Code Based Cryptology at TU/e

Ruud Pellikaan
g.r.pellikaan@tue.nl

University Indonesia, Depok, Nov. 2
University Padjadjaran, Bandung, Nov. 6
Institute Technology Bandung, Bandung, Nov. 6
University Gadjah Mada, Yogyakarta, Nov. 9
University Sebelas Maret, Surakarta, Nov. 11

November 2015
1. Ambassador of TU/e
2. Introduction on Coding, Crypto and Security
3. Public-key crypto systems
4. One-way functions and
5. Code based public-key crypto system
6. Error-correcting codes
7. Error-correcting pairs
Coding

- correct transmission of data
- error-correction
- no secrecy involved
- communication: internet, telephone, ...
- fault tolerant computing
- memory: computer compact disc, DVD, USB stick ...
- private transmission of data
- secrecy involved
- privacy
- eaves dropping
- insert false messages
- authentication
- electronic signature
- identity fraud
Security

- secure transmission of data
- secrecy involved
- electronic voting
- electronic commerce
- money transfer
- databases of patients
Public-key cryptography (PKC)

- Diffie and Hellman 1976 in the public domain in
- Ellis in 1970 for secret service, not made public until 1997
- advantage with respect to symmetric-key cryptography
- no exchange of secret key between sender and receiver
At the heart of any public-key cryptosystem is a one-way function—a function \( y = f(x) \) that is easy to evaluate but for which it is computationally infeasible (one hopes) to find the inverse \( x = f^{-1}(y) \).
Examples of one-way function

- Example 1
  - differentiation a function is easy
  - integrating a function is difficult

- Example 2
  - checking whether a given proof is correct is easy
  - finding the proof of a proposition is difficult
Integer factorization

- $x = (p, q)$ is a pair of distinct prime numbers
- $y = pq$ is its product
- proposed by Cocks in 1973 in secret service
- Rivest-Shamir-Adleman (RSA) in 1978 in public domain
- based on the hardness of factorizing integers
Discrete logarithm

- $G$ is a group (written multiplicatively)
- with $a \in G$ and $x$ an integer
- $y = a^x$
- Diffie-Hellman in 1974 and 1976 in public domain
- proposed by Williamson in 1974 in secret service
- based on difficulty of finding discrete logarithms in a finite field
Elliptic curve discrete logarithm

- $G$ is an elliptic curve group (written additively) over a finite field
- $P$ is a point on the curve
- $x = k$ a positive integer $k$
- $y = kP$ is another point on the curve
- obtained by the multiplication of $P$ with a positive integer $k$
- proposed by Koblitz and Miller in 1985
- based on the difficulty of inverting this function in $G$
Code based cryptography

- $H$ is a given $r \times n$ matrix with entries in $\mathbb{F}_q$
- $x$ is in $\mathbb{F}_q^n$ of weight at most $t$
- $y = xH^T$
- proposed by McEliece in 1978 and later by Niederreiter
- based on the difficulty of decoding error-correcting codes
- it is NP complete
NP complete problems

- NP = nondeterministic polynomial time
- given a problem with yes/no answer
- if answer is yes and the solution is given
- then one can check it in polynomial time

- Input: integer $n$
- Query: can one factorize $n$ in $n = pq$ with $p$ and $q > 1$?
- if answer is yes and someone gives $p$ and $q$
- then one easily checks that $n = pq$
- otherwise it is difficult to find $p$ and $q$
Abstract

- error-correcting codes
- error-correcting pairs correct errors efficiently
- applies to many known codes
- prime example Generalized Reed-Solomon codes
- can be explained in a short time
- is a distinguisher of certain classes of codes
- McEliece public-key cryptosystem
- polynomial attack if algebraic geometry codes are used
- ECP map is a one-way function
Block diagram of a communication system
**Error-correcting codes: Hamming**

*Q alphabet* of *q* elements

**Hamming distance** between 

\[ x = (x_1, \ldots, x_n) \] and 

\[ y = (y_1, \ldots, y_n) \] in \( Q^n \)

\[
d(x, y) = \min \left| \{ i : x_i \neq y_i \} \right|
\]

---

Triangle inequality
**Block codes**

A *block code* is a subset of $Q^n$

$$d(C) = \min \{|d(x, y) : x, y \in C, x \neq y\}|$$

Minimum distance of $C$

$$t(C) = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor$$

Error-correcting capacity of $C$
Venn diagram of the Hamming code
Venn diagram of a code word sent
Venn diagram of a received word
Correction of one error
$\mathbb{F}_q$ the finite field with $q$ elements, $q = p^e$ and $p$ prime

$\mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear vector space of dimension $n$

A linear code is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$

parameters $[n, k, d]_q$ or $[n, k, d]$

$q = \text{size finite field}$
$n = \text{length of } C$
$k = \text{dimension of } C$
$d = \text{minimum distance of } C$
Let $C$ a linear code in $\mathbb{F}_q^n$ of dimension $k$
It has a basis $g_1, \ldots, g_k$
Let $G$ be the $k \times n$ matrix with rows $g_1, \ldots, g_k$
Then $G$ is called a generator matrix of $C$

The encoding

$$\mathcal{E} : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

of $C$ is given by $\mathcal{E}(m) = mG$
 Singleton bound

\[ d \leq n - k + 1 \]

Maximum Distance Separable (MDS)

\[ d = n - k + 1 \]
Inner product

The **standard inner product** is defined by

\[ \mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n \]

Is bilinear and non-degenerate
but "positive definite" makes no sense

Two subsets \( A \) and \( B \) of \( \mathbb{F}_q^n \) are **perpendicular**: \( A \perp B \) if and only if \( \mathbf{a} \cdot \mathbf{b} = 0 \) for all \( \mathbf{a} \in A \) and \( \mathbf{b} \in B \)
Let $C$ be a linear code in $\mathbb{F}_q^n$. The dual code is defined by

$$C^\perp = \{ x : x \cdot c = 0 \text{ for all } c \in C \}$$

If $C$ has dimension $k$, then $C^\perp$ has dimension $n - k$. 
The **star product** is defined by coordinatewise multiplication

\[ a \ast b = (a_1 b_1, \ldots, a_n b_n) \]

For two subsets \( A \) and \( B \) of \( \mathbb{F}^n_q \)

\[ A \ast B = \langle a \ast b \mid a \in A \text{ and } b \in B \rangle \]
Efficient decoding algorithms

The following classes of codes:

▶ Generalized Reed-Solomon codes
▶ Cyclic codes
▶ Alternant codes
▶ Goppa codes
▶ Algebraic geometry codes

have efficient decoding algorithms:

▶ Arimoto, Peterson, Gorenstein, Zierler
▶ Berlekamp, Massey, Sakata
▶ Justesen et al., Vladut-Skrobogatov, ...........
▶ Error-correcting pairs
Let $C$ be a linear code in $\mathbb{F}_q^n$

The pair $(A, B)$ of linear subcodes of $\mathbb{F}_q^m$ is called a t-error correcting pair (ECP) over $\mathbb{F}_q^m$ for $C$ if

E.1 $ (A \ast B) \perp C$
E.2 $k(A) > t$
E.3 $d(B^\perp) > t$
E.4 $d(A) + d(C) > n$
Let $a = (a_1, \ldots, a_n)$ be an $n$-tuple of mutually distinct elements of $\mathbb{F}_q$.

Let $b = (b_1, \ldots, b_n)$ be an $n$-tuple of nonzero elements of $\mathbb{F}_q$.

**Evaluation map:**

$$\text{ev}_{a,b}(f(X)) = (f(a_1)b_1, \ldots, f(a_n)b_n)$$

$$\text{GRS}_k(a, b) = \{ \text{ev}_{a,b}(f(X)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X) < k) \}$$

**Parameters:** $[n, k, n - k + 1]$ if $k \leq n$

Since a polynomial of degree $k - 1$ has at most $k - 1$ zeros.
Furthermore

$$\text{ev}_{a,b}(f(X)) \ast \text{ev}_{a,c}(g(X)) = \text{ev}_{a,b \ast c}(f(X)g(X))$$

$$\text{GRS}_k(a, b) \ast \text{GRS}_l(a, c) = \text{GRS}_{k+l-1}(a, b \ast c)$$
$t$-ECP for $GRS_{n-2t}(a, b)$

Let $C^\perp = GRS_{2t}(a, 1)$
Then $C = GRS_{n-2t}(a, b)$ for some $b$
has parameters: $[n, n - 2t, 2t + 1]$

Let $A = GRS_{t+1}(a, 1)$ and $B = GRS_t(a, 1)$
Then $(A \ast B) \subseteq C^\perp$

$A$ has parameters $[n, t + 1, n - t]$
$B$ has parameters $[n, t, n - t + 1]$
So $B^\perp$ has parameters $[n, n - t, t + 1]$

Hence $(A, B)$ is a $t$-error-correcting pair for $C$
Kernel of a received word

Let $A$ and $B$ be linear subspaces of $\mathbb{F}_{q}^{m}$ and $r \in \mathbb{F}_{q}^{n}$ a received word. Define the kernel

\[ K(r) = \{ a \in A \mid (a \ast b) \cdot r = 0 \text{ for all } b \in B \} \]

Lemma

Let $C$ be an $\mathbb{F}_{q}$-linear code of length $n$. Let $r$ be a received word with error vector $e$. So $r = c + e$ for some $c \in C$. If $(A \ast B) \subseteq C^\perp$, then

\[ K(r) = K(e) \]
Kernel for a GRS code

Let $A = \text{GRS}_{t+1}(a, 1)$ and $B = \text{GRS}_t(a, 1)$ and $C = \langle A \ast B \rangle ^\perp$

Let
\begin{align*}
a_i &= \text{ev}_{a,1}(X^{i-1}) \text{ for } i = 1, \ldots, t + 1 \\
b_j &= \text{ev}_{a,1}(X^j) \text{ for } j = 1, \ldots, t \\
h_l &= \text{ev}_{a,1}(X^l) \text{ for } l = 1, \ldots, 2t
\end{align*}

Then
\begin{align*}
a_1, \ldots, a_{t+1} \text{ is a basis of } A \\
b_1, \ldots, b_t \text{ is a basis of } B \\
h_1, \ldots, h_{2t} \text{ is a basis of } C ^\perp
\end{align*}

Furthermore
\begin{align*}
a_i \ast b_j &= \text{ev}_{a,1}(X^{i+j-1}) = h_{i+j-1}
\end{align*}
Matrix of syndromes for a GRS code

Let \( r \) be a received word and 
\((s_1, \ldots, s_{2t}) = rH^T\) its syndrome
Then 
\[(b_j \ast a_i) \cdot r = s_{i+j-1}.\]

To compute the kernel \( K(r) \) we have to compute the null space of the matrix of syndromes

\[
\begin{pmatrix}
  s_1 & s_2 & \cdots & s_t & s_{t+1} \\
  s_2 & s_3 & \cdots & s_{t+1} & s_{t+2} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  s_t & s_{t+1} & \cdots & s_{2t-1} & s_{2t}
\end{pmatrix}
\]
Let \((A, B)\) be a \(t\)-ECP for \(C\)

Let \(J\) be a subset of \(\{1, \ldots, n\}\)

Define the subspace of \(A\) of \text{error-locating} vectors:

\[
A(J) = \{ a \in A \mid a_j = 0 \text{ for all } j \in J \}
\]

Lemma

Let \((A \ast B) \perp C\)

Let \(e\) be an error vector of the received word \(r\)

If \(I = \text{supp}(e) = \{ i \mid e_i \neq 0 \}\), then

\[
A(I) \subseteq K(r)
\]
Error positions

Lemma
Let \((A \ast B) \perp C\)
Let \(e\) be an error vector of the received word \(r\)
Assume \(d(B^) > \text{wt}(e) = t\)
If \(I = \text{supp}(e) = \{i \mid e_i \neq 0\}\), then

\[ A(I) = K(r) \]

If \(a\) is a nonzero element of \(K(r)\)
\(J\) zero positions of \(a\)
Then

\[ I \subseteq J \]
Basic algorithm

Let \((A, B)\) be a \(t\)-ECP for \(C\) with \(d(C) \geq 2t + 1\)

Suppose that \(c \in C\) is the code word sent and \(r = c + e\) is the received word for some error vector \(e\) with \(\text{wt}(e) \leq t\)

The basic algorithm for the code \(C\):
- Compute the kernel \(K(r)\)
  
  This kernel is nonzero since \(k(A) > t\)
- Take a nonzero element \(a\) of \(K(r)\)
  \(K(r) = K(e)\) since \((A \ast B) \perp C\)
- Determine the set \(J\) of zero positions of \(a\)
  \(\text{supp}(e) \subseteq J\) since \(d(B^\perp) > t\)
- Compute the error values by erasure decoding
  \(|J| < d(C)\) since \(n - d(A) < d(C)\)
Theorem

Let $C$ be an $\mathbb{F}_q$-linear code of length $n$
Let $(A, B)$ be a $t$-error-correcting pair over $\mathbb{F}_{q^m}$ for $C$

Then the basic algorithm corrects $t$ errors for the code $C$ with complexity $O((mn)^3)$
McEliece:
Let $C$ be a class of codes that have efficient decoding algorithms correcting $t$ errors with $t \leq (d - 1)/2$

**Secret key:** $(S, G, P)$

- $S$ an invertible $k \times k$ matrix
- $G$ a $k \times n$ generator matrix of a code $C$ in $C$.
- $P$ an $n \times n$ permutation matrix

**Public key:** $G' = SGP$
McEliece:

**Encryption** with public key $G' = SGP$ and message $m$ in $\mathbb{F}_q^k$:

$$y = mG' + e$$

with random chosen $e$ in $\mathbb{F}_q^n$ of weight $t$

**Decryption** with secret key $(S, G, P)$:

$$yP^{-1} = (mG' + e)P^{-1} = mSG + eP^{-1}$$

$SG$ and $G$ are generator matrices of the same code $C$
eP^{-1}$ has weight $t$

Decoder gives $c = mSG$ as closest codeword
Minimum distance decoding is NP-hard
(Berlekamp-McEliece-Van Tilborg)

It is assumed that:

1. $P \neq NP$
2. Decoding up to half the minimum distance is hard
3. One cannot distinguish nor retrieve the original code by disguising it by $S$ and $P$
Generic attack – decoding algorithms:

– McEliece 1978
– Brickell, Lee 1988
– Leon 1988
– van Tilburg 1988
– Stern 1989
– Canteaut, Chabaud, Sendrier 1998
– Finiasz-Sendrier 2009
– Bernstein-Lange-Peters 2008-2011
– Becker-Joux-May-Meurer Eurocrypt 2012
Structural attacks:

– GRS codes (Sidelnikov-Shestakov)
– subcodes of GRS codes (Wieschebrink, Márquez-Martínez-P)
– Alternant codes: open
– Goppa codes: open
– Algebraic geometry codes: (Faure-Minder, genus $g \leq 2$)
– VSAG codes: (Márquez-Martínez-P-Ruano, arbitrary $g$)
– Polynomial attack on AG codes: (Couvreur-Márquez-P, using ECP’s)
Codes with $t$-ECP

$\mathcal{P}(n, t, q)$ is the collection of pairs $(A, B)$ that satisfy

$$E.2 \quad k(A) > t$$
$$E.3 \quad d(B^\perp) > t$$
$$E.5 \quad d(A^\perp) > 1$$
$$E.6 \quad d(A) + 2t > n$$

Let

$$C = \mathbb{F}_q^n \cap (A \ast B)^\perp$$

Then $d(C)$ is at least $2t + 1$

and $(A, B)$ is a $t$-ECP for $C$
$\mathcal{F}(n, t, q)$ is the collection of $\mathbb{F}_q$-linear codes of length $n$ and minimum distance $d \geq 2t + 1$

Consider the following map

$$\varphi(n, t, q) : \mathcal{P}(n, t, q) \rightarrow \mathcal{F}(n, t, q)$$

$$(A, B) \mapsto C$$

Question:
Is this a one-way function?
Many known classes of codes that have decoding algorithm correcting $t$-errors have a $t$-ECP and are not suitable for a code based PKC.

Question for future research
Is the ECP map a one-way function?
Thank you for your attention!