Bernstein Bound is Tight

Mridul Nandi

Indian Statistical Institute, Kolkata.

Rump Session, Eurocrypt 2018
Tel Aviv, Israel

What is Bernstein Bound?

- **Wegman-Carter (WC) Authenticator**: $\mathsf{Poly}_K(m) \oplus \pi(\mathcal{N})$ where π is n-bit random permutation.
- **Bernstein05**: The maximum forgery advantage is at most $B(n, q)$ where q is the number of authentication queries and

$$B(n, q) = \frac{\ell}{2^n} \cdot (1 - \frac{q}{2^n})^{-(q+1)/2}.$$

Interpretation of the Bound

- $B(q,n)$ can be equivalently expressed as $\frac{\ell}{2^n} \cdot \exp^{q(q+1)/2^{n+1}}$.
- Case-1: If $q = 2^{n/2}$ then $B(q,n) \approx 1.65\ell \times 2^{-n}$.
  1. random forgery advantage $\ell \times 2^{-n}$.
  2. So Bernstein bound is already known to be tight among all adversaries making $O(2^{n/2})$ queries.
- Case-2: If $q = o(\sqrt{n}2^{n/2})$ then $B(q,n) \approx 0$. In other words, Bernstein proved beyond birthday bound security for Wegman-Carter.

Luykx-Preneel "Optimality" Claim

- Luykx-Preneel (yesterday) analyzed an attack with $q \leq 2^{n/2}$ (i.e., Case-1).
- The key-recovery advantage is $\frac{1.4}{2^n}$ (worser than recovering a single key-bit, i.e. $\frac{2}{2^n}$).
- Optimality was already known.
- It does not say anything on the key recovery advantage for beyond birthday adversaries.

New Result !!

- If $q = \sqrt{n} \times 2^n$ then key-recovery advantage can be shown to be $1/2$.
- So now we can claim that Bernstein bound is tight.
- Two analysis:
  1. Message is chosen randomly - proof is simple.
  2. Message can be any fixed nonrandom - proof is complex.
- Where do you find details?

New Result !!

- If $q = \sqrt{n} \times 2^n$ then key-recovery advantage can be shown to be $1/2$.
- So now we can claim that Bernstein bound is tight.
- Two analysis:
  1. Message is chosen randomly - proof is simple.
  2. Message can be any fixed nonrandom - proof is complex.
- Where do you find details?

Come to Santa Barbara at Crypto 2018 !