

ПРОБЛЕМИ БЕЗПЕКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СУЧАСНИХ ПРОЦЕСОРІВ

Шевель О. С., ст. (гр. КВ-83мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Дана робота присвячена дослідженню проблем безпеки та перспектив розвитку сучасних процесорів. Було розглянуто ситуацію в галузі на даний час, та описано можливі варіанти розвитку даної галузі. Також проведено аналіз щодо перспектив кожної з технологій.

Ключові слова: комп'ютери, процесори, Закон Мура, нанотрубки, фотони.

Abstract: This paper is devoted to the study of security problems and prospects for the development of modern processors. The situation in the region at present was reviewed, and possible options for the development of the industry were described. In addition, an analysis was conducted regarding the prospects of each of the technologies.

Keywords: computers, processors, Moore's law, nanotubes, photons.

Вступ. В останні 40 років ми спостерігали, як швидкість комп'ютерів зростала експоненціально. У сьогоднішніх центральних процесорах тактова частота в тисячу разів вище, ніж у перших персональних комп'ютерів на початку 1980-х. Об'єм оперативної пам'яті на комп'ютері виріс в десять тисяч разів, а місткість жорсткого диска збільшилася більш ніж в сто тисяч разів.

Разом зі збільшенням обчислювальної потужності дана технологія постійно модернізувалася, ставала складнішою, менш очевидною, а як відомо, чим складніша система, тим більше в ній вразливих місць. Питання безпеки загалом повинні вирішуватися шляхом змін у апаратній або програмній частині, змін, які виключають можливість виникнення так званих дірок в безпеці. Але в умовах складності, обмеженого часу та високої вартості виробникам простіше зробити якесь додаткове обмеження, або додати нову перевірку до вже готової системи, яка буде виступати латкою для певної дірки в безпеці.

З часом архітектура процесорів «обросла» такими латками, що не могло не вплинути на їх швидкодію, енергетичну ефективність, а також на вартість. Одними з останніх, а також одними з самих масштабних вразливостей, які було виявлено за останні роки стали Meltdown та Spectre, які вразили відповідно процесори від компанії Intel та AMD. Тимчасові рішення які були прийняті компаніями для вирішення проблеми, пов'язаної з даними вразливостями, сповільнили деякі моделі процесорів до 30%, що є неприйнятним. Ці проблеми буде вирішено в одному з майбутніх поколінь процесорів, але це є гарним прикладом того, що іноді треба кардинально змінювати підхід, щоб уникнути ефекту снігової кулі.

Але проблема безпеки не єдиний привід щось змінити, ми зараз наближаємося до фізичної межі, де швидкість обчислень обмежена розміром атома і швидкістю світла. Ми наближаємося до межі, де розмір транзистора складає всього кілька атомів. Інше фізичне обмеження – це швидкість передачі даних, яка не може перевищувати швидкість світла. Потрібно декілька тактових

циклів, щоб дані потрапили з одного кінця CPU в інший кінець. У міру того як мікросхеми стають більшими та з більшою кількістю транзисторів, швидкість починає обмежуватися самою передачею даних на мікросхемі.

Мета дослідження

Отже, які є інші шляхи покращення безпеки сучасних процесорів та збільшення їх потужності? Напівпровідникова індустрія експериментує з матеріалами, які можна використовувати замість кремнію. Деякі напівпровідникові матеріали III-V здатні працювати на більш низькій напрузі і на більш високих частотах, ніж кремній, але вони не роблять атоми менше або світло повільніше. Фізичні обмеження як і раніше в силі.

Основна частина

Коли-небудь ми зможемо побачити тривимірні багат шарові чіпи. Це дозволить ущільнити схеми, зменшити відстані, а отже, і затримки. Але як ефективно охолоджувати такий чіп, коли енергія поширюється всюди всередині нього? Будуть потрібні нові технології охолодження. Мікросхема не зможе передавати енергію на всі схеми одночасно без перегріву. Їй доведеться тримати відключеними більшість своїх частин основну частину часу і подавати харчування в кожную частину тільки під час її використання.

Зараз кращі можливості щодо поліпшення продуктивності, як я думаю, з програмної сторони. Розробники ПЗ швидко знайшли застосування експоненціальному зростанню продуктивності сучасних комп'ютерів, який стався завдяки закону Мура. Програмна індустрія стала використовувати її, а також почала використовувати більш і більш просунуті інструменти розробки і програмні фреймворки.

Ці високорівневі інструменти розробки і фреймворки зробили можливим прискорити розробку ПО, але за рахунок споживання більшої кількості обчислювальних ресурсів кінцевим продуктом. Багато які з сьогоденних програм досить марнотратні у своєму надмірному споживанні апаратної обчислювальної потужності.

Протягом багатьох років ми спостерігали симбіоз між апаратною і програмною індустріями, де остання виробляла все більш просунуті і ресурсомісткі продукти, які підштовхували користувачів купувати все більш потужне обладнання. Оскільки швидкість зростання апаратних технологій сповільнилася, а користувачі перейшли на маленькі портативні пристрої, де ємність батареї важливіше, ніж продуктивність, програмної індустрії тепер доведеться змінити курс.

Їй доведеться урізати ресурсомісткі інструменти розробки і багаторівневий софт і розробляти програми, не так набиті функціями. Терміни розробки збільшаться, але програми стануть споживати менше апаратних ресурсів і швидше працювати на маленьких портативних пристроях з обмеженим ресурсом батареї. Якщо індустрія комерційного ПЗ зараз не змінить курс, то може поступитися часткою ринку більше аскетичним продуктам open source.

Щодо безпеки, перехід на абсолютно нові технології дозволить почати все з початку та розроблювати системи з урахуванням минулого досвіду, які не обтяжені теперішньою кількістю латок та мають апаратно більш безпечну та закриту структуру. Як приклад величезна кількість шляхів злому системи пов'язана з перевантаженнями, якщо розробити новий тип процесорів в яких такий сценарій оброблюється апаратно, то ми отримаємо систему заздалегідь більш безпечну.

Тепер саме час поговорити про нові і альтернативні технології.

IBM: Нанотрубки. Нещодавно було опубліковано статтю про створення 5нм техпроцесу, що дозволяє створювати більш продуктивні і економічні процесори. Сьогодні IBM публікує ще одну важливу новину – справа в тому, що фахівці корпорації, використовуючи матеріали нового типу, створили транзистори, які менше всіх інших транзисторів за розміром і в той же час швидше.

Новий матеріал – це вуглецеві нанотрубки, згорнуті листи атомів вуглецю товщиною в 1 нанометр. Про існування даного матеріалу відомо давно, але ось створювати щось або з нього було складно через низку його особливостей. На даний час фахівцям вдалося опанувати дану технологію, та створити перші дослідні зразки.

Але, на жаль, це лише прототип, який не можна використовувати. В результаті було вирішено створити окремі транзистори, і це себе виправдало. Кожен з 192 транзисторів вийшов робочим. Після цього вчені розробили дослідну схему кільцевого генератора, яка запрацювала. Вийшло 55 кільцевих генераторів із загальною продуктивністю в 2,8 ГГц. Правда, не всі генератори вийшли робочими, оскільки всього було зроблено близько 160 спроб.

Але через кілька років активної роботи технологію можна довести до можливості практичного її використання.

Фотонна технологія. Дослідження в цій галузі велися ще в 80-х роках Седжівом Джоном. Насправді він вивчав явище локалізації світлових хвиль можливість якої сам і довів. Як з'ясувалося, при зміні електромагнітних властивостей середовища за певним законом, в ній утворюються фотонні заборонені зони ФЗЗ (photonic band gap), в яких фотони існувати не можуть.

Таким чином, світло в них має не будь-яку довжину хвилі і не будь-який напрямок, і в певному сенсі локалізується. Звичайно, виникає напівпровідникова аналогія із забороненими зонами і приналежністю електронів лише особливим, строго обмеженим енергетичним рівням. Попросту кажучи, перспектива відкриття в тому, що місце електронів в новій технології займуть фотони. При цьому, що цікаво, не обов'язково використання оптоволоконних технологій в конструктивних схемах.

До особливо вигідних переваг світла перед електрикою особливо хотілося б підкреслити, що, по-перше, промені (потoki) світла ніяк не реагують один на одного, і, внаслідок цього, можуть бути зведені на мікро відстань і не вимагають взаємної ізоляції. По-друге, хотілося б відзначити, що проходження

світла через речовина не викликає такого колосального тепловиділення, як той же електрострум.

Але в кожній бочці меду є своя ложка дьогтю. Так і у ФЗЗ-технології є свої складності. Головне, це те, що явище ФЗЗ в природних діелектриках не зустрічається, а значить, необхідний цілий ряд специфічних умов (певний інтервал довжин хвиль) для його відтворення.

Але вже зараз вчені здатні синтезувати тривимірні ФЗЗ структури в області близько 1,5 мкм. Тут використовуються кристали все того ж кремнію з симетрично розташованими сферичними порожнинами, куди вводиться рідкокристалічна речовина.

Подібні процесори поки не можуть виступати в якості елемента повноцінного комп'ютера, зате можуть послужити в ролі прискорювачів при виконанні певних завдань, наприклад, обробки алгоритмів комп'ютерної графіки або обробки іншого великого масиву даних.

Висновки. На цій ноті, хочеться закінчити, бо про перспективність тієї чи іншої технології можна говорити дуже довго, однак не нам вирішувати – які ідеї втілювати в життя. Як показує історія, не одна технологія народилася в променях «безперечною» перспективності, і не одна геніальна технологія залишилася позаду потяга індустрії.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Fog A. Moores law hits the roof [Електронний ресурс] / Agner Fog. – 2015. – Режим доступу до ресурсу: <https://www.agner.org/optimize/blog/read.php?i=417>.

2. Череповский К. О перспективах и существующих технологиях создания полупроводниковых устройств [Електронний ресурс] / Костянтин Череповский. – 2001. – Режим доступу до ресурсу: <https://3dnews.ru/172015>.

3. Кузнецов В. Hewlett Packard создали фотонный процессор Hewlett Packard создали фотонный процессор [Електронний ресурс] / Володимир Кузнецов. – 2017. – Режим доступу до ресурсу: <https://hi-news.ru/technology/hewlett-packard-sozdali-fotonnyj-processor-s-tysyachej-komponentov-na-chipe.html>.

4. Уильямс М. IBM совершает прорыв в области углеродных нанотрубок [Електронний ресурс] / Мартін Уильямс. – 2015. – Режим доступу до ресурсу: <https://www.osp.ru/news/articles/2015/42/13047455/>.

5. В IBM создали новое поколение транзисторов из углеродных нанотрубок [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://habr.com/company/ibm/blog/333000/>.

Збірник матеріалів Дев'ятнадцятої Всеукраїнської науково-методичної конференції (з участю студентів) “Проблеми охорони праці, промислової та цивільної безпеки”.

Редакційна колегія:

О.Г. Левченко, докт. техн. наук, проф., зав. каф. ОППЦБ – головний редактор,
Ю.О. Полукаров, канд. техн. наук, доц. – заступник головного редактора,
науковий редактор
Т.Є. Луц, ст. викладач – член оргкомітету