Tate Pairing with Strong Fault Resiliency

E. Ozturk, G. Gaubatz and B. Sunar
Worcester Polytechnic Institute

September 10, 2007

FDTC 2007
Vienna, Austria

Outline

- Identity Based Cryptography
- Tate Pairing
- A Fault Attack on Tate Pairing
- Robust Codes
- Our Scheme
- Analysis

Identity Based Cryptography

- Proposed by Shamir in 1984
- Idea: User's identity plays the role of public key
  - Reduce the amount of computations
  - Simplify key management
  - Simplify public-key infrastructure

Identity Based Cryptography

- First IBE Scheme with proof of security: Boneh-Franklin in 2001
  - Based on pairing algorithms
  - Triggered a rapid increase in the amount of research for pairing based cryptography

Pairing Based Cryptography

- Generally, Tate or Weil pairings are utilized
- Tate pairing seems to be of particular of interest, improved by Duursma and Lee
- Kwon improved the algorithm further, known as Kwon-BGOS Algorithm
- We are interested in Kwon-BGOS Algorithm for parameterisation purposes.

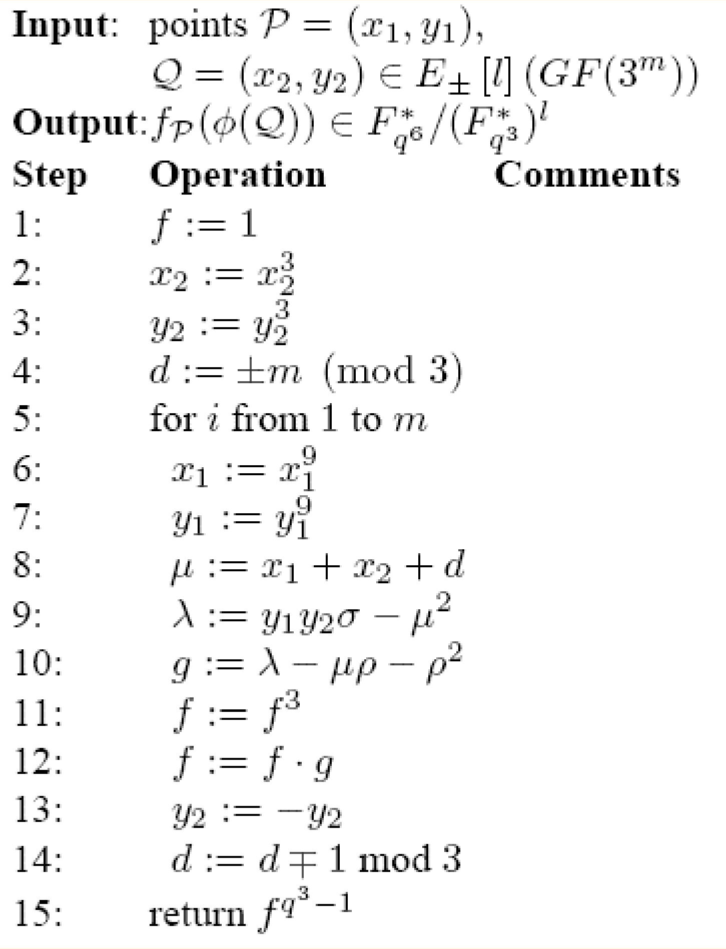
Tate Pairing

- A bilinear map between groups G_1 and G_T

$$e: G_1 x G_1 \square\, G_T$$

Tate Pairing

- **Kwon-BGOS Algorithm**
  - **Compute e(P,Q) from P=(x_1,y_1) and Q = (x_2,y_2)**



Input: points $\mathcal{P} = (x_1, y_1)$,
$\mathcal{Q} = (x_2, y_2) \in E_{\pm}[l](GF(3^m))$
Output: $f_{\mathcal{P}}(\phi(\mathcal{Q})) \in F^*_{q^6}/(F^*_{q^3})^l$

```
Step   Operation                          Comments
1:     $f := 1$
2:     $x_2 := x_2^3$
3:     $y_2 := y_2^3$
4:     $d := \pm m \pmod 3$
5:     for $i$ from 1 to $m$
6:       $x_1 := x_1^9$
7:       $y_1 := y_1^9$
8:       $\mu := x_1 + x_2 + d$
9:       $\lambda := y_1 y_2 \sigma - \mu^2$
10:      $g := \lambda - \mu\rho - \rho^2$
11:      $f := f^3$
12:      $f := f \cdot g$
13:      $y_2 := -y_2$
14:      $d := d \mp 1 \bmod 3$
15:    return $f^{q^3-1}$
```

A Fault Attack on Tate Pairing

- Security issues are emerging with the increase in the number of implementations.
- Page et. al. investigated a fault attack on Duursma-Lee Tate Pairing Algorithm

A Fault Attack on Tate Pairing

- Attack Objective: From the result R = e(P,Q), and with knowledge of Q, find P
  - Manipulate the loop counter
  - Extract one factor of the product, then recover P parameters.

Tate Pairing Security

- New types of attacks will be discovered
- To provide the highest level of assurance, the entire system needs to be protected with a robust error detection mechanism.

Robust Codes

- Karpovsky and Taubin introduced a novel family of non-linear systematic error detecting codes
- Let V be a linear p-ary (n,k) code with n<2k and rank(P) = r = n-k. Then

$$C_v = \{(x, w) \mid x \in GF(p^k), w = (Px)^2 \in GF(p^r)\}$$

- Code Cv is robust if it minimizes the maxima of undetectable errors.

Our Scheme

- Our objectives:
  - Protect the arithmetic operations used in a Tate pairing computation against a sufficiently large class of error patterns.
  - Keep the overhead in performance low.

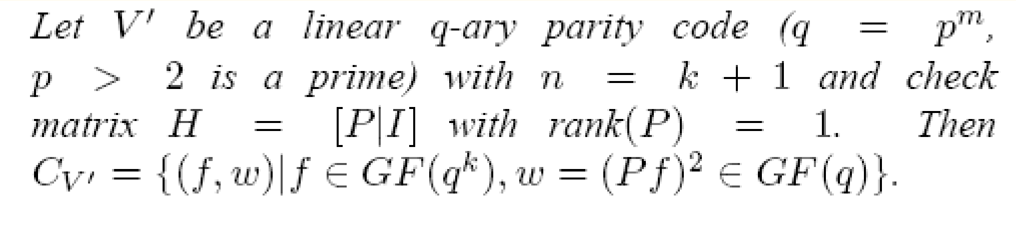
Our Scheme

- We built our error detection scheme on arithmetic operations on GF(3^{6m})
  - Less overhead than applying on GF(3^{m})
  - Easier implementation.
- Kwon-BGOS algorithm includes multiplication and cubing in GF(3^{6m}). We applied robust codes on both operations.

Our Scheme

- We derived a modified construction from robust codes of Karpovsky and Taubin, while maintaining robustness properties.
- The original robust codes were defined over GF(p^k), we extended the definition to robust codes defined over field extensions GF(q^{6m}), with $p=q^m$ and $k=6$

Our Scheme



Let V' *be a linear* q*-ary parity code* ($q = p^m$, $p > 2$ *is a prime) with* $n = k + 1$ *and check matrix* $H = [P|I]$ *with rank*$(P) = 1$. *Then* $C_{V'} = \{(f, w) | f \in GF(q^k), w = (Pf)^2 \in GF(q)\}$.

- **A non-zero error on a codeword will not be detected if and only if it satisfies the error masking equation:**

$$(Pf)^2 + e_w = (P(f + e_f))^2$$

- possible errors: 3^{7m}
  - undetected errors: 3^{5m}
  - reliably detected errors: $3^{6m} - 3^{5m}$
  - errors detected with prob. $1-3^{-m}$: $3^{7m} - 3^{6m}$
- Probability of detecting an error: $1-3^{-m}$

Robust GF(3^{6m}) Arithmetic

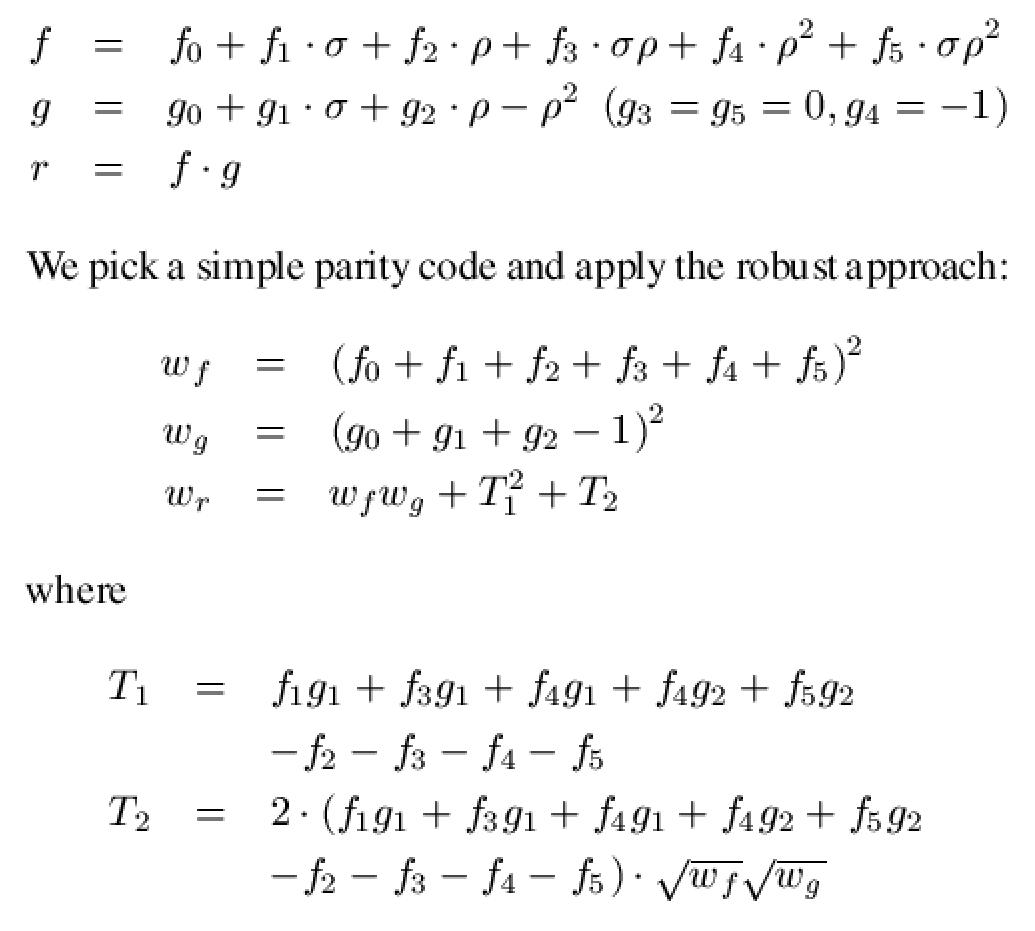
- The elements of GF(3^{6m}) are represented in the basis :

$$\{1,\sigma,\rho,\sigma\rho,\rho^2,\sigma\rho^2\}$$

- satisfying:

$$\sigma^2 \square 1 = \rho^3 - \rho \square 1 = 0 \in GF \square 3^{6m} \square$$

Multiplication in GF(3^{6m})



$$\begin{aligned} f &= f_0 + f_1 \cdot \sigma + f_2 \cdot \rho + f_3 \cdot \sigma\rho + f_4 \cdot \rho^2 + f_5 \cdot \sigma\rho^2 \\ g &= g_0 + g_1 \cdot \sigma + g_2 \cdot \rho - \rho^2 \;\; (g_3 = g_5 = 0, g_4 = -1) \\ r &= f \cdot g \end{aligned}$$

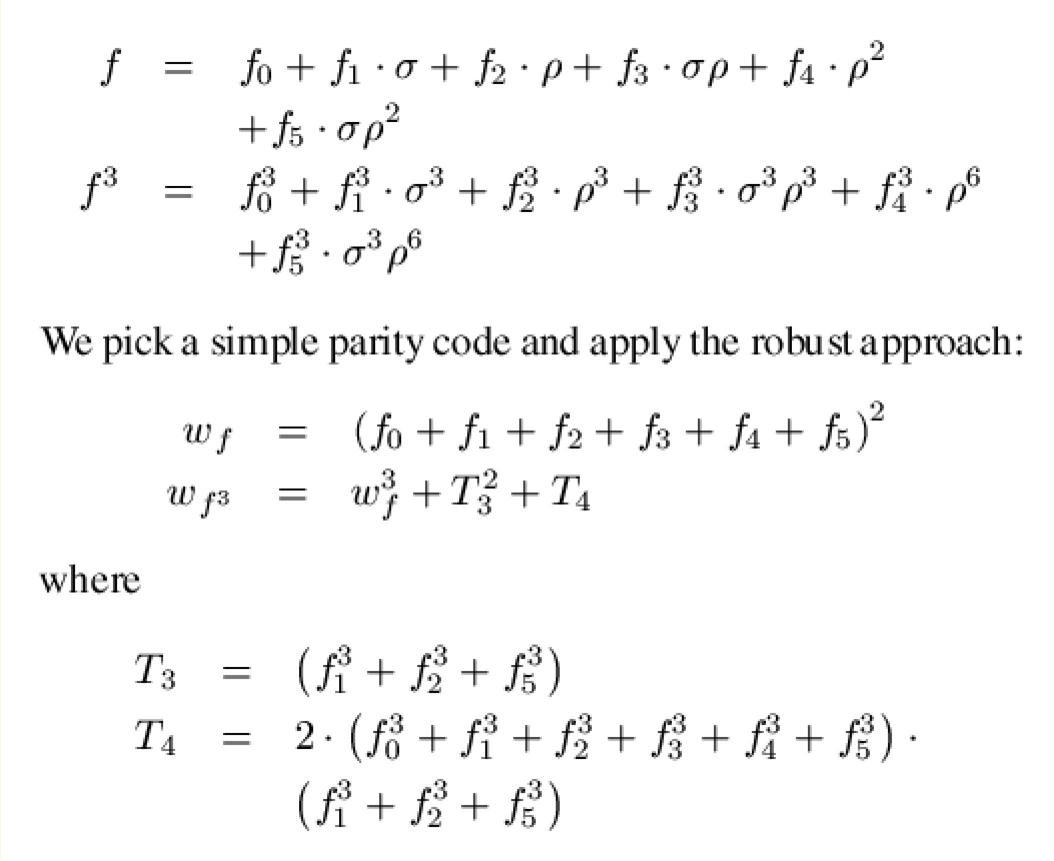
We pick a simple parity code and apply the robust approach:

$$\begin{aligned} w_f &= (f_0 + f_1 + f_2 + f_3 + f_4 + f_5)^2 \\ w_g &= (g_0 + g_1 + g_2 - 1)^2 \\ w_r &= w_f w_g + T_1^2 + T_2 \end{aligned}$$

where

$$\begin{aligned} T_1 &= f_1 g_1 + f_3 g_1 + f_4 g_1 + f_4 g_2 + f_5 g_2 \\ &\quad - f_2 - f_3 - f_4 - f_5 \\ T_2 &= 2 \cdot (f_1 g_1 + f_3 g_1 + f_4 g_1 + f_4 g_2 + f_5 g_2 \\ &\quad - f_2 - f_3 - f_4 - f_5) \cdot \sqrt{w_f}\sqrt{w_g} \end{aligned}$$

Cubing in GF(3^{6m})



$$
\begin{aligned}
f &= f_0 + f_1 \cdot \sigma + f_2 \cdot \rho + f_3 \cdot \sigma\rho + f_4 \cdot \rho^2 \\
&\quad + f_5 \cdot \sigma\rho^2 \\
f^3 &= f_0^3 + f_1^3 \cdot \sigma^3 + f_2^3 \cdot \rho^3 + f_3^3 \cdot \sigma^3\rho^3 + f_4^3 \cdot \rho^6 \\
&\quad + f_5^3 \cdot \sigma^3\rho^6
\end{aligned}
$$

We pick a simple parity code and apply the robust approach:

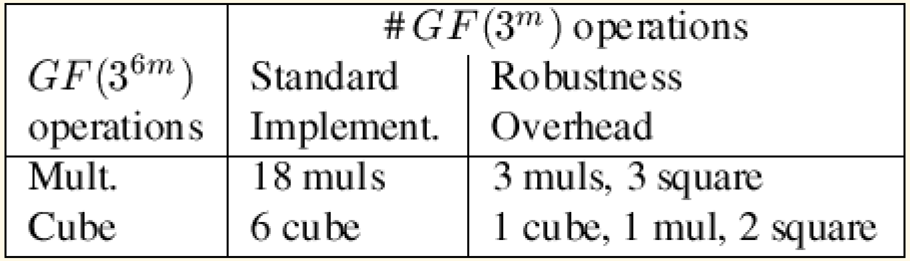
$$
\begin{aligned}
w_f &= (f_0 + f_1 + f_2 + f_3 + f_4 + f_5)^2 \\
w_{f^3} &= w_f^3 + T_3^2 + T_4
\end{aligned}
$$

where

$$
\begin{aligned}
T_3 &= (f_1^3 + f_2^3 + f_5^3) \\
T_4 &= 2 \cdot (f_0^3 + f_1^3 + f_2^3 + f_3^3 + f_4^3 + f_5^3) \cdot \\
&\quad (f_1^3 + f_2^3 + f_5^3)
\end{aligned}
$$

Performance Analysis

- Complexity of GF(3^{6m}) operations for standard and robust implementations:



	$\#GF(3^m)$ operations	
$GF(3^{6m})$ operations	Standard Implement.	Robustness Overhead
Mult.	18 muls	3 muls, 3 square
Cube	6 cube	1 cube, 1 mul, 2 square

- The robustness approach causes an area overhead of about 50%, without an impact on the latency.

Conclusion

- The proposed scheme provides quantifiable levels of protection in a well defined strong attacker model.
- We believe further reduction of the area overhead is desired and possible.
- The proposed technique should be considered only as a proof of concept implementation.