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 $0 \leq r \leq \mathrm{ord}(P)$ 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 $0 \leq r \leq \mathrm{ord}(P)$ 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 $0 \leq r \leq \mathrm{ord}(P)$ 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

- P. Gaudry, F.Hess, N.P. Smart, *Constructive and Destructive Facets of Weil Descent on Elliptic curves*, J. Cryptology (2002) 15, 19-46

References

- P. Gaudry, F.Hess, N.P. Smart, *Constructive and Destructive Facets of Weil Descent on Elliptic curves*, J. Cryptology (2002) 15, 19-46
- A. Menezes, M. Qu, *Analysis of the Weil Descent Attack of Gaudry, Hess and Smart*, Lecture Notes in Comput. Sci. (2020), Springer, Berlin, 2001

References

- P. Gaudry, F.Hess, N.P. Smart, *Constructive and Destructive Facets of Weil Descent on Elliptic curves*, J. Cryptology (2002) 15, 19-46
- A. Menezes, M. Qu, *Analysis of the Weil Descent Attack of Gaudry, Hess and Smart*, Lecture Notes in Comput. Sci. (2020), Springer, Berlin, 2001
- S.D. Galbraith, F. Hess, N.P. Smart, *Extending the GHS Weil Descent Attack*, Advances in Cryptology - Eurocrypt 2002, 29-44, Lecture Notes in Comput. Sci. 2332, Springer, Berlin, 2002

Contents

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

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 $\mathrm{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_q)$

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 $\mathrm{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\mathrm{Jac}(C)(\mathbb{F}_q)$ using index calculus

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 $\mathrm{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\mathrm{Jac}(C)(\mathbb{F}_q)$ using index calculus
- Deduce the result of the ECDLP for 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
- Reduce the DLP from E to $\mathrm{Jac}(C)$ by using a map $\varphi : E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_q)$
- Solve the DLP in $\mathrm{Jac}(C)(\mathbb{F}_q)$ 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 $\mathrm{Jac}(C_1)$

Construction of the map φ

- 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 σ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$

Construction of the map φ

- 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 σ 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 φ

- 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 σ 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 $\mathbb{F}_{q^n}$
- Use properties of Jac to obtain a map $\mathrm{Jac}(E) \to \mathrm{Jac}(C)$

Construction of the map φ

- 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 σ 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 $\mathbb{F}_{q^n}$
- Use properties of Jac to obtain a map $\mathrm{Jac}(E) \to \mathrm{Jac}(C)$
- Since E is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$

Construction of the map φ

- 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 σ 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 $\mathbb{F}_{q^n}$
- Use properties of Jac to obtain a map $\mathrm{Jac}(E) \to \mathrm{Jac}(C)$
- Since E is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$
- Combining all these construct a map $E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_{q^n})$

Construction of the map φ

- 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 σ 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 $\mathbb{F}_{q^n}$
- Use properties of Jac to obtain a map $\mathrm{Jac}(E) \to \mathrm{Jac}(C)$
- Since E is an elliptic curve, we have $E \simeq \mathrm{Jac}(E)$
- Combining all these construct a map $E(\mathbb{F}_{q^n}) \to \mathrm{Jac}(C)(\mathbb{F}_{q^n})$
- Go down to $\mathrm{Jac}(C)(\mathbb{F}_q)$ by applying the trace map:

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

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 $\mathcal{O}(q^{2+\epsilon})$, 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 $\mathcal{O}(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard's rho

- GHS is asymptotically faster then Pollard's rho method ($\mathcal{O}(\sqrt{p})$)

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 $\mathcal{O}(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard's rho

- GHS is asymptotically faster then Pollard's rho method $(\mathcal{O}(\sqrt{p}))$
- 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 $\mathcal{O}(q^{2+\epsilon})$, where $r \geq 4$ is fixed and $q \to \infty$.

Comparison with Pollard's rho

- GHS is asymptotically faster then Pollard's rho method ($\mathcal{O}(\sqrt{p})$)
- 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 $x = x_1 + ux_2$, $y = y_1 + uy_2$, $a = a_1 + ua_2$, $b = b_1 + ub_2$, $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$

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 $x = x_1 + ux_2$, $y = y_1 + uy_2$, $a = a_1 + ua_2$, $b = b_1 + ub_2$, $x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2 \in \mathbb{F}_p$
- 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.

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 σ is the Frobenius automorphism of K/k, then W is an abelian variety isomorphic to $E \times E^{\sigma} \times E^{\sigma^2} \times ... \times E^{\sigma^{n-1}}$ 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 $\theta + \theta^2 + \theta^4 + ... + \theta^{2^{n-1}} = 1$

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

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

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

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

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

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

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

- σ can be extended to $K[x, w_0, \ldots, w_{n-1}]$ via $\sigma(x) = x$, $\sigma(w_i) = \sigma(w_{i+1})$, $\sigma(w_{n-1}) = w_0$

Compositum of splitting fields

- Let F_i be the splitting field of the i^{th} equation defining D over $K(x)$. Then the F_is are quadratic 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_is 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 $K(x)$)

Compositum of splitting fields

- Let F_i be the splitting field of the i^{th} equation defining D over $K(x)$. Then the F_is 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_is 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 $[F : K(x)] = 2^m$

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:

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

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:

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

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

$$\begin{array}{ccc} \text{Galois extensions} & \longleftrightarrow & \text{splitting fields of polynomials} \\ \text{of exponent 2 of } K & & \text{of the type } x^2 - x + d,\ d \in K \end{array}$$

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

Computation of m

- We need to compute m because it gives full information on the genus of F
- $m = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, \beta_0^{\frac{1}{2}}), ..., (1, \beta_{n-1}^{\frac{1}{2}})\})$
- The β_is are easy to compute

Computation of m

- We need to compute m because it gives full information on the genus of F
- $m = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, \beta_0^{\frac{1}{2}}), ..., (1, \beta_{n-1}^{\frac{1}{2}})\})$
- The β_is are easy to compute

Exact function field of F

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

Hyperellipticity

- By eliminating variables we obtain $t_i^2 + t_i + \delta_i z + \gamma_i = 0,\ 1 \leq i \leq m-1$ with splitting field L_i.

Hyperellipticity

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

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, ..., L_{m-1} over $K(z)$
- L is a rational subfield of index 2 of F

Hyperellipticity

- By eliminating variables we obtain $t_i^2 + t_i + \delta_i z + \gamma_i = 0,\ 1 \leq i \leq m-1$ with splitting field L_i.
- $F = F_0 L$ with L the compositum of L_1, ..., 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 $K(x)$

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, ..., 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
  $y^2 + h(x)y = f(x)$, $h, f \in K[x]$, $\deg(h) \leq g+1$, $\deg(g) \leq 2g+2$

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, ..., 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 $y^2 + h(x)y = f(x),\ h, f \in K[x],\ \deg(h) \leq g+1,\ \deg(g) \leq 2g+2$

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 $C_1 \to C_2$ of curves gives a relation between the genera of the curves and the degree of the covering (plus some additional information - the ramification indexes)
- 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 σ

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 σ
- Suppose **(*)** **either n is odd or ($m = n$ and $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$)**

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 σ
- Suppose **(*)** **either n is odd or ($m = n$ and $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$)**
- In this case, σ 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 σ
- Suppose **(*)** **either n is odd or ($m = n$ and $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$)**
- In this case, σ can be chosen with order exactly n
- Let F' be the field of elements of F fixed by σ.

$$
\begin{tikzcd}
F \arrow[dr, dash, "n"] \arrow[dd, dash, "2"] & \\
 & F' \arrow[dd, dash, "2"] \\
L \arrow[dr, dash, "n"] \arrow[dd, dash, "2^{m-1}"] & \\
 & L' \arrow[dd, dash, "2^{m-1}"] \\
K(x) \arrow[dr, dash, "n"] \arrow[dd, dash] & \\
 & k(x) \arrow[dd, dash] \\
K \arrow[dr, dash, "n"] & \\
 & k
\end{tikzcd}
$$

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.

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.
- 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 $\mathrm{Jac}(C)(k)$ by using a map $\varphi : E(K) \to \mathrm{Jac}(C)(k)$

Question

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

Question

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

Answer

- It is highly unlikely

Question

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

Answer

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

Question

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

Answer

- It is highly unlikely
- The kernel of the trace map: $\mathrm{Jac}(C)(K) \to \mathrm{Jac}(C)(k)$ 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

1. A. Menezes, M. Qu, *Analysis of the Weil Descent Attack of Gaudry, Hess and Smart*, LNCS 2020, Springer, Berlin, 2001
2. S.D. Galbraith, F. Hess, N.P. Smart, *Extending the GHS Weil Descent Attack*, Eurocrypt 2002, 29-44, LNCS 2332, Springer, Berlin, 2002

Recall

- Let ℓ 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 ℓ 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 ℓ 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 ℓ 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 $\mathcal{O}(g^2 \log^2 q)$ bit operations by Cantor's algorithm.

DLP

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 $\mathcal{O}(g^2 q^{n/2} \log^2 q)$ bit operations.

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

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

DLP

- Gaudry's algorithm is faster than Pollard's rho algorithm for small genera, e.g. $g < 10$

DLP

- 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. $q^g \approx 2^{1024}$

DLP

- 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 $m \neq 1$

DLP

- 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:

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

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:

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

Lemma

*Let n be an odd prime, and let $t =$*ord$_n(2)$ be the order of 2 modulo n. Let $n = st + 1$. Then $x^n - 1$ factors over $\mathbb{F}_2$ as $x^n - 1 = (x-1)f_1 f_2 \dots f_s$ where f_i's are distinct ireducible 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:

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

Lemma

Let n be an odd prime, and let $t = \mathrm{ord}_n(2)$ be the order of 2 modulo n. Let $n = st + 1$. Then $x^n - 1$ factors over $\mathbb{F}_2$ as $x^n - 1 = (x-1)f_1 f_2 \dots f_s$ where f_i's are distinct ireducible polynomials of degree t.

Corollary

Let n be an odd prime, and let $t = \mathrm{ord}_n(2)$. Let $n = st + 1$, and let $b \in \mathbb{F}_{q^n}$. Then $m(b^2) = it + 1$ where $0 \le i \le s$.

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 $M(n) = \mathrm{ord}_n(2) + 1$ where n is an odd prime.

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

Since $t = \mathrm{ord}_n(2) \geq \lceil \log_2 n \rceil$, 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 $M(n) = \mathrm{ord}_n(2) + 1$ where n is an odd prime.

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

Since $t = \mathrm{ord}_n(2) \geq \lceil \log_2 n \rceil$, 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.*

n	101	103	107	109	113	127	131	137	139	149	151	157
M(n)	101	52	107	37	29	8	131	137	139	149	16	53

n	163	167	173	179	181	191	193	197	199	211	223	227
M(n)	163	84	173	179	181	96	97	197	100	211	38	227

n	229	233	239	241	251	257	263	269	271	277	281	283
M(n)	77	30	120	25	51	17	132	269	136	93	71	95

n	293	307	311	313	317	331	337	347	349	353	359	367
M(n)	293	103	156	157	317	31	22	347	349	89	180	184

n	373	379	383	389	397	401	409	419	421	431	433	439
M(n)	373	379	192	389	45	201	205	419	421	44	73	74

n	443	449	457	461	463	467	479	487	491	499	503	509
M(n)	443	225	77	461	232	467	240	244	491	167	252	509

n	521	523	541	547	557	563	569	571	577	587	593	599
M(n)	261	523	541	547	557	563	285	115	145	587	149	300

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 $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{283}}$, $\mathbb{F}_{2^{409}}$, 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 againts 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:

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.

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 $s = 6 \Rightarrow$ $m(b) = 1, 6, 11, 16, 21, 26$, or 31. GHS is successful if $m(b) = 6$. Probability of this event is $\approx \frac{2^{33}}{2^{155}} = 2^{-122}$.

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 $s = 6 \Rightarrow$ $m(b) = 1, 6, 11, 16, 21, 26$, 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 $\phi : E_1 \to E_2$ 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 $\phi : E_1 \to E_2$ 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 $\phi : E_1 \to E_2$ 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: $\mathcal{O}(sq^{t+1}/(n\ell))$)

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: $\mathcal{O}(q^{n/4+\epsilon})$)

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).

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 againts the Extended GHS attack.

Conclusion

- 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