SOME CRYPTOGRAPHIC ASPECTS OF WOMCODES

Philippe Godlewski and Gérard D. Cohen
ENST, Département SYC, 46 rue Barrault, 75013 PARIS, France.

Abstract

We consider the following crytographic and coding questions in relation with the use of "write-once" memories (or woms)

-How to prevent anyone from reusing the wom (**immutable codes**).

-How to fix the written information in the wom after a given number of generations (**locking codes**).

-How to encode a "credit" in a way that guarantees the user t generations or "purchases" in any possible way and makes it impossible to cheat : i.e. writing on the wom necessarily increases the spent amount of money. The coding will be called "**incremental locked**".

These questions were only raised in [5], where the accent was put on the generation of womcodes possessing an "easy reading-reserved writing" property.

1. Definitions and notations

Let us suppose we have a storage medium, called **wom** ([1]), consisting of n binary positions or **wits**, initially containing a "0". At some step, a wit can be irreversibly overwritten with a "1" (e.g. by some laser beam in digital optical disks, or burning microscopic fuses in PROMS).

For two binary n-tuples x and y, we say that x covers y, and write $y<x$ if $supp(y) \subset supp(x)$, where for a binary n-tuple $z=(z_1, z_2, \dots, z_n)$, $supp(z) = \{i ; z_i = 1\}$ is the support of z. Then $|z|=|supp(z)|$ is the Hamming weight of z. The binary complement of z is denoted by $\bar{z}$.

The first problem we address is the following : how to construct codes with maximal rate (or cardinality) and forwarding impossible updating?

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 458-467, 1986.

2. Immutable codes

Let F be the binary field. A subset C of F^n is called **immutable** (see [6]) if, for any a and b in C, a<b never holds. Clearly, if such a code is used to write on a wom, no updating is possible (updating a into b would imply a<b). The characterization of maximal immutable codes is a well known combinatorial problem, solved by Sperner [2].

Proposition. The set S of all the n-tuples of weight $\lfloor n/2 \rfloor$ is a maximal immutable code (called **Sperner code**). The solution is unique for odd n. For even n, there is another solution $\bar{S}$, where $\bar{S}=\{ \bar{s} \in F_2^n \ ; s \in S\}$.

The rate of these codes, $R=(1/n).\log(|S|)$, is approximately

$R \approx 1 - (1/2n) \log(n)$.

These Sperner codes are however not very easy to encode (see e.g. [7]). One way to overcome this is to impose linearity. This will be very suboptimal, as we now show. Let us say that a linear [n,k] code C is **intersecting** if any two non-zero codewords have intersecting supports, then one has :

Proposition. A linear code C is intersecting iff C\{0} is immutable.

Proof. C\{0} is not immutable iff there exist two distinct nonzero elements in C, say a and b, with a < b. Then a + b is in C and has disjoint support with a, hence C is not intersecting. □

Intersecting codes are studied in, e.g. [3], and have low rate, namely :

Proposition. For n large enough, intersecting [n,k] codes have rate $R < 0.283\ n$.

We now propose a slightly suboptimal solution, first introduced in [7], with a very simple encoding scheme. Let us denote by 2(i) the writing of the integer i in base 2, and by |2(i)| the weight of such a writing. Define the coding of $i < 2^k$ by

$$i \longrightarrow c(i) = (\ 2(i), \ \overline{2(|2(i)|)} \ ) \qquad (1)$$

where the two parts of $c(i)$ are written using k and $\lceil \log(k) \rceil$ bits respectively. For example, if $k=7$, $i=98$, then $2(i) = 1100010$, $|2(i)|=3$, $2(|2(i)|) = 011$ and $c(98) = (1100010\ 100)$.
In fact, this encoding is **systematic**, i.e. the information written on the wom is contained in k fixed positions, say the first ones. Clearly, one has :

Proposition. The encoding scheme described in (1) gives immutable codes with rate $R \approx 1 - (1/n)\log(n)$.

Proposition. The encoding scheme of (1) is optimal, i.e. yields the largest possible rate for a systematic immutable code.

Proof. Let C be systematic with k information bits. Consider the chain (for inclusion) of k-tuples (000...0), (100...0), (110...0), ..., (111...1). For C to be immutable, these k+1 vectors must be appended different suffixes of size n−k. Hence $2^{n-k} \geq k+1$. □
We thank D. Coopersmith for suggesting this proof.

3. Locking codes

The problem of **locking**, i.e. of fixing the written information in the wom after a given number of generations, is closely related to the previous one. The only difference is that one now has the possibility of choosing when the written information should become immutable, which is a slightly stronger assumption. Among the techniques described in paragraph 2, the coding scheme (1) allows locking : to that end, take a wom of $k+\lceil \log k \rceil$ wit,
- use m wits for the updatings,
- to lock the wom when v is written, write $2(|v|)$ on the remaining wits.

4. Incremental locked codes

The following problem is introduced in [4] : write successively t messages $v_1, v_2, \ldots, v_t$ on a wom, such that

$$0 \leq v_1 \leq v_2 \leq \ldots \leq v_t \leq v-1. \qquad (2)$$

Such a code is called **incremental** (IW).

We consider the problem where any writing on the wom can only increase the value of the written message. Such a code will be called a **incremental locked womcode** (ILW) and can be used to eliminate cheating possibilities on credit cards. This assumption is stronger than the previous one : now (2) is a necessary and sufficient condition on a set of t messages for its writing to be possible, whereas it was only sufficient in the case of IW.

We shall study in the following an easy way to construct a ILW : the **knapsack (or coins) scheme**. Each wit represents a coin with value a_i. Thus the spent amount of money corresponds to the sum of "marked" coins

$$v_j = \sum_{i \in I} a_i ,$$

where I is the set of written wits. We call **incremental K womcodes** (IKW) the corresponding codes. Clearly we have

$$w^{ik} \geq w^{il} \geq w^{i}$$

where w^{ik}, w^{il}, w^{i} are the minimal lengths of a IKW, ILW, IW, respectively.

We consider the directed graph (treillis) representing all the possible transitions in the WOM. A vertex is identified with a binary n-tuple, and there is an edge from x to y iff $y > x$ and $|y-x|=1$. To every y is associated a message $\alpha(y) \in Z_v \cup \{\omega\}$ by means of the interpreting function α : $\alpha(\omega)$ means that the state y is not used (achievable as a coding state) in the coding process. The incremental code is locked iff for achievable x and y

$y > x \implies \alpha(y) \geq \alpha(x)$.

For every set

$V=(v_1, v_2, \ldots, v_t)$, with $v_1 \leq v_2 \leq \ldots \; v_t \leq v-1$

of t messages to be written, we consider the "history" of writings

$Y=(y^{(1)}, y^{(2)}, \ldots , y^{(t)})$ where $y^{(i)} \in F^n$, $y^{(1)} < y^{(2)} < \ldots < y^{(t)}$

and $\alpha(y^{(i)})=v_i$.

Let H be the set of all possible Y. The number of possible V must be less than the number of possible Y. Thus we obtain :

<u>Proposition</u>. The parameters of a $\langle v\rangle^t/n$ IW must satisfy

$$\binom{v+t}{t} \leq (t+1)^n .$$

We now define for $y \in F^n$:

$$\theta(x) = \inf(i \mid x=y^{(i)} \text{ for some } Y=(y^{(1)},\ldots,y^{(i)},\ldots),\ Y\in H).$$

<u>Proposition</u>. If y is a state in the WOM such that $\theta(y)=j$, then
$n-|y| \geq w^{\lambda}(\langle v-\alpha(y)\rangle^{t-j}) + j$,
where λ stands for i, il, ik in the case of a IW, IL, IKW respectively.

Indeed, at state j, there are at least $t-j$ generations to write on $n-|y|$ wits.
Using this Proposition we can begin to fill up a table of the w^{λ} for small v and t. We start from the first line $w(\langle v\rangle^1)=\lceil \log_2(v)\rceil$. The noticeable points are

$$w^{ik}(\langle 9\rangle^3)=6 > 5=w^{il}(\langle 9\rangle^3) \quad\text{and}\quad w^{il}(\langle 9\rangle^2)=5 > 4=w^{i}(\langle 9\rangle^2).$$

t= \ v =	1	2	3	4	5	6	7	8	9	10	11	12
1	0	1	2	2	3	3	3	3	4	4	4	4
2			2	3	3	4	4	4	4,5,5	5	5	5
3				3	4	4	5	5	5,5,6		6	6,6,7
4					4	5	5	6	6			
5						5	6	6	7			

Table : values of $w^{i}(\langle v\rangle^{t})$, $w^{il}(\langle v\rangle^{t})$, $w^{ik}(\langle v\rangle^{t})$ for small v and t.

5. Construction of incremental K womcodes (IKW)

As we said before an incremental K womcode is based on a set of coins $P=\{\ldots,\underline{i},\ldots,\underline{j},\ldots\}$, where $\underline{i}$ is a coin with value i and $|P|=n$. The set P is hereafter refered to as a **purse**. The coding algorithm obeys the following rule : "use first the heaviest remaining coin compatible with the purchase". We shall say that a $\langle(s+1)\rangle^t/n$ IKW **realizes** (s,t). Let us introduce some notations :

$n_j(P)$ is the number of coins in P with value j ;

$\Sigma_i(P) = \sum_{j=1}^{i} j\, n_j$, $\Sigma(P) = \Sigma_\infty(P)$;

P/i is the set of coins in P with value at most i ;

then $|P/i| = \sum_{j=1}^{i} n_j(P)$ and $\Sigma_i(P) = \Sigma(P/i)$;

$Q_i[k]$ or Q_i : a purse with only k coins of value i (then $k=|Q_i|=n_i(Q_i)$) ;

$D = (d_1, d_2, \ldots , d_t)$ a t-tuple of purchases ; $\Sigma(D) = \sum_j d_j$.

In the following, P denotes a purse realizing (s,t), and $m=\lfloor s/t\rfloor+1$.

<u>Proposition K1</u>. For every integers $\mu\leq m$, r,

$P^{(r)} = P \cup Q_\mu[r]$ realizes $(s+r\mu,t)$.

<u>Proof</u>. By induction on r. Suppose it is true up to k i.e. $P^{(k)}=P\cup Q_\mu[k]$ realizes $(s+k\mu,t)$. Let D be a t-tuple to be spent using $P^{(k+1)}$, let jo be the first j such that $d_j\geq\mu$ (if no such jo exists $\Sigma(D)\leq(\mu-1)t\leq s$ and we are done). Set

$D' =(d'_j) = (d_1,d_2,\ldots,d_{jo}-\mu,\ldots,d_t)$.

From our "heavy coin first" algorithm, realizing D with $P^{(k+1)}$ amounts to realizing D' with $P^{(k)}$, hence is possible since $\Sigma(D)\leq s+k\mu$. □

Proposition K2. The purse P_i defined recursively by

$P_1 = Q_1[t]$,

$P_2 = P_1 \cup Q_2[n_2]$ where n_2 is the smallest integer such that $\Sigma(P_2) \geq 2t$,

...

$P_i = P_{i-1} \cup Q_i[n_i]$ where n_i is the smallest integer s.t. $\Sigma(P_i) \geq it$,

realizes every t-tuple of purchases $D=(d_1, d_2, \ldots, d_t)$ with $\Sigma(D) \leq \Sigma(P_i)$.

Proof. By induction. For any fixed j, $0<j\leq i-1$, step $P_j \to P_{j+1}$ is achieved by applying Proposition K1 with $\mu=j+1$, $r=n_{j+1}$, $s=jt$ and therefore $m=j+1$. □

Remark. The construction in Proposition K2 also works without assuming the n_j minimal. By stopping at some level k, we obtain purses P for which the following also holds

$\Sigma(P/j) \geq jt$, $\forall$ j s.t. $1\leq j\leq k$

or equivalently

$\Sigma(P/j) \geq jt$, $\forall$ j s.t. $jt \leq \Sigma(P)$ (*)

But (*) is at the same time a necessary condition for a purse P to realize $(\Sigma_k(P),t)$ because every t-tuple D with $\Sigma(D) \leq \Sigma_k(P)$ and $\mathrm{Max}_i\, d_i \leq j$ must be realized with P/j. This shows :

Corollary. For given s and t, a necessary and sufficient condition for a purse P with $\Sigma(P/m) \geq s$, $m=\lfloor s/t \rfloor+1$, to realize (s,t) is that the m-1 following t-tuples of purchases be realizable :

$(j,j,\ldots j)$ for $1\leq j<m$.

Optimality of the proposed construction

Now we want to prove that the purse defined by Proposition K2 is optimal in the class of IKW. For fixed t, a purse P is said **saturated** if P realizes $(\Sigma(P),t)$. We first show that we can restrict ourselves to saturated purses. As before, P denotes a purse realizing (s,t), with $m=\lfloor s/t \rfloor+1$.

__Proposition__. For any P realizing (s,t), there exists a saturated P^o such that $\Sigma(P^o)=s$ and $|P^o|\leqslant|P|$.

__Proof__. We first show that P/m realizes (s,t) : Consider $D=(d_i)$, $\Sigma(D)=s$ and $d_i\in\{m-1,m\}$. Such a set of purchases uses coins with value at most m, hence $\Sigma(P/m)\geqslant s$. Then apply Corollary, which shows that P/j realizes $(\Sigma(P/j),t)$ if $1\leqslant j\leqslant m$.

Define m' by

$\Sigma(P/(m'-1)) < s \leqslant \Sigma(P/m')$.

It is clear that $m'\leqslant m$. The purse $P'=Q_{m'}[k]\cup(P/(m'-1))$ realizes $(\Sigma(P'),t)$ by proposition K1. Choose k s.t. $\Sigma(P')\leqslant s<\Sigma(P')+m'$. If the left-hand side inequality is achieved then $P^o=P'$ is a desired purse. If not, consider $P^o=P'\cup\{j\}$, $j=s-\Sigma(P')$, then P^o realizes (s,t), again by proposition K1, and $\Sigma(P^o)=s$. After straightforward counting, we get

$|P^o|=|P/m'| - \lfloor(\Sigma(P/m')-s)/m'\rfloor \leqslant |P/m'| \leqslant |P|$

We have transformed P into a saturated P^o with fewer coins. □

Let now $f(s,t)$ be the minimum number of coins for a purse realizing (s,t) : $f(s,t) = w^{ik}(\langle(s+1)\rangle^t)$. Then we have :

__Proposition__. The purse P_i defined by Proposition K2 is optimal. That is, $f(\Sigma(P_i),t)=|P_i|$.

__Proof__. By induction on i. Suppose it is true up to $i-1$. We first recall that P_i is obtained from P_{i-1} by possibly adding coins with value i. Then setting $s_j=\Sigma(P_j)$, $s=s_{i-1}$ and $s'=s_i$, we have $s'-s=ki$ for some integer k. Let P be an optimal saturated purse realizing (s',t) ; therefore $P=P/i$ (see previous proof). From P we can construct, as before, a saturated P^o realizing (s,t) by suppressing heaviest coins (with value at most i) and possibly adding a "cheapened" extra one.

$|P^o| \leqslant |P| - \lfloor(s'-s)/i\rfloor$.

Now if $|P|=f(s',t)<|P_i|$, then $f(s,t)<|P_{i-1}|$ and we get a contradiction. □

6. Asymptotical results

For womcodes, the asymptotical behavior is studied in [1]. Focusing on the case when t is fixed and v goes to infinity, one has

$w(\langle v\rangle^t) \approx f(t)\log_2(v)$,
with $f(2) \approx 1.29$ and $f(t) \approx t/\log_2(t)$ for t large.

Clearly, an incremental womcode realizing $(v+1,t)$ is also a $\langle (v+1)/t\rangle^t$ womcode. Hence, for fixed t

$$w^i(\langle v\rangle^t) \geq w(\langle (v+1)/t\rangle^t) \approx f(t)\log_2((v+1)/t) \approx w(\langle v\rangle^t).$$

That is, $w^i \approx w$ (cf. [4]).

From the previous section, we know that recursive purses yield incremental K womcodes with

$$(i+1)t > \Sigma(P_i) \geq it$$

and maximum coin of value $(i+1)$.

For fixed t and i going to infinity, the average increase of $\Sigma(P_i)$, $E(\Sigma(P_{i+1}) - \Sigma(P_i))$ is equal to t, or

$$E(|P_{i+\lfloor i/t\rfloor}| - |P_i|) = 1.$$

In others words, the purse P_i realizing $(s_i \approx it, t)$ has j coins, with

$$j \approx \sum_{k=1}^{i} t/k \approx t\ln(i) \approx t\ln(s_i/t).$$

Finally, since these codes are optimal

$$w^{ik} \approx t(\ln(v) + O(1)).$$

The asymptotical behavior of w^{il} is still unknown. It would be interesting to estimate
$R = \limsup \; w^{il} / w^{ik}$,
for fixed t and v going to infinity, and to prove that
$R < 1$.

Let us summarize what we know about w.

	t large	t=2	t=3
no coding	$w_0 = t \log_2 v$	$2 \log_2 v$	$3 \log_2 v$
incremental K womcodes	$w^{ik} \approx t \log_e v$	$1.38 \log_2 v$	$2.07 \log_2 v$
womcodes (incremental or not)	$w \approx w^{i} \approx t \log_t v$	$1.29 \log_2 v$	$1.55 \log_2 v$

We thank our graduate students Beveraggi, Assaraf and Luguern for their helpful comments.

References.

[1] R.L. Rivest and A. Shamir, "How to Reuse a "Write-Once" Memory", Inform. and Control 55, 1-19(1982).

[2] E. Sperner, "Ein Satz uber Untermengen einer endlichen Menge." (1928), Math. Z. 27. 544-548.

[3] G. D. Cohen et A. Lempel, "Linear Intersecting Codes", To appear in Discrete Mathematics (1985) vol.56(1), pp.35-43.

[4] A. Fiat et A. Shamir, "Generalized Write-Once Memories", IEEE Trans. on Inform. Theory, Vol. IT-30, No3, pp. 470-480, may 1984.

[5] G. D. Cohen et P. Godlewski, "Authorized writing for "write-once" memories", Eurocrypt'85, April 9-11, 1985. To appear in "Springer Lecture Notes in Computer Science".

[6] E.L. Leis, "Data Integrity in Digital Opical Disks", IEEE Trans. on Computers, vol.C-33, pp.818-827, September 1984.

[7] T.M. Cover, "Enumerative Source encoding", IEEE Trans. on Inform. Theory, vol. IT-19, pp.73-77, January 1973.

[8] J.M. Berger, "A note on Error Detection codes for Asymmetric Channel", Information and Control 4, pp.68-73, 1961.