Primeless Cryptography

Sonia Mihaela Bogos

School of Computer and Communication Sciences

Responsible
Prof. Serge Vaudenay
EPFL/LASEC

Coordinator
Ioana Boureanu
EPFL/LASEC

Outline

- **Motivation**
- Background
- A first attempt
- New Proposal
- Conclusion

Motivation (1)

The goal of this report is to analyse and construct cryptographic primitives that use primeless cryptography.

What is **primeless cryptography**?
The universe of cryptography where prime numbers are not generated. In our case, random numbers are used.

Motivation (2)

The purpose is to reduce the asymptotic complexity. For example, RSA has a complexity of:

- Setup: $O(l^4)$
- Encryption: $O(l^3)$
- Decryption: $O(l^3)$

when we generate two different prime numbers, p and q, of size l.

Outline

- Motivation
- **Background**
- A first attempt
- New Proposal
- Conclusion

Characters

Definition

Let G be an Abelian group. A **character** χ is a function $\chi : G \to \mathbb{C}\backslash\{0\}$ such that

$$\chi(a+b) = \chi(a) \cdot \chi(b),\ \forall a, b \in G.$$

- group structure over the set of all characters on G.
- we use characters of order 2 and 4.
- denote by ε the trivial character where $\varepsilon(x) = 1,\ \forall x \in G$.

Characters of order 2

- $p \in \mathbb{Z}$ prime.
- two characters in Z_p^*, solutions of $\chi^2 = \varepsilon$: Legendre symbol, $(\frac{\cdot}{p})$, and ε.
- Jacobi - extension of the Legendre symbol.
- a list of four characters, solutions of $\chi^2 = \varepsilon$, in $\mathbb{Z}_n^*$: ε, $(\frac{\cdot}{n})$, $(\frac{\cdot}{p})$ and $(\frac{\cdot}{q})$, for $n = p \cdot q$ with p and q two different odd primes.

Gaussian Integers

- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$.
- for $\alpha = a + bi$, $N(\alpha) = \alpha \cdot \bar{\alpha} = a^2 + b^2$.

Proposition

Value α is a prime in $\mathbb{Z}[i]$, iff α satisfies one of the following:

- $\alpha = 1 + i$ *or* $\alpha = 1 - i$.
- α *is prime in* $\mathbb{Z}$ *and* $\alpha \equiv 3 \pmod 4$.
- $\alpha \cdot \bar{\alpha}$ *is a prime in* $\mathbb{Z}$ *and* $\alpha \cdot \bar{\alpha} \equiv 1 \pmod 4$.

Quartic Residue Symbol (1)

Definition

Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $(1+i) \nmid \beta$. Values β and α are relatively prime.

$\chi_\beta : \mathbb{Z}[i] \to \{\pm 1, \pm i\}$:

- $\chi_\beta = (\alpha^{\frac{N(\beta)-1}{4}}) \bmod \beta$, for β prime.
- $\chi_\beta = \prod_i \chi_{\beta_i}(\alpha)$, for $\beta = \prod_i \beta_i$, where β_i is prime.

Quartic Residue Symbol (2)

Definition

A nonunit $\alpha \in \mathbb{Z}[i]$ is primary if $\alpha \equiv 1 \pmod{(1+i)^3}$.

Proposition

Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $(1+i) \nmid \beta$, $\gcd(\beta, \alpha) = 1$ and $\gcd(\beta, \alpha') = 1$.

- *(Multiplicativity) $\chi_\beta(\alpha\alpha') = \chi_\beta(\alpha) \cdot \chi_\beta(\alpha')$.*
- *(Modularity) If $\alpha \equiv \alpha' \pmod{\beta}$, $\chi_\beta(\alpha) = \chi_\beta(\alpha')$.*
- *(Quartic Reciprocity Law) If α, β are primary,*
$$\chi_\beta(\alpha) = \chi_\alpha(\beta) \cdot (-1)^{\frac{N(\alpha)-1}{4} \cdot \frac{N(\beta)-1}{4}}.$$
- *(Complementary Laws) If $\beta = a + bi$ is primary,*
$$\chi_\beta(i) = i^{\frac{N(\beta)-1}{2}}, \ \chi_\beta(1+i) = i^{\frac{a-b-b^2-1}{4}}.$$

Algorithm to compute the quartic residue symbol [5]

$t \leftarrow 0$

While $(N(\alpha) > 1)$ **do**

- $\alpha \leftarrow \alpha \bmod \beta$ (Modularity)
- find α' primary such that $\alpha = i^j \cdot (1+i)^k \cdot \alpha'$
- set $\alpha \leftarrow \alpha'$ and adjust t (Multiplicativity)
- swap α and β and adjust t (Reciprocity Law)

If $(N(\alpha) = 1)$ return i^t

Outline

- Motivation
- Background
- **A first attempt**
- New Proposal
- Conclusion

Scheme 1 [1]

Key generation
Input: Security parameter s.
Output: Public key: (n, p); Private key: γ.

1. Select a big $\gamma \in \mathbb{Z}[i]$, *i.e.* $\gamma = a' + b'i$, where $a', b' \in \mathbb{Z}$ and the size of a', b' depends on the security parameter s .
2. Compute $n = \gamma\bar{\gamma}$ $(n \in \mathbb{Z})$.
3. Pick a $p \in \mathbb{Z}$ such that $\chi_\gamma(p) = i$.

Scheme 1 [1]

Encryption
Input: a bit b.
Output: the encryption c, $c \in \mathbb{Z}_n$.
Public key: (n, p).

1. Pick an $a \in \mathbb{Z}$ such that **if** $b = 0$ **then** $a \equiv 1 \pmod 4$ **else** $a \equiv 3 \pmod 4$.
2. $c \equiv p^a \pmod n$.

Decryption
Input: the encryption c, $c \in \mathbb{Z}_n$.
Output: a bit b.
Secret key: γ.

1. Compute the quartic residue symbol $\chi_\gamma(c)$.
2. **if** $\chi_\gamma(c) = i$ **then** $b = 0$ **else** $b = 1$.

Weakness of Scheme 1

- an adversary $\mathcal{A}$ does not need to know γ, but only an *equivalent* key γ' to γ.
- equivalent key: a gaussian factor $\gamma' \in \mathbb{Z}[i]$ of n with $\chi_{\gamma'}(p) = \pm i$.
- for a prime $f \equiv 1 \pmod 4$, $f = \gamma' \cdot \bar{\gamma'}$, with probability of $\frac{1}{2}$, $\chi_{\gamma'}(p) = \pm i$.
- $Prob_{n \in \mathbb{Z}, 2 \not| n}[f_1 \equiv 1 \pmod 4, f_2 \equiv 1 \pmod 4, f_1 \neq f_2\ ] = \frac{1}{2^2 \cdot f_1 \cdot f_2}$.

Breaking Scheme 1

Input: the encrypted bit c, $c \in \mathbb{Z}_n$.
Output: a bit b.
Public key: (n, p).

1. Find two small prime factors of n, $f_j \in \mathbb{Z}$, such that $f_j \equiv 1 \pmod 4$ for $1 \leq j \leq 2$.
2. Run *Cornacchia* and *Tonelli* algorithms to find $\gamma_j \in \mathbb{Z}[i]$ such that $\gamma_j \cdot \bar{\gamma}_j = f_j$.
3. **if** $\chi_{\gamma_j}(p) = i$ or $\chi_{\gamma_j}(p) = -i$ **then** decrypt the value c using the following rules:
   for $\chi_{\gamma_j}(p) = i$: **if** $\chi_{\gamma_j}(c) = i$ **then** $b = 0$ **else** $b = 1$
   for $\chi_{\gamma_j}(p) = -i$: **if** $\chi_{\gamma_j}(c) = -i$ **then** $b = 0$ **else** $b = 1$
   otherwise abort.

Outline

- Motivation
- Background
- A first attempt
- **New Proposal**
- Conclusion

Key Agreement

A	B
pick $\alpha = \prod_{i=1}^{i=k} \alpha_i$, where $\alpha_i \in \mathbb{Z}$	
pick $\beta = \prod_{i=1}^{i=k} \beta_i$, where $\beta_i \in \mathbb{Z}$	
compute $n = \alpha \cdot \beta$	
pick $x_1, x_2, \ldots x_t \in \mathbb{Z}_n^*$	
compute $y_i = (\frac{x_i}{\alpha}), 1 \leq i \leq t$	
$\xrightarrow{n, x_1, x_2, \ldots, x_t}$	
$\xrightarrow[y_1, y_2, \ldots, y_t]{}$	
	pick $b_1, b_2, \ldots, b_t \in \{0, 1\}$
	$z = x_1^{b_1} \cdots x_t^{b_t} \pmod{n}$
$\xleftarrow{z}$	
$K = (\frac{z}{\alpha})$	$K = y_1^{b_1} \cdots y_t^{b_t}$

Scheme 2

Choice of parameters

- $s \in \mathbb{Z}$ security parameter.
- α_i and β_i are of size l, for $1 \leq i \leq k$. (See next slides)
- value t assures the uniqueness of character $(\frac{\cdot}{\alpha})$ and $t \geq s$.
- $x_i's$ randomly chosen from $\mathbb{Z}_n^*$, $y_i's$ not all equal to 1.
- $b_i's$ not all equal to 0.

Complexity: $O(tk^2l^2)$.

Security (1)

Scheme 2 is secure if, after the run of it,

$$Adv_{\mathcal{A}}(s) = Prob[K = K'] - \frac{1}{2},$$

is negligible in terms of s, where K' is the bit guessed by $\mathcal{A}$ and K is the agreed key.

Computational Problems

Factorization. Given $n \in \mathbb{Z}$, find the prime factorization of n.

MOVA^d. Let $n \in \mathbb{Z}$, t be a positive integer and χ be a *hard character* of order d on $\mathbb{Z}_n^*$. Given t pairs of the form $(x_i, \chi(x_i))$, with $1 \leq i \leq t$, and given $x \in \mathbb{Z}_n^*$, compute $\chi(x)$.

Proposition

We have the following Karp reduction:

$$\textit{MOVA}^d \leq \textit{Factorization.}$$

Factorization for random numbers (1)

Prob. $n_i < n^x$	x for n_1	x for n_2
0.01	0.26974	0.00558
0.02	0.29341	0.0111
0.10	0.37851	0.05308
0.50	0.606	0.21172
0.90	0.90484	0.35899

Table: Distribution size for the largest two prime factors [2]

It is necessary to have the following inequality:

$$\frac{C_{ECM}(x \cdot l)}{F_2(x)} \geq C_{GNFS}(L')[3], \tag{1}$$

where l is the size of n, $0 < x < 1$ and $F_2(x) = \text{Prob}\,[n_2 < n^x]$.

Factorization for random numbers (2)

- take n to be a product of random numbers p_i:
$$n = p_1 p_2 \cdots p_k, \text{ with } |p_i| = l \text{ for all } 1 \leq i \leq k, \; |n| = k \cdot l.$$
- modification of (1):
$$min_{0<x<1}(C_{ECM}(x \cdot l), F_2(x)^{-k}) \geq C_{GNFS}(L').$$
- sufficient condition:
$$min[F_2(x)^{-k}, min_{x \leq u \leq y} \frac{C_{ECM}(ul)}{F_2(u)^k}, C_{ECM}(yl)] \geq C_{GNFS}(L'). \quad (2)$$

The inequality (2) can be simplified with:
$$C_{ECM}(x \cdot l) = F_2(x)^{-k} = C_{GNFS}(L').$$

Factorization for random numbers (3)

We obtain the following approximations for the size of n:

x	$F_2(x)$	l	k	$\lvert n\rvert = k \cdot l$
0.21172	0.5	1 276	45	57 420
0.01110	0.02	24 500	8	196 000
0.40681	0.96	660	750	495 000

Table: Required size of n for $L' = 1024$

Security (2)

Theorem

Let $\varphi : G \to \mathbb{Z}_d$ be a group homomorphism. If one can compute a f such that $Prob_{z \in G}(f(z) \neq \varphi(z)) \leq \frac{\xi}{12}$ with a constant $\xi < 1$, then one can compute φ in a number of calls to f bounded by a polynomial in $log(\#G)$ [4] .

Corollary (Security of Scheme 2)

Assuming that Factorization and $MOVA^d$ are hard, then no adversary $\mathcal{A}$ can guess the bit K from one run of the agreement but with a probability bounded by $\frac{1}{2}$.

Probabilistic Encryption

A	B
pick $\alpha = \prod_{i=1}^{i=k} \alpha_i$, where $\alpha_i \in \mathbb{Z}$	
pick $\beta = \prod_{i=1}^{i=k} \beta_i$, where $\beta_i \in \mathbb{Z}$	
compute $n = \alpha \cdot \beta$	
pick $x_1, x_2, \ldots x_t \in \mathbb{Z}_n^*$	
compute $y_i = (\frac{x_i}{\alpha}), 1 \leq i \leq t$	
$\xrightarrow{n, x_1, x_2, \ldots, x_t}$	
$\xrightarrow[y_1, y_2, \ldots, y_t]{}$	
	pick $b_1, b_2, \ldots, b_t \in \{0, 1\}$
	$K = y_1^{b_1} \cdots y_t^{b_t}$
$\xleftarrow{z = x_1^{b_1} \cdots x_t^{b_t} \pmod{n}}$	
$K = (\frac{z}{\alpha})$	

Scheme 3

Using characters of order 4

- improve the schemes by using characters of order 4: agree on a 2 bit value K (or encrypt two bits).
- compute n as $\prod_i \alpha_i \cdot \bar{\alpha}_i \cdot \beta_i \cdot \bar{\beta}_i$.
- $b_i's$ are randomly chosen from $\{0, 1, 2, 3\}$.
- correctness and the security proof are maintained.

Outline

- Motivation
- Background
- A first attempt
- New Proposal
- **Conclusion**

Conclusion

- two cryptographic primitives, that use primeless cryptography, were introduced.
- the need to have the factorization problem hard.
- smaller complexity for the setup of n.
- hard to work with too big numbers.

Future work:

- asymptotic analysis on values k and l.
- construction of a more efficient cryptographic primitive.


Ehsan Kazemi.
Primeless cryptography.
Semester project, EPFL, January 2011.


Donald E. Knuth and Luis Trabb Pardo.
Analysis of a simple factorization algorithm, 1976.


Jean Monnerat.
Short undeniable signatures:Design, Analysis, and Applications.
PhD thesis, École Polytechnique Fédérale de Lausanne, 2006.


Jean Monnerat and Serge Vaudenay.
Undeniable signatures based on characters: How to sign with one bit.
In *Public Key Cryptography*, pages 69–85, 2004.


Yvonne Anne Oswald.
Generic homomorphic undeniable signature scheme: Optimizations.
Semester project, EPFL, February 2005.