Ball-collision decoding

Christiane Peters

Technische Universiteit Eindhoven

joint work with Daniel J. Bernstein and Tanja Lange

PQCrypto 2010
Recent Results Session

May 28, 2010

Problem

- Today only binary linear codes.
- Given a parity-check matrix $H \in \mathbf{F}_2^{(n-k)\times n}$, a syndrome $s \in \mathbf{F}_2^{n-k}$, and a weight $w \in \{0, 1, 2, \ldots\}$.
- Find a vector $e \in \mathbf{F}_2^n$ of weight w such that $s = He^t$.
- Assume that the attacker does not know the structure of the underlying code.

Well-known ISD algorithms

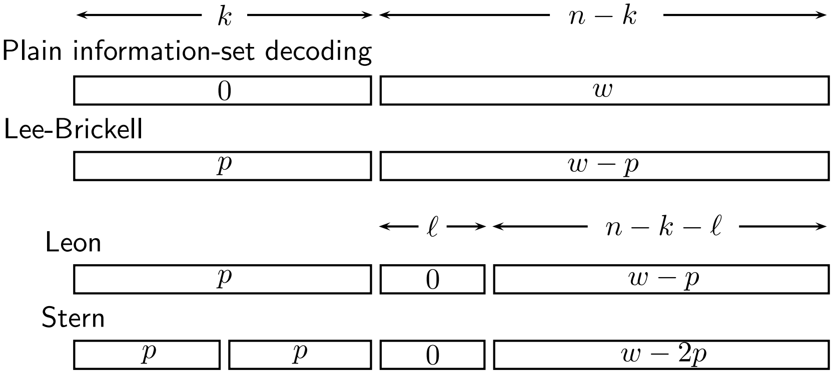


Figure from Overbeck and Sendrier: *Code-based Cryptography*, in *Post-Quantum Cryptography* (eds.: Bernstein, Buchmann, and Dahmen)

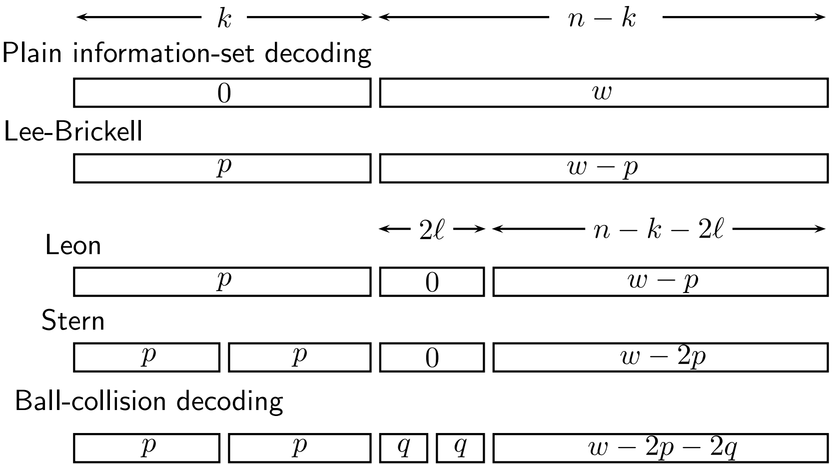
Lower bound on collision decoding

Finiasz and Sendrier. Security bounds for the design of code-based cryptosystems. Asiacrypt 2009.

- Lower bound on cost of collision decoding.
- Birthday-decoding trick increasing the probability of an iteration to succeed in Stern's algorithm.

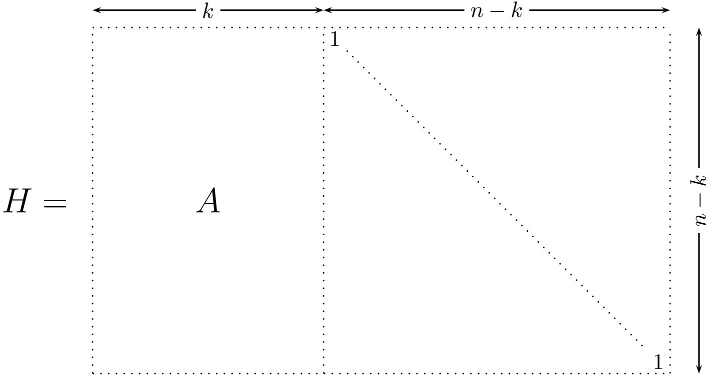
Bound is tight for original McEliece parameters $(1024, 524, 50)$.

News


k
n − k
Plain information-set decoding
0
w
Lee-Brickell
p
w − p
2ℓ
n − k − 2ℓ
Leon
p
0
w − p
Stern
p
p
0
w − 2p
Ball-collision decoding
p
p
q
q
w − 2p − 2q

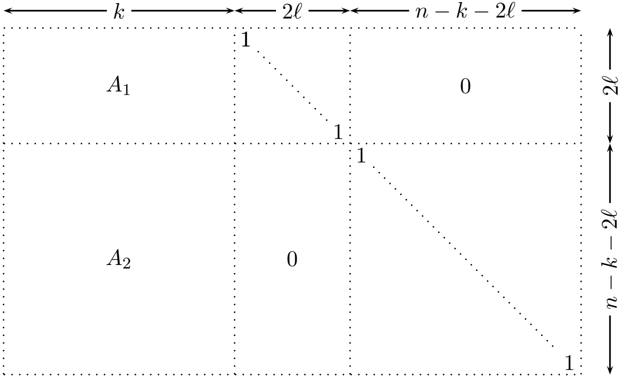
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



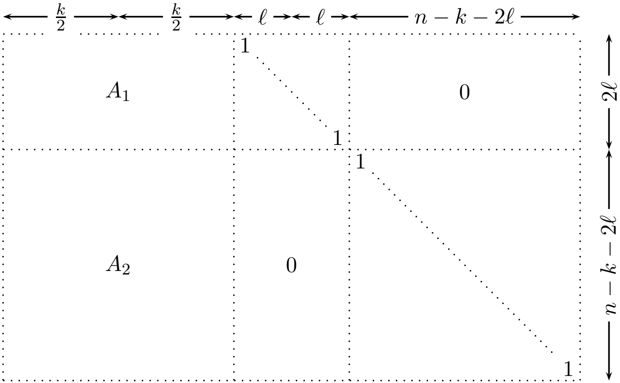
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



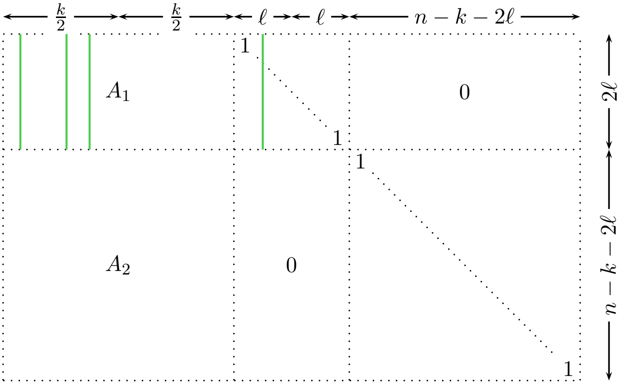
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



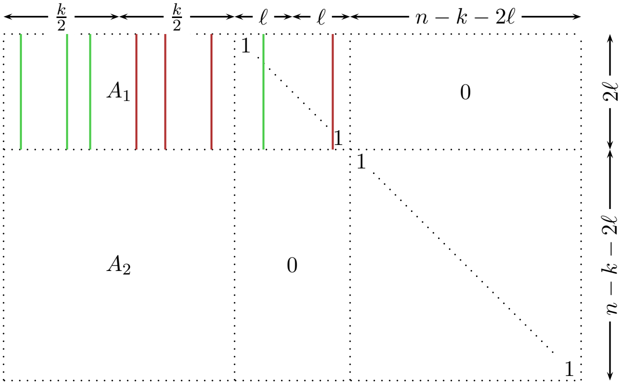
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



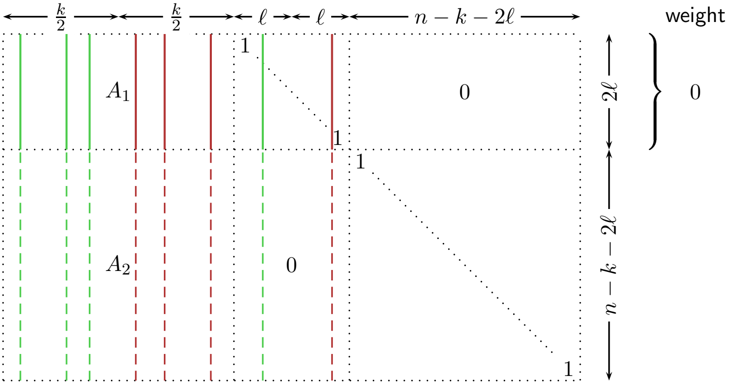
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



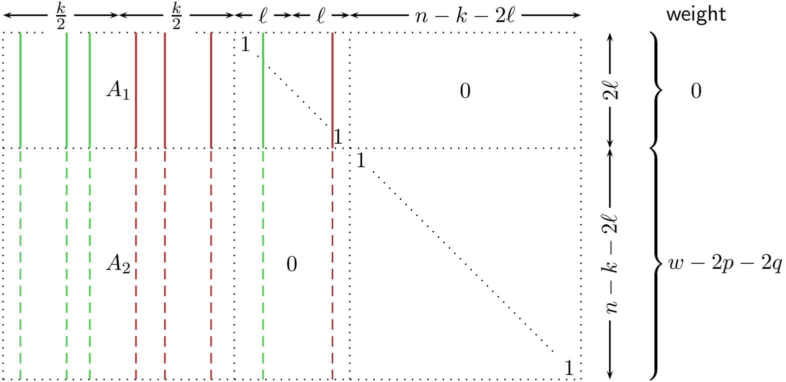
Ball-collision decoding

For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



Ball-collision decoding

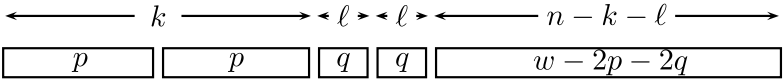
For simplicity assume $s = 0$. Goal: find w columns of the parity check matrix H adding up to zero.



If the sum has weight $w - 2p - 2q$ add the corresponding $w - 2p - 2q$ columns in the $(n-k-2\ell) \times (n-k-2\ell)$ submatrix.

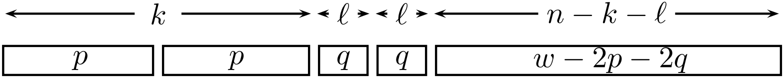
Else make a new column selection.

Ball-collision decoding



- Collision decoding is the special case $q = 0$ of ball-collision decoding.
- Disadvantage of collision decoding is that errors are required to avoid an asymptotically quite large stretch of ℓ positions.

Ball-collision decoding



- Ball-collision assumes that there are asymptotically increasingly many errors in those ℓ positions.
- Expand each p-sum A_1x_0 into a small ball namely $\{A_1x_0 + x_1 : x_1 \in \mathbf{F}_2^\ell \times \{0\}^\ell, \mathrm{wt}(x_1) = q\}$.
- Expand each p-sum A_1y_0 into a small ball.
- Search for collisions between these balls.

Ball-collision decoding

- Some extra work is required to enumerate the points in each ball.
- But it is only about the square root of the improvement in success probability.
- The cost ratio is asymptotically superpolynomial as shown in our analysis.

Success probability

- The chance that the algorithm succeeds after the first round is

$$\frac{\binom{k/2}{p}^2 \binom{\ell}{q}^2 \binom{n-k-2\ell}{w-2p-2q}}{\binom{n}{w}}.$$

- The expected number of iterations is very close to the reciprocal of the success probability of a single iteration.
- Ignore extremely unusual codes for which the average number of iterations is significantly different from the reciprocal of the success probability of a single iteration.

Cost of one iteration

- (Updating the matrix: row-reduction)

$$\frac{1}{2}(n-k)^2(n+k)$$

- $+$ (Hashing step: building sums corresponding to the balls)

$$2\ell\Big(2L(k/2,p)-k/2\Big)+2\min\{1,q\}\binom{k/2}{p}L(\ell,q)$$

- $+$ (Collision step: compute the whole vector and check its weight)

$$2(w-2p-2q+1)(2p)\binom{k/2}{p}^2\binom{\ell}{q}^2 2^{-2\ell}$$

where $L(k,p)=\sum_{i=1}^{p}\binom{k}{i}$.

Example #1

- Bernstein-Lange-P. (PQCrypto 2008): parameters $(6624, 5129, 117)$ achieve 256-bit security ($2^{255.87}$ bit ops)
- Using collision decoding with the birthday speedup takes $2^{255.54880}$ bit operations ($1.2467039\times$ speedup).
- A lower bound on collision decoding are $2^{255.1787}$ bit operations (Finiasz-Sendrier, Asiacrypt 2009). ($1.6112985\times$ speedup compared to collision decoding)
- Ball-collision decoding with parameters $\ell = 47$, $p = 8$, and $q = 1$ needs only $2^{254.1519}$ bit operations to attack the same system.
- Ball-collision decoding results in a $3.2830\times$ speedup compared to the upper bound given at PQCrypto 2008.

Example #2

- Attacking a system based on a code with parameters $(30332, 22968, 494)$ requires $2^{1000.9577}$ bit operations using collision decoding with the optimal parameters $\ell = 140$, $p = 27$ and $q = 0$.

- The lower bound by Finiasz and Sendrier breaks the complexity down to $2^{999.45027}$, $2.8430\times$ smaller than the cost of collision decoding.

- Ball-collision decoding takes $2^{996.21534}$ bit operations. This is $26.767\times$ smaller than the cost of collision decoding, and $9.415\times$ smaller than the Finiasz–Sendrier lower bound. (using parameters $\ell = 156$, $p = 29$ and $q = 1$).

Further results

- Our paper includes a proof that asymptotically $q = 0$ is suboptimal for any code rate.
- Our paper proposes a new lower bound

$$\min\left\{\frac{1}{2}\binom{n}{w}\binom{n-k}{w-p}^{-1}\binom{k}{p}^{-1/2} : p \geq 0\right\}$$

which gives security levels in the same ballpark of the cost of known attacks.
- Parameters protecting against this bound pay only about a 20% performance penalty at high security levels, compared to parameters that merely protect against known attacks.

Thank you for your attention!