Bern University
of Applied Sciences

A New DDH Secure Group for Applications of ElGamal in Cryptographic Voting Protocols

Rolf Haenni

Verifiable Voting Workshop, Luxembourg, March 22, 2023

DDH Secure Groups for ElGamal

- Prime-order subgroup $\mathbb{G}_q \subset \mathbb{Z}_p^*$ of integers modulo p
  - General case: $p = kq + 1$, for co-factor $k \geq 2$
  - Safe prime: $p = 2q + 1$
- Prime-order subgroup $E_q \subseteq E[\mathbb{F}_p]$ of elliptic curve over $\mathbb{F}_p$
- Prime-order subgroup $F_q \subset \mathbb{F}_{p^k}^*$ of polynomials of degree k over $\mathbb{F}_p$

DDH Secure Groups for ElGamal

- Prime-order subgroup $\mathbb{G}_q \subset \mathbb{Z}_p^*$ of integers modulo p
  - General case: $p = kq + 1$, for co-factor $k \geq 2$
  - Safe prime: $p = 2q + 1$
- Prime-order subgroup $E_q \subseteq E[\mathbb{F}_p]$ of elliptic curve over $\mathbb{F}_p$
- Prime-order subgroup $F_q \subset \mathbb{F}_{p^k}^*$ of polynomials of degree k over $\mathbb{F}_p$

Subgroup of Integers Modulo Safe Prime

- The elements of $\mathbb{G}_q \subset \mathbb{Z}_p^*$ modulo $p = 2q + 1$ are *quadratic residues*:

$$\mathbb{G}_q = \{x^2 \bmod p : 1 \leq x < p\}$$

- Example: $p = 23$, $q = 11$

$\mathbb{Z}_{23}^*$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

$\mathbb{G}_{11}$

1	2	3	4	6	8	9	12	13	16	18

Properties of $\mathbb{G}_q$

- All elements of $\mathbb{G}_q \setminus \{1\}$ are generators
  - 3 is always a generator
  - $4, 9, 16, 25, \ldots$ are always generators
- Subgroup membership
  - Method 1: $x \in \mathbb{G}_q$, iff $x^q \bmod p = 1$
  - Method 2: $x \in \mathbb{G}_q$, iff $\left(\frac{x}{p}\right) = 1$
- Quadratic residues vs. quadratic non-residues
  - $x \in \mathbb{G}_q$ implies $p - x \notin \mathbb{G}_q$
  - $x \notin \mathbb{G}_q$ implies $p - x \in \mathbb{G}_q$

Practical Disadvantages of $\mathbb{G}_q$

- Checking group membership is expensive (1×modexp xor 1×Jacobi symbol)
- Group membership depends on p
  - Selecting generators
  - Generating random group elements
- ElGamal with message space $\mathbb{G}_q$
  - Mapping $\Gamma : \{0,1\}^n \rightarrow \mathbb{G}_q$ for general-purpose messages $M \in \{0,1\}^n$ depends on p
  - Mapping $\Gamma : \mathcal{M} \rightarrow \mathbb{G}_q$ for specific messages $M \in \mathcal{M}$ depends on p
  - Example: prime number encoding of votes

Proposal For a New Group

- Computing absolute values in $\mathbb{Z}_p^*$

$$\operatorname{abs}(x) \stackrel{\text{def.}}{=} \begin{cases} x, & \text{if } 1 \leq x \leq q \\ p - x, & \text{if } q < x < p \end{cases}$$

- Let $\mathbb{Z}_p^+ = \{\operatorname{abs}(x) : x \in \mathbb{Z}_p^*\} = \{1, \ldots, q\}$

1	2	3	4	5	6	7	8	9	10	11

12	13	14	15	16	17	18	19	20	21	22

- Let $x \circ y = \operatorname{abs}(xy \bmod p)$ and $\operatorname{inv}(x) = \operatorname{abs}(x^{-1} \bmod p)$

- $(\mathbb{Z}_p^+, \circ, \operatorname{inv}, 1)$ forms a group, the group of absolute values modulo $p = 2q + 1$

Proposal For a New Group

- Computing absolute values in $\mathbb{Z}_p^*$

$$\mathrm{abs}(x) \overset{\mathrm{def.}}{=} \begin{cases} x, & \text{if } 1 \leq x \leq q \\ p - x, & \text{if } q < x < p \end{cases}$$

- Let $\mathbb{Z}_p^+ = \{\mathrm{abs}(x) : x \in \mathbb{Z}_p^*\} = \{1, \ldots, q\}$

1	2	3	4	5	6	7	8	9	10	11

–11	–10	–9	–8	–7	–6	–5	–4	–3	–2	–1

- Let $x \circ y = \mathrm{abs}(xy \bmod p)$ and $\mathrm{inv}(x) = \mathrm{abs}(x^{-1} \bmod p)$

- $(\mathbb{Z}_p^+, \circ, \mathrm{inv}, 1)$ forms a group, the group of absolute values modulo $p = 2q + 1$

Proposal For a New Group

- Computing absolute values in $\mathbb{Z}_p^*$

$$\mathrm{abs}(x) \stackrel{\text{def.}}{=} \begin{cases} x, & \text{if } 1 \leq x \leq q \\ p - x, & \text{if } q < x < p \end{cases}$$

- Let $\mathbb{Z}_p^+ = \{\mathrm{abs}(x) : x \in \mathbb{Z}_p^*\} = \{1, \ldots, q\}$

1	2	3	4	5	6	7	8	9	10	11

$\mathbb{Z}_{23}^+$

–11	–10	–9	–8	–7	–6	–5	–4	–3	–2	–1

$\mathbb{Z}_{23}^-$

- Let $x \circ y = \mathrm{abs}(xy \bmod p)$ and $\mathrm{inv}(x) = \mathrm{abs}(x^{-1} \bmod p)$

- $(\mathbb{Z}_p^+, \circ, \mathrm{inv}, 1)$ forms a group, the group of absolute values modulo $p = 2q + 1$

Proposal For a New Group

- Computing absolute values in $\mathbb{Z}_p^*$

$$\mathrm{abs}(x) \stackrel{\text{def.}}{=} \begin{cases} x, & \text{if } 1 \leq x \leq q \\ p - x, & \text{if } q < x < p \end{cases}$$

- Let $\mathbb{Z}_p^+ = \{\mathrm{abs}(x) : x \in \mathbb{Z}_p^*\} = \{1, \ldots, q\}$
- Let $x \circ y = \mathrm{abs}(xy \bmod p)$ and $\mathrm{inv}(x) = \mathrm{abs}(x^{-1} \bmod p)$
- $(\mathbb{Z}_p^+, \circ, \mathrm{inv}, 1)$ forms a group, the group of absolute values modulo $p = 2q + 1$

Properties of $\mathbb{Z}_p^+$

- Exponentiations in $\mathbb{Z}_p^+$ can be be computed efficiently as $\mathrm{abs}(x^y \bmod p)$
- From $|\mathbb{Z}_p^+| = |\mathbb{G}_q| = q$, it follows that $\mathbb{Z}_p^+$ is isomorphic to $\mathbb{G}_q$
- The isomorphism can be computed efficiently in both directions
  - $\phi(x) = x^2 \bmod p$, for $x \in \mathbb{Z}_p^+$
  - $\phi^{-1}(y) = \mathrm{abs}(\sqrt{y} \bmod p) = \mathrm{abs}(y^{\frac{q+1}{2}})$, for $y \in \mathbb{G}_q$
- Therefore, if DDH is hard in $\mathbb{G}_q$, it is equally hard in $\mathbb{Z}_p^+$

Properties of $\mathbb{Z}_p^+$

- Exponentiations in $\mathbb{Z}_p^+$ can be be computed efficiently as $\mathrm{abs}(x^y \bmod p)$
- From $|\mathbb{Z}_p^+| = |\mathbb{G}_q| = q$, it follows that $\mathbb{Z}_p^+$ is isomorphic to $\mathbb{G}_q$
- The isomorphism can be computed efficiently in both directions
  - $\phi(x) = x^2 \bmod p$, for $x \in \mathbb{Z}_p^+$
  - $\phi^{-1}(y) = \mathrm{abs}(\sqrt{y} \bmod p) = \mathrm{abs}(y^{\frac{q+1}{2}})$, for $y \in \mathbb{G}_q$
- Therefore, if DDH is hard in $\mathbb{G}_q$, it is equally hard in $\mathbb{Z}_p^+$

Practical Advantages of $\mathbb{Z}_p^+$ Over $\mathbb{G}_q$

- Group membership $x \in \mathbb{Z}_p^+$ can be tested efficiently as $1 \leq x \leq q$
- Since $p < p'$ implies $\mathbb{Z}_p^+ \subset \mathbb{Z}_{p'}^+$, it follows that:
  - $1, 2, 3, 4, 5, \ldots$ are always group elements,
  - $1, 2, 3, 4, 5, \ldots$ are possible random group elements,
  - $2, 3, 4, 5, 6, \ldots$ are always generators,

  independently of p
- General-purpose messages $M \in \{0, 1\}^n$ can be mapped into $\mathbb{Z}_p^+$ by interpreting them as binary numbers (except for 0)
- For specific messages, $\Gamma : \mathcal{M} \rightarrow \mathbb{Z}_p^+$ can be defined independently of p

Conclusion

- From a security perspective, $\mathbb{Z}_p^+$ and $\mathbb{G}_q$ are equivalent (DDH holds)
- Group operation in $\mathbb{Z}_p^+$ is slightly less efficient (but the cost is negligible)
- Membership tests in $\mathbb{Z}_p^+$ are much more efficient
- Plus some other practical advantages
- General recommendation:

Use $\mathbb{Z}_p^+$ instead of $\mathbb{G}_q$ in applications and implementations of ElGamal

Conclusion

- From a security perspective, $\mathbb{Z}_p^+$ and $\mathbb{G}_q$ are equivalent (DDH holds)
- Group operation in $\mathbb{Z}_p^+$ is slightly less efficient (but the cost is negligible)
- Membership tests in $\mathbb{Z}_p^+$ are much more efficient
- Plus some other practical advantages
- General recommendation:

Use $\mathbb{Z}_p^+$ instead of $\mathbb{G}_q$ in applications and implementations of ElGamal