Kryptografia wielu zmiennych

Nicolas Tadeusz Courtois
Uniwersytet Paryż 6 i Uniwersytet w Toulon.
courtois@minrank.org

IV Krajowa Konferencja Zastosowań Kryptografii,
Enigma 2000
Warszawa, 22-25 maja 2000.

Slajdy i dodatkowe materiały:
`http://www.minrank.org/~courtois/myresearch.html`

,,Wszyscy matematycy wiedzą, że przejście
z jednej do wielu zmiennych to nagły skok
któremu towarzyszą wielkie trudności"
Jean Dieudonné
wybitny francuski matematyk

---

1 Kryptografia klucza publicznego

Klasyczna kryptografia, nazywana obecnie **kryptografią symetryczną**, pozwala osiągnąć poufność danych **wyłącznie** przy założeniu uprzedniego istnienia jakiegoś pewnego kanału komunikacyjnego np. walizka dyplomatyczna albo spotkanie w parku bez świadków. Ten kanał jest niezbędny do ustalenia **tajnego klucza** na którym polega bezpieczeństwo dalszej komunikacji.

Kryptografia klucza publicznego to systemy pozwalające bezpiecznie komunikować **bez** uprzedniej wymiany klucza, nawet na linii **stale** podsłuchiwanej przez osoby trzecie. Wymaga ona tylko istnienia tzw. **kanału publicznego** który co prawda każdy może czytać, ale nikt nie może zmodyfikować lub zablokować. Na tym kanale możemy opublikować tzw. **klucz publiczny**, który pozwala zaszyfrować wiadomość, ale nie pozwala jej odszyfrować, do czego niezbędny jest odpowiedni **klucz tajny** który nigdy nie opuszcza właściciela. Ta asymetria jest źródłem terminu **kryptografia asymetryczna**.

1.1 Historia idei klucza publicznego

W ramach otwartych uniwersyteckich badań naukowych została ona wynaleziona w 1976 przez Diffie, Hellman i niezależnie przez Merkle. Najbardziej znany i stosowany kryptosystem to Rivest-Shamir-Adleman (RSA) opublikowany w 1977.

W zamkniętych kręgach specjalistów wojskowych i rządowych była ona jednak znana dużo wcześniej. Właściwym wynalazcą jest James Ellis, jeden z filarów brytyjskiego biura szyfrów CESG przy GCHQ w Cheltenham. Pierwszy (tajny) dokument na ten temat pochodzi ze stycznia 1970 [1]. Następnie w 1973 Clifford Cocks wymyśla wariant późniejszego RSA, a w 1974 Malcolm Williamson wynajduje wariant późniejszej metody wymiany klucza według Diffie-Hellman. Szczegóły opisuje Ellis w artykule z 1977 opublikowanym dopiero po jego śmierci [1], kiedy Clifford Cocks na nieoficjalnej sesji-niespodziance podczas 6-tej konferencji IMA w Cirencester 17-go grudnia 1997 po raz pierwszy ujawnia prawdę.

1.2 Historia kryptografii wielu zmiennych

Wiele wczesnych systemów **kombinatorycznych** oparte na zagadnieniu plecakowym [Merkle-Hellman 1978], teorii grafów i wiele innych zostało szeroko skompromitowanych. Z drugiej strony, istnieją równie stare, **algebraiczne** kryptosystemy wielu zmiennych używające równań liniowych wielu zmiennych nad ciałami skończonymi i zwykle opisywane w terminach kodów korekcyjnych. Począwszy od [McEliece 1978] i dla wielu innych, oparły się one dziesięcioleciom kryptoanalizy i pozwoliły na wyodrębnienie bardzo trudnych problemów zwanych SD i MinRank dla których wszystkie znane ataki sa wykładnicze.

Później pojawiły się algebraiczne kryptosystemy wielu zmiennych używające równań drugiego stopnia, najpierw w Japonii [Matsumoto, Imai], potem w USA [Fell, Diffie, Cade], a następnie w Izraelu [Shamir] i we Francji [Patarin, Goubin, Courtois]. Najnowsze badania pokazują że niektóre z tych systemów, np. HFE, opierają się również na trudnych problemach algebraicznych np. problemy MQ, IP i MinRank.

Siła współczesnej kryptografii wielu zmiennych polega na tym że istniejące kryptosystemy oparte na trudnych algebraicznie problemach można przekształcić w kombinatoryczne wersje, jeszcze trudniejsze do złamania.

1.3 Zagadnienia kryptografii klucza publicznego

Kryptografia klucza publicznego zawiera następujące ściśle ze sobą powiązane zagadnienia:

[1] **Ustalanie klucza**: Dwie osoby które rozmawiają przez publiczny kanał który jest na podsłuchu, ale nie może być przerwany, starają się ustalić wspólny, tajny **klucz sesyjny**.

Jeżeli nie ma pewności co do integralności kanału, nie jest to niestety możliwe (w teorii) i wymaga uprzedniej identyfikacji [3]. W przeciwnym razie ktoś może włączyć się pomiędzy (man-in-the-middle attack) i skutecznie udawać każdą ze stron. W praktyce jednak identyfikacja może odbyć się bez kryptografii, przez wspólny kontekst nieznany innym (znajomość drugiej osoby) lub za pomocą danych biometrycznych (rozpoznanie głosu).

[2] **Szyfrowanie z kluczem publicznym**: Jak opisano poprzednio, pozwala na szyfrowanie za pomocą opublikowanego **klucza publicznego** którego nie można odczytać bez posiadania odpowiedniego **klucza tajnego**. Cel [2] można tez uzyskać to za pomocą [1] i vice versa.

[3] **Identyfikacja, kontrola dostępu**: Dowieść że to ja, a nie kto inny chce wejść do pomieszczenia, systemu, lub że to ja jestem na drugim końcu linii (protokoły w czasie rzeczywistym).

[4] **Uwierzytelnienie, autentyzacja, autentykacja, certyfikacja**: Pozwala zagwarantować ze to ja nie kto inny jestem autorem danego dokumentu, lub wiadomości (certyfikuje pochodzenie). Różnica między identyfikacją i uwierzytelnieniem jest taka że w pierwszym przypadku nie ma wiadomości.

[5] **Podpis cyfrowy**: Tak jak powyżej gwarantuje pochodzenie. W dodatku podpis powinien przekonać w sposób niezbity każdą trzecią osobę (np w sądzie) o swojej autentyczności.

Parametry dobrać tak, aby podpis był być ważny przez b. długi okres czasu np. 20 lat (licząc się z postępem kryptoanalizy).

Kto potrafi więcej, potrafi i mniej, podpis cyfrowy zapewnia też funkcje [3] i [4]. Ale o ile [3] a nawet [4] można osiągnąć w klasycznej kryptografii **symetrycznej** np. z tajnym kluczem DES, podpisu cyfrowego [5] nie można !

[6] **Uwierzytelnienie z protokołami/dowodami wiedzy zerowej (Zero-knowledge)**: Pozwala na osiągnięcie celu [3] w sposób nieskończenie bardziej bezpieczny nią te opisane w [3], [4] i [5]. Załóżmy że Peggy udowadnia swoją tożsamość za pomocą protokołu wiedzy zerowej, osobie która ją sprawdza Victor. Daje to matematycznie dowiedzioną pewność że Victor może dokonać sprawdzenia **dowolną** ilość razy, zawsze być w pełni przekonanym że to Peggy, ale **nigdy** ne zdoła on uzyskać **najmniejszej informacji** która pozwoliłaby mu podanie się za Peggy.

W połaczęniu z kryptograficzną funkcją haszującą która zastępuje pytania (queries), [6] pozwala osiągnąć też [5].

[7] **Różne zagadnienia rozproszone**: Np. głosowanie elektroniczne.

2 Bezpieczeǹstwo kryptosystemów

Bezpieczeǹstwo to precyzyjnie sformułowane wymaganie co do trudności jaką będzie miał dany Przeciwnik aby skutecznie przeprowadzić atak na dany kryptosystem. Przeciwnik jest zdefiniowany formalnie jako probabilistyczna maszyna Turinga.

Bezpieczeǹstwo definiuje się w ogólności w zależności od trzech danych.

1. Jakie są **zasoby** Przeciwnika (resources) ? Dotyczy to mocy obliczeniowej, dostępnej pamięci, i innych parametrów dostępnej technologii (np. posiadanie komputera kwantowego).

2. Jaki **rodzaj bezpieczeǹstwa** (security notion) chcemy osiągnąć ? Jaki jest **cel Przeciwnika** (goal), tzw. **groźba** ?

   Na przykład odzyskać cały klucz lub tylko odszyfrować niektóre wiadomości. Inny przykład: móc podać się za kogoś innego.

3. Jaki jest **model ataku** (attack model), tzn jaki **rodzaj dostępu lub interakcji** istnieje między Przeciwnikiem i konkretnym kryptosystemem który chce on załamać.

   Na przykład atak wybranym tekstem jawnym.

3 Bezpieczeǹstwo kryptosystemów klucza publicznego

3.1 Dla szyfrów asymetrycznych

Podstawowe rodzaje bezpieczeǹstwa to:

- Trudność znalezienia klucza tajnego: Celem przeciwnika jest odzyskania klucza tajnego mając do dyspozycji klucz publiczny.

- Jednokierunkowość (one-wayness, OW).

  To niemożność obliczenia m dla danego szyfrogramu $E(m)$.

- Bezpieczeǹstwo semantyczne (semantic security, polynomial security, IND).

  Sformalizowane przez Goldwasser i Micali. Oznacza niemożliwość rozróżnienia pomiędzy dwoma zaszyfrowanymi tekstami jawnymi $E(m_1)$ i $E(m_2)$. Odpowiada to bezpieczeǹstwu doskonałemu, w kontekście przeciwników o ograniczonej wielomianowo mocy obliczeniowej.

- Niedeformowalność (Non-malleability, NM).

  Sformalizowane przez Dolev, Dwork i Naor. Oznacza niemożliwość wyprodukowania dla danego szyfrogramu y, innego ważnego szyfrogramu y', w taki sposób aby odpowiednie teksty jawne x, x' były ze sobą związane w jakiś sprawdzalny sposób. Na przykład $x = x' + 1$ albo różniące się na jednej tylko pozycji.

- Świadomość tekstu jawnego (plaintext-awareness PA).

  Sformalizowane przez Bellare i Rogaway i uogólnione z pomocą Pointcheval i Desai w [12]. Zdefiniowane na razie tylko przy założeniu tzw. random oracle (RO) i w tym przypadku jest ściśle silniejsze od powyższych. Oznacza z grubsza niemożliwość wyprodukowania ważnego szyfrogramu y, bez uprzedniej znajomości odpowiedniego tekstu jawnego x.

Podstawowe rodzaje ataków to następujące zawierające się w sobie ataki:

- Atak wybranym tekstem jawnym (chosen plaintext attack, CPA), najsłabszy możliwy.
- Atak ze sprawdzaniem tekstu jawnego (plaintext checking attack, PCA). Pozwala sprawdzić czy dana para (wiadomość, szyfrogram) jest poprawna. Dla deterministycznej funkcji z zapadką jest to równoważne CPA.
- Atak wybranym tekstem zaszyfrowanym ((lunchtime) chosen ciphertext attack, CCA1)
- Atak adaptacyjny (wybranym tekstem zaszyfrowanym) (adaptive (chosen ciphertext) attack, CCA2)

W 1998 Bellare, Desai, Pointcheval et Rogaway pokazali że IND-CCA2 jest równoważne NM-CCA2 [12]. Jest to bardzo silne pojęcie bezpieczeǹstwa nazywane "bezpieczeǹstwem z wybranym tekstem zaszyfrowanym"(chosen-ciphertext security). W 1999-2001 Fujisaki, Okamoto i Pointcheval pokazują jak osiągnąć tego typu bezpieczeǹstwo z dowolnej deterministycznej funkcji z zapadką bezpiecznej tylko w najsłabszym sensie OW-CPA. Najlepsza tego typu konstrukcja nazywa się REACT [14]. Ciekawostką jest fake ze REACT pozwala także osiągnąć PA, pojęcie jeszcze silniejsze [12]. REACT pozwala budować systemy udowodnione bezpieczne w chyba najsilniejszym znanym sensie, względem jednego, dobrze zdefiniowanego trudnego problemu matematycznego.
Przykłady: problem wyciągania pierwiastków modulo pewnej liczby złożonej N zwany problemem RSA, albo problem zwany HFE.

3.2 Dla podpisów cyfrowych

Podstawowe rodzaje bezpieczeństwa to następujące zawierające się w sobie pojęcia:

- Totalne złamanie (total break)
- Uniwersalne fałszerstwo (universal forgery), być w stanie podpisać każdą wiadomość.
- Selektywne fałszerstwo (selective forgery), być w stanie podpisać niektóre wiadomości.
- Egzystencjalne fałszerstwo (existential forgery), być w stanie wyprodukować ważną parę (wiadomość, podpis).

Podstawowe rodzaje ataków to następujące zawierające się w sobie ataki:

- Atak bez wiadomości (No-message attack), próbuje złamać sam klucz publiczny.
- Atak ze znaną wiadomością ((plain) known-message attack).
- Atak ogólny wybraną wiadomością (generic chosen-message attack). Lista wiadomości do podpisu jest wybrana zanim poznamy klucz publiczny.
- Atak zorientowany wybraną wiadomością (oriented chosen-message attack). Lista wiadomości do podpisu jest wybrana po tym jak dany jest klucz publiczny.
- Atak adaptacyjny wybraną wiadomością (adaptively chosen-message attack). Dostęp w czasie rzeczywistym do czarnej skrzynki (oracle) która podpisuje wybrane wiadomości.

Istnieją systemy podpisu cyfrowego które mają udowodnione bezpieczeństwo, w tym najsilniejszym sensie np. wersja systemu ElGamal (Stern, Pointcheval 2000 [15]) albo McEliece (Courtois Finiasz Sendrier 2001 [48]).

4 Istniejące systemy klucza publicznego

4.1 Klasyfikacja

1. **Funkcje z zapadką (deterministyczne)**
   (a) Jednej zmiennej:
      i. nad $\mathbb{Z}_N$, duże N - RSA, Rabin
      ii. nad bardziej 'skomplikowanymi grupami' - Krzywe Eliptyczne
      iii. nad małymi ciałami skoǹczonymi - Matsumoto-Imai (C^*), D^*, [C] (HM), HFE, Cade
   (b) Wielu zmiennych liniowe:
      i. nad $\mathbb{Z}$ - zagadnienia plecakowe Merkle-Hellman, redukcja krat (lattice).
      ii. nad małymi ciałami skoǹczonymi - McEliece, Niederreiter, GPT, zagadnienia plecakowe Chor-Rivest.
   (c) Wielu zmiennych kwadratowe:
      i. nad $\mathbb{Z}$ - zagadnienia plecakowe (knapsack), redukcja krat (lattice).
      ii. nad $\mathbb{Z}_N$, duże N - Ong-Schnorr-Shamir, birational permutations [Shamir].
      iii. nad małymi ciałami skoǹczonymi - C^*, D^*, [C] HM, HFE, UOV, HFEv-, TPM , TTM, Flash, Quartz.
2. **Algorytmy uwierzytelnienia Zero-knowledge**
   (a) Jednej zmiennej
      i. nad $\mathbb{Z}_N$, duże N - Fiat-Shamir, GQ, LC2 [!]
   (b) Wielu zmiennych:
      i. nad $\mathbb{Z}$, PPP
      ii. nad małymi ciałami skoǹczonymi - PKP, SD, CLE, Chen, MinRank, IP, GI
3. **Podpisy cyfrowe** - mogą zostać zbudowane używając wszystkich kryptosystemów z (1) i (2). Bezpieczniejsze - (2).
4. **Systemy klucza publicznego probabilistyczne** - modyfikacje kryptosystemów z (1) i wiele innych. Dużo silniejsze niż (1).

4.2 Najważniejsze zagadnienie z punktu widzenia zastosowań w przemyśle

To podpis cyfrowy

Problemy: szybkość, długofalowe bezpieczeǹstwo, długość, łatwość implementacji w karcie czipowej, etc...

4.3 Alternatywy dla RSA:

RSA opiera się na jednym równaniu modularnym z jedną zmienną. Naturalnym uogólnieniem tego podejścia jest rozważanie systemów wielu równań z wieloma zmiennymi (...)
Uważa się że HFE jednym z najsilniejszych kryptosystemów tego typu (...)
ADI SHAMIR

4.3.1 Dwie poważne alternatywy:

EC Bardziej skomplikowane grupy:
Krzywe Eliptyczne [Koblitz, Miller, Crypto'85], [19, 18].

HFE Bardziej skomplikowany wielomian:
HFE. [Patarin, Eurocrypt'96], [33].

4.3.2 Bezpieczeństwo - teoria

RSA opiera swoje bezpieczeństwo na faktoryzacji (nie ma dokładnego dowodu) i na problemie zwanym RSA.

EC Krzywe Eliptyczne opierają się **jedynie** na tym że uogólniają problemy RSA i DL na czymś 'bardzo skomplikowanym' i na co nie ma żadnych znanych ataków (na razie...).

HFE Bezpieczeństwo HFE jest dwupoziomowe:

(a) Algebra: Trudne problemy **MQ, IP, HFE, MinRank**.

(b) Modyfikacje schematu: Niszczą strukturę algebraiczną. Operacje $+$, $-$,v, f. (patrz: Secret public key schemes [5]).

4.3.3 Bezpieczeństwo - praktyka

RSA **512 bitów** - złamany [08.1999], 8 000 MIPS-years.

EC **97 bitów** - złamany, ok. 16 000 MIPS-years [09.1999], zawsze atak z $\sqrt{2^n}$, www.certicom.com

HFE (a) Basic HFE **80 bitów** (tzw. Challenge 1) - Najlepszy atak 2^{62} (Courtois) [35], wymaga niestety 390 Gbajtów dysku.

(b) Istnieją wersje HFE **80 bitów** dla których najlepszy znany atak to ślepe przeszukiwanie (HFE–, HFEv, HFEv-).

5 Podstawy matematyczne kryptografii wielu zmiennych

5.1 Ciała skończone i ich rozszerzenia

Ciało (nieformalnie) - struktura danych (algebraiczna) w których wykonywalne są wszystkie działania $+, -, \times, /$ z wyjątkiem dzielenia przez zero, i rządzące się 'normalnymi' prawami algebry. Przykłady: $\mathbb{Q}$, $\mathbb{R}, \mathbb{C}$.

K - ciało skończone mające q elementów, $K = GF(q)$ (Galois Field). Przykłady:

1. $K = GF(2) = \mathbb{Z}_2 = \{0, 1, + \bmod 2, \times \bmod 2\}$.
2. $K = GF(p) = \mathbb{Z}_p$ - liczby modulo p, liczba pierwsza.
3. $K = GF(q)$, $q = p^\alpha$.

Kilka szczegółowych uwag:
Angielskie *field* odpowiada francuskiemu *corps commutatif* i polskiemu słowu *ciało*. To znaczy że we Francji ciała nie są koniecznie przemienne, co nie robi żadnej różnicy co do ciał skończonych: (Twierdzenie [Wedderburn]: każde ciało skończone jest przemienne).
Jeśli K jest ciałem skończonym mającym q elementów to $K - \{0\}$ jest grupą cykliczną którą oznaczamy K^*. Wynika z tego że każdy element $X \in K$ spełnia następujące równanie zwane równaniem charakterystycznym ciała K: $X^q = X$.
Wszystkie ciała skończone są postaci $GF(p^\alpha)$, w dodatku
$\exists$ jedno z dokładnością co do izomorfizmu ciało skończone $GF(p^\alpha)$. Konstrukcja:

- $GF(p)[X]$ = wielomiany zmiennej X ze współczynnikami modulo p.
- Niech P będzie wielomianem nierozkładalnym stopnia α nad $GF(p)$.
- $GF(p^n) \stackrel{def}{=} GF(p)[X]/P(X)$, to zbiór wielomianów z $GF(p)[X]$ modulo $P(X)$.
- $GF(p^n)$ jest rozszerzeniem $GF(p)$, jak i również przestrzenią wektorową wymiaru α nad $GF(p)$: każdy element $x \in GF(q^n)$ można zakodować jako α współczynników wielomianu $x \in K[X]$ wziętego modulo $P(X)$.

5.2 Konstrukcja ciała $K^n = GF(q^n)$

Od teraz $K = GF(q)$, dla uproszczenia można zakładać że q jest liczbą pierwszą (a niekoniecznie).
Zwykle $q = 2$, $K = \{0, 1\}$
Konstrukcja ciała $GF(q^n)$:

- $GF(q)[X]$ = wielomiany zmiennej X ze współczynnikami w GF(q).
- Niech P będzie wielomianem nierozkładalnym stopnia n nad $GF(q)$.
- $GF(q^n) \stackrel{def}{=} GF(q)[X]/P(X)$, to zbiór wielomianów z $GF(q)[X]$ modulo $P(X)$.

5.2.1 Reprezentacje jednej/wielu-zmiennych

Każdy element $x \in GF(q^n)$ można zakodować jako n współczynników wielomianu $x \in K[X]$ wziętego modulo $P(X)$.

Jeżeli $x = \quad x_1 + x_2 \cdot X + \ldots + x_n \cdot X^{n-1}$,
piszemy w skrócie $x = (x_1, \ldots, x_n)$.

Nb. notacja ta odpowiada użyciu bazy $1, X, X^2, X^{n-1}$. Warto wiedzieć że dla przyspieszenia obliczeń w ciałach skończonych o charakterystyce 2 używa tzw. optymalnych baz normalnych [17].

$GF(q^n)$ - przestrzeń wektorowa, wymiar n nad K.
Utożsamiamy i piszemy $K^n = GF(q^n)$.

5.3 Reprezentacje jedno/wielo-zmienne funkcji

Każdą funkcję $f : K^n \to K^n$ można napisać jako:

- wielomian jednej zmiennej $x \in GF(q^n) \equiv K^n$
- n wielomianów n zmiennych $f_1(x_1, \ldots, x_n), \quad \ldots, \quad f_n(x_1, \ldots, x_n)$.

5.4 Stopień w reprezentacji jednej/wielu zmiennych

- Funkcja o postaci $b = f(a) = a^{q^s}$ daje w reprezentacji wielu zmiennych: $b_i = f_i(a_1, \ldots, a_n)$, gdzie f_i są K-liniowe.
- Jeżeli $f(a) = a^{q^s+q^t}$, funkcje f_i są (co najwyżej) drugiego stopnia nad K.
- Funkcja jest postaci $f(a) = \sum_i \lambda_i a^{q^{s_i}+q^{t_i}} + \sum_i \delta_i a^{q^{s_i}}$,
  z $\lambda_i, \delta_i \in GF(q^n)$, wtedy i tylko wtedy gdy
  wszystkie f_i są (co najwyżej) drugiego stopnia nad K.

5.5 Przykład

$K = GF(2) = \{0, 1\}, \ n = 3$
$P(X) = X^3 + X^2 + 1$ jest nierozkładalny modulo 2.
$K^n = GF(2^3) = K[X]/X^3 + X^2 + 1$

$b = f(a) = a + a^3 + a^5 =$
$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 +$
$(a_2X^2 + a_1X + a_0)^5 \ mod \ X^3 + X^2 + 1 \ = \ (...) \ =$
$(a_2 + a_2a_1 + a_2a_0 + a_1)X^2 + (a_2a_1 + a_1a_0 + a_2)X + (a_0 + a_2 + a_1a_0 + a_2a_0)$

$$\begin{cases} b_2 &= a_2 + a_2a_1 + a_2a_0 + a_1 \\ b_1 &= a_2a_1 + a_1a_0 + a_2 \\ b_0 &= a_0 + a_2 + a_1a_0 + a_2a_0 \end{cases}$$

6 Hidden Field Equation (HFE)

6.1 Ukryty wielomian

$$f(a) = \sum_{q^s+q^t \le d} \gamma_{st}\ a^{q^s+q^t} + \sum_{q^s \le d} \delta_s a^{q^s}$$

- Napisać jako n funkcji drugiego stopnia n zmiennych: $b_1(a_1, \ldots, a_n), \quad \ldots, \quad b_n(a_1, \ldots, a_n)$.
- Zakamuflować strukturę algebraiczną funkcji $f : a \mapsto b$ za pomocą dwóch podstawień linowych (lub afinicznych) S i T, na przykład:

$$S : \begin{cases} a_1 &= x_2 - x_3 + 1 \\ &\vdots \end{cases} \qquad T : \begin{cases} y_1 &= b_1 + b_2 - 1 \\ &\vdots \end{cases}$$

Niech $g : x \mapsto y$, będzie otrzymanym wynikiem podstawień, złożeniem $g = T \circ f \circ S$.

6.2 Używanie 'basic' HFE

6.2.1 Klucz publiczny:

n równań drugiego stopnia
$g : \{ \quad y_i = g_i(x_1, \ldots, x_n) \quad \}_{i=1..n}$

6.2.2 Klucz prywatny:

Znajomość T, S i f.
f jest funkcją jednej zmiennej stopnia $\le d$.
Fakt: można obliczyć f^{-1} (metody jednej zmiennej).
$\exists$ wiele algorytmów, zaczynając od [Berlekamp 1967].
Są one dość wolne.
Przykład: n=128, d=25, 0.17s na PIII-500.

6.2.3 Obliczanie g^{-1} z posiadaniem klucza prywatnego

$$x \xleftarrow{S^{-1}} a \xleftarrow{f^{-1}} b \xleftarrow{T^{-1}} y$$

6.3 O trudności obliczenia g^{-1} bez klucza prywatnego

Otrzymaliśmy funkcję $g : x \mapsto y$, będąca złożeniem $g = T \circ f \circ S$.
Dla osoby nie znającej klucza prywatnego:
g 'wygląda' jak dowolny (losowy) układ równań drugiego stopnia.

6.4 Zalecane implementacje HFE

Patrz http://hfe.minrank.org

- $K = GF(2)$ (operacje na bitach)
- $n \geq 127$, najlepiej liczba pierwsza
- $d \geq 25$, najlepiej w postaci $2^k + 1$

6.5 Kryptologiczne wyzwania

2*500 $

Challenge 1

$K = GF(2)$, $n = 80$, $d = 96$.
Najlepszy znany atak (Courtois) [35] - 2^{62}.

Challenge 2

$K = GF(16)$, $n = 36$, $d = 4352$, tylko 32 na 36 równań są podane. Brak znanych ataków (poza XL).

7 Funkcje jednokierunkowe a kryptografia asymetryczna

Wiele kryptosystemów klucza publicznego została złamanych bez odzyskania klucza publicznego. Atakować bezpośrednio funkcję g systemu HFE, ale jak ?

Podstawowa różnica:

- **Kryptografia symetryczna** - związek x i $g(x)$ nie powinien wyrażać się prosto za pomocą jednego lub kilku równań [parafraza słów Shannon'a], zachowanie nieprzewidywalne, model Random Oracle.
- **Kryptografia asymetryczna** - Klucz publiczny - $g(x)$ wyraża się prosto za pomocą jednego lub kilku równań.

7.1 Heurystyki

Jakiego rodzaju równania mogą, a jakie nie mogą stanowić solidnej deterministycznej funkcji z zapadką ?

Heurystyki (nieformalne):

- **Łatwość użycia** - Równania typu **'explicite'** $g(x) = ...$
- **Trudność złamania** - A priori rozwiązanie $(x_1, \ldots, x_n)$ opisane jest za pomocą równań typu **'implicite'** które są trudne do rozwiązania, np. równania drugiego stopnia (NP-zupełny problem MQ).
- **Idea niezmiennika** - charakter **implicite** x_i powinien zostać zachowany przy różnego rodzaju transformacjach na równaniach.
- **Każdy atak** deterministyczny począwszy z danych 'skomplikowanych' równań **'implicite'** które definiują x_i, 'upraszcza' je (ewentualnie etapami), i na końcu daje równania typu **'explicite'** i 'proste': $x_i = 0$ ou 1.

7.2 Próba algebraicznego zdefiniowania co to jest funkcja jednokierunkowa

Definicja [bardzo nieformalna]: Funkcja jednokierunkowa względem danej miary złożoności:

To funkcja, która **nie pozwala** otrzymać za pomocą podstawowych operacji (algebraicznych)' i ze 'znaczącym' prawdopodobieństwem żadnych równań typu **explicite**, ni żadnych równań **implicite**, prostszych względem danej miary złożoności.

7.2.1 'Podstawowe operacje algebraiczne'

Załóżmy że równania do rozwiązania to

$$\begin{cases} l_1 &= 0 \\ & \vdots \\ l_n &= 0 \end{cases}$$

Definicja [nieformalna]: Podstawowe operacje algebraiczne:
To **wszystkie** operacje które pozwalają otrzymać inne równania 'małego' stopnia (lub 'małego' rozmiaru) równe 0 z prawdopodobieństwem 1, jako kombinacje wielomianowe **explicite** danych równań l_i.

Przykład: $x_1 l_5 + x_2 l_1 + l_3 l_5 = 0$, stopień 4.

Groźba: Co jeśli okaże się że podstawiając l_i, dostajemy np.

$$x_1 l_5 + x_2 l_1 + l_3 l_5 \ = \ x_1,$$

$$0 \ = \ x_1.$$

Chcemy żeby te trywialne kombinacje równań pozostały trywialne.

7.2.2 Pojęcie równań trywialnych

Definicja [nieformalna]: Równanie trywialne (względem danej miary złożoności):

- To suma iloczynów małego stopnia l_j i x_i
- każdy zawierający co najmniej jeden l_j, i taka że
- po podstawieniu $l_k = \sum x_i x_j ...$, jej złożoność względem danej miary złożoności (n.p. stopień w reprezentacji wielu zmiennych) nie spada.

7.2.3 Zastosowanie równań nie-trywialnych

Podstawić $l_j \equiv 0$, co daje **nowe** równania o małej złożoności (np. małego stopnia) dla szukanych x_i.

Iterować atak.

7.3 Automatyczny kryptoanalityk

Najlepsze znane ataki na HFE [35], działają w ten właśnie sposób (z licznymi ulepszeniami).

8 Ciała skoǹczone vs. duże liczby pierwsze

8.1 Własności algebraiczne

Ciała skoǹczone cieszą się dość dużą popularnością w kryptografii. Zarówno HFE, kryptosystemy krzywych eliptycznych, czy wiele algorytmów uwierzytelnienia jak [65, **?**, **?**] czy MinRank opierają się na ciałach skoǹczonych.

Dlaczego tak jest ? (argumentacja heurystyczna).

A dlaczego duże liczby pierwsze ?

Jednym z powodów dla jakich kryptografia używa dużych liczb pierwszych jest następujący:

Rozważmy dowolny system równań do rozwiązania modulo N, duże N.

Jeżeli $p|N$, istnieje homomorfizm (oczywisty) $\mathbb{Z}_N \to \mathbb{Z}_p$ który pozwala otrzymać równania modulo p (prostsze) z mniejszymi rozmiarami danych.

Zatem, jeżeli mierzymy złożoność równań preze liczbę bitów ich niewiadomych, otrzymujemy nowe **nie-trywialne** równania które są prostsze względem danej miary złożoności. To przeczy (odpowiednio interpretowanej) definicji funkcji jednokierunkowej z 7.2.

Jeżeli N jest produktem wyłącznie b. dużych liczb pierwszych, otrzymanie nawet trochę prostszych równań wymaga faktoryzacji N.

Bezpieczeństwo opiera się na fakcie że nie ma homomorfizmu $\mathbb{Z}/N\mathbb{Z} \to A$, z małym pierścieniem A (który byłby łatwy do znalezienia).

Dla ciał skoǹczonych istnieje analogiczna własność:

Twierdzenie: Nie istnieje homomorfizm $\mathbb{F}_q \to K$ dla żadnego mniejszego ciała K.

9 Problem MQ

9.1 Ogólny problem MQ (Multivariate Quadratic):

Rozwiązać układ m równań drugiego stopnia z n zmiennymi nad pierścieniem K.

$$f: \begin{cases} b_k = \sum_{i=0}^{n} \sum_{j=i}^{n} \lambda_{ijk}\ a_i a_j \\ \text{gdzie } k = 1..m, \quad a_0 = 1 \end{cases}$$

9.2 MQ gdy $n = m = 1$

- $\mathbf{K} = \mathbb{Z}_N$ - MQ jest równoważny faktoryzacji N [Rabin], więc najprawdopodobniej nie jest NP-zupełny (le théorème de Brassard [10, 5]).
- $\mathbf{K} = GF(q)$ - MQ można rozwiązać dla każdego stałego d (metody jednej zmiennej), [Berlekamp 1967]. Podstawa HFE.

9.3 MQ gdy $n << m$ albo $m << n$

- Jeśli $m << n$ - 2^{m-n} rozwiązań.

  Ustalić $n - m$ zmiennych i szukać rozwiązania dla pozostałych m równań z m niewiadomymi.
- Jeśli $m \geq \frac{n^2}{2}$ MQ jest łatwy do rozwiązania:

9.3.1 Linearyzacja:

- Nowe zmienne $y_{ij} = x_i x_j$.
- m równań **liniowych** z m zmiennymi (!).

[Kipnis, Shamir, Crypto 99] - Re-linearyzacja.

Twierdzenie [Courtois] Algorytm re-linearyzacji jest gorszy od algorytmu XL [Courtois,Patarin,Shamir,Klimov], Eurocrypt'2000,[30].

9.3.2 Uproszczony opis algorytmu XL

d-parametr algorytmu, $d \in \mathbb{N}, d \geq 2$.

- Pomnożyć wszystkie możliwe równania przez wszystkie możliwe jednomiany stopnia $d - 2$.
- Eliminacja liniowa aż do uzyskania równania jednej zmiennej, np. x_1.
- Rozwiązać równanie jednej zmiennej (stopnia d).

Gröbner bases = ulepszone XL.

9.3.3 Odkrycie [Eurocrypt'2000]

MQ jest słaby dla $m > n$ (ale wykładniczy dla $m \approx n$).

9.4 Trudne instancje MQ, $n \approx m$

Fakt: Na małym ciele skończonym najlepszy znany algorytm nie jest szybszy niż ślepe przeszukiwanie (brute force attack). Patrz [Courtois,Patarin,Shamir,Klimov], Eurocrypt'2000,[30].

Dla HFE $m = n$.

9.5 MQ jest NP-zupełny

MQ jest NP-zupełny dla dowolnego ciała K [Garey,Johnson, Patarin, Goubin], [11, 6, 5].

9.5.1 Dowód dla $GF(2)$:

3-SAT $\mapsto$ równania stopnia 3.

$$\begin{cases} 0 = x \vee y \vee z \\ 1 = \neg t \\ \vdots \end{cases} \quad \begin{cases} 0 = xyz + xy + yz + xz + x + y + z \\ 1 = 1 + t \\ \vdots \end{cases}$$

przekształcić w równania kwadratowe dodając:

- nowe zmienne $y_{ij} = x_i x_j$.
- nowe równania **trywialne** $0 = y_{ij} - x_i x_j$.

10 MQ a funkcje jednokierunkowe

Najbardziej naturalny kandydat na funkcję jednokierunkową - operacje nieliniowe na bitach.

Stopień $3, 4$, - nierealny, pb. z zapisem f (wiele Megabajtów..).

10.0.2 MQ a rodzaje funkcji jednokierunkowych

Ćwiczenie 1:

Czy MQ, w zależności of m, n, spełnia następujące kryteria (odpowiedź uzasadnić):

- OWF (One-Way function) - funkcja jednokierunkowa - **Tak !**.
- CR (Collision Resistant), bezkolizyjna funkcja haszująca - **Nie !**.

Ćwiczenie 2:

Zbudować system podpisu cyfrowego używający wyłącznie HFE i losowej funkcji MQ (bez funkcji haszującej) który podpisuje wiadomości ustalonej długości i dla którego nie jest możliwe wygenerowanie dwóch wiadomości mających takie same podpisy.

Ćwiczenie 3:

Dlaczego w kryptografii klucza publicznego (ogólnie) klucze są zwykle dużo dłuższe niż w kryptografii symetrycznej ?

Odpowiedzi przysłać na: courtois@minrank.org

11 Problem IP

Dane: f,g.

Szukane: odzyskać podstawienia S i T

11.1 Algorytmy dla IP

Najlepszy znany algorytm: $q^{n/2}$ [Courtois, Eurocrypt'98].

11.2 Konsekwencje dla HFE

Jeżeli f jest znane, $\exists$ atak w czasie $q^{n/2}$.

Ale nie jest, i nie jest znana żadna metoda odzyskania f.

Spostrzeżenie: [Shamir] f jest w pewnym sensie 'znane w 99%' ponieważ $d << q^n - 1$

12 Atak Shamir-Kipnis na HFE

12.1 Analiza problemu HFE [Shamir, Crypto'99]

Uproszczenie: załóżmy że funkcje f,g systemu HFE są kwadratowe bez części linowej.

12.1.1 Reprezentacja niestandardowa

Shamir wyraża funkcje f i g w szczególnej reprezentacji:

Reprezentacja niestandardowa: Macierz symetryczna G, $n \times n$ i ze współczynnikami w K^n, taka że:

$$g(x) \;=\; \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} G_{ij}\; x^{q^i+q^j}$$

Shamir Pokazuje jak scharakteryzować fakt że stopień ukrytego wielomianu jest ograniczony przez d,

12.1.2 Właściwości f i g w reprezentacji niestandardowej

Rząd rank(G)= a priori n.

Za to rank(F)=r (nb. $r = \log d$) (ponieważ stopień f jest $\leq d$.)

Artykuł z Crypto'99 sprowadza problem kryptoanalizy HFE do problemu macierzowego MinRank(r) gdzie $r = \log d$.

12.2 Od HFE do MinRank

Z definicji HFE:

$$g \quad = \quad T \circ f \circ S$$

Dane f,g. Szukamy S i T które mogłyby spełniać:

$$T^{-1} \circ g \quad \stackrel{?}{=} \quad f \circ S$$

Lemat 1 [Shamir]:
Reprezentacja niestandardowa funkcji $f \circ S$ jest w postaci $G' = WGW^t$. G' ma ten sam rząd r co G.

Lemat 2 [Shamir]:
$T^{-1} \circ g = \sum_{k=0}^{n-1} t_k G^{*k}$ gdzie $G^{*k} \stackrel{def}{=}$ są reprezentacjami **publicznymi** funkcji g^{q^k}.

12.3 Problem do rozwiązania

Znaleźć takie $t_k \in K^n$ że

$$Rank(\sum_{k=0}^{n-1} t_k G^{*k}) = r$$

Shamir i Kipnis sprowadzają złamanie HFE do problemu macierzowego MinRank.

13 Problem MinRank

MinRank(r)**:** Znaleźć (szczególną) kombinację liniową danych m macierzy $n \times n$, której rząd spada do r.

13.1 Fiasco ataku Shamir-Kipnis

Okazało się że:

- MinRank jest NP-zupełny i b. trudny w praktyce
- zawiera on w sobie wiele słynnych trudnych problemów
- to chyba najtrudniejszy znany problem w kryptografii !

Patrz `http://www.minrank.org/minrank/`.

13.2 Warianty ataku Shamir-Kipnis

13.2.1 Oryginalna

Proponowana kontynuacja ataku (metoda re-linearyzacji) okazała się niewypałem. Ulepszona relinearyzacja $\rightsquigarrow$ algorytm XL [Courtois,Patarin,Shamir,Klimov], Eurocrypt'2000, [30].

Wtedy atak Shamir-Kipnis dla 'HFE Challenge 1' wymaga 2^{152} obliczeǹ,... $>> 2^{80}$ (ślepe przeszukiwanie).

13.2.2 Ulepszona

Ulepszona wersja ataku Shamir-Kipnis wyraża MinRank za pomocą pod-macierzy [35].

Daje 2^{97} dla 'HFE Challenge 1'.

13.3 Złożoność obliczeniowa ataku Shamir-Kipnis-Courtois:

Około $n^{3 \log d}$.

14 Czy MinRank dowodzi solidności HFE ?

Niezupełnie !

Złamać $\neq$ odzyskać klucz prywatny

14.1 Historia kryptoanalizy różnych kryptosystemów wielu zmiennych:

1. W **niektórych** przypadkach odzyskano S i T:
   - D^* [Courtois 97].
   - 'Balanced Oil and Vinegar' [Kipnis, Shamir Crypto'98]
2. **Wiele** zostało złamanych bez odzyskania klucza prywatnego:
   - 2 propozycje Shamir'a. [Stern, Vaudenay, Coppersmith]
   - 2 schematy Matsumoto-Imai: C^*; $[C] = HM$ [Patarin]
   - D^*, Little Dragon, S-boxes, C^{*-} [Patarin, Goubin, Courtois]

15 Ataki bezpośrednie [Patarin, Courtois]

Bardzo techniczne, używają fakt istnienia równań wiążących ze sobą bity wejścia i wyjścia o bardzo złożonej strukturze.

15.1 Ataki równaniowe [Patarin, Courtois]

6 ataków, każdy następny uogólnia poprzedni, dziesiątki typów równań:

15.1.1 Właściwości

- Tylko najprostsze wyniki mają podłoże teoretyczne.
- Niespodzianki (dziedzina bardzo eksperymentalna).
- Równania pojawiają sie począwszy od pewnego progu (n.p. 840 Mb).

15.1.2 Przykład dla HFE Challenge 1

Fakt eksperymentalny: Dla HFE stopnia $d \leq 128$ istnieje $\geq n$ równań typu: $\Sigma\alpha_i + \Sigma\beta_i x_i + \Sigma\gamma_i y_i + \Sigma\delta_{ij} x_i x_j + \Sigma\varepsilon_{ijk} x_i x_j y_k + \Sigma\zeta_{ijk} y_i y_j x_k + \Sigma\theta_{ijk} x_i x_j y_k + \Sigma\kappa_{ijkl} x_i x_j x_k y_l + \Sigma\lambda_{ijkl} x_i x_j y_k y_l = 0$.

15.2 W praktyce - Challenge 1:

Powyższe równania mają 17 milionów współczynników. Metoda klasyczna (redukcja systemów liniowych) aby je odzyskać wymaga 33 Terabajtów pamięci RAM.

Atak ulepszony - czas 2^{62}, tylko 390 Go na dysku [35].

16 Operacje na kryptosystemach wielomianowych

16.1 Ogólne zasady - operacja '-'

1. Na przekór utartym opiniom że niewiele jest kandydatów na systemy klucza publicznego, kryptografia wielu zmiennych, nad małymi ciałami skoǹczonymi zawiera sporo ciekawych kandydatów opartych nad zdrowych zasadach.

2. Pb. Wiele z nich posiada także reprezentacje jednej zmiennej które są źródłem ataków:

   - Ataki na C^* - Patarin [24, 6]
   - Ataki na 'basic' HFE - Shamir-Kipnis [38].
   - Ataki na D^* - Courtois [**?**, 6].
   - Ataki na HM - Courtois [**?**, 6].

3. Jednak wystarczy drobna modyfikacja, na przykład odjąć pewną liczbę $r > 10$ równań w ich reprezentacji wielu zmiennych, aby otrzymać nowe kryptosystemy nazywane odpowiednio C^{*--}, HFE^{--}, D^{*--}, HM^{--} dla których żaden, nawet teoretyczny atak nie jest znany (!).

Wniosek: Definitywne odejście od reprezentacji jednej zmiennej do funkcji wielu zmiennych niszczy zupełnie (bogatą) strukturę algebraiczną funkcji szyfrującej i radykalnie zmniejsza liczbę możliwych ataków.

16.2 Inne operacje

cdn.

17 Bezpieczeǹstwo HFE

17.1 'Dowody' bezpieczeǹstwa ?

Wszystkie dowody bezpieczeǹstwa w dziedzinie kryptografii klucza publicznego opierają się na małej liczbie problemów matematycznych, np. problem rozkładu na czynniki pierwsze (faktoryzacja).

W większości przypadków nie ma dokładnego dowodu że rozwiązanie problemu jest w istocie konieczne do złamania systemu. Np. RSA - faktoryzacja.

17.2 Trudne problemy matematyczne w kryptografii wielu zmiennych

1. **IP**, Isomorphism of Polynomials, nie jest NP-zupełny, $\exists$ algorytm w czasie $q^{n/2}$ zamiast de q^{n^2} [Courtois, Eurocrypt 1998], [57], co jest ciągle exponencjalne.
2. **MQ**, Multivariate Quadratic, jest NP-zupełny, i wygląda na to że nad małym ciałem skoǹczonym, i jeżeli liczba równań $\approx$ liczbie niewiadomych, najlepszym znanym algorytmem jest nadal jeszcze ślepe przeszukiwanie. [Courtois, Shamir, Patarin, Klimov - Eurocrypt' 2000] - [30].
3. **MinRank**, jest NP-zupełny, to chyba najtrudniejszy znany problem kryptografii który zawiera w sobie wiele innych sławnych problemów.
4. **HFE**, Hidden Field Equation, odpowiada najprostszej wersji 'basic HFE'. Okazuje się sub-exponencjalny $e^{log^2 n}$.

17.3 5 argumentów 'dowodzących' bezpieczeǹstwa HFE

1. Asymptotyczne: jeżeli jeden z parametrów $d \to \infty$, HFE $\to MQ$.
2. Nierozróżnialność - HFE wygląda jak losowy problem MQ i nikt nie potrafi (przy dobrze dobranych parametrach) odróżnić HFE od MQ.
3. Ataki z odzyskaniem klucza - powiązane bezpośrednio z b. trudnym problem MinRank [Shamir, Crypto'99].
4. Ataki z odzyskaniem f - nawet gdyby wewnętrzny (ukryty) wielomian f był znany, trzeba jeszcze rozwiązać problem IP (nadal wykładniczy).
5. Nawet gdyby 'basic HFE' był złamany, istnieje wiele wersji $+$, $-$, f, v które udaremniają atak.

18 Podsumowanie o HFE

18.1 Stan wiedzy AD 2000, HFE vs. RSA

18.1.1 Teoria

Oba ataki [Shamir-Kipnis-Courtois] i [Patarin-Courtois], w najlepszej znanej wersji obu ataków opisanej przez Courtois w [35] dają asymptotycznie podobne wyniki:

$$\mathbf{e^{\log^2 n}}$$

W porównaniu dla RSA: $\mathbf{e^{\sqrt[3]{n}}}$

18.1.2 Praktyka

Znane ataki na 'basic HFE' stają się nierealne dla dobrze wybranych parametrów n i d.

Łatwo jest zmodyfikować podstawową wersję 'basic' HFE aby otrzymać kryptosystem nie mający **żadnej** znanej słabości, nawet teoretycznej:

HFE$^-$ [Patarin, Asiacrypt'98], HFEv: [Patarin, Eurocrypt'99].

18.1.3 Szybkość

HFE jest o wiele szybszy i praktyczniejszy od RSA (przy założonym poziomie bezpieczeństwa).

18.2 Kto za, kto przeciw...

"Jakikolwiek algorytm, który opiera swoje bezpieczeństwo na rozkładzie wielomianów na ciele skończonym, powinien być rozważany co najmniej ze sceptycyzmem, jeżeli nie z podejrzeniem."
[Bruce Schneier, Applied cryptography, p.318]

"...skąpość podstaw matematycznych w kryptografii klucza publicznego jest bardzo niepokojąca."
[p. 319]

Komu przeszkadzają monopole: **?SA**

HFE: prawdziwa alternatywa

19 Dodatek: Problem podpisu cyfrowego

f - funkcja z zapadką '(trapdoor function'), n bitów.
Metoda klasyczna z użyciem kryptograficznej funkcji haszującej H:

$$\boxed{\sigma = f^{-1}(\ H(m)\ )}$$

19.1 Existential Forgery:

Atak paradoksu dnia urodzin:

1. Wygenerować $2^{n/2}$ **wersji** wiadomości do podpisania $m_1, \ldots, m_{2^{n/2}}$, dodając spacje, przecinki, tekst itp.
2. Wygenerować listę $2^{n/2}$ wartości $f(\sigma_j)$, dla losowych σ_j.
3. Posortować obie listy, istnieją (i, j) takie że:
   $f(\sigma_j) = H(m_i)$

   Złamać podpis cyfrowy o długości 80 bitów $\rightsquigarrow$ ok. 2^{40} obliczeń.

19.2 Ominięcie ataku [Patarin]

Metoda ulepszona z użyciem dwóch funkcji haszujących H_1,H_2:

$$\boxed{\sigma = f^{-1}\,(\ \ H_1(m) + f^{-1}\,[H_2(m) + f^{-1}(H_1(m))]\ \ )}$$

Daje bezpieczne podpisy o długości 80 a nawet 64 bitów !

19.2.1 HFE vs. konkurencja

Porównanie długości typowych podpisów :

RSA	$\rightsquigarrow$	1024 bitów
DSA	$\rightsquigarrow$	320 bitów
Krzywe Eliptyczne	$\rightsquigarrow$	321 bitów
McEliece [48]	$\rightsquigarrow$	111 bitów
HFE + powyższa metoda	$\rightsquigarrow$	80 bitów

(najkrótsze znane)

19.3 Jakie podpisy są bezpieczne ?

Pytania pułapki: Który najlepszy ?
Zalecamy pluralizm i kumulowanie certyfikatów.

Scenariusz pro-aktywny pozwala stopniowo wycofywać stare i wprowadzać nowe. Na przykład w dniu kiedy RSA 768 zostanie złamany wygasłaby ważność podpisów RSA 1024.

Przykładowy certyfikat
RSA + EC + HFE = $1024 + 161 + 80$ bitów.

RSA jest na tyle wolny i podpisy są na tyle długie że koszt całej reszty jest do pominięcia.

Bibliografia

Ogólne opracowania, monografie i podręczniki - Kryptologia

[1] James Ellis: "The story of non-secret encryption"; Available at http://www.cesg.gov.uk/about/nsecret/

[2] Alfred J. Menezes, Paul C. van Oorshot, Scott A. Vanstone: *Handbook of Applied Cryptography*; CRC Press.

[3] Bruce Schneier: *Applied Cryptography*; Wiley and sons. Istniej polskie tłumaczenie.

[4] Douglas R. Stinson : *Cryptography, theory and practice*; CRC Press 1995.

[5] Jacques Patarin: *La Cryptographie Multivariable*; Mémoire d'habilitation à diriger des recherches de l'Université Paris 7, 1999.

[6] Jacques Patarin, Louis Goubin, Nicolas Courtois, + papers of Eli Biham, Aviad Kipnis, T. T. Moh, et al.: *Asymmetric Cryptography with Multivariate Polynomials over a Small Finite Field*; known as 'orange script', compilation of different papers with added materials. Available from J.Patarin@frlv.bull.fr.

[7] Claude Elmwood Shannon, Collected Papers, Sloane & Wyner eds, New York, IEEE Press, 1993.

Ogólne opracowania, monografie i podreęczniki - Matematyka Stosowana

[8] Rudolf Lidl, Harald Niederreiter: *Finite Fields*; Encyclopedia of Mathematics and its applications, Volume 20, Cambridge University Press.

Funkcje jednokierunkowe

[9] Michael Luby, *Pseudorandomness and Cryptographic Applications*; Princeton University Press, 1996.

Teoria złożoności obliczeniowej

[10] Gilles Brassard: Ą note on the complexity"; IEEE Tran. Inform. Theory, Vol. IT-25, 1979, pp. 232-233.

[11] Michael Garey, David Johnson: *Computers and Intractability, a guide to the theory of NP-completeness*, Freeman, p. 251.

Bezpieczeństwo systemów klucza publicznego, konwersje i dowody bezpieczeństwa

[12] Mihir Bellare, Anand Desai, David Pointcheval, and Philip Rogaway: *Relations among Notions of Security for Public-Key Encryption Schemes;* In Crypto '98, LNCS 1462, pages 26–45. Springer-Verlag, Berlin, 1998.

[13] E. Fujisaki and T. Okamoto: *Secure Integration of Asymmetric and Symmetric Encryption Schemes;* In Crypto '99, LNCS 1666, pages 537-554. Springer-Verlag, Berlin, 1999.

[14] T. Okamoto and D. Pointcheval: *REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform;* In the Cryptographers' Track of the RSA Security Conference '2001, LNCS2020, Springer-Verlag, Berlin, 2001.

[15] D. Pointcheval, J. Stern: *Security arguments for Digital signatures and Blind Signatures;* Journal of Cryptology, Vol.13(3), Summer 2000, pp.361-396.

[16] Victor Shoup: *OAEP Reconsidered;*Preprint, November 2000. Available from http://eprint.iacr.org/.

Krzywe Eliptyczne

[17] Jerzy Gawinecki, Janusz Szmidt: *Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii*; Wojskowa Akademia Techniczna, Bel Studio, Warszawa.

[18] V.S. Miller: *Use of elliptic curves in cryptography*; Crypto'85, LNCS 218.

[19] Neal Koblitz: *Elliptic curve cryptosystems*; Mathematics of Computation, 48 (1987), pp. 203-209.

[20] Michael Rosing: *Elliptic Curve Cryptography*; Manning Publications, USA. The book can be ordered at it's web site, which contains also it's preface, index, the chapter 5, etc. with all the C-programs from the book.

Systemy wielu zmiennych Matsumoto, Imai i ich sukcesorzy

[21] Hans Dobbertin, *Almost Perfect Nonlinear Power Functions on* $GF(2^n)$; paper available from the author.

[22] Neal Koblitz: *Algebraic aspects of cryptography*; Springer-Verlag, ACM3, 1998, Chapter 4 *Hidden Monomial Cryptosystems*, pp. 80-102. Istniej poskie tłumaczenie.

[23] Tsutomu Matsumoto, Hideki Imai: *Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption*; EUROCRYPT'88, Springer-Verlag 1998, pp. 419-453.

[24] Jacques Patarin: *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*; Crypto'95, Springer-Verlag, pp. 248-261.

[25] Jacques Patarin, Nicolas Courtois, Louis Goubin: *C*-+ and HM - Variations around two schemes of T. Matsumoto and H. Imai*; Asiacrypt'98, Springer-Verlag.

[26] Jacques Patarin, Louis Goubin, Nicolas Courtois: *Flash, a fast multivariate signature algorithm*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 Avril 2001, LNCS2020, Springer-Verlag.

Rozwiązywanie równań jednej zmiennej na ciele skończonym

[27] J. von zur Gathen and Victor Shoup, *Computing Fröbenius maps and factoring polynomials*; Proceedings of the 24th Annual ACM Symposium in Theory of Computation, ACM Press, 1992.

[28] Biblioteka NTL, patrz www.shoup.net

Rozwiązywanie równań wielu zmiennych na ciele skończonym

[29] Don Coppersmith: *Finding a small root of a univariate modular equation*; Proceedings of Eurocrypt'96, Springer-Verlag, pp.155-165.

[30] Nicolas Courtois, Adi Shamir, Jacques Patarin, Alexander Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*, In Advances in Cryptology, Eurocrypt'2000, LNCS 1807, Springer-Verlag, pp. 392-407.

[31] Jean-Charles Faugère: *A new efficient algorithm for computing Gröbner bases (F_4)*.Journal of Pure and Applied Algebra 139 (1999) pp. 61-88. See www.elsevier.com/locate/jpaa

[32] Peter L. Montgomery: A Block Lanczos Algorithm for Finding Dependencies over GF(2); Eurocrypt'95, LNCS, Springer-Verlag.

Problem HFE i zastosowania

[33] Jacques Patarin: *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms*; Eurocrypt'96, Springer Verlag, pp. 33-48.

[34] Jacques Patarin, Louis Goubin, Nicolas Courtois: Quartz, **1**28-*bit long digital signatures*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 Avril 2001, LNCS2020, Springer-Verlag.

[35] Nicolas Courtois: *The security of Hidden Field Equations (HFE)*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 Avril 2001, LNCS2020, Springer-Verlag.

[36] Nicolas Courtois: *On multivariate signature-only public key cryptosystems;* To appear in 2001.

[37] Nicolas Courtois: HFE security, the HFE cryptosystem web page. `http://hfe.minrank.org`

[38] Adi Shamir, Aviad Kipnis: *Cryptanalysis of the HFE Public Key Cryptosystem*; In Advances in Cryptology, Proceedings of Crypto'99, Springer-Verlag, LNCS. It can be found at `http://www.nminrank.org/~courtois/hfesubreg.ps`

Inne kryptosystemy wielu zmiennych

[39] Aviad Kipnis, Adi Shamir: *Cryptanalysis of Oil and Vinegar Signature Scheme*; Crypto 98, Springer-Verlag.

[40] Adi Shamir: *Efficient signature schemes based on birational permutations*; Crypto 93, Springer-Verlag, pp1-12.

[41] Aviad Kipnis, Jacques.Patarin, Louis Goubin: Louis Goubin, Kipnis Aviad, Jacques Patarin: *Unbalanced Oil and Vinegar Signature Schemes*; Eurocrypt 1999, Springer-Verlag.

[42] Don Coppersmith, Jacques Stern, Serge Vaudenay: *Attacks on the birational permutation signature schemes*; Crypto 93, Springer-Verlag, pp. 435-443.

[43] Don Coppersmith, Jacques Stern, Serge Vaudenay, *The Security of the Birational Permutation Signature Schemes*, in Journal of Cryptology, 10(3), pp. 207-221, 1997.

Kryptografia klucza publicznego z systemami trójkątnymi: T,TPM,TTM

[44] Louis Goubin, Nicolas Courtois *Cryptanalysis of the TTM Cryptosystem*; Advances of Cryptology, Asiacrypt'2000, 3-9 December 2000, Kyoto, Japan, Springer-Verlag.

[45] T.T. Moh, *A public key system with signature and master key functions*, Communications in Algebra, 27(5), pp. 2207-2222, 1999. Available at http://www.usdsi.com/public.ps

[46] T.T. Moh, *A fast public key system with signature and master key functions*, in Proceedings of CrypTEC'99, International Workshop on Cryptographic Techniques and E-commerce, Hong-Kong City University Press, pages 63-69, July 1999. Available at http://www.usdsi.com/cryptec.ps

[47] *The US Data Security Public-Key Contest*, available at http://www.usdsi.com/contests.html

Liniowe kryptosystemy wielu zmiennych

[48] Nicolas Courtois, Matthieu Finiasz and Nicolas Sendrier: *How to achieve a McEliece-based Digital Signature Scheme*; Preprint available at http://www.minrank.org/mceliece/

[49] R.J. McEliece: *A public key cryptosystem based on algebraic coding theory*; DSN Progress Report42-44, Jet Propulsion Laboratory, 1978, pp. 114-116.

[50] Hans Niederreiter: *Knapsack-type cryptosystems and algebraic coding theory*; In Probl. Contr. and Information Theory, 1986.

Problem MinRank i trudne problemy teorii kodów

[51] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg: *On the inherent intractability of certain coding problems*; IEE Trans. Inf. Th., It-24(3), pp. 384-386, May 1978.

[52] Anne Canteaut, Florent Chabaud: *A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to BCH Codes of length 511;*

[53] http://www.minrank.org, a non-profit web site dedicated to MinRank and Multivariate Cryptography in general.

[54] Jeffrey O. Shallit, Gudmund S. Frandsen, Jonathan F. Buss: *The Computational Complexity of Some Problems of Linear Algebra problems*, BRICS series report, Aaarhus, Denmark, RS-96-33, available on the net http://www.brics.dk/RS/96/33/.

[55] Jacques Stern, Florent Chabaud: *The cryptographic security of the syndrome decoding problem for rank distance codes*. In Advances in Cryptology, Asiacrypt'96, LNCS 1163, pp. 368-381, Springer-Verlag.

Problemy IP, MP i Tensor Rank

[56] Don Coppersmith, Shmuel Winograd, *Matrix multiplication via arithmetic progressions*, J. Symbolic Computation (1990), **9**, pp. 251-280.

[57] Nicolas Courtois, Louis Goubin, Jacques Patarin: *Improved Algorithms for Isomorphism of Polynomials*; Eurocrypt 1998, Springer-Verlag.

[58] patrz [33].

[59] Volker Strassen: *Gaussian elimination is not optimal*; Numerishe Mathematik 13, 1969, pp. 354-356.

Schematy wiedzy zerowej

[60] Kefei Chen: *A new identification algorithm*. Cryptography Policy and algorithms conference, vol. 1029, LNCS, Springer-Verlag, 1996.

[61] Nicolas Courtois: *The power of MinRank and practical Zero-knowledge*. Paper in preparation.

[62] N. Courtois: *The Minrank problem*. MinRank, a new Zero-knowledge scheme based on the NP-complete problem. Presented at the rump session of Crypto 2000, available at http://www.minrank.org/minrank/.

[63] Amos Fiat, Adi. Shamir: *How to prove yourself: Practical solutions to identification and signature problems*. In Advances in Cryptology, Crypto '86, pp. 186-194, Springer-Verlag, 1987.

[64] Adi Shamir: *An efficient Identification Scheme Based on Permuted Kernels*, In Advances in Cryptology, Proceedings of Crypto'89, LNCS 435, pp.606-609, Springer-Verlag.

[65] Jacques Stern: *A new identification scheme based on syndrome decoding*; In Advances in Cryptology, Proceedings of Crypto'93, LNCS 773, pp.13-21, Springer-Verlag.