Algorithms of Information Security: Feige-Fiat-Shamirův identifikační protokol

Faculty of Information Technology
Czech Technical University in Prague

October 21, 2020

Feige-Fiat-Shamirův identifikační protokol

Algorithm 1 Feige-Fiat-Shamirův identifikační protokol

SOUHRN. A dokazuje znalost s uživateli B v t iteracích 3-průchodového protokolu.

1. *Výběr parametrů systému.* Důvěryhodné centrum T po výběru dvou tajných prvočísel p a q každé kongruentné s 3 modulo 4 zveřejňuje společný modulus $n = pq$ pro všechny uživatele, a to takový, že n je výpočetně nerealizovatelné faktorizovat. Celá čísla k a t jsou definována jako parametry zabezpečení.

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

2. *Výběr tajemství podle jednotlivých entit.* Každá entita A provádí následující.
   - Vybere k náhodních celých čísel $s_1, s_2, \ldots, s_k$ v rozsahu $1 \leq s_i \leq n-1$, a k náhodných bitů $b_1, \ldots, b_k$. (Z technických důvodů je vyžadováno $gcd(s_i, n) = 1$, ale to je téměř jistě zaručeno, protože jinak lze faktorizovat n.)
   - Spočte $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1}$ mod n pro $1 \leq i \leq k$.
   - A se identifikuje nekryptografickými prostředky (např. občankou) T, u které si následně zaregistruje veřejný klíč $A : (v_1, \ldots, v_k; n)$, zatímco pouze A zná svůj soukromý klíč $(s_1, \ldots, s_k)$ a n. Tímto je dokončena jednorázová fáze nastavení.

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

3. *Zprávy protokolu.* Každá z t iterací má tři zprávy v následujícím tvaru.

$$A \to B : x \ (= \pm r^2 \bmod n) \tag{1}$$

$$A \leftarrow B : (e_1, \ldots, e_k), e_i \in \{0, 1\} \tag{2}$$

$$A \to B : y \ (= r \cdot \prod_{e_j=1} s_j \bmod n) \tag{3}$$

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

4. *Akce protokolu.* Následující kroky jsou provedeny $t$krát; B přijímá identitu A pokud všechny iterace t uspějí. Předpokládejme, že B má autentický veřejný klíč $A : (v_1, \ldots, v_k; n)$; jinak může být certifikát zaslán ve zprávě (1).
   - A vybere náhodné celé číslo $r, 1 \leq r \leq n-1$, a náhodný bit b; vypočítá $x = (-1)^b \cdot r^2 \bmod n$ a pošle x (svědka) B.
   - B pošle A (výzvu), náhodný $k-$bitový vektor $(e_1, \ldots, e_k)$.
   - A vypočítá a odešle B (odpověď) $y = r \cdot \prod_{j=1}^{k} s_j^{e_j} \bmod n$.
   - B spočte $z = y^2 \cdot \prod_{j=1}^{k} v_j^{e_j} \bmod n$, a ověří, že $z = \pm x$ a $z \neq 0$ (to vylučuje úspěch protivníka výběrem $r = 0$).