Homomorphic Signatures over Binary Fields: Secure Network Coding with Small Coefficients

Dan Boneh and **David Mandell Freeman**

Stanford University, USA

Crypto 2010 Rump Session
17 August 2010

Homomorphic signatures for network coding

Consider an n-dimensional subspace $V \subset \mathbb{F}_p^\ell$.
We want a signature scheme on V with the following properties:

1. **Homomorphic:** For $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\sigma_1 = \mathrm{Sign}(\mathbf{v}_1)$, $\sigma_2 = \mathrm{Sign}(\mathbf{v}_2)$, we can run a public $\mathrm{Combine}$ algorithm to obtain a valid signature τ on $\mathbf{w} = \mathbf{v}_1 + \mathbf{v}_2$.
2. **Security:** No adversary can efficiently produce a valid signature on a vector $\mathbf{y} \notin V$, even when given many signatures on vectors in V.

Motivation: authenticating data for *network coding* [ACLY00].

- Routers linearly combine data represented as vectors; want to produce a signature on output.

Signatures over binary fields

Previous solutions: vector spaces V defined over large field $\mathbb{F}_p$ [BFKW09] or over $\mathbb{Z}$ [GKKR10].

- Want to use small fields, such as $\mathbb{F}_{257}$ or $\mathbb{F}_{2^8}$.

This work: homomorphic signatures on $V \subset \mathbb{F}_2^\ell$ under **SIS assumption on random q-ary lattices**.

- SIS is reducible to worst-case lattice problems.
- System extends to binary fields such as $\mathbb{F}_{2^8}$ and other small fields such as $\mathbb{F}_{257}$.

Overview of the construction

1. Derive matrix $\mathbf{A}_V \in \mathbb{Z}_{\mathbf{2q}}^{n \times m}$ (q odd)
   + short basis $\mathbf{B}$ for $\Lambda_{\mathbf{2q}}^{\perp}(\mathbf{A}_V)$.
   - Uses trapdoor generation [AP09] + basis delegation [CHKP10].
2. To sign $\mathbf{v} \in \mathbb{F}_2^n$, compute a **short** $\vec{\sigma} \in \mathbb{Z}^m$ (using $\mathbf{B}$) such that

$$\mathbf{A}_V \cdot \vec{\sigma} = q \cdot \mathbf{v} \pmod{2q}.$$

Signature is solution to SIS mod q, authenticates message mod 2.
Security idea: mod q and mod 2 parts can't be "decoupled."

– signature is large.

\+ homomorphic signatures over $\mathbb{F}_2$ can be done via lattice assumptions, but not via discrete log or factoring.

Overview of the construction

1. Derive matrix $\mathbf{A}_V \in \mathbb{Z}_{\mathbf{2q}}^{n \times m}$ (q odd)
   + short basis $\mathbf{B}$ for $\Lambda_{\mathbf{2q}}^{\perp}(\mathbf{A}_V)$.
   - Uses trapdoor generation [AP09] + basis delegation [CHKP10].
2. To sign $\mathbf{v} \in \mathbb{F}_2^n$, compute a **short** $\vec{\sigma} \in \mathbb{Z}^m$ (using $\mathbf{B}$) such that

$$\mathbf{A}_V \cdot \vec{\sigma} = q \cdot \mathbf{v} \pmod{2q}.$$

Signature is solution to SIS mod q, authenticates message mod 2.
Security idea: mod q and mod 2 parts can't be "decoupled."

– signature is large.

+ homomorphic signatures over $\mathbb{F}_2$ can be done via lattice assumptions, but not via discrete log or factoring.