Benaloh's Dense Probabilistic Encryption Revisited

Laurent Fousse [1] Pascal Lafourcade[2] Mohamed Alnuaimi[3]

Université Grenoble 1, CNRS, Laboratoire Jean Kuntzmann, France
Laurent.Fousse@imag.fr

Université Grenoble 1, CNRS, Verimag, France
Pascal.Lafourcade@imag.fr

Global Communication & Software Systems, United Arab Emirates
mohamed.alnuaimi@nkc.ae

7th July 2011

Outline

Outline

Homomorphic Encryption

Definition (additively homomorphic)

$$E(m_1) \otimes E(m_2) \equiv E(m_1 \oplus m_2).$$

Applications

- Electronic voting
- Secure Fonction Evaluation
- Private Multi-Party Trust Computation
- Private Information Retrieval
- Private Searching
- ...

A partial history of homomorphic cryptosystems

Year	Name	Security hypothesis	Expansion
1982	Goldwasser-Micali	quadratic residuosity	$\log_2(n)$
1994	Benaloh	higher residuosity	> 2
1998	Naccache–Stern	higher residuosity	> 2
1998	Okamoto–Uchiyama	p-subgroup	3
1999	Paillier	composite residuosity	2
2001	Damgård—Jurik	composite residuosity	$\frac{d+1}{d}$

Outline

Outline

Original cryptosystem [Benaloh 1994]

Key Generation

- Choose a block size r and two large primes p and q such that:
  - r divides $(p-1)$.
  - r and $(p-1)/r$ are relatively prime.
  - r and $q-1$ are relatively prime.
  - $n = pq$, $\varphi(n) = (p-1)(q-1)$.
- Select $y \in (\mathbb{Z}_n)^* = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$ such that

$$y^{\varphi(n)/r} \neq 1 \bmod n$$

The public key is (y, r, n), and the private key is the two primes p and q.

Original cryptosystem

Encryption

For m in $\mathbb{Z}_r$:

$$E_r(m) = \{y^m u^r \bmod n : u \in (\mathbb{Z}_n)^*\}.$$

Homomorphic property

$$E_r(m_1) \times E_r(m_2) = E_r(m_1 + m_2).$$

Original cryptosystem

Decryption

$$\begin{aligned}(y^m u^r)^{(p-1)(q-1)/r} &= y^{m(p-1)(q-1)/r} u^{(p-1)(q-1)} \\ &= y^{m(p-1)(q-1)/r} \mod n.\end{aligned}$$

- Find $m \in \mathbb{Z}_r$ such that

$$(y^{-m}c)^{(p-1)(q-1)/r} = 1 \mod n.$$

- $\rightarrow$ discrete logarithm to perform in the subgroup of order r of $\mathbb{Z}_p^*$.
- usual index-calculus methods
- efficient algorithm when r is smooth.
- $p - 1$ should still have a large co-factor.

Outline

Example

Parameters

- Take $n = pq = 241 \times 179 = 43139$, $r = 15$, $y = 27$.
- r divides $p - 1 = 240$ ✓
- r and $(p-1)/r = 16$ are coprime. ✓
- r and $(q-1) = 2 \times 89$ are coprime. ✓
- y and n are coprime. ✓
- $y^{(p-1)(q-1)/r} = 40097 \neq 1 \mod n$. ✓

Example encryption

$$\begin{aligned} 24187 &= y^1 12^r \in E_r(1) \\ &= y^6 4^r \in E_r(6). \end{aligned}$$

Analysis of the example

Ambiguous encryption

$$\begin{aligned} y^5 &= 27^5 \\ &= 8 \\ &= 41^{15} \\ &= 41^r \mod n. \end{aligned}$$

$\rightarrow$ the cleartext space is now $\mathbb{Z}_5$ instead of $\mathbb{Z}_{15}$.

Outline

Receipt-free elections [Benaloh & Tuinstra, 1994]

Presidential Election

- Maximum number of ballots $< r = 15$.
- Vote for Nicolas $\in E_r(0)$
- Vote for Ségolène $\in E_r(1)$
- Actual result $R \in E_r(11)$ Ségolène is elected
- Computed result $R \in E_r(11) = E_r(1)$ Nicolas is elected

Private Trust Computation [Dovel *et al*, 2010]

Problem

- n users in a network
- each user trusts each other with a given trust value.
- Alice wants to know the global trust of the network in Bob.
- Maybe Alice will grant Bob access to (critical) ressources based on the computed value.

Private Trust Computation [Dovel *et al*, 2010]

Algorithm

- each user splits its trust value t into $n-1$ shares:

$$t = s_1 + s_2 + \ldots + s_{n-1} \bmod r.$$

- each user has a Benaloh keypair with the same parameter r.
- a share from each user is given to every other user, encrypted under the receiving user's key.
- the encrypted values are combined and decrypted locally, then combined globally.

Private Trust Computation [Dovel *et al*, 2010]

Problematic example

- the queried user Bob is a newcomer (trust $= 0$).
- Charlie uses a faulty y parameter with $r_{\text{true}} = r/3$.
- Charlie's recombined value should have been -1.
- Charlie's actual contribution will be $r_{\text{true}} - 1 \approx r/3$.

Analysis

- uses Benaloh's cryptosystem for a common r.
- Naccache–Stern's cryptosystem could be used instead.

Secure Card Dealing [Golle 2005]

Online Poker

- Need to collaboratively compare m_1 and m_2 from $E(m_1)$ and $E(m_2)$.
- Encryption performed using Benaloh's cryptosystem with $r = 53$.
- Not vulnerable to the flaw, with luck (53 is prime).

Outline

Corrected version

Key Generation (recall)

$$\begin{aligned} r &\mid (p-1) \\ \gcd(r,(p-1)/r) &= \gcd(r,q-1) = 1 \\ y^{\varphi(n)/r} &\neq 1 \bmod n \end{aligned}$$

Let g be a generator of the group $(\mathbb{Z}_p)^*$, and since y is coprime with n, let α be the value in $\mathbb{Z}_{p-1}$ such that $y = g^\alpha \bmod p$.

Main theorem

The following properties are equivalent:

a) decryption works unambiguously;

b) for all prime factors s of r, we have $y^{(\varphi(n)/s)} \neq 1 \bmod n$;

c) α and r are coprime.

Proof

$(c) \Rightarrow (a)$ (contrapositive)

- Assume

$$y^{m_1} u_1^r = y^{m_2} u_2^r \bmod n.$$

- Reducing mod p we get:

$$g^{\alpha(m_1 - m_2)} = (u_2/u_1)^r \bmod p$$

- There exists some β such that

$$\begin{aligned} g^{\alpha(m_1 - m_2)} &= g^{\beta r} \bmod p \\ \alpha(m_1 - m_2) &= \beta r \bmod p - 1 \\ \alpha(m_1 - m_2) &= 0 \bmod r. \end{aligned}$$

- Recall r and α are coprime

Proof

$(a) \Rightarrow (c)$ (contrapositive)

Assume α and r are not coprime and let $s = \gcd(\alpha, r)$, $r = sr'$, $\alpha = s\alpha'$.

$$
\begin{aligned}
y^{r'} &= g^{\alpha r'} \bmod p \\
&= (g^{\alpha'})^r \bmod p.
\end{aligned}
$$

- $y^{r'}$ is an r-th power mod p.
- $y^{r'}$ is an r-th power mod q.
- $y^{r'}$ is a valid encryption of 0 and of r'.

Proof

$(c) \Rightarrow (b)$ (contrapositive)

Assume that there exists some prime factor s of r such that

$$y^{(\varphi(n)/s)} = 1 \bmod n.$$

Reduce mod p:

$$\alpha \frac{\varphi(n)}{s} = 0 \bmod p - 1.$$

So

$$\alpha \frac{\varphi(n)}{s} = (p-1)\frac{\alpha(q-1)}{s}$$

is a multiple of $p - 1$ and s divides $\alpha(q-1)$. Since s does not divide $q - 1$, s divides α and α and r are not coprime.

Proof

$(b) \Rightarrow (c)$ (contrapositive)

Assume α and r are not coprime and denote by s some common prime factor. Then

$$\begin{aligned} y^{(\varphi(n)/s)} &= g^{\alpha\varphi(n)/s} \bmod p \\ &= g^{(\alpha/s)\varphi(n)} \bmod p = 1 \bmod p. \end{aligned}$$

And by construction of r, $s \nmid q-1$ so $y^{(\varphi(n)/s)} = 1 \bmod q$.

Outline

Outline

Probability of failure

Incorrect condition

$$y^{\varphi(n)/r} \neq 1 \bmod n \Leftrightarrow r \nmid \alpha.$$

Assume that r divides α: $\alpha = r\alpha'$. So

$$\begin{aligned} y^{\varphi(n)/r} &= g^{\alpha\varphi(n)/r} \bmod p \\ &= (g^{\alpha'})^{\varphi(n)} \bmod p \\ &= 1 \bmod p. \end{aligned}$$

Since r divides $p-1$, $y^{\varphi(n)/r} = 1 \bmod \ q$.

$\Leftarrow$

Conversely, if $y^{\varphi(n)/r} = 1 \bmod n$, then

$$\begin{aligned} g^{\alpha\varphi(n)/r} &= 1 \bmod p \\ \alpha\frac{\varphi(n)}{r} &= 0 \bmod p-1. \end{aligned}$$

Since r divides $p-1$ and is coprime with $\frac{\varphi(n)}{r}$ (by definition), we have $r \mid \alpha$. $\square$

Probability

Estimating the proportion ρ of faulty y's

- Incorrect condition on y: $r \nmid \alpha$.
- Proper condition on y: α and r are coprime.

$$\begin{aligned}
\rho &= 1 - \frac{\varphi(r)}{r-1} \\
&= 1 - \frac{r}{r-1}\frac{\varphi(r)}{r} \\
&= 1 - \frac{r}{r-1}\prod_i \frac{p_i - 1}{p_i} \\
&\approx 1 - \prod_i \frac{p_i - 1}{p_i}
\end{aligned}$$

Probability of error

Practical example

$$
\begin{aligned}
p &= 2 \times (3 \times 5 \times 7 \times 11 \times 13) \times p' + 1 \\
p' &= 446480450547539030954845987286241962287025168850895 5\\
&\ 503737449698209045631060122203397227538517117358538 1\\
&\ 3914691524677018107022404660225439441679953592 \\
q &= 1005585594745694782468051874865438459560952436544429 \\
&\ 5033292671082791323022555160232601405723625177570767 \\
&\ 5238936398645381403154121089599274598252367545682 79.
\end{aligned}
$$

$\#p = \#q = 512$ bits.

Probability of error

Practical example (cont'd)

$$
\begin{aligned}
\gcd(q-1, p-1) &= 2 \\
r &= (3 \times 5 \times 7 \times 11 \times 13) \times p' \\
\rho &= 1 - \frac{r}{r-1} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times \frac{10}{11} \times \frac{12}{13} \times \frac{p'-1}{p'} \\
\rho &> 61\%.
\end{aligned}
$$

Outline

Consequence of a faulty y

Cleartext space reduction

Let $u = \text{gcd}(\alpha, r)$. Then $r' = \frac{r}{u}$. Moreover if $r' \neq r$, this faulty value of y goes undetected by the initial condition as long as $u \neq r$.

Semantic security [Gjøsteen 2005]

DSMP

Let G be an abelian group with subgroups K, H such that $G = KH$ and $K \cap H = \{1\}$. The *Decisional Subgroup Membership Problem* is to decide whether a given $g \in G$ is in K or not.

Examples

- Goldwasser-Micali
- Naccache-Stern
- Okamoto-Uchiyama
- Paillier:

$$E_u(m) = (1+n)^m u^n \bmod n^2$$

  - ciphertext space is $G = (\mathbb{Z}_{n^2})^* \simeq (\mathbb{Z}_n)^* \times \mathbb{Z}_n$
  - H is the subgroup of order n (generated by $g = 1 + n$)
  - K is the set of the invertible n-th powers mod n^2.

Semantic security [Gjøsteen 2005]

Application to Benaloh's corrected scheme

- $G = (\mathbb{Z}_n)^*$
- H the cyclic subgroup of order r of G
- K the set of invertible r-th powers in G
- the public element y must generate H.

The semantic security of our corrected scheme is therefore equivalent to the DSMP for K, that is, being able to distinguish r-th powers modulo n.

Conclusion

- A slight change of description caused an error.
- Undetected for 16 years.
- Used verbatim in several protocol papers, even from last year.
- A huge probability of failure for suggested parameters $r = 3^k$.
- Quite possibly never implemented.