Key Predistribution Schemes and One-Time Broadcast Encryption Schemes from Algebraic Geometry Codes

Hao Chen, San Ling, Carles Padró,
Huaxiong Wang, Chaoping Xing

Seminar MAS-SPMS-NTU, Singapore, January 2010

Key Predistribution Schemes (KPS)

A set of users $\mathcal{U}$ with $|\mathcal{U}| = n$

A secret key $k_P \in K$ for every privileged subset $P \in \mathcal{P} \subseteq 2^{\mathcal{U}}$

A family $\mathcal{F} \subseteq 2^{\mathcal{U}}$ of forbidden subsets

Every user $i \in \mathcal{U}$ receives a fragment $u_i \in U_i$

Every user $i \in \mathcal{U}$ is able to compute all keys k_P with $i \in P$

If $F \in \mathcal{F}$ is such that $F \cap P = \emptyset$,
the users in F have no information about k_P

We consider unconditionally secure schemes

One-Time Broadcast Encryption Schemes (OTBES)

A set of users $\mathcal{U}$ with $|\mathcal{U}| = n$

A secret key $k_P \in K$ for every privileged subset $P \in \mathcal{P} \subseteq 2^{\mathcal{U}}$

A family $\mathcal{F} \subseteq 2^{\mathcal{U}}$ of forbidden subsets

A key predistribution phase, similar to a KPS.
Every user $i \in \mathcal{U}$ receives a fragment $u_i \in U_i$

In the broadcast phase, given a privileged set P
and a secret message $m_P \in K$,
a broadcast message $b_p \in B_P$ is publicly broadcast.

Every user $i \in P$ can obtain m_P from u_i and b_P

If $F \in \mathcal{F}$ is such that $F \cap P = \emptyset$,
the users in F have no information about m_P

Trade-off between the length of the fragments
and the length of the broadcast message

We consider unconditionally secure schemes

A History of Secret Sharing

Shamir (1979)
Threshold secret sharing based on polynomial interpolation

Brickell (1989)
Generalization of Shamir's scheme based on Linear Algebra
Non-threshold access structures

Massey (1993)
Connection between secret sharing and linear error correcting codes

Chen and Cramer (2006)
Application of algebraic geometry codes to secret sharing
Linear secret sharing over constant size fields

A Similar History of KPS and OTBES

Blom 1984, Fiat & Naor 1993, BDHKVY 1992, BFS 1996
Polynomial constructions of KPS and OTBES

PGMM 2002, 2003
A more general construction based on Linear Algebra

In this work
Linear error correcting codes and,
specifically, AG codes are applied to KPS and OTBES

Applications of KPS and OTBES

The obvious application of KPS and OTBES is key distribution

Since we are requiring unconditional security, the schemes cannot be very efficient (lower bounds)

Much more efficient computationally secure solutions

Nevertheless, the schemes in Blom 1984 and BDHKVY 1992 have been proposed for key distribution in wireless sensor networks

In the previous proposals, the size of the secret keys depends on the number of users

Polynomial Constructions of KPS

The (t, w, n)-KPS proposed in BDHKVY 1992 is as follows

Privileged subsets: $P \subseteq \mathcal{U}$ with $|\mathcal{U}| = n$ and $|P| = t$

Forbidden subsets: $F \subseteq \mathcal{U}$ with $|F| \leq w$

The secret keys are taken from $K = \mathbb{F}_q$ with $q \geq n$

Public values $s_1, \ldots, s_n \in \mathbb{F}_q$

A random symmetric polynomial $f(x_1, \ldots, x_t)$ on t variables and degree at most w on each variable

The fragment of user $i \in \mathcal{U}$ is the polynomial $f(s_i, x_2, \ldots, x_t)$

The secret key for a privileged set $P \subseteq \mathcal{U}$ is $k_P = f(s_{i_1}, \ldots, s_{i_t}) \in \mathbb{F}_q$.

The length of every fragment is

$$\binom{t+w-1}{t-1} \log q \geq \binom{t+w-1}{t-1} \log n$$

Optimal information rate, but the length of the fragments grows with the number of users

Linear KPS

The previous construction is linear

A general framework for linear KPS was introduced in PGMM 2002
We need linear mappings

- $\pi_i \colon E \to E_i$ for every $i \in \mathcal{U}$
- $\pi_P \colon E \to \mathbb{F}_q$ for every privileged subset P

such that

- $\sum_{i \in P} \ker \pi_i \subseteq \ker \pi_P$ for every privileged subset P
- $\bigcap_{j \in F} \ker \pi_j \not\subseteq \ker \pi_P$ for every $F \in \mathcal{F}$ with $F \cap P = \emptyset$

That is,

$$\bigcap_{j \in F} \ker \pi_j \not\subseteq \sum_{i \in P} \ker \pi_i \text{ if } F \in \mathcal{F} \text{ and } F \cap P = \emptyset$$

Linear KPS

In particular, a proposal of (t, w, n)-KPS

Privileged subsets: $P \subseteq \mathcal{U}$ with $|\mathcal{U}| = n$ and $|P| = t$

Forbidden subsets: $F \subseteq \mathcal{U}$ with $|F| \leq w$

The secret keys are taken from $K = \mathbb{F}_q$ with $q \geq t$.

Public vectors $v_1, \dots, v_n \in V = \mathbb{F}_q^k$
Every subset of $w + 1$ vectors is linearly independent

A random symmetric t-linear map $T\colon V^t \to \mathbb{F}_q$

The fragment of user $i \in \mathcal{U}$ is the symmetric $(t-1)$-linear map $T_i = T(v_i, *, \dots, *)$

The secret key for a privileged set $P \subseteq \mathcal{U}$ is $k_P = T(v_{i_1}, \dots, v_{i_t}) \in \mathbb{F}_q$.

The length of every fragment is

$$\binom{t+k-2}{t-1} \log q$$

Linear KPS and Linear Codes

Linear (t, w, n)-KPS

The length of every fragment is

$$\binom{t+k-2}{t-1} \log q$$

It does not seem to depend on the number of users

The only restrictions are $q \geq t$
and of course, the existence of vectors $v_1, \ldots, v_n \in V = \mathbb{F}_q^k$ such that
every subset of $w+1$ vectors is linearly independent

That is, a linear (t, w, n)-KPS is obtained
from every $[n, k]$ linear code C with $d^\perp \geq w+2$

The vectors v_i are the columns of a generator matrix of C

$$\begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}$$

KPS with Constant Size Keys

By using this connection between linear KPS and linear codes, we obtain families of linear (t, w, n)-KPS with

- fixed base field $\mathbb{F}_q$
- fixed t with $2 \leq t \leq q$
- arbitrarily large n
- $w = cn$ for some constant c with $0 < c < 1$
- the length of the fragments is asymptotically better than the KPS obtained from BDHKVY 1992

KPS from Codes on the Gilbert-Varshamov Bound

By the Gilbert-Varshamov bound, there exist $[n, k_n, d_n]$ linear codes with $d_n \geq cn + 2$ and $k_n \geq (1 - \alpha)n$ for large enough n.

The KPS constructed from the dual codes have fragment length at most $\binom{t + \alpha n - 2}{t - 1} \log q$

By using BDHKVY 1992, $\binom{t + cn - 1}{t - 1} \log n$

KPS from Algebraic Geometry Codes

By using algebraic geometry codes

Theorem

X a curve over $\mathbb{F}_q$, genus g and N rational points
Positive integers t, w, n with $2 \leq t \leq q$ and $2g + w < n \leq N - 1$
Then there exists a (t, w, n)-KPS with fragment bit length

$$\binom{t + w + g - 1}{t - 1} \log q$$

Proof

In those conditions, there exists a linear code C
with dimension $k = g + w + 1$
and dual minimum distance $d^{\perp} \geq m - 2g + 2 = w + 2$.

KPS from Algebraic Geometry Codes

By taking the family of curves by Garcia and Stichtenoth 1996

For every j, t, w with $2 \leq t \leq q$ and $2q^j + w < (q-1)q^j - 1$,

(t, w, n)-KPS over $\mathbb{F}_{q^2}$ with $n = (q-1)q^j - 1$
and fragment bit-length at most

$$\binom{t + w + q^j - 1}{t - 1} 2 \log q \leq \binom{t + w + \frac{n}{q-1}}{t - 1} 2 \log q$$

Comparison with Blom's KPS

We compare the previous KPS from Algebraic Geometry codes to the ones from BDHKVY 1992 in the case $t = 2$ (Blom 1984) and $w = cn$ with $0 < c < 1 - 2/(q-1)$

Our construction

$(2, w, n)$-KPS over a fixed base field $\mathbb{F}_{q^2}$
with fragment bit-length at most

$$\left(w + \frac{n}{q-1} + 2\right) 2 \log q$$

Blom's KPS

The fragment bit-length of a $(2, w, n)$-KPS is at least

$$(w+1) \log n$$

Our KPS has smaller fragment length if

$$j \geq 2\left(1 + \frac{2}{c(q-1)}\right).$$

OTBES with Constant Size Messages

The OTBES proposed in BFS 1996 are a combination of KPS and ramp secret sharing schemes

By combining the previous construction of KPS from AG codes with the construction of OTBES in BFS 1996, we obtain OTBES in which the length of the secret message does not depend on the number of users

We could not obtain similar results from other constructions of OTBES as Stinson & Wei 1999