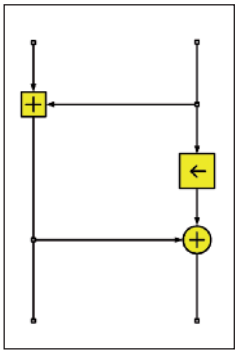
CipherCAD – kryptoanalýza s radostí

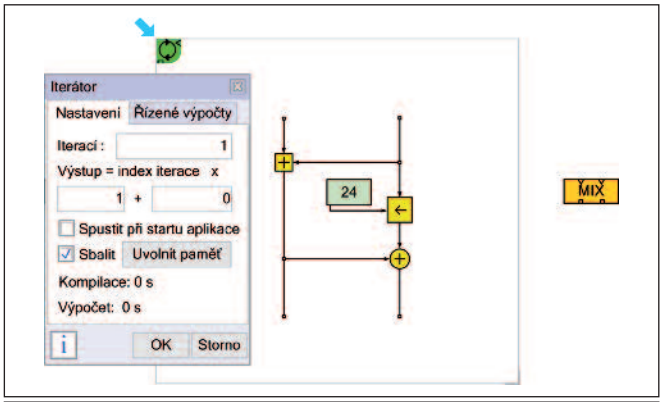
V tomto článku bude představen velice pěkný program CipherCAD výzkumníků z Brna, jehož vznik inicioval Národní bezpečnostní úřad [1]. Je to grafický programovací nástroj, který může být využit k modelování a zkoumání kryptografických funkcí, protokolů apod. Po přečtení článku čtenáře jistě napadne, že by se mohl hodit i k modelování a zkoumání chování jakýchkoliv jiných funkcí.

Modelování

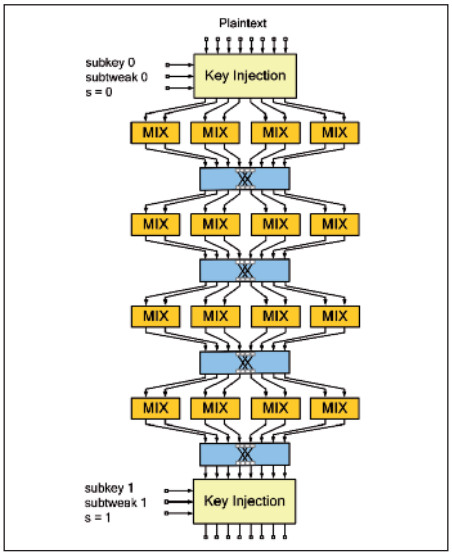
Abychom představili jeho schopnosti, ukážeme si ho v akci na modelu hašovacího algoritmu Skein-512-512, kandidáta na standard



Obr. 1 Pomocí spojů a komponent vzniká logická struktura MIX



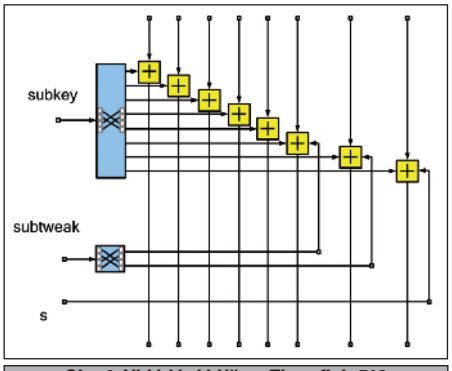
Obr. 2 Iterátor, zapouzdření a vznik nové funkce MIX



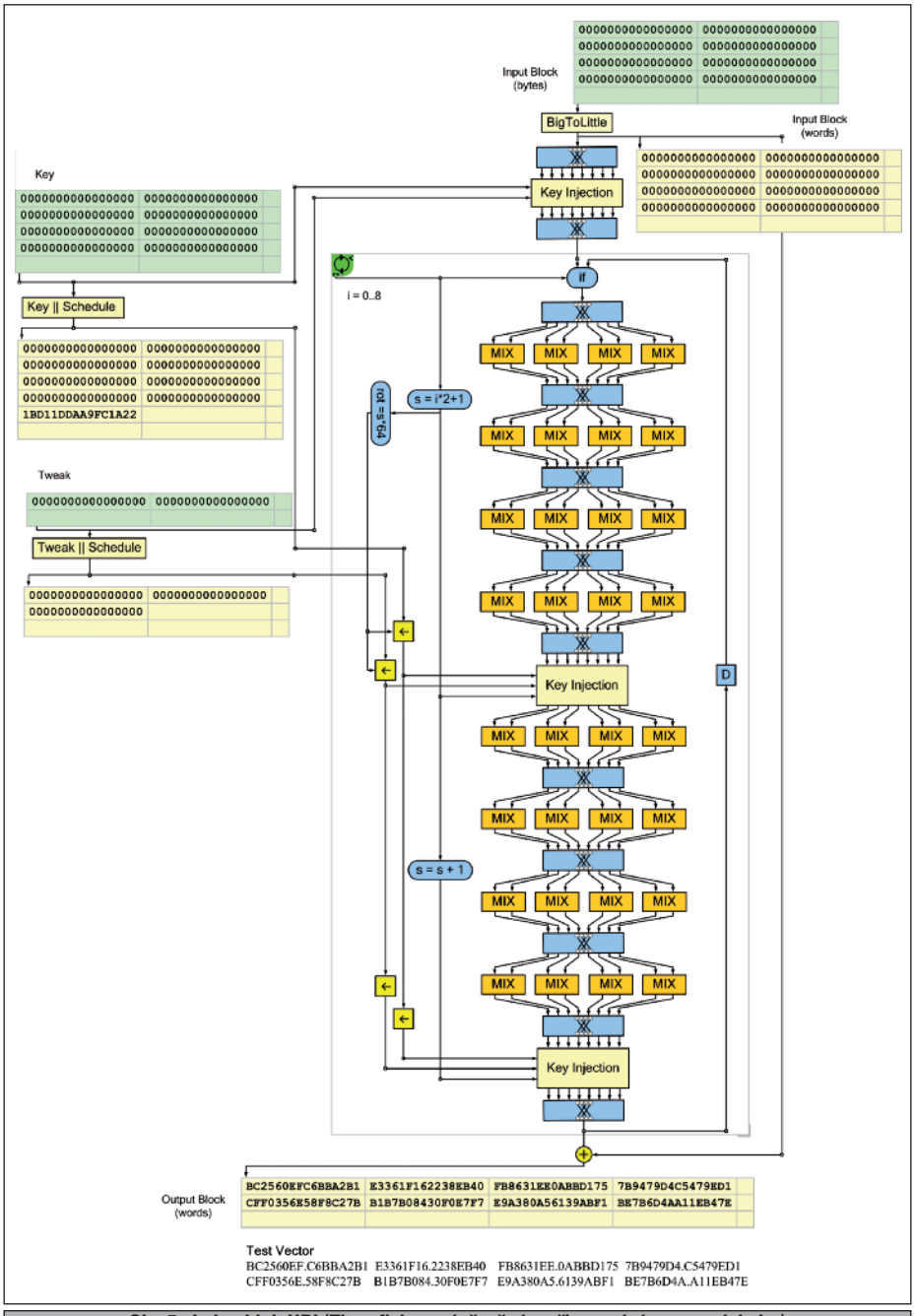
Obr. 3 Čtyři ze 72 rund blokové šifry Threefish-512

hašovací funkce SHA-3 [2]. Jeho jádrem je tweakovatelná bloková šifra Threefish-512 s klíčem o 512 bitech a tweakem o 128 bitech. Threefish využívá operace XOR, ADD (sčítání dvou 64bitových čísel modulo 2^{64}) a ROT (rotace o konstantní počet bitů) se 64bitovými slovy. Z těchto operací je sestavena nová malá funkce nazvaná MIX, viz *obr. 1*. Sestavování provádíme pomocí kontextového menu a spojovacích čar – prostě kreslíme schéma.

Pokud nakreslíme nějakou malou funkci, kterou budeme dále hojně používat,

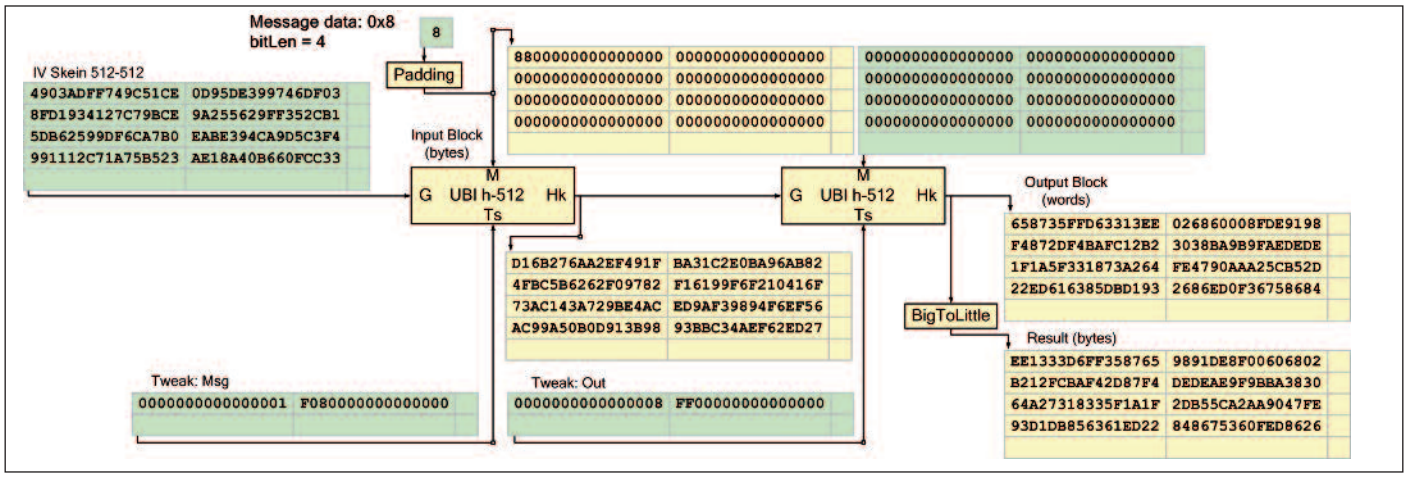


Obr. 4 Vkládání klíče v Threefish-512



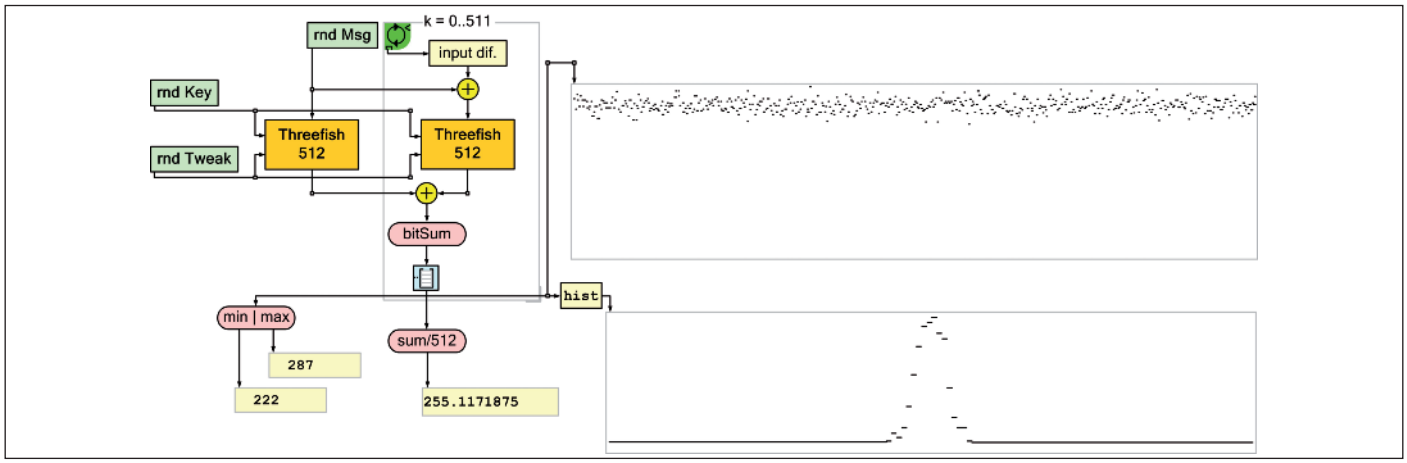
Obr. 5 Jeden blok UBI (Threefish se závěrečným přixorováním vstupních dat)

můžeme ji tzv. zapouzdřit, tj. z ní vytvořit stavební částečku, reprezentovanou malým obdélníčkem. Zapouzdření této struktury do tzv. iterátoru (kolečko vlevo v rohu no hašování dat tak, jak ukazuje *obr. 6*. Zde se (pro jednoduchost obrázku) hašuje zpráva o čtyřech bitech. Ovšem tímto zřetězením můžeme pomocí UBI zpracovat *obr. 7* je test lavinovitosti pro celou blokovou šifru Threefish-512 se 72 rundami. Z výsledků je vidět, že nedochází k významným odchylkám od předpokládaných pa-



Obr. 6 Zobrazení průběžných hodnot UBI při hašování zprávy „1000“ o délce 4 bit

struktury), sbalení do obdélníku a označení nové funkce jako MIX je vidět na *obr. 2*. MIX je nově vzniklá funkce, která má dva zprávu libovolné délky. Pokud budete chtít vědět všechny detaily definic, stačí nahlédnout do [2]. rametrů a z histogramu je patrné, že se změní vždy kolem poloviny výstupních bitů.



Obr. 7 Test lavinovitosti metodou kráčejícího bitu pro blokovou šifru Threefish-512

64bitové vstupy a dva 64bitové výstupy, a odteď ji můžeme používat jako nový stavební blok.

Pomocí MIX a dalších nových stavebních bloků (permutace a key injection), vytvoříme větší stavební blok, tvořený 4 vrstvami (rundami) blokové šifry Threefish. Ta má 72 rund, z nichž každá se skládá ze čtyř funkcí MIX a jedné permutace osmi 64bitových slov, viz *obr. 3*.

Vždy po čtyřech rundách je na data přičten příslušný podklíč, jak ukazují *obr. 3* a *obr. 4* (key injection).

Na *obr. 5* je znázorněn celý algoritmus Threefish s přídavným závěrečným přixorováním otevřeného textu. Hlavní částí Threefish je iterátor, který obsahuje osm rund a je volán devětkrát, což dává 72 rund Threefish. Výstup z jedné iterace je veden na vstup další iterace pomocí paměťové komponenty „zpětná vazba D“. Pokud funkci na *obr. 5* opět sbalíme, dostaneme blok UBI. Pomocí UBI je pak už definová-

V CipherCADu je možné zobrazit libovolnou hodnotu přímo ve schématu, jak je to vidět u vstupů a výstupů bloků UBI na *obr. 6*.

Kryptoanalýza v CipherCADu

Po vytvoření modelu algoritmu lze za pomoci CipherCADu provádět různá zkoumání algoritmu. Jeden ze základních testů u blokových šifer je test lavinovitosti, který testuje zda změna jednoho bitu na vstupu vede ke změně každého bitu na výstupu s pravděpodobností 0.5. Aby bylo možno otestovat vliv každého jednotlivého bitu na vstupu blokové šifry, postupujeme s měnícím se bitem od nejméně významného až po nejvíce významný bit vstupního bloku (metoda kráčejícího bitu). Nyní pro každou vstupní pozici vypočítáme, kolik se změnilo bitů výstupního bloku. Výsledek zobrazíme v grafu, kde na ose x je pozice vstupní jednobitové diference a na ose y je počet bitových změn na výstupu. Na

Závěr

V příspěvku jsme uvedli některé možnosti aplikace CipherCAD pro kryptoanalýzu. Ukazuje se, že je to velmi dobrý a názorný nástroj pro kryptoanalytické zkoumání i srovnávací analýzy. Pokud byste se chtěli seznámit s dalšími ukázkami kryptoanalýzy, jsou součástí příspěvku autorů na konferenci SPI konané 10. až 12. května 2011 v Brně (http://spi.unob.cz) a budou k dispozici v archivu [3].

Vlastimil Klíma, kryptolog,
vlastimil.klima@knzsro.cz
Václav Plátěnka, Univerzita obrany,
vaclav.platenka@unob.cz

LITERATURA:

[1] Sobotík, J., Plátěnka, V.: Aplikovaný výzkum a rozvoj pracoviště pro návrh a analýzu kryptografických systémů. Závěrečná zpráva k projektu NBÚ. Brno, 2009.

[2] Skein: http://www.skein-hash.info/.

[3] Archiv (článků ST) 1. autora: http://cryptography.hyperlink.cz.