Tatra Mt. Math. Publ. **33** (2006), 149–157

TATRA MOUNTAINS
Mathematical Publications

CHOSEN CIPHERTEXT ATTACKS AS COMMON VULNERABILITY OF SOME GROUP- AND POLYNOMIAL-BASED ENCRYPTION SCHEMES

María Isabel González Vasco — Rainer Steinwandt

ABSTRACT. In the last few years, certain group- and polynomial-based public key encryption schemes have succumbed to reaction or chosen ciphertext attacks. We show that the principles underlying these group- and polynomial-based encryption schemes are identical and that the applied attack technique naturally carries over to a generalization of Koblitz's Polly Cracker scheme using Gröbner bases. Finally, we demonstrate that a countermeasure against chosen ciphertext attacks proposed for the Polly Two encryption scheme is insufficient when being combined with the recommended choice of the ground field.

1. Introduction

In [8] Wagner and Magyarik proposed a conceptual public key encryption scheme based on a variant of the word problem in finitely presented groups, which conceptually is rather appealing. However, in [7] it is shown that in the proposed form the scheme offers basically no protection against "active" attacks: a quite simple reaction attack can reveal large parts of the secret key. Recall that so-called reaction attacks are carried out by an adversary having access to an encryption oracle and to a black-box which identifies whether a given input is a valid ciphertext or not.

Something rather similar happened with a (multivariate) polynomial-based encryption scheme that has been published about 10 years after Wagner and Magyarik's proposal: The Polly Cracker scheme introduced by Fellows and Koblitz [1] turned out to be susceptible to a chosen ciphertext attack [6].

Subsequently we show that the (polynomial-based) Polly Cracker scheme is essentially a special case of the (group-based) proposal in [8], and that from this point of view, the cryptanalysis of Polly Cracker in [6] follows immediately from the mentioned attack on the proposal in [8]. Moreover, we show how to adapt

2000 Mathematics Subject Classification: Primary 94A60; Secondary 11T71.
Keywords: cryptanalysis, group based cryptography, polynomial based cryptography.

the chosen ciphertext attack against Polly Cracker so that it also succeeds when applied to a generalization of this scheme considered in [3]. Finally, we take a look at the Polly Two scheme of Ly [4, 5], which is related to Polly Cracker, and for which a protection against chosen ciphertext attacks has been proposed. Here we show that when being combined with the recommended choice of the ground field, this countermeasure does not prevent certain types of reaction/chosen ciphertext attacks.

2. A unified description of two encryption schemes and two corresponding attacks

A proposal of Wagner and Magyarik

At CRYPTO '84, Wagner and Magyarik put forward a new encryption scheme founded in the difficulty of the word problem for finitely presented groups [8]. Their proposal may be described as follows:

Key generation: produce a finite presentation (X, R) of a group G for which the word problem is *hard*, together with a set $S \subseteq \{X \cup X^{-1}\}^*$ such that for the quotient group $\widetilde{G}$, specified by $(X, R \cup S)$, the word problem can be solved efficiently by means of an algorithm $\mathcal{A}$.

Now let Σ be a finite alphabet and $W(\Sigma) = \{w_\sigma : \sigma \in \Sigma\}$ a subset of $\{X \cup X^{-1}\}^*$ such that if $\sigma \neq \tau$, then w_σ and w_τ are neither equivalent over G nor over $\widetilde{G}$.

The public key consists then of the presentation (X, R) and the set $W(\Sigma)$, whereas the set S (or, equivalently, the quotient $\widetilde{G}$) constitutes the private key.

Encryption: construct the ciphertext corresponding to $\sigma \in \Sigma$ by setting $w := w_\sigma$ and rewriting w using the public relations specified by R.

Decryption: recover the plaintext corresponding to w by running $\mathcal{A}$ with the inputs $w{w_\sigma}^{-1}$ $(\sigma \in \Sigma)$.

As the authors pointed out, some care must be taken in the key generation procedure in order to avoid very simple attacks to the above scheme: clearly, it must be the case that for most quotient groups of G with an easy word problem all the words in $W(\Sigma)$ collide (i.e., represent the same group element).

Also, more subtle problems may arise when turning this abstract description into a concrete encryption scheme. In particular, [7] shows that a concrete proposal put forward in [8] succumbs to a *reaction attack* in which the attacker proceeds as follows: to check whether a word r in $\{X \cup X^{-1}\}^*$ represents the identity in $\widetilde{G}$, he attaches it to a valid ciphertext. Then, he checks whether the word obtained is accepted as valid or rejected by the legitimate recipient.

Polly Cracker

Fellows and Koblitz [1] introduced the so-called *Polly Cracker scheme* in 1994. It may be described as follows:

Key generation: fix a polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ over a finite field $\mathbb{F}_q$, and select an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ along with a point $\xi := (\xi_1, \ldots, \xi_n) \in \mathbb{F}_q^n$ in the variety of I (that is, all polynomials of I have ξ as a zero).

A finite basis of I forms the public key, whereas the secret key is the point ξ.

Encryption: construct the ciphertext c corresponding to $\sigma \in \mathbb{F}_q$ by selecting a polynomial $p \in I$ and adding it to the plaintext, i.e., $c := \sigma + p \in \mathbb{F}_q[x_1, \ldots, x_n]$.

Decryption: recover the plaintext σ by evaluating c at ξ.

It is crucial how concrete instances are derived, and several proposals turned out to be weak. In particular, [6] points out the following chosen ciphertext attack: If the attacker sends a "fake" ciphertext of the form $x_i + p$ with $p \in I$, and learns the corresponding plaintext, then he learns the ith coordinate of the secret key. Doing this n times is sufficient to reveal the complete secret key.

A unifying view

Note that there are obvious common patterns in the two encryption schemes depicted above. For the polynomial based scheme, all encryptions of a plaintext $\sigma \in \mathbb{F}_q$ under a public ideal I are contained in the same residue class $\sigma + I \in \mathbb{F}_q[x_1, \ldots, x_n]/I$. This quotient ring is in particular an abelian group, and thus we may reformulate the Polly Cracker scheme in the following fashion:

Key generation: fix some $\xi \in \mathbb{F}_q^n$ and set $S := \{x_1 - \xi_1, \ldots, x_n - \xi_n\}$. Then choose a basis R of an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ contained in the ideal spanned by S in $\mathbb{F}_q[x_1, \ldots, x_n]$.

The abelian group $G := \mathbb{F}_q[x_1, \ldots, x_n]/(R)$ is made public, whereas $\widetilde{G} := \mathbb{F}_q[x_1, \ldots, x_n]/(R \cup S)$ is now the secret key. Moreover, we use the plaintext alphabet $\Sigma := \mathbb{F}_q$ and set $W(\Sigma) := \Sigma$ (which is the second element of our public key).

Note that clearly different elements from $W(\Sigma)$ never represent the same element in G or $\widetilde{G}$.

Encryption: construct a ciphertext for $\sigma \in \Sigma$ by simply rewriting $w_\sigma = \sigma$ with the public relations in R.

Decryption: subtract an element of $W(\Sigma)$ from w, and check whether the obtained difference reduces to 0 modulo the secret Gröbner basis S of the ideal spanned by $R \cup S$, i.e., check whether the difference represents the identity in $\widetilde{G}$.

Thus, clearly the Polly Cracker scheme can be seen as an instantiation of Wagner and Magyarik's proposal.

Now it is natural to try to apply the attack from [7]: The secret relations have the form $x_i - \xi_i$, and [7] suggests to fix some $w_\sigma \in W(\Sigma)$ and a ciphertext $w := w_\sigma + (x_i - \eta)$ with η a guess for ξ_i. In the attack model in [7] now the attacker learns whether w is a valid ciphertext, but Polly Cracker *never* rejects a polynomial. So it is natural to consider an attacker who learns the obtained plaintext. In our case, this plaintext is $w_\sigma + \xi_i - \eta$, i.e., the attacker learns ξ_i. Clearly, the choice of w_σ and η is irrelevant, so the attack we found through our reformulation is basically the one in [6].

3. Adapting the attack technique to a generalized Polly Cracker scheme

In [3, Ch. 5, Section 3.3] the following generalization of Polly Cracker is discussed:

Key generation: fix a polynomial ring $\mathbb{F}_q[x_1, \dots, x_n]$ over a finite field $\mathbb{F}_q$, and select an ideal $I \subseteq \mathbb{F}_q[x_1, \dots, x_n]$, which is explicited through a set of polynomials R. Let S be a Gröbner basis s.t. $I \subseteq (S)$.

The public key consists of the set R together with an alphabet $\Sigma \subseteq \mathbb{F}_q[x_1, \dots, x_n]$ s.t. no $\sigma \in \Sigma$ can be reduced modulo S (again, $W(\Sigma) = \Sigma$). The secret key is the Gröbner basis S.

Encryption: proceed as in the preceding scheme.

Decryption: recover the plaintext corresponding to a ciphertext polynomial c by computing its normal form modulo S.

Clearly, as it was the case for the preceding scheme, the above scheme can also be rewritten in an analogous group-theoretic terminology. In this case, S allows for an efficient solution of the word problem in the abelian group $\mathbb{F}_q[x_1, \dots, x_n]/(R \cup S)$.

As an example, [3, Ch. 5, Example 3.4] considers a secret Gröbner basis S comprised of all polynomials of the form $\prod_{i=1}^{n} (x_i - \xi_i)^{\alpha_i}$ with $\alpha_1 + \dots + \alpha_n = d$ and Σ consisting of all polynomials of total degree $< d$. In particular, as d is public, S is determined by ξ up to searching all partitions of d. Moreover, for $1 \leqslant i \leqslant n$

we have $(x_i - \xi_i)^d \in S$. To enforce an application of the latter "rewriting rule" during decryption, we can, e.g., send a "fake" ciphertext $c := 0 + (x_i - 0)^d + p$ with $p \in I$ arbitrary. The normal form of c modulo S is $x_i^d - (x_i - \xi_i)^d$, i.e., it involves the monomial $d \cdot \xi_i \cdot x_i^{d-1}$. Hence for $\mathrm{char}(\mathbb{F}_q) \nmid d$ we immediately obtain ξ_i from the plaintext. The case $\mathrm{char}(\mathbb{F}_q) \mid d$ can be handled similarly, and hence independent of d and q we can find "fake" chosen ciphertexts that enable us to reveal the secret key.

4. Dodging a protection mechanism against chosen ciphertext attacks: Polly Two

In [4] Ly introduces the probabilistic encryption scheme Polly Two, which can be regarded as a successor of Polly Cracker. As pointed out in [4, Section 4.4] in its original form Polly Two is also vulnerable to chosen ciphertext attacks, and therefore Ly suggests a countermeasure that is to overcome this problem. The basic ingredients of Polly Two with "CCA-protection" are as follows (see [4] for details):

Key generation: the public information consists of

- (system-wide identical) polynomials $g_1, \dots, g_t \in \mathbb{F}_q[x_1, \dots, x_n]$ and
- (a user-specific) ideal $J \subseteq \mathbb{F}_q[y_1, \dots, y_t]$.

The secret data is given by points $(\xi_1, \dots, \xi_n) \neq (\eta_1, \dots, \eta_n) \in \mathbb{F}_q^n$ such that for $(\nu_1, \dots, \nu_n) \in \{(\xi_1, \dots, \xi_n), (\eta_1, \dots, \eta_n)\}$ we have

- $\prod_{i=1}^{t} g_i(\nu_1, \dots, \nu_n) \neq 0$,
- $f\big(g_1(\nu_1, \dots, \nu_n), \dots, g_t(\nu_1, \dots, \nu_n)\big) = 0$ for all $f \in J$.

Encryption: to encrypt a plaintext $\sigma \in \mathbb{F}_q$, we choose

- an exponent $(\kappa_1, \dots, \kappa_t) \in \mathbb{N}_0^t$,
- a polynomial $p \in J$ and
- a polynomial h from the kernel of

$$\begin{aligned} \mathbb{F}_q[y_1, \dots, y_t] &\longrightarrow \mathbb{F}_q[g_1, \dots, g_t], \\ y_i &\longmapsto g_i, \end{aligned}$$

and define the ciphertext c encrypting σ as the pair

$$c := \Big(p + h + \sigma \cdot \prod_{i=1}^{t} y_i^{\kappa_i}, (\kappa_1, \dots, \kappa_t)\Big).$$

Decryption: to decrypt a ciphertext $\big(c,(\kappa_1,\dots,\kappa_t)\big)$, for both $(\nu_1,\dots,\nu_n)\in\big\{(\xi_1,\dots,\xi_n),(\eta_1,\dots,\eta_n)\big\}$ we compute

$$\sigma_{(\nu_1,\dots,\nu_n)} := \frac{c\big(g_1(\nu_1,\dots,\nu_n),\dots,g_t(\nu_1,\dots,\nu_n)\big)}{\prod_{i=1}^{t} g_i(\nu_1,\dots,\nu_n)^{\kappa_i}}\,. \tag{1}$$

In case of $\sigma_{(\xi_1,\dots,\xi_n)}\neq\sigma_{(\eta_1,\dots,\eta_n)}$ the ciphertext c is considered as invalid, and otherwise the plaintext $m_{(\xi_1,\dots,\xi_n)}=m_{(\eta_1,\dots,\eta_n)}$ is returned.[1]

Naively applying (an analogue of) the chosen ciphertext attack against the original Polly Cracker scheme does not pay off here, as ciphertexts of, say, the form $\big(y_i,(0,\dots,0)\big)$ will be recognized as invalid whenever $g_i(\xi_1,\dots,\xi_n)\neq g_i(\eta_1,\dots,\eta_n)$. However, in the sequel we show that for the recommended choices $\mathbb{F}_q=\mathbb{F}_{2^{23}}$ for the ground field and $t=11$ [4] reaction/chosen ciphertext attacks are nevertheless feasible, independent of how the other parameters of the scheme are chosen.[2]

4.1 Attacking individual plaintexts with a reaction attack

Suppose we are given a ciphertext $\big(c,(\kappa_1,\dots,\kappa_t)\big)\in\mathbb{F}_q[y_1,\dots,y_t]\times\mathbb{N}_0^t$ encrypting some unknown plaintext $\sigma\in\mathbb{F}_q$. Now, for $i\in\{1,\dots,t\}$, $\tau\in\mathbb{F}_q$, consider the polynomial

$$c_{i,\tau} := \left(c-\tau\cdot\prod_{i=1}^{t} y_i^{\kappa_i}\right)\cdot y_i\,.$$

For $\tau=\sigma$ and all $i\in\{1,\dots,t\}$ this polynomial $c_{i,\tau}$ decrypts to 0, and thus in particular is not rejected as invalid by the decryption procedure. On the other hand, for $\tau\neq\sigma$ at least one of $c_{1,\tau},\dots,c_{t,\tau}$ is considered as invalid by the decryption procedure: Applying the decryption formulae (1) to $c_{i,\tau}$ yields $\sigma_{(\xi_1,\dots,\xi_n)}=(\sigma-\tau)\cdot g_i(\xi_1,\dots,\xi_n)$ resp. $\sigma_{(\eta_1,\dots,\eta_n)}=(\sigma-\tau)\cdot g_i(\eta_1,\dots,\eta_n)$, and by assumption the values $g_i(\xi_1,\dots,\xi_n)$ and $g_i(\eta_1,\dots,\eta_n)$ differ for at least one i. Thus to reveal σ it is certainly sufficient to check for $t\cdot q$ "fake" ciphertexts $\big(c_{i,\tau},(\kappa_1,\dots,\kappa_t)\big)$ whether they are rejected by the decryption procedure. In particular, for the parameter choice $q=2^{23}$, $t=11$ proposed in [4] this attack can be regarded as feasible.

Remark. In [4, Section 4.4] Ly considers another countermeasure to chosen ciphertext attacks where the decryption procedure becomes stateful: There a

[1] For this countermeasure to be effective at all, $g_i(\xi_1,\dots,\xi_n)\neq g_i(\eta_1,\dots,\eta_n)$ must hold for at least one $i\in\{1,\dots,t\}$; throughout we assume this condition to be met.

[2] For the specific challenge parameters in [4] Grassl and Steinwandt have recently demonstrated that in fact the public data is sufficient to reconstruct a secret key equivalent to the original one [2]; for the attack considered in this paper only q and t are relevant.

ciphertext $(p, (\kappa_1, \ldots, \kappa_t))$ is rejected if the same $(\kappa_1, \ldots, \kappa_t)$ has already been used earlier. Adapting the above attack to this setting is straightforward: Instead of ciphertexts $(c_{i,\tau}, (\kappa_1, \ldots, \kappa_t))$ we can use $\left(c_{i,\tau} \cdot \prod_{i=1}^{t} y_i^{\varepsilon_i}, (\kappa_1 + \varepsilon_1, \ldots, \kappa_t + \varepsilon_t)\right)$, where for each query to the decryption oracle a new $(\varepsilon_1, \ldots, \varepsilon_t) \in \mathbb{N}_0^t$ is selected.

4.2 Attacking the secret key with a reaction/chosen ciphertext attack

With the usual security requirements on public key encryption schemes in mind, for the proposed parameter choices $q = 2^{23}$ and $t = 11$ even a reaction attack against the secret key may be considered as feasible. More precisely, we do not recover the secret zeroes $(\xi_1, \ldots, \xi_n), (\eta_1, \ldots, \eta_n)$, but the values $g_1(\nu_1, \ldots, \nu_n), \ldots, g_t(\nu_1, \ldots, \nu_n)$ $((\nu_1, \ldots, \nu_n) \in \{(\xi_1, \ldots, \xi_n), (\eta_1, \ldots, \eta_n)\})$, which is sufficient for applying the decryption procedure. For finding these values, we adapt an attack from [6] against the original Polly Cracker scheme:

In a first step, for each $1 \leqslant i \leqslant t$ we send for all $\alpha, \beta \in \mathbb{F}_q$ a chosen ciphertext $(c_{\alpha,\beta}, \kappa)$ to the decryption oracle where $\kappa \in \mathbb{N}_0^t$ can be chosen arbitrarily and $c_{\alpha,\beta} := (y_i - \alpha)(y_i - \beta) + p$ for some (arbitrary) $p \in J$. If $(c_{\alpha,\beta}, \kappa)$ decrypts to the valid plaintext 0, then we may assume that the "ith coordinates" $g_i(\xi_1, \ldots, \xi_n)$, $g_i(\eta_1, \ldots, \eta_n)$ are contained in the (one- or two-element) set $\{\alpha\} \cup \{\beta\}$. Thus we may assume that with no more than q^2 chosen "fake" ciphertexts we get t candidate pairs $\{\alpha_1, \beta_1\}, \ldots, \{\alpha_t, \beta_t\}$ for the values of $g_i(\xi_1, \ldots, \xi_n)$, $g_i(\eta_1, \ldots, \eta_n)$ $(1 \leqslant i \leqslant t)$, and we are left to assign the coordinates to $g_i(\xi_1, \ldots, \xi_n)$ and $g_i(\eta_1, \ldots, \eta_n)$ accordingly. Of course, for those coordinates i with $g_i(\xi_1, \ldots, \xi_n) = g_i(\eta_1, \ldots, \eta_n)$ nothing is left to do, and in the remainder of this section we take only two-element sets $\{\alpha, \beta\}$ into account.

One possible strategy for "sorting together" the coordinates is the following which also occurs in [6] in connection with the original Polly Cracker: We send (along with an arbitrary $(\kappa_1, \ldots, \kappa_t) \in \mathbb{N}_0^t$) a polynomial of the form

$$(y_1 - \alpha_1)(y_2 - \alpha_2) + (y_1 - \beta_1)(y_2 - \beta_2) + p \quad (p \in J \text{ arbitrary})$$

to the decryption oracle. In dependence on whether (α_1, α_2) and (β_1, β_2) are substituted for (y_1, y_2), or whether the evaluation takes place at (α_1, β_2) and (β_1, α_2), the resulting plaintext will be invalid/non-zero[3] or zero. Thus, at least with a chosen ciphertext attack, we learn which of the first two coordinates fit together. Continuing analogously with the remaining coordinates, we learn the whole sequences $g_1(\nu_1, \ldots, \nu_n), \ldots, g_t(\nu_1, \ldots, \nu_n)$ $((\nu_1, \ldots, \nu_n) \in \{(\xi_1, \ldots, \xi_n), (\eta_1, \ldots, \eta_n)\})$.

[3] For $\prod_{i=1}^{t} g_i(\xi_1, \ldots, \xi_n)^{\kappa_i} \neq \prod_{i=1}^{t} g_i(\eta_1, \ldots, \eta_n)^{\kappa_i}$ the plaintext is invalid, otherwise we may only conclude that the plaintext is non-zero.

In summary, about $q^2 + t$ chosen "fake" ciphertexts enable an attacker to get an equivalent secret key, and for the proposed parameter choices $q = 2^{23}$, $t = 11$ this attack cannot really be considered as infeasible. Also, similarly as in the previous section, the requirement of not reusing $(\kappa_1, \ldots, \kappa_t)$-values does not affect the attack's effectiveness.

5. Conclusion

Polly Cracker can be taken for a special instance of a group-based proposal. In this interpretation, the cryptanalysis of Polly Cracker is immediate from an attack on Wagner and Magyarik's scheme. Moreover, a generalization of Polly Cracker (which could also be seen as a group theoretic scheme) is vulnerable to the same attack technique.

Polly Two is a cryptosystem inspired by Polly Cracker, which ambitioned to dodge some of the known attacks of its ancestor. For the proposed parameter choices, here we have shown, however, that individual plaintexts can be recovered with a simple reaction attack and, moreover, an equivalent secret key can be constructed by a similar strategy (for the proposed parameter choices).

REFERENCES

[1] FELLOWS, M.—KOBLITZ, N.: *Combinatorial cryptosystems galore!*, in: Contemp. Math., Vol. 168 (Gary L. Mullen and Peter Jau-Shyong Shiue, eds.), 2nd International Conference on Finite Fields: Theory, Applications, and Algorithms, August 17–21, 1993, American Mathematical Society, Providence, 1994, pp. 51–61.

[2] GRASSL, M.—STEINWANDT, R.: E-mail communication with Le Van Ly. Unpublished, August 2004.

[3] KOBLITZ, N.: *Algebraic Aspects of Cryptography. With an Appendix on Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato*, Algorithms Comput. Math., Vol. 3, Springer-Verlag, Berlin, 1998.

[4] LE VAN LY: *Polly Two—a Public-Key Cryptosystem Based on Polly Cracker*, PhD thesis, Ruhr-Universität Bochum, Germany, October 2002. `http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/LyLeVan/diss.pdf`.

[5] LE VAN LY: *Gröbner Basen und das Kryptoverfahren Polly Two*, Presented at Tagung der Fachgruppe Computeralgebra in Kassel, Germany, Abstract available at `http://www.mathematik.uni-kassel.de/~compmath/Tagung2003/Ly.pdf`.

[6] STEINWANDT, R.—GEISELMANN, W.: *Cryptanalysis of Polly Cracker*, in: IEEE Trans. Inform. Theory, Vol. 48, Piscatavay, NJ, 2002, pp. 2990–2991.

[7] GONZÁLEZ VASCO, M. I.—STEINWANDT, R.: *A reaction attack on a public key cryptosystem based on the word problem*, in: Appl. Algebra Engrg., Comm. Comput., Vol 14, Springer-Verlag, Berlin, 2004, pp. 335–340.

[8] WAGNER, N. R.—MAGYARIK, M. R.: *A public key cryptosystem based on the word problem*, in: Adv. Cryptology, CRYPTO '84 (G. R. Blakley and David Chaum, eds.), Lecture Notes in Comput. Sci., Vol. 196, Springer-Verlag, Berlin, 1985, pp. 19–36.

Received September 22, 2004

María Isabel González Vasco
Departamento de Matemática Aplicada
Universidad Rey Juan Carlos
c/ Tulipán, s/n
28933 Madrid
SPAIN
E-mail: mariaisabel.vasco@urjc.es

Rainer Steinwandt
Institut für Algorithmen und Kognitive Systeme
Arbeitsgruppe Systemsicherheit, Prof. Beth
Universität Karlsruhe
G–76128 Karlsruhe
GERMANY
E-mail: steinwan@ira.uka.de