Temat nr 1: **Opracowanie, implementacja i ocena bezpieczeństwa algorytmów postkwantowych pk. APQ**

1.	**Nazwa projektu**	**Opracowanie, implementacja i ocena bezpieczeństwa algorytmów postkwantowych pk. APQ.**
2.	**Zgłaszający / Koordynator**	Podmiot zgłaszający propozycję projektu: Minister Obrony Narodowej. Koordynator: Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni - Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni
3.	**Określenie obszarów obronności i bezpieczeństwa państwa, których projekt będzie dotyczył**	Przedmiotem projektu jest opracowanie asymetrycznych algorytmów szyfrowania, uzgadniania klucza (KEM lub KEX) i podpisu cyfrowego, które będą odporne na zagrożenia wynikające z możliwości realizacji obliczeń na komputerze kwantowym. Zakres realizacji projektu wpisuje się w priorytetowy obszar technologiczny 6, tj. Nowoczesne technologie lub rozwiązania innowacyjne w sferze bezpieczeństwa teleinformatycznego, ochrony informacji w systemach i sieciach teleinformatycznych oraz narodowej kryptografii, określony dla 7 strategicznego kierunku badań naukowych i prac rozwojowych bezpieczeństwo i obronność państwa w Krajowym Programie Badań. Wdrożenie wyników projektu ma służyć pozyskaniu priorytetowej zdolności operacyjnej służb odpowiedzialnych za obronność cyberprzestrzeni. Realizacja projektu jest zgodna z „Priorytetowymi kierunkami badań w Resorcie Obrony Narodowej na lata 2017-2026”, a w szczególności wpisuje się obszar techniki i technologii obronnych (techniki informacyjne i sieciowe), gdzie do kluczowych technologii zaliczono technologie osiągania i utrzymywania zdolności do ochrony kryptograficznej oraz do reagowania na incydenty komputerowe w systemach teleinformatycznych, w tym: technologia ochrony kryptograficznej systemu teleinformatycznego oparta o kryptografię kwantową. Wymienionej technologii nadano wysoki priorytet badawczy.
4.	**Opis projektu**	W cyberprzestrzeni podstawową metodą zabezpieczania poufności i integralności informacji są mechanizmy kryptograficzne. Do tego celu można wykorzystywać algorytmy symetryczne np. szyfry blokowe czy kluczowane (parametryzowane) funkcje skrótu. Posiadają one jednak tę wadę, że wymagają dystrybucji tajnego sekretu (klucza) do wszystkich uczestników komunikacji. Wady tej nie posiadają algorytmy asymetryczne, ale z kolei ich wydajność jest znacznie mniejsza niż algorytmów symetrycznych. Do ochrony poufności danych stosuje się zatem systemy hybrydowe, w których algorytm asymetryczny służy do uzgodnienia klucza, a algorytm symetryczny do ochrony poufności. Obecnie jednym z istotnych problemów w systemach teleinformatycznych jest wdrożenie takich mechanizmów zabezpieczeń, które będą skuteczne także wtedy, gdy atakujący będzie miał możliwość wykonywania obliczeń na komputerze kwantowym. Mechanizmy te w kryptologii powszechnie nazywane są algorytmami postkwantowymi. W odniesieniu do algorytmów

		symetrycznych wiadome są sposoby zapobiegania zagrożeniom wynikającym z możliwości użycia komputera kwantowego. Inaczej jest w przypadku algorytmów asymetrycznych, w tym m.in. algorytmu uzgadniania klucza i podpisu cyfrowego. Na tę chwilę w środowisku naukowym związanym z kryptologią trwają intensywne badania mające na celu opracowanie algorytmów asymetrycznych odpornych na ataki z użyciem komputera kwantowego. Z punktu widzenia bezpieczeństwa informacji w sieciach teleinformatycznych algorytmy asymetryczne realizujące szyfrowanie, uzgodnienie klucza lub podpis cyfrowy są niezwykle istotne ze względu na powszechność ich stosowania m.in. w rozwiązaniach PKI. Od algorytmów kryptograficznych, ze względu na funkcję jaką pełnią w systemach teleinformatycznych, wymaga się odpowiedniej siły bezpieczeństwa oraz wydajności. Oczekuje się, że zaproponowane w badaniu algorytmy będą zapewniały bezpieczeństwo szacowane wg sposobu określonego w założeniach[1] do konkursu Post-Quantum Cryptography organizowanego przez amerykańską agencję standaryzacyjną NIST. Oczekuje się także, że wydajność zaproponowanych algorytmów, długość stosowanych kluczy czy szyfrogramów będą podobne do parametrów algorytmów zakwalifikowanych do 3 rundy (finalistów) tegoż konkursu[2]. W badaniu za postkwantowe algorytmy asymetryczne uważa się kryptosystemy, których główne składowe są uważane za bezpieczne jeżeli nie istnieje na nie żaden skuteczny atak, włączając w to ataki wykorzystujące obliczenia na komputerze kwantowym. Dla przykładu, hybrydowe rozwiązanie wykorzystujące w szyfrowaniu lub podpisie problem faktoryzacji lub logarytmu dyskretnego nie jest algorytmem postkwantowym. Postkwantowe algorytmy asymetryczne powinny posiadać przynajmniej po jednej z następujących funkcjonalności: 1. Schematy **szyfrowania kluczem publicznym** powinny zawierać następujące algorytmy: generację kluczy, szyfrowanie oraz deszyfrowanie. Algorytm generacji kluczy powinien generować klucz publiczny oraz klucz prywatny, tak aby zaszyfrowaną wiadomość przy użyciu klucza publicznego można było z wysokim prawdopodobieństwem (prawdopodobieństwo błędu nie większe niż 2^{-64}) odszyfrować wykorzystując odpowiedni klucz prywatny. Schemat szyfrowania kluczem publicznym powinien umożliwiać szyfrowanie wiadomości, której długość wynosi przynajmniej 256 bitów. 2. Schematy **uzgadniania klucza** powinny zawierać następujące algorytmy: generację kluczy, enkapsulację oraz dekapsulację. Algorytm generacji kluczy powinien generować klucz publiczny oraz klucz prywatny, tak aby

[1] *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*, 81 Federal Register 92787 (December 20, 2016), pp.92787-92788. https://federalregister.gov/a/2016-30615

[2] *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standarization Process - NIST 8309*, https://doi.org/10.6028/NIST.IR.8309

		enkapsulacja z kluczem publicznym oraz dekapsulacja z kluczem prywatnym z wysokim prawdopodobieństwem wytworzyły ten sam współdzielony sekret, gdy szyfrogram jest wejściem do funkcji dekapsulacji. Schemat wymiany klucza powinien umożliwić wyznaczenie współdzielonego sekretu, którego długość wynosi przynajmniej 256 bitów. 3. Schematy **podpisów cyfrowych** powinny zawierać algorytmy: generację kluczy, podpisywanie oraz weryfikację. Algorytm generacji kluczy powinien generować klucz publiczny oraz klucz prywatny, tak aby wiadomość podpisaną kluczem publicznym mogła zostać zweryfikowana przy pomocy klucza prywatnego. Schemat podpisu cyfrowego powinien umożliwić podpisywanie wiadomości, których długość może wynieść do 2^{63} bitów. Bezpieczeństwo postkwantowych algorytmów asymetrycznych szyfrowania i uzgadniania klucza powinno bazować na dwóch modelach ataków. Pierwszym jest semantyczne bezpieczeństwo wobec ataków z wybranym tekstem jawnym (w literaturze znane jako *IND-CPA*). Drugim jest semantyczne bezpieczeństwo szyfrowania lub enkapsulacji w odniesieniu do adaptacyjnych ataków z wybranym szyfrogramem (w literaturze znane jako *IND-CCA2*). Bezpieczeństwo schematów podpisów cyfrowych powinno bazować na modelu niepodrabialności podpisu cyfrowego w wobec adaptacyjnych ataków z wybranym tekstem jawnym (w literaturze znany jako EUF-CMA). Przewiduje się niepewności w dokładnym przeprowadzeniu dowodu bezpieczeństwa kryptosystemów postkwantowych, których źródłem jest możliwość odkrycia nowych rodzajów ataków kryptograficznych wykorzystujących komputery kwantowe i trudność dokładnego oszacowania wydajności komputerów kwantowych w przyszłości wyrażona w ich koszcie, szybkości czy wymaganej wielkości pamięci. W celu unifikacji poziomów bezpieczeństwa kryptosystemów postkwantowych sposób szacowania odporności algorytmów powinien być dokonywany w sposób zaproponowany przez NIST[3]. Wyróżnia się w nim 3 poziomy bezpieczeństwa dla schematów wymiany klucza oraz szyfrowania kluczem publicznym: 1. Każdy atak – zarówno w klasycznym jak i kwantowym modelu złożoności – powodujący kompromitację bezpieczeństwa algorytmu (z wybranym zestawem parametrów) powinien wymagać wykonania nie mniej operacji niż klasyczny atak na bezpieczny algorytm blokowy o długości klucza 128 bitów – poziom bezpieczeństwa *NIST level 1*. 2. Każdy atak – zarówno w klasycznym jak i kwantowym modelu złożoności – powodujący kompromitację bezpieczeństwa algorytmu (z wybranym zestawem parametrów) powinien wymagać wykonania nie mniej operacji niż klasyczny atak na bezpieczny algorytm blokowy o długości klucza 192 bitów – poziom bezpieczeństwa *NIST level 3*.

[3] „Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms”, 81 Federal Register 92787 (December 20, 2016), pp.92787-92788. https://federalregister.gov/a/2016-30615

		3. Każdy atak – zarówno w klasycznym jak i kwantowym modelu złożoności – powodujący kompromitację bezpieczeństwa algorytmu (z wybranym zestawem parametrów) powinien wymagać wykonania nie mniej operacji niż klasyczny atak na bezpieczny algorytm blokowy o długości klucza 256 bitów – poziom bezpieczeństwa *NIST level 5*. Dla schematów podpisu cyfrowego wyróżnione zostały w poziomy bezpieczeństwa: 1. Każdy atak – zarówno w klasycznym modelu złożoności jak i w kwantowym – powodujący kompromitację bezpieczeństwa algorytmu (z wybranym zestawem parametrów) powinien wymagać wykonania nie mniej operacji niż wymaga znalezienie kolizji dla bezpiecznej funkcji skrótu o długości skrótu 256 bitów – poziom bezpieczeństwa *NIST level 2*. 2. Każdy atak – zarówno w klasycznym modelu złożoności jak i w kwantowym – powodujący kompromitację bezpieczeństwa algorytmu (z wybranym zestawem parametrów) powinien wymagać wykonania nie mniej operacji niż wymaga znalezienie kolizji dla bezpiecznej funkcji skrótu o długości skrótu 384 bitów – poziom bezpieczeństwa *NIST level 4*. Efektami planowanego projektu są: 1. specyfikacja asymetrycznych algorytmów postkwantowych: szyfrowania, podpisu cyfrowego i uzgadniania klucza, których poziom bezpieczeństwa jest zgodny ze zdefiniowanym powyżej; 2. analiza bezpieczeństwa opracowanych algorytmów; 3. implementacje programowe opracowanych algorytmów.
5.	**Określenie celu głównego i celów szczegółowych realizacji projektu oraz ich relacji do celów innych programów i projektów.**	**Celem głównym** realizacji badania jest opracowanie oraz przeprowadzenie badań bezpieczeństwa asymetrycznych algorytmów szyfrowania, uzgadniania klucza i podpisu cyfrowego, które są odporne na ataki z wykorzystaniem komputera kwantowego. W środowisku kryptologicznym jako najbardziej perspektywiczne kryptosystemy postkwantowe wymienia się bazujące na: 1. kratach teorioliczbowych; 2. kodach korekcyjnych; 3. układach równań wielu zmiennych; 4. izogeniach w krzywych eliptycznych; 5. funkcjach skrótu. Powyższe pięć obszarów problemów obliczeniowych nazywane będzie na potrzeby badania *postkwantowymi problemami perspektywicznymi*.

		Cele szczegółowe: 1. Analiza złożoności problemów trudnych obliczeniowo wykorzystywanych w znanych asymetrycznych algorytmach postkwantowych. 2. Analiza metod badania bezpieczeństwa asymetrycznych algorytmów postkwantowych. 3. Opracowanie trzech asymetrycznych algorytmów służących odpowiednio do: szyfrowania, uzgadniania klucza (KEM lub KEX) i podpisu cyfrowego wraz racjonalnym uzasadnieniem wyboru problemów trudnych obliczeniowo oraz innych decyzji projektowych. Każdy z tych algorytmów powinien mieć możliwość zmiany poziomu bezpieczeństwa (dla zdefiniowanych wcześniej poziomów) poprzez modyfikację parametrów algorytmów. 4. Wykonanie programowych implementacji referencyjnych algorytmów w języku wysokiego poziomu (np. Python). 5. Opracowanie metody oceny bezpieczeństwa opracowanych algorytmów. 6. Przeprowadzenie oceny bezpieczeństwa opracowanych algorytmów. 7. Wykonanie programowych implementacji algorytmów w języku systemowym (np. C, C++). Demonstracja funkcjonalności, analiza wydajności oraz poprawności (np. opracowanie plików KAT (ang. *Known Answer Tests*)[4]) implementacji w symulowanych warunkach operacyjnych. Dla celów szczegółowych zakłada się osiągnięcie VI poziomu gotowości technologii. Cele (główny i szczegółowe) projektu nie pozostają w relacji z innymi projektami planowanymi do uruchomienia, realizowanych albo ukończonych w NCBR dlatego też nie zachodzi możliwość wykorzystania wyników innych projektów przy realizacji zadania pk. APQ.
6.	**Wskazanie technologii krytycznych o znaczeniu determinującym powodzenie projektu, w szczególności dla projektu badawczego**	Technologią krytyczną o znaczeniu determinującym powodzenie całego projektu będzie implementacja programowa algorytmów.

[4] *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*, 81 Federal Register 92787 (December 20, 2016), pp.92787-92788. https://federalregister.gov/a/2016-30615

7. Harmonogram pożądanych terminów realizacji projektu

Proponowany okres realizacji projektu, który powinien zapewnić właściwy przebieg badań, to 24 miesiące

Lp.	Nazwa etapu	Okres realizacji [mies.]	Oczekiwany wynik/efekt zadań zrealizowanych w etapie	Poziom gotowości technologii	Opis
1.	Analiza konstrukcji algorytmów postkwantowych oraz opracowanie koncepcji technologii dotyczącej realizacji funkcjonalności.	6 m-cy	1. Analiza konstrukcji i bezpieczeństwa publicznie znanych algorytmów postkwantowych opartych na postkwantowych problemach perspektywicznych, które będzie m.in. zawierać opis wpływu parametrów algorytmu na bezpieczeństwo oraz aplikacyjne wykorzystanie. 2. Koncepcja technologii przedstawiająca realizację funkcjonalności: szyfrowania, uzgadniania klucza (KEM lub KEX) i podpisu cyfrowego przez badane kryptosystemy. 3. Raport z realizacji etapu.	II	W zadaniu badawczym należy wykonać: 1. Analizę publicznie znanych propozycji algorytmów postkwantowych. 2. Analizę metod oceny bezpieczeństwa algorytmów, o których mowa w pkt. 1 – analiza powinna uwzględniać metody oceny bezpieczeństwa zarówno w kontekście komputerów kwantowych jak i komputerów obecnie stosowanych. 3. Analizę metod doboru parametrów bezpieczeństwa dla algorytmów postkwantowych.
Uzasadnienie:		Celem realizacji zagadnienia badawczego jest: 1. usystematyzowanie wiedzy dotyczącej konstrukcji publicznie znanych asymetrycznych algorytmów postkwantowych oraz problemów trudnych obliczeniowo wykorzystywanych w tych algorytmach; 2. zapoznanie się zespołu badawczego ze sposobami uzasadniania ich bezpieczeństwa oraz wykorzystywanymi to tego celu narzędziami; 3. zapoznanie się zespołu badawczego ze sposobami parametryzowania algorytmów celem zmiany poziomu bezpieczeństwa lub aplikacyjnego zastosowania. W ramach punktu kontrolnego zostanie dokonana ocena merytoryczna Raportu z realizacji etapu oraz koncepcji technologii umożliwiających realizację funkcjonalności, co będzie miało przełożenie na kontynuowanie dalszych badań.		

		2.	Analiza, opracowanie i wybór koncepcji wykorzystania problemów trudnych obliczeniowo.	6 m-cy	1. Opracowanie pisemne dotyczące analizy wymagań bezpieczeństwa dla opracowywanych algorytmów kryptograficznych. 2. Opracowanie pisemne dotyczące analizy problemów trudnych obliczeniowo w kwantowym modelu obliczeń – zakłada się, że w dokumencie będzie zawarty teoretyczny opis problemu oraz wydajność implementacji programowych wybranych algorytmów (opartych na analizowanym problemie). 3. Koncepcja wykorzystania problemów trudnych obliczeniowo dla każdego algorytmu (alternatywnych rozwiązań / ścieżek realizacji zadania badawczego) wraz z uzasadnieniem wyboru. 4. Opracowanie i wykonanie eksperymentów obliczeniowych potwierdzających złożoności rozważanych problemów. 5. Raport z realizacji etapu.	III	Głównym celem realizacji zadania jest wskazanie przez zespół badawczy propozycji problemów trudnych obliczeniowo, na bazie których opracowane będą asymetryczne postkwantowe algorytmy szyfrowania, uzgadniania klucza i podpisu cyfrowego. Ponadto, w ramach zadania powinny zostać przeanalizowane wymagania bezpieczeństwa dla tych algorytmów. Analiza problemów trudnych obliczeniowo powinna uwzględniać konieczność późniejszego wykonania programowej implementacji algorytmów na nich opartych. Zakłada się, że dla każdego algorytmu zostaną przedstawione przynajmniej 2 problemy trudne obliczeniowo, z których jeden będzie należał do grupy postkwantowych problemów perspektywicznych. Dla każdego z rozważanych problemów obliczeniowych należy wykonać eksperyment obliczeniowy polegający na rozwiązaniu losowych instancji danego problemu. Zamawiający wskaże przynajmniej jeden problem z przedstawionych przez Wykonawcę, na bazie którego Wykonawca będzie zobowiązany do opracowania propozycji konstrukcji algorytmu.	
		Uzasadnienie:		Bezpieczeństwo obecnie znanych asymetrycznych algorytmów (w tym postkwantowych) szyfrowania, uzgadniania klucza i podpisu cyfrowego oparte jest na problemie trudnym obliczeniowo. Wybór tego problemu bezpośrednio determinuje poziom bezpieczeństwa algorytmu oraz ma znaczący wpływ na efektywność implementacji programowych i sprzętowych. Wykonanie eksperymentów obliczeniowych wyznaczających i/lub potwierdzających wartości parametrów				

				problemów trudnych obliczeniowo, które umożliwią zastosowanie w kryptografii, ma dominujący wpływ na efektywność docelowego kryptosystemu. Wykonanie analizy problemów trudnych obliczeniowo na podstawie której wykonany zostanie wybór problemu dla przyszłych algorytmów jest najważniejszą decyzją projektową dokonywaną w badaniu. W sytuacji gdy Wykonawca przedstawi dwa interesujące (z punktu widzenia Zamawiającego) problemy trudne obliczeniowo Zamawiający może zobowiązać Wykonawcę do dalszego opracowywania algorytmów opartych na obu problemach. Poszczególne podzadania badawcze są niezbędne do opracowania docelowego demonstratora. Przeanalizowane problemy będą podstawą wykonania kluczowych elementów programowej implementacji, która będzie spełniała założone zdolności funkcjonalne. W ramach punktu kontrolnego zostanie dokonana ocena merytoryczna raportu z realizacji etapu, wykonanych analiz oraz koncepcji wykorzystania problemów trudnych obliczeniowo dla każdego algorytmu.		
		3.	Opracowanie modeli algorytmów.	6 m-cy	1. Specyfikacje asymetrycznych postkwantowych algorytmów szyfrowania, uzgadniania klucza i podpisu cyfrowego. 2. Programowe implementacje referencyjne opracowanych algorytmów w języku wysokiego poziomu. 3. Wstępna analiza bezpieczeństwa, która będzie zawierać oszacowanie odporności algorytmów na ataki generyczne oraz wyniki i wnioski wynikające z badań statystycznych. 4. Raport z realizacji etapu. 5. Sprawozdanie z badań funkcjonalnych modeli.	IV	Głównym celem realizacji zadania badawczego jest opracowanie specyfikacji projektowanych algorytmów. Ponadto, zakłada się, że dla każdego algorytmu zostanie przedstawiona referencyjna implementacja programowa oraz wstępna analiza bezpieczeństwa, która powinna zawierać: 1. odniesienie do zastosowanego problemu trudnego obliczeniowo oraz złożoności obliczeniowej ataków generycznych (rozumianych jako nie wynikających z podatności zastosowanych przekształceń); 2. wyniki badań statystycznych.
		Uzasadnienie:		Kolejnym etapem opracowania algorytmów jest opracowanie ich specyfikacji oraz wstępna ocena spełniania założeń dotyczących oczekiwanego poziomu bezpieczeństwa oraz zbadanie wydajności. Wyniki z realizacji zagadnienia mają za zadanie potwierdzić słuszność dokonanych decyzji projektowych oraz stanowić podstawę do wykonania gruntownej analizy bezpieczeństwa opracowanych algorytmów. Na tym etapie ocenie będzie można poddać długość kluczy i szyfrogramów oraz wskazać potencjalne zastosowanie opracowanych algorytmów. W ramach punktu kontrolnego zostanie dokonana ocena merytoryczna raportu z realizacji etapu i sprawozdania z badań funkcjonalnych modeli algorytmów.		

		4.	Analiza bezpieczeństwa oraz opracowanie demonstratora technologii w postaci programowej implementacji opracowanych algorytmów.	6 m-cy	1. Dowód bezpieczeństwa opracowanych algorytmów. 2. Opracowanie pisemne dotyczące metod doboru parametrów algorytmów dla wszystkich zdefiniowanych poziomów bezpieczeństwa. 3. Programowe implementacje opracowanych algorytmów w języku niskiego poziomu wraz z raportem z analizy poprawności rozwiązania. 4. Raport z badań wydajności opracowanych implementacji oraz analiza możliwości jej zwiększenia. Badanie wydajności powinno być wykonane zgodnie z pakietem badań SUPERCOP (bench.cr.yp.to). 5. Raport z realizacji etapu 6. Metodyka badań demonstratora systemu. 7. Sprawozdanie z badań demonstratora.	VI	Celem realizacji zadania badawczego jest wykonanie analizy bezpieczeństwa opracowanych algorytmów. Kolejnym celem jest wytworzenie implementacji programowych zaproponowanych algorytmów porównywalnych do docelowych produktów wykorzystywanych w warunkach rzeczywistych. Należy przedstawić demonstracje funkcjonalności algorytmów oraz analizę poprawności. Ponadto w ramach zadania, na podstawie implementacji programowych, zbadana zostanie wydajność opracowanych algorytmów.
		Uzasadnienie:		W etapie 4 potwierdzone zostanie spełnianie przez algorytmy zdefiniowanych poziomów bezpieczeństwa. Opracowania pisemne powstałe w etapie są kluczowe pod kątem możliwości parametryzowania zaproponowanych algorytmów oraz przyszłego ich wykorzystania do ochrony informacji niejawnych. Weryfikacja prawidłowego działania programowej implementacji i jej poszczególnych właściwości w środowisku symulującym rzeczywiste warunki (zasilanie systemu odpowiednio przygotowanymi danymi). W ramach punktu kontrolnego zostanie dokonana ocena merytoryczna wykonania i sprawdzenia elementów kluczowych oraz ich integracja, która pozwoli na weryfikację prawidłowego działania demonstratora systemu. Ponadto ocenie merytorycznej zostaną poddane ww. dokumenty wynikowe z realizacji projektu.			
8.	**Użytkownik końcowy**	Użytkownikiem końcowym powstałych wyników (PWI oraz demonstratorów) będzie Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni - Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni					

9.	**Szacunkowe koszty projektu**	Wnioskodawca przedstawi we wniosku o dofinansowanie kalkulację kosztów realizacji projektu z podziałem na poszczególne lata. Planowany koszt realizacji projektu ujęty w „Planie badań naukowych w resorcie obrony narodowej na lata …" może być modyfikowany na podstawie wniosków złożonych przez wnioskodawców i w trakcie negocjacji przed zawarciem umowy. Po zawarciu umowy dopuszcza się możliwość przesunięcia kosztów pomiędzy poszczególnymi etapami/latami okresu realizacji projektu bez wzrostu kosztów całkowitych. Projekt będzie finansowany lub współfinansowany ze środków NCBR przewidzianych na finansowanie badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności państwa (dotacja celowa).
10.	**Przysługiwanie praw własności intelektualnej do wyników projektu i korzystanie z tych praw, w tym określenie podmiotu uprawnionego do reprezentacji Skarbu Państwa**	1. Właścicielem wynalazków, wzorów użytkowych i wzorów przemysłowych lub topografii układu scalonego oraz wyhodowanej albo odkrytej i wyprowadzonej odmiany rośliny powstałych w wyniku wykonania Projektu jest Skarb Państwa reprezentowany przez Ministra Obrony Narodowej. W celu uniknięcia jakichkolwiek wątpliwości, Strony potwierdzają, że w związku z powyższym Skarb Państwa jest uprawniony do nieograniczonego czasowo, terytorialnie lub w inny sposób korzystania oraz rozporządzania wynalazkami, wzorami użytkowymi, wzorami przemysłowymi lub topografią układu scalonego, wyhodowaną albo odkrytą i wyprowadzoną odmianą rośliny powstałymi w wyniku wykonania Projektu, w tym Skarbowi Państwa przysługuje prawo do uzyskania patentu na wynalazki, prawa ochronnego na wzory użytkowe, jak również prawa z rejestracji wzorów przemysłowych lub topografii układu scalonego, prawo do wyhodowanej albo odkrytej i wyprowadzonej odmiany rośliny. Zgłoszenie wynalazku, wzoru użytkowego, wzoru przemysłowego lub topografii układu scalonego oraz wyhodowanej albo odkrytej i wyprowadzonej odmiany rośliny w celu uzyskania patentu, prawa ochronnego lub prawa z rejestracji dokonywane jest przez Skarb Państwa lub na rzecz Skarbu Państwa. Skarb Państwa reprezentowany jest przez Ministra Obrony Narodowej w przypadku wykonywania wszelkich praw i obowiązków Skarbu Państwa wynikających z Umowy. 2. Wykonawca, w związku z otrzymanym finansowaniem Projektu, zobowiązuje się przenieść na Skarb Państwa, reprezentowany zgodnie z ust. 1, całość autorskich praw majątkowych do utworów powstałych w wyniku wykonania Projektu na wszelkich znanych na dzień zawarcia umowy o przeniesienie autorskich praw majątkowych do utworów powstałych w ramach wykonania Projektu polach eksploatacji oraz prawo wykonywania zależnych praw autorskich do utworów z możliwością przenoszenia tych praw na osoby trzecie bez zgody twórców lub Wykonawcy. Przeniesienie autorskich praw majątkowych do utworów powstałych w wyniku wykonania Projektu nastąpi po otrzymaniu przez Wykonawcę zawiadomienia z Centrum o pozytywnej ocenie raportu końcowego wraz z informacją, że warunkiem uznania Umowy za wykonaną jest wywiązanie się Wykonawcy z określonych w Umowie obowiązków w zakresie praw własności intelektualnej.

		3. Zakres istniejącej wiedzy i rozwiązań posiadanych przez Wykonawcę– w tym w szczególności takich, które są lub mogą być przedmiotami praw własności intelektualnej i które w ramach Finansowania zostaną wykorzystane w celu realizacji Projektu, oraz zasady ich wykorzystania w Projekcie – zostały określone w Opisie Projektu. 4. Wykonawca jest zobowiązany, w formie pisemnego wykazu, którego wzór jest dostępny na stronie internetowej Centrum (www.gov.pl/ncbr), do szczegółowego wskazania PWI oraz Praw Związanych wraz ze wskazaniem przedmiotów wskazanych praw; w wykazie wskazuje się również materialne rezultaty Projektu, w szczególności demonstratory technologii. Wykaz, o którym mowa w zdaniu poprzednim, zostanie przekazany Centrum wraz z Raportem końcowym, o którym mowa w § 6 Umowy. W terminie złożenia raportu końcowego wykaz zostanie również przekazany przez Wykonawcę Skarbowi Państwa. 5. Wykonawca zobowiązuje się do dnia złożenia wykazu, o którym mowa w ust. 3, nabyć całość PWI od podwykonawców, personelu (niezależnie od podstawy zatrudnienia/współpracy), osób trzecich. 6. Niezwłocznie po powstaniu przedmiotu PWI Wykonawca zobowiązany jest powiadomić o tym Skarb Państwa. Przedmioty PWI zostaną przekazane Skarbowi Państwa z inicjatywy Wykonawcy lub na wezwanie Skarbu Państwa po otrzymaniu przez Wykonawcę zawiadomienia z Centrum o pozytywnej ocenie raportu końcowego wraz z informacją, że warunkiem uznania Umowy za wykonaną jest wywiązanie się Wykonawcy z określonych w Umowie obowiązków w zakresie praw własności intelektualnej. Wykonawca zobowiązany jest przekazać w szczególności wszelką dokumentację, materiały i informacje dotyczące przedmiotów PWI, a w szczególności ich podstawowe założenia, opis techniczny, specyfikację oraz wizualizacje, kody źródłowe, wynikowe, maszynowe i inne, dokumentację projektową, techniczną i eksploatacyjną. Wykonawca przekaże Skarbowi Państwa przedmioty PWI w terminie określonym w wezwaniu Skarbu Państwa, o którym mowa w niniejszym ustępie. 7. W przypadku, gdy przedmioty PWI zostaną przekazane Skarbowi Państwa na nośnikach, na których je utrwalono, w szczególności nośnikach elektronicznych (płytach CD, DVD, tzw. pendrive itp.), wraz z przekazaniem Skarbowi Państwa danego nośnika, przechodzi na Skarb Państwa bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie Umowy przez Wykonawcę finansowania) prawo własności tego nośnika, z zastrzeżeniem ust. 9. 8. Wykonawca przeniesie na Skarb Państwa własność demonstratorów powstałych w wyniku wykonania Projektu, bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie Umowy przez Wykonawcę Finansowania), wyłącznie na wyraźne żądanie Skarbu Państwa zgłoszone w terminie czterech miesięcy od dnia doręczenia Skarbowi Państwa wykazu, o którym mowa w ust. 4.

		9. Wykonawca zobowiązuje się udzielić Skarbowi Państwa licencji na korzystanie z przedmiotów Praw Związanych na następujących warunkach: 1) licencja będzie licencją pełną, nieograniczoną terytorialnie ani czasowo; 2) licencja zostanie udzielona w zakresie niezbędnym do swobodnego korzystania z oraz rozporządzania prawami objętymi zakresem art. 32 ust. 3 Ustawy; 3) licencja zostanie udzielona bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie Umowy przez Wykonawcę Finansowania); 4) licencja zostanie udzielona z chwilą przekazania przez Wykonawcę przedmiotów PWI, chyba że Skarb Państwa wyrazi zgodę na przedłużenie wskazanego terminu; 5) rozwiązanie umowy licencyjnej będzie możliwe z zachowaniem 15-letniego okresu wypowiedzenia, chyba że Skarb Państwa wyrazi zgodę na skrócenie okresu wypowiedzenia. 10. W przypadku zmiany sytuacji faktycznej lub prawnej w ten sposób, że do swobodnego korzystania i rozporządzania przez Skarb Państwa PWI w zakresie określonym w art. 32 ust. 3 Ustawy konieczna jest zmiana umowy licencyjnej, o której mowa w ust. 9, lub zawarcie dodatkowej umowy, Wykonawcą zobowiązuje się, bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie Umowy przez Wykonawcę Finansowania), zmienić umowę licencyjną lub zawrzeć inną właściwą umowę, w terminie trzech miesięcy od dnia zaistnienia wskazanych w niniejszym ustępie okoliczności, chyba że Skarb Państwa wyrazi zgodę na przedłużenie tego terminu. 11. Wykonawca, za zgodą Skarbu Państwa wyrażoną na piśmie, może zastosować w Projekcie przedmioty Praw Związanych, w stosunku do których nie będzie zobowiązany udzielić Skarbowi Państwa licencji na podstawie ust. 9. 12. Wykonawca oświadcza i gwarantuje, że: 1) prawa, o których mowa w ust. 1,2, 7, 8 , 9 i 10, nie będą posiadały żadnych wad prawnych ani nie będą ograniczać Skarbu Państwa w swobodnym korzystaniu z nich i rozporządzaniu nimi – w szczególności nie będą ograniczać Skarbowi Państwa ich samodzielnego lub za pomocą osób trzecich rozwoju, modyfikacji i utrzymania; 2) korzystanie z oraz rozporządzanie PWI nie będzie naruszać jakichkolwiek praw osób trzecich; 3) osoby uprawnione z tytułu praw osobistych do przedmiotów PWI nie będą wykonywać tych praw w stosunku do Skarbu Państwa lub osób trzecich działających na jego zlecenie. Wykonawca zobowiązuje się uzyskać od twórców przedmiotów PWI, nie później niż w chwili przeniesienia, o którym mowa w ust. 2, bezterminowe upoważnienie dla Skarbu Państwa do:

		a. wykonywania w imieniu twórców przysługujących im praw osobistych; jednocześnie Wykonawca, gwarantuje i zobowiązuje się, że w stosunku do przedmiotów PWI twórcy nie będą wykonywać, ani zezwalać innym wykonywać, przysługujących im praw osobistych wobec Skarbu Państwa oraz osób przez niego upoważnionych, b. do anonimowego rozpowszechniania przedmiotów PWI i ich wszelkich egzemplarzy według własnego uznania, to jest bez wskazywania imienia, nazwiska, pseudonimu twórców oraz do nie wymieniania twórcy w opisach, rejestrach oraz innych dokumentach i publikacjach, w tym w przypadku fonogramów i wideogramów zamieszczania na ich egzemplarzach oznaczeń dotyczących autorstwa, tytułów utworów, dat sporządzania, nazwiska lub firmy (nazwy) producenta – przy czym w celu uniknięcia wszelkich wątpliwości Strony potwierdzają, że Skarb Państwa nie jest zobowiązany do rozpowszechniania przedmiotów PWI lub ich części, c. wprowadzania zmian i przeróbek do przedmiotów PWI podyktowanych potrzebami korzystania z nich, w tym wykorzystywania ich w części lub w całości oraz łączenia z innymi przedmiotami własności intelektualnej lub innymi elementami, a także dokonywania ich wszelkich modyfikacji oraz rozpowszechniania tak zmienionych przedmiotów praw własności intelektualnej, d. zadecydowania o pierwszej publikacji przedmiotów PWI lub o zaniechaniu publikacji, e. wykonywania w ich imieniu nadzoru nad sposobem korzystania z PWI; 4) twórcy przedmiotów PWI nie odwołają upoważnienia określonego w pkt 3; 5) Wykonawca ani żadna osoba trzecia nie będzie żądać zapłaty jakiegokolwiek wynagrodzenia za korzystanie z PWI i przekazanie przedmiotów PWI na rzecz Skarbu Państwa. 13. Z zastrzeżeniem ust. 18, Wykonawca zobowiązuje się: 1) zachować w tajemnicy wszelkie informacje, w szczególności informacje techniczne, technologiczne, ekonomiczne, finansowe, handlowe, prawne i organizacyjne dotyczące Projektu, niezależnie od formy ich pozyskania i ich źródła, które związane są z prowadzonymi w Projekcie pracami lub dotyczą rezultatu Projektu i których ujawnienie może mieć wpływ na ochronę, korzystanie lub rozporządzanie PWI (dalej: „Informacje Poufne”); 2) nie kopiować, nie powielać, w jakikolwiek sposób nie rozpowszechniać ani nie wykorzystywać jakiejkolwiek części Informacji Poufnych w sposób, który mógłby zagrażać ich ujawnieniu; 3) podjąć stosowne przedsięwzięcia niezbędne do zapewnienia ochrony Informacji Poufnych i ich źródła zarówno w całości, jak i co do poszczególnych części.

		14. Zobowiązania, o których mowa w ust. 13, obejmują również wszelkie informacje mające charakter Informacji Poufnych, które dotyczą przedmiotów Praw Związanych w zakresie niezbędnym do zachowania pełnej ochrony PWI. 15. Postanowienia ust. 13-14 nie będą miały zastosowania w stosunku do tych informacji, które: 1) są opublikowane, znane lub urzędowo podane do publicznej wiadomości bez naruszania postanowień Umowy; 2) są powszechnie znane lub zostały przekazane przez osobę trzecią, bez naruszenia jakichkolwiek zobowiązań o ich nieujawnianiu; 3) podlegają ujawnieniu zgodnie z powszechnie obowiązującymi przepisami prawa. 16. Zobowiązania, o których mowa w ust. 13-14, z uwagi na konieczność pełnej ochrony PWI, obowiązują Wykonawcę również po wykonaniu, wygaśnięciu, rozwiązaniu Umowy bez ograniczeń czasowych, tj. do czasu gdy informacje, o których mowa w ust. 13-14, będą miały charakter Informacji Poufnych. 17. Wykonawca zobowiązuje się zapewnić przestrzeganie zobowiązań, o których mowa w ust. 13-14 przez swoich pracowników oraz jakiekolwiek osoby, z którymi współpracuje w związku z wykonywaniem Umowy. 18. Wykonawca jest uprawniony do rozpowszechnienia przedmiotów PWI lub ich części, w tym publikacji naukowych utworów wytworzonych w ramach Projektu, po uprzednim uzyskaniu pisemnej zgody Skarbu Państwa. 19. Wykonawca dokona przeniesienia autorskich praw majątkowych do utworów powstałych w ramach wykonania Projektu na rzecz Skarbu Państwa na mocy odrębnej umowy zawartej pomiędzy Skarbem Państwa a Wykonawcą. Wykonawcy może zostać udzielona licencja na korzystanie z PWI. Ustalenie rodzaju i zakresu licencji, o której mowa w zdaniu poprzedzającym, nastąpi z uwzględnieniem interesu bezpieczeństwa i obronności Państwa oraz interesu Skarbu Państwa. 20. Wykonawca zobowiązany jest powiadomić Centrum na piśmie o: 1) fakcie wywiązania się z obowiązku udzielenia licencji, o której mowa w ust. 9, w terminie 30 dni od dnia zawarcia umowy licencyjnej; 2) innych ustaleniach między Wykonawcą a Skarbem Państwa, poczynionych do momentu przyjęcia i oceny wyników Projektu przez Centrum, które mogą mieć bezpośredni wpływ na prawa i obowiązki wynikające z Umowy w zakresie PWI, w terminie 30 dni od dnia dokonania ustaleń; 3) fakcie przekazania Skarbowi Państwa przedmiotów PWI, w terminie 30 dni od dnia przekazania przedmiotów PWI; 4) fakcie wyrażenia przez Skarb Państwa zgody, o której mowa w ust. 10, w terminie 30 dni od dnia otrzymania informacji o wyrażeniu zgody;

		5) fakcie zawarcia umowy przenoszącej autorskie prawa majątkowe do utworów powstałych w ramach wykonania projektu w terminie 30 dni od dnia zawarcia tej umowy. 21. Centrum nie ponosi odpowiedzialności z tytułu wzajemnych rozliczeń finansowych między Skarbem Państwa a Liderem lub Konsorcjantami, a także rozliczeń podatkowych – związanych z nabyciem lub przekazaniem przedmiotów PWI, a także udzieleniem licencji, o której mowa w ust. 9 i 10. 22. Demonstrator po zakończeniu projektu zostanie nieodpłatnie przekazany na własność Skarbu Państwa.
11.	**Wskazanie potrzeby objęcia projektu ochroną informacji niejawnych**	Wyżej wymieniony projekt ma być realizowany w całości jako projekt jawny.
12.	**Sposób realizacji i zarządzania projektem**	Wykonawca będzie realizował projekt i zarządzał nim w oparciu o uznaną metodykę zarządzania projektami. Realizacją projektu zarządza Wykonawca przy wykorzystaniu powszechnie stosowanych metodyk zarzadzania projektami. Wykonawca zaproponuje metodykę zarządzania, zgodnie z którą projekt będzie realizowany. Wykonawca zagwarantuje użytkownikowi końcowemu, za pośrednictwem narzędzi teleinformatycznych, stałą możliwość obserwowania/śledzenia prac projektowych. Jednocześnie Wykonawca, cyklicznie (raz na dwa miesiące), organizował będzie seminaria z udziałem użytkownika końcowego i zespołu przedstawicieli Ministra do współpracy z NCBR, na których omawiane będą aktualne wyniki projektu. Seminaria będą miały charakter wyłącznie informacyjny. W ramach seminariów nie będzie realizowana ocena czy odbiór wyników projektu. W ramach prowadzonego nadzoru dokonywana będzie ocena poszczególnych etapów realizacji projektu na podstawie sporządzonych przez wykonawcę i przekazanych do NCBR raportów okresowych, a także pełnej dokumentacji wynikowej danego etapu oraz pozostałych produktów (np. modeli, programów, schematów, demonstratorów, itp.), których wymóg opracowania przez Wykonawcę zostanie zawarty w Umowie o wykonanie i finansowanie projektu. W razie potrzeby (etapy kluczowe, punkty kontrolne, testowanie rozwiązań), w ramach prowadzonego nadzoru dokonywana będzie ocena poszczególnych etapów realizacji projektu w siedzibie wykonawcy projektu lub w innym miejscu jego realizacji. Po uzyskaniu końcowej ewaluacji merytorycznej projektu zostanie przez NCBR dokonana ocena, rozliczenie finansowe oraz przyjęcie wyników projektu – uznanie Umowy za wykonaną pod warunkiem wywiązania się wykonawcy ze zobowiązań dotyczących PWI wobec Skarbu Państwa.

13.	**Wskazanie dodatkowych warunków i kryteriów udziału w konkursie na wykonanie i finansowanie projektu**	Zgodnie z regulaminem Konkursu.
14.	**Zmiany w projekcie**	Zakres projektu może być modyfikowany pod warunkiem, że cel główny projektu nie zostanie zmieniony przez Komitet Sterujący do spraw badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności państwa przy realizacji jego zadań oraz przez Dyrektora NCBC – DKWOC na etapie inicjowania projektu oraz w trakcie nadzoru nad realizacją umowy o wykonanie i finansowanie projektu na podstawie opinii, rekomendacji zespołu przedstawicieli Ministra zainteresowanego lub Komitetu Sterującego, a w razie potrzeby ekspertów i w przypadku pozytywnej opinii zespołu przedstawicieli Ministra zainteresowanego. Zmiany te nie wymagają uzgadniania z Ministrem Obrony Narodowej.