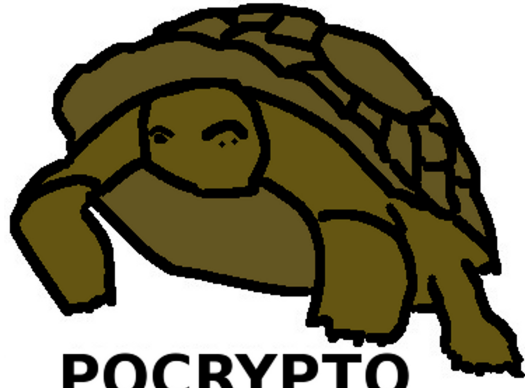
Digital Signatures From Code-Based Zero-Knowledge Protocols

Nicolas Sendrier



PQCRYPTO Miniworkshop, Utrecht, June 28 2016

Stern ZK Authentication Protocol

Parameters: $H \in \{0,1\}^{(n-k)\times n}$, weight $w > 0$, commitment scheme $h(\cdot)$
Secret: some word e of weight w ($w \approx$ Gilbert-Varshamov distance)
Public: the syndrome $s = eH^T$

	Prover		Verifier
Commitment	$\sigma \leftarrow \mathcal{S}_n$ $y \leftarrow \{0,1\}^n$	$\xrightarrow{c_0, c_1, c_2}$	
Challenge		$\xleftarrow{b}$	$b \leftarrow \{0,1,2\}$
Answer		$\xrightarrow{A(b)}$	check commitments

$$\begin{cases} c_0 = h(\sigma(y)) \\ c_1 = h(yH^T, \sigma) \\ c_2 = h(\sigma(y+e)) \end{cases} \qquad \begin{cases} A(0) = y+e, \sigma \\ A(1) = \sigma(y), \sigma(e) \\ A(2) = y, \sigma \end{cases}$$

Check: $\begin{cases} \text{if } b = 0\text{: check } c_1,\ c_2 \\ \text{if } b = 1\text{: check } c_0,\ c_2,\ \mathrm{wt}(\sigma(e)) = w \\ \text{if } b = 2\text{: check } c_0,\ c_1 \end{cases}$

Véron ZK Authentication Protocol

Parameters: $G \in \{0,1\}^{k \times n}$, weight $w > 0$, commitment scheme $h(\cdot)$
Secret: $x \in \{0,1\}^k$, $e \in \{0,1\}^n$ with $\mathrm{wt}(e) = w$
Public: noisy codeword $y = xG + e$

	Prover		Verifier
Commitment	$\sigma \leftarrow \mathcal{S}_n$ $u \leftarrow \{0,1\}^k$	$\xrightarrow{c_0, c_1, c_2}$	
Challenge		$\xleftarrow{b}$	$b \leftarrow \{0,1,2\}$
Answer		$\xrightarrow{A(b)}$	check commitments

$$\begin{cases} c_0 &= h(\sigma(uG + y)) \\ c_1 &= h(\sigma) \\ c_2 &= h(\sigma((u+x)G)) \end{cases} \qquad \begin{cases} A(0) &= u + x, \sigma \\ A(1) &= \sigma((u+x)G), \sigma(e) \\ A(2) &= u, \sigma \end{cases}$$

$$\text{Check:} \begin{cases} \text{if } b = 0\text{: check } c_1,\ c_2 \\ \text{if } b = 1\text{: check } c_0,\ c_2,\ \mathrm{wt}(\sigma(e)) = w \\ \text{if } b = 2\text{: check } c_0,\ c_1 \end{cases}$$

Stern ZK Authentication Protocol – Security

- An honest prover always succeeds (**completeness**)
- A dishonest prover succeeds for one round with probability $2/3$ at most (eventually leading to **soundness**) - next slide
- No information on the secret leaks (**zero-knowledge**)
  A simulator without knowledge of the secret may produce a valid execution of the protocol

$\rightarrow$ For a security level S, $S/\log_2(3/2) \approx 1.7S$ rounds are needed
(80 bits security $\rightarrow 137$ rounds, 128 bits security $\rightarrow 219$ rounds)

$\rightarrow$ Can be transformed into a signature (Fiat-Shamir NIZK)

$\rightarrow$ A tight security reduction to syndrome decoding

Stern ZK Authentication Protocol – Reduction

Assume an adversary has a success probability $> 2/3 + \varepsilon$ for one round

$\Rightarrow$ with probability $> \varepsilon$ this adversary could produce $c_0, c_1, c_2, A(0), A(1), A(2)$ which would all be successfully checked

$\Rightarrow$ with probability $> \varepsilon$ this adversary could produce either a collision for $h(\cdot)$ or a solution to $\mathrm{CSD}(H, s, w)$

Computational Syndrome Decoding NP-hard

Instance: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, w integer

Output: $e \in \{0,1\}^n$ such that $\mathrm{wt}(e) \leq w$ and $eH^T = s$

Signing with Stern ZK Protocol

	Prover		Verifier
Commitment	$\sigma_i \leftarrow \mathcal{S}_n$ $y_i \leftarrow \{0,1\}^n$	$\xrightarrow{c_{0,i}, c_{1,i}, c_{2,i}}$	
Challenge		$\xleftarrow{b_i}$	$b_i \leftarrow \{0,1,2\}$
Answer		$\xrightarrow{A_i(b_i)}$	check commitments

- Draw σ_i, y_i, and compute $c_{0,i}, c_{1,i}, c_{2,i}$ for all i, $1 \leq i \leq R$
- Compute $c_* = h((c_{0,i}, c_{1,i}, c_{2,i})_{1 \leq i \leq R})$
- Draw b_i, $1 \leq i \leq R$, using a PRNG with seed c_*
- The signature is $(A_i(b_i), c_{0,i}, c_{1,i}, c_{2,i})_{1 \leq i \leq R}$

(assuming $k/n = 2$, we have $w \approx S$ and $n \approx 9S$)
80 bits security $\rightarrow$ signature of 159 Kbits on average
128 bits security $\rightarrow$ signature of 406 Kbits on average

Signing with Stern ZK Protocol – Shorter

[Gaborit, Schrek, 2010(?)]

	Prover		Verifier
Commitment	$\sigma_i \leftarrow \mathcal{S}_n$ $y_i \leftarrow \{0,1\}^n$	$\xrightarrow{c_{0,i}, c_{1,i}, c_{2,i}}$	
Challenge		$\xleftarrow{b_i}$	$b_i \leftarrow \{0,1,2\}$
Answer		$\xrightarrow{A_i(b_i)}$	check commitments

- Draw σ_i, y_i, and compute $c_{0,i}, c_{1,i}, c_{2,i}$ for all i, $1 \leq i \leq R$
- Compute $c_* = h((c_{0,i}, c_{1,i}, c_{2,i})_{1 \leq i \leq R})$
- Draw b_i, $1 \leq i \leq R$, using a PRNG with seed c_*
- The signature is $c_*, (A_i(b_i), c_{b_i,i})_{1 \leq i \leq R}$

(assuming $k/n = 2$, we have $w \approx S$ and $n \approx 9S$)
80 bits security $\rightarrow$ signature of 115 Kbits on average
128 bits security $\rightarrow$ signature of 294 Kbits on average

Signing with Véron ZK Protocol – Shorter

[Gaborit, Schrek, 2010(?)]

	Prover		Verifier
Commitment	$\sigma_i \leftarrow \mathcal{S}_n$ $u_i \leftarrow \{0,1\}^k$	$\xrightarrow{c_{0,i}, c_{1,i}, c_{2,i}}$	
Challenge		$\xleftarrow{b_i}$	$b_i \leftarrow \{0,1,2\}$
Answer		$\xrightarrow{A_i(b_i)}$	check commitments

- Draw σ_i, u_i, and compute $c_{0,i}, c_{1,i}, c_{2,i}$ for all i, $1 \leq i \leq R$
- Compute $c_* = h((c_{0,i}, c_{1,i}, c_{2,i})_{1 \leq i \leq R})$
- Draw b_i, $1 \leq i \leq R$, using a PRNG with seed c_*
- The signature is $c_*, (A_i(b_i), c_{b_i,i})_{1 \leq i \leq R}$

(assuming $k/n = 2$, we have $w \approx S$ and $n \approx 9S$)
80 bits security $\rightarrow$ signature of 99 Kbits on average
128 bits security $\rightarrow$ signature of 252 Kbits on average

Variant with Cheating Probability $\to 1/2$ (Véron)

[Aguilar, Gaborit, Schrek, 2011] G block-circulant of block size p

Let ρ denote the "block-wise cyclic shift" ($\rho^p = 1$)

	Prover		Verifier
Commitment	$\sigma \leftarrow \mathcal{S}_n$ $u \leftarrow \{0,1\}^k$	$\xrightarrow{c_0, c_1}$	
Challenge		$\xleftarrow{r}$	$0 \leq r < p$
Commitment		$\xrightarrow{c_2(r)}$	
Challenge		$\xleftarrow{b}$	$b \leftarrow \{0,1\}$
Answer		$\xrightarrow{A(b,r)}$	check commitments

$$\begin{cases} c_0 &= h(\sigma(uG)) \\ c_1 &= h(\sigma) \\ c_2(r) &= h(\sigma(uG + \rho^r(e))) \end{cases} \qquad \begin{cases} A(0,r) &= u + \rho^r(x), \sigma \\ A(1,r) &= \sigma(uG), \sigma(\rho^r(e)) \end{cases}$$

Check: $\begin{cases} \text{if } b = 0\text{: check } c_1,\ c_2(r) \\ \text{if } b = 1\text{: check } c_0,\ c_2(r),\ \mathrm{wt}(\sigma(\rho^r(e))) = w \end{cases}$

Variant with Cheating Probability $\to 1/2$ (Stern)

H block-circulant of block size p

	Prover		Verifier
Commitment	$\sigma \leftarrow \mathcal{S}_n$ $y \leftarrow \{0,1\}^n$	$\xrightarrow{c_0, c_1}$	
Challenge		$\xleftarrow{r}$	$0 \leq r < p$
Commitment		$\xrightarrow{c_2(r)}$	
Challenge		$\xleftarrow{b}$	$b \leftarrow \{0,1\}$
Answer		$\xrightarrow{A(b,r)}$	check commitments

$$\begin{cases} c_0 &= h(\sigma(y)) \\ c_1 &= h(yH^T, \sigma) \\ c_2 &= h(\sigma(y) + \sigma(\rho^r(e))) \end{cases} \qquad \begin{cases} A(0,r) &= y + \rho^r(e), \sigma \\ A(1,r) &= \sigma(y), \sigma(\rho^r(e)) \end{cases}$$

Check: $\begin{cases} \text{if } b = 0\text{: check } c_1,\ c_2(r) \\ \text{if } b = 1\text{: check } c_0,\ c_2(r),\ \mathrm{wt}(\sigma(\rho^r(e))) = w \end{cases}$

QC Stern/Véron ZK Protocol – Security Reduction

An adversary with success probability $> 1/2 + \ell/2p + \varepsilon$ for one round has probability $> \varepsilon$ to find a collision for $h(\cdot)$ or to solve $\mathrm{RSD}(H, s, w, \ell)$

$\mathrm{RSD}(H, s, w, \ell)$ **Related Syndromes Decoding**

Instance:
- $H \in \{0,1\}^{(n-k)\times n}$ block circulant of block size p
- $s \in \{0,1\}^{n-k}$, w and ℓ integers

Output:
- $L \subset \{0, \ldots, p-1\}$ with $|L| = \ell$ and $(e_r)_{r\in L}$ such that
- $\mathrm{wt}(e_r) \leq w$ and all $e_r H^T + \rho^r(s)$ are identical

$\mathrm{RSD}(H, s, w, 1)$ is trivial

$\mathrm{RSD}(H, s, w, p)$ is not harder than $\mathrm{CSD}(H, s, w)$ $(e_r = \rho^r(e))$

Hopefully $\mathrm{RSD}(H, s, w, \ell)$ is hard for small values of ℓ

Decoding Related Syndromes

$\boxed{\ell = 2}$ Let $E \in \{0,1\}^n$ be a set of words of weight w. Solve $\mathrm{CSD}(H, u, w)$ for some $u \in \left\{ s + \rho^r(s) + e_0 H^T \mid e_0 \in E, 0 \leq r < p \right\}$.

For $e' \in \mathrm{CSD}(H, u, w)$, we have $e' H^T + \rho^r(s) = e_0 + s$ for some r and some $e_0 \in E$ and a solution of $\mathrm{RSD}(H, s, w, 2)$.

Best known solver: DOOM (Decoding One Out of Many) [S., 2011].
Cost $K \rightarrow$ cost $K^{2/3}$

$\boxed{\ell \geq 2}$ DOOM in cascade. Cost $K \rightarrow K^a$, $a = 1 - \frac{1}{2^\ell - 1}$

- Another approach:
  [Aguilar, Gaborit, Schrek, 2011]: choose ℓ such that $(e_r = \rho^r(s))_{0 \leq r < p}$ is the only solution with overwhelming probability. *Possible only if w is slightly below the GV bound.*

Signature with "QC Véron"

	Prover		Verifier
Commitment	$\sigma_i \leftarrow \mathcal{S}_n$ $u_i \leftarrow \{0,1\}^k$	$\xrightarrow{c_{0,i}, c_{1,i}}$	
Challenge		$\xleftarrow{r_i}$	$0 \leq r_i < p$
Commitment		$\xrightarrow{c_{2,i}(r_i)}$	
Challenge		$\xleftarrow{b_i}$	$b \leftarrow \{0,1\}$
Answer		$\xrightarrow{A_i(b_i, r_i)}$	check commitments

- Draw σ_i, u_i, and compute $c_{0,i}, c_{1,i}$ for all i, $1 \leq i \leq R$
- Draw r_i, $1 \leq i \leq R$, using a PRNG with seed $c_* = h((c_{0,i}, c_{1,i})_i)$
- Draw b_i, $1 \leq i \leq R$, using a PRNG with seed $c'_* = h(c_*, (c_{2,i})_i)$
- The signature is $c_*, (A_i(b_i, r_i), c_{b_i,i})_{1 \leq i \leq R}$
  $A(0, r) \in \{0,1\}^k \times \mathcal{S}_n$ and $A(1, r) \in \{0,1\}^n \times W_{n,w}$
  (data in green can be replaced by a PRNG seed)

80 bits security $\rightarrow$ signature of 79 Kbits on average [AGS11]
($\times 2.5$ for 128 bits and $\times 10$ for 256 bits)

Signature with "QC Stern"

	Prover		Verifier
Commitment	$\sigma_i \leftarrow \mathcal{S}_n$ $y_i \leftarrow \{0,1\}^n$	$\xrightarrow{c_{0,i}, c_{1,i}}$	
Challenge		$\xleftarrow{r_i}$	$0 \leq r_i < p$
Commitment		$\xrightarrow{c_{2,i}(r_i)}$	
Challenge		$\xleftarrow{b_i}$	$b \leftarrow \{0,1\}$
Answer		$\xrightarrow{A_i(b_i, r_i)}$	check commitments

- Draw σ_i, y_i, and compute $c_{0,i}, c_{1,i}$ for all i, $1 \leq i \leq R$
- Draw r_i, $1 \leq i \leq R$, using a PRNG with seed $c_* = h((c_{0,i}, c_{1,i})_i)$
- Draw b_i, $1 \leq i \leq R$, using a PRNG with seed $c'_* = h(c_*, (c_{2,i})_i)$
- The signature is $c_*, (A_i(b_i, r_i), c_{b_i,i})_{1 \leq i \leq R}$
  $A(0, r) \in \{0,1\}^n \times \mathcal{S}_n$ and $A(1, r) \in \{0,1\}^n \times W_{n,w}$
  (data in green can be replaced by a PRNG seed)

80 bits security $\rightarrow$ signature of $\approx$ 60 Kbits on average
(weaker security reduction; $\times 2.5$ for 128 bits and $\times 10$ for 256 bits)

Classical Issues

- Related Syndromes Decoding

$\mathrm{RSD}(H, s, w, \ell)$

Instance: $H \in \{0,1\}^{(n-k)\times n}$ block circulant of block size p; $s \in \{0,1\}^{n-k}$, w and ℓ integers

Output: $L \subset \{0, \ldots, p-1\}$ with $|L| = \ell$ and $(e_r)_{r\in L}$ such that $\mathrm{wt}(e_r) \leq w$ and all $e_r H^T + \rho^r(s)$ are identical

- Variable length signature ($A(0)$ is longer than $A(1)$)
  - fix the Hamming weight of the challenges $(b_1, \ldots, b_R)$
  - choose a weight larger than half of R

but increase R to keep the same entropy.

Quantum Issues

The Fiat Shamir paradigm has some issues in a quantum setting. In fact, its proof does not hold. We need to either

- fix the proof
- modify the construction

Conclusion

A nice and efficient solution to produce code-based digital signatures (in the Random Oracle Model)

- A tight security reduction to (variants of) Syndrome Decoding
- Public keys are short, $\approx 5\,S$ bits for S bits of security
- Signature size scales as S^2, $\approx 10\,S^2$ bits for S bits of security
- Adjustments are needed to obtain a security proof against a quantum adversary