A new Construction of Secret Sharing Scheme using the primitive polynomial over Galois fields

Yuji Suga suga@iij.ad.jp
Internet Initiative Japan Inc.,
Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, 102-0071, Japan

***Abstract*—Fast (k, n)-threshold secret sharing schemes with XOR operations have proposed. Their methods are ideal that share size is equal to the size of the data to be distributed with the benefits that can be handled very fast for using the only XOR operations at distribution and reconstruction processes. After that, alternative methods in WAIS2013 and NBiS2013 have proposed, first method leads to general constructions of $(2, n_p+1)$-threshold secret sharing schemes where n_p is a prime. The later proposal realizes $(2, m(m+1)/2)$-threshold secret sharing schemes for small positive integer m.**

In this paper, we use m-dimensional vector spaces over $\mathbb{Z}_2$ on having bases that meet certain conditions in order to construct proposed methods proposed in NBiS2013 that has some errors of construction. So we corrects faults in NBiS2013 paper and also proposes an accurate construction by using Galois field $GF(2^m)$ that elements are represented in the ring $F_p[X]/f(X)$ where $f(X)$ is a primitive polynomial, these functionalities lead to general constructions of $(2, 2^m)$-threshold secret sharing schemes for all integers m.

I. A construction of XOR-$(2, n_p + 1)$-SSS proposed in WAIS2013

A new method have proposed in WAIS2013 [2], this leads to general constructions of $(2, n_p+1)$-threshold secret sharing schemes using only exclusive-OR operations with the same assumption of previous XOR-based (k,n)-thereshold schemes. Let $n^{'}$ be the number of pieces of blocks, previous schemes [1] have a restriction about $n^{'}$, that is $n^{'}$ must equal $n_p - 1$ for a certain prime n_p. For example, XOR-(2,4)-SSS must be used part of shares from XOR-(2,5)-SSS with $n^{'} = 4$.

For a given prime n_p, the following is a set of shares $\{W_i\}$ of XOR-(2,n)-SSS that satisfies $n^{'} = n_p - 1$ and $n = n_p + 1$. $W_i (i = 0, \ldots, n-1) := W_{i0} \mid\mid \ldots \mid\mid W_{ij} \mid\mid \ldots \mid\mid W_{in^{''}}$ $(j = 0, \ldots, n^{''} := n^{'} - 1)$. Let a secret be $M = M_1 \mid\mid \ldots \mid\mid M_{n^{'}}$ where $M_1, \ldots, M_{n^{'}} \in \{0,1\}^d$, $M_0 \in \{0\}^d$ and d-bit randomly choose binaries $R_0, \ldots, R_{n^{''}} \in \{0,1\}^d$.

- $W_{00} := R_0$, $W_{10} := M_1 \oplus R_0$
- $W_{i0} := M_1 \oplus M_{n^{'}+2-i} \oplus R_0 \quad (i = 2, \ldots, n^{'})$
- $W_{0j} := M_1 \oplus M_{j+1} \oplus R_j \quad (j = 1, \ldots, n^{'} - 1)$
- $W_{1j} := W_{0,j-1} \oplus R_{j-1} \oplus R_j \quad (j = 1, \ldots, n^{'} - 1)$
- $W_{ij} := W_{i-1,j-1} \oplus R_{j-1} \oplus R_j$
  $(i = 1, \ldots, n^{'}, j = 1, \ldots, n^{'} - 1)$
- $W_{n^{'}+1,j} := M_2 \ \oplus, \ldots, \oplus \ M_{n^{'}} \oplus R_j$
  $(j = 0, \ldots, n^{'} - 1)$

Example 1 ($n_p = 3$: XOR-$(2, 4)$-SSS in [2]):

W_0	$M_0 \oplus R_0$	$M_0 \oplus R_1$
W_1	$M_1 \oplus M_2 \oplus R_0$	$M_2 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$
W_3	$M_2 \oplus R_0$	$M_1 \oplus R_1$

II. An alternative construction of XOR-$(2, m(m+1)/2)$-SSS proposed in NBiS2013

For a set of basis over $\mathbb{Z}_2^m$, this paper defines a new concept "2-propagation bases set", and proposed new constructions of $(2, m(m+1)/2)$-threshold secret sharing schemes using exclusive-OR operations.

Definition 1 (2-propagation bases set): 2-propagation bases set $\{b_i\}(i = 1, \ldots, l)$ is a set of bases over $\mathbb{Z}_2^m$ satisfies the following properties: b_1 is a set of m zero-vectors and for all distinct two bases b_u, b_v, $\{b_u + b_v\}$ is also a basis over $\mathbb{Z}_2^m$.

Lemma 2: The order of 2-propagation bases set $\{b_i\}$ over $\mathbb{Z}_2^m$ is represented as 2^t (optimal case: 2^m). A set $\{b_i\}$ has t generator bases $\{c_i\}(i = 1, \ldots, t)$, for all b_i it satisfies that $b_i = \sum_{j=1}^{t} \lambda_j c_j$ where $\lambda_j \in \mathbb{Z}_2$.

Theorem 3: When an optimal 2-propagation bases set $\{b_i\}$ $(i = 1, \ldots, 2^m)$ over $\mathbb{Z}_2^m$, these exists an XOR-$(2, m(m+1)/2)$-SSS with vector-representation $\{w_{ij}\} = b_i^j$ $(i = 1, \ldots, 2^m, j = 1, \ldots, m)$.

Proof. From the definition of 2-propagation bases set, for 2 indices $u > v$, $b_u + b_v$ is a basis, so $w_1^* = w_{u1} + w_{v1}$ $, \ldots, w_m^* = w_{um} + w_{vm}$ are bases over $\mathbb{Z}_2^m$. The l-th element of $W_u \oplus W_v$ equals $\bigoplus_{s=1}^{m} w_l^{*(s)} M_s$. In this case, these exist m linearly independent simultaneous equations for $M_s (s = 1, \ldots, m)$, so we can reconstruct all M_s. ∎

Theorem 3 indicates the existence of 2-propagation bases sets is important. Here are some concrete examples of 2-propagation bases sets for small order. Note that W_0 corresponds to the zero vector bases and $W_1, \ldots, W_m$ are generator bases c_i related to Lemma 2. All shares are constructed by $\bigoplus_{s=1}^{m} w_l^{*(s)} M_s$ mentioned in Theorem 3.

Example 4 ($m = 3$: XOR-$(2, 3 \cdot 4/2)$-SSS in [3]):

W_0	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
W_1	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$
W_2	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$
W_3	$(1,1,0)$	$(0,1,1)$	$(1,0,0)$
$W_1 + W_2$	$(1,1,1)$	$(1,1,0)$	$(0,1,1)$
$W_1 + W_3$	$(0,1,0)$	$(0,0,1)$	$(1,1,0)$

Example 5 ($m = 4$: XOR-$(2, 4 \cdot 5/2)$-SSS in [3]):

W_0	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$
W_1	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
W_2	$(1,1,0,0)$	$(1,0,0,0)$	$(0,0,1,1)$	$(0,0,1,0)$
W_3	$(0,0,1,1)$	$(1,0,0,1)$	$(0,1,1,0)$	$(0,1,0,0)$
W_4	$(0,1,0,1)$	$(0,1,1,0)$	$(1,1,0,0)$	$(1,0,0,0)$
$W_1 + W_2$				
$W_1 + W_3$				
$W_1 + W_4$				
$W_2 + W_3$				
$W_2 + W_4$				

III. New construction of XOR-$(2, 2^m)$-SSS

The following example is a starting point of this section, this is leaded by previous work in a empirical program for parameter $m = 3$. This example is unintentionally generated because $W_2 + W_3$ is the 7-th unexpected share and also $W_1 + W_2 + W_3$ is the 8-th unexpected share. So this paper analyzes the algebraic interpretation of Example 6 and as a result we could find a brand-new elegant construction for any integers $m \geq 4$.

Example 6: [$m = 3$: XOR-$(2, 2^3)$-SSS in [3]]

W_0	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
W_1	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$
W_2	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$
W_3	$(1,1,0)$	$(0,1,1)$	$(1,0,0)$
$W_1 + W_2$			
$W_1 + W_3$			
$W_2 + W_3$			
$W_1 + W_2 + W_3$	$(0,0,1)$	$(1,0,1)$	$(1,1,1)$

Each m-dimension vectors can be expressed by a element of Galois field $GF(2^3)$, so we attempt the previous example could be rewritten:

Let a primitive polynomial $f(X)$ in $GF(2^3)$ be $X^3 + X + 1$, so we consider the field of 8 elements defined by $\mathbb{F}_{2^3} = F_2[X]/f(X)$. In this field, there are 8 elements: $0, 1, \alpha, \alpha^2, \ldots, \alpha^6$ where α is a primitive element in $\mathbb{F}_{2^3}$. All non-zero elements are follows:

$$\begin{array}{llll|l} \alpha^1 = & & +\alpha & & (0,1,0) \\ \alpha^2 = & \alpha^2 & & & (1,0,0) \\ \alpha^3 = & & +\alpha & +1 & (0,1,1) \\ \alpha^4 = & \alpha^2 & +\alpha & & (1,1,0) \\ \alpha^5 = & \alpha^2 & +\alpha & +1 & (1,1,1) \\ \alpha^6 = & \alpha^2 & & +1 & (1,0,1) \\ \alpha^7 = & & & +1 & (0,0,1) \end{array}$$

by using the equation "$\alpha^3 = \alpha + 1$". The binary vectors written in right is the vector representations that indicate the coefficients of $(\alpha^2, \alpha^1, 1)$. So we archive and rewrite the previous example as follows:

Example 7: ($m = 3$: XOR-$(2, 2^3)$-SSS with the vector representation)

W_0	$[[0]]$	$[[0]]$	$[[0]]$
W_1	$[[\alpha^2]]$	$[[\alpha^1]]$	$[[\alpha^0]]$
W_2	$[[\alpha^3]]$	$[[\alpha^2]]$	$[[\alpha^1]]$
W_3	$[[\alpha^4]]$	$[[\alpha^3]]$	$[[\alpha^2]]$
$W_1 + W_2$	$[[\alpha^5]]$	$[[\alpha^4]]$	$[[\alpha^3]]$
$W_1 + W_3$	$[[\alpha^6]]$	$[[\alpha^5]]$	$[[\alpha^4]]$
$W_2 + W_3$	$[[\alpha^0]]$	$[[\alpha^6]]$	$[[\alpha^5]]$
$W_1 + W_2 + W_3$	$[[\alpha^1]]$	$[[\alpha^0]]$	$[[\alpha^6]]$

where $[[x]]$ is the vector representation with related to $x \in GF(2^m)$ and $[[0]]$ is the zero vector.

A. Outline of proof about general construction for $m > 3$

In the general case for parameter $m > 3$, there exists a primitive polynomial (for instance: formed by $X^m + X + 1$) in $\mathbb{F}_{2^m}$. For the grantee of existence about XOR-$(2, 2^m)$-SSS, we should find the existence of the set of basis over $GF(2^m)$ with the following conditions:

- Bases $\{[[\alpha^{i+m}]], [[\alpha^{i+m-1}]], \ldots, [[\alpha^i]]\}$ are linearly independent for all $i = 0, \ldots, m-1$.
- Any additive combination of bases is also a basis (linearly independent for each other).

In the first condition, we consider the determinant of vectors, so we can apply Gaussian elimination method by using some primitive polynomial over $GF(2^m)$. The second condition needs the concept of the group action over the finite field, that is the ring algebraically closed in the ring $F_p[X]/f(X)$.

IV. Conclusions and future work

This paper corrects faults in NBiS2013 paper and also proposes an accurate construction by using Galois field $GF(2^m)$ that elements are represented in the ring $F_2[X]/f(X)$ where f(X) is a primitive polynomial, these functionalities lead to general constructions of $(2, 2^m)$-threshold secret sharing schemes for all integers m.

In the future we need estimations about computation costs by implementing our simple methods, and extend proposals to the cases with $k \geq 3$ with considering the primitive polynomials over $GF(p^m)$.

References

[1] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, On a fast (k, n)-threshold secret sharing scheme, IEICE Trans. Fundamentals, vol.91-A, no.9, Sep. 2008.

[2] Y. Suga, "New Constructions of (2,n)-Threshold Secret Sharing Schemes Using Exclusive-OR Operations", The 7th International Workshop on Advances in Information Security (WAIS2013), 2013.

[3] Y. Suga, "A Fast $(2, 2^m)$-Threshold Secret Sharing Scheme Using m Linearly Independent Binary Vectors", The 16th International Conference on Network-Based Information Systems, NBiS 2013, pp.539-544, 2013.

[4] Y. Suga, "Consideration of the XOR-operation based Secure Multiparty Computationg", The Ninth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS2015), 2015.