSoC

**mgr inż. Szymon Sarna**

**PROMOTOR**

**dr hab. inż. Robert Czerwiński, Prof. PŚ**

**DYSCYPLINA**

**Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne**

**Katedra Systemów Cyfrowych**

**Wydział Automatyki, Elektroniki i Informatyki**

**OPIEKUN POMOCNICZY**

**mgr inż. Tomasz Krzyżak, Digital Core Design**

Praca badawcza finansowana w ramach programu Doktorat Wdrożeniowy — III edycja

**Gliwice 2024**

## Tytuł pracy

System kryptograficzny implementowany w pSoC

## Streszczenie

Rozprawa doktorska pt. „System kryptograficzny implementowany w pSoC" przedstawia przebieg badań i rozwój systemu kryptograficznego firmy Digital Core Design. Poprzez analizę źródeł literaturowych i początkowej implementacji tytułowego systemu zidentyfikowano obszary, w których można podnieść jego bezpieczeństwo i efektywność. Za cel obrano m.in.: implementację układu mnożącego, generatora liczb prawdziwie losowych, zweryfikowanie odporności na ataki kanałem pobocznym oraz opracowanie protokołu z kluczami jednorazowymi.

Kluczowym elementem rozwijanego systemu kryptograficznego jest ko-procesor CryptOne, umożliwiający akceleracje obliczeń w algorytmach kryptografii asymetrycznej, takich jak RSA i ECC. Krytyczny wpływ na ich wydajność ma operacja mnożenia modulo, w związku z czym weryfikowano możliwość jej optymalizacji. W trakcie procesu badań i implementacji opracowano unikalne połączenie metod zaproponowanych w literaturze oraz oryginalnych rozwiązań, czego efektem jest podniesienie wydajności oraz ograniczenie zapotrzebowania na zasoby logiczne względem wersji referencyjnej. Opracowana architektura charakteryzuje się też bardzo dobrymi parametrami na tle innych rozwiązań opublikowanych w literaturze.

Obok układu mnożącego, na poziomie sprzętowym weryfikowano również możliwość wdrożenia generatora liczb prawdziwie losowych. Co do zasady, jest to fundamentalny komponent każdego systemu kryptograficznego, niemniej jego wiarygodna implementacja w układzie cyfrowym jest istotnym wyzwaniem ze względu na ograniczenia narzędzi projektowych oraz specyfikę mierzonych zjawisk fizycznych. Przeprowadzone badania i analizy pozwoliły na implementację generatora, którego źródłem losowości jest błąd fazy sygnału zegarowego. Zgodność z modelem stochastycznym oraz pozytywna weryfikacja przez zestaw testów statystycznych istotnie podnoszą wiarygodność opracowanej implementacji.

Obok generacji kluczy kryptograficznych generatory liczb losowych odgrywają istotną rolę w mechanizmach zabezpieczających przed atakami kanałem pobocznym. Jest to grupa ataków, które umożliwiają przełamywanie zabezpieczeń układów kryptograficznych, m.in. na podstawie obserwacji różnego rodzaju zjawisk fizycznych towarzyszących obliczeniom. Może to być np. czas, rozpraszana moc lub promieniowanie elektromagnetyczne. Ataki te stanowią poważne zagrożenie dla bezpieczeństwa nieomal każdej implementacji, dlatego postanowiono przygotować stanowisko pomiarowe i środowisko programowe, które umożliwią weryfikację podatności i skuteczności zastosowanych zabezpieczeń. Badania obejmowały przeprowadzenie takich ataków jak prosta i różnicowa analiza rozpraszanej

mocy. Opracowane metody, narzędzia i wnioski stanowią fundament do weryfikowania bezpieczeństwa rozwijanego systemu kryptograficznego w kontekście ataków kanałem pobocznym.

Systemy kryptograficzne, jak sama nazwa wskazuje, łączą w sobie różne funkcje i poziomy abstrakcji. W części sprzętowej implementowane są mechanizmy, które realizują operacje opisane przez instrukcje maszynowe, algorytmy i aplikacje. Świadomość zakresu tych zagadnień i możliwość podniesienia bezpieczeństwa na różnych poziomach były przyczynkiem do przeprowadzenia badań nad algorytmami z kluczami jednorazowymi. Wśród powszechnie używanych rozwiązań można spotkać algorytmy z akronimem OTP (ang. *One-Time-Password*), oznaczającym hasła jednorazowe, jednak pomimo unikalności kodów lub haseł czesto „wewnątrz" zaszyty jest stały klucz kryptograficzny. W związku z tym przygotowano koncepcję protokołu z kluczami jednorazowymi, który został następnie wdrożony i uruchomiany w oparciu o rozwijany system kryptograficzny. Protokół ten charakteryzuje się unikalnymi własnościami, które sprawiają, że może być on odpowiedzią na niektóre ze współczesnych wyzwań związanych z bezpieczeństwem teleinformatycznym.

Podsumowując, w ramach pracy doktorskiej osiągnięto postawione cele badawcze. Opracowane rozwiązania, również o oryginalnym charakterze, przełożyły się na poprawę parametrów i właściwości sytemu kryptograficznego w zakresie bezpieczeństwa, wydajności oraz zapotrzebowania na zasoby logiczne. Finalne efekty przeprowadzonych badań znalazły również zastosowanie i zostały wdrożone w produktach firmy Digital Core Design.

**Słowa kluczowe**

kryptografia, układy mnożące, ataki kanałem pobocznym, generatory liczb losowych, klucze jednorazowe

**Thesis title**

Cryptographic system implemented in pSoC

**Abstract**

The doctoral dissertation entitled „A cryptographic system implemented in pSoC", presents the research and development of Digital Core Design cryptographic system. By analyzing sources from the literature and the initial implementation of the title system, areas where its security and efficiency could be improved were identified. The objectives included the implementation of a multiplication circuit, a true random number generator, the execution of side-channel attacks, and the development of a protocol with one-time keys.

A key component of the cryptographic system under development is the CryptOne co-processor, enabling accelerated computation in asymmetric cryptography algorithms such as RSA and ECC. Critical to their performance is the modulo multiplication operation. Therefore, the possibility of its optimization was verified. In the course of the research and implementation process, a unique combination of methods proposed in the literature and original solutions were developed, resulting in improved performance and reduced logical resource requirements as compared to the reference version. The developed architecture is also characterized by very good performance compared to other solutions published in the literature.

In addition to the multiplication circuit, the possibility of implementing a true random number generator was also verified at the hardware level. In principle, this is a fundamental component of any cryptographic system, but its reliable implementation in a digital system is a significant challenge due to the limitations of design tools and the specificity of the physical phenomena measured. The research and analysis carried out allowed the implementation of a generator whose source of randomness is a clock signal jitter. However, compliance with the stochastic model and positive verification by a set of statistical tests significantly increase the reliability of the developed implementation.

In addition to cryptographic key generation, random number generators are the basis for side-channel attacks countermeasures. This is a group of attacks that allows breaching the cryptographic systems security on the basis of, among others, the observation of various physical phenomena accompanying the calculations. These may be, for example, time, power dissipation or electromagnetic radiation. These attacks pose a serious threat to the security of almost any implementation, which is why it was decided to prepare a measurement station and a software environment, which would enable the verification of vulnerability and effectiveness of applied countermeasures. The research involved carrying out attacks such as a simple and differential power analysis. The methods, tools, and conclusions developed provide the foundation for verifying the security of the cryptographic system under development in the context of side-channel attacks.

Cryptographic systems, as the name suggests, combine various functions and levels of abstraction. The hardware part implements mechanisms that perform operations described by machine instructions, and then algorithms and applications. Awareness of the scope of these issues and the possibility of improving security at various levels were the reason for conducting research on algorithms with one-time keys. Among the commonly used solutions, you can find algorithms with the acronym OTP, meaning one-time password, but despite the uniqueness of codes or passwords, a permanent cryptographic key is often hidden ”inside”. In connection with this, a concept of a protocol with one-time keys was prepared, which was then implemented and launched based on the developed cryptographic system. This protocol is characterized by unique properties that make it a response to some of the contemporary challenges related to IT security.

In summary, the research goals established were achieved within the framework of the doctoral thesis. The solutions developed, also of an original nature, resulted in the improvement of the parameters and properties of the cryptographic system in terms of security, efficiency, and demand for logical resources. The final results of the conducted research were also used and implemented in the Digital Core Design products.

**Key words**

cryptography, security, multiplier circuits, side channel attacks, random number generators, one-time keys