Efficient Digital Signatures From Coding Theory

A paper by: Edoardo Persichetti
A talk by: Scott Simon

NIST

June 22, 2017

SDP-based Identification Scheme

- Public: Positive integers q, n, k, w, and an $(n-k) \times n$ matrix H over $\mathbb{F}_q$.
- Private Key: $s \in \mathbb{F}_q^n$, $\mathrm{wt}(s) \le w/2$.
- Publkic Key: $S = Hs$.

Prover		Verifier
Choose $y \in \mathbb{F}_q^n$, $\mathrm{wt}(y) \le w/2$.		
Set $Y := Hy$.	$\xrightarrow{Y}$	
	$\xleftarrow{c}$	Choose $c \in \mathbb{F}_q \setminus \{0\}$
$z := y + cs$	$\xrightarrow{z}$	Accept if $Hz = Y + cS$ and $\mathrm{wt}(z) \le w$.

Fiat-Shamir transform

- Eliminate extra pass: challenge from Verifier.
- Commitment: $Y = Hy$
- Challenge $c = \mathcal{H}(M||Y)$ for message M and some hash function $\mathcal{H}$.
- Proceed as in Identification Scheme.
- Signature $= (Y, z)$, or $(\mathcal{H}(Y), z)$.

Vulnerability

- For reasons to be discussed later, w should be chosen small.
- This means that y is biased towards 0, and therefore so is $c^{-1}y$.
- Attack: Generate lots of signatures, and use statistical analysis on $c_i^{-1}z_i = c_i^{-1}y_i + s$ to determine s.

Solution: Ring

- Use lattice-based cryptography.
- Let $\mathcal{R} := \mathbb{F}_2[x]/(x^p + 1)$.
- Use multiplication in $\mathcal{R}$ rather than by a scalar, because this will change the weight of (and generally scramble) $c^{-1}y$.

Cyclic Identification Scheme

- Public: Positive integers p, w, w_1, w_2, δ, and $h \in \mathcal{R}$ and hash function $\mathcal{H}$.
- Private Key: $s = (s_0, s_1) \in \mathcal{R} \times \mathcal{R}$ of weight w_1.
- Publkic Key: $S = s_0 + s_1 h$.

Prover		Verifier
Choose $y = (y_0, y_1) \in \mathcal{R} \times \mathcal{R}$ of weight w_2.		
Set $Y := y_0 + y_1 h$.		
Set $K := \mathcal{H}(Y)$.	$\xrightarrow{K}$	
	$\xleftarrow{c}$	Choose $c \in \mathcal{R}$ invertible, $\mathrm{wt}(c) \leq \delta$.
$z := y + cs$	$\xrightarrow{z}$	Accept if $\mathcal{H}(z_0 + z_1 h + cS) = K$ and $\mathrm{wt}(z) \leq w$.

Notes on the Cyclic Identification Scheme

- Use the Fiat-Shamir Transform to make this into a signature.
- Observe that this does not need to be resistant to a malicious Verifier in the challenge phase.
- $\mathrm{wt}(z) \leq w_2 + \delta w_1 =: w$.
- If w is sufficiently small, then z is unique.
- Lyubashevsky points to collision resistance in [5], but Persichetti uses the Gilbert-Varshamov bound from coding theory.
- For base 2 and an $[n, k]$-code, this bound is the largest d such that

$$\sum_{i=0}^{d-1} \binom{n}{i} \leq 2^{n-k}.$$

Connection to Coding Theory

- A cyclic code is a linear code closed under circular shifts.
- The generator and parity-check matrices are circulant.
- This code can be identified with an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$.
- A quasi-cyclic code is a linear code closed under right circular shifts by some fixed n_0 number of places.
- An $[n, k]$ quasi-cyclic code where $n = n_0 p$ has both generator and parity check matrices in the following form: a block matrix of n_0 $p \times p$ blocks.
- This corresponds to elements of $\mathcal{R}^{n_0}$, where $\mathcal{R} = \mathbb{F}_q[x]/(x^p - 1)$.

Quasi-cyclic Syndrome Decoding Problem

- (QC-SDP) Given $h, S \in \mathcal{R}$, find $e_0, e_1 \in \mathcal{R}$ such that $e_0 + e_1 h = S$.
- This is NP complete*.
- If the Cyclic Identification Scheme is vulnerable to an active attack, then so is QC-SDP.

Proof Outline

- Let (h^*, S^*, w^*) be an instance of QC-DSP.
- Forge identity: (K', z') with public key S^*, private key of weight $w^* = w_1$, $\mathrm{wt}(z') \leq w = w_2 + \delta w_1$.
- Since this signature is correctly validated, we must have $\mathcal{H}(z'_0 + z'_1 h^* + cS^*) = K'$.
- Since K' was chosen before c, this means that we must have computed the correct preimage $y_0 + y_1 h$.
- Therefore, we have $z'_0 + z'_1 h + cs^*_0 + cs^*_1 h = y_0 + y_1 h$.
- Regrouping, $z'_0 + z'_1 h = (y_0 + cs^*_0) + (y_1 + cs^*_1)h$.
- If $\mathrm{wt}(y) \leq w_2$ and $\mathrm{wt}(c) \leq \delta$ with $w = w_2 + \delta w_1$ below the GV bound, then by uniqueness, $z' = y + cs$.
- Using the same $y_0 + y_1 h$, forge the signature for another message to produce $z'' = y + c'' s^*$.
- Repeat until $c + c''$ is invertible, and then $s^* = (c + c'')^{-1}(z' + z'')$.

Parameters

p	w_1	w_2	δ	Security (log)	Signature Size (bits)	Public Data (bits)
4801	90	100	10	80	$9602 + \ell_{\mathcal{F}}$	9602
9857	150	200	12	128	$19714 + \ell_{\mathcal{F}}$	19714
3072	85	85	7	80	$6144 + \ell_{\mathcal{F}}$	6144
6272	125	125	10	128	$12544 + \ell_{\mathcal{F}}$	12544

$\ell_{\mathcal{F}}$ = length of hash output. Table from [3]

Other zero-knowledge identification schemes

	Stern 3	Stern 5	Véron	CVE	AGS
Rounds	28	16	28	16	18
Public Data	122500	122500	122500	32768	350
Private Key	700	4900	1050	1024	700
Public Key	350	2450	700	512	700
Total Communication Cost	42019	62272	35486	31888	20080

Table from [3].

- All values in bits.
- The values above correspond to a cheating probability of 2^{-16}. Multiply values by 5 for a probability of 2^{-80}.
- For AGS, the signature size is 93 Kb, compared with 6 Kb for this proposal.

*

- Transform the $k_0p \times n_0p$ parity check matrix into a block matrix with p^2 blocks of size $k_0 \times n_0$:
$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1p} \\ \vdots & & & \vdots \\ A_{p1} & A_{p2} & \dots & A_{pp} \end{pmatrix}.$$
- In the case where $p = 2$, if $A_{11} = H$ and $A_{12} = 0$, we can use the QC-SDP to solve:
$$\begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} e \\ e \end{pmatrix} = \begin{pmatrix} z \\ z \end{pmatrix}.$$
- Therefore we can solve the general syndrome decoding problem $He = z$.
- But if n_0 and k_0 are small, then the general syndrome decoding problem is easy.

Fiat-Shamir with Aborts

- Lyubashevsky had almost the same idea for a signature in 2009, see [4].
- There, q is larger, and he starts with small vectors and aborts if z is too large (so as not to leak information about s).
- He has a security proof that this is at least as secure as SVP_γ for a cyclic lattice.

References

- T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In B. Preneel, editor, AFRICACRYPT, volume 5580 of *Lecture Notes in Computer Science*, pages 77-97. Springer, 2009.
- A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In A. M. Odlyzko, editor, CRYPTO, volume 263 of *Lecture Notes in Computer Science*, pages 186-194. Springer, 1986.
- E. Persichetti, Efficient Digital Signatures From Coding Theory. *Cryptology ePrint Archive* 2017/397.
- V. Lyubashevsky. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In M. Matsui, editor, ASIACRYPT, volume 5912 of *Lecture Notes in Computer Science*, pages 598-616. Springer, 2009.
- V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *ICALP* (2), pages 144-155, 2006.

Questions?