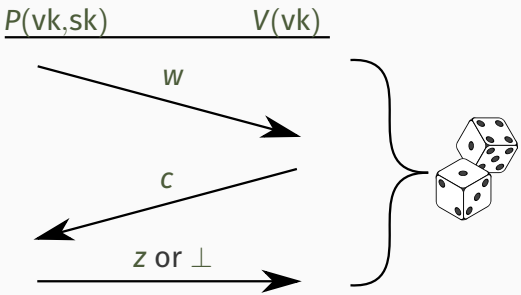
A Detailed Analysis of Fiat-Shamir with Aborts

Julien Devevey[1], Pouria Fallahpour[1], Alain Passelègue[1,2], Damien Stehlé[3]
Last minute presenter: **Thomas Espitau**

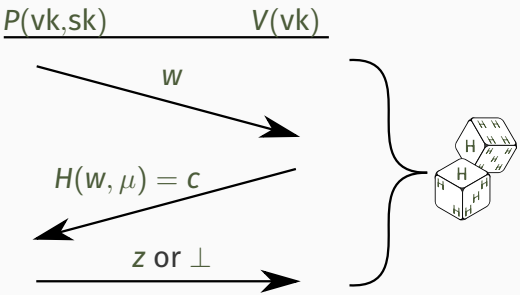
1. ENS de Lyon, France
2. INRIA, France
3. Cryptolab Inc., France

Aborting Σ-Protocol



- $\Pr\left(\text{  }\right) = \beta$
- HVZK: simulator without sk  $\approx_{\varepsilon_{zk}}$ 

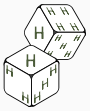
Aborting Σ-Protocol



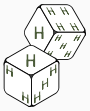
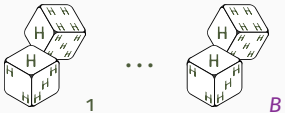
- $\Pr\left(\text{  }\right) = \beta$

- HVZK: simulator without sk  $\approx_{\varepsilon_{zk}}$ 

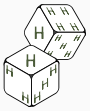
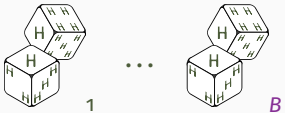
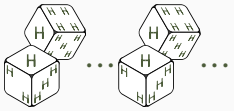
From Aborting Σ-Protocol to Signature

	Fiat-Shamir		
Sign			
Repetitions	1		
Intuition	Unif. challenge		
Drawback	Not correct		
Today			

From Aborting Σ-Protocol to Signature

	Fiat-Shamir	Bounded FS_B
Sign		
Repetitions	1	at most B
Intuition	Unif. challenge	$\Pr\left(\text{  }\right) = \beta^B$
Drawback	Not correct	Above not true
Today		Recovered analysis

From Aborting Σ-Protocol to Signature

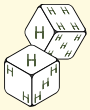
	Fiat-Shamir	Bounded FS_B	Unbounded FS_∞
Sign			
Repetitions	1	at most B	While 
Intuition	Unif. challenge	$\Pr\left(\text{  }\right) = \beta^B$	Correct
Drawback	Not correct	Above not true	No analysis
Today		Recovered analysis	Complete analysis

Security of FS_B in the QROM

Step 1: From H values to uniform challenges

$\mathsf{Sign}(\mathsf{sk}, \mu)$

For $i = 1$ to B



End for

Output the first non- 

$\mathsf{Sign}_1(\mathsf{sk}, \mu)$

For $i = 1$ to B

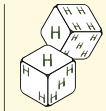
Reprogram H

End for

Output the first non- 

Security of FS_B in the QROM

Step 1: From H values to uniform challenges

$\underline{\mathsf{Sign}(\mathsf{sk}, \mu)}$
For $i = 1$ to B


End for
Output the first non-🎲

$\underline{\mathsf{Sign}_1(\mathsf{sk}, \mu)}$
For $i = 1$ to B

Reprogram H
End for
Output the first non-🎲

Adaptive Reprogramming [GHHM21] allows to reprogram even on previously reprogrammed point, even in the QROM

Security of FS_B in the QROM (2)

Step 2: Rely on simulation

$\mathsf{Sign}_1(\mathsf{sk}, \mu)$

For $i = 1$ to B

Reprogram H

End for

Output the first non- 

$\mathsf{Sign}_2(\mathsf{vk}, \mu)$

For $i = 1$ to B

Reprogram H

End for

Output the first non- 

Security of FS_B in the QROM (2)

Step 2: Rely on simulation

$\mathsf{Sign}_1(\mathsf{sk}, \mu)$

For $i = 1$ to B

Reprogram H

End for

Output the first non- 

$\mathsf{Sign}_2(\mathsf{vk}, \mu)$

For $i = 1$ to B

Reprogram H

End for

Output the first non- 

- HVZK for  to know where and when to reprogram
- Other solution: de-program (previous half-talk)

Security of FS_B in the QROM (3)

Security bound in the QROM

$$\mathsf{Adv}^{UF-CMA}(\mathcal{A}_B) \leq \mathsf{Adv}^{UF-NMA}(\mathcal{B}) + 2^{-\alpha/2}\frac{3}{2}BQ_S\sqrt{BQ_S + Q_H + 1} + \varepsilon_{\mathsf{zk}}BQ_S$$

- α: commitment min-entropy
- $\varepsilon_{\mathsf{zk}}$: SD between  and 
- Security recovered with minimal loss in both ROM and QROM

Stronger HVZK for Lyubashevsky's Scheme

Previously known:

-  for non- 
- Exact value of β

Aborting case analysis

When  , $w \approx U(\mathcal{W})$

Leveraged Simulator

Run  with proba $1 - \beta$.
Else, output uniform $(w, c, z) \in \mathcal{W} \times \mathcal{C} \times \{\perp\}$

Complete Analysis: A False Intuition

$$\Pr(\text{  }_1, \ldots, \text{  }_B) = \beta^B$$

Intuition: Correctness of FS_B

If $B = \omega(\lambda)$, $\mathbb{Z}(\mathsf{Sign}_B) = \mathsf{poly}(\lambda)$ and $\Pr(\mathsf{Sign}_B \rightarrow \perp) = \mathsf{negl}(\lambda)$

Intuition: Security of FS_∞

If $B = \omega(\lambda)$, $\mathsf{Sign}_B \approx \mathsf{Sign}_\infty$

Intuition: Runtime of FS_∞

$\mathbb{E}\left[\mathbb{Z}(\mathsf{Sign}_\infty)\right] = \mathsf{poly}(\lambda)$

Complete Analysis: A False Intuition

$$\Pr_H(\text{  }_1, \ldots, \text{  }_B) = \beta^B$$

Intuition: Correctness of FS_B

If $B = \omega(\lambda)$, $\text{⌛}(\mathsf{Sign}_B) = \mathrm{poly}(\lambda)$ and $\Pr_H(\mathsf{Sign}_B \rightarrow \perp) = \mathrm{negl}(\lambda)$ in the ROM

Intuition: Security of FS_∞

If $B = \omega(\lambda)$, $\mathsf{Sign}_B \approx \mathsf{Sign}_\infty$ in the ROM

Intuition: Runtime of FS_∞

$\mathbb{E}_H\left[\text{⌛}(\mathsf{Sign}_\infty)\right] = \mathrm{poly}(\lambda)$ in the ROM

Complete Analysis: A False Intuition

$$\Pr_H(\text{  }_1, \ldots, \text{  }_B) \neq \beta^B$$

Intuition: Correctness of FS_B

If $B = \omega(\lambda)$, $⌛(\mathsf{Sign}_B) = \mathrm{poly}(\lambda)$ and $\Pr_H(\mathsf{Sign}_B \rightarrow \perp) = \mathrm{negl}(\lambda)$ in the ROM maybe

Intuition: Security of FS_∞

If $B = \omega(\lambda)$, $\mathsf{Sign}_B \approx \mathsf{Sign}_\infty$ in the ROM maybe

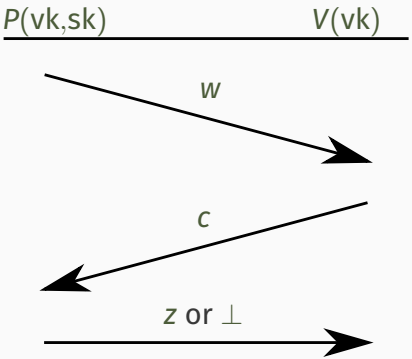
Intuition: Runtime of FS_∞

$\mathbb{E}_H\left[⌛(\mathsf{Sign}_\infty)\right] = \mathrm{poly}(\lambda)$ in the ROM maybe

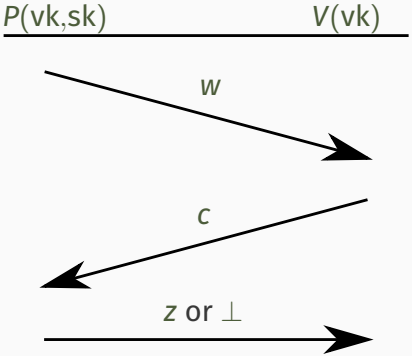
A Counter-Example: Degenerate Dilithium

- Deterministic z and rejection test $\mathsf{Rej}_{\mathsf{sk}}$

Goal: $\forall w, \exists c, \mathsf{Rej}_{\mathsf{sk}}(w, c) = 1$



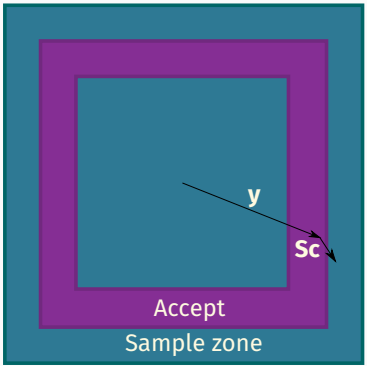
A Counter-Example: Degenerate Dilithium



- Deterministic z and rejection test $\mathsf{Rej}_{\mathsf{sk}}$

Goal: $\forall w, \exists c, \mathsf{Rej}_{\mathsf{sk}}(w, c) = 1$

For viewers familiar with Dilithium:



New Definitions

$$\Pr_H\left[\forall w, H(w,\mu) = \right] \neq 0 \implies \mathbb{E}_H\left(\text{⌛}(\mathsf{Sign}_\infty(\mathsf{sk},\mu))\right) = +\infty$$

Definitions update in the ROM

- Correctness: conditioned on termination
- Runtime: poly bound with overwhelming probability
- T'-UF-CMA: automatic win if ⌛(Sign) $> T'$

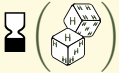
Final Bounds for FS_∞

Runtime

$$\Pr_{H,\mathsf{Sign}_\infty}\left[\#\left(\text{  }\right) > B\right] \leq \beta^B + \frac{2^{-\alpha}}{(1-\beta)^3}$$

Security

$$\left|\mathsf{Adv}^{T'}(\mathcal{A}_\infty) - \mathsf{Adv}(\mathcal{A}_B)\right| \leq Q_S\beta^B + \frac{\beta^B 2^{-\alpha}}{(1-\beta)^3} + 2^{-\alpha/2}\frac{3}{2}BQ_S\sqrt{BQ_S + Q_H + 1}$$

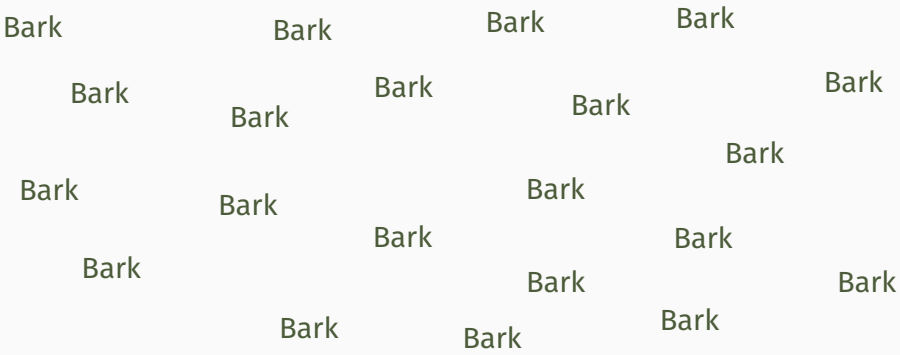
If $T' > B \cdot \max$ 

Extra Results

See ia.cr/2023/245 for:

- More identified flaws
- Fixing the history-free approach of [KLS18] with our HVZK notion
- $\{\text{sUF-CMA}, \text{UF-CMA}\} \times \{\text{QROM}, \text{ROM}\}$ bounds
- Rényi Divergence-based approach
- Computational HVZK discussion

Thank you!



Riddle 1: English saying describing the flaws