Využití RSA pro dohodu na klíči

Vlastimil Klíma

Využití šifry RSA pro dohodu na klíči je překvapivé. Dohoda na klíči je totiž tradičně spojena se slavným vynálezem a protokolem Diffie-Hellmann. Důvodem, proč NIST vydal standard i pro dohodu na klíči pomocí RSA, je ten, že mnohé čipy a SW knihovny mají už zabudovánu víceúčelovou funkci RSA, ale ne protokol Diffie-Hellmann. Přitom použití RSA pro protokol stejných vlastností je velmi jednoduché.

Norma NIST

K čemu je taková dohoda na klíči [1] je dobrá? Může to být například pro šifrování e-mailů nebo hovorů mezi dvěma komunikujícími stranami, které se neznají. Z nich jen jedna strana může být „zavedená“, tj. mít certifikát, zatímco druhá strana nemusí být vedena v žádném systému, ale chce „zavedené“ straně šifrovaně zatelefonovat či poslat e-mail. Volané straně nemusí vadit, že jí šifrovaně volá nebo šifrovaně e-mailuje někdo neznámý. Naproti tomu ten, kdo se komunikace dožaduje, je rád, že příjemce je skutečně ten, kdo je uveden v certifikátu. Tím má jistotu, že hovor nebo e-mail odšifruje jen potvrzený příjemce. Jednostranná autentizace může být prakticky užitečná. Na druhé straně, pokud certifikáty mají obě strany, je přirozené, když je využijí k oboustranné autentizaci. Pro tyto účely tu tedy máme dva protokoly, které se mírně odlišují v tom, zda iniciátor protokolu má nebo nemá certifikát, zatímco u příjemce předpokládáme, že certifikát má vždy. Případ, že ani jedna ze stran certifikát nemá, je nadmíru zajímavý a budeme se mu věnovat naposled. V první fázi protokolu si obě strany nějak ustaví společný klíč. Pak nastává jednostranná nebo oboustranná autentizace, pokud to obě strany chtějí a mají k tomu certifikát. Ukážeme si variantu, kdy obě strany mají certifikát a obě strany chtějí autentizaci od partnera. Zbylé varianty vznikají zjednodušením tohoto protokolu, viz *tabulka*.

Tabulka KAS2 – protokol výměny klíče s oboustrannou autentizací

Krok	Odesílatel U		Příjemce V
1	Má k dispozici: $PubKey_U$, $PrivKey_U$		Má k dispozici: $PubKey_V$, $PrivKey_V$
2	Odešle svůj veřejný klíč $PubKey_U$	$PubKey_U \rightarrow$	Obdrží veřejný klíč strany U
3	Obdrží veřejný klíč strany V	$\leftarrow PubKey_V$	Odešle svůj veřejný klíč $PubKey_V$
4	Generuje náhodné Z_U, zašifruje ho pomocí veřejného klíče RSA příjemce: $C_U = ENC_{PubKeyV}(Z_U)$	$C_U \rightarrow$	Odšifruje C_U, získá Z_U
5	Odšifruje C_V, získá Z_V	$\leftarrow C_V$	Generuje náhodné Z_V, zašifruje ho pomocí veřejného klíče RSA příjemce: $C_V = ENC_{PubKeyU}(Z_V)$
6	Vypočte $Z = Z_U \| Z_V$		Vypočte $Z = Z_U \| Z_V$
7	Nyní obě strany sdílí společné tajemství Z, z něhož odvodí potřebné klíče pro šifrování následné komunikace (DataKey) a pro autentizaci (MacKey). Následuje výměna autentizačních tokenů na bázi MacKey.		
8	Vypočte autentizační token $MacTag_U$	$MacTag_U \rightarrow$	Zkontroluje autentizační token $MacTag_U$. Je-li platný, strana U je autentizovaná k V.
9	Zkontroluje autentizační token $MacTag_V$. Je-li platný, strana V je autentizovaná k U.	$\leftarrow MacTag_V$	Vypočte autentizační token $MacTag_V$
Protokol může pokračovat výměnou dat, šifrovaných na bázi klíče DataKey.			

Bez certifikátu pozor na Muže uprostřed

Z hlediska výpočtů jsou kroky 8 a 9 v protokolu nejsložitější, avšak jejich podstata je jednoduchá – na bázi dohodnutého tajemství Z a „čerstvých“ (právě teď v protokolu vzniklých) hodnot C_U a C_V vytvořit hodnoty MacTagU a MacTagV, které nemůže vytvořit nikdo jiný než vlastník hodnoty Z. To

Komentáře k tabulce

Krok 1: Obě strany mají v plné verzi protokolu k dispozici i certifikáty svých veřejných klíčů.

Krok 2: U odešle svůj veřejný klíč $PubKey_U$. Může ho poslat samotný nebo v rámci certifikátu nebo ho neodesílá vůbec, protože ho nemá, případně si ho strana V může stáhnout z veřejného místa.

Krok 4: Při zašifrování se používá veřejný klíč protistrany, při dešifrování vlastní privátní klíč.

Krok 7: Výpočet hodnoty sdíleného tajemství je jednoduché – je to zřetězení dvou náhodných řetězců obou stran. Na sdíleném tajemství se tedy podílí obě strany. V jednostranné variantě protokolu, kde odesílatel nemá veřejný klíč, strana V posílá místo C_V prostě náhodné číslo N_V, které vstupuje do následujících výpočtů místo Z_V. Tím se opět obě strany podílí na vytvoření sdíleného tajemství Z. Výpočty hodnot klíčů a tokenů jsou následující: Klíč pro výpočet autentizačního tokenu je MacKey a klíč pro šifrování dat je DataKey. Vypočtou se pomocí funkce pro odvození klíčů (viz Sdělovací technka 10–12/2010, [2]) KDF takto: MacKey || DataKey = KDF (Z, ID_U, ID_V), kde ID_U, ID_V jsou vhodné jednoznačné identifikátory komunikujících stran.

Krok 8 a 9: MAcKey použijeme jako klíč ve funkci MAC (Message Authentication Code, viz ST 9/2003, [2]), které předložíme k autentizaci následující data MacData. Při jednostranné autentizaci V vůči U máme $MacData = MacData_V$ = =„KC_1_V“ || ID_V || ID_U || N_V || C_U. Při oboustranné autentizaci máme $MacData_V$ = „KC_2_V“ || ID_V || ID_U || C_V || C_U a $MacData_U$ = „KC_2_U“ || ID_U || ID_V || C_U|| || C_V. Použitím funkce MAC s klíčem MacKey na data MacData získáme u jednostranné autentizace autentizační kód $MacTag_V$ = MAC(MacKey, $MacData_V$) a u oboustranné autentizace $MacTag_V$ = = MAC(MacKey, $MacData_V$) a $MacTag_U$ = = MAC(MacKey, $MacData_U$).

vede zpětně k důkazu znalosti příslušného privátního klíče, neboli k autentizaci pomocí certitikátu. Pokud certifikát chybí u obou stran, nikdo neví, s kým komunikuje. Tím, že chybí certifikát veřejného klíče, certifikační autorita neověřila identitu vlastníka příslušného privátního klíče. Nemůžeme o něm tedy vědět nic jiného, než že „je to ten, kdo nám poslal veřejný klíč“ (viz krok 2 a 3) nebo „ten, kdo má privátní klíč k jím zaslanému veřejnému klíči“. Je to pochopitelné, protože my mu přijatým veřejným klíčem něco posíláme a může to rozšifrovat jen vlastník privátního klíče. Tento klíč ovšem nemá přiřazenu žádnou identitu.

Útočník, který se umí postavit doprostřed mezi komunikující strany, pak na obě strany vede uvedený protokol „za sebe“. Ve skutečnosti tak může vytvořit „jenom router“, čili data poslouchá, ale přehazuje je z jedné strany na druhou tak, jak chtějí obě strany. Nebo může data jakkoli měnit nebo může dokonce v routeru vytvořit virtuální existenci protistrany. Z tohoto maléru nelze jednoduše vybřednut. V případě šifrované hlasové komunikace, kdy dotyčného člověka známe, máme určitou šanci muže uprostřed zjistit, a to jednoduše tím, že si vzájemně hlasově přečteme kousek veřejného klíče našeho i protistrany (nebo jeho digitální otisk). Ovšem pozor, pokud to děláme v našem utajeném kanálu, máme smůlu, pokud si Mužíček uprostřed nahraje náš hlas v době, kdy vyslovujeme jednotlivé cifry nebo čísla. Pak může v době ověřování pouštět namísto vyslovování našeho otisku vyslovování jeho otisku naším hlasem. Čili vidíme, že na stávajícím komunikačním kanálu to bude obtížné. Pokud však máme jiný komunikační kanál, kterým můžeme náš veřejný klíč nebo jeho otisk předat s naší identitou (třeba e-mailem v případě hlasové komunikace nebo pomocí SMS v případě e-mailového spojení), můžeme tím do jisté (a někdy zcela postačující) míry nahradit certifikační autoritu a dostatečně spojit veřejný klíč s naší identitou. Potom můžeme čerpat výhody uvedeného protokolu – ustavení společného klíče a následnou autentizaci a utajení spojení.

LITERATURA

[1] Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, NIST Special Publication 800-56B, August 2009, http://csrc.nist.gov/publications/PubsSPs.html.

[2] Archiv článků autora na http://cryptography.hyperlink.cz.

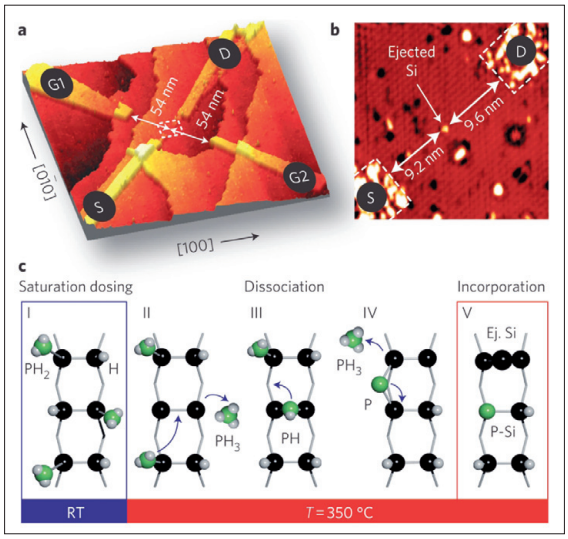
Jednoatomový tranzistor

Schopnost manipulovat s hmotou na úrovni jednotlivých atomů a vytvářet z nich elektronické součástky a logické obvody je základem pro budoucí nanotechnologie. Postupy založené na elektrickém odporu umožňovaly vytvářet struktury v měřítku atomů na povrchu křemíku, ale vytvoření fungující součástky, jako je tranzistor s extrémně malými hradly, kvantový počítač založený na spinu nebo optoelektronické součástky s jednotlivými dopanty vyžaduje schopnost umísťovat jednotlivé atomy na křemíkovém substrátu s přesností na úrovni jednotlivých atomů.

Vědcům z Univerzity v Novém Jižním Walesu (University of New South Wales, UNSW) se podařilo vytvořit fungující tranzistor, který se skládá z jediného atomu přesně umístěného ve struktuře křemíkového krystalu. Tato miniaturní elektronická součástka, která je popsaná v článku publikovaném v časopisu Nature Nanotechnology, využívá jako aktivní prvek (dopant) jednotlivé atomy fosforu umístěné do křemíkové struktury mezi elektrody a elektrostatická řídicí hradla. Taková dosud nevídaná přesnost na úrovni jednotlivých atomů se může stát základním stavebním kamenem pro budoucí kvantové počítače s obrovskou výpočetní výkonností.

„Až dosud byly jednoatomové tranzistory realizovány jen náhodně, a to buď když vědci hledali ve velkém počtu elektronických prvků, anebo když se snažili vytvořit logický prvek z několika atomů, a pak izolovat atom, který funguje. Ovšem naše součástka je dokonale přesná“, uvedl profesor Michelle Simmons, vedoucí skupiny a ředitel centra ARC pro kvantové výpočty a komunikačních technologií v UNSW. „Je to poprvé, co je někdo schopen manipulovat s jedním atomem na křemíkovém substrátu s takovou úrovní přesnosti.“

„Mikroskopická součástka má dokonce drobné viditelné značky vyryté na povrchu, takže výzkumní pracovníci mohou připojit kovové kontakty a aplikovat napětí,“ uvádí výzkumný pracovník Dr. Martin Fuechsle z UNSW.



Obr. 1 Jednoatomový tranzistor založený na deterministickém umisťování atomu fosforu na epitaxním křemíkovém substrátu

„Náš tým prokázal, že je skutečně možné umístit jeden atom fosforu do křemíkové struktury, a to přesně tak, jak potřebujeme, s téměř atomickou přesností a současně zapisovací hradla.“

Podle Dr. Fuechsle elektronické vlastnosti součástky přesně odpovídají teoretickým předpokladům skupiny profesora Gerharda Klimecka z Purdue University v USA a skupiny profesora Hollenberga z univerzity v Melbourne.

Tým z Univerzity v Novém Jižním Walesu použil řádkovací tunelový mikroskop (Scanning Tunneling Microscope, STM), kterým lze vidět a manipulovat s atomy na povrchu krystalu uvnitř komory s velmi vysokým vakuem při teplotě kapalného helia. Pomocí procesu elektronové litografie byly jednotlivé dopanty, tj. atomy fosforu, deterministicky uspořádány do funkčních prvků na epitaxním křemíkovém substrátu, a následně pokryty vrstvou nereaktivního vodíku. Atomy vodíku byly odebrány selektivně v přesně vymezených oblastech super jemným kovovým hrotem STM. Řízená chemická reakce pak začlenila atomy fosforu do křemíkového povrchu.

Konečná struktura byla zapouzdřena vrstvou silikonu a součástka elektricky připojena pomocí složitého systémů nastavení značek na křemíkovém čipu pro připojení ke kovovým kontaktům. Elektronické vlastnosti součástky byly ve shodě s teoretickými předpoklady pro tranzistor z jednoho atomu fosforu. Podle prognózy Moorova zákona se odhaduje, že tranzistory dosáhnou úrovně jednoho atomu kolem roku 2020, což naznačuje pokračující trend v počítačovém hardwaru, kdy se počet tranzistorů na čipu zdvojnásobuje každých 18 měsíců. „Toto významné vylepšení povede k technologii, která bude jednak umožňovat rychlejší dosažení limitů Moorova zákona, jednak poskytovat cenné poznatky o chování takových součástek v atomickém měřítku,“ uvedl profesor Simmons.