Thales Paiva
7/11/18

WAVE

ESQUEMA DE ASSINATURA BASEADO EM CÓDIGOS

T. Debris-Alazar, N. Sendrier, e JP Tillich, 2018

(Artigo por enquanto)

1 ASSINATURAS COM CÓDIGOS

- CFS (Courtois, Finiasz, Sendrier · Asiacrypt '01)

KeyGen:

$g \leftarrow$ polinômio gerador de código de GOPPA, grau

$PK = H \leftarrow$ matriz de Paridade do código escolhido

$SK = \Psi \leftarrow$ Decodificador para o código escolhido

Sign: Seja m a mensagem

- $s = h(m)$
- Para $i = 0, 1, \ldots$
  - $s_i = h(s \mid i)$
  - Tenta obter z tal que $Hz^T = s_i$ usando Ψ. Se sucesso, Devolva (z, i)

ASSINATURA

VERIFY: Assinatura σ da mensagem m

$z, i = \sigma$

$y_1 = H z^T$

$y_2 = h(h(m) \mid i)$

Se $y_1 = y_2$: Aceita σ.

Senão rejeita σ

- Problemas:

. Chaves grandes. Para $\lambda = 128$, chave pública tem gigabytes e demora segundos para assinar (usabilidade)

. Usa códigos de Goppa de taxa alta, que não são indistinguíveis de aleatórios (segurança).

ALTERNATIVAS

- Fiat-Shamir no IDS de Stern
  → Chaves muito grandes

- Outras famílias de códigos
  → Maioria foi quebrada ou só pode ser usada para assinar uma vez (OTS)

2 WAVE

- Sumário do artigo
  1) Intro
  2) Background
  3) The Wave Signature Scheme
     3.1) Outline of the Scheme
     3.2) One-way Preimage Sampleable code-based functions (GPV08)
  4) Inverting the Syndrome function
     4.1) Generic Solutions.
     4.2) Solution with Trapdoor

5) Obtaining a Preimage Sampleable Scheme

5.1) Achieving the domain Sampling with the Generalized Admissible $(U, U+V)$ code family

5.2) Achieving a Uniformly Distributed Output

6) Security Proof

6.1) Basic Tools

6.2) Code-Based Problems

6.3) EUF-CMA Security Proof

sequence reduction

7) Hardness of Finding Errors of Large Weight with prescribed Syndrome

7.1) Solving Syndrome Decoding for high weights

7.2) Complexity Analysis

7.3) Application to the proposed signature

8) Distinguishing a Permuted Admissible Generalized $(U, U+V)$ code

8.1) Recovering the U code up to a permutation

8.2) Recovering the V code up to perm

8.3) Distinguishing a Generalized $(U, U+V)$ code

9) Parameters selection

10) Concluding Remarks and Future Work

2.1 Descrição do Esquema

- Seja $\mathcal{C}$ um código linear de dimensão K e comprimento n, i.e. $[n, K]$-linear, definido por uma matriz de paridade H $(n-K) \times n$. Considere a função

$$f_H : S_W \to \mathbb{F}_q^{n-K}, \text{ onde}$$

$$S_W = \{ e \in \mathbb{F}_q^n : \underbrace{w(e)}_{\text{peso}} = w \}.$$

Definida por $f_H(e) = eH^T$.

Então pela dificuldade do problema da decodificação (suposição), $\{f_H\}$ é uma família de funções unidirecionais.
(por síndrome)

Suponha que conhecemos $\mathcal{F} \subset \mathbb{F}_q^{(n-k)\times n}$ tal que $\forall H_{sk} \in \mathcal{F}$, existe um algoritmo $D_{H_{sk}}$ que para qualquer $s \in \mathbb{F}_q^{n-k}$, encontra um $\underline{e}$ tal que

$$f_{H_{sk}}(e) = s .$$

Então o $\mathcal{F}$-Wave é definido por

- KeyGen

$$H_{sk} \xleftarrow{\$} \mathcal{F}$$

$$S \xleftarrow{\$} \mathbb{F}_q^{(n-k)\times(n-k)}$$

$$P \xleftarrow{\$} \text{Matriz de permutação}$$

$$H_{pk} = S H_{sk} P$$

$$\begin{cases} sk = (S, H_{sk}, P) \\ pk = H_{pk} \end{cases}$$

Note que

$$\mathcal{C}_{PK} = \{ c \in \mathbb{F}_q^n : \underbrace{c H_{PK}^T = 0}, \}$$

$$\Leftrightarrow c.(S H_{SK} P)^T = 0$$

$$\Leftrightarrow c P^T H_{SK}^T S^T = 0$$

$$\Leftrightarrow c P^T H_{SK}^T = 0 \Leftrightarrow c P^T \in \mathcal{C}_{SK}$$

$$= \{ \hat{c} : \hat{c} P^T \in \mathcal{C}_{SK} \}$$

$$\hat{c} = cP$$

$$= \{ cP : c \underbrace{P P^T}_{I} \in \mathcal{C}_{SK} \}.$$

SIGN:

$$r \xleftarrow{\$} \{0,1\}^{\lambda_0}$$

$$D \leftarrow \text{Hash}(m, r), \quad \text{Hash} : \{0,1\}^* \to \mathbb{F}_q^{n-k}$$

$$e \leftarrow D_{H_{SK}}(D(S^{-1})^T)$$

$$\sigma = (eP, r)$$

→ Para evitar que atacante extraia informação

VERIFY

$\bar{e}, r = \sigma$

$s = \text{Hash}(m, r)$

Se $\bar{e} H_{pk}^T = s$ e $|\bar{e}| = w$,

aceita a assinatura

senão rejeita.

Correctude. Se $\bar{e} = eP$

$$\Rightarrow \bar{e} H_{pk}^T = eP H_{pk}^T = eP (S H_{sk} P)^T$$

$$= eP P^T H_{sk}^T S^T = e H_{sk}^T S^T = *$$

Mas como $e = D_{H_{sk}}(s (S^{-1})^T)$

$$\Rightarrow e H_{sk}^T = s (S^{-1})^T$$

$$\Rightarrow * = s (S^{-1})^T S^T = s .$$

$$\in w(\bar{e}) = w(eP) = w$$

↳ Peso de Hamming ■

2.2 PROBLEMAS

(P1) Idealmente se a mensagem a ser assinada segue distribuição uniforme, assinat. também deve ser uniforme. Compare com

RSA: $\sigma(m) = m^d \bmod N$.

Se m é unif. m^d também é pois m^d é PERMUTAÇÃO.

No caso do Wave, podem haver mais de um vetor $\underline{e}$ tal que $eH_{SK}^T = s$ para um mesmo s.

Solução: generalizar trapdoor permutations →

DEF One-way preimage sampleable code-based functions.

Par de algoritmos PPT (Trapdoor, InvertAlg) e parametros $\left.\begin{matrix} n \\ k \\ w \end{matrix}\right\}$ poly(λ) t.q.

- Trapdoor(λ) devolve (H, T), onde $H \in \mathbb{F}_q^{(n-k)\times n}$ e T o trapdoor correspondente para inverter síndromes
- InvertAlg(T, s) com $s \in \mathbb{F}_q^{n-k}$ devolve $e \in S_{w,n} = \{x \in \mathbb{F}_q^n : w(x) = w\}$ tal que $eH^T = s$.

Devem valer para (Trapdoor, InvertAlg) que, a menos de uma porção desprezível de matrizes H,:

① Amostragem do domínio tem saída uniforme.

$$\rho(eH^T, s) = negl(\lambda),$$

onde ρ é medida de diferença de distribuição

$$\rho(D_0, P_1) = \sum_{x \in \Omega} \frac{\| D_0(x) - D_1(x) \|}{2}$$

Obs: Abusamos de notação para variáveis aleatórias.

Quando $e \xleftarrow{\$} S_{w,n}$ e $s \xleftarrow{\$} \mathbb{F}_q^{n-k}$.

⇒ Vai permitir fazer redução de segurança

② Amostragem da preimagem com trapdoor é uniforme:

$$\rho(InvertAlg(s, T), e) = negl(\lambda),$$

onde $e \xleftarrow{\$} S_{w,n}$.

⇒ Assinaturas não vazam informação da chave secreta

③ Unidirecional sem trapdoor:

Para todo algoritmo PPT A que recebe $H \in \mathbb{F}_q^{(n-k)\times n}$ e $s \in \mathbb{F}_q^{n-k}$, a probabilidade de A devolver $e \in S_{w,n}$ tal que $eH^T = s$ é desprezível (i.e. $\in$ negl(

Isso nos leva ao segundo problema.

(P2) Quais famílias de códigos nos dá OWPSF's?

Resposta: Códigos $(U, U+V) \to$ Wave.

(P3) Como escolher parâmetros para que toda síndrome s seja inversível?

Resposta a seguir.

3 Invertendo a Função Síndrome

Problema (Decodificação por síndrome com peso fixo) Dada $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$ e w inteiro positivo, encontre $e \in \mathbb{F}_q^n$ tal que $eH^T = s$, com $w(e) = w$.

$$f_H(e) = s.$$

3.1 Condição **necessária** para f_H ser sobrejetora. ⇒ Podemos achar preimagem de qualquer síndrome.

$$\#\text{Domínio} \geq \#\text{Imagem}$$

$$f_H \text{ sobrejetora} \Rightarrow |S_w| \geq q^{n-k}$$

$$|S_w| = \underbrace{\binom{n}{w}}_{\text{Posições não nulas}} \underbrace{(q-1)^w}_{\mathbb{F}_q - \{0\}}$$

Então para f_H ser sobrejetora

$\Rightarrow w \in [\![w^-, w^+]\!]$, onde

$w^- = \min W$ e $w^+ = \max W$ para

$$W = \left\{ w \in [\![0, n]\!] , \binom{n}{w} (q-1)^w \geq q^{n-k} \right\}.$$

Supondo $R = \frac{k}{n}$ cte ; os limites podem ser encontrados

$\Rightarrow k = nR$

$$\binom{n}{w} (q-1)^w \geq q^{n(1-R)}$$

$$\log_q \binom{n}{w} (q-1)^w \geq n(1-R)$$

$$\log_q \binom{n}{w} + w \log_q (q-1) \geq n(1-R)$$

$$H_q\left(\frac{w}{n}\right) n \left(1 + o(1)\right) + w \log_q (q-1) \geq n(1-R)$$

$\hookrightarrow$ Entropia q-ária

$$\Rightarrow \begin{cases} \frac{w^+}{n} \cong g_q^+(1-R) + o(1) \\ \frac{w^-}{n} \cong g_q^-(1-R) + o(1) \end{cases}$$

Então podemos definir:

$$\omega^- := g_q^-(1-R)$$

$$\omega^+ = \begin{cases} g_q^+(1-R) & , \text{ se } R \leq \log_q\left(\frac{q}{q-1}\right) \\ 1 & , \text{ caso contrário} \end{cases}$$

Evita que $\frac{\omega}{n} \approx \frac{1-R}{\log(q-1)}$ fique negativo

Onde g_q^- e g_q^+ podem ser calculados usando a equação anterior.

Proposição. O número esperado de soluções de $eH^T = s$ com $w(e) = w$ quando H é escolhida aleatoriamente é

$$\frac{\binom{n}{w}(q-1)^w}{q^{n-k}} = \frac{\#e}{\#s}.$$

Mas quando $\frac{w}{n} \in (\omega^-, \omega^+)$ e para taxa fixa em $\frac{k}{n} = R$, temos que $\log_q \binom{n}{w} \leq H_q\left(\frac{w}{n}\right) n (1+o(1))$

$$\Rightarrow \binom{n}{w} \leq q^{\alpha n (1+o(1))}$$

$\Rightarrow$ Número esperado de soluções é exponencial em n.

Nota Apesar disso, não se conhece algoritmo eficiente para decodificar em todo o intervalo (ω^-, ω^+). O melhor que se pode fazer é usar o alg. de Prange que resolve num subintervalo.

3.2 Intervalo de w onde o problema da decodificação é fácil.

Proposição É fácil resolver o problema da decodificação no intervalo $\frac{w}{n} \in [w^-_{easy}, w^+_{easy}]$

onde: $w^-_{easy} = \frac{q-1}{q}(1-R)$

$$w^+_{easy} = \frac{q-1}{q}(1-R) + R$$

(Intuição)

Solução: Algoritmo de Prange.

Tome $e = [e_1 | e_2]$ e $H = [H_1 | H_2]$

$$eH^T = s \Rightarrow e_1 H_1^T + e_2 H_2^T = s$$

$$\Rightarrow e_2 H_2^T = s - e_1 H_1^T$$

e_2: determinado — e_1: livre p/ escolher

Idéia: usar e_1 de peso 0 ou 1 ou 2

Detalhe: H_2 precisa ter posto completo. Se não tiver, basta tomar outra permutação de H