# FORWARD SECURE DIGITAL SIGNATURE SCHEME

Tomáš WAGNER, Master Degree Programme (5)
Dept. of Information Systems, FIT, BUT
E-mail: xwagne04@stud.fit.vutbr.cz

Supervised by: Dr. Daniel Cvrček

## ABSTRACT

I describe a digital signature scheme by Michael Abdalla and Leonid Reyzin, in which the public key is fixed but the secret signing key is updated at regular intervals so as to provide a forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be useful to mitigate the damage caused by key exposure without requiring distribution of keys. This scheme is based on the hardness of factoring.

## 1 ÚVOD

Velké množství dnešních kryptografických technik považujeme za zcela bezpečné. Při rozumných předpokladech můžeme skutečně dokázat jejich bezpečnost, to však platí jen tak dlouho, dokud není prozrazeno tajemství, na kterém jsou tyto techniky založeny (v našem případě soukromý klíč). Pokud je tato informace prozrazena, bezpečnost je zkompromitována nejen pro následující použití tajemství, ale také pro jeho všechna dřívější použití. Vlastnost dopředná bezpečnost snižuje potenciálního nebezpečí v případě vyzrazení tajemství.

## 2 POPIS SCHÉMA

Operace dopředné bezpečnosti (podepisování zprávy, ověřování zprávy, generování nového soukromého klíče) jsou rozděleny do několika časových úseků, kterým odpovídají různé soukromé klíče. Každý soukromý klíč je používán k podepisování zpráv pouze během jednoho časového úseku a na konci tohoto úseku je přepsán nově vygenerovaným soukromým klíčem. Ověřovací funkce kontroluje jestli je podpis platný a také jestli byl vytvořen během odpovídajícího časového úseku.

Schéma má vlastnost dopředné bezpečnosti, pokud je pro útočníka nemožné zaútočit na zprávy i po skončení platnosti klíčového páru, i když objeví soukromý klíč pro odpovídající časový úsek. Proto mohou být v tomto schématu bezpečné podpisy i v případě, že je současný soukromý klíč ohrožen.

## 2.1 TEORIE

Definujme k a l jako dva bezpečnostní parametry. Dále $p_1$ a $p_2$ s vlastnostmi:

$p_1 \equiv p_2 \equiv 3 \pmod 4$, tedy dvě prvočísla přibližně stejné velikosti. Dále definujme N, $N = p_1 p_2$ je k-bitové číslo. Q bude označovat množinu nenulových kvadratických zbytků modulo N.

Nechť $U \in Q$, potom definujme $F_0(Z) = Z^2 \bmod N$, $F_1(Z) = UZ^2 \bmod N$ a pro l-bitový binární řetězec $\sigma = b_1 \ldots b_l$ definujme:

$F_\sigma: Q \rightarrow Q$ jako $F_\sigma(Z) = F_{bl}(\ldots.(F_{b2}(F_{b1}(Z)))\ldots.) = Z^{2^l} U^\sigma \bmod N$

Protože druhá mocnina je permutace přes Q a $U \in Q$, $F_\sigma$ je permutací přes Q. Je velmi obtížné vypočítat $F_\sigma^{-1}$, pokud neznáme druhou odmocninu z U.

## 2.2 GEOMETRICKÁ INTERPRETACE

Použijeme kompletní binární strom hloubky l, kde každý uzel obsahuje hodnotu z Q. V kořenu (na vrcholu stromu) je uložena hodnota Y. Hodnoty synů uzlu, který obsahuje A jsou $F_0^{-1}(A)$ jako hodnota uložená v levém synu a $F_1^{-1}(A)$ jako hodnota uložená v pravém synu. Potom výpočet $F_\sigma^{-1}(Y)$ vyjadřuje nalezení hodnoty listu, pro který je cesta z kořene dána $\sigma$ (ve kterém směr zprava do leva odpovídá směru shora dolů ve stromě).

Je velmi snadné vypočítat z daného uzlu hodnotu na vrcholu stromu, ale velmi obtížné vypočítat hodnotu nacházející se níže ve stromu bez schopnosti získat její druhou odmocninu. Pokud známe dvě cesty z listu stromu, můžeme získat druhou odmocninu kořene U pomocí hodnot synů z uzlu, kde se obě cesty setkávají.

Poznamenejme, že hodnota R uložená na levém-spodním listu stromu je

$F_{00\ldots0}^{-1}(Y) = Y^{2^{-l}}$, tedy pokud známe $S = 1/U^{2^{-l}}$ a R, můžeme získat hodnotu libovolného listu (daného pomocí $\sigma$) vypočítáním $RS^\sigma \bmod N$.

## 2.3 POPIS OPERACÍ

Podpisující vygeneruje modul N, vybere náhodné $S \in Q$, aby jej použil jako soukromý klíč. Vypočítá $U = 1/S^{2^l}$ a vrátí (N,U) jako veřejný klíč.

Abychom podepsali zprávu M, musíme nejprve vygenerovat náhodné $R \in Q$ a vypočítat $Y = R^{2^l}$ (tímto získáme schopnost nalézt libovolný list binárního stromu s kořenem v Y). Dále vypočítáme $\sigma = H(Y,M)$ a $Z = F_\sigma^{-1}(Y) = RS^\sigma \bmod N$ jehož výstupem je podpis.

Ověřovací funkce zkontroluje zda $Z \neq 0 \pmod N$ a vypočítá

$Y' = F_\sigma(Z) = Z^{2^l} U^\sigma \pmod N$. Potom ověří, zda $\sigma = H(Y',M)$.

Ověřovatel nyní může důvěřovat podpisu, neboť podpisující byl schopen projít náhodnými cestami (dány hashovací funkcí H) stromu s kořenem Y. Protože schopnost projít dolů dvěma odlišnými cestami zahrnuje znalost mocniny U, schopnost projít dolů náhodnou cestou z $2^l$-tého kořene také zahrnuje tuto znalost.

## 2.4 SCHÉMA S VLASTNOSTÍ DOPŘEDNÉ BEZPEČNOSTI

Schéma je tvořeno čtveřicí algoritmů pro: generování klíče, ověření zprávy, vygenerování podpisu zprávy a update soukromého klíče.

**algorithm FSIG.key(k, T)**

begin
Generuje náhodná prvočísla $p_1$, $p_2$ taková že:
$p_1 \equiv p_2 \equiv 3 \pmod 4$
$2^{k-1} \le (p_1-1)(p_2-1)$
$p_1 p_2 < 2^k$
$N \leftarrow p_1 p_2$
$S_0 \xleftarrow{R} Z_N^*$
$U \leftarrow 1/S_0^{2^{l(T+1)}} \bmod N$
$SK \leftarrow (N,T,0,S_0)$
$PK \leftarrow (N,U,T)$
return (S,U)
end

**algorithm FSIG.sign$^H$(M,SK)**

begin
rozděl SK na (N, T , j, $S_j$)
$R \leftarrow Z^*_N$
$Y \leftarrow R^{2^{l(T+1-j)}} \bmod N$
$\sigma \leftarrow H(j, Y, M)$
$Z \leftarrow RS_j^{\sigma} \bmod N$
return (j, (Z, σ))
end

**algorithm FSIG.vf$^H$(M,PK,sign)**

begin
rozděl PK na (N, U, T)
rozděl zprávu na (j, (Z, σ))
if $Z \equiv 0 \pmod N$
then return 0
else $Y' \leftarrow Z^{2^{l(T+1-j)}} U^{\sigma} \bmod N$
if $\sigma = H(j, Y', M)$
then return 1
else return 0
end

**algorithm FSIG.update(SK)**

begin
rozděl SK na (N, T, j, $S_j$)
if j = T
then SK ← ε
else $SK \leftarrow \left(N, T, j+1, S_j^{2^l} \bmod N\right)$
return SK
end

# 3 ZÁVĚR

Cílem této práce bylo poskytnou náhled do problému bezpečnosti digitálního podpisu při vyzrazení tajemství. Popsané schéma nabízí v současnosti bezpečné řešení při zachování délky klíčů v závislosti na počtu časových period bez nutnosti jejich distribuování.

V současné době implementuji více schémat s vlastností dopředné bezpečnosti a porovnávám je z hlediska velikosti klíčů, bezpečnosti a výpočetní náročnosti. Implementované schémata budou přidány ke známé a volně šiřitelné kryptografické knihovně CryptLib.

## LITERATURA


[1] Bellare, M., Miner, S.: A Forward-Secure Digital Signature Scheme, University of California http://www-cse.ucsd.edu/users/mihir

[2] Itkis, G., Reyzin, L.: Forward-Secure Signatures with Optimal Signing and Verifing, Boston, USA, http://theory.lcs.mit.edu/~reyzin

[3] Abdalla, M., Reyzin, L.: A New Forward-Secure Digital Scheme, December 1, 2000 Překlad z: Advances in Cryptology | Asiacrypt 2000, Tatsuaki Okamoto