Dr hab. Michał Oszmaniec
Centrum Fizyki Teoretycznej PAN

Recenzja rozprawy doktorskiej mgr. inż. Adama Jagielskiego pt. „Synteza i optymalizacja kwantowych układów logicznych reprezentujących prymitywy kryptograficzne”

Rozprawa doktorska Pana mgr. inż. Adama Jagielskiego poświęcona jest syntezie i optymalizacji kwantowych oraz odwracalnych układów logicznych reprezentujących wybrane prymitywy kryptografii symetrycznej, w szczególności prymitywy kryptografii lekkiej. Tematyka pracy lokuje się na styku informatyki technicznej, syntezy układów logicznych, kryptografii symetrycznej oraz obliczeń kwantowych. Jest to obszar w zasadzie ważny: wraz z rozwojem komputerów kwantowych naturalne staje się pytanie, jak kosztowne byłoby wykonanie ataków typu wyczerpującego przeszukiwania klucza przy użyciu algorytmu Grovera oraz jak koszty te zależą od implementacji szyfru w modelu odwracalnym.

Zasadnicza idea pracy jest następująca. Skoro algorytm Grovera wymaga kwantowej wyroczni rozpoznającej poprawny klucz, to trzeba umieć zaimplementować szyfrowanie jako obwód odwracalny lub kwantowy. Koszt takiej implementacji przekłada się następnie na koszt pojedynczego wywołania wyroczni, a więc na koszt całego ataku Grovera. Z tego punktu widzenia naturalne jest badanie implementacji skrzynek podstawieniowych, szablonów optymalizacyjnych dla obwodów odwracalnych oraz zasobów potrzebnych do implementacji wybranych szyfrów AEAD, takich jak SPARKLE i Ascon.

Jest to tematyka potencjalnie wartościowa i praktycznie motywowana. Niestety, w mojej ocenie rozprawa nie realizuje w satysfakcjonujący sposób obietnicy zawartej w tytule i celu pracy. Problem badawczy jest sformułowany zbyt ogólnie, jego motywacja jest powierzchowna, a część wynikowa ma przede wszystkim charakter inżyniersko-numeryczny, ograniczony do małych przykładów lub do oszacowań kosztu dobrze znanego schematu ataku Grovera. Co więcej, prezentacja podstaw teoretycznych jest miejscami niepoprawna, niepedagogiczna i nie pozwala czytelnikowi nabrać zaufania do formalnej warstwy rozprawy.

Publikacje stanowiące podstawę rozprawy

Z treści rozprawy wynika, że jej zasadnicze wyniki są związane z następującymi pracami Autora lub współautorskimi publikacjami:

- A. Jagielski, „Optimal SAT Solver Synthesis of Quantum Circuits Representing Cryptographic Nonlinear Functions”, International Journal of Electronics and Telecommunications 69, 261-267 (2023). Wyniki tej pracy odpowiadają przede wszystkim rozdziałowi 5 rozprawy.
- A. Jagielski, „Complete synthesis of identity templates for quantum and reversible logic MCT circuits using SAT-solvers and proposal of suboptimality witness notion”, International Journal of Electronics and Telecommunications 70, 727-732 (2024). Wyniki te odpowiadają rozdziałowi 6.
- A. Jagielski i K. Kanciak, „Grover on SPARKLE: quantum resource estimation for a NIST LWC call finalist”, Quantum Information and Computation 22, 1132-1143 (2022). Wyniki te odpowiadają rozdziałowi 8.
- W rozprawie stwierdza się ponadto, że badania dotyczące korelacji własności kryptograficznych skrzynek podstawieniowych oraz badania dotyczące szyfru Ascon zostały zgłoszone do publikacji. W samej rozprawie nie znalazłem jednak klarownego, wydzielonego zestawienia tych prac wraz z pełnymi danymi bibliograficznymi, co utrudnia ocenę, które części mają status wyników opublikowanych, a które są wyłącznie materiałem rozprawy.

Struktura rozprawy

Rozprawa składa się z wprowadzenia, dziewięciu rozdziałów, podsumowania, opisu dalszych kierunków rozwoju oraz bibliografii. Wprowadzenie ma uzasadnić wagę kryptografii lekkiej i wskazać, że analiza bezpieczeństwa symetrycznych prymitywów kryptograficznych w obecności komputerów kwantowych jest zagadnieniem istotnym. Rozdział 1 wprowadza podstawowe pojęcia z algebry Boole'a i kryptografii symetrycznej. Rozdział 2 przedstawia model obliczeń kwantowych. Rozdział 3 dotyczy logiki odwracalnej, bramek NCT/MCT, operacji ARX oraz podstaw syntezy obwodów. Rozdział 4 omawia algorytm Grovera oraz model ataku na szyfr symetryczny ze znanym tekstem jawnym.

Zasadnicza część rozprawy zawarta jest w rozdziałach 5-9. Rozdział 5 opisuje użycie SAT-solverów do poszukiwania krótkich implementacji wybranych małych skrzynek podstawieniowych. Rozdział 6 dotyczy syntezy szablonów identyczności i świadków suboptymalności dla układów MCT. Rozdział 7 bada korelacje między klasycznymi parametrami kryptograficznymi małych skrzynek podstawieniowych a rozmiarem ich optymalnej implementacji jako układów MCT. Rozdziały 8 i 9 opisują implementacje wyroczni szyfrujących oraz koszt ataku Grovera odpowiednio dla rodziny SPARKLE i dla szyfru Ascon.

Taka struktura jest w zasadzie czytelna. Do mocniejszych stron rozprawy zaliczam fakt, że Autor stara się prowadzić narrację od elementów lokalnych, takich jak skrzynki podstawieniowe i szablony, do pełniejszych oszacowań kosztu ataku na konkretne szyfry. Rozprawa zawiera też sporo konkretnych tabel z kosztami obwodów, co potencjalnie ułatwia odtwarzalność wyników. Niestety, sposób przedstawienia materiału znacząco obniża wartość naukową pracy. Zbyt duża część tekstu poświęcona jest elementarnym definicjom lub technicznym opisom implementacyjnym, podczas gdy kluczowe pytania metodologiczne, interpretacyjne i kryptograficzne pozostają niedostatecznie omówione.

Opis i ocena wyników technicznych rozdziałów 5-9

Rozdział 5: optymalne układy implementujące skrzynki podstawieniowe

W rozdziale 5 Autor formułuje problem znalezienia układu złożonego z bramek NCT lub MCT implementującego daną odwracalną funkcję boolowską jako problem spełnialności SAT. Badane są skrzynki podstawieniowe i inne nieliniowe funkcje pochodzące z prymitywów kryptograficznych, m.in. Xoodyak, Elephant, GIFT-COFB, PHOTON-Beetle, Mini-AES, Whirlpool, JH, Ascon/ISAP oraz Keccak/ISAP. Rozważane są funkcje 3-, 4- i 5-bitowe. Dla każdej funkcji Autor bada kilka wariantów warunków początkowych: zestawy bramek NCT i MCT oraz różne liczby (qu)bitów pomocniczych.

Najbardziej konkretne wyniki rozdziału to tabele 5.3-5.8, zawierające długości znalezionych implementacji i same sekwencje bramek. Dla funkcji 3 x 3, 4 x 4 oraz części funkcji 5 x 5 uzyskano krótkie implementacje, np. dla Xoodyak układ sześciobramkowy, dla wybranych skrzynek 4-bitowych układy o długości 9-13, a dla Keccak i Ascon układy 12-17-bramkowe zależnie od zestawu bramek. Autor przedstawia następnie prostą transpilację tych układów do zestawu Clifford+T przy użyciu Qiskit.

Samo użycie SAT-solverów do syntezy małych obwodów odwracalnych jest metodologicznie poprawnem. Warto też odnotować, że Autor zebrał wiele wyników liczbowych w jednym miejscu. Jednak naukowa wartość tych wyników jest ograniczona. Badane funkcje są bardzo małe, a zastosowana procedura ma charakter de facto brutalnego przeszukiwania z pomocą SAT-solvera. Nie jest przekonująco wyjaśnione, co te konkretne wyniki dają dla realnej analizy kryptograficznej większych prymitywów. Brakuje też jasnego związku z kwantową teorią informacji poza obserwacją, że logika odwracalna jest potrzebna do konstrukcji wyroczni Grovera.

.

Część dotycząca transpilacji do Clifford+T jest w mojej ocenie bardzo słabo umotywowana. Zastosowanie ogólnego narzędzia do transpilacji kilku małych obwodów nie wnosi wiele naukowo, zwłaszcza że Autor sam zaznacza, iż uzyskane metryki nie są optymalne w nowym zestawie bramek.

Rozdział 6: synteza szablonów identyczności

Rozdział 6 dotyczy generowania szablonów identyczności, czyli obwodów odwracalnych realizujących funkcję identyczności. Autor opisuje algorytm naiwny, a następnie przyspiesza go dzięki generowaniu klas szablonów przez odbicie, permutację linii, rotacje oraz zamiany niezależnych bramek. W tabeli 6.1 pokazuje przyspieszenia względem algorytmu naiwnego, a w tabelach 6.2 i 6.3 liczbę znalezionych unikalnych szablonów identyczności do rozmiaru 6 x 7 oraz świadków suboptymalności do rozmiaru 6 x 4.

Jest to jeden z bardziej konkretnych fragmentów rozprawy. Wyniki są mierzalne, a metoda wykorzystująca symetrie szablonów jest naturalna i potencjalnie przydatna w praktycznej optymalizacji obwodów odwracalnych. Jednocześnie rozdział ma charakter bardziej katalogowy. Nie dostajemy głębszego opisu struktury przestrzeni szablonów, dowodów własności klas abstrakcji ani analizy tego, kiedy i jak świadkowie suboptymalności realnie przyspieszają syntezę optymalną.

W rozdziale pojawiają się też niejasności prezentacyjne. Skrót DFS używany jest w opisie algorytmu generowania, ale w tekście nie jest wprowadzony pedagogicznie. W szczególności czytelnik nie otrzymuje jasnego opisu, jakie dokładnie drzewo przeszukiwań jest tworzone i jak unikane są powtórzenia. Nie jest też dostatecznie wyjaśnione stwierdzenie, że szablony głębokości 2n-2 oraz 2n-1 są konieczne do znalezienia kompletu świadków suboptymalności o głębokości n. Ta obserwacja może być poprawna, ale powinna zostać sformułowana i uzasadniona znacznie precyzyjniej.

Rozdział 7: korelacja właściwości kryptograficznych

Rozdział 7 bada zależność między rozmiarem optymalnej implementacji małych skrzynek podstawieniowych jako układów MCT a klasycznymi parametrami kryptograficznymi: stopniem algebraicznym, stopniem nieliniowości, kryterium lawinowym, tablicą rozkładu różniczek oraz tablicą przybliżeń liniowych. Autor analizuje pełną przestrzeń 3- i 4-bitowych odwracalnych skrzynek podstawieniowych. Technicznie wykorzystuje przeszukiwanie grafu, którego wierzchołkami są permutacje, a krawędzie odpowiadają działaniu generatorów MCT. W naturalnym języku matematycznym jest to graf Cayleya odpowiedniej grupy permutacji względem wybranego zbioru generatorów; szkoda, że ta nazwa i związana z nią interpretacja nie pojawiają się w rozprawie.

Autor twierdzi, że obserwuje dodatnią korelację między „dobrymi” klasycznymi własnościami kryptograficznymi a rozmiarem implementacji. W szczególności, wybór profili kryptograficznych ma zmieniać rozkład rozmiarów obwodów. Ten wynik jest potencjalnie interesujący jako obserwacja empiryczna dla małych funkcji. Nie jest jednak wystarczająco przekonujący jako wynik o znaczeniu kryptograficznym. Po pierwsze, badane są wyłącznie skrzynki 3- i 4-bitowe, a realne prymitywy często korzystają z większych struktur. Po drugie, nie jest jasne, dlaczego rozmiar implementacji w bramkach MCT powinien być traktowany jako istotna miara bezpieczeństwa kwantowego. Po trzecie, wnioski z korelacji są przedstawione zbyt mocno: zbadanie pełnej przestrzeni małych skrzynek nie jest dowodem ogólnego twierdzenia dla skrzynek większych.

W rozdziale 7 brakuje też jasnej motywacji wyboru i sposobu obliczania parametrów kryptograficznych dla ogólnych odwracalnych skrzynek podstawieniowych. Autor koncentruje się m.in. na stopniu nieliniowości, ale nie wyjaśnia wystarczająco, dlaczego nie analizuje pełniejszego rozkładu widma Walsha-Hadamarda, rzędu, rozkładów częstości ani innych statystyk. Definicje tablic różniczek i przybliżeń liniowych są przedstawione dość formalnie, ale bez przekonującego wyjaśnienia, jak ich wartości mają być interpretowane w kontekście kryptograficznym.

Autor podkreśla poprawę względem pracy Golubitskiego i Maslova, m.in. skrócenie czasu przeszukiwania przestrzeni z 13 dni do 3,5 dnia. Tego typu porównanie jest jednak mało informatywne bez ścisłej normalizacji sprzętu, implementacji i środowiska obliczeniowego. Sam fakt uruchomienia algorytmu na innym sprzęcie nie stanowi istotnego wkładu naukowego, o ile nie towarzyszy mu analiza algorytmiczna lub udostępnienie niezależnie weryfikowalnego kodu i danych.

Rozdziały 8 i 9: ataki Grovera na SPARKLE i Ascon

Rozdziały 8 i 9 przedstawiają oszacowania zasobów potrzebnych do ataku Grovera na wybrane szyfry lekkie AEAD: SPARKLE oraz Ascon. Schemat jest analogiczny do klasycznej pracy M. Grassla, B. Langenberga, M. Roettelera i R. Steinwandta „Applying Grover's Algorithm to AES: Quantum Resource Estimates", PQCrypto 2016, 29-43. Ogólna idea polega na skonstruowaniu odwracalnej implementacji funkcji szyfrującej, użyciu jej jako części wyroczni Grovera, a następnie przemnożeniu kosztu wyroczni przez liczbę iteracji rzędu 2^{|K|/2}.

W rozdziale 8 Autor rozkłada szyfry rodziny SPARKLE na elementy składowe: dodawanie stałych rundowych, warstwę podstawieniową opartą o skrzynkę ARX Alzette, warstwę przestawieniową oraz operacje pomocnicze używane w konstrukcji gąbki. Następnie szacuje koszt wyroczni szyfrującej dla wariantów SCHWAEMM128-128, SCHWAEMM192-192, SCHWAEMM256-128 i SCHWAEMM256-256 oraz koszt pełnego ataku. W rozdziale 9 analogiczna analiza wykonana jest dla Ascon-128 i Ascon-128a. Autor uwzględnia warianty bez użycia tagu uwierzytelnienia, z użyciem tagu oraz wariant minimalny, w którym dopuszcza się ryzyko kolizji kluczy.

Na pierwszy rzut oka taki program badawczy jest adekwatny: aby oszacować koszt ataku Grovera, trzeba znać koszt wyroczni. Problem polega jednak na interpretacji wyników. Dla szyfrów z kluczem 128-bitowym liczba iteracji Grovera jest rzędu 2^64. Już bez jakiejkolwiek szczegółowej analizy implementacji wyroczni wiadomo więc, że koszt czasowy jest astronomiczny. Gdyby skrajnie optymistycznie założyć, że całe pojedyncze wywołanie wyroczni wraz z narzutami trwa tylko 10^{-6} sekundy (szacowany czas realizacji pojedynczej bramki kwantowej w reżimie fault tolerance), samo 2^64 wywołań trwałoby około 5,8 x 10^5 lat. Założenie to jest zresztą absurdalnie korzystne dla atakującego, ponieważ rzeczywista wyrocznia składałaby się z wielu logicznych bramek kwantowych.

To elementerne oszacowanie znacząco podważa praktyczne znaczenie analiz z rozdziałów 8 i 9. Dokładne policzenie, czy jeden wariant wyroczni ma kilka lub kilkadziesiąt procent mniej bramek, nie zmienia faktu, że atak Grovera na przestrzeń kluczy 128-bitowych pozostaje poza jakimkolwiek realistycznym horyzontem technologicznym. Tymczasem w podsumowaniu rozprawy pojawiają się daleko idące sugestie, że wyniki mogą mieć znaczenie dla procesów analizy bezpieczeństwa kryptografii narodowej, bezpieczeństwa wewnętrznego czy obrony narodowej. W mojej ocenie są to konkluzje zdecydowanie przesadzone w stosunku do rzeczywistego znaczenia wyników.

Należy też podkreślić, że przyszłe ataki kwantowe na kryptografię symetryczną mogą potencjalnie wykorzystywać prymitywy algorytmiczne inne niż algorytm Grovera. Jeśli takie ataki zostaną opracowane, analiza kosztu oparta wyłącznie na wyroczni Grovera może nie mieć do nich zastosowania.

Uwagi krytyczne

Moja zasadnicza krytyka dotyczy nie tylko poszczególnych błędów technicznych, ale ogólnego poziomu rozprawy. Praca jest napisana niestarannie, miejscami niepedagogicznie, a jej główne wnioski są często niewspółmierne do uzyskanych wyników. Wstęp zawiera wiele informacji o kryptografii lekkiej i konkursach NIST, ale nie wyjaśnia w sposób przystępny, na czym dokładnie polega „lekkość" kryptografii lekkiej: czy chodzi o rozmiar układu sprzętowego, zużycie energii, pamięć, opóźnienie, szerokość danych, czy kompromis między tymi parametrami. Pojawiają się liczne skróty i nazwy protokołów, ale brakuje podstawowych intuicji dla czytelnika spoza wąskiej specjalizacji. Cele pracy

nie wynikają naturalnie z wprowadzenia, a pojęcia kluczowe dla dalszego tekstu, takie jak skrzynka podstawieniowa czy szablon identyczności, nie są na początku objaśnione nawet na poziomie intuicyjnym.

Rozdział 2, poświęcony modelowi obliczeń kwantowych, zawiera szczególnie niepokojące błędy. Wprowadzenie ma charakter zbioru luźnych definicji i nie tworzy spójnej narracji. Referencje do prac Blocha, Cohen-Tannoudjiego i Shankara jako źródeł modelu obliczeń kwantowych są nieadekwatne; brakuje standardowych odniesień do podręczników i prac z obliczeń kwantowych. Wiele omawianych faktów jest elementarnych, a mimo to przedstawione są one nieprecyzyjnie. Na stronie 22 obiekt oznaczony jako H_n jest przestrzenią ilorazową unormowanych wektorów względem fazy globalnej, czyli raczej przestrzenią stanów czystych/projective Hilbert space niż przestrzenią wektorową; nie można więc w niej wskazywać bazy w zwykłym sensie liniowym. Opis kuli Blocha redukuje stan qubitu do sfery, pomijając stany mieszane. Definicja stanów splątanych we wzorze 2.15 jest niepoprawna formalnie: skoro produkt stanów pojedynczych qubitów ma być podzbiorem H_n, to różnica H_1^n \ H_n powinna być pusta, a nie zbiorem stanów splątanych.

Rozdział 3 zawiera wiele bardzo prostych faktów o permutacjach ciągów bitów i bramkach odwracalnych. Nie byłoby to samo w sobie problemem, gdyby służyło to przejrzystemu wprowadzeniu do późniejszych wyników. Niestety, tekst jest miejscami nieprecyzyjny i zawiera dziwne sformułowania, np. że aby skorzystać z darmowości rotacji, trzeba nadać qubitom indeksy fizyczne i logiczne. Literatura dotycząca syntezy i kompilacji układów kwantowych jest dobrana przypadkowo i nie tworzy wiarygodnego obrazu dziedziny. Zabrakło natomiast podstawowej dyskusji o uniwersalności zestawów bramek i twierdzeniu Solovaya-Kitaeva, które jest jednym z kanonicznych punktów odniesienia przy kompilacji obwodów kwantowych.

Rozdział 4 przedstawia algorytm Grovera w sposób elementarny, lecz mało informatywny. Podobny materiał można znaleźć w standardowych podręcznikach, np. u Nielsena i Chuanga, i nie stanowi on samodzielnej wartości rozprawy. Dyskusja ataku na szyfr symetryczny poprawnie identyfikuje ideę odbicia fazy na podstawie znanej pary tekst jawny-szyfrogram, ale nie prowadzi do adekwatnej oceny praktycznego znaczenia takiego ataku. Autor w zbyt małym stopniu podkreśla, że Grover daje jedynie pierwiastkowe przyspieszenie i w standardowym modelu nie łamie praktycznie używanych długości kluczy symetrycznych, a jedynie sugeruje podwojenie długości klucza w celu zachowania marginesu bezpieczeństwa.

Rozdział 5 ma problem z metodologią dowodzenia optymalności. O ile samo sformułowanie problemu syntezy jako SAT jest naturalne, to w rozprawie brakuje pełnej postaci równań, dokładnej formuły CNF, certyfikatów UNSAT oraz informacji umożliwiających niezależną weryfikację negatywnych wyników dla mniejszych głębokości. Bez tego twierdzenia o optymalności są słabo udokumentowane. Ponadto wyniki dotyczą wyłącznie małych funkcji 3-, 4- i 5-bitowych, a ich wpływ na praktyczne bezpieczeństwo kryptograficzne jest niejasny.

Rozdział 6 wprowadza świadków suboptymalności, ale nie pokazuje przekonująco, czy i kiedy ich użycie rzeczywiście poprawia syntezę optymalną ogólnych obwodów. Rozdział 7 myli obserwację empiryczną dla małych przestrzeni z mocniejszym wnioskiem o projektowaniu bezpiecznych skrzynek podstawieniowych. Rozdziały 8 i 9 przedstawiają obszerne tabele kosztów, ale pomijają najważniejszą interpretację: nawet minimalny atak Grovera na klucz 128-bitowy wymaga astronomicznej liczby wywołań wyroczni, a więc nie stanowi praktycznego zagrożenia. W rezultacie najdalej idące konkluzje rozprawy nie są uzasadnione przez przedstawione wyniki.

Istotny jest również ogólny poziom redakcyjny. W tekście występują błędy językowe, niezręczności terminologiczne, nierówna notacja i niedostateczne uzasadnienia przejść. Część referencji sprawia wrażenie dobranych przypadkowo i nie wspiera bezpośrednio twierdzeń, przy których się pojawia.

Pytania do treści rozprawy

1. W przypadku funkcji Ascon w rozdziale 5 nie potwierdzono optymalności. Jak należy interpretować późniejsze użycie tej implementacji w rozdziale 9? Czy wszystkie końcowe oszacowania kosztu ataku są wyłącznie górnymi ograniczeniami?
2. Jaki jest praktyczny sens transpilacji małych układów NCT/MCT do Clifford+T przy użyciu Qiskit, skoro otrzymane liczby nie są optymalne ani nie są powiązane z konkretną architekturą, kodem korekcyjnym lub kosztem bramek T?
3. Czy istnieje teoretyczne uzasadnienie korelacji badanej w rozdziale 7, czy jest to wyłącznie obserwacja empiryczna dla 3- i 4-bitowych skrzynek podstawieniowych? Jak silne są podstawy do ekstrapolacji tych wyników na większe S-boxy, takie jak skrzynka AES?
4. Dlaczego analiza własności kryptograficznych w rozdziale 7 ogranicza się do wybranych zagregowanych wielkości, a nie uwzględnia pełniejszych statystyk, takich jak rozkład wartości transformacji Walsha-Hadamarda?

Podsumowanie i konkluzja

Rozprawa podejmuje temat ważny i aktualny, a Autor wykonał pewną ilość pracy implementacyjnej i obliczeniowej. Do pozytywnych elementów zaliczam zebranie kosztów implementacji wybranych elementów kryptograficznych, użycie SAT-solverów do syntezy małych układów odwracalnych oraz opublikowanie części wyników w czasopismach. Nie są to jednak, w mojej ocenie, zalety wystarczające do pozytywnej oceny całości.

Najważniejsze wyniki rozprawy są ograniczone do małych przypadków, mają głównie charakter numeryczno-inżynierski i nie są wystarczająco mocno powiązane z realną oceną bezpieczeństwa kryptograficznego. Co gorsza, warstwa wprowadzająca i formalna zawiera elementarne błędy dotyczące podstaw obliczeń kwantowych i stanów kwantowych. Rozprawa jest także słabo napisana, nieprecyzyjna terminologicznie i nadmiernie rozbudowana w miejscach elementarnych, podczas gdy kluczowe kwestie metodologiczne pozostają niewystarczająco wyjaśnione.

W mojej ocenie przedstawiona rozprawa w obecnym kształcie nie spełnia standardów merytorycznych i redakcyjnych oczekiwanych od rozprawy doktorskiej w dyscyplinie informatyka techniczna i telekomunikacja. Nie rekomenduję przyjęcia rozprawy ani nadania Panu mgr. inż. Adamowi Jagielskiemu stopnia doktora na jej podstawie.

Warszawa, 07.06.2026