RecInt Une bibliothèque pour l'arithmétique sur les entiers de taille cryptographique.

Chabot C., Dumas J.-G., Fousse L. et Giorgi P.

Ces travaux font partie du Projet SHIVA (Secured Hardware Immune Versatile Architecture) qui a pour but de fournir un module hardware programmable et reconfigurable à haut niveau de sécurité.

Nous partons du fait qu'en cryptographie asymétrique, la plupart des cryptosystèmes requièrent une arithmétique sur les entiers modulaires ou sur les courbes elliptiques. De plus, les entiers sont manipulés modulo un entier fixé de taille relativement modeste ($<$3000 bits). Nous proposons donc ici d'utiliser une structure d'entiers récursive de taille fixe :

$$\begin{cases} \texttt{RecInt<}K+1\texttt{>} = \texttt{RecInt<}K\texttt{>} * 2^{2^K} + \texttt{RecInt<}K\texttt{>} \\ \texttt{RecInt<}K_0\texttt{>} \text{ de taille } 2^{K_0} \text{ que l'on nomme } \textbf{limb} \end{cases}$$

Ainsi les entiers ayant pour taille une puissance de 2 (ce qui est souvent le cas en cryptographie, ou alors proche d'une puissance de 2) sont très facilement représentables. Par exemple, un entier de 1024 bits est représenté par un `RecInt<10>`.

Dans cet exposé, nous présentons une bibliothèque C++ s'appuyant sur les routines de GMP par souci de portabilité. Dans ce cas, le limb peut être du type `RecInt<6> = uint64` et/ou `RecInt<5> = uint32` selon l'architecture utilisée. Nous avons implémenté les opérations de base `+,-,*,/` ainsi que leurs variantes modulaires et d'autres opérations utiles en cryptographie. Les expérimentations actuelles montrent des performances équivalentes à GMP pour des tailles cryptographiques.

De plus, la simplicité de cette structure permet une implémentation sur FPGA. Nous montrerons dans cet exposé les performances obtenues durant des simulations sur des FPGA de type Virtex.

Group Signatures are Suitable for Constrained Devices

Iwen Coisel, UCL Crypto Group

In a group signature scheme, group members are able to sign messages on behalf of the group. Moreover, resulting signatures are anonymous and unlinkable for every verifier except for a given authority. In this paper, we mainly focus on one of the most secure and efficient group signature scheme, namely XSGS proposed by Delerabl´ee and Pointcheval at Vietcrypt 2006. We show that it can efficiently be implemented in a sensor node or an RFID tag, even if it requires 13 elliptic curve point multiplications, 2 modular exponentiations and one pairing evaluation to produce a group signature. This is done by securely outsourcing part of the computation to an untrusted powerful intermediary. The result is that XSGS can be executed in the MICAz (8-bit 7.37MHz ATmega128 microprocessor) and the TelosB (16-bit 4MHz MSP430 processor) sensor nodes in less than 200 ms.

Rayon de Recouvrement des LEBC

Rabiî DARITI & El Mamoun SOUIDI
Département d'informatique Faculté des Sciences - Rabat - Maroc
rabiedariti@yahoo.fr , souidi@fsr.ac.ma

Les LEBC (linear error-block codes) sont une généralisation des codes correcteurs linéaires. Ils ont été introduits en 2006 par Feng et al. [1], et étudiés dans plusieurs travaux ultérieurs et récents. Soit $\mathbb{F}_q$ le corps fini à q éléments. Ces codes se caractérisent par le "découpage" de l'espace $\mathbb{F}_q^n$ en blocs $\mathbb{F}_q^{n_i}$ où $n = \sum_{i=1}^{s} n_i$ tel que que tout vecteur $v \in \mathbb{F}_q^n$ s'écrive sous la forme unique $v = (v_1, v_2, \cdots, v_s)$ où $v_i \in \mathbb{F}_q^{n_i}$. Par conséquent, un LEBC, qui n'est autre qu'un $\mathbb{F}_q$-sous-espace vectoriel de $V := \oplus_{i=1}^{s} \mathbb{F}_q^{n_i}$, possède un nouveau paramètre qui s'ajoute à sa longueur n et sa dimension k. Il s'agit de la partition π du nombre n, nommée type du code. Cette partition définit la taille n_i de chaque bloc de V. On note $\pi = [n_1][n_2]\cdots[n_s]$, ou $\pi = [m_1]^{l_1}[m_2]^{l_2}\cdots[m_s]^{l_s}$ si $n_i = l_i m_i$. Les codes correcteurs linéaires classiques sont des LEBC de type $[1]^n$. La distance définie sur l'espace V, appelée la π-distance, est $d_\pi(u,v) = |\{i/1 \leq i \leq s, u_i \neq v_i\}|$. De même, le π-poids d'un mot est défini par $w_\pi(u) = |\{i/1 \leq i \leq s, u_i \neq 0 \in \mathbb{F}_q^{n_i}\}|$.

Lors des journées "Codage et Cryptographie" 2009 à Fréjus, les auteurs ont présenté de nouvelles familles de linear error-block codes parfaits [2].

Dans le présent travail, nous nous intéressons à étudier les propriétés de recouvrement des linear error-block codes. La définition de la π-distance induit la définition suivante du π-rayon de recouvrement $\rho = max\{d_\pi(x, \mathcal{C}), x \in V\}$ où $\mathcal{C}$ est le code considéré. D'autres définitions du rayon de recouvrement sont généralisées en passant à la π-distance. Dans le cadre de cette généralisation, nous étudions des méthodes de construction de codes à partir d'autres codes, telles que la somme directe, la concaténation, la construction $(u, u+v)$, l'extension et la poncturation. Un prochain travail serait dédié à la construction la plus générale de produit de matrice (matrix product codes). Nous donnons également des bornes inférieures et/ou supérieures sur le π-rayon de recouvrement des codes construits, ainsi que dans d'autres situations telles que les supercodes, la borne $1 + \rho$ et la borne $\rho_1 + \rho_2$.

References

[1] Linear error-block codes Keqin Feng, Lanju Xu , Fred J. Hickernell, Finite Fields and Their Applications, **12** (2006), pp 638 – 652.

[2] R. DARITI & E. M. SOUIDI, New Families of Perfect Linear Error-Block Codes, Journées "Codage et Cryptographie" du 4 au 9 Octobre 2009, Fréjus, `www-salsa.lip6.fr/~bettale/C2/pdf/01.pdf`.

Polynômes cyclotomiques, arithmétique et cryptographie à base de tores algébriques

Clément Dunand

Résumé

La cryptographie basée sur le logarithme discret a connu de nombreuses avancées dans les dix dernières années, notamment avec l'utilisation de tores algébriques introduite par Lenstra et Verheul. Visant un paramétrage efficace de ces structures, Van Dijk et Woodruff ont récemment proposé une solution pour représenter de manière compacte une famille de points d'un tore algébrique. C'est en examinant les objets manipulés que l'on voit naturellement apparaître des polynômes cyclotomiques et leurs inverses modulaires. L'amplitude de leurs coefficients intervient directement dans l'étude de complexité. Si les polynômes cyclotomiques ont fait l'objet de nombreux travaux et suscité beaucoup de fascination depuis plus d'un siècle, l'étude de leurs inverses modulaires est un sujet plus neuf.

Dans cet esposé on reviendra sur le résultat arithmétique ci-dessous et on présentera son utilité dans la cryptographie à base de tores algébriques. Dans le cas où les indices de deux polynômes cyclotomiques divisent un produit de deux nombres premiers, on trouve des bornes voire des expressions explicites pour les coefficients de leurs inverses modulaires.

Theorème.
Pour tous nombres premiers distincts p et r,

(i) $\Phi_p^{-1} \bmod \Phi_1 = 1/p$ *et* $\Phi_1^{-1} \bmod \Phi_p = (-1/p)(X^{p-2} + 2X^{p-3} + \ldots + p - 1)$.

(ii) $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$ *et* $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

(iii) $\Phi_{pr}^{-1} \bmod \Phi_p = \frac{1}{r} \sum_{i=0}^{d-1} X^i$ *avec* $d = r \bmod p$ *et*

$\Phi_p^{-1} \bmod \Phi_{pr} = \frac{1}{r} \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $|v_i| < r$.

(iv) $\Phi_p^{-1} \bmod \Phi_r = \sum_{i=0}^{\varphi(r)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

Quantum Secret Sharing

Jérôme Javelle - Université de Grenoble, LIG

The link between computer science and quantum mechanics introduced a new kind of information and a new category of algorithms. Therefore, it becomes necessary to have a theory to handle this information, and the usual questions of privacy, authentication and encoding arise the same way. This talk is focused on quantum secret sharing [Got00], that is how to share a quantum secret between several people and without leaks.

It is well known that one can share a classical bit between n players, so that any set of k players can access the secret [Sha79], and every set of less than k players can not learn any information about the secret. During this presentation, we will explain the extension of such a protocol in the quantum world (with a quantum state $|\phi\rangle$ to share).

In order to encode a quantum secret, it is possible to use graph states which are quantum entangled states with the geometry of a graph [MS08]. Thus, each player has one qubit which corresponds to one vertex of the graph. Then, we establish a characterization of accessing sets based on some specific properties of the subsets of vertices on these graphs.

Sharing a quantum secret seems to have more constraints than sharing a classical secret since the "no-cloning theorem" forbids the duplication of the secret, for example. Thus, a protocol that realizes the threshold $k = n$ has been realized [BCT08], and we can notice the existence of a C_5 graph with a threshold of $k = 3$ among $n = 5$ players. As regards actual results, a family of graphs that realize the threshold $k \geq n - n^{0.68}$ will be detailed, and we prove that no such family of protocols can be found if $k \leq \frac{n}{2} + cn$ for some constant c.

References

[BCT08] Anne Broadbent, Paul Robert Chouha, and Alain Tapp. The GHZ state in secret sharing and entanglement simulation. *http://arxiv.org/abs/0810.0259*, October 2008.

[Got00] Daniel Gottesman. On the theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, 2000.

[MS08] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78:042309, 2008.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

Une preuve de deux conjectures sur les fonctions APN

Elodie Leducq

Résumé

Soit $q = p^n$, p un nombre premier, n un entier.
Si $f : \mathbb{F}_q \to \mathbb{F}_q$, pour tout a et b dans $\mathbb{F}_q$, on note $N_f(a, b)$ le nombre de solutions dans $\mathbb{F}_q$ de l'équation $f(x+a) - f(x) = b$. On dit que f est APN si

$$\Delta_f = \max(N_f(a, b), a, b \in \mathbb{F}_q, a \neq 0) = 2.$$

Dobbertin, Mills, Müller, Pott et Willems ont fait les conjectures suivantes :

Conjecture 1 *Pour $n \geq 5$ impair, dans $\mathbb{F}_{3^n}$, la fonction $x \mapsto x^d$ est APN pour*

$$d = \begin{cases} \frac{3^m-1}{2} & \text{si } n \equiv 3 \mod 4 \\ \frac{3^m-1}{2} + \frac{3^n-1}{2} & \text{si } n \equiv 1 \mod 4 \end{cases}$$

Conjecture 2 *Si n est un entier impair, dans $\mathbb{F}_{5^n}$, la fonction $x \mapsto x^d$ est APN pour*

$$d = \frac{5^n - 1}{4} + \frac{5^m - 1}{2}.$$

Ici nous nous proposons de démontrer ces deux conjectures.

Equitable Cake Cutting without Mediator

Sophie Mawet, Olivier Pereira and Christophe Petit

Université catholique de Louvain
ICTEAM – Crypto Group
B-1348 Louvain-la-Neuve, Belgium

We consider enhancing solutions to the fair division problem of cake cutting by proposing a cryptographic protocol preserving the privacy of the players' preferences in each step. This addresses an important shortcoming of traditional division procedures, that disclose some of the players' preferences and offer other players the possibility to dynamically adjust their behaviour in order to obtain unfair advantages. By contrast, the only thing that players learn when applying our procedure is strictly minimal, that is, players only learn the cutting point that would be determined by a fair mediator.

Our approach relies on the description of the players' utility function through step functions, a choice that enables us to obtain an efficient procedure for the secure evaluation of cutting points in the two-player case. We also explore a procedure that could be applied for more players.

Keywords: Secure multiparty computation, Game theory

References

[1] J. Algesheimer, J. Camenisch and V. Shoup. Efficient computation modulo a shared secret with application to the generation of shared safe-prime products. In *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 417-432, Springer, 2002.

[2] S.J. Brams and A.D. Taylor. Fair division, from cake-cutting to dispute resolution. Cambridge University Press, 1996.

[3] R. Cramer and I. Damgård. Secure distributed linear algebra in a constant number of rounds. In *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *LNCS*, pages 119-136, Springer, 2001

[4] I. Damgård, M. Fitzi, E. Kiltz, J.B. Nielsen and T. Toft. Unconditionally secure constant round multiparty computation for equality, comparison, bits and exponentiation. In *Theory of Cryptography*, volume 3876 of *LNCS*, pages 285-304, Springer, 2006.

[5] M. Geisler. Cryptographic protocols: theory and implementation. PhD thesis, Aarhus University Denmark, Department of Computer Science, February 2010.

Quasi-dyadic CFS signatures

Paulo S. L. M. Barreto[1] and Pierre-Louis Cayrel[2] and Rafael Misoczki[1,4] and Robert Niebuhr[3]

[1] Escola Politécnica	[2] CASED	[3] Technische Universität	[4] Project SECRET
Universidade de São Paulo	Darmstadt	Darmstadt	INRIA-Rocquencourt
Brazil	Germany	Germany	France

Digital signatures are among the most useful and pervasive cryptographic primitives, either *per se* or as part of more elaborate, derived protocols. Yet the overwhelming majority of actually deployed signature schemes seem to rely on the hardness of certain computational problems that are efficiently solvable by quantum computers [6]. Should quantum computers become a technological reality, the task of ensuring that suitable quantum-resistant signatures are available for deployment becomes critical.

The signature algorithm proposed by Courtois, Finiasz and Sendrier, or CFS for short [1], is one of the few and most promising schemes known based on the difficulty of decoding linear error-correcting codes. However, it has the drawback that public keys tend to be exceedingly large [2], all the more so due to an attack due to Bleichenbacher (unpublished, but described in [2]).

Part of the difficulty resides in obtaining codes with high density of decodable syndromes, since the CFS signing mechanism involves sampling random syndromes until a decodable one is found. Essentially the only family of suitable codes for this purpose is that of binary Goppa codes, for which one can actually correct all t design errors, leading to a signing complexity of $O(t!)$. In comparison, for other classes of codes, no decoding method is known that is capable of efficiently correcting more than about half as many errors; since one has then to design the error correcting capacity twice as high, the CFS signing complexity becomes $O((2t)!) \approx O((t!)^2 \cdot 4^t/\sqrt{t})$, far too much for any secure parameter set.

Quasi-dyadic (QD) codes [4], which constitute a proper subfamily of Goppa codes, have been proposed to address the problem of key reduction in the related McEliece and Niederreiter cryptosystems [3, 5]. However, the original QD construction only yields codes with a fairly low density of decodable syndromes, comparable to generic alternant codes rather than to other Goppa codes.

In this paper we modify the construction algorithm for t-error correcting quasi-dyadic codes [4], where the density of decodable syndromes is high, while also allowing for a reduction by a factor up to t in the key size. This yields dense binary Goppa codes as needed for practical instantiation of CFS signatures.

The adoption of binary quasi-dyadic (QD) codes allows for a reduction of key sizes by a factor of 4 in practice. Although the number of signing attempts increases by a factor of 2, a proper implementation of the more efficient arithmetic enabled by QD codes is likely to make the actual signing time comparable to plain CFS, possibly faster.

References

1. N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology – Asiacrypt'2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 157–174, Gold Coast, Australia, 2001. Springer.
2. M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In *Advances in Cryptology – Asiacrypt'2009*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.
3. R. McEliece. A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42–44, 1978. `http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF`.
4. R. Misoczki and P. S. L. M. Barreto. Compact McEliece keys from goppa codes. In *Selected Areas in Cryptography – SAC'2009*, volume 5867 of *LNCS*, pages 276–392. Springer, 2009.
5. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.
6. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1995.

Construction de codes maximaux à w-témoins

Bretrand Meyer, EPFL

Étant donné un code C et un mot de code c, on dit qu'un ensemble d'indice W est un témoin de c par rapport à C si la restriction à W de c diffère de la restriction à W de tout autre mot de code de C. Quand tout mot de C possède un témoin de cardinal w, le code C est appelé code à w-témoins. Nous donnons quelques nouvelles constructions de tels codes et nous prouvons que leur cardinal est maximal par une méthode d'optimisation semidéfinie positive.

Hash functions and Cayley graphs: the end of the story?

Christophe Petit, UCL Crypto Group, Louvain-la-Neuve

Hash functions are a fundamental primitive in cryptography, practically used for digital signatures, message authentication codes and password storage.

In this talk, we review a mathematical construction of hash functions that is based on finite groups and Cayley graphs. We describe the advantages and drawbacks of this construction. The mathematical structure helps in understanding the security properties and improving the efficiency of the functions, but it is also useful to the attacker who wants to break it. In particular, we present three attacks specific to these hash functions, trapdoor attacks, subgroup attacks and lifting attacks, and illustrate their use in old and recent attacks against particular functions.

Although most concrete proposals have been broken, we point out that each of these proposals was also particularly weak in some sense. Since the generic design has very interesting properties, its security definitely deserves further studies. We conclude with some recent results for the group $SL(2, \mathbb{F}_{2^n})$.

P-signatures à seuil
Application : Techniques de management de clés

Amar SIAD, Moncef AMARA
Université Paris 8, 2 rue de la Liberté
93526 SAINT-DENIS, FRANCE
siad@math.univ-paris13.fr

Résumé :

Récemment, de nombreux schémas de signatures préservant la vie privée des utilisateurs, particulièrement l'anonymat, ont été développées. Ces signatures, à partir de points de vues différents, mettent l'accent sur l'anonymat et développent des propriétés intéressante. Parmi ces schémas : signatures de groupe, signatures en anneau, signatures traçables, et signatures sur messages engagés. Ces dernières faisaient l'objet des plusieurs travaux [1,2,3], où plusieurs approches ont été proposées comme CL-signatures [1], P-signatures [2], et les signatures automorphes [3]. Cependant, malgré qu'elle présentent des propriétés très importantes, elle n'ont pas encore été transférées en systèmes pratiques, et personne n'a étudier dans quel système peuvent être intégrées.

Par extension des travaux de *Belenkiy et al.* [1] nous proposons le concept de *p-signatures à seuil* (*threshold P-signature* en anglais), qui permet la génération des P-signatures de manière distribuée. Dans ce contexte, nous donnons une définition formelle des P-signatures à seuil, le modèle de sécurité approprié, et nous donnons des constructions pratiques dont les preuves de sécurité sont en cours de développement.

Les P-signatures à seuil ont une application très intéressante dans les techniques de management de clés pour les cryptosystèmes distribués. Elles permettent l'extension de l'architecture proposée par *Chow* [4], et de développer ainsi des protocoles anonymes de génération de clés de manière distribuée.

Références :

1. J. Camenisch and A. Lysyanskaya, signature scheme with efficient protocols," in SCN 2002, volume 2576 of LNCS. Springer Verlag, 2002, pp. 268-289.
2. M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, P-signatures and noninteractive anonymous credentials," in In Theory of Cryptography Conference,2008, pp. 356-374.
3. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-Preserving Signatures and Commitments to Group Elements. In CRYPTO 2010, volume 6223 of LNCS, pages 209-236. Springer, 2010.
4. S. Chow. Removing escrow from identity-based encryption. In 12th International Conference on Practice and Theory in Public Key Cryptography, pages 256-272, 2009.

Naive algebraic computation of low-degree isogenies in genus 2

Benjamin Smith, LIX, École polytechnique

Recent work of Lubicz and Robert (implemented in the AVIsogenies software package by Bisson, Cosset, and Robert) has given us an effective means of computing (l, l)-isogenies of abelian surfaces over finite fields. Their approach is based on theta functions, and requires a (possibly large) field extension to ensure enough theta $4l$-level structure is rational. In this talk we describe an algebraic construction, avoiding (explicit) theta functions, which allows us to rapidly compute $(3, 3)$-isogenies with at most a quadratic field extension, avoiding the bottleneck introduced by the theta structure field extensions.

Identity-Based Trace and Revoke Schemes Resisting to Pirates 2.0 and Pirate Evolution Attacks

February 9, 2011

We study the problem of Broadcast Encryption and Traitor Tracing in the Identity-based setting.

Identity-based cryptography, introduced by Shamir, enables an user to use its identity such as its email address as its public key and to get the corresponding secret key from the trusted center. However, it's only very recently that Identity-based schemes in "one-to-many" settings were introduced, namely Identity-based traitor tracing at PKC '07 and Identity-based broadcast encryption at ASIACRYPT'07.

Broadcast encryption systems enables a center to encrypt a message for any subset of legitimate users and to prevent any set of revoked users from recovering the broadcasted information; *Traitor tracing schemes* enables the center to trace users who collude to produce pirate decoders. *Trace and Revoke systems* provide both the properties of broadcast encryption and traitor tracing systems. The most famous trace and revoke schemes are those from the subset-cover framework of Naor-Naor-Lotspiech, namely Complete Subtree scheme and Subset Difference scheme.

In this work, we propose the first Identity-Based Trace and Revoke (IDTR) schemes which are efficient and resist to advanced types of attacks. They are in an extended model of Identity based Traitor Tracing scheme introduced by Abdalla *et al.* (PKC '07) with an additional property : revocability. Moreover, our schemes are more efficient than the scheme of Abdalla *et al.*.

Our constructions follow the subset cover framework. We first propose a generic construction which transforms an Identity-Based Encryption with wildcard WIBE of depth $\log(N)$ (N is the number of users) into an Identity-Based Trace and Revoke scheme by relying on the Complete Subtree framework (of depth $\log(N)$). This leads, however, to a scheme with $\log(N)$ private key size (as in a complete subtree scheme). To improve this, we introduce Generalized WIBE (GWIBE) and propose a second construction that is based on GWIBE of two levels. This latter scheme provides a nice feature of constant private key size (3 group elements).

An important property of our constructions is that they resist to advanced attacks on subset cover framework, namely the Pirate Evolution attacks (proposed by Kiayias and Pehlivanoglu at Crypto '07) and Pirates 2.0 (proposed by Billet-Phan at Eurocrypt '09). The only known way for defending Pirate Evolution attacks in the subset cover framework is proposed by Jin and Lotspiech at ISPEC '09 but it decreases seriously the efficiency of the original schemes (their method results in schemes with sub-linear size ciphertext in the number of total users). Our schemes are, in contrast, very competitive to the original complete subtree scheme.

Le problèms SD q-aire et ses applications

P.-L. Cayrel (cayrel@cased.de)
CASED, Allemagne

P. Véron (veron@univ-tln.fr)
IMATH, Université du Sud Toulon-Var, France

M. El Yousfi Alaoui (elyousfi@cased.de)
CASED, Allemagne

1. Introduction

L'algorithme de Shor [1] permet de mener une attaque polynomiale en temps sur un ordinateur quantique envers de nombreux protocoles cryptographiques dont la sécurité dépend de la difficulté de la factorisation ou de la résolution du problème du logarithme discret. Ce n'est pas le cas des protocoles basés sur les systèmes d'équations multivariés, les réseaux ou les codes correcteurs d'erreurs. Dans ce travail, nous nous intéressons aux applications d'un problème NP-complet issu de la théorie des codes : le décodage du syndrome (problème SD).

Nom	:	**SD**
Entrée	:	H une matrice binaire $k \times n$, i un vecteur binaire de taille k, p un entier
Question	:	Existe-t-il un vecteur binaire s de taille n et de poids p tel que $Hs^t = i$?

Le problème SD q-aire est une généralisation du problème ci-dessus où l'on considère les objets manipulés dans le corps fini à q éléments. Sous ces conditions, le problème reste NP-complet comme cela a été démontré par A. Barg en 1994 [2]. Ce n'est cependant que depuis des travaux récemment développés en 2009 et 2010 que l'on peut caractériser les instances difficiles de ce problème et définir des paramètres à utiliser dans le cadre d'une application cryptographique [3], [4]. Nous montrons dans ce papier que l'utilisation du problème SD sur $\mathbb{F}_q$ permet la définition de protocoles améliorant les performances de ceux basés sur le problème SD binaire classique.

2. Un schéma d'identification à 5 passes

C'est en 1993 que J. Stern a proposé le premier protocole d'identification zéro-knowledge dont la sécurité dépend du problème SD binaire [5]. Il s'agit d'un protocole interactif dans lequel une entité (communément appelé le prouveur) démontre qu'il connaît une solution s pour une instance publique de SD donnée. A la fin du protocole, un intrus ayant capturé les échanges effectués ne pourra en déduire aucune information sur le secret s qui lui permettrait à son tour de simuler un faux processus d'identification. Le protocole proposé par J. Stern se compose de r tours, à chaque tour le prouveur doit être capable de répondre à une question tirée au hasard parmi 3. Un intrus a au plus deux chances sur 3 de pouvoir répondre correctement ce qui borne sa probabilité de réussite globale par $(2/3)^r$. Il suffit donc de régler le paramètre r pour limiter le seuil de fraude tout en sachant que le nombre d'informations échangées et le nombre de calculs effectués par le prouveur croît avec r.

L'un des inconvénients majeurs du protocole de Stern est la taille de la donnée publique ainsi que le nombre de bits échangés au cours du processus d'identification. En utilisant la version q-aire du problème SD, nous proposons un nouveau schéma d'identification zéro-knowledge pour lequel la taille de ces deux paramètres est réduite. Le protocole se déroule en r tours et la probabilité de fraude est bornée par $(\frac{q}{2(q-1)})^r$, ce qui permet pour un seuil de fraude équivalent de réduire le nombre de tours à effectuer. Le tableau ci-après résume les performances du schéma proposé pour une probabilité de fraude de l'ordre de 2^{-16} et une complexité d'attaque du problème SD de l'ordre de 2^{87}.

	Stern SD	Schéma q-SD
Rounds	28	16
Matrix size (bits)	122500	32768
Public Id (bits)	350	512
Secret key (bits)	700	1024
Communication (bits)	42019	31888

3. Un schéma de signature de cercle à seuil

En généralisant le protocole de Stern et en appliquant l'heuristique de Fiat-Shamir, C. Aguilar, P-L. Cayrel et P. Gaborit ont introduit en 2008 le premier schéma de signature de cercle à seuil (t-out-of-N) fondé sur la théorie des codes [6]. Ce schéma permet à t membres de coopérer pour construire une signature, tout en préservant leur anonymat parmi les N membres du cercle. Afin de bénéficier des résultats présentés dans le tableau ci-dessus, nous proposons une signature du cercle à seuil amélioré qui est anonyme et sûr dans le modèle de l'oracle aléatoire. La table ci-après compare la taille de la clé publique et de la signature de notre schéma avec celle d'Aguilar et. al utilisant des codes aléatoires, avec $(N, t) = (100, 50)$.

	Schéma d'Aguilar et. al	Notre schéma
Pk size (KBytes)	1500	400
Sign. size (KBytes)	2448	1844

Bibliographie

1. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput., vol. 26(5), pp.1484–1509, 1997*,
2. S. Barg, Some New NP-Complete Coding Problems, *Probl. Peredachi Inf., vol. 30(3), pp.23–28, 1994*,
3. C. Peters, Information-set decoding for linear codes over Fq, *Cryptology ePrint Archive, Report 2009/589,2009*,
4. R. Niebuhr, P.-L. Cayrel, S. Bulygin, J. Buchmann, On lower bounds for Information Set Decoding over Fq, *preprint,SCC 2010*,
5. J. Stern, A new identification scheme based on syndrome decoding, *Crypto'93, LNCS vol. 773, pp. 13–21*,
6. C. Aguilar Melchor and P.-L. Cayrel and P. Gaborit, A new efficient threshold ring signature scheme based on coding theory, *Post-quantum cryptography, second international workshop, PQCrypto 2008, Lecture Notes in Computer Science. vol. 5299, pp. 1–16*,

Decoding Interleaved Reed–Solomon Codes Beyond their Joint Error–Correcting Capability

Antonia Wachter
Inst. of Telecomm. and Applied Information Theory
Ulm University, Germany and
Inst. de recherche math. de Rennes (IRMAR)
Université de Rennes 1, Rennes, France
antonia.wachter@uni-ulm.de

Alexander Zeh
Inst. of Telecomm. and Applied Information Theory
Ulm University, Germany and
École Polytechnique
LIX/CNRS, INRIA-Saclay, Paris, France
alexander.zeh@uni-ulm.de

***Abstract*—A new decoding algorithm for Interleaved Reed–Solomon (IRS) codes is presented. This approach increases the error correcting capability of IRS codes compared to other known approaches (e.g. joint decoding). Moreover, it generalizes well–known decoding approaches from a theoretical point of view.**

I. Introduction

Interleaved Reed–Solomon (IRS) codes [1], [2], [3] can be seen as s parallel codewords of *Reed–Solomon* (RS) codes with the same length n. IRS codes make sense in scenarios where burst errors occur, i.e., the error affects all s RS codewords at the same position. Joint decoding of homogenous IRS with dimension k can be done up to a decoding radius $\tau_{IRS} = \lfloor s(n-k)/(s+1) \rfloor$. The scheme from [4] virtually extends a usual low–rate RS code to an IRS code and increases the decoding radius of usual RS codes. In [5], the ideas of IRS codes and a virtual extension are combined. Each of the s codewords is virtually extended with the scheme from [4].

We generalize the scheme from [5] by virtually extending the IRS code, but use also combinations among the s RS codes. Our approach increases the decoding radius of IRS codes significantly beyond the joint error–correcting bound for IRS codes [3] and also beyond the scheme from [5]. From a theoretical point of view, our approach can be seen as the generalization of both [4] and [5].

II. Increasing the Decoding Radius

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be nonzero distinct elements (code locators) of the finite field $\mathbb{F} = \mathrm{GF}(q)$ and denote $\mathcal{L} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Denote $f(\mathcal{L}) = (f(\alpha_i), \ldots, f(\alpha_n))$ for a given polynomial $f(x)$ over $\mathbb{F}$. An RS code $\mathcal{RS}(n,k)$ over $\mathbb{F}$ with $n < q$ is given by $\mathcal{RS}(n,k) = \{\mathbf{c} = f(\mathcal{L}) : f(x) \in \mathbb{F}_k[x]\}$, where $\mathbb{F}_k[x]$ stands for the set of all polynomials with degree less than k. Let a homogenous IRS code $\mathcal{IRS}(n,k,s)$ of interleaving order s be defined by s $\mathcal{RS}(n,k)$ codes with the evaluation polynomials $f^{(1)}(x), \ldots, f^{(s)}(x)$ where $f^{(i)}(x) \in \mathbb{F}_k[x]$, for all $i = 1, \ldots, s$.

In this contribution, we virtually extend a low–rate homogenous $\mathcal{IRS}(n,k,s)$ code by combining codewords from the s $\mathcal{RS}(n,k)$ codes among each other. We call this extended code a *mixed* virtually extended IRS code $\mathcal{MIRS}(n,k,s,\ell)$ of extension order ℓ, which is is given by

$$\mathcal{MIRS}(n,k,s,\ell) = \begin{pmatrix} f^{(j_1)}(\mathcal{L}), & j_1 = 1, \ldots, s \\ f^{(j_1,j_2)}(\mathcal{L}), & j_1, j_2 = 1, \ldots, s \\ \vdots & \\ f^{(j_1,\ldots,j_\ell)}(\mathcal{L}), & j_1, \ldots, j_\ell = 1, \ldots, s \end{pmatrix},$$

where $f^{(j_1,j_2,\ldots,j_h)}(x) = \prod_{i=1}^{h} f^{(j_i)}(x) \in \mathbb{F}_{h(k-1)+1}[x]$.

Hence, $f^{(j_1,j_2,\ldots,j_h)}(\mathcal{L})$ is a codeword of an $\mathcal{RS}(n, h(k-1)+1)$ code, for all $h = 1, \ldots, s$.

We consider the transmission of an $\mathcal{IRS}(n,k,s)$ code over a channel with burst errors and obtain s received words.

To increase the error correcting capability of this homogenous low–rate $\mathcal{IRS}(n,k,s)$ code, we show how to extend it to an $\mathcal{MIRS}(n,k,s,\ell)$ using the received words. The resulting $\mathcal{MIRS}(n,k,s,\ell)$ can be seen as a heterogenous IRS code with interleaving order $u = \binom{s+\ell}{s} - 1$.

We give an efficient decoding algorithm and calculate the new decoding radius and rate restrictions.

The normalized asymptotic decoding radius depending on the rate $R = k/n$ for $n \to \infty$ of our new approach is:

$$\frac{\tau^{(s,\ell)}}{n} = 1 - \frac{\ell!}{\prod_{h=1}^{\ell}(s+h)} - R \cdot \frac{\ell s}{s+1}.$$

In Fig. 1, this asymptotic decoding radius is shown, and compared with joint decoding and the approach from [5].

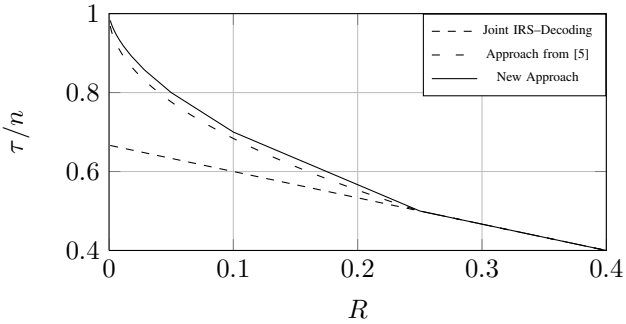

Fig. 1. Asymp. Decoding Radius ($n \to \infty$) for an $\mathcal{IRS}(n,k,s=2)$ code

REFERENCES

[1] Krachkovsky and Y. X. Lee, "Decoding for iterative Reed-Solomon coding schemes," *IEEE Transactions on Magnetics*, vol. 33, no. 5, pp. 2740–2742, Sept 1997. [Online]. Available: http://dx.doi.org/10.1109/20.617715

[2] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding of Interleaved Reed Solomon Codes over Noisy Data," in *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, J. C. M. Baeten, J. K. Lenstra, J. Parrow, and G. J. Woeginger, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, June 2003, vol. 2719, ch. 9, p. 188. [Online]. Available: http://dx.doi.org/10.1007/3-540-45061-0_9

[3] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative Decoding of Interleaved Reed-Solomon Codes and Concatenated Code Designs," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 2991–3012, 2009. [Online]. Available: http://dx.doi.org/10.1109/TIT.2009.2021308

[4] ——, "Syndrome Decoding of Reed–Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5245–5252, October 2010. [Online]. Available: http://dx.doi.org/10.1109/TIT.2010.2060130

[5] G. Schmidt, V. Sidorenko, and M. Bossert, "Enhancing the Correcting Radius of Interleaved Reed-Solomon Decoding using Syndrome Extension Techniques," in *IEEE International Symposium on Information Theory 2007 (ISIT 2007)*, June 2007. [Online]. Available: http://dx.doi.org/xpls/abs_all.jsp?arnumber=4557409\&tag=1

Decoding of Some Classes of Binary Cyclic Codes beyond the BCH Bound

Alexander Zeh
Institute of Telecommunications
and Applied Information Theory
Ulm University, Germany and
École Polytechnique
LIX/CNRS, INRIA-Saclay, Paris, France
{alexander.zeh}@uni-ulm.de

Antonia Wachter
Institute of Telecommunications
and Applied Information Theory
Ulm University, Germany and
Inst. de recherche math. de Rennes (IRMAR)
Université de Rennes 1, Rennes, France
{antonia.wachter}@uni-ulm.de

Sergey Bezzateev
Saint Petersburg State University
of Airspace Instrumentation
St. Petersburg, Russia
bsv@aanet.ru

***Abstract*—We give new bounds on the minimum distance of several classes of binary cyclic codes. The approach is based on the description of binary cyclic codes as rational functions. Furthermore, a quadratic–time decoding algorithm up to this bound for these classes is developed.**

I. Introduction

Classical decoding algorithms like the Extended Euclidean Algorithm (EEA, [1]) or the Berlekamp–Massey Algorithm (BMA, [2], [3]) up to the BCH [4], [5] bound use the longest set of consecutive roots of a cyclic code. Other lower bounds of the minimum distance of cyclic codes are the Hartmann–Tzeng [6], [7], [8] bound and the Roos [9], [10] bound, where multiple sets of consecutive roots are considered. Feng and Tzeng [11], [12] have shown an extended syndrome matrix for binary cyclic codes up to a length of 63, which allows decoding up to the actual distance of the code. They fit the available syndromes manually into this structure and for some codes they calculate missing syndrome elements by using linear dependencies between existing syndromes.

Our approach is different. We identify sequences of zeros (and non-zeros) of binary cyclic codes that are equal to sequences of power series of rational functions. We prove a general new lower bound of the minimum distance and identify several classes of binary cyclic codes by means of their lengths and their defining sets.

II. Binary Cyclic Codes Revisited

A binary cyclic code of length n, dimension k and distance d is denoted by $\mathcal{C}(2^m; n, k, d)$. It is a multiple of its generator polynomial $g(x)$ with roots in $\mathbb{GF}(2^m)$, where $n \mid (2^m - 1)$. A cyclotomic coset M_r is given by: $M_r = \{r2^j \,|\, j = 0, 1, \ldots, n_r - 1\}$, where n_r is the smallest integer such that $r2^{n_r} \equiv r \mod n$. Let α be a nth root of unity of $\mathbb{GF}(2^m)$. It is well–known that the minimal polynomial of the element r is given by: $M_r(x) = \prod_{i \in M_r}(x - \alpha^i)$. The defining set $D_\mathcal{C}$ of a binary cyclic code $\mathcal{C}(2^m; n, k, d)$ is the set of zeros of the generator polynomial $g(x)$ and it can be partitioned into s cyclotomic cosets:

$$\begin{aligned} D_\mathcal{C} &= \{0 \le i \le n-1 \,|\, g(\alpha^i) = 0\} \\ &= M_{r_1} \cup M_{r_2} \cup \cdots \cup M_{r_s}. \end{aligned} \tag{1}$$

Hence, the generator polynomial is

$$g(x) = \prod_{i=1}^{s} M_{r_i}(x). \tag{2}$$

III. Description by Rational Functions

For a given binary cyclic code with generator polynomial $g(x)$, we know that $g(\alpha^i) = 0$, $\forall i \in D_\mathcal{C}$ and therefore $S_i = 0$. We associate a rational function $h(x, \alpha_i, \delta)/f(x, \alpha_i)$ with the code such that for each codeword $\mathbf{c} = (c_0 \; c_1 \; \ldots \; c_{n-1})$ the following holds [13] (compare [14, Chapter 12]):

$$\sum_{i=0}^{n-1} c_i \frac{h(x, \alpha_i, \delta)}{f(x, \alpha_i)} \equiv \frac{\Omega(x)}{\Lambda(x)} \equiv 0 \mod x^T, \tag{3}$$

where $u = \deg f(x, \alpha_i) > v = \deg h(x, \alpha_i)$, $\gcd(f(x, \alpha_i), h(x, \alpha_i, \delta)) = 1$, $\gcd(f(x, \alpha_i), f(x, \alpha_j)) = 1$ for all $i \neq j$ and with $S_{i+\delta}\overline{f}_i = 0$ for all $i = 0, \ldots, T-1$.

The minimum distance of a $\mathcal{C}(2^m; n, k, d)$ code that can be described by such a rational function $h(x, \alpha_i, \delta)/f(x, \alpha_i)$ is given by the following lemma.

Lemma 1 (Minimum Distance) *[13] The minimum distance d of a $\mathcal{C}(2^m; n, k, d)$ code defined by* (3) *satisfies the following inequality*

$$d \ge \left\lceil \frac{T - v}{u} + 1 \right\rceil \tag{4}$$

Proof: Let us consider a codeword of minimal weight d, then the sum in (3) consists only of d fractions. By definition $\gcd(f(x, \alpha^i), f(x, \alpha^j)) = 1$ for all i, j, hence, the least common denominator $\Lambda(x)$ is the product of the d denominators. Each numerator of the d fractions is therefore multiplied by the other $(d-1)$ denominators. Hence, the degree of the resulting numerator is $\deg \Omega(x) = (d-1) \cdot u + v$.

Since $\Omega(x) \neq 0$, (3) is fulfilled if and only if $\deg \Omega(x) \ge T$, we obtain $(d-1) \cdot u + v \ge T$ and the statement (4) follows. ∎

Based on this lemma we will identify several classes of binary cyclic codes and give an appropriate decoding algorithm.

REFERENCES

[1] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A Method for Solving Key Equation for Decoding Goppa Codes," *Information and Control*, vol. 27, no. 1, pp. 87–99, 1975. [Online]. Available: http://dblp.uni-trier.de/db/journals/iandc/iandc27.html#SugiyamaKHN75

[2] E. R. Berlekamp, *Algebraic coding theory*. McGraw-Hill, 1968. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20\&path=ASIN/B0006YH9F4

[3] J. Massey, "Shift-register synthesis and BCH decoding," *Information Theory, IEEE Transactions on*, vol. 15, no. 1, pp. 122–127, January 2003. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1054260

[4] A. Hocquenghem, "Codes Correcteurs d'Erreurs," *Chiffres (paris)*, vol. 2, pp. 147–156, September 1959.

[5] R. C. Bose and D. K. R. Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, March 1960. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(60)90287-4

[6] C. Hartmann, "Decoding beyond the BCH bound (Corresp.)," *IEEE Transactions on Information Theory*, vol. 18, no. 3, pp. 441–444, May 1972. [Online]. Available: http://dx.doi.org/10.1109/TIT.1972.1054824

[7] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, no. 5, pp. 489–498, June 1972. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(72)90887-X

[8] ——, "Decoding beyond the BCH bound using multiple sets of syndrome sequences (Corresp.)," *Information Theory, IEEE Transactions on*, vol. 20, no. 2, March 1974.

[9] C. Roos, "A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound," *Journal of Combinatorial Theory, Series A*, vol. 33, no. 2, pp. 229–232, September 1982. [Online]. Available: http://dx.doi.org/10.1016/0097-3165(82)90014-0

[10] ——, "A new lower bound for the minimum distance of a cyclic code," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 330–332, May 1983. [Online]. Available: http://dx.doi.org/10.1109/TIT.1983.1056672

[11] G. L. Feng and K. K. Tzeng, "Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations," *IEEE Transactions on Information Theory*, vol. 37, no. 6, pp. 1716–1723, 1991. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=104340

[12] ——, "A new procedure for decoding cyclic and BCH codes up to actual minimum distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1364–1374, 1994. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=333854

[13] S. V. Bezzateev and N. A. Shekhunova, "One Generalization of Goppa Codes," pp. 299+, 1997. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=\&arnumber=613221

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes (North-Holland Mathematical Library)*. North Holland, June 1988. [Online]. Available: http://www.worldcat.org/isbn/0444851933