

УДК 006.029

ВИМОГИ ТА СТАН СТАНДАРТИЗАЦІЇ ПОТОКОВИХ СИМЕТРИЧНИХ ШИФРІВ НА МІЖНАРОДНОМУ РІВНІ

Андрій Нейванов, Іван Горбенко

Харківський національний університет радіоелектроніки

Анотація: В цій тезі описуються вимоги та стан стандартизації поточкових симетричних шифрів на міжнародному рівні.

Summary: This summary describes the requirements and state of the standardization stream symmetric ciphers at the international level.

Ключові слова: Стандартизація, поточкові симетричні шифри, інформаційна безпека.

Історія стандартизації поточкових симетричних шифрів дуже коротка та не дуже розповсюджена. На протязі 2001 року, коли почалася робота над стандартом ISO/IEC 18033 не було жодних пропозицій міжнародного стандарту шифрування. Саме це вплинуло на рішення ISO/IEC не робити стандартів на алгоритми шифрування. Це рішення виникає також в зв'язку з невдалою спробою у середині 1980-х зробити алгоритм DES міжнародним стандартом з ряду політичних причин.

Як результат, ми маємо лише стандарти описуючи поточкові шифри як режими CTR, OFB та CFB блокових симетричних шифрів. Також помітні поточкові шифри A 5/1, A 5/2 та A 5/3 розроблені для використання в GSM мережах; поточковий шифр RC4 стандартизований для використання з IEEE 802.11 бездротові мережі як частина розповсюдженої системи за назвою WEP (Wired Equivalent Privacy – еквівалент приватної дротової системи); та поточковий шифр функція f_8 системи зв'язку UMTS/3GPP. Далі ми поверхово розглянемо ці алгоритми.

Поточкові шифри A 5/1 та A 5/2 були двома схемами спочатку включеними до стандарту GSM. Використання цих двох схем було обов'язковим, але деталі алгоритмів тримались у таємниці. На протязі 1990 алгоритм був підданий методу «зворотної інженерії», що дозволило виявити в обох алгоритмах серйозні вразливості. По факту, алгоритм A 5/2 було навмисно зроблено як більш слабку версію алгоритму A 5/1 як пропозицію для обмеженого експорту. Враховуючи ці труднощі і те що обидва алгоритми були сконструйовані в 1980 роках, той факт, що ці алгоритми успішно атакували не є сюрпризом.

В результаті ці алгоритми замінили на новий алгоритм, який отримав назву A 5/3. Цей алгоритм базується на режимах роботи блокового симетричного шифру KASUMI та вважається безпечним. Однак проблеми пов'язані з шифруванням GSM лишилися. Наприклад, можна заставити телефон використовувати алгоритми A 5/1 чи A 5/2 для компрометації ключа алгоритму A 5/3.

RC4 був розроблений Рівестом у 1980-х, і спочатку його операції не піддавались огласці. Повні деталі алгоритму були невідомі до 1994 року. На даний час він є дуже розповсюджений та використовується як одна із технологій шифрування SSL. Однак затвердження його як частини IEEE 802.11b WEP протоколу зробило його більш популярним. Також за багатьма джерелами задокументовано, що використання алгоритму RC4 таким чином, яким він використаний в протоколі WEP не є безпечним. Про це пишуть Флукхер, Мантон та Шамір описуючи небажані властивості ключової схеми алгоритму RC4 у випадку коли частина ключа відома.

Як ми вже казали, алгоритм A 5/3 використовує режим блочного симетричного шифру KASUMI. Також це стосується функції f_8 використовуваної для поточкового шифрування в мобільних системах зв'язку UMTS/3GPP яка базується також на алгоритмі KASUMI.

15 червня 2005 року вийшов стандарт ISO/IEC 18033-4 який присвячений інформаційній безпеці і зокрема поточковим симетричним шифрам. Це мабуть один з перших стандартів міжнародного рівня де вперше з'являються поточкові шифри. У ньому зображено ті поточкові симетричні системи які ISO/IEC рекомендує для використання на міжнародному рівні.

За змістом наведені у стандарті ISO/IEC 18033-4 поточкові симетричні системи можна поділити на три групи. Група перша містить у собі загальну модель для поточкових симетричних шифрів. Друга група являє собою поточкові симетричні шифри (ключові генератори) основані на режимах OFB, CTR та CFB блокових симетричних шифрів. Третя група містить у собі виділені для використання поточкові генератори.

Як було сказано вище перша група описує загальну модель для поточкових симетричних шифрів. Як відомо, поточкові симетричні шифри складаються з комбінації ключових генераторів або генераторів ключового потоку та функцій виходу. Тому першу групу можна поділити за змістом на дві підгрупи. Це підгрупа присвячена генераторам ключового потоку та підгрупа вихідних функцій або так би мовити

функцій виходу. Генератори ключового потоку являються методом для генерації псевдо-випадкової послідовності символів (зазвичай біт) з секретного ключа, стартового значення і, можливо, деяких інших вхідних даних. Вихідні функції визначають як саме вихід з генератора ключового потоку (ключовий потік) буде поєднаний з відкритим текстом при формуванні криптограми.

В той же час підгрупа генераторів ключового потоку теж складається з двох підгруп. Вона включає в себе під-підгрупу синхронних генераторів ключового потоку та під-підгрупу генераторів ключового потоку самостійної синхронізації. Другі відрізняються від перших тим фактом, що при втратах синхронізації в каналі зв'язку «шифратор-дешифратор» (при затримці) здатні відновлювати її.

Підгрупа вихідних функцій також поділяється на дві під-підгрупи. Це під-підгрупа функцій які забезпечують тільки конфіденційність інформації (до неї входить часто використовувана у поточних системах функція XOR) та під-підгрупа функцій які забезпечують конфіденційність та цілісність даних (до неї за стандартом ISO/IEC 18033-4 входить функція MULTI-S01). Також важливо буде помітити, що під-підгрупа функцій які забезпечують конфіденційність та цілісність даних використовується тільки з під-підгрупою синхронних генераторів ключового потоку. З під-підгрупою генераторів ключового потоку самостійної синхронізації ця під-підгрупа не взаємодіє.

Друга група, як було вже наведено вище, являє собою ключові генератори основані на режимах блокових симетричних шифрів. Це режими CTR (Counter – лічильник), OFB (Output Feedback – зворотного зв'язку за виходом) та CFB (Ciphertext Feedback – зворотного зв'язку за шифртекстом). Ключові генератори на основі режимів лічильника та зворотного зв'язку за виходом можна віднести до синхронних генераторів ключового потоку, а ключові генератори на основі режиму зворотного зв'язку за шифртекстом можна віднести до генераторів ключового потоку самостійної синхронізації. Не маловажний той аспект, що хоча усі ці ключові генератори основані на режимах роботи БСШ і задовольняють вимогам безпеки, вони виявляються дуже повільними на відміну від ключових генераторів спеціально розроблених для високошвидкісних операцій.

Третя група, як сказано вище, описує виділені для використання потокові генератори. В неї за стандартом ISO/IEC 18033-4 входять алгоритм SNOW 2.0 та алгоритм MUGI.

Алгоритм SNOW 2.0 є прямим нащадком алгоритму SNOW 1.0 вперше опублікованим у 2000 році. Також відомо, що алгоритм SNOW 2.0 дозволяє використовувати 128 бітний та 256 бітний ключі та використовує змінні стани які складаються з 18 32 бітних блоків (усього 576 біт). Нова версія алгоритму здатна протистояти атакам реалізованим на попередню версію.

Алгоритм MUGI базується на генераторі ключового потоку Панама запропонованим Дайменом і Клапом в 1998 році. Основна ціль змін була спрямована на те, щоб зробити модель більш ефективною для апаратної реалізації та зробити аналіз безпеки простої моделі. Алгоритм MUGI дозволяє використовувати 128 бітний ключ та використовує змінні стани які складаються з 19 64 бітних блоків (усього 1216 біт).

В висновку хотілося б додати, що це лише один стандарт існуючий на міжнародному рівні в якому описані потокові симетричні системи. На державному рівні в Україні аналогічних стандартів не існує.

Як ми можемо побачити на даний час дуже повільно просувається стандартизація поточкових симетричних шифрів на міжнародному рівні. Багато аспектів впливають на її стан. Основними з них хочеться відзначити відкриті (прозору) структуру алгоритму, що ми не завжди бачимо. Можливість атакувати та досліджувати систему різними випробувачами. Мала кількість відкритих конкурсних проектів.

Врахувавши усі ці аспекти, або так би мовити вимоги, можна прискорити стандартизацію на міжнародних рівнях та звісно на рівнях держав.