Introduction to Weil descent for (hyper)elliptic curves

Daniel Arnold Moldovan, Cihangir Tezcan

École Polytechnique Fédérale de Lausanne

25th May 2011
The Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let $E$ be an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_{q^n})$, $Q \in \langle P \rangle$. Find the integer $0 \leq r \leq \text{ord}(P)$ such that $Q = rP$. 
The Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let $E$ be an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_{q^n})$, $Q \in \langle P \rangle$. Find the integer $0 \leq r \leq \text{ord}(P)$ such that $Q = rP$.

Idea

Map the ECDLP into the Jacobian of a hyperelliptic curve, where we have efficient arithmetic due to D.G.Cantor and a good notion of factor base for an index calculus-type method.
The Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let $E$ be an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_{q^n})$, $Q \in \langle P \rangle$. Find the integer $0 \leq r \leq \text{ord}(P)$ such that $Q = rP$.

Idea

Map the ECDLP into the Jacobian of a hyperelliptic curve, where we have efficient arithmetic due to D.G.Cantor and a good notion of factor base for an index calculus-type method.

Aim of this talk

The aim of this talk is to give an introduction to the Weil descent attack for (hyper)elliptic curves, due to Gaudry, Hess and Smart, known as the GHS attack.
References

References

References

Contents

1. The Weil descent attack
   - The Weil descent attack

2. Analysis and Limitations of GHS Attack
   - Analysis and Limitations of GHS Attack

3. Extended GHS Attack
   - Extended GHS Attack
General framework of the GHS attack

- Let \( E \) be an elliptic curve defined over \( \mathbb{F}_{q^n} \)
General framework of the GHS attack

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, the Weil restriction of $E$
General framework of the GHS attack

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, the Weil restriction of $E$
- Construct a hyperelliptic curve of ”small genus” $C$ in $W$ by hyperplane sections
The Weil descent attack

Analysis and Limitations of GHS Attack

Extended GHS Attack

General framework of the GHS attack

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, the Weil restriction of $E$
- Construct a hyperelliptic curve of ”small genus” $C$ in $W$ by hyperplane sections
- Reduce the DLP from $E$ to $\text{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \rightarrow \text{Jac}(C)(\mathbb{F}_q)$
**General framework of the GHS attack**

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, *the Weil restriction* of $E$
- Construct a hyperelliptic curve of ”small genus” $C$ in $W$ by hyperplane sections
- Reduce the DLP from $E$ to $\text{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \rightarrow \text{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\text{Jac}(C)(\mathbb{F}_q)$ using index calculus
The Weil descent attack

Analysis and Limitations of GHS Attack

Extended GHS Attack

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves

General framework of the GHS attack

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, the Weil restriction of $E$
- Construct a hyperelliptic curve of ”small genus” $C$ in $W$ by hyperplane sections
- Reduce the DLP from $E$ to $\text{Jac}(C)$ by using a map $\varphi: E(\mathbb{F}_{q^n}) \to \text{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\text{Jac}(C)(\mathbb{F}_q)$ using index calculus
- Deduce the result of the ECDLP for $E$. 

Observe that the GHS attack is actually a “cover attack”: if we have a cover of curves $C_1 \to C_2$, we transfer the DLP from $C_2$ into $\text{Jac}(C_1)$.
General framework of the GHS attack

- Let $E$ be an elliptic curve defined over $\mathbb{F}_{q^n}$
- Construct an abelian variety $W$ over $\mathbb{F}_q$, the Weil restriction of $E$
- Construct a hyperelliptic curve of "small genus" $C$ in $W$ by hyperplane sections
- Reduce the DLP from $E$ to $\text{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \to \text{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\text{Jac}(C)(\mathbb{F}_q)$ using index calculus
- Deduce the result of the ECDLP for $E$.

Observe that the GHS attack is actually a "cover attack": if we have a cover of curves $C_1 \to C_2$, we transfer the DLP from $C_2$ into $\text{Jac}(C_1)$
Construction of the map $\varphi$

- We have $E(F_{q^n}) \simeq W(F_q)$ and $W \simeq E \times E^\sigma \times E^{\sigma^2} \times \ldots \times E^{\sigma^{n-1}}$ over $F_{q^n}$, where $\sigma$ is the Frobenius automorphism of $F_{q^n}/F_q$. 
Construction of the map $\varphi$

- We have $E(\mathbb{F}_{q^n}) \cong W(\mathbb{F}_q)$ and $W \cong E \times E^\sigma \times E^{\sigma^2} \times \ldots \times E^{\sigma^{n-1}}$ over $\mathbb{F}_{q^n}$, where $\sigma$ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$.
- Project $W$ onto $E$ and compose with $C \hookrightarrow W$ to obtain a covering $C \to E$ over $\mathbb{F}_{q^n}$.
Construction of the map $\varphi$

- We have $E(\mathbb{F}_{q^n}) \simeq W(\mathbb{F}_q)$ and $W \simeq E \times E^\sigma \times E^{\sigma^2} \times \ldots \times E^{\sigma^{n-1}}$ over $\mathbb{F}_{q^n}$, where $\sigma$ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$.
- Project $W$ onto $E$ and compose with $C \hookrightarrow W$ to obtain a covering $C \rightarrow E$ over $\mathbb{F}_{q^n}$.
- Use properties of $\text{Jac}$ to obtain a map $\text{Jac}(E) \rightarrow \text{Jac}(C)$. 
Construction of the map $\varphi$

- We have $E(\mathbb{F}_{q^n}) \simeq W(\mathbb{F}_q)$ and $W \simeq E \times E^\sigma \times E^{\sigma^2} \times \cdots \times E^{\sigma^{n-1}}$ over $\mathbb{F}_{q^n}$, where $\sigma$ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$.
- Project $W$ onto $E$ and compose with $C \hookrightarrow W$ to obtain a covering $C \rightarrow E$ over $\mathbb{F}_{q^n}$.
- Use properties of $\text{Jac}$ to obtain a map $\text{Jac}(E) \rightarrow \text{Jac}(C)$.
- Since $E$ is an elliptic curve, we have $E \simeq \text{Jac}(E)$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
Construction of the map $\varphi$

- We have $E(F_{q^n}) \simeq W(F_q)$ and $W \simeq E \times E^\sigma \times E^{\sigma^2} \times \ldots \times E^{\sigma^{n-1}}$ over $F_{q^n}$, where $\sigma$ is the Frobenius automorphism of $F_{q^n}/F_q$.
- Project $W$ onto $E$ and compose with $C \hookrightarrow W$ to obtain a covering $C \to E$ over $F_{q^n}$.
- Use properties of $\text{Jac}$ to obtain a map $\text{Jac}(E) \to \text{Jac}(C)$.
- Since $E$ is an elliptic curve, we have $E \simeq \text{Jac}(E)$.
- Combining all these construct a map $E(F_{q^n}) \to \text{Jac}(C)(F_{q^n})$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
Construction of the map $\varphi$

- We have $E(\mathbb{F}_{q^n}) \simeq W(\mathbb{F}_q)$ and $W \simeq E \times E^\sigma \times E^\sigma^2 \times \ldots \times E^\sigma^{n-1}$ over $\mathbb{F}_{q^n}$, where $\sigma$ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$.

- Project $W$ onto $E$ and compose with $C \hookrightarrow W$ to obtain a covering $C \rightarrow E$ over $\mathbb{F}_{q^n}$.

- Use properties of $\text{Jac}$ to obtain a map $\text{Jac}(E) \rightarrow \text{Jac}(C)$.

- Since $E$ is an elliptic curve, we have $E \simeq \text{Jac}(E)$.

- Combining all these construct a map $E(\mathbb{F}_{q^n}) \rightarrow \text{Jac}(C)(\mathbb{F}_{q^n})$.

- Go down to $\text{Jac}(C)(\mathbb{F}_q)$ by applying the trace map:

$$\sum_{P \in C} n_P P \mapsto \sum_{P \in C} n_P \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(P)$$
Main result

Let $E$ be an elliptic curve over a field $\mathbb{F}_{q^n}$ of characteristic 2 and $p$ be a large prime dividing $\#E(\mathbb{F}_{q^n})$. Supposing that some conditions are satisfied (which guarantee the existence of a curve of small genus in the Weil restriction), one can solve the ECDLP in the $p$-cyclic subgroup of $\#E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$. 
Main result

Let $E$ be an elliptic curve over a field $\mathbb{F}_{q^n}$ of characteristic 2 and $p$ be a large prime dividing $\#E(\mathbb{F}_{q^n})$. Supposing that some conditions are satisfied (which guarantee the existence of a curve of small genus in the Weil restriction), one can solve the ECDLP in the $p$-cyclic subgroup of $\#E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard’s rho

- GHS is asymptotically faster than Pollard’s rho method ($O(\sqrt{p})$)
Main result

Let $E$ be an elliptic curve over a field $\mathbb{F}_{q^n}$ of characteristic 2 and $p$ be a large prime dividing $\#E(\mathbb{F}_{q^n})$. Supposing that some conditions are satisfied (which guarantee the existence of a curve of small genus in the Weil restriction), one can solve the ECDLP in the $p$-cyclic subgroup of $\#E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard’s rho

- GHS is asymptotically faster then Pollard’s rho method ($O(\sqrt{p})$)
- GHS becomes impractical for large genera (e.g. $g \geq 10$) because of the large multiplicative factor $g!$
Main result

Let $E$ be an elliptic curve over a field $\mathbb{F}_{q^n}$ of characteristic 2 and $p$ be a large prime dividing $\#E(\mathbb{F}_{q^n})$. Supposing that some conditions are satisfied (which guarantee the existence of a curve of small genus in the Weil restriction), one can solve the ECDLP in the $p$-cyclic subgroup of $\#E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard’s rho

- GHS is asymptotically faster than Pollard’s rho method ($O(\sqrt{p})$)
- GHS becomes impractical for large genera (e.g. $g \geq 10$) because of the large multiplicative factor $g!$

Main task

How to keep the genus of the curve $C$ small?
The Weil restriction - through an example

- Let $\mathbb{F}_{p^2}/\mathbb{F}_p$ be a quadratic field extension, with basis $\{1, u\}$ and $E: y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_{p^2}$, $b \neq 0$ be an elliptic curve over $\mathbb{F}_{p^2}$.
The Weil restriction - through an example

- Let $\mathbb{F}_{p^2}/\mathbb{F}_p$ be a quadratic field extension, with basis $\{1, u\}$ and $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_{p^2}$, $b \neq 0$ be an elliptic curve over $\mathbb{F}_{p^2}$.

- Write all variables and coefficients of the equations in the basis $x = x_1 + ux_2$, $y = y_1 + uy_2$, $a = a_1 + ua_2$, $b = b_1 + ub_2$, $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$. 

properties of the Weil restriction

$W$ is a variety over $k$ of dimension $n = [K:k]$.

$\mathbb{V}(K) \cong W(k)$

If $\sigma$ is the Frobenius automorphism of $K/k$, then $W$ is an abelian variety isomorphic to $E \times E \sigma \times E \sigma^2 \times \ldots \times E \sigma^{n-1}$ over $K$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
The Weil restriction - through an example

- Let \( \mathbb{F}_{p^2} / \mathbb{F}_p \) be a quadratic field extension, with basis \( \{1, u\} \) and \( E : y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}_{p^2}, \ b \neq 0 \) be an elliptic curve over \( \mathbb{F}_{p^2} \).

- Write all variables and coefficients of the equations in the basis 
  \( x = x_1 + ux_2, \ y = y_1 + uy_2, \ a = a_1 + ua_2, \ b = b_1 + ub_2, \)
  \( x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p \)

- Perform all computations and expand in the basis
The Weil restriction - through an example

- Let \( \mathbb{F}_{p^2}/\mathbb{F}_p \) be a quadratic field extension, with basis \( \{1, u\} \) and \( E : y^2 = x^3 + ax + b, a, b \in \mathbb{F}_{p^2}, b \neq 0 \) be an elliptic curve over \( \mathbb{F}_{p^2} \).

- Write all variables and coefficients of the equations in the basis:
  \[
  x = x_1 + ux_2, \quad y = y_1 + uy_2, \quad a = a_1 + ua_2, \quad b = b_1 + ub_2,
  \]
  \[
  x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p
  \]

- Perform all computations and expand in the basis.

- By equating the coefficients of 1 and \( u \) with 0, obtain 2 equations in \( x_i, y_i, a_i, b_i \), which define a variety \( W \) over \( k \).
The Weil restriction - through an example

- Let $\mathbb{F}_{p^2}/\mathbb{F}_p$ be a quadratic field extension, with basis $\{1, u\}$ and $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_{p^2}$, $b \neq 0$ be an elliptic curve over $\mathbb{F}_{p^2}$.

- Write all variables and coefficients of the equations in the basis $x = x_1 + ux_2, y = y_1 + uy_2, a = a_1 + ua_2, b = b_1 + ub_2$, $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$.

- Perform all computations and expand in the basis.

- By equating the coefficients of 1 and $u$ with 0, obtain 2 equations in $x_i, y_i, a_i, b_i$, which define a variety $W$ over $k$.

Properties of the Weil restriction

- $W$ is a variety over $k$ of dimension $n = [K : k]$. 
The Weil restriction - through an example

- Let $\mathbb{F}_{p^2}/\mathbb{F}_p$ be a quadratic field extension, with basis $\{1, u\}$ and $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_{p^2}$, $b \neq 0$ be an elliptic curve over $\mathbb{F}_{p^2}$

- Write all variables and coefficients of the equations in the basis
  
  $x = x_1 + ux_2$, $y = y_1 + uy_2$, $a = a_1 + ua_2$, $b = b_1 + ub_2$,
  
  $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$

- Perform all computations and expand in the basis

- By equating the coefficients of 1 and $u$ with 0, obtain 2 equations in $x_i, y_i, a_i, b_i$, which define a variety $W$ over $k$.

Properties of the Weil restriction

- $W$ is a variety over $k$ of dimension $n = [K : k]$

- $V(K) \simeq W(k)$
The Weil restriction - through an example

- Let $\mathbb{F}_p^2/\mathbb{F}_p$ be a quadratic field extension, with basis $\{1, u\}$ and $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_p^2$, $b \neq 0$ be an elliptic curve over $\mathbb{F}_p^2$

- Write all variables and coefficients of the equations in the basis:
  
  - $x = x_1 + ux_2$, $y = y_1 + uy_2$, $a = a_1 + ua_2$, $b = b_1 + ub_2$,
  
  - $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$

- Perform all computations and expand in the basis.

- By equating the coefficients of 1 and $u$ with 0, obtain 2 equations in $x_i, y_i, a_i, b_i$, which define a variety $W$ over $k$.

Properties of the Weil restriction

- $W$ is a variety over $k$ of dimension $n = [K : k]$

- $V(K) \simeq W(k)$

- If $\sigma$ is the Frobenius automorphism of $K/k$, then $W$ is an abelian variety isomorphic to $E \times E^\sigma \times E^{\sigma^2} \times \ldots \times E^{\sigma^{n-1}}$ over $K$
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a "large" finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ ("quite small")
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a “large” finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ (“quite small”)
- Let $E : Y^2 + XY = X^3 + aX^2 + b$, $a, b \in K$, $b \neq 0$ be a non-supersingular elliptic curve over $K$
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a "large" finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ ("quite small")
- Let $E : Y^2 + XY = X^3 + aX^2 + b$, $a, b \in K$, $b \neq 0$ be a non-supersingular elliptic curve over $K$
- Suppose that $E(K)$ contains a subgroup of prime order $p \approx \#K$
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a "large" finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ ("quite small")
- Let $E : Y^2 + XY = X^3 + aX^2 + b$, $a, b \in K$, $b \neq 0$ be a non-supersingular elliptic curve over $K$
- Suppose that $E(K)$ contains a subgroup of prime order $p \approx \#K$
- Construct the Weil restriction $W$ of $E$, an $n$-dimensional abelian variety over $k$
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a "large" finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ ("quite small")
- Let $E : Y^2 + XY = X^3 + aX^2 + b, \ a, b \in K, \ b \neq 0$ be a non-supersingular elliptic curve over $K$
- Suppose that $E(K)$ contains a subgroup of prime order $p \approx \#K$
- Construct the Weil restriction $W$ of $E$, an $n$-dimensional abelian variety over $k$
- Intersect $W$ with $n - 1$ hyperplanes (we are free to choose these). Example: if $n = 2$, we have a surface over $k$ embedded in $\mathbb{P}^2 \times \mathbb{P}^2$ and we have to cut it with a hyperplane
Curves in the Weil restriction of an elliptic curve

- Let $k$ be a "large" finite field of characteristic 2 and $K$ be an extension of $k$ of degree $n$ ("quite small")
- Let $E : Y^2 + XY = X^3 + aX^2 + b$, $a, b \in K$, $b \neq 0$ be a non-supersingular elliptic curve over $K$
- Suppose that $E(K)$ contains a subgroup of prime order $p \approx \#K$
- Construct the Weil restriction $W$ of $E$, an $n$-dimensional abelian variety over $k$
- Intersect $W$ with $n - 1$ hyperplanes (we are free to choose these). Example: if $n = 2$, we have a surface over $k$ embedded in $\mathbb{P}^2 \times \mathbb{P}^2$ and we have to cut it with a hyperplane
- We obtain a curve $C$ over $k$
Examples of such curves

- Take \( E : Y^2 + XY = X^3 + b, \ b \in K^* \)
Examples of such curves

- Take $E : Y^2 + XY = X^3 + b$, $b \in K^*$
- Suppose that $K/k$ has a basis of the form $u_i = \theta^{2^i}$, $1 \leq i \leq n - 1$, with $\theta + \theta^2 + \theta^4 + \ldots + \theta^{2^{n-1}} = 1$
Examples of such curves

- Take $E : Y^2 + XY = X^3 + b$, $b \in K^*$
- Suppose that $K/k$ has a basis of the form $u_i = \theta^{2^i}$, $1 \leq i \leq n-1$, with $\theta + \theta^2 + \theta^4 + \ldots + \theta^{2^{n-1}} = 1$
- Since $\theta^{2^n} = \theta$, squaring an element represented in such a basis is simply a cyclic shift of the coefficients
Examples of such curves

- Take $E : Y^2 + XY = X^3 + b$, $b \in K^*$
- Suppose that $K/k$ has a basis of the form $u_i = \theta^{2^i}$, $1 \leq i \leq n - 1$, with $\theta + \theta^2 + \theta^4 + \ldots + \theta^{2^{n-1}} = 1$
- Since $\theta^{2^n} = \theta$, squaring an element represented in such a basis is simply a cyclic shift of the coefficients
- We intersect $W$ with the hyperplanes given by $x_0 = \ldots = x_{n-1} = x$ (where $X = x_0 u_0 + x_1 u_1 + \ldots + x_{n-1} u_{n-1}$ etc.)
Examples of such curves

- Take $E : Y^2 + XY = X^3 + b$, $b \in K^*$
- Suppose that $K/k$ has a basis of the form $u_i = \theta^{2^i}$, $1 \leq i \leq n - 1$, with $\theta + \theta^2 + \theta^4 + \ldots + \theta^{2^{n-1}} = 1$
- Since $\theta^{2^n} = \theta$, squaring an element represented in such a basis is simply a cyclic shift of the coefficients
- We intersect $W$ with the hyperplanes given by $x_0 = \ldots = x_{n-1} = x$ (where $X = x_0 u_0 + x_1 u_1 + \ldots + x_{n-1} u_{n-1}$ etc.)
- We obtain a curve $C$ defined by the equations

$$\begin{cases}
y_{n-1}^2 + xy_0 + x^3 + b_0 = 0 \\
y_0^2 + xy_1 + x^3 + b_1 = 0 \\
\vdots \\
y_{n-2}^2 + xy_{n-1} + x^3 + b_{n-1} = 0
\end{cases}$$
### Examples of such curves

- Take $E : \ Y^2 + XY = X^3 + b$, $b \in K^*$
- Suppose that $K/k$ has a basis of the form $u_i = \theta^{2^i}$, $1 \leq i \leq n-1$, with $\theta + \theta^2 + \theta^4 + \ldots + \theta^{2^{n-1}} = 1$
- Since $\theta^{2^n} = \theta$, squaring an element represented in such a basis is simply a cyclic shift of the coefficients
- We intersect $W$ with the hyperplanes given by $x_0 = \ldots = x_{n-1} = x$ (where $X = x_0 u_0 + x_1 u_1 + \ldots + x_{n-1} u_{n-1}$ etc.)
- We obtain a curve $C$ defined by the equations

\[
\begin{align*}
    y_{n-1}^2 + xy_0 + x^3 + b_0 &= 0 \\
    y_0^2 + xy_1 + x^3 + b_1 &= 0 \\
    &\vdots \\
    y_{n-2}^2 + xy_{n-1} + x^3 + b_{n-1} &= 0
\end{align*}
\]

- Experimentally, the genus of $C$ is quite small
Appropriate models for the curve

- Back to the general case $E : Y^2 + XY = X^3 + aX^2 + b$, $a \in K$, $b \in K^*$
Appropriate models for the curve

- Back to the general case $E : Y^2 + XY = X^3 + aX^2 + b$, $a \in K, b \in K^*$
- Take $\{u_0, ..., u_{n-1}\}$ to be a basis of $K$ over $k$ such that $u_0 + ... + u_{n-1} = 1$ and let $\sigma$ be the Frobenius of $K/k$. 
Appropriate models for the curve

- Back to the general case $E: Y^2 + XY = X^3 + aX^2 + b$, $a \in K$, $b \in K^*$
- Take $\{u_0, \ldots, u_{n-1}\}$ to be a basis of $K$ over $k$ such that $u_0 + \ldots + u_{n-1} = 1$ and let $\sigma$ be the Frobenius of $K/k$.
- Write $X = x_0 u_0 + \ldots + x_{n-1} u_{n-1}$, $Y = y_0 u_0 + \ldots + y_{n-1} u_{n-1}$ etc.
Appropriate models for the curve

- Back to the general case $E : Y^2 + XY = X^3 + aX^2 + b$, $a \in K$, $b \in K^*$

- Take $\{u_0, ..., u_{n-1}\}$ to be a basis of $K$ over $k$ such that $u_0 + ... + u_{n-1} = 1$ and let $\sigma$ be the Frobenius of $K/k$.

- Write $X = x_0 u_0 + ... + x_{n-1} u_{n-1}$, $Y = y_0 u_0 + ... + y_{n-1} u_{n-1}$ etc.

- By a linear change of variables $y_i \mapsto w_i$, defined over $K$, $C$ is birationally equivalent to

$$D : \begin{cases} 
    w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0 = 0 \\
    \vdots \\
    w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1} x^2 + \beta_{n-1} = 0 
\end{cases}$$
The Weil descent attack

Analysis and Limitations of GHS Attack

Extended GHS Attack

Appropriate models for the curve

- Back to the general case $E : Y^2 + XY = X^3 + aX^2 + b$, $a \in K, b \in K^*$
- Take $\{u_0, ..., u_{n-1}\}$ to be a basis of $K$ over $k$ such that $u_0 + ... + u_{n-1} = 1$ and let $\sigma$ be the Frobenius of $K/k$.
- Write $X = x_0u_0 + ... + x_{n-1}u_{n-1}$, $Y = y_0u_0 + ... + y_{n-1}u_{n-1}$ etc.
- By a linear change of variables $y_i \mapsto w_i$, defined over $K$, $C$ is birationally equivalent to

$$D : \begin{cases} w_0^2 + xw_0 + x^3 + \alpha_0x^2 + \beta_0 = 0 \\ \vdots \\ w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1}x^2 + \beta_{n-1} = 0 \end{cases}$$

- $\sigma$ can be extended to $K[x, w_0, ..., w_{n-1}]$ via $\sigma(x) = x$, $\sigma(w_i) = \sigma(w_{i+1})$, $\sigma(w_{n-1}) = w_0$
Let $F_i$ be the splitting field of the $i^{th}$ equation defining $D$ over $K(x)$. Then the $F_i$s are quadratic extensions of $K(x)$. 

Daniel Arnold Moldovan, Cihangir Tezcan
Introduction to Weil descent for (hyper)elliptic curves
Compositum of splitting fields

- Let $F_i$ be the splitting field of the $i^{\text{th}}$ equation defining $D$ over $K(x)$. Then the $F_i$s are quadratic extensions of $K(x)$.
- Construct $F$ as the compositum of $F_0, \ldots, F_{n-1}$ over $K(x)$ (there is no ambiguity since they are Galois extensions of $K(x)$).
Compositum of splitting fields

- Let $F_i$ be the splitting field of the $i^{th}$ equation defining $D$ over $K(x)$. Then the $F_i$s are quadratic extensions of $K(x)$.
- Construct $F$ as the compositum of $F_0, ..., F_{n-1}$ over $K(x)$ (there is no ambiguity since they are Galois extensions of $K(x)$).
- Let $m \in \mathbb{N}$ be such that $[F : K(x)] = 2^m$
Compositum of splitting fields

- Let $F_i$ be the splitting field of the $i^{th}$ equation defining $D$ over $K(x)$. Then the $F_i$s are quadratic extensions of $K(x)$.
- Construct $F$ as the compositum of $F_0, \ldots, F_{n-1}$ over $K(x)$ (there is no ambiguity since they are Galois extensions of $K(x)$).
- Let $m \in \mathbb{N}$ be such that $[F : K(x)] = 2^m$.

Irreducible components

As a curve over $K$, $D$ has $2^{n-m}$ irreducible reduced components, each having function field $K$-isomorphic to $F$. 
Artin-Schreier properties

- Dividing the equations of $D$ by $x^2$ and substituting $s_i = \frac{w_i}{x} + \frac{\beta^{1/2}}{x}$ and $z = \frac{1}{x}$ we obtain a new model:

$$
F : \begin{cases}
    s_0^2 + s_0 + z^{-1} + \alpha_0 + \beta_0^{1/2}z = 0 \\
    \vdots \\
    s_{n-1}^2 + s_{n-1} + z^{-1} + \alpha_{n-1} + \beta_{n-1}^{1/2}z = 0
\end{cases}
$$
Artin-Schreier properties

- Dividing the equations of $D$ by $x^2$ and substituting $s_i = \frac{w_i}{x} + \frac{\beta^{1/2}}{x}$ and $z = \frac{1}{x}$ we obtain a new model:

$$
\begin{align*}
F:\begin{cases}
  s_0^2 + s_0 + z^{-1} + \alpha_0 + \beta_0^{1/2}z = 0 \\
  \\
  \vdots \\
  s_{n-1}^2 + s_{n-1} + z^{-1} + \alpha_{n-1} + \beta_{n-1}^{1/2}z = 0
\end{cases}
\end{align*}
$$

- We can now apply the Artin-Schreier theory, which gives a bijection:

Galois extensions $\leftrightarrow$ splitting fields of polynomials of exponent 2 of $K$ of the type $x^2 - x + d$, $d \in K$
Computation of $m$

- We need to compute $m$ because it gives full information on the genus of $F$
Computation of $m$

- We need to compute $m$ because it gives full information on the genus of $F$
- $m = \dim_{F_2}(\text{Span}_{F_2}\{(1, \beta_0^{\frac{1}{2}}), \ldots, (1, \beta_{n-1}^{\frac{1}{2}})\})$
The Weil descent attack
Analysis and Limitations of GHS Attack
Extended GHS Attack

Computation of $m$

- We need to compute $m$ because it gives full information on the genus of $F$
- $m = \dim_{\mathbb{F}_2}(\text{Span}_{\mathbb{F}_2}\{(1, \beta_0^1), ..., (1, \beta_{n-1}^1)\})$
- The $\beta_i$s are easy to compute
We need to compute $m$ because it gives full information on the genus of $F$

$m = \dim_{F_2}(\text{Span}_{F_2}\{(1, \beta_0^{1/2}), ..., (1, \beta_{n-1}^{1/2})\})$

The $\beta_i$s are easy to compute

The exact function field of $F$ is $K$ and $F = F_0...F_{m-1}$ over $K(z)$
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad 1 \leq i \leq m - 1 \]
  with splitting field \( L_i \).
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad 1 \leq i \leq m - 1 \text{ with splitting field } L_i. \]
- \[ F = F_0L \text{ with } L \text{ the compositum of } L_1, \ldots, L_{m-1} \text{ over } K(z) \]
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad 1 \leq i \leq m - 1 \text{ with splitting field } L_i. \]
- \( F = F_0 L \) with \( L \) the compositum of \( L_1, \ldots, L_{m-1} \) over \( K(z) \)
- \( L \) is a rational subfield of index 2 of \( F \)
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad 1 \leq i \leq m - 1 \text{ with splitting field } L_i. \]
- \( F = F_0 L \) with \( L \) the compositum of \( L_1, \ldots, L_{m-1} \) over \( K(z) \)
- \( L \) is a rational subfield of index 2 of \( F \)

An alternative definition of hyperellipticity

- A nonsingular curve \( C \) over \( K \) of genus larger than 1 is called \textit{hyperelliptic} if the function field \( K(C) \) is a separable extension of degree 2 of the rational function field \( K(x) \)
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \; 1 \leq i \leq m - 1 \] with splitting field \( L_i \).
- \( F = F_0 L \) with \( L \) the compositum of \( L_1, \ldots, L_{m-1} \) over \( K(z) \).
- \( L \) is a rational subfield of index 2 of \( F \).

An alternative definition of hyperellipticity

- A nonsingular curve \( C \) over \( K \) of genus larger than 1 is called \textit{hyperelliptic} if the function field \( K(C) \) is a separable extension of degree 2 of the rational function field \( K(x) \).
- Every hyperelliptic curve of genus \( g \) has an equation of the form
  \[ y^2 + h(x)y = f(x), \; h, f \in K[x], \; \deg(h) \leq g + 1, \; \deg(f) \leq 2g + 2 \]
Hyperellipticity

- By eliminating variables we obtain
  \[ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad 1 \leq i \leq m - 1 \] with splitting field \( L_i \).
- \( F = F_0 L \) with \( L \) the compositum of \( L_1, \ldots, L_{m-1} \) over \( K(z) \).
- \( L \) is a rational subfield of index 2 of \( F \).

An alternative definition of hyperellipticity

- A nonsingular curve \( C \) over \( K \) of genus larger than 1 is called *hyperelliptic* if the function field \( K(C) \) is a separable extension of degree 2 of the rational function field \( K(x) \).
- Every hyperelliptic curve of genus \( g \) has an equation of the form
  \[ y^2 + h(x)y = f(x), \quad h, f \in K[x], \quad \deg(h) \leq g + 1, \quad \deg(f) \leq 2g + 2 \]

Conclusion

\( F \) is a hyperelliptic function field over the exact constant field \( K \).
Genus computation

- We use the Riemann-Hurwitz formula, which for a covering $C_1 \to C_2$ of curves gives a relation between the genera of the curves and the degree of the covering (plus some additional information - the ramification indexes)
Genus computation

- We use the Riemann-Hurwitz formula, which for a covering \( C_1 \rightarrow C_2 \) of curves gives a relation between the genera of the curves and the degree of the covering (plus some additional information - the ramification indexes)
- The genus of \( F \) is either \( 2^{m-1} \) or \( 2^{m-1} - 1 \)
Restriction to a smaller constant field

- The Frobenius of $K/k$ extends (nonuniquely) to a $k$-automorphism of $F$ of order $n$ or $2n$, again denoted by $\sigma$
Restriction to a smaller constant field

- The Frobenius of $K/k$ extends (nonuniquely) to a $k$-automorphism of $F$ of order $n$ or $2n$, again denoted by $\sigma$.
- Suppose (*) either $n$ is odd or ($m = n$ and $\text{Tr}_{K/F_2}(\alpha) = 0$).

\[ \text{In this case, } \sigma \text{ can be chosen with order exactly } n. \]

Let $F'$ be the field of elements of $F$ fixed by $\sigma$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
 Restriction to a smaller constant field

- The Frobenius of $K/k$ extends (nonuniquely) to a $k$-automorphism of $F$ of order $n$ or $2n$, again denoted by $\sigma$.
- Suppose (*) either $n$ is odd or $(m = n$ and $\text{Tr}_{K/F}(\alpha) = 0)$
- In this case, $\sigma$ can be chosen with order exactly $n$
Restriction to a smaller constant field

- The Frobenius of $K/k$ extends (nonuniquely) to a $k$-automorphism of $F$ of order $n$ or $2n$, again denoted by $\sigma$.
- Suppose (*) either $n$ is odd or $(m = n$ and $\text{Tr}_{K/F_2}(\alpha) = 0$).
- In this case, $\sigma$ can be chosen with order exactly $n$.
- Let $F'$ be the field of elements of $F$ fixed by $\sigma$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
The Weil descent attack

Analysis and Limitations of GHS Attack

Extended GHS Attack

Introduction to Weil descent for (hyper)elliptic curves

\[ F \xrightarrow{n} F' \]
\[ L \xrightarrow{n} 2 \]
\[ 2^{m-1} \]
\[ K(x) \xrightarrow{n} 2^{m-1} \]
\[ k(x) \]
\[ K \xrightarrow{n} k \]
Result

Suppose that condition (*) is satisfied.

- Then $F'$ is a hyperelliptic function field of genus $2^{m-1}$ or $2^{m-1} - 1$ over the exact constant field $k$. 
Suppose that condition (*) is satisfied.

- Then $F'$ is a hyperelliptic function field of genus $2^{m-1}$ or $2^{m-1} - 1$ over the exact constant field $k$.
- The curve $C$ has an irreducible reduced component with function field $F'$. For the transfer of the DLP we will use this irreducible component, still denoted by $C$. 
Summary of the GHS attack

- Let $E$ be an elliptic curve over $K$ satisfying condition (*)
Summary of the GHS attack

- Let $E$ be an elliptic curve over $K$ satisfying condition (*)
- Let $W$ be the Weil restriction of $E$; it is an abelian variety over $k$
Summary of the GHS attack

- Let $E$ be an elliptic curve over $K$ satisfying condition (*)
- Let $W$ be the Weil restriction of $E$; it is an abelian variety over $k$
- We have constructed in $W$ a hyperelliptic curve $C$ of ”small” genus
Summary of the GHS attack

- Let $E$ be an elliptic curve over $K$ satisfying condition (*)
- Let $W$ be the Weil restriction of $E$; it is an abelian variety over $k$
- We have constructed in $W$ a hyperelliptic curve $C$ of ”small” genus
- We can reduce the ECDLP from $E(K)$ to $\text{Jac}(C)(k)$ by using a map $\varphi : E(K) \to \text{Jac}(C)(k)$
Question

- Does $\varphi$ map the large $p$-subgroup of $E(K)$ to 0?
Question

- Does $\varphi$ map the large $p$-subgroup of $E(K)$ to 0?

Answer

- It is highly unlikely
Question

- Does $\varphi$ map the large $p$-subgroup of $E(K)$ to 0?

Answer

- It is highly unlikely
- The kernel of the trace map: $\text{Jac}(C)(K) \rightarrow \text{Jac}(C)(k)$ can only consist of 2-power torsion elements.
**Question**

- Does \( \varphi \) map the large \( p \)-subgroup of \( E(K) \) to 0?

**Answer**

- It is highly unlikely
- The kernel of the trace map: \( \text{Jac}(C)(K) \rightarrow \text{Jac}(C)(k) \) can only consist of 2-power torsion elements
- For large values of \( m \) (larger than \( \log_2(n) \)) the large \( p \)-subgroup is preserved in many instances
Aim of This Talk

The aim of this talk is to

1. analyze the GHS attack and its implications
Aim of This Talk

The aim of this talk is to

1. analyze the GHS attack and its implications
2. briefly introduce the Extended GHS attack and its consequences
Aim of This Talk

The aim of this talk is to

1. analyze the GHS attack and its implications
2. briefly introduce the Extended GHS attack and its consequences

References

Recall

- Let $\ell$ and $n$ be positive integers with $\gcd(\ell, n) = 1$, $q = 2^\ell$, $k = \mathbb{F}_q$, and $K = \mathbb{F}_{q^n}$.
Recall

- Let \( \ell \) and \( n \) be positive integers with \( \gcd(\ell, n) = 1 \), \( q = 2^\ell \), \( k = \mathbb{F}_q \), and \( K = \mathbb{F}_{q^n} \).
- We consider the elliptic curve \( E \) defined over \( K \) by the equation

\[
E : y^2 + xy = x^3 + ax^2 + b
\]

where \( a \in \{0, 1\} \) and \( b \in K^* \).
Recall

- Let $\ell$ and $n$ be positive integers with $\gcd(\ell, n) = 1$, $q = 2^\ell$, $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$.
- We consider the elliptic curve $E$ defined over $K$ by the equation
  \[ E : y^2 + xy = x^3 + ax^2 + b \]
  where $a \in \{0, 1\}$ and $b \in K^*$.
- GHS attack reduces the ECDLP in $E(K)$ to the DLP in a subgroup of order $r \approx q^n$ of the Jacobian $J_C(k)$ of a hyperelliptic curve $C$ of genus $g$ defined over $k$. 
Recall

- Let $\ell$ and $n$ be positive integers with $\gcd(\ell, n) = 1$, $q = 2^\ell$, $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$.
- We consider the elliptic curve $E$ defined over $K$ by the equation
  \[
  E : y^2 + xy = x^3 + ax^2 + b
  \]
  where $a \in \{0, 1\}$ and $b \in K^*$.
- GHS attack reduces the ECDLP in $E(K)$ to the DLP in a subgroup of order $r \approx q^n$ of the Jacobian $J_C(k)$ of a hyperelliptic curve $C$ of genus $g$ defined over $k$.

Note

*Note that $\# J_C(k) \approx q^g$ and a group operation in $J_C(k)$ can be performed in $O(g^2 \log^2 q)$ bit operations by Cantor's algorithm.*
The DLP in $J_C(k)$ can be solved using one of the following three methods:
DLP

The DLP in $J_C(k)$ can be solved using one of the following three methods:

1. **Pollard’s rho algorithm:** Expected running time of $O(g^2 q^{n/2} \log^2 q)$ bit operations.
The DLP in $J_C(k)$ can be solved using one of the following three methods:

1. **Pollard’s rho algorithm**: Expected running time of $O(g^2 q^{n/2} \log^2 q)$ bit operations.

2. **Adleman-DeMarrais-Huang algorithm (refined by Enge and Gaudry)**: Expected running time of $L_{g^q}(\frac{1}{2}, \sqrt{2})$ bit operations where $L_x(\frac{1}{2}, c) = O(exp((c + o(1))\sqrt{\log x \log \log x}))$ as $g / \log q \rightarrow \infty$. 
The DLP in $J_C(k)$ can be solved using one of the following three methods:

1. **Pollard’s rho algorithm**: Expected running time of $\mathcal{O}(g^2 q^{n/2} \log^2 q)$ bit operations.

2. **Adleman-DeMarrais-Huang algorithm (refined by Enge and Gaudry)**: Expected running time of $L_g q \left( \frac{1}{2}, \sqrt{2} \right)$ bit operations where $L_x \left( \frac{1}{2}, c \right) = \mathcal{O}(\exp((c + o(1))\sqrt{\log x} \sqrt{\log \log x}))$ as $g / \log q \to \infty$.

3. **Gaudry’s algorithm**: Expected running time of $\mathcal{O}(g^3 q^2 \log^2 q + g^2 g! q \log^2 q)$ bit operations. It can be modified to $\mathcal{O}(q^{2g+1+\epsilon})$ as $q \to \infty$. 

Daniel Arnold Moldovan, Cihangir Tezcan

Introduction to Weil descent for (hyper)elliptic curves
Gaudry’s algorithm is faster than Pollard’s rho algorithm for small genera, e.g. $g < 10$
- Gaudry’s algorithm is faster than Pollard’s rho algorithm for small genera, e.g. $g < 10$

- For larger $g$, Enge and Gaudry’s algorithm should be used. However, it is infeasible when $q^g$ is very large, e.g. $q^g \approx 2^{1024}$
Gaudry’s algorithm is faster than Pollard’s rho algorithm for small genera, e.g. \( g < 10 \)

For larger \( g \), Enge and Gaudry’s algorithm should be used. However, it is infeasible when \( q^g \) is very large, e.g. \( q^g \approx 2^{1024} \)

Thus, we say that GHS attack is successful if \( q^g < 2^{1024} \) and \( g \neq 1 \). For \( q = 2 \), this means \( m < 11 \) and \( m \neq 1 \).
Gaudry’s algorithm is faster than Pollard’s rho algorithm for small genera, e.g. \( g < 10 \)

For larger \( g \), Enge and Gaudry’s algorithm should be used. However, it is infeasible when \( q^g \) is very large, e.g. \( q^g \approx 2^{1024} \)

Thus, we say that GHS attack is successful if \( q^g < 2^{1024} \) and \( g \neq 1 \). For \( q = 2 \), this means \( m < 11 \) and \( m \neq 1 \)

**Note**

*The failure of the GHS attack does not imply failure of the Weil descent methodology.*
Genus of the Hyperelliptic Curve

The genus $g$ of $C$ is either $2^{m(b)} - 1$ or $2^{m(b)} - 1 - 1$ where $m(b)$ is calculated as follows:

$$m = \dim_{F_2}(\text{Span}_{F_2}\{(1, \beta_0^{1/2}), \ldots, (1, \beta_{n-1}^{1/2})\})$$
Genus of the Hyperelliptic Curve

The genus $g$ of $C$ is either $2^{m(b)-1}$ or $2^{m(b)-1} - 1$ where $m(b)$ is calculated as follows:

$$m = \dim_{\mathbb{F}_2}(\text{Span}_{\mathbb{F}_2}\{(1, \beta_0^{\frac{1}{2}}), ..., (1, \beta_{n-1}^{\frac{1}{2}})\})$$

Lemma

*Let $n$ be an odd prime, and let $t = \text{ord}_n(2)$ be the order of 2 modulo $n$. Let $n = st + 1$. Then $x^n - 1$ factors over $\mathbb{F}_2$ as $x^n - 1 = (x - 1)f_1f_2\ldots f_s$ where $f_i$’s are distinct irreducible polynomials of degree $t$.***
Genus of the Hyperelliptic Curve

The genus $g$ of $C$ is either $2^{m(b)} - 1$ or $2^{m(b)} - 1 - 1$ where $m(b)$ is calculated as follows:

$$m = \dim_{\mathbb{F}_2} (\text{Span}_{\mathbb{F}_2} \{(1, \beta_0^{\frac{1}{2}}), ..., (1, \beta_{n-1}^{\frac{1}{2}})\})$$

Lemma

Let $n$ be an odd prime, and let $t = \text{ord}_n(2)$ be the order of 2 modulo $n$. Let $n = st + 1$. Then $x^n - 1$ factors over $\mathbb{F}_2$ as $x^n - 1 = (x - 1)f_1f_2\ldots f_s$ where $f_i$'s are distinct irreducible polynomials of degree $t$.

Corollary

Let $n$ be an odd prime, and let $t = \text{ord}_n(2)$. Let $n = st + 1$, and let $b \in \mathbb{F}_q^n$. Then $m(b^2) = it + 1$ where $0 \leq i \leq s$. 
Genus of the Hyperelliptic Curve

Definition

We define the smallest attainable value $m(b) > 1$ for $b \in \mathbb{F}_{q^n}$ as $M(n) = \text{ord}_n(2) + 1$ where $n$ is an odd prime.
Genus of the Hyperelliptic Curve

Definition

We define the smallest attainable value \( m(b) > 1 \) for \( b \in \mathbb{F}_{q^n} \) as 
\[
M(n) = \text{ord}_n(2) + 1
\]
where \( n \) is an odd prime.

Remark (Lower bound for \( M(n) \))

Since \( t = \text{ord}_n(2) \geq \lceil \log_2 n \rceil \), we have 
\[
M(n) \geq \lceil \log_2 n \rceil + 1
\]
Genus of the Hyperelliptic Curve

Definition
We define the smallest attainable value $m(b) > 1$ for $b \in \mathbb{F}_{q^n}$ as $M(n) = \text{ord}_n(2) + 1$ where $n$ is an odd prime.

Remark (Lower bound for $M(n)$)
Since $t = \text{ord}_n(2) \geq \lceil \log_2 n \rceil$, we have $M(n) \geq \lceil \log_2 n \rceil + 1$

Note
In practice, for $q = 2$, $n$ is chosen to be a prime number in $[160, 600]$ for elliptic curve cryptographic schemes.
The Weil descent attack

Analysis and Limitations of GHS Attack

Extended GHS Attack

<table>
<thead>
<tr>
<th>n</th>
<th>101</th>
<th>103</th>
<th>107</th>
<th>109</th>
<th>113</th>
<th>127</th>
<th>131</th>
<th>137</th>
<th>139</th>
<th>149</th>
<th>151</th>
<th>157</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>101</td>
<td>52</td>
<td>107</td>
<td>37</td>
<td>29</td>
<td>8</td>
<td>131</td>
<td>137</td>
<td>139</td>
<td>149</td>
<td>16</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>163</th>
<th>167</th>
<th>173</th>
<th>179</th>
<th>181</th>
<th>191</th>
<th>193</th>
<th>197</th>
<th>199</th>
<th>211</th>
<th>223</th>
<th>227</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>163</td>
<td>84</td>
<td>173</td>
<td>179</td>
<td>181</td>
<td>96</td>
<td>97</td>
<td>197</td>
<td>100</td>
<td>211</td>
<td>38</td>
<td>227</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>229</th>
<th>233</th>
<th>239</th>
<th>241</th>
<th>251</th>
<th>257</th>
<th>263</th>
<th>269</th>
<th>271</th>
<th>277</th>
<th>281</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>77</td>
<td>30</td>
<td>120</td>
<td>25</td>
<td>51</td>
<td>17</td>
<td>132</td>
<td>269</td>
<td>136</td>
<td>93</td>
<td>71</td>
<td>95</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>293</th>
<th>307</th>
<th>311</th>
<th>313</th>
<th>317</th>
<th>331</th>
<th>337</th>
<th>347</th>
<th>349</th>
<th>353</th>
<th>359</th>
<th>367</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>293</td>
<td>103</td>
<td>156</td>
<td>157</td>
<td>317</td>
<td>31</td>
<td>22</td>
<td>347</td>
<td>349</td>
<td>89</td>
<td>180</td>
<td>184</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>373</th>
<th>379</th>
<th>383</th>
<th>389</th>
<th>397</th>
<th>401</th>
<th>409</th>
<th>419</th>
<th>421</th>
<th>431</th>
<th>433</th>
<th>439</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>373</td>
<td>379</td>
<td>192</td>
<td>389</td>
<td>45</td>
<td>201</td>
<td>205</td>
<td>419</td>
<td>421</td>
<td>44</td>
<td>73</td>
<td>74</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>443</th>
<th>449</th>
<th>457</th>
<th>461</th>
<th>463</th>
<th>467</th>
<th>479</th>
<th>487</th>
<th>491</th>
<th>499</th>
<th>503</th>
<th>509</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>443</td>
<td>225</td>
<td>77</td>
<td>461</td>
<td>232</td>
<td>467</td>
<td>240</td>
<td>244</td>
<td>491</td>
<td>167</td>
<td>252</td>
<td>509</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>521</th>
<th>523</th>
<th>541</th>
<th>547</th>
<th>557</th>
<th>563</th>
<th>569</th>
<th>571</th>
<th>577</th>
<th>587</th>
<th>593</th>
<th>599</th>
</tr>
</thead>
<tbody>
<tr>
<td>M(n)</td>
<td>261</td>
<td>523</td>
<td>541</td>
<td>547</td>
<td>557</td>
<td>563</td>
<td>285</td>
<td>115</td>
<td>145</td>
<td>587</td>
<td>149</td>
<td>300</td>
</tr>
</tbody>
</table>

**Table:** Values of $M(n)$ for primes $n \in [100, 600]$
Consequences

- GHS attack is infeasible for all elliptic curves defined over $\mathbb{F}_{2^n}$ for prime $n$ in $[160, 600]$
Consequences

- GHS attack is infeasible for all elliptic curves defined over $\mathbb{F}_{2^n}$ for prime $n$ in $[160, 600]$

- Thus, the elliptic curves defined over NIST’s recommended fields $\mathbb{F}_{2^{163}}, \mathbb{F}_{2^{233}}, \mathbb{F}_{2^{283}}, \mathbb{F}_{2^{409}}, \text{ and } \mathbb{F}_{2^{571}}$ are secure against GHS attack
Consequences

- GHS attack is infeasible for all elliptic curves defined over $\mathbb{F}_2^n$ for prime $n$ in $[160, 600]$

- Thus, the elliptic curves defined over NIST’s recommended fields $\mathbb{F}_{2^{163}}, \mathbb{F}_{2^{233}}, \mathbb{F}_{2^{283}}, \mathbb{F}_{2^{409}},$ and $\mathbb{F}_{2^{571}}$ are secure against GHS attack

- Koblitz curves (elliptic curves defined over $\mathbb{F}_2$) are secure against the GHS attack since $m = 1$ for Koblitz curves
Consequences

The field $\mathbb{F}_{2^{155}}$ is used for an elliptic curve group for key agreement in the IPSEC set of protocols (IETF standard). There are 3 ways to apply GHS attack:

1. If $q = 2^{31}$ and $n = 5$, then $t = \text{ord}_5(2) = 4$. Thus $m(b) = 1$ or $5$ $\Rightarrow$ we obtain a hyperelliptic curve of genus 1, 15, or 16 over $\mathbb{F}_{2^{31}}$. Most probably, DLP for such a curve is infeasible.

2. If $q = 2^{5}$ and $n = 31$, then $t = \text{ord}_{31}(2) = 5$ and $s = 6$ $\Rightarrow$ $m(b) = 1, 6, 11, 16, 21, 26, 31$. GHS is successful if $m(b) = 6$. Probability of this event is $\approx 2^{-122}$.

3. If $q = 2$ and $n = 155$, best we can get a hyperelliptic curve of genus 511 or 512. Most probably infeasible.
Consequences

The field $\mathbb{F}_{2^{155}}$ is used for an elliptic curve group for key agreement in the IPSEC set of protocols (IETF standard). There are 3 ways to apply GHS attack:

1. If $q = 2^{31}$ and $n = 5$, then $t = \text{ord}_5(2) = 4$. Thus $m(b)$ is either 1 or 5 $\Rightarrow$ we obtain a hyperelliptic curve of genus 1, 15, or 16 over $\mathbb{F}_{2^{31}}$. Most probably, DLP for such a curve is infeasible.
The field $\mathbb{F}_{2^{155}}$ is used for an elliptic curve group for key agreement in the IPSEC set of protocols (IETF standard). There are 3 ways to apply GHS attack:

1. If $q = 2^{31}$ and $n = 5$, then $t = \text{ord}_5(2) = 4$. Thus $m(b)$ is either 1 or 5 $\Rightarrow$ we obtain a hyperelliptic curve of genus 1, 15, or 16 over $\mathbb{F}_{2^{31}}$. Most probably, DLP for such a curve is infeasible.

2. If $q = 2^5$ and $n = 31$, then $t = \text{ord}_{31}(2) = 5$ and $s = 6 \Rightarrow m(b) = 1, 6, 11, 16, 21, 26, \text{ or } 31$. GHS is successful if $m(b) = 6$. Probability of this event is $\approx \frac{2^{33}}{2^{155}} = 2^{-122}$. 

The Weil descent attack
Analysis and Limitations of GHS Attack
Extended GHS Attack

Consequences
The field $\mathbb{F}_{2^{155}}$ is used for an elliptic curve group for key agreement in the IPSEC set of protocols (IETF standard). There are 3 ways to apply GHS attack:

1. If $q = 2^{31}$ and $n = 5$, then $t = \text{ord}_5(2) = 4$. Thus $m(b)$ is either 1 or 5 $\Rightarrow$ we obtain a hyperelliptic curve of genus 1, 15, or 16 over $\mathbb{F}_{2^{31}}$. Most probably, DLP for such a curve is infeasible.

2. If $q = 2^5$ and $n = 31$, then $t = \text{ord}_{31}(2) = 5$ and $s = 6 \Rightarrow m(b) = 1, 6, 11, 16, 21, 26, \text{ or } 31$. GHS is successful if $m(b) = 6$. Probability of this event is $\approx \frac{2^{33}}{2^{155}} = 2^{-122}$.

3. If $q = 2$ and $n = 155$, best we can get a hyperelliptic curve of genus 511 or 512. Most probably infeasible.
Extended GHS Attack

Definition

An **isogeny** between two elliptic curves $E_1$ and $E_2$ is a surjective morphism $\phi : E_1 \rightarrow E_2$ of curves that maps the infinity point of $E_1$ to the infinity point of $E_2$ (Note that $\#E_1(K) = \#E_2(K)$ for isogenous curves).
Extended GHS Attack

Definition

An **isogeny** between two elliptic curves $E_1$ and $E_2$ is a surjective morphism $\phi : E_1 \rightarrow E_2$ of curves that maps the infinity point of $E_1$ to the infinity point of $E_2$ (Note that $\#E_1(K) = \#E_2(K)$ for isogenous curves).

Idea

For an elliptic curve that is not vulnerable to the GHS attack, find an isogenous curve for which the GHS attack is effective. The ECDLP on the target curve can be transformed into a ECDLP on the isogenous curve.
Extended GHS Attack

Definition

An **isogeny** between two elliptic curves $E_1$ and $E_2$ is a surjective morphism $\phi : E_1 \rightarrow E_2$ of curves that maps the infinity point of $E_1$ to the infinity point of $E_2$ (Note that $\#E_1(K) = \#E_2(K)$ for isogenous curves).

Idea

For an elliptic curve that is not vulnerable to the GHS attack, find an isogenous curve for which the GHS attack is effective. The ECDLP on the target curve can be transformed into a ECDLP on the isogenous curve.

Note

*The Extended GHS Attack applies to fields of composite degree over $\mathbb{F}_2$.***
Extended GHS Attack

Given an elliptic curve $E_1$ over $\mathbb{F}_{q^n}$ with $N = \#E_1(\mathbb{F}_{q^n})$, 
Extended GHS Attack

Given an elliptic curve $E_1$ over $\mathbb{F}_{q^n}$ with $N = \#E_1(\mathbb{F}_{q^n})$,

1. Search over all elliptic curves that GHS is effective until one is found with $N$ points (Time complexity: $O(sq^{t+1}/(n\ell))$)
Extended GHS Attack

Given an elliptic curve $E_1$ over $\mathbb{F}_{q^n}$ with $N = \#E_1(\mathbb{F}_{q^n})$,

1. Search over all elliptic curves that GHS is effective until one is found with $N$ points (Time complexity: $\mathcal{O}(sq^{t+1}/(n\ell))$)

2. Construct an isogeny explicitly ((Average) Time complexity: $\mathcal{O}(q^{n/4+\epsilon})$)
Probability that an elliptic curve defined over $\mathbb{F}_{2^{155}}$ is susceptible to the Extended GHS attack is $\approx 2^{-52}$ (which was $2^{-122}$ for the GHS attack).
Results

Probability that an elliptic curve defined over $\mathbb{F}_{2^{155}}$ is susceptible to the Extended GHS attack is $\approx 2^{-52}$ (which was $2^{-122}$ for the GHS attack).

Note

The IPSEC curve is not isogenous to an elliptic curve that is vulnerable to GHS attack. Hence, it is secure against the Extended GHS attack.
GHS attack does not apply to most of the deployed systems
Conclusion

- GHS attack does not apply to most of the deployed systems

- Further research on Weil descent is required before saying that all elliptic curves over composite fields are weak