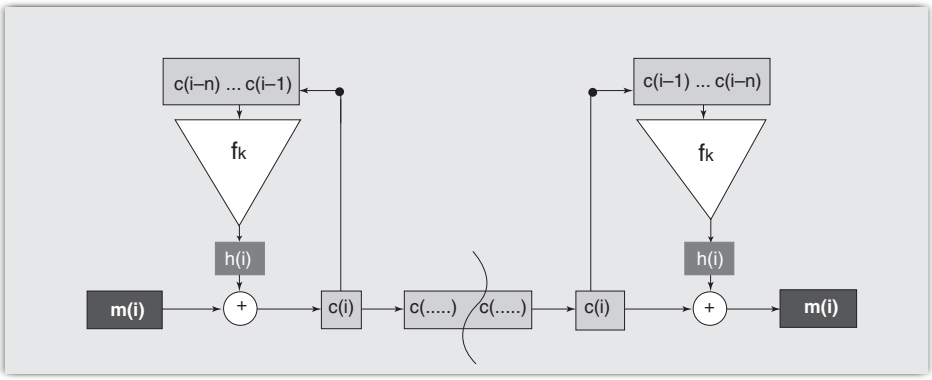
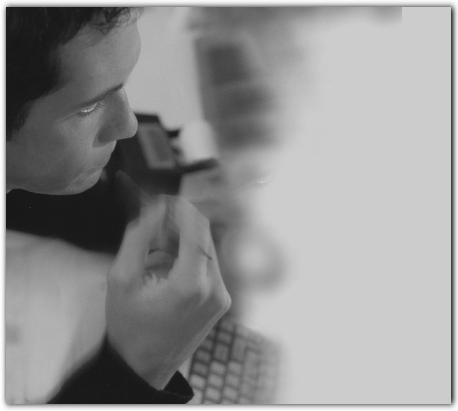
Kryptologie pro praxi – asynchronní šifry pro zarušené spoje

Slovem „asynchronní" v praxi většinou označujeme přenosové protokoly, při nichž není implicitně přepokládána synchronizace vysílací a přijímací strany. Nejčastěji se jedná o synchronizaci časovou, avšak možné jsou i jiné varianty (pořadí bitů, atp.). Pojem asynchronní však neznamená, že bychom z přenosového schématu synchronizaci zcela eliminovali. Zjednodušeně vzato pouze říkáme, že synchronizační informaci musí nést samotná data. Důvodem pro zavedení bývá efektivní využití přenosové kapacity s ohledem na proměnlivou míru aktuálně přenášené informace, například při přenosu reálného obrazu, hlasu apod. U šifrovacích algoritmů se obracíme k asynchronním variantám zejména v případě, kdy potřebujeme eliminovat vliv chyb na přenosovém kanále. I zarušené spoje totiž často nesou citlivá data, která je zapotřebí chránit.

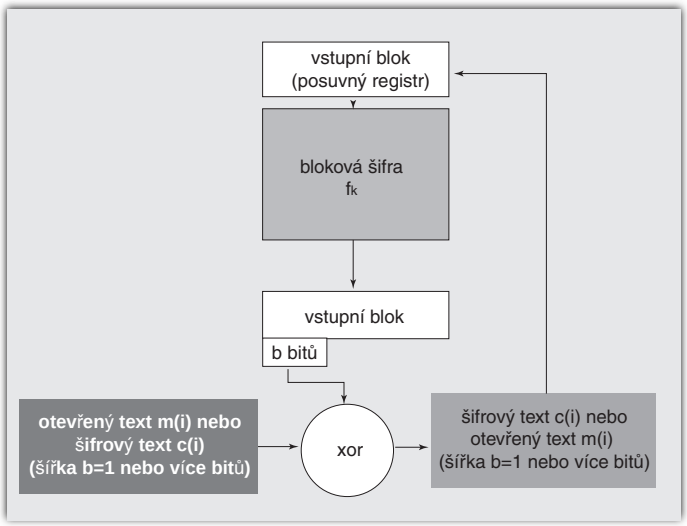


Obr. 1 Princip asynchronní proudové šifry



Ilustrace problému

Předpokládejme, že máme na zarušeném kanále zajistit důvěrnost tak, aby použitá šifra za prvé nesnížila rychlost přenosu a za druhé nezvýšila chybovost kanálu. První požadavek je víceméně splnitelný. Míra zpomalení závisí na technických parametrech spojení a výběru vhodného algoritmu. Pokud použijeme Vernamovu šifru (ST 7/2003, [6]), potřebujeme k zašifrování sice obrovské množství klíče, ale pro zašifrování jednoho bitu postačuje už jen jediná operace: *xor*. Vernamova šifra nám tak se zcela zanedbatelným zpomalením zajistí požadovanou důvěrnost. Běda ovšem, pokud se na kanálu ztratí jediný bit šifrového textu nebo jejich shluk. V ten okamžik dojde k porušení implicitní podmínky synchronního přenosu a přijímající strana začne systematicky používat správné heslo na nesprávné bity šifrového textu. Od té chvíle bude spojení trvale špatně dešifrováno. Tento problém se přitom týká většiny klasických proudových šifer, které pracují tak, že z nějakého počátečního nastavení na základě šifrovacího klíče generují proud hesla, který se *xoruje* na otevřený text při šifrování nebo na šifrový text při dešifrování. Výhodou tohoto uspořádání je, že proud hesla lze nezávisle na datech předvypočítat do vyrovnávací paměti a poté použít v okamžiku náporu intenzivního datového toku. Tím splníme požadavek propustnosti. Ta samá výhoda je však zároveň nevýhodou, neboť nezávislý výpočet hesla musí nutně spoléhat na implicitní synchronizaci šifrátoru s dešifrátorem. Z této ilustrace vidíme, že požadavky rychlosti a odolnosti proti chybám jsou v jistém směru protichůdné, a tak lze očekávat, že hledání optimálního řešení bude přinejmenším teoreticky zajímavá úloha. Přitom snad ani není nutné dodávat, že tato úloha je velmi zajímavá i z hlediska praktického.



Obr. 2 Blokovou šifru v modu CFB lze využít jako asynchronní proudovou šifru

Asynchronní proudové šifry

K řešení našeho problému byly zavedeny tzv. asynchronní proudové šifry, které sice také produkují heslo, které se *xoruje* na otevřený nebo šifrový text, ale toto heslo se vypočítává nejen v závislosti na klíči, ale i na bloku předchozích *N* bitů šifrového textu. V tomto případě, který znázorňuje *obr. 1*, skutečně dojde k požadované explicitní synchronizaci na přijímací straně. Stačí si uvědomit, že ke stanovení správného bitu hesla pro daný bit přijatého šifrového textu a pro bity následující, postačuje, aby byl správně přijat souvislý blok *N* bitů předchozího šifrového textu. Podle *obr . 1* se pak odpovídající bit hesla i bity hesla následující již budou počítat správně. Ztratí-li se na kanále shluk *D* bitů, zotaví se spojení z pohledu vysílače po *D*+*N* bitech.

Standardy

Před příchodem počítačové kryptografie v 80. letech minulého století byly nejpoužívanějšími proudovými šiframi šifry na bázi lineárních posuvných registrů se zpětnou vazbou. Registry (označme je souhrnně *ZPR*) se naplnily klíčovým materiálem (odvozeným například od klíče *K* a nějakého inicializačního vektoru). Poté funkce *f* (nazývaná nelineární filtr) vygenerovala bit hesla jako $f_K(ZPR)$, registry se posunuly atd. Také asynchronní

šifry se řešily tímto způsobem, jen do *ZPR* se plnil předchozí šifrový text v délce *N* bitů (*N* je zde souhrnná délka všech použitých lineárních registrů; obecněji to je délka zpětné vazby ze šifrového textu). Bit hesla se počítal opět jako $f_K(ZPR)$. Po příchodu počítačové kryptografie a rozvoji blokových šifer se od této konstrukce ustoupilo. K řešení našeho problému se začaly používat blokové šifry v modu zpětné vazby ze šifrového textu (CFB, Cipher Feedback). Téma využití blokových šifer k různým službám naleznete v článku ve *ST 9/2003* [6], kde je právě hovořeno o modech činnosti blokových šifer. Konkrétně schéma CFB ukazuje *obr. 2*, kde je vidět, že na vstup nelineárního filtru jde posledních *N* bitů šifrového textu, které jsou zpracovány blokovou šifrou. Z jejího výstupu se potom bere jeden nebo více bitů (například 8) jako heslo, což se poté značí CFB-*b* (například CFB-8). Heslo se pak už obvyklým způsobem *xoruje* na otevřený nebo šifrový text. Žádné jiné standardy pro asynchronní proudové šifrování než ty, které jsou založeny na CFB, nenaleznete.

Současné návrhy asynchronních šifer jsou nevyzrálé

Je to trochu kuriózní situace, že za posledních 20 let, kdy se kryptografie „exponenciálně" rozvětvila a prohloubila, nevznikl v oblasti asynchronních proudových šifer žádný nový standard. Vysvětlení je prosté. Na trhu byly k dispozici čipy, které realizovaly blokové šifry, a tak vývojáři použili s výhodou právě je. Rychlosti, kterých dosahují blokové šifry, dokázaly uspokojit většinu komerčních požadavků. Tam, kde jsou požadovány extrémně vysoké rychlosti, je potřeba si uvědomit, že bloková šifra určitým způsobem mrhá výkonností tím, že zahazuje část své produkce (*N–b* bitů), a není proto nejefektivnějším řešením pro generování jednoho bitu hesla. Použijeme-li 128bitovou šifru AES (viz ST 11/2003, [6]), lze pragmaticky odhadovat, že bychom mohli rychlost šifrování zvýšit až 128krát. To ovšem znamená nový návrh funkce *f* (nelineárního filtru) tak, aby byl kvalitní a zároveň rychlý, tj. nepříliš složitý. Tyto požadavky jsou ovšem v rozporu a kryptologové tento problém v komerční oblasti dosud uspokojivě nevyřešili. Od roku 1984 vznikly pouze tři koncepty konstrukce funkce f a u všech byly později nalezeny kryptografické slabiny ([1], [2], [3]). Posledním pokusem bylo navržení asynchronní šifry HBB v roce 2003 [4]. Loni bylo ovšem ukázáno, že i tato šifra je slabá, a to dokonce extrémně [5] (prezentace a článek z MKB v češtině je na [6]).

Proprietární šifry

Lze očekávat, že existuje velké množství komunikačních zařízení, která implementují proprietární asynchronní proudové šifry. Je to logické, neboť vývojáři realizující spojovací část mohou snadno integrovat i část šifrovací. Velká část těchto zařízení ovšem končí ve vojenství nebo na jiných citlivých místech. Proto se o používaných proprietárních šifrách (zejména jejich funkcích *f*) většinou nedozvíme ani ty nejzákladnější kryptografické vlastnosti, natož jejich schéma.

Závěr

Chcete-li spolehlivě vyřešit svůj problém s výběrem asynchronní proudové šifry, nezbývá dnes nic jiného, než použít standardní CFB-1 (nebo CFB-b, pokud je zajištěn přenos na úrovni b bitových jednotek) v kombinaci s vybranou blokovou šifrou. Zde pochopitelně doporučujeme opět standardy, nejlépe AES s 256bitovým klíčem. Jestliže nebudete schopni tímto způsobem pokrýt požadovanou rychlost spojení, nezbývá než použít proprietární šifru. Toto téma je však už bohužel daleko za hranicí našeho seriálu.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Proctor, N.: A Self-synchronizing Cascaded Cipher System With Dynamic Control of Error Propagation, Crypto _84, pp. 174 – 190, 1984

[2] Maurer, U.: New Approaches to the Design of Self-Synchronizing Stream Ciphers, Eurocrypt 91, pp. 458 – 471, 1991

[3] Daemen, J.: Cipher and Hash Function Design. Doctoral Dissertation, http://www.esat.kuleuven.ac.be/~cosicart/ps/JD-9500/, March 1995

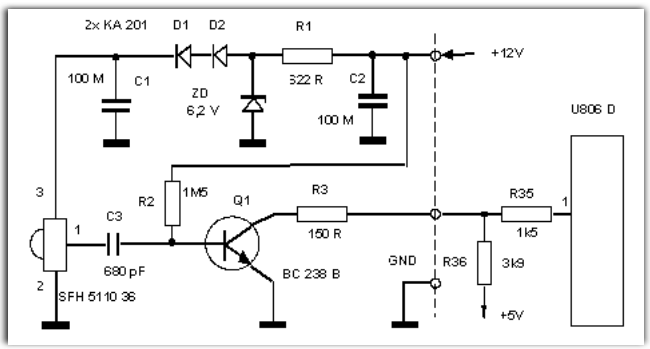
[4] Sarkar, P.: Hiji-bij-bij: A New Stream Cipher with a Self-Synchronizing Mode of Operation, INDOCRYPT 2003, pp. 36 – 51, 2003

[5] Klíma, V.: Cryptanalysis of Hiji-bij-bij (HBB), IACR ePrint archive, Report 2005/003, January 2005, http://eprint.iacr.org/2005/003.pdf, prezentováno na workshopu MKB 2004, Praha, http://www.tns.cz/kryptobesidka/, prosinec 2004

[6] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz

Dialkové ovládanie a elektromagnetický smog

Prijímače diaľkového ovládania moderných televíznych prijímačov používajú ako prijímač diaľkového ovládania integrovanú štruktúru s TTL výstupom. Staré modely prijímačov používali nie príliš šťastnú kombináciu infradiódy a tranzistora JFET v impulznom režime, napríklad KS 4393V. Takéto riešenie je extrémne citlivé na elektromagnetický smog. Znižuje sa citlivosť modulu, resp. dochádza k deštrukcii vstupných častí hromadením náboja na hradle tranzistora JFET.



Obr. 1 Schéma zapojení ovladače

Na *obr. 1* je možné náhradné riešenie, prispôsobené pre „archaické" televízne prijímače. Zapojenie rešpektuje obvodovú štruktúru za rozhraním konektora *Z64*. Prúdový odber obvodu SHF (stredná hodnota pri aktivite) je iba 1,3 mA. V danom zapojení je na vývode 3 menej ako 5 V a obvody zaťažia zdroj 12 V menej ako pôvodný modul, ktorý bol naviac dokonale tienený v úplne uzavretom kovovom kryte. Signálový vodič rozhrania po mikroprocesor je v prípade problémov vhodné tieniť a uzemniť iba na strane infraprijímača. Hodnoty C_3, R_2, a typ Q_1 je potrebné dodržať, aby úroveň na ovládaných častiach za rozhraním bola rovnaká ako v prípade pôvodného modulu.

Problém je zvlášť aktuálny v podmienkach s intenzívnym signálom bezdrátových sietí pásma 2,4 GHz, keď bežné Wireless karty pracujú aj s odpojeným koaxiálným káblikom. Taktiež úrovne v LW, SW a VHF pásmach často prekračujú normu zostavenú európskou komisiou CENELEC v dobe, keď o podobnej prevádzke sa viedli iba teoretické úvahy.

Pre iné aplikácie použitý infraprijímač nepotrebuje pre napájanie prúdovú limitáciu, iba dodržanie doporučeného U_{CC}. Signálový výstup obvodu SHF 5110 36 kHz (resp. 40 kHz) má v kľude potenciál U_{CC} a platnú úroveň impulzov 0 V.

Ing. Jaroslav Rákoš, CSc.